



METADATA FRAMEWORK 6.3.190

Release Notes

Publishing Information

Software version	6.3.190
Document version	45
Publication date	September 27, 2017

Copyright © 2005 - 2017 Varonis Systems Inc.

All rights reserved.

This information shall only be used in conjunction with services contracted for with Varonis Systems, Inc. and shall not be used to the detriment of Varonis Systems, Inc. in any manner. User agrees not to copy, reproduce, sell, license, or transfer this information without prior written consent of Varonis Systems, Inc.

Other brands and products are trademarks of their respective holders.

CONTENTS

Chapter 1: Executive Summary.....	1
Chapter 2: New Enhancements.....	21
DatAdvantage.....	21
Support for SharePoint 2016.....	21
New DatAdvantage Operations.....	21
Restoring Archived Data Per User.....	21
Defining Ownership for an Entire Group.....	21
Eliminating Unnecessary Columns in DatAdvantage Reports.....	22
Removing Tags and Global Flags via Enterprise Manager Role.....	22
Setting Groups as Resource Custodians.....	22
Enhancements to SharePoint Online and OneDrive Capabilities.....	23
Bulk Upload of Tags and Flags for DFS/Logical Paths.....	23
New Log Columns.....	23
Copying Group Members to New Groups.....	23
Tactical Errors Enhancements.....	24
Editing Existing Permission Entries.....	24
Dictionaries View.....	24
Support for UTC.....	25
Support for DFS Aliases.....	25
Keyboard Shortcuts.....	25
Commit API.....	25
Committing Changes on Folders with Broken Inheritance.....	26
Auditing Capabilities for SharePoint Online and OneDrive.....	26
Office 365 Displaying and Marking Guest Links.....	26
Creating a Recognized Folder.....	26
Collection of Directory Service Events.....	26
Platforms Supporting IP Address/Hostname.....	26
DataPrivilege.....	27
DataPrivilege API.....	27
DataPrivilege Windows Extension.....	28
Beta Release.....	28
Support for Server Volumes Configured in Mixed Mode.....	29
Exporting Permissions on Managed Folders.....	29
Separate Mail Settings for DataPrivilege.....	29
DataPrivilege Application Settings.....	30
DataPrivilege Windows Extension.....	30
Web Farm Support.....	31
Direct Permissions and Nested Groups.....	31
DataPrivilege Bulk Upload Utility.....	31
Entitlement Review Search.....	32
Multiple Schedules for Entitlement Reviews.....	32
Unsupported Features.....	32

DataPrivilege Database Schema Converter.....	32
Renaming of the Floor Support Role.....	34
Cancelling Pending Entitlement Review Requests.....	34
Email Link for Mac Computers.....	35
Local Group Management Support.....	35
Multi-Language Support.....	35
DatAlert.....	35
Changes to DatAlert Templates.....	35
DatAlert API.....	36
New DatAlert Placeholders.....	36
Changes to Threat Models.....	36
Disabled or Deleted Threat Models.....	46
DatAlert Template Modification.....	46
New Varonis App for Splunk Template.....	46
Changes to DatAlert Email Templates.....	46
Ability to Define Multiple Syslog and SNMP Servers.....	46
Support for TLS Encryption.....	47
New DatAlert Analytics Threat Model.....	47
DatAlert Integration with Security Management Systems.....	47
Validating Alerts via Timestamps.....	47
DatAlert Web Interface.....	48
New Web Interface Design.....	48
Advanced Search Enhancements.....	70
Managing Alerts.....	70
Exporting to CSV.....	71
Changes to Context Cards.....	71
Watch List Global Flag.....	72
DatAlert Analytics Installation.....	72
Automation Engine.....	72
Automation Engine Beta Release.....	72
Global Access Groups Remediation Module.....	73
Data Transport Engine.....	73
Converting Local Groups to Domain Groups.....	73
Aged Data Retrieval Process.....	74
Copying Non-Sensitive Stale Data Only.....	74
Calculating Results of Copying Files Prior to Execution.....	74
Data Transport Engine Configuration Enhancements.....	74
Renaming Source Folders During Migration.....	74
DCF.....	75
New GDPR Predefined Rules List.....	75
Importing Archived Results from RSA via DCF Lite.....	75
File Scanning Improvements.....	75
Enhancements to Dictionary Types.....	76
Support for Additional File Types - DCF and DatAnswers.....	77
Enhancements to Patterns and Regular Expressions.....	86
Assignment of Global Flags to a Rule.....	86

Rescan Rules without Deleting Results.....	86
Enhancements to DCF Advanced Condition Settings.....	87
Changes to Extended File Properties.....	87
Importing Special Files.....	87
Management Console.....	87
Incremental FileWalk.....	87
Monitoring all Top-level Shares Per Protocol.....	88
Configuring User Feedback and Log Collection.....	88
Privileged Account Configuration Enhancements.....	88
Configuring Reasons for Closing DataAlerts.....	89
Update Manager.....	89
Separate Mail Settings for DataPrivilege.....	89
Migrating NetApp 7-Mode to Cluster Mode.....	89
IDU Service Components - DataAlert Web Server and DataAlert Analytics.....	90
Storing Flattened Events.....	90
Configuration of Network Segments.....	90
Data Loss Notifications.....	90
Resource Monitor Improvements.....	91
Designation of Executive Accounts.....	91
New Jobs.....	91
Configuring Expiration Notifications.....	92
Incremental FileWalk Scheduler.....	92
Installation.....	92
Configuring User Feedback and Log Collection through the Enterprise Installer.....	92
DataAlert Analytics Installation.....	93
Reports.....	94
Changes to Filters.....	94
New Reports in This Version.....	104
Changes to Existing Reports.....	105
Query RESTful API Improvements.....	109
Accessing SharePoint Objects via URL in Reports.....	109
Query RESTful API.....	109
Changes to Report Functionality.....	110
DatAnswers.....	110
Default Searched Languages.....	110
DatAnswers over HTTPS.....	110
Support for Chinese.....	111
Changes to Extended File Properties.....	111
Support for SharePoint Online Items.....	111
Core and Infrastructure.....	111
Windows Server 2016.....	111
Active Directory 2016.....	111
Disk Space Limits.....	111
Access Denied Events on Hitachi NAS Devices.....	111
End of Life for Windows 2008 and 2008 SP1 for DataAlert Analytics.....	112
EMC Unity Support.....	112

CONTENTS

SQL Server 2016.....	112
Changes to Jobs.....	112
Support for Oracle Outside In Technology.....	113
Support for Additional File Types - DCF and DatAnswers.....	114
New Exchange On-Premises Events.....	123
End of Life for SQL Server 2005.....	123
Support for Scalify RING File Servers.....	124
Integration with CyberArk Application Identity Manager.....	124
Support for Linux.....	125
Support for Windows 7 as a File Server.....	125
Change Permission Events on IBM Storwize.....	125
Increased Support for Source IP in Events.....	125
Support for Windows 10 as a File Server.....	127
Support for Dell FluidFS File Systems.....	127
Support for Access Denied Events on EMC.....	127
EMC Isilon Support.....	127
Support for Exchange 2016.....	128
Support for Solaris.....	128
Restricting FileWalk's Schedule.....	128
Licensing.....	128
GDPR Patterns License.....	128
Enhancements to the Automation Engine Evaluation License.....	129
DatAlert Analytics License.....	129
DCF Lite License Enforcement.....	129
License Configuration Changes.....	130
OneDrive for Business License.....	130
Office 365 License Changes.....	130
DatAnswers and DCF License Enhancements.....	131
Upgrade.....	135
Upgrade Flows.....	135
Upgrade - Global Access Groups Remediation Utility.....	152
Agent Upgrade and Data Deduplication.....	153
Documentation.....	153
Noteworthy or Changed Behavior.....	153
Resolved Issues.....	161
Known Issues.....	210

EXECUTIVE SUMMARY

Important: Certain features included in the software may be subject to separate fees. This may apply to features which were initially provided in the software as free-of-charge features.

What's New in 6.3.190

This version of the Metadata Framework is declared generally available, except for the Automation Engine. The Automation Engine remains a beta version.

The version contains only bug fixes. It does not contain any new features.

What's New in 6.3.189

This version of the Metadata Framework is declared generally available, except for the Automation Engine. The Automation Engine remains a beta version.

The version contains only bug fixes. It does not contain any new features.

What's New in 6.3.188

This version of the Metadata Framework is a release candidate (RC) version.

The version contains only bug fixes. It does not contain any new features.

What's New in 6.3.187

This version of the Metadata Framework is a release candidate (RC) version.

The version contains only bug fixes. It does not contain any new features.

What's New in 6.3.186

This version of the Metadata Framework is a beta version.

The version contains only bug fixes. It does not contain any new features.

What's New in 6.3.185

This version of the Metadata Framework is a beta version.

- DatAdvantage
- DataPrivilege
 - New ownership-related API methods enable setting and/or replacing owners and authorizers in DataPrivilege, so that 3rd-party systems can use that API.
 - The Query RESTful API is now renamed to Reports API.
 - The "Managed Folders User Level Permission" report has a new filter:
 - *Groups_Managed_Status* - Filters out folders with managed or unmanaged permission groups. Available only via the Reports API. For details, see the *DatAdvantage Query API Reference Guide*.
- DatAlert
 - This version introduces a new predefined DatAlert template, Varonis LEEF Template, which enables sending alerts to external platforms (e.g., IBM QRadar) via syslog. The template is in Log Event Extended Format (LEEF) format.
- DatAlert Web Interface
 - New icons have been added to the Alerts and Events grids.
 - The *Auto run search* checkbox has been moved to the context menu at the top right of each page.
 - The DatAlert Web Interface now supports the **Back** and **Next** browser buttons, which enables users to navigate backward and forward in their browsing history. In addition, the **Refresh** button is now supported, which enables reloading the current page.
 - The **Feedback** button has been added to all pages, enabling users to provide feedback about the DatAlert Web Interface. In addition, the **Feedback** dialog box displays a link to Varonis Support, enabling users to submit a question or report a bug.
 - The **Select Users/Computers** dialog box has been added to the advanced search to enable selecting one or more users and computers from a list of available entities.
- DCF
 - The DCF has a new set of rules and regular expressions which identify Personally Identifiable Information (PII) for citizens of the European Union countries, in order to help customers comply with General Data Protection Regulation (GDPR). Rules are listed per country, with the name, description, and the accompanying patterns/logic. This content will be provided under a license (GDPR Add-on).
 - When importing archived results from RSA via DCF Lite (DCF Import), the DCF aggregates and displays on the archive file all the hits embedded within the file.
- Management Console
 - Incremental FileWalk now supports NFS protocol.
 - In the Management Console, it is now possible to configure DatAdvantage to detect and monitor automatically all top-level shares per protocol.
 - The Management Console now enables configuring whether users can send feedback to improve the user experience of the Varonis Metadata Framework. The **Feedback and Logs** page has been added to the Configuration menu to support this configuration. This page also enables configuring log collection, replacing the previous **Log Collection** page.

- Installation
 - The Enterprise Installer now includes the **User Feedback** page, which enables configuring whether or not users can send feedback to improve the user experience of the Varonis Metadata Framework.
 - The **Help to Improve the Varonis Metadata Framework** page in the Enterprise Installer has been renamed to **Log Collection**.
- Reports
 - Report 19, the Match Report, displays the match count for a file's matches, and which rule conditions triggered the hit. New filters for this report are:
 - Match Count
 - Condition Type
 - Report 4.f.02 has two new filters:
 - Staleness Method
 - Display Only Top-level Stale Folders
- Licensing
 - The GDPR Patterns license is now available. This license is required to use GDPR predefined patterns and rules in the Data Classification Framework and to retrieve classification results based on GDPR content.
 - With this version, license site administrators can now enforce or remove the limitations defined in the Automation Engine Evaluation license.
- Upgrade
- Noteworthy or Changed Behavior
- Resolved Issues
- Known Issues

What's New in 6.3.173

This version of the Metadata Framework is a beta version.

- DatAdvantage
 - The Varonis SharePoint agent and Management Console now support SharePoint 2016.
 - The *DatAlert Alert Status Changed* and *DatAlert Note Added* operation types were added in this version.
 - The following changes have been made to the DataPrivilege reports exposed by the DatAdvantage Query RESTful API:
 - Managed Folder User Level Permission
 - Managed Folder Permissions
- DataPrivilege
 - New API methods enable creating DataPrivilege supported requests as well as many other folder-related operations.
 - DataPrivilege can now be configured to work over HTTPS.
 - DataPrivilege now supports Traditional Chinese.
 - DataPrivilege now supports NT LAN Manager version 2 (NTLMv2) Microsoft security protocols.

- DatAlert
 - The DatAlert workflow API enables changing the status of alerts and adding notes to them.
 - This version enables closing all alerts that are related to deleted or disabled threat models.
 - A new threat model indicator is introduced, *Personal user of another computer*, used by the Alerts page to inform users if the device that they are using belongs to another user.
 - New threat models were introduced in this version:
 - *Abnormal user behavior: password reset by an administrator followed by access to a computer other than the user's personal computer*
 - *Abnormal user behavior: password reset by an administrator followed by access to a computer to which the user does not normally access*
 - *Abnormal service behavior: unusual amount of logons to personal devices*
 - *Abnormal service behavior: atypical actions performed on mailbox owned by other users*
 - *Abnormal behavior: unusual amount of emails sent to a single recipient*
 - *Abnormal service behavior: service account attempted to access a personal device for the first time*
 - *Abnormal computer behavior: computer account attempted to access a personal device for the first time*
 - *Abnormal access behavior: possible credential stuffing attack from a single source*
 - *Abnormal access behavior: possible distributed credential stuffing attack*
 - *Abnormal service behavior: service account logged on to a personal device for the first time*
 - *Abnormal behavior: unusual amount of logons to personal devices*
 - *Abnormal behavior: accumulative increase in the number of logons to personal devices*
 - *Abnormal behavior: unusual amount of logons to devices*
 - *Abnormal behavior: accumulative increase in the amount of logons to devices*
 - *Abnormal service behavior: unusual amount of devices accessed*
 - *Abnormal service behavior: accumulative increase in amount of devices accessed*
 - *Abnormal computer behavior: unusual amount of devices accessed*
 - *Abnormal computer behavior: accumulative increase in amount of devices accessed*
 - *Abnormal admin behavior: unusual amount of devices accessed*
 - *Abnormal admin behavior: accumulative increase in amount of devices accessed*
 - *Abnormal behavior: unusual amount of devices accessed*
 - *Abnormal behavior: accumulative increase in amount of devices accessed*
 - *Abnormal behavior: unusual amount of public devices accessed*
 - *Abnormal behavior: accumulative amount in number of public devices accessed*
 - *Abnormal behavior: unusual number of authentications to personal devices by end-user account*
 - *Abnormal behavior: accumulative increase in number of authentications to personal devices by end-user account*
 - *Abnormal behavior: unusual number of authentications to devices by end-user account*
 - *Abnormal behavior: accumulative increase in the number of account authentications to devices by end-user account*

- *Abnormal admin behavior: unusual number of authentications to personal devices by admin account*
- *Abnormal admin behavior: accumulative increase in number of authentications to personal devices by admin account*
- *Abnormal admin behavior: unusual number of authentications to devices by admin account*
- *Abnormal admin behavior: accumulative increase in the number of account authentications to devices by admin account*
- *Creation: automatic forwarding of incoming messages on mailbox*
- The default alert template now includes the *Alert Page URL* parameter, enabling users to open the **Alerts** page directly from email or SIEM services.
- A new alert template was created, Varonis App for Splunk, in order to integrate Splunk with Varonis. The template is in CEF format.
- DatAlert Web Interface
 - Context cards have a new look and feel. In addition, the *Threat Model Search Results*, *Category Search Results* and *Day Search Results* context cards are no longer available in the DatAlert Web Interface.
 - Alerts can be managed from the **Alerts** page and the **Alert Info** page.
 - The **Export** button in the **Alerts** and **Events** pages enables exporting table data to a CSV file. It also enables exporting the list of connected entities in the File Servers, Directory Services, Exchange and SharePoint dashboards.
 - The *Alert status* filter now appears at the top of the Alerts dashboard and the **Alerts** page.
 - By default, in the **Alerts** and **Events** pages, the search is now run automatically when performing a basic search, using insights and selecting attributes from the Refine pane. Users can run the search manually by clearing the **Auto run search** checkbox and clicking the **Search** icon.
 - The **Print** icon has been added to the top right of the File Servers, Directory Services, Exchange and SharePoint dashboards to enable printing the widget display.
 - The Top Alerted widgets in the Alerts dashboard have an updated look.
 - The following risk assessment insight has been added to the list of available insights:
 - *Personal computer of another user* - Devices usually used by a specific account were used by another user. This may indicate that the accounts are breached.
 - New columns, filters and refinements have been added in this version of the DatAlert Web Interface.
- Automation Engine
 - Improved global settings functionality in the Global Access Groups Remediation Module. These settings affect all rules, and can be overridden by rule-specific settings.
 - Improved remediation functionality whereby all Global Access Group permissions are remediated, including those used by users for current activities and regardless of the number of users that are using these permissions. In order to preserve active users' permissions, these users are added as members of new permission groups. As a result, any disruption to the organizational flow is eliminated.

- Data Transport Engine
 - In this version, it is possible to convert local groups to domain groups during data transport.
- DCF
 - The file scanning functionality now enables extracting content from files without file extensions (configurable per file server), and introduces the ability to determine an unknown file extension through analyzing the file header.
 - Dictionaries now must be assigned to a product, currently either DatAlert or the DCF, thus impacting the available filters.
 - The DCF and DatAnswers now support the email file types .eml and .msg.
 - The *US Passport Number* pattern has been added in this version.
 - A number of keywords were added to the DE Driver's License number pattern.
- Management Console
 - The Management Console now enables editing account classification information in an exported CSV file and importing the edited file back into the Management Console. Additional changes have been made to the configuration of privileged user and group accounts.
 - This version of the Management Console now enables configuring valid reasons for disabling or deleting alerts generated by DatAlert.
- Reports
 - Report capping is now applied only to reports.
 - Report 4.a.01 has a new filter:
 - *Exclude permissions granted by groups* - Filters out selected groups and irrelevant entries from effective permissions calculation in order to focus on relevant users and groups.
 - Report 4.b.01, User or Group Permissions for Directory has a new column:
 - *Assigned Owner*
 - In Report 4n, Share Discovery Report, the Monitored in DatAdvantage column has new values:
 - *Server Not Monitored, Share Not Monitored*
 - *Server Monitored, Share Monitored*
 - *Server Monitored, Share Not Monitored*
 - Report 18.a.01, Global Access Groups - Run Summary - Execution, has new columns:
 - *Actual New Created Groups*
 - *Actual Remediated Unique Folders*
 - *Actual Remediated Unique Global Access Groups Permissions*
 - *Expected New Created Groups*
 - *Expected Remediated Unique Folders*
 - *Expected Remediated Unique Global Access Groups Permissions*
 - *Max Members in a Group*
 - *Max Groups for a User*
 - *Method*
 - *Prevented Access Errors*
 - *Actual Added New Group Permissions*

- *Actual Deleted New Groups*
- *Actual Removed New Group Permissions*
- *Actual Restored Unique Global Access Groups Permissions*
- *Actual Rolled Back Folders*
- *Actual Rolled Back Unique Folders*
- Report 18.a.02, Global Access Groups - Run Summary - Rollback, has new columns:
 - *Actual Added New Group Permissions*
 - *Actual Created New Groups*
 - *Actual Deleted New Groups*
 - *Actual Remediated Unique Folders*
 - *Actual Removed New Group Permissions*
 - *Actual Restored Unique Global Access Groups Permissions*
 - *Actual Rolled Back Folders*
 - *Actual Rolled Back Unique Folders*
- Report 18.b.01, Global Access Groups - Run Errors by Rule, has new columns:
 - *Method*
 - *Action Details*
- Report 18.c.01, Global Access Groups - Folders Remediated by Rule, has new columns:
 - *Members in New Groups*
 - *New Permitted Groups*
 - *Expected Remediated Global Access Groups Permissions* was changed to *Total Number of Unique Global Access Groups Permissions in Scope*
- Report 18.d.01, Global Access Groups - Permissions Handled by Rule, has new columns:
 - *Method*
 - *Permitted Groups Name*
 - *Rule Type*
 - *Rule Creator*
 - *Rule Description*
 - *Rule Name*
- Report 18.e.01, Global Access Groups - Rule Snapshot, has new columns:
 - *Group Limitations*
 - *Log off Waiting Period*
 - *Method*
 - *New Groups Details*
 - *New Groups Permission Mapping*
 - *User Memberships Limitations*

- Additional enhancements to the Query RESTful API are as follows:
 - For use in queries, the API documentation now lists the supported filter values for DataPrivilege and DataAdvantage. Also included are how the filters are displayed in the UI, and how they must be written in the API query.
 - A new section is provided which provides sample code (C#) and describes how to use the API. Procedures include Accessing the Sample Code, Updating the NuGet Resource, and Running the Sample Code.
- Additional new filters for this version are as follows:
 - *Actual added new group permissions*
 - *Actual deleted new groups*
 - *Actual new created groups*
 - *Actual remediated unique folders*
 - *Actual remediated unique Global Access Groups permissions*
 - *Actual removed new group permissions*
 - *Actual restored unique global access groups permissions*
 - *Actual rolled back unique folders*
 - *Execution end date*
 - *Expected new created groups*
 - *Expected remediated unique folders*
 - *Expected remediated unique Global Access Groups permissions*
 - *Max groups for a user*
 - *Max members in a group*
 - *Members in new groups*
 - *Method*
 - *New permitted groups*
 - *Total number of unique global access groups permissions in scope*
 - *Total user access errors*
- Core and Infrastructure
 - This version adds support for Windows Server 2016, for both IDU Server installation and as a monitored file server.
 - This version adds support for Microsoft Active Directory 2016, for both IDU Server installation and as a monitored file server (directory services).
 - In this version, disk space is calculated separately for scopes and reports.
 - This version provides support for Access Denied events on Hitachi NAS devices.
- Upgrade
- Noteworthy or Changed Behavior
- Resolved Issues
- Known Issues

What's New in 6.3.164

This version of the Metadata Framework is declared generally available, except for the Automation Engine. The Automation Engine remains a beta version.

- Upgrade - Although upgrade from 6.2.8x is supported, 6.3.163 only includes content up to 6.2.7x. It does not include 6.2.8x.

What's New in 6.3.163

This version of the Metadata Framework is declared generally available, except for the Automation Engine. The Automation Engine remains a beta version.

- Upgrade - Although upgrade from 6.2.8x is supported, 6.3.163 only includes content up to 6.2.7x. It does not include 6.2.8x.

What's New in 6.3.162

This version of the Metadata Framework is declared generally available, except for the Automation Engine. The Automation Engine remains a beta version.

- Upgrade - Although upgrade from 6.2.8x is supported, 6.3.162 only includes content up to 6.2.7x. It does not include 6.2.8x.

What's New in 6.3.161

This version of the Metadata Framework is declared generally available, except for the Automation Engine. The Automation Engine remains a beta version.

- Upgrade - Although upgrade from 6.2.8x is supported, 6.3.161 only includes content up to 6.2.7x. It does not include 6.2.8x.

What's New in 6.3.160

This version of the Metadata Framework is a release candidate, except for the Automation Engine. The Automation Engine remains a beta version.

- DataPrivilege
 - DataPrivilege now supports NT LAN Manager version 2 (NTLMv2) Microsoft security protocols.
- Core
 - The Metadata Framework Exchange agent for Exchange 2016 is now generally available (GA).
 - Isilon OneFS 8.1 is now supported.
- Upgrade - Although upgrade from 6.2.8x is supported, 6.3.160 only includes content up to 6.2.7x. It does not include 6.2.8x.

What's New in 6.3.157

- DataPrivilege
 - In this version, DataPrivilege is declared a Release Candidate.

What's New in 6.3.154

- Core
 - This version provides support for NetApp CM 9.1.
 - Bug fixes

What's New in 6.3.153

- DatAdvantage
 - DatAdvantage now provides the ability to define ownership for an entire group, in addition to per user. This option reduces the logistics of managing ownership changes.
 - Users assigned to the Enterprise Manager role can clear tags and global flags attached by other DatAdvantage users, including those also assigned to the Enterprise Manager role.
 - Beginning in this version, when a DatAdvantage report's results exceed the maximum limit configured in the Management Console, and a CSV dump file is created, the CSV file will include only the selected columns from the report template. This potentially reduces the size of the generated reports.
 - DatAdvantage now provides the ability to restore only the data for specific users for a specific time range.
 - The Global Access Groups Permissions Remediation Module includes new functionality such as notifications creation for both global-level rules or a single rule, and improved ability to define remediation scope.
- DataPrivilege

Important: In this version, DataPrivilege remains a beta release.

- DataPrivilege provides support for server volumes configured as both CIFS and NFS, also called *mixed mode*.
- Integrated - Permissions reports can now be generated directly from the main Permissions pane. It is also possible to customize the content of email notifications regarding exported permissions as needed. This feature is disabled by default.
- In this version, the Management Console enables configuring separate mail settings for DataPrivilege.
- Changes to application settings
 - *Set the permissions to be exported* - The name has been changed to *Set the view mode for export permissions*.
 - *New - Allow owners to copy permissions when making a folder protected* - Enables owners and authorizers to copy permissions from the parent folder to the protected folder.

- DatAlert
 - DatAlerts can now be generated upon the addition or removal of forward delivery options in Exchange file servers.
 - New placeholders have been added to the predefined alert templates and to the list of optional placeholders in the **Add Alert Template** window.
 - The default alert template now includes the Event status parameter.
 - This version provides a number of enhancements to the DatAlert and DatAlert Analytics email templates.
- DatAlert Web Interface
 - The DatAlert Web Interface introduces the **Alert Info** page, which enables investigating specific alerts.
 - New dashboards provide aggregated metric data for the selected scope:
 - *File Servers*
 - *Directory Services*
 - *Exchange*
 - *SharePoint*
 - The previous dashboard has been renamed to *Alerts Dashboard*.
 - The Alerts dashboard now displays the Top Alerted Devices panel, which provides a list of up to five top alerted devices matching the search criteria specified and sorted by the number of alerts.
 - The Device Search Results context card has been added, to enable viewing data about the device involved in the alert.
 - The Watch List flag is a unique global flag that enables keeping track of specified users at a glance.
- Data Transport Engine
 - Beginning in this version, it is now possible to copy only the non-sensitive files of a folder.
 - In order to prevent users from modifying archived files, the Data Transport Engine now provides a dedicated permissions mapping per rule so that administrators will be able to reduce permissions while archiving the data.
- Management Console
 - In this version, the Management Console enables configuring separate mail settings for DataPrivilege.
 - It is now possible to migrate from NetApp 7-Mode to Cluster Mode via the NetApp Migration tool (7MTT), enabling customers to continue working with the existing Shadow databases without the need to re-add all file servers.
 - With this version, the Management Console and Enterprise Installer enable installing and configuring the DatAlert Web Server component. Additionally, the DatAlert and DatAlert Analytics component has been renamed to *DatAlert Analytics* to enable installing and configuring DatAlert Analytics separately.
 - The Management Console now enables storing flattened events to enhance the overall performance in the DatAlert Web Interface. The DatAlert Web Server component must be installed to enable this feature.

- It is now possible to configure network segments and exclude specific segments from IP resolving.
- The Management Console now includes an Update Manager tab for deploying Varonis updates for each component, server, and client application.
- Reports
- DatAnswers
- Core and Infrastructure
 - This version adds support for EMC Unity 4.1 and Unity Family 300-600, including events.
 - This version adds support for SQL Server 2016.
 - In this version, the DatAlert Analytics jobs have been changed. A number of jobs have been added, and others have been removed.
 - Microsoft Access and Open Office file types are now scanned using Oracle Outside In Technology instead of iFilters.
 - The following Exchange On-Premises events are now supported:
 - *Mailbox forward delivery option added*
 - *Mailbox forward delivery option removed*
- Licensing
- Upgrade
 - The Global Access Group rules from version 6.3.10x are not supported in the upgrade to 6.3.15x. Rules that were created in 6.3.10x must be deleted before the upgrade.
- Documentation
 - This version introduces the *DatAlert Web Interface Triage Guide*. This document provides a recommended workflow scenario for conducting a full alert investigation in the DatAlert Web Interface. It triages the process of identifying the threats which require immediate attention and the steps to take while investigating them.
- Noteworthy or Changed Behavior
- Resolved Issues
- Known Issues

What's New in 6.3.102

Version 6.3.102 includes both 6.2.50 and 6.3.50. This means it includes DatAlert Analytics.

- DatAdvantage
 - It is now possible to assign groups as resource custodians to grant all users in the group custodian privileges on the file server. The **Set Ownership over Entities** dialog box now enables adding groups as custodians on file servers only.
 - With this version, several enhancements have been made to SharePoint Online and OneDrive capabilities.
 - Users who work with DFS/logical paths can upload flags and tags based on DFS/logical paths rather than only physical paths.
 - For files with guest links, it is now possible to remove guest link permissions for Anonymous Logon built-in groups.
 - This version introduces new events metadata, by resolving a device's IP address into a hostname that is more human-readable and more easily monitored in a DHCP environment.

- When new groups are created, it is now possible to add members of other groups to the new group. It is possible to select whether all the direct and nested user and computer members of another group will be added as direct members to the new group, or whether the membership hierarchy of another group will be added as is as members of the new group, thus preserving the group members hierarchy. It is also possible to add members of several groups to the new group. If the new group is created with permissions to a folder, it is possible to easily add already permitted users (via other groups) to be members of the new group.
- The Global Access Groups Remediation Module enables IT to locate folders where global access permissions are not in use and safely remove (remediate) those permissions. This process reduces the security risk to the organization while avoiding any disruption to the organization's business processes.
- The synchronization button on the status bar has been changed from **Synchronization** to **Calculate Access Errors**. The functionality remains the same.
- Administrators can now either allow or deny users with edit/commit role to perform commit operations on folders with broken inheritance. If the administrator allows this ability, then each user can select whether to perform the commit operation on such folders or avoid doing so.
- Tactical error enhancements:
 - In the Work Area, the Errors pane has been renamed to Expected Access Errors and contains new columns.
 - The Permission Sources window contains a new tab, Permission Sources Causing Access Errors, displaying information about edited permissions.
- Integrated - When editing an existing permission entry in the Group Creation Wizard, it is now possible to select the objects to which the permissions will be applied. This feature is only available for Windows file servers.
- Integrated - The Dictionaries tab has been moved from the DCF and DW Configuration window to a window of its own, accessible through the Tools menu.
- Integrated - In the log, times are now normalized to UTC.
- Integrated - CNAME aliases for file servers are now supported in DFS management.
- DataPrivilege
 - This version introduces the DataPrivilege Windows Extension, which enables users to create permission requests directly from the file system.
 - Installation on web farms is supported in this version.
 - It is possible to grant folder permissions to a group nested within another group, if the parent group has direct permission on the folder.
 - In the Excel data file, the Bulk Upload Utility now includes a separation in managed folders between Windows and SharePoint.
 - Integrated - It is now possible to search for entitlement reviews according to specific folder names, group names or rule names.
 - Integrated - Multiple entitlement review schedules are now available for groups too.

- DatAlert
 - This version introduces numerous changes to threat models, including name changes as well as changes in severity and category. In addition, it introduces two new threat models.
 - Two new placeholders, Device Name and Device IP Address, were added to Alerts, and also appear in predefined alerts templates (replacing the existing IP/Hostname placeholder).
 - Multiple syslog and SNMP servers can be configured.
 - This version provides support for the TLS encryption protocol, for email sent by DatAlert.
 - Integrated - In this version, DatAlert includes a predefined alert template that complies with the CEF format, to enable sending DatAlerts to HP ArcSight via Syslog.
- DatAlert Web UI
 - The DatAlert Web Interface has been redesigned. The new design includes:
 - Dashboard view
 - Analytics view
 - Events view
 - Alerts view
 - Changes to columns, filters and refinements
 - Complete event log.
 - Insights and refinements.
 - Links to launch the DatAlert Web Interface from DatAdvantage and DatAlert
- Management Console
 - The Data Loss Notifications feature now includes the ability to define the frequency of the email notifications, and define different rules for different sets of file servers. Each file server can appear in a single set only. A notification will not be sent for file servers that are predefined as excluded.
 - Several features were added to improve the resource monitor, including enabling users to decide which shares can be ignored and hence not be the subject of notifications by the resource monitor.
 - Integrated - This version enables identifying *executive accounts* during discovery of privileged accounts.
 - Integrated - A number of new jobs have been added to the *DatAlert Analytics* jobs category in the Management Console.
- DCF
 - This version provides the ability to assign one or more global flags to files based on DCF rule criteria.
 - It is now possible to update DCF rules and patterns without causing an automatic rescan.
 - The DCF now enables limiting the search to specific file parts or locations in Microsoft Office files, Excel files or hyperlink addresses.
 - Integrated - Several enhancements have been made to patterns and regular expressions.
- Data Transport Engine
 - A new ability has been added to the Data Transport Engine that will perform a "dry run", meaning it will calculate the results of copying files before execution. This function scans

the file server (not the database), thereby providing a more accurate estimation of copied data.

- Integrated - With this version, the Data Transport Engine now copies unique as well as inherited permission entries from the source to the destination.
- Reports
 - A new filter has been added to reports 3b, 4a, 4b, 4d, 4j, and 6b, which filters according to users and computers listed in a CSV file.
 - Report 5a has new columns:
 - *Permission Source*
 - *Current Permissions via Source*
 - *Current Flags via Source*
 - *Recommended Permissions via Source*
 - *Recommended Flags via Source*
 - *Current Effective Permissions*
 - *Recommended Effective Permissions*
 - *Missing Permission Required by Events*
 - *Access Path of Folder with Permission Change*
 - *Time of Permission Change*
 - *Change By*
 - *Change Description*
 - Report 5a has new filters:
 - *Current permissions via source*
 - *Recommended permissions via source*
 - *Current effective permissions*
 - *Recommended effective permissions*
 - *Missing permission required by events*
 - *Access path of folder with permission change*
 - *Change description*
 - *Permission source*
 - *Change source* (also for 5b and 5c)
 - *Data Transport Engine rule* (also for 5b and 5c)
 - Report 5a has changed filters:
 - *Change by* - Filter category is now *Changed by*.
 - *Date* - renamed to *Time of Permission Change*.
 - In some reports, the access path filter now includes the equals operator, with an option to search in all child objects. The affected reports are 1a, 2a, 4a, 4b, 4f, 4j, 12e, 12d, 12l, and 7b.
 - The following have been added to reports 1a and 1b under columns and additional columns to replace the currently-inactive IP Address Hostname:
 - *Device Name*
 - *Device IP Address*

- The following report templates are new in this version of DatAdvantage:
 - *Report 18.a.01, Global Access Groups- Run Summary*
 - *Report 18.b.01, Global Access Groups - Run Errors By Rule*
 - *Report 18.c.01, Global Access Groups - Folders Remediated by Rule*
 - *Report 18.d.01, Global Access Groups - Permissions Handled By Rule*
 - *Report 18.e.01, Global Access Groups - Rule Snapshot*
- Integrated - It is now possible to access SharePoint content (files and folders) directly from reports 4.f.1 and 4.g.1 via a valid URL.
- Integrated - The DatAdvantage Reporting API provides customers with restful APIs that enable accessing and extracting data from DatAdvantage.
- Integrated - Report subscriptions can now be exported to the XLSX format.
- Integrated - The column headers in the subscription CSV files now match those of reports generated in the UI.
- Integrated - Data-driven subscriptions now support Traditional Chinese.
- Core
 - **SQL Server 2005 has reached its end of life. It is no longer possible to install or upgrade the Metadata Framework using this SQL version.**
 - Scalify RING 5.0.6 is now supported.
 - CyberArk Application Identity Manager is now used to manage all passwords required by the user accounts that are used by DatAdvantage and DataPrivilege for daily work.
 - Several new Linux flavors are supported.
 - Windows 7 is now supported as a file server.
 - To increase support for Oracle Outside In, a number of additional file types are now supported by the DCF and DatAnswers.
 - Change Permission events are supported on IBM Storwize V7000.
 - Integrated - This version provides increased support for the source IP in events.
- Licensing
 - DatAlert Analytics now requires a separate license from standard DatAlert.
 - This version provides license enforcement improvements to the DCF Lite license.
 - With this version, the **License Configuration** page of the Varonis Setup Wizard now enables entering the ID of the customer for validation purposes. It is possible to enter either the customer ID or email.
 - OneDrive for Business now requires a separate license from the SharePoint Online license.

What's New in 6.3.50

Version 6.3.50 is based on version 6.2.10. Therefore, only the original set of predefined DatAlert rules is available. DatAlert Analytics will be available in 6.3 in the future.

- DatAdvantage
 - This version provides keyboard shortcuts in DatAdvantage and its sub-products.
 - The new Commit API enables creating commit operations and transactions.
 - Changes on folders with broken inheritance can now be committed.
 - Auditing capabilities have been added for SharePoint Online and OneDrive.

- SharePoint Online and OneDrive now mark guest links and files with external users as special files.
- It is now possible to create a folder directly from the DatAdvantage interface that will be automatically recognized.
- The Full FileWalk schedule functionality is now available through the regular job scheduling, via the Edit Schedule button in the Jobs grid.
- Directory service events generated by unresolved entities can now be collected and presented in the UI.
- DataPrivilege
 - The new DataPrivilege Schema Converter enables upgrade from DataPrivilege versions that do not support SharePoint to versions that do.
 - The Bulk Upload Utility is supported in this version.
 - The *Floor Support* role has been renamed to *Request Supervisor*.
 - This version provides support for Japanese, Portuguese (Brazil) and Spanish (Latin America).
 - Changes to application settings
 - Integrated - *Allow folder owners to edit names of new groups*
 - Integrated - It is now possible for administrators to cancel pending entitlement review requests.
 - Integrated - The Entitlement Review Configuration page now enables selecting all entities for various actions.
 - Integrated - DataPrivilege email templates now include a <MacPCLink> placeholder, to enable using Mac directory paths in email notifications.
 - Integrated - In this version, DataPrivilege provides separate default entitlement review schedules for different scopes of folders, as well as the ability to define additional scopes and schedules for folders.
 - Integrated - It is now possible to manage local users and groups. Additionally, users can now create group membership requests for local groups. This feature is disabled by default.
- DatAlert
 - A new timestamp function was added that validates each alert during the file server scan process, thereby increasing the scan's efficiency.
- Management Console
 - It is now possible to configure the products for which to display an indication when a platform expires. By default, license expiration notifications are displayed throughout the Management Console for expired platforms.
- DCF
 - Extended file properties are now defined only in the Management Console, not on the Advanced page of the DCF and DatAnswers Configuration window.
 - A new timestamp function was added that validates each alert during the file server scan process.
 - With this version, customers who want to import special files must purchase a DCF or DCF Lite license. In addition, it is no longer possible to import special files from platforms that are not supported by the DCF (e.g., Exchange).

- Data Transport Engine
 - It is now possible to rename source folders while migrating them to destination folders according to a predefined renaming mapping table.
- Reports
 - The following filters have been added in this version:
 - *Access path of folder with permission change*
 - *Account type in size calculation*
 - *Calculate group size*
 - *Calculate group size by direct members*
 - *Change description*
 - *Change source*
 - *Changed AD property name*
 - *Current effective permissions*
 - *Current permissions via source*
 - *Data Transport Engine rule*
 - *Dell access paths*
 - *externalUserShareSentToEmailAddress*
 - *Group size % (out of domain users)*
 - *Group size % (out of all users)*
 - *Hide global access groups*
 - *Includes guest link*
 - *Is Azure external user*
 - *No. of domain members*
 - *No. of group members*
 - *No. of group members from external domains*
 - *Permitted entity name*
 - *Recommended effective permissions*
 - *Recommended permissions via source*
 - *Removed global access groups permissions*
 - *Search scope*
 - *Shared externally*
 - *Total number of added permissions*
 - *Total number of folders with broken inheritance in scope*
 - *Total number of folders with unique permissions of global access groups in scope*
 - *Total number of new folders*
 - *Total number of new groups*
 - *Total number of permissions with broken inheritance*
 - *Total number of preserved permissions*
 - *Total number of remediated folders*
 - *Total number of removed permissions*
 - *Total number of repaired folders*
 - *Total number of repaired permissions*

- *Total number of run errors*
- *Total number of unique global access groups permissions in scope*
- *Total user access error*
- Category 3 has been renamed to *Group Membership*.
- The following additional columns have been added to report 15a:
 - *Added Folder Name*
 - *Search Scope*
- *No. of Enabled Users with Password that Never Expires* can be added as an additional column to reports 14d and 14e.
- The following report templates are new in this version of DatAdvantage:
 - *Report 3.d.02, Large Groups*
 - *Report 17.a.01, Broken Inheritance Repair - Run Summary*
 - *Report 17.b.01, Broken Inheritance Repair - Run Errors By Rule*
 - *Report 17.c.01, Broken Inheritance Repair - Folders Repaired by Rules*
 - *Report 17.d.01, Broken Inheritance Repair - Folder Permissions Handled By Rule*
 - *Report 17.e.01, Broken Inheritance Repair - Rule Snapshot*
- **DatAnswers**
 - By default, the searched languages are those configured in an individual user's browser.
 - DatAnswers can now be configured over HTTPS.
 - This version supports searching in Chinese.
 - Extended file properties are now defined only in the Management Console, not through the DCF and DatAnswers Configuration window.
 - DatAnswers now supports selecting scopes for SharePoint Online items, such as document libraries, sites, lists and OneDrive for Business personal sites.
- **Core and Infrastructure**
 - This version supports Windows 10 x64 as a file server.
 - This version provides support for Dell FluidFS 6.2 file systems.
 - Access Denied CIFS events are now supported on EMC Celerra/VNX servers.
 - This version provides support for EMC Isilon 8.0.x file servers, including support for NFS events.
 - Microsoft Office and PDF file types are now scanned using Oracle Outside In Technology instead of iFilters.
 - This version provides beta support for Exchange 2016.
 - This version provides support for Linux Red Hat 6, 2.6.32-573.3.1.el6.x86_64 and Ubuntu 12.04 kernel 3.2.0-83-generic 64 bit.
 - This version adds support for sparc on Solaris 11.
 - In this version, FileWalk's run schedule can be restricted to specific hours.

- Licensing
 - With this version, DCF and DatAnswers licenses can now be installed per platform.
 - DatAnswers can now be installed without a valid DatAdvantage license.
 - With this version, the following licenses are now available:
 - SharePoint Online - Full
 - OneDrive - Full
 - DatAnswers - SharePoint Online
 - DatAnswers - OneDrive

The SharePoint Online and OneDrive full licenses include auditing and event collection capabilities. These licenses are separate from the Office 365 Lite licenses, which provide bi-directional visibility only, and must be purchased separately. A full Office 365 license can be purchased only if the corresponding Office 365 Lite license is purchased.

- Upgrade
- Noteworthy or Changed Behavior
- Resolved Issues
- Known Issues

2

NEW ENHANCEMENTS

DatAdvantage

Support for SharePoint 2016

6.3.173

The Varonis SharePoint agent and Management Console now support SharePoint 2016. The support includes: FileWalk and Permissions visibility, auditing events and Real-time (RT) alerts, scanning content with DCF and the ability to commit changes, Data Transport Engine, DataPrivilege, and Ownership.

New DatAdvantage Operations

6.3.173

With this version, the following DatAdvantage operations are now audited:

Operation Type	Subcategory	Mapping To Operation Category Filter
DatAlert Alert Status Changed	DatAlert	Changed
DatAlert Note Added	DatAlert	Added

Restoring Archived Data Per User

6.3.153

DatAdvantage now provides the ability to restore only the archived data (events and statistics) for specific users for a specific time range, in addition to the option to restore the whole file server's data. This option can be used if only archived data of a particular user or several users is needed and will require less storage.

Defining Ownership for an Entire Group

6.3.153

DatAdvantage now provides the ability to define ownership for an entire group, in addition to per user. This option reduces the logistics of managing ownership changes. A group - and not just a user - can also have ownership of both domains and file servers. Assigning ownership to a group reduces the logistics of managing ownership changes.

Eliminating Unnecessary Columns in DatAdvantage Reports

6.3.153

When a DatAdvantage report's results exceed the maximum limit configured in the Management Console, and a CSV dump file is created, the CSV file will include only the selected columns from the report template. This potentially reduces the size of the generated reports.

Removing Tags and Global Flags via Enterprise Manager Role

6.3.153

Users assigned to the Enterprise Manager role can clear tags and global flags attached by other DatAdvantage users, including those also assigned to the Enterprise Manager role.

Setting Groups as Resource Custodians

6.3.102

With this version, it is now possible to assign groups as resource custodians to grant all users in the group custodian privileges on the file server. Security or distribution groups can be defined as custodians. Abstract, global or virtual groups cannot be defined as custodians.

If a user is a folder owner on the resource, the user can also be defined as a custodian. In this case, the user is limited to custodian privileges only on the file server.

To support this enhancement, the **Set Ownership over Entities** dialog box now enables adding groups as custodians on file servers only.

Data-Driven Subscriptions

The Data-Driven Settings area of the Subscription Form now enables selecting groups which are defined as resource custodians. If a group is selected, the subscription will be sent to all members in the group. Managers of group members will also receive the subscription, enabling them to view information regarding all the data for which the user is ultimately responsible.

Groups defined as resource custodians can be selected only if one of the following options is selected from the Data-Driven Settings area:

- *Selected recipients*
- *All owners*

If the *Recipients by rule* option is selected, groups defined as custodians cannot be selected.

Reports

Additional report filters were added to report 4f to support this new enhancement. See [Changes to Filters](#) for more information.

Enhancements to SharePoint Online and OneDrive Capabilities

6.3.102

With this version, several enhancements have been made to SharePoint Online and OneDrive capabilities. The following activities can now be performed:

- Commit changes - For SharePoint Online and OneDrive directories and files
- View commit history
- Add, remove and edit permissions
- Add, remove and edit permission levels - Relevant only for SharePoint Online site collections
- Add protection to a directory or file
- Remove protection from directories and files
- Create new folders in the Work Area

Changes have been made throughout the DatAdvantage UI to support these enhancements. For example, the **Change Management and Commit** window has been optimized to enable managing changes and commit processes for SharePoint Online and OneDrive. Relevant reports now display results for SharePoint Online and OneDrive file servers.

In addition, for files with guest links, it is now possible to remove guest link permissions for Anonymous Logon built-in groups. The following Anonymous permissions levels are displayed for SharePoint Online and OneDrive in the **Edit Permissions** window:

- *Guest Link Edit*
- *Guest Link View*

Bulk Upload of Tags and Flags for DFS/Logical Paths

6.3.102

Users who work with DFS/logical paths can upload flags and tags based on DFS/logical paths rather than only physical paths.

New Log Columns

6.3.102

The IP address/hostname column in the Log has been split into two separate columns, Device Name and Device IP Address.

- Device IP - The IP address of the user from which the event originated.
- Device Name - The resolved hostname of the Device IP, from which the event originated.

Copying Group Members to New Groups

6.3.102

When new groups are created, it is now possible to add members of other groups to the new group. It is possible to select whether all the direct and nested user and computer members of another group will be added as direct members to the new group, or whether the membership hierarchy of another group will be added as is as members of the new group, thus preserving the group members hierarchy. It is also possible to add members of several groups to the new

group. If the new group is created with permissions to a folder, it is possible to easily add already permitted users (via other groups) to be members of the new group.

Tactical Errors Enhancements

6.3.102

- In the Work Area, the Errors pane has been renamed to Expected Access Errors and contains new columns.
- The Permission Sources window contains a new tab, Permission Sources Causing Access Errors, displaying information about edited permissions, for example:
 - The path of the folder or special file to which the permission source has unique permissions.
 - The source through which the user has permissions to the folder and on which an editing command exists.
 - The date and time when the DatAdvantage user/system editing action occurred, based on IDU server time

Editing Existing Permission Entries

6.3.102

Now available in 6.3.102, integrated from 6.2.51.

When editing an existing permission entry in the Group Creation Wizard, it is now possible to select the objects to which the permissions will be applied. The **Apply To** drop-down list in the **Permission Entry For** dialog box is now enabled to reflect this enhancement. The drop-down list includes the following options:

- This folder only
- This folder, subfolders and files
- This folder and subfolders
- This folder and files
- Subfolders and files only
- Subfolders only

Note: This feature is only available for Windows file servers. In addition, this feature is not relevant if repairing recommendation errors on a particular directory.

Dictionaries View

6.3.102

Now available in 6.3.102, integrated from 6.2.35

In this version, the Dictionaries tab has been moved out of the DCF and DW Configuration window and now resides in a window of its own. This means dictionaries can now be used by other subproducts, including DatAlert and DatAlert Analytics.

- Security - The *Classification Dictionaries* view user role has been renamed to *Dictionaries View*.
- In applying a dictionary to a threat model, the DatAlert/DatAlert Analytics engine respects wildcards and skips terms that have been disabled (the DCF does not support wildcards).
- The following filters have been added to the *File properties* compound filter:
 - *File name and extension dictionary*
 - *Excluded file name and extension dictionary*

Support for UTC

6.3.102

Now available in 6.3.102, integrated from 6.2.35.

In this version, event times in the log have been normalized with UTC. To support this, a column has been added to the log, indicating UTC time to the second.

In this version, event times in the log have been normalized with UTC. To support this, a column has been added to the log, indicating UTC time to the second.

Support for DFS Aliases

6.3.102

Now available in 6.3.102, integrated from 6.2.15.

CNAME aliases for file servers are now supported in DFS management. Aliases can be defined as needed for each CIFS-capable file server defined in the Management Console. More than one can be defined if needed, or none at all.

Keyboard Shortcuts

6.3.50

This version provides keyboard shortcuts for most features and functions of DatAdvantage and its sub-products. A list of available keyboard shortcuts is available in the *DatAdvantage User Guide*.

Commit API

6.3.50

The Commit API enables creating commit operations and transactions. The Commit API supports the Windows and SharePoint operating systems. The API is exposed over HTTP and HTTP/S and uses JSON objects to transfer data.

Committing Changes on Folders with Broken Inheritance

6.3.50

This feature enables administrators to either allow or deny users with edit/commit role to perform commit operations on folders with broken inheritance. If the administrator allows this ability, then each user can select whether to perform the commit operation on such folders or avoid doing so.

Auditing Capabilities for SharePoint Online and OneDrive

6.3.50

DatAdvantage's Office 365 support now extends to auditing capabilities for SharePoint Online and OneDrive. This functionality is similar to the existing on-premise SharePoint auditing. Office 365 auditing uses Microsoft's Activity Feed API to retrieve events.

Office 365 Displaying and Marking Guest Links

6.3.50

For users of SharePoint Online and OneDrive, this feature displays and marks guest links and files with external users as special files.

Creating a Recognized Folder

6.3.50

It is now possible to create a folder directly from the DatAdvantage interface that will be automatically recognized without the need to run the FileWalk and PullWalk jobs. The new folder will be displayed as virtual until it is committed.

Collection of Directory Service Events

6.3.50

In this version, events on directory services by unresolved entities are collected. If such an event is generated, the *affected object* field displays *Unknown user*.

Platforms Supporting IP Address/Hostname

- This version introduces new events metadata, by resolving a device's IP address into a hostname that is more human-readable and more easily monitored in a DHCP environment.
- The following platforms provide support for device IP address/hostname for audited events (as visible in the Log area, and in the 1.a and 1.b group of reports).
 - NetApp
 - EMC CEPA (Celerra, VNX and Isilon)
 - Hitachi NAS
 - Directory Services

- Exchange 2010
 - Device ID for ActiveSync
 - IP for Outlook clients on Ex07/Ex10, in case IP Agents are installed on the Client Access Servers
- Unix - support for Linux-based platforms (not for AIX, Solaris, Novell). This support is only when login is done via CIFS (Samba) and SSH login via SSH. Login via NFS is not supported.
- Windows
- SharePoint:
 - SharePoint Online
 - SharePoint on Premise
- The IP address/hostname field or parameter in filters and various reports has been split into two separate columns, *Device IP Address* and *Device Name*.
 - *Device IP Address* - The IP address of the user from which the event originated.
 - *Device Name* - The resolved host name of the Device IP, from which the event originated.

DataPrivilege

DataPrivilege API

6.3.185

In this version, new ownership-related API methods enable setting and/or replacing owners and authorizers in DataPrivilege, so that 3rd-party systems can use that API. For example, these API methods allow adding or removing folder or group owners, removing an owner from all resources or replacing one owner or authorizer with another on all resources. The above capabilities support only single operations, not bulk operations.

The API methods support both SharePoint and Windows resources. A use case may be an employee leaving the company and being replaced by another employee. That employee is assigned as owner or authorizer in DataPrivilege and now needs to be replaced by the new employee. Sometimes, the ownership information is stored in 3rd party systems such as ITSM or IAM, hence the need for this capability to be exposed as an API.

The following ownership-related methods have been added to DataPrivilege API:

- *AddFolderOwner*
- *AddGroupOwner*
- *RemoveFolderOwner*
- *RemoveGroupOwner*
- *RemoveOwnersFromAll*
- *ReplaceOwnerAuthorizer*

The Query RESTful API is now renamed to Reports API.

The following changes have been made to the DataPrivilege reports exposed by the DatAdvantage Reports API:

- The "Managed Folders User Level Permission" report has a new filter:
 - *Groups_Managed_Status* - Filters out folders with managed or unmanaged permission groups. For details, see the *DatAdvantage Query API Reference Guide*.

6.3.173

In this version, new API methods are now available, which enable creating DataPrivilege supported requests as well as many other folder-related operations.

The following request-related methods have been added to DataPrivilege API:

- *CreateManagedFolder*

The following folder-related methods have been added to DataPrivilege API:

- *AddFolder*
- *RemoveFolder*
- *SyncFolder*
- *AddNewPermissionToFolder*
- *AddAutoApprovedDirectPermissionRequest*
- *GetFolderManageStatus*
- *GetFolderOwners*
- *GetFolderAuthorizers*
- *GetAclsForFolder*
- *GetGroupMembers*
- *EnforceFolderRules*
- *GetFolderAutomaticRules*
- The Query RESTful API exposes the following reports for DataPrivilege:
 - Managed Folder User Level Permission
 - Managed Folder Permissions

DataPrivilege Windows Extension

Secure connectivity with DataPrivilege via HTTPS (over SSL) is now supported.

Beta Release

6.3.153

DataPrivilege remains a *beta* version in 6.3.153.

Support for Server Volumes Configured in Mixed Mode

6.3.153

In this version, DataPrivilege provides support for server volumes configured as both CIFS and NFS, also called *mixed mode*. Supported platforms include:

- NetApp, both 7 mode and cluster mode
- EMC Celerra

Exporting Permissions on Managed Folders

6.3.153

Now available in 6.3.153, integrated from 5.9.70.

With this version, permissions reports can now be generated directly from the main Permissions pane. This feature is disabled by default and can be enabled if it is configured in Application Settings.

Depending on the configuration for this setting, one or both of the following DataPrivilege reports can be generated:

- Managed Folder Permissions
- Managed Folder User Level Permissions

It is also possible to customize the content of email notifications regarding exported permissions. The **Export Template** tab has been added to the Mail Configuration pane to enable this customization. Upon export, an email is sent to the specified email address, containing an Excel file with either one or two spreadsheets describing the permissions on the specified folder or group.

See [DataPrivilege Application Settings](#) for information about the *Set the permissions to be exported* application setting.

Separate Mail Settings for DataPrivilege

6.3.153

In this version, the Management Console enables configuring separate mail settings for DataPrivilege. Configuration options include:

- Outgoing email - Overrides the settings defined for DatAdvantage
- Incoming email - Enables approving DataPrivilege requests by email.

DataPrivilege Application Settings

6.3.153

The following application settings have been added or changed in this version:

- *Set the permissions to be exported* - The name has been changed to *Set the view mode for export permissions*.
- *New - Allow owners to copy permissions when making a folder protected* - Enables owners and authorizers to copy permissions from the parent folder to the protected folder.

6.3.50

The following application settings have been added in this version:

- *Integrated - Allow ellipsis as browse button* - Set this value to True to set the text of the Browse button to an ellipsis (...) rather than the word "Browse."
- *Integrated - Allow folder owners to edit names of new groups* - By default, folder owners can edit names of new groups. Set this option to False to prevent folder owners from editing names of new groups while editing a folder. If set to False, folder owners will not be permitted to create new groups for new folders. Folder owners must first create the folder and then edit it to create new groups.
- *Integrated - Default search mode for users & groups* - Set the default search mode for users and groups. Options are *Database* and *Active Directory*.

DataPrivilege Windows Extension

6.3.102

The DataPrivilege Windows Extension enables creating a permission request for any shared folder that is managed by DataPrivilege, directly from the file system. The extension can be installed on the following versions of Windows:

- Windows Vista (x86 and x64)
- Windows 7 (x86 and x64)
- Windows 8 (x86 and x64)
- Windows 10 (x86 and x64)

Note: On Windows 10, DataPrivilege opens in Internet Explorer 11, not Edge.

Secure connectivity with DataPrivilege via HTTPS (over SSL) is not supported.

Web Farm Support

6.3.102

This version supports installation of DataPrivilege on a web farm. Web farm installation assumes the following:

- The web farm is set up and all prerequisites described in *Metadata Framework Installation Prerequisites and Requirements* have been met.
- DataPrivilege is installed and functioning on the main IDU machine.

Direct Permissions and Nested Groups

6.3.102

In this version, it is possible to grant folder permissions to a group nested within another group, if the parent group has direct permission on the folder. Permissions for nested groups are managed as follows:

- The permitted group on the folder must be a local group.
- The members of this group must be global groups.
- Users are permitted to the folder through membership in the global group.
- In this way, data owners can manage user membership in the group even if they are not direct members of the directly permitted group.
- Entitlement reviews do not allow removing monitored nested groups from the parent groups that are permitted to a folder.

To facilitate this, the following application settings have been added:

- Manage nested groups with permissions: Set the level at which members of the directly permitted domain groups can be set as monitored on folders
- Manage nested groups with permissions: Set the scope of the directly permitted domain groups whose members can be set as monitored on folders
- Manage nested groups with permissions: allow owners and authorizers to manage real direct permissions in addition to nested groups with permissions
- Select the view that is allowed for owners and authorizers on the Permissions tab for managed folders

DataPrivilege Bulk Upload Utility

6.3.102

In the Excel data file, the Bulk Upload Utility now includes a separation in Managed Folders between Windows and SharePoint.

6.3.50

The Bulk Upload Utility is supported in this version.

Entitlement Review Search

6.3.102

Now available in this version.

It is now possible to search for entitlement reviews according to specific folder names, group names or rule names.

Multiple Schedules for Entitlement Reviews

6.3.102

Multiple entitlement review schedules are now available for groups too.

Now available in 6.3, partially integrated from 6.0.x. Additional schedules may be defined for folders only.

In this version, DataPrivilege enables defining separate entitlement review schedules for different scopes of folders. Default scheduling rules are provided separately for folders and groups that are not included in any other scheduling rule, or that are included in rules that have been disabled. Default rules cannot be deleted, but they can be disabled.

The exceptions list now functions as follows:

- If the *Require entitlement review* option is selected, entitlement review requests are *not* created for entities added to the exceptions list.
- If this option is *not* selected, entitlement review requests are created *only* for entities added to the exceptions list.

Unsupported Features

6.3.102

The following features are available only in previous versions of DataPrivilege. They are not available in 6.3.102.

- Create Folder
- Permission Type for default monitored groups
- Exclude built-in groups from FileWalk
- Export permissions from Permissions tab
- Assign multiple owners and authorizers to added folders and groups
- Default owner for non-owned groups
- Support migration for renaming file server
- Synchronize Varonis group owner to Active Directory *Managed By* attribute

DataPrivilege Database Schema Converter

The DataPrivilege Upgrade and Conversion Assessment Tool enables upgrade from older DataPrivilege versions to the newest version. The architecture of DataPrivilege changed significantly to support integration with DatAdvantage, so it is not possible to upgrade without

converting the database schema to the new format. The Upgrade and Conversion Assessment Tool is run automatically by the Enterprise Installer following upgrade.

The Upgrade and Conversion Assessment Tool checks whether all domains, file servers, and DFS roots managed in the current version of DataPrivilege are defined in the Varonis Management Console as required for schema conversion. This process might take several hours. The prerequisites checker can be run through the Enterprise Installer, as the first step in the schema conversion process. In addition, it can be run separately through the Upgrade and Conversion Assessment Tool tool.

Following schema conversion, the path format for managed folders is changed from `<file_server_name.domain_name\share_name` to `<file_server_name>\share_name`. Use this format when configuring file servers in the Management Console.

Important: Do not make any configuration change in DataPrivilege or the Management Console while the DataPrivilege Conversion Assessment Tool or the Database Schema Conversion is running.

For DataPrivilege-Only Environments:

The Varonis Management Console is installed on the computer during the upgrade process. If data is missing, it must be configured manually in the Management Console after the upgrade. If a specific domain, file server, or DFS root is not required for schema conversion, it must be manually removed from the current version of DataPrivilege. If the physical server of a domain or file server is no longer in use and is configured in DataPrivilege for historical purposes only, the Management Console enables setting it as decommissioned to preserve the historical data.

Unsupported Features

DataPrivilege does not support the features listed below. **If you proceed with the upgrade, these features will not be functional.** If you require any of these features, cancel the upgrade process.

- Folder creation requests
- Default ownership of non-owned groups
- Synchronization of Varonis group owner to Active Directory *Managed By* attribute
- Definition of multiple owners and authorizers while adding or editing base or managed folders
- Exclusion of built-in groups from DataPrivilege management.
- Export of permissions from the Permissions tab.

Possible Upgrade Flows

The DataPrivilege schema can only be upgraded and converted from version 6.0.100.

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.

Source DataPrivilege Version	Possible Upgrade
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

Renaming of the Floor Support Role

6.3.50

In this version, the Floor Support role is renamed to *Request Supervisor*.

Cancelling Pending Entitlement Review Requests

6.3.50

Note: Now available in 6.3, integrated from 5.9

With this version, administrators can now cancel entitlement review requests that are pending for folder owners and group owners.

Email Link for Mac Computers

6.3.50

Note: Now available in 6.3, integrated from 6.0.x.

DataPrivilege email templates now include a <MacPCLink> placeholder, to enable using Mac directory paths in email notifications.

Local Group Management Support

6.3.50

Note: Now available in 6.3, integrated from 6.0.x.

With this version, DataPrivilege now supports the management of local users and groups.

All management activities that enable managing domain groups are now available for local users and groups. Additionally, users can now create group membership requests for local groups.

This feature is disabled by default and can be enabled when adding or editing a file server. If enabled, the local host on which the file server resides becomes a monitored domain.

Multi-Language Support

6.3.50

Support for the following languages has been integrated in this version:

- Japanese
- Portuguese (Brazilian)
- Spanish (Latin America)
- Polish

DatAlert

Changes to DatAlert Templates

6.3.185

This version introduces a new predefined DatAlert template, Varonis LEEF Template, which enables sending alerts to external platforms (e.g., IBM QRadar) via syslog. The template is in Log Event Extended Format (LEEF) format.

6.3.173

The following changes are new in this version:

- The default alert template now includes the *Alert page URL* parameter, enabling users to open the alerts page directly from email or SIEM services.
- A new alert template was created, Varonis App for Splunk, in order to integrate Splunk with Varonis. The template is in CEF format.

6.3.153

The default alert template now includes the *Event status* parameter.

DatAlert API

6.3.173

The DatAlert workflow API enables changing the status of alerts and adding notes to them. The API is exposed over HTTP and HTTPS and uses JSON objects to transfer data.

New DatAlert Placeholders

6.3.173

The *Alert Page URL* placeholder has been added to the predefined alert templates and to the list of optional placeholders in the **Add Alert Template** window.

6.3.153

The following placeholders have been added to the predefined alert templates and to the list of optional placeholders in the **Add Alert Template** window:

- *Access Path*
- *DatAdvantage Version* - The DatAdvantage software version, for use with rules run on HP-NAS devices.
- *Rule Description* - A detailed description of the threat model.
- *Rule Storyline* - A detailed description of the alert. Relevant only for DatAlert Analytics alert templates.

The alert displays information about the last event that was performed.

6.3.102

- Two new placeholders, Device Name and Device IP Address, were added to Alerts, and also appear in predefined alerts templates (replacing the existing IP/Hostname placeholder).
 - *Device IP Address* - The IP address of the user from where the event originated
 - *Device Name* - The resolved host name of the Device IP, from which the event originated
- Alerts email templates include a new field, **Where From**, displaying the device's name and IP address.

Changes to Threat Models

6.3.173

The following threat models are new in this version:

- *Abnormal user behavior: password reset by an administrator followed by access to a computer other than the user's personal computer* - Resetting a password enables a privileged user to hijack a user account and perform actions on the user's behalf, ensuring that the activity cannot be traced back to the administrator. The model monitors password reset events followed by

access of the user for which the password was reset to a computer with which the user is not associated.

- *Abnormal user behavior: password reset by an administrator followed by access to a computer to which the user does not normally access* - Resetting a password enables a privileged user to hijack a user account and perform actions on the user's behalf, ensuring that the activity cannot be traced back to the administrator. The model monitors password reset events followed by access of the user for which the password was reset to a computer which the user does not normally access.
- *Abnormal service behavior: unusual amount of logons to personal devices* - A statistically significant increase in the number of logons to personal devices was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker is searching for devices to which the account has access, in order to exploit their assets. It also exposes the credentials of the service to harvesting and re-use.
- *Abnormal service behavior: atypical actions performed on mailbox owned by other users* - A service account performed new actions on mailbox it entered in the past and owned by other users. Service accounts can be expected to perform the same actions repeatedly; therefore, a behavioral change is suspicious. Attackers may impersonate a service account and exploit its privileges.
- *Abnormal behavior: unusual amount of emails sent to a single recipient* - A statistically significant increase was detected in number of emails sent by the user to a single recipient, compared to his behavioral profile. Mails commonly contain sensitive information which may be stolen.
- *Abnormal service behavior: service account attempted to access a personal device for the first time* - A service which has not accessed personal devices in the past has attempted to access one. This may indicate an attacker is abusing the account in order to access personal devices and exploit their assets.
- *Abnormal computer behavior: computer account attempted to access a personal device for the first time* - A computer account which has not accessed personal devices in the past has attempted to access one. This may indicate an attacker is abusing the account in order to access personal devices and exploit their assets.
- *Abnormal access behavior: possible credential stuffing attack from a single source* - An unusual number of login attempts with an invalid username occurred from a single device. Such an unusual number may indicate that an attacker is trying to guess domain user names. If the source of the username list is credentials stolen from a breached website, this is a *credential stuffing* attack, in which the attacker assumes that users use the same credentials everywhere. If the list is a random list, the alert may indicate the first phase in a *brute force* attack. Once the attackers succeed in guessing a username, they will continue to attempt to guess the password for the user.
- *Abnormal access behavior: possible distributed credential stuffing attack* - An unusual number of login attempts with an invalid username occurred observed from multiple devices. This unusual number may indicate that an attacker is trying to guess domain user names using several devices to accelerate the attack or attempt to disguise it. If the source of the username list is credentials stolen from a breached website, this is a *credential stuffing* attack, in which the attacker assumes that users use the same credentials everywhere. If the list is a random

list, the alert may indicate the first phase in a *brute force* attack. Once the attackers succeed in guessing a username, they will continue to attempt to guess the password for the user.

- *Abnormal service behavior: service account logged on to a personal device for the first time* - A service which has not logged on to personal devices in the past month has logged on to one. This may indicate an attacker is abusing the account in order to access personal devices and exploit their assets. It also exposes the credentials of the service to harvesting and re-use.
- *Abnormal behavior: unusual amount of logons to personal devices* - A statistically significant increase in the number of logons to personal devices was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker has accessed the network and is searching for data that is ultimately the target for an attack.
- *Abnormal behavior: accumulative increase in the number of logons to personal devices* - A statistically significant increase in the number of logons to personal devices, over time, was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker has accessed the network and is gradually searching for data that is ultimately the target for an attack.
- *Abnormal behavior: unusual amount of logons to devices* - A statistically significant increase in the number of logons to devices was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker has accessed the network and is searching for data that is ultimately the target for an attack.
- *Abnormal behavior: accumulative increase in the amount of logons to devices* - A statistically significant increase in the number of logons to devices, over time, was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker has accessed the network and is gradually searching for data that is ultimately the target for an attack.
- *Abnormal service behavior: unusual amount of devices accessed* - A statistically significant increase in the number of attempts to access devices was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker is searching for devices to which the account has access in order to exploit their assets. Public devices such as domain controllers and Exchange servers are excluded from this threat model.
- *Abnormal service behavior: accumulative increase in amount of devices accessed* - A statistically significant increase in the number of attempts to access devices, over time, was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker is gradually searching for devices to which the account has access, in order to exploit their assets. Public devices such as domain controllers and Exchange servers are excluded from this threat model.
- *Abnormal computer behavior: unusual amount of devices accessed* - A statistically significant increase in the number of attempts to access devices was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker is searching for devices to which the account

has access, in order to exploit their assets. Public devices such as domain controllers and Exchange servers are excluded from this threat model.

- *Abnormal computer behavior: accumulative increase in amount of devices accessed* - A statistically significant increase in the number of attempts to access devices, over time, was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker is gradually searching for devices to which the account has access, in order to exploit their assets. Public devices such as domain controllers and Exchange servers are excluded from this threat model.
- *Abnormal admin behavior: unusual amount of devices accessed* - A statistically significant increase in the number of attempts to access devices was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker is searching for devices to which the account has access, in order to exploit their assets. This threat model may generate a false positive alert, in case network discovery is turned on. Public devices such as domain controllers and Exchange servers are excluded from this threat model.
- *Abnormal admin behavior: accumulative increase in amount of devices accessed* - A statistically significant increase in the number of attempts to access devices, over time, was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker is gradually searching for devices to which the account has access, in order to exploit their assets. This threat model may generate a false positive alert, in case network discovery is turned on. Public devices such as domain controllers and Exchange servers are excluded from this threat model.
- *Abnormal behavior: unusual amount of devices accessed* - A statistically significant increase in the number of attempts to access devices was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker is searching for devices to which the account has access, in order to exploit their assets. This threat model may generate a false positive alert, in case network discovery is turned on. Public devices such as domain controllers and Exchange servers are excluded from this threat model.
- *Abnormal behavior: accumulative increase in amount of devices accessed* - A statistically significant increase in the number of attempts to access devices, over time, was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker is gradually searching for devices to which the account has access, in order to exploit their assets. This threat model may generate a false positive alert, in case network discovery is turned on. Public devices such as domain controllers and Exchange servers are excluded from this threat model.
- *Abnormal behavior: unusual amount of public devices accessed* - A statistically significant increase in the number of attempts to access public devices was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker is searching for devices to which the account has access, in order to exploit their assets. This threat model may generate a false positive alert, in case network discovery is turned on.

- *Abnormal behavior: accumulative increase in amount of public devices accessed* - A statistically significant increase in the number of attempts to access public devices, over time, was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker is gradually searching for devices to which the account has access, in order to exploit the assets. The model may generate a false positive alert, in case network discovery is turned on.
- *Abnormal behavior: unusual number of authentications to personal devices by end-user account* - A statistically significant increase in the number of authentications to personal devices was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker has accessed the network and is searching for data that is ultimately the target for an attack.
- *Abnormal behavior: accumulative increase in number of authentications to personal devices by end-user account* - A statistically significant increase in the number of authentications to personal devices, over time, was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker has accessed the network and is gradually searching for data that is ultimately the target for an attack.
- *Abnormal behavior: unusual number of authentications to devices by end-user account* - A statistically significant increase in the number of authentications to devices was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker has accessed the network and is searching for data that is ultimately the target of an attack.
- *Abnormal behavior: accumulative increase in the number of account authentications to devices by end-user account* - A statistically significant increase in the number of authentications to devices, over time, was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker has accessed the network and is gradually searching for data that is ultimately the target for an attack.
- *Abnormal admin behavior: unusual number of authentications to personal devices by admin account* - A statistically significant increase in the number of authentications to personal devices was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker has accessed the network and is searching for data that is ultimately the target for an attack.
- *Abnormal admin behavior: accumulative increase in number of authentications to personal devices by admin account* - A statistically significant increase in the number of authentications to personal devices, over time, was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker has accessed the network and is gradually searching for data that is ultimately the target of an attack.
- *Abnormal admin behavior: unusual number of authentications to devices by admin account* - A statistically significant increase in the number of authentications to devices was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker has accessed the network and is searching for data that is ultimately the target for an attack.

- *Abnormal admin behavior: accumulative increase in the number of account authentications to devices by admin account* - A statistically significant increase in the number of authentications to devices, over time, was detected for the account, compared to its behavioral profile. Accounts without behavioral profiles are compared to the default behavioral profile. This may indicate an attacker has accessed the network and is gradually searching for data that is ultimately the target for an attack.
- *Creation: automatic forwarding of incoming messages on mailbox* - Mailbox was marked to automatically forward any incoming messages to another recipient. This may indicate that an attacker is trying to redirect data out of the organization, especially if performed outside of change control processes. Mailboxes commonly contain sensitive information which attackers target.

The following threat model indicators are new:

- *Personal user of another computer*, used by the Alerts page to inform users if the device that they are using belongs to another user.

6.3.102

The following threat models are new in this version:

- *File encrypted by ransomware* - A file with a known encrypted ransomware extension was created or renamed. The list of extensions is configurable via the *Ransomware encrypted file extensions* dictionary. This indicates a ransomware attack underway, with the intent to deny access to data.
- *Suspected crypto intrusion activity* - Multiple files were created with, opened or renamed to a suspected crypto tool or ransom note file name. The list of names is configurable via the *Suspected ransomware note file names* dictionary. This indicates that ransomware may have intruded into the system.

The following changes have been made to threat models:

- *Abnormal admin behavior: access to atypical mailboxes*
 - New severity level - 4 - Warning
- *Abnormal admin behavior: accumulative increase in lockouts across admin accounts*
 - New severity level - 3 - Error
- *Abnormal admin behavior: accumulative increase in lockouts for individual admin accounts*
 - New severity level - 4 - Warning
- *Abnormal admin behavior: unusual amount of lockouts across admin accounts*
 - New severity level - 2 - Critical
- *Abnormal behavior: Accumulative create and delete actions resemble ransomware*
 - Resource types added - SharePoint Online, OneDrive, Dell FluidFS
- *Abnormal behavior: accumulative increase in access to idle and sensitive data*
 - New name - *Abnormal behavior: accumulative increase in amount of idle and sensitive data accessed*
 - Resource types added - SharePoint Online, One Drive, Dell FluidFS

- *Abnormal behavior: accumulative increase in access to idle data*
 - New name - *Abnormal behavior: accumulative increase in amount of idle data accessed*
 - New severity level - 3 - Error
 - Resource types added - SharePoint Online, One Drive, Dell FluidFS
- *Abnormal behavior: accumulative increase in lockouts across end-user accounts*
 - New severity level - 4 - Warning
- *Abnormal behavior: accumulative increase in lockouts for individual end-user accounts*
 - New severity level - 5 - Notice
- *Abnormal behavior: Accumulative user rename and modify actions resemble ransomware*
 - Resource type added - Dell FluidFS
- *Abnormal behavior: unusual amount of access denied events*
 - New name - *Abnormal behavior: unusual amount of files with denied access*
 - New severity level - 3 - Error
- *Abnormal behavior: unusual amount of access-denied events*
 - New name - *Abnormal behavior: unusual amount of files with denied access*
 - New severity level - 5 - Notice
- *Abnormal behavior: unusual amount of access to configuration and backup files*
 - New name - *Abnormal behavior: unusual amount of configuration and backup files accessed*
 - New severity level - 3 - Error
 - Resource type added - Dell FluidFS
- *Abnormal behavior: unusual amount of access to idle data*
 - New name - *Abnormal behavior: access to an unusual amount of idle data*
 - New severity level - 2 - Critical
 - Resource types added - SharePoint Online, One Drive, Dell FluidFS
- *Abnormal behavior: unusual amount of access to sensitive data*
 - New name - *Abnormal behavior: access to an unusual amount of idle sensitive data*
 - New severity level - 0 - Emergency
 - Resource types added - SharePoint Online, One Drive, Dell FluidFS
- *Abnormal behavior: unusual amount of lockout across end-user accounts*
 - New severity level - 3 - Error
- *Abnormal behavior: unusual amount of script file creations*
 - New name - *Abnormal behavior: unusual amount of script files accessed*
 - New category - Intrusion
 - New severity level - 2 - Critical
 - Resource type added - Dell FluidFS
- *Abnormal behavior: unusual amount of system files accessed*
 - New name - *Abnormal behavior: unusual amount of system files accessed*
 - New category - Reconnaissance
 - New severity level - 3 - Error
 - Resource type added - Dell FluidFS

- *Abnormal behavior: unusual number of file deletions*
 - New name - *Abnormal behavior: unusual number of files deleted*
 - Resource types added - SharePoint Online, One Drive, Dell FluidFS
- *Abnormal behavior: unusual number of sensitive file deletions*
 - New name - *Abnormal behavior: unusual number of sensitive files deleted*
 - Resource types added - SharePoint Online, OneDrive, Dell FluidFS
- *Abnormal behavior: User create and delete actions resemble ransomware*
 - Resource types added - SharePoint Online, OneDrive, Dell FluidFS
- *Abnormal behavior: user rename and modify actions resemble ransomware*
 - New name - *Abnormal behavior: User rename and modify actions resemble ransomware*
 - Resource type added - Dell FluidFS
- *Abnormal executive behavior: accumulative increase in access-denied events across executive accounts*
 - New name - *Abnormal executive behavior: accumulative increase in access-denied events across executive accounts*
 - New severity level - 4 - Warning
- *Abnormal executive behavior: accumulative increase in access to script, configuration and backup files across executive accounts*
 - New name - *Abnormal executive behavior: accumulative increase in amount of script, configuration and backup files accessed across executive accounts*
 - New severity level - 3 - Error
 - Resource type added - Dell FluidFS
- *Abnormal executive behavior: unusual amounts of access-denied events across executive accounts*
 - New name - *Abnormal executive behavior: unusual amount of files with denied access across executive accounts*
 - New severity level - 3 - Error
- *Abnormal executive behavior: unusual amounts of access to script, configuration and backup files across executive accounts*
 - New name - *Abnormal executive behavior: unusual amount of script, configuration and backup files accessed*
 - New severity level - 2 - Critical
 - Resource type added - Dell FluidFS
- *Abnormal service behavior: access to atypical files*
 - New severity level - 3 - Error
 - Resource types added - SharePoint Online, One Drive, Dell FluidFS
- *Abnormal service behavior: access to atypical folders*
 - New severity level - 3 - Error
 - Resource type added - Dell FluidFS

- *Abnormal service behavior: access to atypical mailboxes*
 - New severity level - 3 - Error
- *Abnormal service behavior: accumulative increase in lockouts across service accounts*
 - New severity level - 4 - Warning
- *Abnormal service behavior: accumulative increase in lockouts for individual service accounts*
 - New severity level - 5 - Notice
- *Abnormal service behavior: atypical failure to access data*
 - New severity level - 4 - Warning
- *Abnormal service behavior: unusual amounts of lockouts across service accounts*
 - New severity level - 3 - Error
- *Administrative or service account disabled or deleted*
 - New severity level - 4 - Warning
- *Administrative or service account reset*
 - New severity level - 4 - Warning
- *Crypto intrusion activity*
 - New name - *Crypto activity detected*
 - New category - Denial of Service
 - New severity level - 0 - Emergency
 - Resource types added - SharePoint Online, One Drive, Dell FluidFS
- *Deletion: Multiple directory service objects*
 - New severity level - 4 - Warning
- *Encryption of multiple files*
 - Resource types added - SharePoint Online, One Drive, Dell FluidFS
- *Executive account locked-out/disabled/deleted/password reset*
 - New category - Obfuscation
- *Exploitation tools detected*
 - New severity level - 4 - Warning
 - Resource types added - SharePoint Online, One Drive, Dell FluidFS
- *Immediate pattern detected: user actions resemble ransomware*
 - Resource type added - Dell FluidFS
- *Lockout: Multiple accounts locked out*
 - New severity level - 3 - Error
- *Membership changes: admin groups*
 - New category - Privilege Escalation
 - New severity level - 2 - Critical

- *Membership Changes: Service Accounts*
 - New severity level - 3 - Error
- *Modification: Critical GPOs*
 - New severity level - 2 - Critical
- *Modification: Critical Organizational Units*
 - New severity level - 3 - Error
- *Modification: GPO Security Settings*
 - New severity level - 3 - Error
- *Modification: Hosts file*
 - New severity level - 5 - Notice
- *Multiple open events on files likely to contain credentials*
 - New severity level - 3 - Error
 - Resource types added - SharePoint Online, One Drive, Dell FluidFS
- *Permission changes on OU*
 - New severity level - 3 - Error
- *Permissions granted directly to user in directory services*
 - New severity level - 5 - Notice
- *Permissions granted directly to user in Windows file system*
 - New severity level - 5 - Notice
- *Potential masked intrusion: system binaries found in unusual locations*
 - New name - *Suspicious access activity: non-admin access to system binaries in non-system locations*
 - New severity level - 5 - Notice
- *Recon tools detected*
 - New severity level - 4 - Warning
 - Resource types added - SharePoint Online, One Drive, Dell FluidFS
- *Security certificate activity by non-administrators*
 - Resource types added - SharePoint Online, One Drive, Dell FluidFS
- *Suspicious access activity: non-admin access to files containing credentials*
 - New severity level - 3 - Error
- *Suspicious access activity: non-admin access to startup files and scripts*
 - New severity level - 2 - Critical
- *Suspicious access activity: service account access to file containing credentials*
 - New category - Privilege Escalation
 - New severity level - 3 - Error
- *Suspicious mailbox activity: multiple messages marked as unread by user other than the mailbox owner*
 - New category - Obfuscation
 - New severity level - 3 - Error

Disabled or Deleted Threat Models

6.3.173

This version now enables closing all alerts that are related to deleted or disabled threat models. When a threat model is deleted or disabled, a confirmation message is displayed, enabling users to close related alerts.

DatAlert Template Modification

6.3.173

The default alert template now includes the *Alert Page URL* parameter, enabling users to open the **Alerts** page directly from email or SIEM services.

New Varonis App for Splunk Template

6.3.173

A new alert template was created, Varonis App for Splunk, in order to integrate Splunk with Varonis. The template is in CEF format.

Changes to DatAlert Email Templates

6.3.153

This version provides the following enhancements to the DatAlert and DatAlert Analytics email templates:

- The SAM account name has been added after the user name.
- The hostname and IP address are displayed (if available).
- A detailed description of the threat model is now displayed at the bottom of the template.

The DatAlert Analytics template now also includes:

- The name of the threat model
- A detailed description of the alert
- **To investigate alert** link at the bottom of the template, which enables jumping to the **Alert Info** page in the DatAlert Web Interface.

The alert displays information about the last event that was performed.

Ability to Define Multiple Syslog and SNMP Servers

6.3.102

In this version, it is possible to define more than one syslog or SNMP server. DatAlerts are sent to all defined servers. All servers use the same alert template.

Support for TLS Encryption

6.3.102

This version provides support for the TLS encryption protocol, for email sent by DatAlert. Email sent by any other product in the Metadata Framework is still sent using SSL encryption (if encryption is configured).

New DatAlert Analytics Threat Model

6.3.102

Now available in 6.3.102, integrated from 6.2.51.

A new DatAlert Analytics threat model has been introduced, *Immediate pattern detected: user actions resemble ransomware*. This threat model alerts in real time (or nearly so) if a user's file activity matches a ransomware pattern over several folders, perhaps indicating a ransomware attack is underway with the intent to deny access to data.

DatAlert Integration with Security Management Systems

6.3.102

Now available in 6.3.102, integrated from 6.2.35.

With this version, Varonis now supports the integration of DatAlert with the following security management systems:

- HP ArcSight
- FireEye TAP
- LogRhythm

With the certified integration of DatAlert and these security management systems, users can automatically send DatAlerts into these external platforms, thereby increasing the speed and accuracy with which they are able to identify, prioritize and investigate unusual user behavior surrounding unstructured data.

New Predefined Alert Template

DatAlert now includes a predefined alert template that complies with the CEF format, to enable sending DatAlerts to the external platforms via Syslog. The External system default template is now available for selection in the DatAlert window. The template is read-only. See [HP ArcSight Alert Template](#).

Validating Alerts via Timestamps

6.3.50

A new timestamp function was added that validates each alert during the file server scan process, thereby increasing the scan's efficiency. Additionally, a new job called *ask more* was added, providing greater efficiency in pulling for new alerts and the way that the results are published.

DatAlert Web Interface

New Web Interface Design

6.3.185

This version of the DatAlert Web Interface includes the following enhancements:

- The DatAlert Web Interface now supports the **Back** and **Next** browser buttons, which enables users to navigate backward and forward in their browsing history. In addition, the **Refresh** button is now supported, which enables reloading the current page.
- The **Feedback** button has been added to all pages, enabling users to provide feedback about the DatAlert Web Interface. In addition, the **Feedback** dialog box displays a link to Varonis Support, enabling users to submit a question or report a bug.
- The *Auto run search* checkbox has been moved to the context menu at the top right of each page. Clicking **My Account** will open the context menu.
- The Analytics pages have an updated look:
 - New icons have been added to the Alerts and Events grids.
 - The **Select Users/Computers** dialog box has been added to the advanced search to enable selecting one or more users and computers from a list of available entities. See [Advanced Search Enhancements](#) for more information.

6.3.173

This version of the DatAlert Web Interface includes the following enhancements:

- Context cards have a new look and feel. See below for more information.
- Alerts can be managed from the **Alerts** page and the **Alert Info** page. See [Managing Alerts](#) for more information.
- The **Export** button in the **Alerts** and **Events** pages enables exporting table data to a CSV file. It also enables exporting the list of connected entities in the File Servers, Directory Services, Exchange and SharePoint dashboards.
- The *Alert status* filter now appears at the top of the Alerts dashboard and the **Alerts** page. See below for more information.
- By default, in the **Alerts** and **Events** pages, the search is now run automatically when performing a basic search, using insights and selecting attributes from the Refine pane. Users can run the search manually by clearing the **Auto run search** checkbox and clicking the **Search** icon.
- The **Print** icon has been added to the top right of the File Servers, Directory Services, Exchange and SharePoint dashboards to enable printing the widget display.
- The Top Alerted widgets in the Alerts dashboard have an updated look. For more information, see [Alerts Dashboard View](#).
- The following risk assessment insight has been added to the list of available insights:
 - *Personal computer of another user* - Devices usually used by a specific account were used by another user. This may indicate that the accounts are breached.

See the following sections for more information about the new enhancements.

6.3.153

This version of the DatAlert Web Interface includes the following enhancements:

- A new **Alert Info** page, which enables investigating specific alerts. See below for more information.
- New dashboards provide aggregated metric data for the selected scope.
- The previous dashboard has been renamed to *Alerts Dashboard*.
- The Alerts dashboard now displays the Top Alerted Devices panel, which provides a list of up to five top alerted devices matching the search criteria specified and sorted by the number of alerts.
- The Device Search Results context card has been added, to enable viewing data about the device involved in the alert.

6.3.102

The DatAlert Web Interface has been redesigned, to provide a streamlined, enhanced user experience.

- A new menu enables selecting either the Dashboard view or the Analytics view. See below for more information.
- The resource pickers now support multi-selection and filtering, to enable focusing only on the relevant objects.
- User changes to the page layout are saved.
- Resource selection is saved until the user makes a change.
- Error notifications and handling have been improved.
- Users can now terminate a search on demand.
- Charts and graphs have an updated look.

See the following sections for more information about the new design.

Alerts Dashboard View

6.3.173

The following enhancements have been made in this version:

- The widgets now display the **More options** button located to the right of each entity, which enables:
 - Jumping to the **Alerts** page to view all alerts for a specific entity.
 - Opening the entity's context card.
- The *Alert status* filter now appears at the top of the dashboard, which enables filtering the results according to one or more alert statuses.
- In the Top Alerted Users widget, the **W** icon next to the name of a user indicates that the user is on the Watch List.
- It is now necessary to set at least one of the mandatory filters in order to view results in the Alerts dashboard.

6.3.153

In this version, the previous dashboard has been renamed to *Alerts Dashboard*.

In addition, the Alerts dashboard now displays the Top Alerted Devices panel, which provides a list of up to five top alerted devices matching the search criteria specified and sorted by the number of alerts. Clicking the name of the device will open the Device Search Results context card.

6.3.102

The dashboard provides an "at a glance" view of the alert information retrieved for the specified timeframe. It allows users to quickly view and detect suspicious activity for further analysis.

The dashboard is comprised of the following elements:

- *Alerts Over Time* - A stacked bar chart illustrating the dispersion of alerts matching the defined timeframe and search criteria
- *Top Alerted Users* - A list of up to five top alerted users matching the search criteria specified and sorted by the number of alerts
- *Top Alerted Assets* - A list of up to five top alerted assets matching the search criteria specified and sorted by the number of alerts
- *Top Alerted Threat Models* - A list of up to five top alerted threat models matching the search criteria specified and sorted by the number of alerts
- *Kill Chain Analysis* - Shows the dispersion of alerts matching the search criteria over an attack path

Alert Info Page

6.3.173

In this version, the following changes have been made to the **Alert Info** page:

- The status of the alert is now presented at the top of the page. Clicking the status will enable managing the alert. For more information about managing alerts, see [Managing Alerts](#).
- The **Manage alert** link has been added to the Next Steps pane, which also enables managing the alert.
- The following risk assessment insight has been added to the list of available insights:
 - *Personal computer of another user* - Devices usually used by a specific account were used by another user. This may indicate that the accounts are breached.

The insights that are presented in the **Alert Info** page vary for each threat model, depending on the type of information the threat model retrieves.

6.3.153

This version of the DatAlert Web Interface introduces the **Alert Info** page, which enables investigating specific alerts. It provides a quick and easy way to drill down and analyze the details of each alert, allowing investigators to make an informed decision regarding the intentions of the alerted activity.

The information in this page also provides a better understanding of the nature of the alerted activity. For example, investigators can check an entity's activity to see whether there are usage patterns that may explain the behavior. For DatAlert Analytics alerts, investigators can also compare the actions of the alerted user to those of other users in the peer group.

The **Alert Info** page also displays risk assessment insights, which highlight valuable information about the events, users and data of a specific alert.

The Next Steps pane enables jumping to the **Events** page to analyze the actual events which triggered the alert.

Context cards can be opened from various areas of the **Alert Info** page to enable viewing information about a specific entity, category or threat model.

The **Alert** page can be accessed by clicking the alert ID in the **Events** and **Alerts** pages.

The left menu of the **Alert Info** page includes the following options:

- *Summary* - Provides a detailed overview of the relevant alert and critical risk assessment insights. The summary also presents graphical views of the alert information, depending on the type of information retrieved by the threat model.
- *Users* - Provides important insights into the actions of the users who performed the event which triggered the alert. The Users pane also provides insightful information about similar users.
- *Devices* - Displays information about the devices that were involved in the alert.
- *Data* - Presents information about the alerted data.
- *Time* - Displays the date and time of the alerted event. It also provides information about whether the alerted activity exceeded the user's regular working hours.

New Dashboards

6.3.173

It is now possible to print the widgets displayed for each dashboard. The **Print** icon has been added to the top right of each dashboard to support this enhancement.

6.3.153

In addition to the Alerts dashboard, this version of the DatAlert Web Interface now provides the following dashboards:

- *File Servers* - Provides aggregated file system statistics for selected file servers. The widgets display data retrieved by report 14.a.01 (General File System Statistics).
- *Directory Services* - Provides aggregated directory service statistics for selected domains. The widgets display data retrieved by report 14.d.01 (General Directory Service Statistics).
- *Exchange* - Displays aggregated file system statistics for selected on-premises Exchange and Exchange Online file servers. The widgets display data retrieved by report 14.a.01 (General File System Statistics).
- *SharePoint* - Presents aggregated file system statistics for selected on-premises SharePoint and SharePoint Online file servers. The widgets display data retrieved by report 14.a.01 (General File System Statistics).

The dashboards enable performing the following actions:

- Add and remove widgets
- Edit the widget display
- View a timeline of the change trends
- View additional information about the metric

- Jump to connected entities
- Drag and drop dashboard widgets

Each dashboard widget presents aggregated metric data for the selected scope, calculated at the time the report was last run. For more information, see the *DatAlert Web Interface User Guide*. For a list of available widgets, see [Changes to Columns, Filters, Widgets and Refinements](#).

Note: Only users with the *DatAlert Configuration user* and *Reports View user* roles can view and edit dashboards.

Analytics View

6.3.102

The Analytics view enables selecting either the Alerts view or the Events view for further investigation. Additional pages for either of these views can be added as necessary (up to 100 pages).

Alerts View

6.3.173

In this version, the following changes have been made to the **Alerts** page:

- The *Alert status* filter now appears at the top of the page, which enables filtering the results according to one or more alert statuses. The following alert statuses are available for selection:
 - Open
 - Under investigation
 - Closed
- By default, the search is now run automatically when performing a basic search, using insights and selecting attributes from the Refine pane. Users can run the search manually by clearing the **Auto run search** checkbox and clicking the **Search** icon.
- The **More options** button has been added to the left of each table row, enabling users to:
 - Manage specific alerts. For more information about managing alerts, see [Managing Alerts](#).
 - View the events related to a specific alert.
 - Investigate a specific alert.
- The **Export** button is now displayed above the table, to enable exporting the table data to a CSV file. For more information, see [Exporting to CSV](#).
- The *Connected Events* option in the Refine pane has been renamed to *View all related events*, which enables exploring the events which triggered a specific alert or all alerts retrieved for the defined time period.

6.3.102

The **Alerts** page displays both a graphical and tabular view of the alert data matching the specified search criteria. The Alerts view is comprised of the following elements:

- *Timeline* - A stacked bar chart illustrating the dispersion of alerts matching the defined time period and search criteria. Each bar in the chart displays up to three severities, divided into

stacks. Each stack represents a different severity - high, medium or low. The color code represents the severity of the alert:

- *Red* - High severity. Alerts with a severity of Emergency, Alert or Critical
- *Orange* - Medium severity. Alerts with a severity of Error or Warning
- *Green* - Low severity. Alerts with a severity of Warning, Notice, Informational and Debug
- *Alerts List* - A grid, displaying the alert data matching the defined search criteria.

Events View

6.3.173

In this version, the following changes have been made to the **Events** page:

- By default, the search is now run automatically when performing a basic search, using insights and selecting attributes from the Refine pane. Users can run the search manually by clearing the **Auto run search** checkbox and clicking the **Search** icon.
- The **Export** button is now displayed above the table, to enable exporting the table data to a CSV file. For more information, see [Exporting to CSV](#).
- From the Events view, it is now possible to jump to the **Alerts** page to explore all alerts related to the events displayed on the **Events** page. The **View all related alerts** option has been added to the Refine pane to support this enhancement.

6.3.102

The Events view displays a line chart illustrating the dispersion of events over the specified timeline. This view also displays the event information in the form of a table.

You can use this information to analyze the events which triggered the alerts.

The Events pane is comprised of the following elements:

- *Timeline* - A line chart illustrating the dispersion of events matching the defined timeline and search criteria.
- A grid, displaying the event data in table form. The event data detailed in the table matches the timeline and search criteria specified.

Changes to Columns, Filters, Widgets and Refinements

6.3.173

The following columns, filters and refinements have been added in this version:

Column/Widget	Description	Available In
Alert status	Filters according to the status of the alert that was generated. Can be: • Open • Under investigation • Closed	• Alert dashboard • Alerts page
Close Reason	The reason the alert was closed. Default options are: • Resolved • Misconfiguration • Threat model disabled or deleted • Account misclassification • Legitimate activity • Other	• Alert Details

6.3.153

The following columns and dashboard widgets have been added in this version:

Column/Widget	Description	Available In
Classification Results	A list of DCF threat models with hits on the object.	• Dashboards - Available column
Email	The email address of the user, as displayed in Active Directory.	• Dashboards - Available column
Enabled but stale users	Number of enabled but stale users per domain as defined in Management Console > Configuration > Account Management	Directory Services dashboard
Group	The display name of the affected group	• Dashboards - Available column

Column/Widget	Description	Available In
No. of folders that contain sensitive files	Number of folders per file server that directly contain at least one sensitive file	- SharePoint dashboard - File Servers dashboard
No. of folders with inconsistent permissions	Number of folders per file server with inconsistent permissions	File Servers dashboard
No. of folders with open access	Number of folders per file server that can be accessed by global access groups. In Windows file servers, the metric counts only open shares.	File Servers dashboard
No. of folders with open access (Inc. Inherited)	Number of folders per file server that can be accessed by global access groups, including inherited folders. In Windows file servers, the metric counts only open shares.	File Servers dashboard
No. of folders with stale data	Number of folders per file server that are considered stale as defined in Management Console > Reports > Trend Reports	- SharePoint dashboard - File Servers dashboard
No. of folders with unresolved SIDs	No. of nested folders with at least one permission that contains an unresolved SID	File Servers dashboard
No. of folders with user ACEs	Number of folders per file server with at least one unique permission entry granted to an individual account	- SharePoint dashboard - File Servers dashboard
No. of computer accounts	Number of computer accounts per domain	Directory Services dashboard
No. of disabled users	Number of disabled users per domain	Directory Services dashboard
No. of empty groups	Number of groups per domain with no members (including computer accounts)	Directory Services dashboard

Column/Widget	Description	Available In
No. of enabled locked-out users	Number of enabled locked-out users per domain	Directory Services dashboard
No. of enabled users with expired password	Number of enabled users with an expired password per domain	Directory Services dashboard
No. of files	Number of files per file server	• SharePoint dashboard • File Servers dashboard
No. of global access groups	Number of global access groups as defined in Management Console > Configuration > Global Access Groups	Directory Services dashboard
No. of groups	Number of groups per domain	Directory Services dashboard
No. of groups with removal recommendations	Number of groups per domain with members that the IDU Analytics engine recommended to remove	Directory Services dashboard
No. of inherited folders	Number of folders per file server with only inherited permissions	• SharePoint dashboard • File Servers dashboard
No. of looped groups	Number of groups per domain that are part of a membership loop in Directory Services	Directory Services dashboard
No. of mailboxes	Number of Exchange mailboxes per Exchange file server. This metric is calculated only on Exchange file servers.	Exchange dashboard

Column/Widget	Description	Available In
No. of mailboxes with permissions for users/groups other than the mailbox owner	Number of mailboxes with permissions for users/groups other than the mailbox owner (excluding permissions for administrators)	Exchange dashboard
No. of managed folders	Number of folders per file server that have at least one parent folder that has been assigned an owner in DatAdvantage	- SharePoint dashboard - File Servers dashboard
No. of nested folders	Number of folders per file server	- SharePoint dashboard - File Servers dashboard
No. of non-administrator groups with administrator members	Number of non-administrator groups with administrator members	Directory Services dashboard
No. of permission entries	Total number of permission entries per file server	- SharePoint dashboard - File Servers dashboard
No. of protected folders	Number of folders per file server with no inherited permissions	- SharePoint dashboard - File Servers dashboard
No. of public folders	Number of Exchange public folders (not including calendar, contacts folders, and so on). This metric is only calculated on Exchange file servers.	Exchange dashboard
No. of sensitive files	Number of files that have a classification hit count greater than zero (minus the hits on excluded rules defined in Management Console > Reports > Trend Reports)	- SharePoint dashboard - File Servers dashboard

Column/Widget	Description	Available In
No. of sensitive files with open access	Number of sensitive files per file server that can be accessed via global access groups. In Windows file servers, the metric counts only files that are inside open shares.	File Servers dashboard
No. of sensitive folders with open access	No. of nested folders which directly contain sensitive information that can be accessed via global access groups through both file system and share permissions. A folder is considered to have sensitive information if at least one file in the folder has more than one hit on any DCF rule that is considered sensitive.	File Servers dashboard
No. of stale public folders	Number of public folders per file server that are considered stale as defined in Management Console > Reports > Trend Reports	Exchange dashboard
No. of stale sensitive files	Number of files per file server that are sensitive and stale	- SharePoint dashboard - File Servers dashboard
No. of stale user accounts	Number of stale user accounts per domain as defined in Management Console > Configuration > Account Management	Directory Services dashboard
No. of unique folders	Number of folders per file server with at least one non-inherited permission entry	- SharePoint dashboard - File Servers dashboard
No. of unique permission entries	Number of unique permission entries per file server	- SharePoint dashboard - File Servers dashboard
No. of unmanaged protected folders	No. of nested folders with no inherited permissions per file server (not including distinguished unique permissions) that have no owner assigned to them directly	File Servers dashboard

Column/Widget	Description	Available In
No. of users	Number of users per domain	Directory Services dashboard
No. of users with removal recommendations	Number of users per domain that the IDU Analytics engine recommends to remove from one or more groups	Directory Services dashboard
On Watch List	Indicates whether or not the user, group, or object is on the watch list	• Dashboards - Available column
Privileged Account	A list of users classified as privileged accounts, such as an administrator or executive	• Dashboards - Available column
Size of all files and folders (GB)	Size of all files and folders (including temporary folders) on the file server, in gigabytes	• SharePoint dashboard • File Servers dashboard
Size of Folder and Subfolders (in MB)	The size of the folder and its subfolders (in MB)	• Dashboards - Available column
Size of folders with stale data (GB)	Size of folders per file server that are considered stale as defined in Management Console > Reports > Trend Reports	• SharePoint dashboard • File Servers dashboard
Size of managed folders (GB)	Total size of managed folders per file server	• SharePoint dashboard • File Servers dashboard
Size of public folders (GB)	Size of all public folders (not including calendar, contacts folders, and so on). This metric is calculated only on Exchange file servers.	Exchange dashboard

Column/Widget	Description	Available In
Size of stale public folders (GB)	Size of public folders per file server that are considered stale as defined in Management Console > Reports > Trend Reports	Exchange dashboard
Total size of sensitive files (GB)	Total size of files per file server that are considered sensitive	- SharePoint dashboard - File Servers dashboard
Varonis Owner	The display name of the owner assigned to the object in DatAdvantage (i.e., the "Varonis owner")	Dashboards - Available column

6.3.102

This version provides a number of grid columns, filters and search refinements to help users narrow their focus on the most important data. These include:

Filter/Refinement	Description	Available In
Access date	Filters according to the specified time frame during which the file system object was accessed.	Event On Resource
Account type	Filters according to the specified type of privileged account. Can be: - Service accounts - Admin accounts - Executive accounts - Test accounts Note: Account usage is undefined. Therefore, accounts of this type are excluded from all behavioral DatAlert rules.	- Event By User - Event On User
Affected data has follow-up indicators	There are flags, tags or notes defined on the affected data	- Alert On - Event By User
Alert category	The category of the specified alert. Can be: <i>Reconnaissance</i> - The discovery and mapping of systems, services or vulnerabilities	Alert Details

Filter/Refinement	Description	Available In
	• <i>Intrusion</i> - Infection of the IT environment with malware • <i>Exploitation</i> - A piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur in the IT environment. Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation or a denial-of-service attack. • <i>Privilege Escalation</i> - Exploitation of a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user • <i>Lateral Movement</i> - Movement throughout the company's network, seeking valuable hosts that house sensitive information • <i>Exfiltration</i> - Transmission of information from within the target organization's perimeter to a location the threat actor controls • <i>Denial Of Service</i> - An attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the internet • <i>Obfuscation (anti-forensics)</i> - Obscuring an attack by deleting relevant logs or reverting its actions back to the expected state. • <i>Other</i> - An attack that does not fall in any of the above categories.	
Alert date	The date on which the alert occurred	• Alert Details
Alert ID	Filters according to the specified alert ID.	• Alert Details
Alert severity	Filters according to the specified alert severity.	• Alert Details
Alert time	Filters according to the date and time at which the alert occurred.	• Alert Details

Filter/Refinement	Description	Available In
Asset	- Column - The path of the alerted asset - Filters to display the item shown at the level of a volume in DatAdvantage: - CIFS file servers - Either a volume or a monitored share - SharePoint - Site collection - Exchange - Mailbox store or public folders - Directory services - Usually the domain	- Alert On - Event By User
Asset has follow-up indicators	There are flags, tags or notes defined on the alerted asset.	Event By User
Category	Filters according to the specified alert categories. Can be: <i>Reconnaissance</i> - The discovery and mapping of systems, services or vulnerabilities <i>Intrusion</i> - Infection of the IT environment with malware <i>Exploitation</i> - A piece of software, a chunk of data, or a sequence of commands that takes advantage of a bug or vulnerability in order to cause unintended or unanticipated behavior to occur in the IT environment. Such behavior frequently includes things like gaining control of a computer system, allowing privilege escalation or a denial-of-service attack. <i>Privilege Escalation</i> - Exploitation of a bug, design flaw or configuration oversight in an operating system or software application to gain elevated access to resources that are normally protected from an application or user <i>Lateral Movement</i> - Movement throughout the company's network, seeking valuable hosts that house sensitive information <i>Exfiltration</i> - Transmission of information from within the target organization's perimeter to a location the threat actor controls <i>Denial Of Service</i> - An attempt to make a machine or network resource unavailable to its intended users, such as to temporarily or indefinitely interrupt or suspend services of a host connected to the internet	Alert Details

Filter/Refinement	Description	Available In
	• <i>Obfuscation (anti-forensics)</i> - Obscuring an attack by deleting relevant logs or reverting its actions back to the expected state. • <i>Other</i> - An attack that does not fall in any of the above categories.	
Classification Rules	Filters according to files and folders that directly contain files that have hits on the selected rules.	• Event On Resource
Department	Filters according to the <i>department</i> AD property, which is the name of the department in which the user works.	• Alert By • Event By User
Description	Filters the results according to the description of the event. Important: The filter is used to further filter results after a report has been generated. Only text that appeared in the Event Description column of the report can be entered in the filter text box.	• Event Details
Device name	• Column - The name of the device from which the user generated the event. • Filters according to the name of the device from which the user generated the event.	• Alert Device • Event By User
Disabled user account	Filters to display accounts for acting objects that are both disabled and stale. The amount of time after which an account is considered stale can be configured in the Management Console, on the Configuration > Account Management tab.	• Event By User
Distinguished Name (Event By)	The distinguished name of the entity that generated the event	• Event By User
Domain	Filters according to the selected file server or domain.	• Event By User • Event On Group • Event On User

Filter/Refinement	Description	Available In
Event count	The number of events generated by or on the specified entity	Event Details
Event description	A description of the specified event	Event Details
Event operation	The type of operation that occurred during the event, which can be: - Accessed - Added - Changed - Removed - Sent - Received	Event Details
Events	The number of events which triggered the alert, by the specified user on the specified asset	Event Details
Event status	The status of the event, which can be one of the following: - Fail - Success	Event Details
Event time	The time at which the event occurred	Event Details
Event type	- For accounts - Indicates whether the event was created by a user or computer. - For events - Indicates the type of event.	Event Details
File name	Filters according to the specified file name.	Event On Resource
File server	Filters according to the selected file server.	- Alert On - Event On Resource
File server/Domain	Filters according to the specified file server and domain.	- Alert On - Event On Resource

Filter/Refinement	Description	Available In
File type	Filters according to the specified file type.	Event On Resource
Flags	The flags defined on the alerted entity	Event On
From department	Filters according to the <i>department</i> AD property, which is the name of the department in which the user works.	Event By User
FS owner	Filters according to the specified file system owner of the object.	Event On Resource
Group notes	The notes assigned to the users or groups on which the event was generated	Event On Group
IP Address	The computer from which the event was generated (IP address or host name)	Event By User
Is alerted	Filters to return only events on which alerts have been generated.	Event Details
Is sensitive	Filters according to whether the affected object is sensitive.	- Event By User - Event On Resource
Last logon time	Filters according to the <i>lastLogonTimeStamp</i> AD property, which is the last time a user logged in.	Event By User
Mail item type	Filters according to the selected mail item type.	Event On Resource
Mail recipient	Filters according to the specified recipient (To, CC, and BCC).	Event On Resource

Filter/Refinement	Description	Available In
Mail source	Filters according to the specified sender (from). The required format for this filter is <domain>/<user name>.	Event On Resource
Manager	Filters according to the <i>manager</i> Active Directory property.	- Alert By - Event By User
Member of group	Groups to which the user that performed the event belongs	- Event By User - Event On User
Modify date	Filters according to the date on which the object was modified.	Event On Resource
Name	Filters according to the specified user or group.	- Event On Group - Event By User - Event On User
No. of Alerted Events	The number of events having alerts	- Alert Details - Event By User
Notes	The notes assigned to the entity on which the event was generated	Event On Resource
Object type	Filters according to the affected object type.	Event Details
Operation	Filters the results according to the specified event category, which can be: - Accessed - Added - Changed - Removed - Sent - Received	Event Details

Filter/Refinement	Description	Available In
Path	Filters according to the specified path name.	Event On Resource
Privileged account type	Filters to display users classified as privileged accounts	Alert By
Rule names	Filters according to files and folders that directly contain files that have hits on the selected classification rules.	Event On Resource
SAM account name	The SAM account name of the account that generated the alert	- Alert By - Event By User
Sensitive Data Exposed	Indicates whether data marked as sensitive (with hits by DCF rules marked as sensitive) was exposed in this alert on this asset	- Alert On - Event By User
Severity	Filters according to the severity code defined in the RFC 5424 syslog protocol. The rule may be enabled, disabled or deleted.	Alert Details
Source	The source of the generated alerts	Alert Details
Stale account	Filters to display accounts for acting objects that are both disabled and stale. The amount of time after which an account is considered stale can be configured in the Management Console, on the Configuration > Account Management tab.	Event By User
Stale User Account	Accounts for acting objects that are both disabled and stale. The amount of time after which an account is considered stale can be configured in the Management Console, on the Configuration > Account Management tab.	Event By User
Status	Filters according to the status of the event, which can be one of the following: - Fail - Success	Event Details

Filter/Refinement	Description	Available In
Tags	The tags defined on the entity on which the event occurred	Event On
Alert data is flagged		Alert On
Alert data is sensitive		Alert On
Threat model name	The type of threat model which was violated	Alert Details
Total hit count	The hit count on the folder on which the event was generated	Event On Resource
Type	- For accounts - Filters according to whether the event was created by a user or computer. - For events - Filters the results according to the type of event.	- Event Details - Event By User
User	The name of the user who performed the event which triggered the alert	Alert By
User Account Type	The specified type of privileged account. Can be: - Service accounts - Admin accounts - Executive accounts - Test accounts Note: Account usage is undefined. Therefore, accounts of this type are excluded from all behavioral DatAlert rules.	Event By User
User Flags (Event By)	Aggregates the number of flags set for the user who generated the event	Event By User
User has follow-up indicators	Filters to display alerts or events generated by users marked with global flags, tags or notes	- Alert By - Event By User
User name	Filters according to the specified user	Alert By

Filter/Refinement	Description	Available In
		Event By User
User Notes (Event By)	Aggregates the notes set for the user who generated the event	Event By User
User SAM Account Name	The SAM account name of the user who generated the event	Alert By
User Tags (Event By)	Aggregates the number of tags set for the user who generated the event	Event By User
UTC Time	The UTC time at which the event occurred	Event Details
With flags	Filters according to global flags defined on the acting object.	- Event By User - Event On Group - Event On Resource - Event On User
With notes	Filters according to notes defined for users or groups.	- Event By User - Event On Group - Event On Resource - Event On User
With tags	Filters according to global tags defined on the acting object.	- Event By User - Event On Group - Event On Resource - Event On User

Complete Event Log

6.3.102

This version of the DatAlert Web Interface provides a complete event log, to facilitate conducting a full alert investigation. The log includes events that were not alerted on, so that investigators can see what else happened during the alert timeframe and learn about the normal behaviors of users who generate alerts.

Insights and Refinements

6.3.102

This version of the DatAlert Web Interface provides insights and refinements, to ease threat investigation and highlight valuable information.

- *Insights* - Located at the top of both the Events and the Alerts tabs. These insights, which are provided out of the box, provide a quick way to reach meaningful information, even before users apply a search filter or refinement.
- *Refinements* - The Refine pane presents the number of distinct values retrieved per attribute. This pane can be used to refine the scope of a search according to one or more values for a specific attribute. It also provides a quick and easy way to drill down and analyze the results per attribute.

Link to DatAlert Web Interface

6.3.102

This version provides the following links to the DatAlert Web Interface, allowing users to launch it quickly and easily:

- From **Tools > DatAlert > DatAlert Web UI**
- On the main window of the DatAlert rule configuration wizard

Advanced Search Enhancements

6.3.185

The **Select Users/Computers** dialog box has been added to the advanced search to enable selecting one or more users and computers from a list of available entities. The dialog box can be opened for the following filters:

- *User name*
- *Manager*
- *Name*
- *FS owner*

Managing Alerts

6.3.173

The DatAlert Web Interface now enables managing alerts from the **Alerts** page and the **Alert Info** page. The **Alert Management** dialog box enables changing the alert status, selecting a reason for closing the alert, adding a note to the alert and viewing recently added ones.

In the **Alerts** page, the **Alert Management** dialog box can be accessed by clicking the **More options** button located to the left of the table row and selecting **Manage Alert** from the context menu. In the **Alert Info** page, it can be accessed from the Next Steps pane or by selecting the status of the alert at the top of the page.

It is possible to select a reason for closing an alert only when the status of the alert is closed. The list of reasons can be configured in the Management Console. For more information, see [Configuring Reasons for Closing DatAlerts](#).

Exporting to CSV

6.3.173

The DatAlert Web Interface now enables exporting table data to a CSV file. The exported data reflects the results retrieved for the defined search scope.

The following information can be exported:

- Alerts and Events tables
- The data presented in an attribute's dialog box, accessible from the Refine pane
- The list of connected entities, available in all dashboards except for the Alerts dashboard

To support this enhancement, the **Export** button is now displayed in these areas.

Changes to Context Cards

6.3.173

With this version, context cards have a new look and feel.

A context card now provides the following information:

- Details about the entity:
 - *Insights* - Provides meaningful information about the entity. For example, the User context card indicates whether a user is on the Watch List or whether the account is disabled or stale. The insights that are presented vary per entity.
 - *General Information* - Provides general information about the entity (e.g., the user's email and SAM account name).
 - *Manager* - Displays the manager's name and email address. This information is only available in the User context card.
 - *Follow-Up* - Provides follow-up information (global flags and notes) about the entity. It also enables:
 - Viewing and editing notes on the entity
 - Adding or removing users from the Watch List
- An analysis of the alerts or events by the entity within the defined search scope. The Alert Search Info tab is displayed if the context card is opened from the Alerts dashboard, the **Alerts** page or the **Alert Info** page. The Event Search Info tab is displayed if the context card is opened from the **Events** page.

In addition, the following changes have been made to context cards:

- The *Threat Model Search Results*, *Category Search Results* and *Day Search Results* context cards are no longer available in the DatAlert Web Interface.
- In the Alerts dashboard, a context card can now be opened from the **More Options** context menu, available to the right of each entity in the widget.
- Users can be added or removed from the Watch List.
- Notes can be viewed or added on entities.
- It is now possible to view results based on a specific insight or attribute displayed in the entity's context card.

Watch List Global Flag

6.3.153

The Watch List flag is a unique global flag that enables keeping track of specified users at a glance. This predefined flag can be attached to users whose behavior bears special attention. While it cannot be deleted through the DatAdvantage UI, it can be detached from a specific user through the DatAlert web interface.

DatAlert Analytics Installation

6.3.153

With this version, the Management Console and Enterprise Installer enable installing and configuring the DatAlert Web Server component. This component enables monitoring and investigating the various alerts generated by DatAlert and DatAlert Analytics in the DatAlert Web Interface.

Additionally, the DatAlert and DatAlert Analytics component has been renamed to *DatAlert Analytics* to enable installing and configuring DatAlert Analytics separately.

Installing the DatAlert Web Server component requires a valid DatAlert license. The DatAlert Analytics component requires a valid DatAlert Analytics license.

Automation Engine

Automation Engine Beta Release

6.3.173

In this version, the Automation Engine remains a beta release. This includes the following modules:

- Broken Inheritance Repair
- Global Access Group Remediation

Global Access Groups Remediation Module

6.3.173

The Global Access Groups Permissions Remediation Module includes the following new functionality:

- Improved global settings functionality. These settings affect all rules, and can be overridden by rule-specific settings.
- Improved remediation functionality whereby all Global Access Group permissions are remediated, including those used by users for current activities and regardless of the number of users that are using these permissions. In order to preserve active users' permissions, these users are added as members of new permission groups. As a result, any disruption to the organizational flow is eliminated.

6.3.153

The Global Access Groups Permissions Remediation Module includes the following new functionality:

- Improved ability to define remediation scope.
- Rollback results displayed via a new report.

6.3.102

The Automation Suite now includes the Global Access Groups Remediation Module. This module enables IT to locate folders where global access permissions are not in use and safely remove (remediate) those permissions. This process reduces the security risk to the organization while avoiding any disruption to the organization's business processes.

This utility enables the following:

- Create, edit, and delete rules that determine which permissions will undergo remediation.
- Calculate the effect of the implementation of those rules on the organization's business processes.
- View the expected outcome - before remediation is performed.
- Perform immediate rollback to undo remediation if your needs are not met.

Data Transport Engine

Converting Local Groups to Domain Groups

6.3.173

In this version, it is possible to convert local groups to domain groups during data transport. If the *Grant permissions directly to domain members of local groups* option is selected, permissions of local groups are *not* copied. Rather, the same permissions are granted to the domain members of those groups at the destination. This option is not relevant if the permitted entities on the source are all domain entities.

Aged Data Retrieval Process

6.3.153

In order to prevent users from modifying archived files, the Data Transport Engine now provides a dedicated permissions mapping per rule so that administrators will be able to reduce permissions while archiving the data. In addition, the administrator can configure that rules that create stub files will automatically create a readme file that explains to users what the stub files are that they see in the folder, and what the limitations are related to using those stub files. The readme file can be either text file or a link to a custom web page.

Copying Non-Sensitive Stale Data Only

6.3.153

The Data Transport Engine now allows copying only non-sensitive files of a folder.

A new filter, *Is sensitive*, enables users to set the copying mode, where either all sensitive files or all non-sensitive files are retrieved and copied.

Note: This feature is not related to the DCF feature marking rules as sensitive.

Calculating Results of Copying Files Prior to Execution

6.3.102

A new ability has been added to the Data Transport Engine that will perform a "dry run", meaning it will calculate the results of copying files before execution. This function scans the file server (not the database), thereby providing a more accurate estimation of copied data.

Data Transport Engine Configuration Enhancements

6.3.102

Now available in 6.3.102, integrated from 6.2.51.

Prior to this version, when unique folders were transported from Windows to SharePoint, the folders at the destination were set as protected but only unique permission entries were copied from the source to the destination. With this version, the Data Transport Engine copies unique as well as inherited permission entries from the source to the destination. All inherited permission entries copied from the source will be set as unique at the destination.

Renaming Source Folders During Migration

6.3.50

It is now possible to rename source folders while migrating them to destination folders according to a predefined renaming mapping table. This option is useful when the migration includes multiple source folders with the same name, so that each source folder will have its own unique name on the destination folder. Renaming folders can be done manually or via CSV files.

DCF

New GDPR Predefined Rules List

6.3.185

The DCF has a new set of rules and regular expressions which identify Personally Identifiable Information (PII) for citizens of the European Union countries, in order to help customers comply with General Data Protection Regulation (GDPR). Rules are listed per country, with the name, description, and the accompanying patterns/logic. This content will be provided under a license (GDPR Add-on).

Countries included are as follows:

- Belgium
- Croatia
- Cyprus
- Czech Republic
- Estonia
- France
- Germany
- Greece
- Hungary
- Italy
- Latvia
- Lithuania
- Luxemburg
- Netherlands
- Poland
- Portugal
- Romania
- Spain
- United Kingdom

Importing Archived Results from RSA via DCF Lite

6.3.185

When importing archived results from RSA via DCF Lite (DCF Import), the DCF aggregates and displays on the archive file all the hits embedded within the file.

File Scanning Improvements

6.3.173

The file scanning functionality now enables extracting content from files without file extensions (configurable per file server), and introduces the ability to determine an unknown file extension through analyzing the file header.

Enhancements to Dictionary Types

6.3.173

Dictionaries now must be assigned to a product, currently either DatAlert or the DCF, thus impacting the available filters. For example, the DCF rule conditions will display only DCF-relevant dictionaries.

Support for Additional File Types - DCF and DatAnswers

6.3.173

This version adds support for Email Message File and Message Format File types:

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.eml	Email Message File	Selected by default	Selected by default	Selected by default	Selected by default
.msg	Message Format File	Selected by default	Selected by default	Selected by default	Selected by default

6.3.153

This version adds support for Open Office and Microsoft Access file types:

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.sxw	OpenOffice Writer 1.x Document	Selected by default	Selected by default	Selected by default	Selected by default
.stw	OpenOffice Writer 1.x Document Template				

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.odt	OpenOffice Writer 2.x (and above) Document	Selected by default	Selected by default	Selected by default	Selected by default
.ott	OpenOffice Writer 2.x (and above) Document Template				
.sxc	OpenOffice Calc 1.0 Spreadsheet	Selected by default	Selected by default	Selected by default	Selected by default
.stc	OpenOffice Calc 1.0 Spreadsheet Template				
.ods	OpenOffice Writer 2.x (and above) Spreadsheet	Selected by default	Selected by default	Selected by default	Selected by default
.ots	OpenOffice Writer 2.x (and above) Spreadsheet Template				

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.sxi	OpenOffice Impress 1.x Presentation	Selected by default	Selected by default	Selected by default	Selected by default
.sti	OpenOffice Impress 1.x Presentation Template				
.odp	OpenOffice Impress 2.x (and above) Presentation	Selected by default	Selected by default	Selected by default	Selected by default
.otp	OpenOffice Impress 2.x (and above) Presentation Template				
.mdb	Microsoft Access (95-2003) Database				
.accdb	Microsoft Access (2007 and above) Database				

6.3.102

In this version, additional file types are supported as support for Oracle Outside In is increased. The following file types are available for both metadata and content.

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.csv	Comma Separated Values File	Selected by default	Selected by default		
.doc	Microsoft Word Document	Selected by default	Selected by default	Selected by default	Selected by default
.docm	Microsoft Word Open XML Macro-Enabled Document	Selected by default	Selected by default	Selected by default	Selected by default
.docx	Microsoft Word Open XML Document	Selected by default	Selected by default	Selected by default	Selected by default
.dot	Microsoft Word Template				
.dotx	Microsoft Word Open XML Template				

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.dwg	AutoCad Drawing File	Selected by default	Selected by default	Selected by default	Selected by default
.dxf	AutoCad Drawing Exchange File	Selected by default	Selected by default	Selected by default	Selected by default
.log	Log File	Selected by default	Selected by default		
.one	Microsoft Onete	Selected by default	Selected by default	Selected by default	Selected by default
.onepkg	Microsoft Onete Package	Selected by default	Selected by default	Selected by default	Selected by default
.pdf	Portable Document Format File	Selected by default	Selected by default	Selected by default	Selected by default
.pot	Microsoft PowerPoint Template				
.potx	Microsoft PowerPoint Open XML Template				

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.pps	Microsoft PowerPoint Slide Show	Selected by default	Selected by default	Selected by default	Selected by default
.ppsx	Microsoft PowerPoint Open XML Show	Selected by default	Selected by default	Selected by default	Selected by default
.ppt	Microsoft PowerPoint Presentation	Selected by default	Selected by default	Selected by default	Selected by default
.pptx	Microsoft PowerPoint Open XML Presentation	Selected by default	Selected by default	Selected by default	Selected by default
.rtf	Rich Text Format File	Selected by default	Selected by default	Selected by default	Selected by default
.srt	Subtitle Text File				
.sub	Subtitle Text File				
.txt	Text File	Selected by default	Selected by default		

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.vsd	Microsoft Visio Drawing	Selected by default	Selected by default	Selected by default	Selected by default
.vsdm	Microsoft Visio Macro-Enabled-Drawing	Selected by default	Selected by default	Selected by default	Selected by default
.vsdx	Microsoft Visio Open XML Drawing	Selected by default	Selected by default	Selected by default	Selected by default
.vss	Microsoft Visio Smart Shapes				
.vssm	Microsoft Visio Macro-Enabled-Stencil				
.vssx	Microsoft Visio Stencil				
.vst	Microsoft Visio Binary Document				

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.vstm	Microsoft Visio Macro-Enabled Template				
.vstx	Microsoft Visio Template				
.xls	Microsoft Excel Spreadsheet	Selected by default	Selected by default	Selected by default	Selected by default
.xlsb	Microsoft Excel Binary Spreadsheet				
.xlsm	Microsoft Excel Macro-Enabled Spreadsheet	Selected by default	Selected by default	Selected by default	Selected by default
.xlsx	Microsoft Excel Open XML Spreadsheet	Selected by default	Selected by default	Selected by default	Selected by default
.xlt	Microsoft Excel Spreadsheet Template				

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.xltx	Microsoft Excel Open XML Spreadsheet Template				
.xml	XML File	Selected by default	Selected by default		

Enhancements to Patterns and Regular Expressions

6.3.173

- The following pattern has been added in this version:
 - US Passport Number
- The following keywords were added to the DE Driver's License number:
 - Fuhrerschein
 - Fuehrerschein
 - Fuhrerscheinnummer
 - Fuehrerscheinnummer
 - FührerscheinnummerNr
 - FuhrerscheinnummerNr
 - FuehrerscheinnummerNr

6.3.102

Now available in 6.3.102, integrated from 6.2.51.

Prior to this version, values enclosed in parentheses () or square brackets [] were excluded from the results even if they met the pattern's criteria. With this version, a match is considered valid even though the pattern is enclosed in parentheses or square brackets. For example, if a regular expression searches for 9-digit numbers, the following matches are valid:

- 123456789
- (123456789)
- [123456789]

Assignment of Global Flags to a Rule

6.3.102

This version provides the ability to assign one or more global flags to files based on DCF rule criteria. To support this enhancement, the *Enable assigning global flags to a rule* configuration option has been added to the **Security** page of the Management Console.

When creating or editing a DCF rule, users can select one or more global flags from the *Assign global flag(s)* drop-down list. Global flags are applied to files only. Flags will be unassigned automatically upon rescan if no hits were found.

Rescan Rules without Deleting Results

6.3.102

With this version, it is possible to update DCF rules and the patterns they use without automatically running a rescan. Instead, users can choose to retain the existing scan results when updating rules and patterns.

Enhancements to DCF Advanced Condition Settings

6.3.102

The DCF now enables limiting the search to specific file parts or locations in Microsoft Office files, Excel files or hyperlink addresses. This option is enabled only for the following conditions:

- String
- Regular expression
- Pattern
- Dictionary

It is possible to search for matches to these conditions in the following file locations:

- *Search everywhere* - Searches all parts of all files. This is the default value.
- *Excel files - Specific rows (any sheet)* - Searches one or more rows on any Excel sheet.
- *Office files - Header, footer or watermark (any page)* - Searches for a match to the condition in headers, footers or watermarks on any page in Microsoft Office files.
- *Hyperlink address (any page)* - Searches for a match to the condition in hyperlink addresses on any page in Office files and PDF files.

This feature is relevant only for Microsoft Office 97 until 2016 and PDF 1.0 and above.

Changes to Extended File Properties

6.3.50

Extended file properties are now defined only in the Management Console, not on the Advanced page of the DCF and DatAnswers Configuration window. Upgrading to this version does not cause DCF rules containing extended file properties to be rescanned.

Importing Special Files

6.3.50

Customers who were able to import special files with a DatAdvantage license only are no longer able to do so. With this version, customers who want to import special files must purchase a DCF or DCF Lite license.

In addition, it is no longer possible to import special files from platforms that are not supported by the DCF (e.g., Exchange).

Management Console

Incremental FileWalk

Incremental FileWalk now supports NFS protocol.

Monitoring all Top-level Shares Per Protocol

6.3.185

In the Management Console, it is now possible to configure DatAdvantage to detect and monitor automatically all top-level shares per protocol. In the Automatic Detection section of the Management Console, it is now possible to configure the *Automatically detect shares option* as *Detect, monitor and notify* or *Detect and monitor*. Both values add all the top-level shares per protocol (type) automatically as monitoring shares.

Configuring User Feedback and Log Collection

6.3.185

With this version, the Management Console now enables configuring whether users can send feedback to improve the user experience of the Varonis Metadata Framework.

In the DatAlert Web Interface, users can provide feedback about the DatAlert Web UI. For more information about the types of information Varonis collects, see [Configuring User Feedback and Log Collection through the Enterprise Installer](#).

The **Feedback and Logs** page has been added to the Configuration menu in the Management Console to support this new configuration. This page also enables configuring log collection, replacing the previous **Log Collection** page.

Both settings can be changed through the Management Console at any time.

Privileged Account Configuration Enhancements

6.3.173

With this version, the Management Console now enables editing account classification information in an exported CSV file and importing the edited file back into the Management Console. All manual changes made to the CSV file are marked as *Manual* following import.

It is also possible to create and import a file with the required account classification information. The file must be in CSV format and must contain the mandatory information (User name and SAM account name).

It is recommended to approve the classification of accounts which require feedback to help fine-tune the algorithm. The **Approve Classification** button has been added to the toolbar to support this enhancement.

In addition, the following changes have been made to the configuration of privileged user and group accounts:

- The *Status* drop-down list has been renamed to *Discovery Source*, which now displays values identical to those provided by the *Discovery Source* column.
- The *Requires feedback* option has been added to the *Discovery Source* drop-down list in the Privileged Users and Privileged Groups tabs of the **Privileged Account Discovery** page, enabling users to filter the list of accounts according to those that require feedback.

- The OU path is now provided for each listed account.
- The **Restore Default** button has been renamed to **Discard Manual Changes**.
- The **Import** button has been added to the toolbar, to enable importing the edited CSV file.

Configuring Reasons for Closing DatAlerts

The Management Console now enables configuring valid reasons for disabling or deleting alerts generated by DatAlert.

The *DatAlert Workflow* option has been added to the Configuration menu to support this configuration.

Reasons can be added, edited or removed from the list as necessary. The following reasons are predefined and cannot be modified:

- Resolved
- Misconfiguration
- Threat model disabled or deleted
- Account misclassification
- Legitimate activity
- Other

For information about selecting a reason for closing an alert, see [Managing Alerts](#).

Update Manager

The Management Console now contains the Update Manager tab, which allows deploying updates for each component, server, and client application. The updates are created by Varonis and sent to customers as VIP files.

Separate Mail Settings for DataPrivilege

6.3.153

In this version, the Management Console enables configuring separate mail settings for DataPrivilege. Configuration options include:

- Outgoing email - Overrides the settings defined for DatAdvantage
- Incoming email - Enables approving DataPrivilege requests by email.

Migrating NetApp 7-Mode to Cluster Mode

6.3.153

This feature enables customers to migrate from NetApp 7-Mode to Cluster Mode via the NetApp Migration tool (7MTT), enabling customers to continue working with the existing Shadow databases without the need to re-add all file servers.

IDU Service Components - DatAlert Web Server and DatAlert Analytics

6.3.153

With this version, the Management Console and Enterprise Installer enable installing and configuring the DatAlert Web Server component. This component enables monitoring and investigating the various alerts generated by DatAlert and DatAlert Analytics in the DatAlert Web Interface.

Additionally, the DatAlert and DatAlert Analytics component has been renamed to *DatAlert Analytics* to enable installing and configuring DatAlert Analytics separately.

The IDU Server - Service Components pane in the Management Console now displays the new components, to enable installation and configuration.

Installing the DatAlert Web Server component requires a valid DatAlert license. The DatAlert Analytics component requires a valid DatAlert Analytics license.

Storing Flattened Events

6.3.153

With this version, the Management Console now enables storing flattened events to enhance the overall performance in the DatAlert Web Interface. The DatAlert Web Server component must be installed to enable this feature.

The Event Flattening (Enhanced Web UI Performance) area has been added to the DatAlert Web Server component configuration in the Management Console to support this new enhancement. This option enables specifying the last number of days for which flat data is stored. For each day on which flattened events are stored, domain database storage use increases by approximately 2% of the Shadow database size.

Upon installation of the DatAlert Web Server component, event flattening is enabled by default. Upon upgrade, it is disabled. It is recommended to enable this feature to improve performance.

Configuration of Network Segments

6.3.153

In this version, it is possible to configure network segments and exclude specific segments from IP resolving. Unless otherwise specified, IPs are resolved to the device name for events from all segments.

Data Loss Notifications

6.3.102

The Data Loss Notifications feature now includes the ability to define the frequency of the email notifications, and define different rules for different sets of file servers. Each file server can appear in a single set only. A notification will not be sent for file servers that are predefined as excluded.

Resource Monitor Improvements

6.3.102

Several features were added to improve the resource monitor, including enabling users to decide which shares can be ignored and hence not be the subject of notifications by the resource monitor.

Designation of Executive Accounts

6.3.102

Now available in 6.3.102, integrated from 6.2.35.

This version enables automatic discovery of *executive accounts* during discovery of privileged accounts. This enables tailoring DatAlert and DatAlert Analytics rules for these sensitive accounts.

The top manager in the organization, such as the CEO or the head of the site, must be configured so that other executive accounts can be discovered automatically. This account is configured in the Management Console, through **Configuration > Privileged Account Discovery > Configuration > Executive Accounts**. If no account is configured, automatic discovery of other executive accounts cannot take place; a notification is sent to this effect.

New Jobs

6.3.102

In this version, the following jobs have been added to the new *DataPrivilege* jobs category in the Management Console:

- *DataPrivilege Entitlement Review Rules Scope Calculation* - Manages the Entitlement Review rules. Decides when and for each folder or group an Entitlement Review should be created. Once an Entitlement Review is created, it creates a new job dedicated for it.
- *EntitlementRule_XXX* - This job is executed for each entitlement rule.

In this version, the following jobs have been added to the new *Data Transport Engine* jobs category in the Management Console:

- *DTE Dry Run* - Used internally by the Data Transport Engine to execute the rule, by calculating the results of copying files before execution.

In this version, the following jobs have been added to the new *DatAdvantage* jobs category in the Management Console:

- The *SHS Walk* job has been renamed to *Share Discovery Walk*.
- The *Logs Collector* job has been renamed to *Dashboard*.

In this version, the following jobs have been added to the new *Data Classification Framework and DatAnswers* jobs category in the Management Console:

- The *Collector DCF Processing* job has been renamed to *Collector DCF Delivery*.

Now available in 6.3.102, integrated from 6.2.35.

In this version, the following jobs have been added to the new *DatAlert Analytics* jobs category in the Management Console:

- *DatAlert Analytics Trigger Publisher* - Runs when the database informs the DatAlert Analytics publisher that new rules have been configured.
- *DatAlert Analytics Calculate Entities* - Runs whenever there is a change in the accounts detected as privileged.
- *DatAlert Analytics Calc Stats* - Calculates statistics for the DatAlert Analytics rules.
- *DatAlert Analytics Windows service rules* - Runs all the rules related to atypical folders or data, not just files.
- *DatAlert Analytics Exchange rules* - Runs all the rules related to Exchange.
- *DatAlert Analytics Lockout rules* - Runs all the rules related to locking of accounts.
- *DatAlert Analytics Extensions rules* - Runs rules related to files and extensions.
- *DatAlert Analytics Crypto rules* - Runs all rules related to ransomware attacks.

6.3.50

The following jobs were added in this version:

- *Broken Inheritance Repair Rule Job* - Used internally by the Broken Inheritance Repair utility to execute the rule.

Configuring Expiration Notifications

6.3.50

It is now possible to configure the products for which to display an indication when a platform expires. By default, license expiration notifications are displayed throughout the Management Console for expired platforms.

This option is only available if one or more platforms are expired.

Incremental FileWalk Scheduler

6.3.50

The Full FileWalk schedule functionality is now available through the regular job scheduling, via the Edit Schedule button in the Jobs grid. The file server must be configured to the “incremental FW” option in order to see the Full FileWalk scheduling tab.

Installation

Configuring User Feedback and Log Collection through the Enterprise Installer

6.3.185

User Feedback

With this version, the Enterprise Installer now includes the **User Feedback** page, which enables configuring whether or not users can send feedback to improve the user experience of the Varonis Metadata Framework.

Varonis may collect, either by itself or by its trusted service providers, the following types of information from users (which may include personal information):

- Feedback rating, tags and text
- Email address (optional), IP address, browser type and language, operating system, and viewport of the screen
- URL page on which the feedback has been given
- Screen capture of the screen on which feedback was provided, with all textual strings redacted
- Varonis customer ID or customer email provided to Varonis during license registration, and the Varonis software version

The DatAlert Web Interface displays the **Feedback** button on every page, enabling users to provide feedback about the DatAlert Web Interface.

Log Collection

In addition to the above, the **Help to Improve the Varonis Metadata Framework** page in the Enterprise Installer has been renamed to **Log Collection**.

A link to the Varonis Privacy Policy has been added to the **User Feedback** and **Log Collection** pages, replacing the previous Privacy Disclaimer. The Varonis Privacy Policy can also be accessed through the **License Agreement** page of the Enterprise Installer.

Both configuration options can be changed through the Management Console at any time. For more information, see [Configuring User Feedback and Log Collection](#).

DatAlert Analytics Installation

6.3.153

With this version, the Management Console and Enterprise Installer enable installing and configuring the DatAlert Web Server component. This component enables monitoring and investigating the various alerts generated by DatAlert and DatAlert Analytics in the DatAlert Web Interface.

Additionally, the DatAlert and DatAlert Analytics component has been renamed to *DatAlert Analytics* to enable installing and configuring DatAlert Analytics separately.

Installing the DatAlert Web Server component requires a valid DatAlert license. The DatAlert Analytics component requires a valid DatAlert Analytics license.

Reports

Changes to Filters

6.3.200

The following filters have been added in this version:

Filter Name	Description
OwnersUniqueName	Filters to display the names of the data owners of the managed folders, separated by a comma. The names are the sAMAccountNames as specified in Active Directory (DataPrivilege Managed Folder User Level Permissions Report). Available in the DataPrivilege UI and in the DatAdvantage Reports API.
Is sensitive	Filters according to files and folders that contain files with hits on rules which are sensitive. (Available in the Classification menu in DatAdvantage reports 04.f, 04.g, 12.e, and 12.l).

6.3.185

The following filters have been added in this version:

Filter Name	Description
Condition Type	Filters to display matches for the selected condition types (report 19a).
Match Count	Filters according to matches whose occurrences are equal, less than or greater than the defined number (report 19a).
Staleness Method	Enables selecting between the modify date of the latest file (the current method in the report) and the access date of the latest file. For report 4.f.02.
Display Only Top-level Stale Folders	Filters for folder objects where all nested sub-folders are stale according to the staleness threshold period and the selected (or default) staleness method. For report 4.f.02.

The following filters have been changed in this version:

- A compound filter Stale date was created, and the existing Staleness Threshold filter was placed in it.

6.3.173

Changes to Report 4b.0.1

The following filters have undergone changes in this version:

- Display assigned owner: In report 4b: If set to true, information related to the folder owner is displayed. If this filter is NOT selected, the **Assigned Owner** column will NOT show the owner at all. Possible values include:
 - *Show owner name*
 - *Show all details*

The following filters have been added in this version:

Filter Name	Description
Exclude permissions granted by groups	Report 4.a.01 only. Filters out selected groups and irrelevant entries from effective permissions calculation in order to focus on relevant users and groups.
Actual added new group permissions	Filters according to the number of deleted groups in the Global Access Groups Remediation process.
Actual new created groups	Filters according to the number of new created groups in the Global Access Groups Remediation process.
Actual remediated unique folders	Filters according to the number of unique folders that were successfully remediated by the Global Access Groups remediation process.
Actual remediated unique Global Access Groups permissions	Filters according to the number of unique Global Access Groups permissions that were remediated.
Actual removed new group permissions	Filters according to the number of actual removed Global Access Group permissions.
Actual restored unique global access groups permissions	Filters according to the number of unique Global Access Groups permissions that were restored after rollback in the Global Access Groups remediation process.
Actual rolled back unique folders	Filters for the number of unique folders that were successfully rolled back to their previous states as part of the Global Access Groups remediation process.
Execution end date	Filters according to the rule execution's end date.
Expected new created groups	Filters according to the number of new Global Access Groups that are expected to be created as part of the remediation process.

Filter Name	Description
Expected remediated unique folders	Filters according to the number of unique folders from which all Global Access Group permissions were expected to be remediated.
Expected remediated unique Global Access Groups permissions	Filters according to the number of unique Global Access Group permissions that were expected to be remediated.
Max groups for a user	Filters according to the number of groups of the user with the maximum number of group memberships.
Max members in a group	Filters according to the number of members in the largest new group.
Members in new groups	Filters according to the number of users added as members to the new group in Global Access Groups remediation.
Method	Filters according to the selected remediation method.
New permitted groups	Filters according to the number of new groups with unique permissions on a specific folder.
Total number of unique global access groups permissions in scope.	Filters according to the number of unique Global Access Groups permissions in scope on the folder.
Total user access errors	Filters according to the total number of users/computers with access errors on the folder/subfolders as result of Global Access Groups permission removal.

Integrated from 6.2.70

The following filter has been added in this version:

Filter Name	Description
Exclude files with hits on these rules	Filters out only files that have hits on the selected rules. Part of the <i>Classification results</i> compound filter, this filter does not work in conjunction with the <i>Hit count</i> filter in the <i>Classification results</i> compound filter; it only excludes files that meet all other criteria in the compound, if they have the selected rules.

6.3.153**New Filters**

The following filters have been added in this version:

Filter Name	Description
Hide Errors Caused by Parent Commands	Filters out errors caused by parent commands.
Max number of matches per condition	Filters according to the display number of matched phrases per condition.
Show members of custodian groups	Filters for all the owner's group's members, and displays them in separate rows in addition to the group owner info.

The following filters have undergone changes in this version:

- Total Number of Run Errors has been changed to Run Errors.
- Total Number of Remediated Folders has been changed to Actual Remediated Folders.
- Total Number of Remediated Global Access Groups Permissions has been changed to Actual Remediated Global Access Groups Permissions.
- Total Number of Restored Permissions has been changed to Actual Restored Global Access Groups Permissions.
- Total Number of Folders with Unique Permissions of Global Access Groups in Scope has been changed to Remediated Folders.
- Total Number of Unique Global Access Groups Permissions in Scope has been changed to Expected Remediated Global Access Groups Permissions.

6.3.102**New Filters**

The following filters have been added in this version:

Filter Name	Description
Access path of folder with permission change	Filters according to the value selected in the Access Path of Folder with Permission Change column.
Change description	Filters according to the value selected in the Change Description column.
Change source	Filters the editing commands from the selected sources.

Filter Name	Description
Current effective permissions	Filters according to the value selected in the Current Effective Permissions column.
Current permissions via source	Filters according to the value selected in the Current Permissions of Source column.
Data Transport Engine rule	Filters editing commands where the source is the selected Data Transport Engine rule.
Device IP	The IP address of the user from which the event originated. Replaces IP address/hostname.
Device Name	The resolved hostname of the Device IP, from which the event originated.
Missing permission required by events	Filters according to the value selected in the Missing Permissions Required By Events column.
Permission source	Filters according to the value selected in the Permission Source column.
Recommended effective permissions	Filters according to the value selected in the Recommended Effective Permissions column.
Recommended permissions via source	Filters according to the value selected in the Recommended Permissions of Source column.
SharePoint online access path	Part of the <i>Included access paths</i> and <i>Excluded access paths</i> compound filters. Enables filtering according to the specified SharePoint resource.

Change in Access Path Filter

In some reports, the access path filter now includes the equals operator, with an option to search in all child objects. The affected reports are:

- 1a
- 2a
- 4a
- 4b
- 4f
- 4j
- 7b
- 12d

- 12e
- 12l

Changes to Report 5a

Report 5a has changed filters:

- *Change by* - Filter category is now *Changed by*.
- *Date* - Renamed to *Time of Permission Change*.

Ability to Upload List of Users/Groups from CSV/Excel

A new filter has been added to reports 3b, 4a, 4b, 4d, 4j, and 6b, which filters according to users and computers listed in a CSV file.

New Filter Operator in Rule Names Filter

Report 4G now includes the *Not contained in* filter operator for the *Rule names* filter, to exclude results from one or more DCF rules.

Now available in this version, integrated from 6.2.35

New Filters

The following filters have been added in this version:

Filter Name	Description
Alert category	Filters according to the specified alert categories. Can be: • Reconnaissance • Privilege escalation • Lateral movement • Exploitation • Exfiltration • Intrusion • Denial of service • Other
Alert ID	Filters according to the specified alert ID.
Alert severity	Filters according to the specified alert severity.
Alert source	Filters according to the specified alert source, which can be: • User-defined • Predefined

Filter Name	Description
Asset	Filters to display the item shown at the level of a volume in DatAdvantage: • CIFS file servers - Either a volume or a monitored share • SharePoint - Site collection • Exchange - Mailbox store or public folders • Directory services - Usually the domain
Excluded file name and extension	Part of the <i>File properties</i> compound filter. Returns both the name and extension of files to be excluded from the results.
Excluded file name and extension dictionary	Part of the <i>File properties</i> compound filter. Enables selecting a dictionary by which to exclude file names and extensions from the results.
File name and extension	Part of the <i>File properties</i> compound filter. Returns both the name and extension of the relevant file.
File name and extension dictionary	Part of the <i>File properties</i> compound filter. Enables selecting a dictionary according to which file names and extensions are returned.
Only alerted events	Filters to return only events on which alerts have been generated.
Show DatAlert details	Controls whether to show data in the DatAlert columns, such as Rule Name, etc.
Number of alerts	Filters according to the specified number of alerts that were generated by the same rule.
Number of events	Filters according to the specified number of events that occurred to trigger the rule.

6.3.50

New Filters

The following filters have been added in this version:

Filter Name	Description
Account type in size calculation	Defines the account types that are taken into consideration in the calculation of the following column values: • Group size % (out of domain users) • Group size % (out of all users) • No. of group members • No. of domain members If the filter is not present, both user and computer accounts are calculated.
Calculate group size	Determines how the filters in the <i>Group size</i> category are calculated. • True, whether or not other <i>Group size</i> filters are set – all new columns are calculated • Not set and no other filters are set – no effect • Not set but at least one other filter is set – all new columns are calculated
Calculate group size by direct members	Calculates the following columns on direct members only: • Group size % (out of domain users) • Group size % (out of all users) • No. group members
Changed AD property name	Provides the ability to define which scope will enable filtering on specific AD attribute changes.
Dell access paths	Part of the <i>Included access paths</i> and <i>Excluded access paths</i> compound filters. Includes or excludes all specified access paths for Dell file servers.
externalUserShareSentToEmailAddress	The email address to which sharing invitations were sent to the external user.
externalUserSignInEmailAddress	The email address used by the external user to sign in to the Office 365 portal.

Filter Name	Description
Group size % (out of domain users)	Returns a percentage representing the number of group members out of the total number of users in the domain.
Group size % (out of all users)	Returns a percentage representing the number of group members out of the total number of users.
Hide global access groups	Filters the results to hide global access groups defined in the Management Console (parent groups are not hidden).
Includes guest link	Filters according to all files in SharePoint Online that have a guest link.
Is Azure external user	Filters to return all Azure external users.
No. of domain members	Filters to return the number of users in the domain.
No. of group members	Filters to return the number of group members in the domain.
No. of group members from external domains	Filters to return the number of group members from external domains.
Permitted entity name	Filters according to rule executions that result in the permissions added, removed, or preserved on folders for the selected entity name.
Search scope	Filters according to the scope of the DatAnswers search. Options are: • Folder list • All content
Shared externally	Filters to return all files, folders and sites in SharePoint Online that are shared with external users.
Total number of added permissions	Filters according to rule executions that resulted in the specified number of added permissions.

Filter Name	Description
Total number of folders with broken inheritance in scope	Filters according to rule executions that resulted in the specified number of folders with broken inheritance in scope.
Total number of new folders	Filters according to rule executions that resulted in the specified number of new folders.
Total number of new groups	Filters according to rule executions that resulted in the specified number of new folders.
Total number of permissions with broken inheritance	Filters according to rule executions that result in the specified number of permissions with broken inheritance.
Total number of preserved permissions	Filters according to rule executions that result in the specified number of preserved permissions.
Total number of removed permissions	Filters according to rule executions that result in the specified number of removed permissions.
Total number of repaired folders	Filters according to rule executions that return the specified number of repaired folders.
Total number of repaired permissions	Filters according to rule executions that result in the specified number of repaired permissions.
Total number of run errors	The total number of errors that occurred during the execution of the rule.

New Reports in This Version

6.3.185

The following report templates are new in this version of the Data Transport Engine:

- *Report 19.a.01, Match Reports - Classification Match Review* - Displays the match count for a file's matches, and which rule conditions triggered the hit.

6.3.153

The following report template is new in this version of DatAdvantage:

- *Report 18.a.02, Global Access Groups - Run Summary - Rollback* - This report summarizes the details of each Global Access Groups rollback implementation.

6.3.102

The following report templates are new in this version of DatAdvantage:

- *Report 18.a.01, Global Access Groups - Run Summary* - This report summarizes Global Access Groups Remediation rules that have run during a defined period of time.
- *Report 18.b.01, Global Access Groups - Run Errors by Rule* - This report provides details of errors that occurred during Global Access Groups Remediation rule execution. For example, the report displays which errors occurred when trying to remove permissions of global access groups from a folder.
- *Report 18.c.01, Global Access Groups - Folders Remediated By Rule* - The Folders Remediated by Rule report provides information on folders that were remediated by rules, such as the number of removed Global Access Groups permissions.
- *Report 18.d.01, Global Access Groups - Permissions Handled By Rule* - The Permissions Handled By Rule report provides information on permissions that were handled by rules, summarizing the permissions that were added or removed on the folder for each group.
- *Report 18.e.01, Global Access Groups - Rule Snapshot* - The Rule Snapshot report provides a snapshot of each rule configuration setting as it was before every execution of the rule. The report displays all rule executions performed during the specified dates.

6.3.50

The following report templates are new in this version of DatAdvantage:

- *Report 3.d.02, Large Groups* - This report lists large groups, which are groups containing more than 80% of the domain members (users and computers) monitored in DatAdvantage in all domains.
- *Report 17.a.01, Broken Inheritance Repair - Run Summary* - This report summarizes Broken Inheritance Repair rules that have run during a defined period of time.
- *Report 17.b.01, Broken Inheritance Repair - Run Errors By Rule* - This report provides details of errors that occurred when a rule was executed, such as when repairing inconsistent permissions in a folder.
- *Report 17.c.01, Broken Inheritance Repair - Folders Repaired by Rules* - This report lists and provides information on folders that were repaired by rules, such as the number of repaired permissions, and the number of added, removed, and preserved permissions.

- *Report 17.d.01, Broken Inheritance Repair - Folder Permissions Handled By Rule* - This report summarizes the folder permissions that were added, removed, or preserved on each folder by Broken Inheritance Repair.
- *Report 17.e.01, Broken Inheritance Repair - Rule Snapshot* - This report provides a snapshot of each rule's configuration settings prior to each execution of the rule. The report displays all rule executions performed on the specified dates.

Changes to Existing Reports

6.3.173

The following changes have been made to existing reports in this version:

- Report capping is now applied only to reports.
- *4.b.01, User or Group Permissions for Directory:*
The following columns were added:
 - *Assigned Owner* - It includes information related to the assigned owners on the folder.
- *4n, Share Discovery Report:*
The following values were added:
 - Server Not Monitored, Share Not Monitored
 - Server Monitored, Share Monitored
 - Server Monitored, Share Not Monitored
- *18.a.01, Global Access Groups - Run Summary - Execution:*
The following columns were added:
 - *Actual New Created Groups*
 - *Actual Remediated Unique Folders*
 - *Actual Remediated Unique Global Access Groups Permissions*
 - *Expected New Created Groups*
 - *Expected Remediated Unique Folders*
 - *Expected Remediated Unique Global Access Groups Permissions*
 - *Max Members in a Group*
 - *Max Groups for a User*
 - *Method*
 - *Prevented Access Errors*
 - *Actual Added New Group Permissions*
 - *Actual Deleted New Groups*
 - *Actual Removed New Group Permissions*
 - *Actual Restored Unique Global Access Groups Permissions*
 - *Actual Rolled Back Folders*
 - *Actual Rolled Back Unique Folders*
- *18.a.02, Global Access Groups - Run Summary - Rollback:*

The following columns were added:

- *Actual Added New Group Permissions*
- *Actual Created New Groups*
- *Actual Deleted New Groups*
- *Actual Remediated Unique Folders*
- *Actual Removed New Group Permissions*
- *Actual Restored Unique Global Access Groups Permissions*
- *Actual Rolled Back Folders*
- *Actual Rolled Back Unique Folders*
- *18.b.01, Global Access Groups - Run Errors by Rule:*

The following columns were added:

- *Method*
- *Action Details*
- *18.c.01, Global Access Groups - Folders Remediated by Rule:*

The following columns were added:

- *Members in New Groups*
- *New Permitted Groups*
- *Expected Remediated Global Access Groups Permissions* was changed to *Total Number of Unique Global Access Groups Permissions in Scope*
- *18.d.01, Global Access Groups - Permissions Handled by Rule:*

The following columns were added:

- *Method*
- *Permitted Groups Name*
- *Rule Type*
- *Rule Creator*
- *Rule Description*
- *Rule Name*
- *18.e.01, Global Access Groups - Rule Snapshot:*

The following columns were added:

- *Group Limitations*
- *Log off Waiting Period*
- *Method*
- *New Groups Details*

- *New Groups Permission Mapping*
- *User Memberships Limitations*

6.3.153

The following changes have been made to existing reports in this version:

- *3.d.01, Users and Groups List:*
 - The following columns were added:
 - *Ownership Source*
- *4.f.01, File System Objects List:*
 - The following columns were added:
 - *Ownership Source*
- *18.a.01, Run Summary - Execution:*
 - *Total Number of Remediated Folders* was renamed to *Actual Remediated Folders*
 - *Total Number of Folders with Unique Permissions of Global Access Groups in Scope* was renamed to *Expected Remediated Folders*
 - *Total Number of Remediated Global Access Groups Permissions* was renamed to *Actual Remediated Global Access Groups Permissions*
 - *Total Number of Unique Global Access Groups Permissions in Scope* was renamed to *Expected Remediated Global Access Groups Permissions*
 - *Total Number of Run Errors* was renamed to *Run Errors*
 - *Total Number of Restored Permissions* was renamed to *Actual Restored Global Access Groups Permissions*
 - The following columns were added:
 - *Rule Type*
- *18.b.01, Run Errors By Rule:*
 - The following columns were added:
 - *Rule Type*
- *18.e.01, Rule Snapshot:*
 - The following columns were added:
 - *Included Scope*
 - *Excluded Scope*
 - *Administrative Notifications*
 - The following columns were removed:
 - *Scope*
 - *Commit Credentials*

6.3.102

The following changes have been made to existing reports in this version:

- The IP address/hostname field or parameter in filters and various reports has been split into two separate columns, *Device IP Address* and *Device Name*.
 - *Device IP Address* - The IP address of the user from which the event originated.
 - *Device Name* - The resolved host name of the Device IP, from which the event originated.

The affected reports are as follows:

- 1a
- 1b
- Report 5a has new columns:
 - *Permission Source*
 - *Current Permissions via Source*
 - *Current Flags via Source*
 - *Recommended Permissions via Source*
 - *Recommended Flags via Source*
 - *Current Effective Permissions*
 - *Recommended Effective Permissions*
 - *Missing Permission Required by Events*
 - *Access Path of Folder with Permission Change*
 - *Time of Permission Change*
 - *Change By*
 - *Change Description*
- Report 5a has new filters:
 - *Current permissions via source*
 - *Recommended permissions via source*
 - *Current effective permissions*
 - *Recommended effective permissions*
 - *Missing permission required by events*
 - *Access path of folder with permission change*
 - *Change description*
 - *Permission source*
 - *Change source* (also for 5b and 5c)
 - *Data Transport Engine rule* (also for 5b and 5c)

6.3.50

The following changes have been made to existing reports in this version:

- Category 3 has been renamed to *Group Membership*.
- The following additional columns have been added to report 15a:
 - *Added Folder Name*
 - *Search Scope*
- *No. of Enabled Users with Password that Never Expires* can be added as an additional column to reports 14d and 14e.

Query RESTful API Improvements

6.3.173

This version provides the following enhancements to the Query RESTful API:

- For use in queries, the API documentation now lists the supported filter values for DataPrivilege and DatAdvantage. Also included are how the filters are displayed in the UI, and how they must be written in the API query.
- A new section is provided which provides sample code (C#) and describes how to use the API. Procedures include Accessing the Sample Code, Updating the NuGet Resource, and Running the Sample Code.
- The Query RESTful API exposes the following reports for DataPrivilege:
 - Managed Folder User Level Permission
 - Managed Folder Permissions

Accessing SharePoint Objects via URL in Reports

6.3.102

Now available in 6.3.102 *for all reports*, integrated from 6.2.51.

It is now possible to access SharePoint content (files and folders) directly from reports 4.f.1 and 4.g.1 via a valid URL.

Query RESTful API

6.3.102

Now available in this version, integrated from 6.2.15.

This version provides the DatAdvantage reporting API. The Query RESTful API enables querying DatAdvantage and using the retrieved data in other applications.

Important: Contact Varonis Support for assistance in activating the API.

The Query RESTful API supports the following reports:

- 1.a, User Access Log
- 2.a, Access Statistics Report
- 3.a, Group Members
- 3.e, Historical Group Membership
- 4.b, User or Group Permissions for Directory
- 4.f, File System Objects List
- 4.j, Effective Share and NTFS Permissions for Users and Groups
- 4.k, Historical Effective User or Group Permissions
- 4.m, Delegate Permissions (Permissions for Users and Groups Other than the Mailbox Owner)
- 10.a, Ownership

Documentation describing the API is provided in the Reference folder of the documentation package.

Changes to Report Functionality

6.2.70

In this version, the new *ShouldAlwaysLimitReportServerExportOutputRows* configuration key enables setting how report subscriptions are generated.

Note: In order to change the key, you must contact Technical Support.

- If set to 0
 - For subscriptions that *do not* exceed the defined threshold (*Maximum rows to display in report*) - Only one file is created, in the format selected by the user.
 - For subscriptions that *do* exceed the defined threshold - Two files are created:
 - One short file in the format selected by the user, containing only the number of rows specified by the *Maximum rows to display in report* option.
 - One full file in CSV format, containing the complete results.
- If set to 1 - For all subscriptions - Two files are created:
 - One short file in the format selected by the user, containing only the number of rows specified by the *Maximum rows to display in report* option.
 - One full file in CSV format, containing the complete results.

6.3.100

Now available in this version, integrated from 6.2.15.

In this version, the following changes have been made to reports:

- Report subscriptions can now be exported to the XLSX format.
- The column headers in the subscription CSV files now match those of reports generated in the UI.
- Data-driven subscriptions now support Traditional Chinese.

DatAnswers

Default Searched Languages

6.3.50

By default, the searched languages are those configured in an individual user's browser. These settings are used until the user specifically changes them.

DatAnswers over HTTPS

6.3.50

DatAnswers can now be configured over HTTPS. Instructions for such configuration are included as an appendix in the *Management Console User Guide*.

Support for Chinese

6.3.50

In this version, DatAnswers supports searching in both Simplified and Traditional Chinese.

Changes to Extended File Properties

6.3.50

Extended file properties are now defined only in the Management Console, not on the Advanced page of the DCF and DatAnswers Configuration window. Upgrading to this version does not cause DCF rules containing extended file properties to be rescanned.

Support for SharePoint Online Items

6.3.50

DatAnswers now supports selecting scopes for SharePoint Online items, such as document libraries, sites, lists and OneDrive for Business personal sites.

Core and Infrastructure

Windows Server 2016

6.3.173

This version adds support for Windows Server 2016, for both IDU Server installation and as a monitored file server.

Active Directory 2016

6.3.173

This version adds support for Microsoft Active Directory 2016, for both IDU Server installation and as a monitored file server (directory services).

Disk Space Limits

6.3.173

In this version, report capping is applied only to report generation. Scope calculations (in DatAlert, the DCF, and the Data Transport Engine) are not capped.

Access Denied Events on Hitachi NAS Devices

6.3.173

This version provides support for Access Denied events on Hitachi NAS devices.

End of Life for Windows 2008 and 2008 SP1 for DatAlert Analytics

6.3.153

With this version, Varonis declares end of life for Windows 2008 and 2008 SP1 **for the server on which DatAlert Analytics is installed**. These Windows versions may still be used for other Metadata Framework products.

EMC Unity Support

6.3.153

This version adds support for EMC Unity 4.1 and Unity Family 300-600, including events. EMC Unity interacts with the Metadata Framework via the EMC CEPA mechanism.

SQL Server 2016

6.3.153

This version adds support for SQL Server 2016.

Changes to Jobs

6.3.153

In this version, the DatAlert Analytics jobs have been changed.

- The following jobs have been added:

Job Name	Description
DatAlert Analytics Alert Generation and Profile Updates	Compares events to saved profiles and generates alerts if required. Updates profiles.
DatAlert Analytics Execute Learning	Runs learning on existing database using three months of historical data.
DatAlert Analytics Export	Exports events and associated data for the calculation of alerts and profiles.
DatAlert Analytics Import	Imports statistical data from the engine to the database.
DatAlert Analytics Peers Calculation	Calculates peers for each user.
DatAlert Analytics Peers Optimal Configuration	Selects the optimal configuration for peer calculation.

Job Name	Description
DatAlert Analytics Work Hours Calculation	Calculates the regular work hours of each of the users.

- The following jobs have been removed:

Job Name	Description
DatAlert Analytics Calculate Entities	Runs whenever there is a change in the accounts detected as privileged.
DatAlert Analytics Trigger Publisher	Runs when the database informs the DatAlert Analytics publisher that new rules have been configured.

Support for Oracle Outside In Technology

6.3.153

With this version, the DCF and DatAnswers support Open Office and Access file types.

6.3.50

With this version, the DCF and DatAnswers support Oracle Outside In technology for Microsoft Office and PDF file types. There is no need for iFilters for these file types. Outside In is installed automatically; there is no need for further configuration.

Support for Additional File Types - DCF and DatAnswers

6.3.173

This version adds support for Email Message File and Message Format File types:

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.eml	Email Message File	Selected by default	Selected by default	Selected by default	Selected by default
.msg	Message Format File	Selected by default	Selected by default	Selected by default	Selected by default

6.3.153

This version adds support for Open Office and Microsoft Access file types:

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.sxw	OpenOffice Writer 1.x Document	Selected by default	Selected by default	Selected by default	Selected by default
.stw	OpenOffice Writer 1.x Document Template				

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.odt	OpenOffice Writer 2.x (and above) Document	Selected by default	Selected by default	Selected by default	Selected by default
.ott	OpenOffice Writer 2.x (and above) Document Template				
.sxc	OpenOffice Calc 1.0 Spreadsheet	Selected by default	Selected by default	Selected by default	Selected by default
.stc	OpenOffice Calc 1.0 Spreadsheet Template				
.ods	OpenOffice Writer 2.x (and above) Spreadsheet	Selected by default	Selected by default	Selected by default	Selected by default
.ots	OpenOffice Writer 2.x (and above) Spreadsheet Template				

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.sxi	OpenOffice Impress 1.x Presentation	Selected by default	Selected by default	Selected by default	Selected by default
.sti	OpenOffice Impress 1.x Presentation Template				
.odp	OpenOffice Impress 2.x (and above) Presentation	Selected by default	Selected by default	Selected by default	Selected by default
.otp	OpenOffice Impress 2.x (and above) Presentation Template				
.mdb	Microsoft Access (95-2003) Database				
.accdb	Microsoft Access (2007 and above) Database				

6.3.102

In this version, additional file types are supported as support for Oracle Outside In is increased. The following file types are available for both metadata and content.

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.csv	Comma Separated Values File	Selected by default	Selected by default		
.doc	Microsoft Word Document	Selected by default	Selected by default	Selected by default	Selected by default
.docm	Microsoft Word Open XML Macro-Enabled Document	Selected by default	Selected by default	Selected by default	Selected by default
.docx	Microsoft Word Open XML Document	Selected by default	Selected by default	Selected by default	Selected by default
.dot	Microsoft Word Template				
.dotx	Microsoft Word Open XML Template				

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.dwg	AutoCad Drawing File	Selected by default	Selected by default	Selected by default	Selected by default
.dxf	AutoCad Drawing Exchange File	Selected by default	Selected by default	Selected by default	Selected by default
.log	Log File	Selected by default	Selected by default		
.one	Microsoft Onete	Selected by default	Selected by default	Selected by default	Selected by default
.onepkg	Microsoft Onete Package	Selected by default	Selected by default	Selected by default	Selected by default
.pdf	Portable Document Format File	Selected by default	Selected by default	Selected by default	Selected by default
.pot	Microsoft PowerPoint Template				
.potx	Microsoft PowerPoint Open XML Template				

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.pps	Microsoft PowerPoint Slide Show	Selected by default	Selected by default	Selected by default	Selected by default
.ppsx	Microsoft PowerPoint Open XML Show	Selected by default	Selected by default	Selected by default	Selected by default
.ppt	Microsoft PowerPoint Presentation	Selected by default	Selected by default	Selected by default	Selected by default
.pptx	Microsoft PowerPoint Open XML Presentation	Selected by default	Selected by default	Selected by default	Selected by default
.rtf	Rich Text Format File	Selected by default	Selected by default	Selected by default	Selected by default
.srt	Subtitle Text File				
.sub	Subtitle Text File				
.txt	Text File	Selected by default	Selected by default		

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.vsd	Microsoft Visio Drawing	Selected by default	Selected by default	Selected by default	Selected by default
.vsdm	Microsoft Visio Macro-Enabled-Drawing	Selected by default	Selected by default	Selected by default	Selected by default
.vsdx	Microsoft Visio Open XML Drawing	Selected by default	Selected by default	Selected by default	Selected by default
.vss	Microsoft Visio Smart Shapes				
.vssm	Microsoft Visio Macro-Enabled-Stencil				
.vssx	Microsoft Visio Stencil				
.vst	Microsoft Visio Binary Document				

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.vstm	Microsoft Visio Macro-Enabled Template				
.vstx	Microsoft Visio Template				
.xls	Microsoft Excel Spreadsheet	Selected by default	Selected by default	Selected by default	Selected by default
.xlsb	Microsoft Excel Binary Spreadsheet				
.xlsm	Microsoft Excel Macro-Enabled Spreadsheet	Selected by default	Selected by default	Selected by default	Selected by default
.xlsx	Microsoft Excel Open XML Spreadsheet	Selected by default	Selected by default	Selected by default	Selected by default
.xlt	Microsoft Excel Spreadsheet Template				

Extension	Description	DCF Metadata	DCF Content	DatAnswers Metadata	DatAnswers Content
.xltx	Microsoft Excel Open XML Spreadsheet Template				
.xml	XML File	Selected by default	Selected by default		

New Exchange On-Premises Events

6.3.153

With this version, DatAlerts can now be generated upon the addition or removal of forward delivery options in Exchange file servers.

The following Exchange On-Premises events are now supported:

- *Mailbox forward delivery option added*
- *Mailbox forward delivery option removed*

These event types are supported in Exchange 2010 only, by PowerShell and EMC.

The Management Console now enables configuring these event types, which are monitored by default. In addition, the new event types have been added to the list of *Event Type* filter options in the DatAdvantage log and in the **What (Event Details)** page of the DatAlert **Add Rule** window. These event types can be added to rules so that DatAlerts are generated.

End of Life for SQL Server 2005

6.3.102

With this version, Varonis declares end of life for SQL Server 2005. It is no longer possible to install or upgrade the Metadata Framework using this version of SQL Server. Any customer still using it must upgrade to at least SQL Server 2008 to continue working with the Metadata Framework. The following versions are supported:

- 2008 Standard or Enterprise, with SP3 and above
- 2008 R2 Standard or Enterprise, with SP3 and above
- 2012 Standard or Enterprise, with or without SP1, SP2 or SP3
- 2012 R2 Standard or Enterprise

Note: Cumulative Update 4 is also required.

- 2014 Standard or Enterprise, with or without SP1

Note: Cumulative Update 6 is also required.

- 2016
 - For 2016 - See Microsoft [KB 3182270](#)
 - SP1 or higher

Support for Scality RING File Servers

6.3.102

This version provides support for Scality RING file servers. The following version is supported:

- 5.0.6

Integration with CyberArk Application Identity Manager

6.3.102

In this version, the Metadata Framework integrates with CyberArk Application Identity Manager. The CyberArk vault manages all passwords required by the user accounts that are used by DatAdvantage and DataPrivilege for daily work.

- Passwords are still stored by Varonis components. It is not possible to manage all passwords used by the Metadata Framework via CyberArk; only those which require elevated permissions are managed thus.
- A new database job polls the CyberArk vault for updated passwords of the user accounts that run specific tasks such as FileWalk.
- The change does not affect installation or configuration; for these tasks, passwords are still required.
- CyberArk installation, configuration and maintenance is the customer's responsibility. This includes:
 - Creating and configuring the Varonis vault
 - Adding users to the vault and removing them
 - Installing CyberArk providers on all Varonis IDU servers
 - Maintaining the vault's configuration after upgrade

Support for Linux

6.3.102

This version provides support for

- Oracle Linux Server:
 - SMP - 64 bit
 - Release 6.3: kernel 2.6.39-200
 - Release 6.8: kernel 3.8.13-118
- Red Hat 6 Kernel 2.6.32
 - SMP - X86 64 bit
 - 2.6.32-279
 - 2.6.32-642
- SUSE SLES 11.4 Kernel 3.0.101
 - SMP - 64 bit
 - 3.0.101-63
 - 3.0.101-68
- SUSE SLES 12.1 Kernel 3.12.49 - Supported types:
 - SMP - 64 bit
 - 3.12.49-11

Now available in this version, integrated from 6.2.51

- Ubuntu 14.04 LTS Kernel 3.13.0
 - SMP - 64 bit
 - 3.13.0-74

6.3.50

This version provides support for Linux Red Hat 6, 2.6.32-573.3.1.el6.x86_64 and Ubuntu 12.04 kernel 3.2.0-83-generic 64 bit.

Support for Windows 7 as a File Server

6.3.102

In this version, Windows 7 x64 is supported as a file server.

Change Permission Events on IBM Storwize

6.3.102

This version includes support for Change Permission events on IBM Storwize V7000.

Increased Support for Source IP in Events

6.3.102

Now available in this version, integrated from 6.2.35.

This version provides increased support for the source IP in events. To collect the source IP, the Varonis agent must be upgraded and the relevant file server must be restarted.

Support now includes the following platforms:

Platform	IP Support	Comments
Windows	Yes	
Unix	No	AIX, Solaris
Linux	Yes	
SharePoint On-Premises	Yes	
SharePoint O365	Yes	
Exchange On-Premises	Partial	DeviceID for ActiveSync. IP for Outlook clients on Exchange 2007 and 2010 if IP agents are installed on CAS servers.
Exchange O365	No	
NetApp and NetApp CM	Yes	
EMC CEPA and Isilon	Yes	
EMC Celerra	No	
Hitachi NAS	Yes	
Unix SMB	Yes	
HP NAS	No	

Platform	IP Support	Comments
Directory Services	Yes	

Support for Windows 10 as a File Server

6.3.50

In this version, Windows 10 x64 is supported as a file server.

Support for Dell FluidFS File Systems

6.3.50

This version provides support for Dell Fluid File Systems, such as EqualLogic and Compellent. All Dell servers using FluidFS 6.2 are supported.

- Local accounts are not supported.
- DataPrivilege supports only the CIFS portion of the server.
- Permission Change events are collected only on the folder on which they occurred, not the sub-tree.

Support for Access Denied Events on EMC

6.3.50

In this version, additional support is provided for Access Denied CIFS events on EMC Celerra/VNX servers. The following Access Denied events are supported:

- File Create
- File Delete
- File Open
- File Modify
- File Rename
- File Set Permissions
- Folder Create
- Folder Open
- Folder Rename
- Folder Delete
- Folder Set Permissions

EMC Isilon Support

6.3.160

This version adds support for Isilon 8.1.

6.3.50

This version adds support for Isilon 8.0.x, including NFS events.

Support for Exchange 2016

6.3.160

The Metadata Framework Exchange agent for Exchange 2016 is now generally available (GA).

6.3.50

This version provides beta support for Exchange 2016.

Support for Solaris

6.3.50

This version adds support for Solaris 11 sparc.

Restricting FileWalk's Schedule

6.3.50

This feature enables FileWalk's run schedule to be restricted to specific hours. If the run is not finished, it will be paused, whereupon it will continue the next day from the point where it was paused. As a result, it might take several days for FileWalk to complete one full run. To enable this feature, FileWalk's permitted run schedule can be configured in the configuration file.

Licensing

GDPR Patterns License

6.3.185

Now available.

The GDPR Patterns license is required to use GDPR predefined patterns and rules in the Data Classification Framework and to retrieve classification results based on GDPR content.

This license requires a valid DCF license and cannot be purchased separately. At least one DCF platform *must* be valid.

The behavior of the GDPR Patterns license changes as follows when the number of days set for the license is reached:

During Grace Period	Expired
• Will continue to scan and index data • Will continue to display GDPR patterns in the Patterns repository • Will continue to display predefined GDPR rules in the Classification Rules tab of the DCF and DW Configuration window • All GDPR rules will continue to be enabled	• All classification results retrieved by using GDPR content will be deleted • Will cease to display GDPR patterns in the Patterns repository • Will cease to display predefined GDPR rules in the Classification Rules tab of the DCF and DW Configuration window • All GDPR-related rules will be disabled. User-defined GDPR rules will continue to be displayed in the Classification Rules tab of the DCF and DW Configuration window.

Enhancements to the Automation Engine Evaluation License

6.3.185

With this version, license site administrators can now enforce or remove the limitations defined in the Automation Engine Evaluation license.

The *Enforce limitations* checkbox is now displayed in the Automation Engine area of the license site. By default, this option is selected. Only users with the License Site Admin or License Site Support Admin roles can view this new option in the license site.

This option is not relevant for customers who have a permanent Automation Engine license.

DatAlert Analytics License

6.3.102

DatAlert Analytics now requires a separate license from standard DatAlert. However, while a standard DatAlert license can be purchased without DatAlert Analytics, the DatAlert Analytics license can only be purchased if a standard DatAlert license is also purchased.

DCF Lite License Enforcement

6.3.102

This version provides license enforcement improvements to the DCF Lite license. This license is required in order to import files from external sources.

License Configuration Changes

6.3.102

With this version, the **License Configuration** page of the Varonis Setup Wizard now enables entering the ID of the customer for validation purposes. It is possible to enter either the customer ID or email. If selected, the ID replaces the email as the customer identifier.

The customer ID is displayed together with the serial number, which is supplied by Varonis.

OneDrive for Business License

6.3.102

With this version, OneDrive for Business now requires a separate license from the SharePoint Online license. The OneDrive license is required in order to add OneDrive file servers through the Management Console and monitor OneDrive for Business sites.

Office 365 License Changes

With this version, the following licenses are now available:

- SharePoint Online - Full
- OneDrive - Full
- DatAnswers - SharePoint Online
- DatAnswers - OneDrive

The SharePoint Online and OneDrive full licenses include auditing and event collection capabilities. These licenses are separate from the Office 365 Lite licenses, which provide bi-directional visibility only, and must be purchased separately. A full Office 365 license can be purchased only if the corresponding Office 365 Lite license is purchased.

Note: The DatAdvantage Lite license supports Office 365 Lite licenses only. It does not support full Office 365 licenses.

In addition, the following changes have been made:

- The number of days set for the SharePoint Online full license cannot exceed the number of days set for the SharePoint Online Lite license.
- When DCF or DatAnswers is selected for a particular platform in the license site, the corresponding DatAdvantage license must also be selected. For example, DatAdvantage for SharePoint must be selected when Data Classification for SharePoint is selected.
- DatAlert can be selected only if a license with auditing capabilities (e.g., Windows, Unix, SharePoint Online auditing, etc.) is selected.
- The Data Transport Engine is supported for Windows and on-premises SharePoint only. The corresponding DatAdvantage licenses must be selected.

DatAnswers and DCF License Enhancements

6.3.50

With this version, DCF and DatAnswers licenses can now be installed per platform. In addition, DatAnswers can be installed without a valid DatAdvantage license.

Data Classification Framework

Licensing for the DCF requires the general DatAdvantage license.

A DCF license can be purchased for one or more of the following platforms:

- Windows and SharePoint
- Unix
- SharePoint Online
- OneDrive

When a DCF license is selected for a particular platform in the license site, the corresponding DatAdvantage license must also be selected.

The behavior of the DCF license changes as follows when the number of days set for a particular platform's license is reached:

Component	During Grace Period	Expired
Data Classification Engine	Will continue to run. Folders will be scanned and classified based on existing rules.	Will cease to run.

Component	During Grace Period	Expired
DCF and DW Configuration and Monitor	Will continue to be available. Data for the relevant platform will be presented.	Will cease to be available. Data for the relevant platform will not be presented.
DatAdvantage UI	• Will not present data regarding special files and classification hit counts • Volumes of mixed file servers - Will continue to display data regarding special files and classification hit counts provided that at least one license is in grace or valid.	• Will not present data regarding special files and classification hit counts • Volumes of mixed file servers - Will continue to display data regarding special files and classification hit counts provided that at least one license is in grace or valid.
Reports and log	• Will not present data regarding special files and classification hit counts • DCF-related filters will cease to retrieve data • Reports 8a, 8c and 8d - Will continue to display data	• Will not present data regarding special files and classification hit counts • DCF-related filters will cease to retrieve data • Reports 8a, 8c and 8d - Will continue to display data
DatAlert and DTE	• Sensitive files will be removed from scopes • DCF-related filters will cease to retrieve data	• Sensitive files will be removed from scopes • DCF-related filters will cease to retrieve data
Errors, statistics and alerts	Will cease to display data regarding special files and classification hit counts.	Will cease to display data regarding special files and classification hit counts.

Indications of expired licenses will *not* be displayed in the DatAdvantage and Management Console UIs for platforms that are in grace or that have an expired DCF license. An expired license notification will be displayed when the UI is opened. In addition, email notifications will be sent to the system administrator regarding the license expiration.

If the DCF license expires for one or more platforms, the **DCF and DW Configuration** window and monitor will continue to display specific options, provided that at least one platform is in grace or valid for DatAnswers.

Note: For DCF Lite, only the Schedules, File Types, Priorities and Advanced tabs in the **DCF and DW Configuration** window will be available, provided that at least one platform is valid.

DatAnswers

A DatAnswers license can be purchased for one or more of the following platforms:

- Windows
- SharePoint
- SharePoint Online
- OneDrive

The behavior of the DatAnswers license changes as follows if it is purchased without the DatAdvantage license:

- Installation
 - The Metadata Framework Infrastructure license must be installed.
 - Will continue to be installed through the Management Console.
 - Only the Active Directory domain type can be installed.
 - When configuring domain properties during installation, the option to crawl directory services for structure and permissions will not be available.
 - Only relevant file servers will be available for selection.
- Crawling and event collection
 - Will continue on all defined file servers.
- DatAnswers - Will display search results in the DatAnswers UI.
- Management Console - The *Expiration Notification* option will be available in the File Server settings, which enables selecting the products for which to display an indication when a platform expires.
- Jobs - All DatAnswers, DatAdvantage (those relevant) and DCF jobs will run on all defined file servers and volumes of mixed file servers.
- DCF
 - The **DCF and DW Configuration** window and DCF and DW Monitor will be available.
 - Will scan and index data for DatAnswers.
 - The options to add new rules and import special files will be disabled.
- DatAdvantage
 - Will display the Reports view only. All reports will be displayed. However, data will be retrieved only for the following reports:
 - All DatAnswers reports (category 15)
 - Report 5.b.01, Recommended Changes on User Repository
 - Report 8.a.01, Customer Data
 - Report 8.c.01, Active User Count by Platform
 - Report 8.c.02, Active User List by Platform
 - Report 8.d.01, Potential User Count by Platform
 - Report 8.d.02, Potential User List by Platform
 - Defining subscriptions and managing templates will be available only for the above reports.

- Pickers will continue to display folders from relevant platforms. These folders are available for selection.
- Only the following options are available from the Tools menu:
 - Select IDU Server
 - DCF and DW
 - Management Console

The behavior of the DatAnswers license changes as follows when the number of days set for a particular platform's license is reached:

Note: The below information is also relevant for evaluation licenses.

Component	During Grace Period	Expired
DatAnswers UI	Will cease to display data related to the platform	Will cease to display data related to the platform
DCF	Will continue to run. Folders will be scanned and classified based on existing rules.	Will cease to run
DCF and DW Configuration and Monitor	Will continue to be available. Data for the relevant platform will be presented.	Will cease to be available. Data for the relevant platform will not be presented.
Reports	• DatAnswers reports and Report 5b - Will cease to display data • Reports 8a, 8c and 8d - Will continue to display data	• Will cease to display data • Reports 8a, 8c and 8d - Will continue to display data

Indications of expired licenses will be displayed in the DatAdvantage and Management Console UIs for platforms that are in grace or that have an expired DatAnswers license. The indications will display the product for which the platforms are expired. An expired license notification will be displayed when the UI is opened. In addition, email notifications will be sent to the system administrator regarding the license expiration.

If the DatAnswers license expires for one or more platforms, the **DCF and DW Configuration** window and monitor will continue to display specific options, provided that at least one platform is in grace or valid for DatAdvantage and the DCF.

Licensed Users and Data Counters

The behavior of the licenses changes as follows when the licensed users and data counters have exceeded their configured limit:

- If the *Enforce users number* or *Enforce size data* options are selected, the 30-day grace period will begin.
- If the *Enforce users number* or *Enforce size data* options are cleared, the Metadata Framework will remain as it was prior to the grace period. Additionally, mail alerts will be sent regarding pending license expiration.

If the counters return to their configured limit, the 30-day grace period will be cancelled. Folders and users can be set as unmonitored in the Management Console so that the counters' configured limit is not exceeded.

Upgrade

Upgrade Flows

6.3.190

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x through 6.2.8x, and 6.3.x directly to 6.3.190.
- DatAdvantage+DataPrivilege 6.2.x and 6.3.x installations cannot be upgraded separately.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.

Source DataPrivilege Version	Possible Upgrade
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	- Distributed environments: - Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. - Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. - Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. - Consolidated environments: - Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. - Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.189

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x through 6.2.8x, and 6.3.x directly to 6.3.189.
- DatAdvantage+DataPrivilege 6.2.x and 6.3.x installations cannot be upgraded separately.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.

Source DataPrivilege Version	Possible Upgrade
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.188

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x through 6.2.8x, and 6.3.x directly to 6.3.188.
- DatAdvantage+DataPrivilege 6.2.x and 6.3.x installations cannot be upgraded separately.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.187

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x through 6.2.8x, and 6.3.x directly to 6.3.187.
- DatAdvantage+DataPrivilege 6.2.x and 6.3.x installations cannot be upgraded separately.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.186

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x through 6.2.8x, and 6.3.x directly to 6.3.186.
- DatAdvantage+DataPrivilege 6.2.x and 6.3.x installations cannot be upgraded separately.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.185

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x through 6.2.8x, and 6.3.x directly to 6.3.185.
- DatAdvantage+DataPrivilege 6.2.x and 6.3.x installations cannot be upgraded separately.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.173

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x through 6.2.8x, and 6.3.x directly to 6.3.173.
- DatAdvantage+DataPrivilege 6.2.x and 6.3.x installations cannot be upgraded separately.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.163

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x through 6.2.8x, and 6.3.x directly to 6.3.163.

Note: Although upgrade from 6.2.8x is supported, 6.3.163 only includes content up to 6.2.7x. It does not include 6.2.8x.

- DatAdvantage+DataPrivilege 6.2.x and 6.3.x installations cannot be upgraded separately.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.162

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x through 6.2.8x, and 6.3.x directly to 6.3.162.

Note: Although upgrade from 6.2.8x is supported, 6.3.162 only includes content up to 6.2.7x. It does not include 6.2.8x.

- DatAdvantage+DataPrivilege 6.2.x and 6.3.x installations cannot be upgraded separately.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.

Source DataPrivilege Version	Possible Upgrade
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	- Distributed environments: - Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. - Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. - Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. - Consolidated environments: - Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. - Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.161

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x through 6.2.8x, and 6.3.x directly to 6.3.161.

Note: Although upgrade from 6.2.8x is supported, 6.3.161 only includes content up to 6.2.7x. It does not include 6.2.8x.

- DatAdvantage+DataPrivilege 6.2.x and 6.3.x installations cannot be upgraded separately.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.

Source DataPrivilege Version	Possible Upgrade
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.160

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x through 6.2.8x, and 6.3.x directly to 6.3.160.

Note: Although upgrade from 6.2.8x is supported, 6.3.160 only includes content up to 6.2.7x. It does not include 6.2.8x.

- DatAdvantage+DataPrivilege 6.2.x and 6.3.x installations cannot be upgraded separately.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.157

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x through 6.2.7x, and 6.3.10x directly to 6.3.157.
- DatAdvantage+DataPrivilege 6.2.x and 6.3.x installations cannot be upgraded separately.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.154

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x, 6.2.5x and 6.3.10x directly to 6.3.154.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.153

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x, 6.1.x, 6.2.1x, 6.2.5x and 6.3.10x directly to 6.3.153.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.102

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 5.9.x, 6.0.x, 6.1.x, 6.2.1x and 6.2.5x directly to 6.3.102
- DatAdvantage cannot be upgraded from 6.2.60 or higher at all.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Upgrade and Conversion Assessment Tool to upgrade to DataPrivilege 6.3.x.
6.2.x, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Upgrade and Conversion Assessment Tool on the upgraded DataPrivilege database.

6.3.50

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 5.9.x, 6.0.x, 6.1.x and 6.2.10 directly to 6.3.50
- DatAdvantage cannot be upgraded from 6.2.15 or higher at all.
- DataPrivilege-only installations and DatAdvantage+DataPrivilege installations may be upgraded as follows:

Source DataPrivilege Version	Possible Upgrade
Lower than 6.0.100	First upgrade DataPrivilege to 6.0.100. Then use the Database Schema Converter to upgrade to DataPrivilege 6.3.x.
6.0.100, DataPrivilege-only environments	Use the Database Schema Converter to upgrade to DataPrivilege 6.3.x.
6.0.100, DatAdvantage + DataPrivilege	1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Use the Database Schema Converter to upgrade to DataPrivilege 6.3.x.
6.2-6.2.10, DatAdvantage + DataPrivilege	No schema conversion is necessary. Use only the standard upgrade mechanism provided in the Enterprise Installer.
6.2.15 or higher, DatAdvantage + DataPrivilege	• DatAdvantage cannot be upgraded from 6.2.15. • Use the Database Schema Converter to upgrade to DataPrivilege 6.3.x.
6.0.100 DataPrivilege, with 6.2 DatAdvantage	• Distributed environments: 1. Use the 6.3.x Enterprise Installer to upgrade only DatAdvantage. DataPrivilege upgrade is now disabled. 2. Use the same 6.3.x Enterprise Installer to upgrade DataPrivilege to 6.3.x. 3. Run the Database Schema Converter on the upgraded DataPrivilege database. • Consolidated environments: 1. Use the 6.3.x Enterprise Installer to upgrade both DatAdvantage and DataPrivilege at the same time. 2. Run the Database Schema Converter on the upgraded DataPrivilege database.

Upgrade - Global Access Groups Remediation Utility

6.3.153

The Global Access Group rules from version 6.3.10x are not supported in the upgrade to 6.3.15x. Rules that were created in 6.3.10x must be deleted before the upgrade.

Agent Upgrade and Data Deduplication

6.3.102

The Metadata Framework supports data deduplication on Windows 2012 when both the CIFS and the Varonis FileWalk methods are in use. To enable use of the Varonis method, the agent needs to be upgraded.

Documentation

6.3.153

This version introduces two new documents:

- *DataAlert Web Interface Triage Guide* - Provides a recommended workflow scenario for conducting a full alert investigation in the DataAlert Web Interface. It triages the process of identifying the threats which require immediate attention and the steps to take while investigating them.

Note: This document replaces *DataAlert and DataAlert Analytics 6.3 Reference and Investigation Guide*, which was previously available for internal use.

- *DataPrivilege 6.0.x - 6.3.x Comparison* - Provides a feature-by-feature comparison of DataPrivilege 6.0.x and 6.3.x, with a complete description of the differences between the two versions.

Noteworthy or Changed Behavior

6.3.190

N/A

6.3.189

N/A

6.3.188

N/A

6.3.187

Issue ID	Description
578609	When a file server having a question mark (?) in its name is installed, the Enterprise Installer replaces the question mark with an underscore (_) in the database.
587223	NFS exports on NetApp can now be enumerated using either a dedicated ONTAPI function (Nfs_Exportfs_List_Rules_2) or the older detection method, whereby each volume is considered an export.

Issue ID	Description
588796	The Log Collector job schedule was changed. It is now configured to run every Saturday, Monday, and Wednesday at 9:00 PM.

6.3.186

N/A

6.3.185

Issue ID	Description
536578	The job history cleanup procedure was optimized.
543393	In the Management Console, in Configuration > Archive Policy, the Report CSV Export Path is now available for manual editing, and users are now able to enter a UNC path.
562856	In DataPrivilege, migration failed when the "Converting Report Subscriptions" step was executed for customer subscriptions in which the owner was removed from Active Directory.

6.3.173

ID	Documentation
471581	The "LastAccess Date" calculation was changed to MAX (create date, modify date,access date).
527795	The UK postal code pattern has been renamed to UK post code.
528211	In DataPrivilege, the theme cache is now refreshed the moment the theme is updated or replaced.
534453	FPolicy was automatically re-enabled on a NetApp file server after it was disabled.
539857	The File encrypted by ransomware has been removed from the dictionary and is no longer available.
541782	In order to support delete file operations over SMB3, by FPolicyregistration to open and close events, an extra open directory event was generated.

ID	Documentation
542578	When the account was being unlocked, the action object was overridden by the affected object.
537071	In Windows Server 2016, in addition to event ID 4742, events with ID 5136 (Permission Added and Permission Removed) are collected; therefore, the Metadata Framework reports on three events: 5015, 5016, and 5017.

6.3.163

N/A

6.3.162

N/A

6.3.161

N/A

6.3.160

N/A

6.3.157

Issue ID	Description
526915	Performance enhancements were made to the DataPrivilege UI.
528806	Solr now stops indexing and processing files when there is less than 20 GB of free disk space.
530767	The dependency of the delivery engine was removed from the host machine regional settings; in particular, a decimal separator can be either a dot or a comma.

6.3.154

N/A

6.3.153

Issue ID	Description
335666	ADWalk thread management was improved for better handling of local accounts.

Issue ID	Description
404807	The DCF includes a new pattern, Canadian postal code.
430594	Anti CrossSite Scripting (Anti-XSS) validations are now implemented.
446135	For ADWalk on Microsoft Office 365, support was added for HTTP proxy.
475363	Improvements have been made to the upgrade script: History_35\Shadow\changes\20120102-V58-ADEventsUpdate.sql.
479056	Improvements have been made to the repository cleanup process. Logging was improved in the data import area, and unit tests were fixed.
481275	In Netapp Cluster Mode, allNetwork File System (NFS) exports are now detected.
483447	The performance of Pull FileWalk [spUpdateHistory] was improved for inserts into the pv_Hist_FS_Properties table.
484923	The <i>Modification: Hosts file</i> threat model does not apply to NetApp or NetApp clusters.
490064	When the CSV delivery option was selected for a data-driven subscription, two output files were created instead of one.
490325	Solr now stops indexing and processing files when there is less than 50 GB of free disk space.
490405	For reporting purposes, only the following languages are supported for the SQL Server: English, German, Russian, and Chinese.
494080	To enhance security in the DatAnswers UI, the encrypted SID for each search request is now validated. In addition, it is now possible to disable the DatAnswers API.
495572	spMergePublishedData now allows unpublished Exchange ACLs.
495719	The function fncExportBcpReplaceNonLetter changed the numbers of the DBColumn name to '_' (for example, 'extendedAttribute_4', 'extendedAttribute_5').

Issue ID	Description
496909	Global Access Group user permissions were not properly removed after a rule was run.
496943	The following threat models do not apply to Exchange: • <i>Abnormal behavior: access to an unusual amount of idle data</i> • <i>Abnormal behavior: access to an unusual amount of idle sensitive data</i>
497002	In the Data Transport Engine, a rule configuration was added to allow disabling sandbox calculation, which can significantly improve rule calculation performance.
497113	In DataPrivilege, performance enhancements have been achieved by removing the license-checking job during queries.
497149	It is now possible to disable VSS in the Windows agent.
497162	FileWalk translation failure reporting has been improved to contain the requested characters in HEX representation.
498780	The Manage Ownership window in DatAdvantage now displays the SAM account name and email address for each owner in the list.
499110	On NetApp file servers, local groups could not be resolved.
499757	The CEPA events buffer size is now configurable.
500153	Loading time in DatAlert has been reduced.
500196	Logging of the crypto algorithm was improved.
500212	In the Data Transport Engine, when files and folders containing special characters are migrated from Windows to SharePoint, the special characters are automatically converted to hyphens (-).
500214	<i>Mailbox permission added</i> and <i>Mailbox permission removed</i> PowerShell events are now supported on Exchange 2013.
503693	DataPrivilege reports are not deployed when the Report Deployment Tool is set to All and then used to deploy reports on a different reporting server. In this scenario, DatAdvantage reports are deployed as expected.

Issue ID	Description
503697	Following migration of the VrnDomainDB database to a new SQL instance and running the Report Deployment Tool, friendly names are no longer displayed for report columns.
503760	DatAdvantage Lite and DCF Lite licenses cannot be upgraded to 6.3.153.
508913	The acting object in user lockout events is now reported as the account that is locked out.

6.3.102

Issue ID	Description
425333	The default port used for license verification has been changed from 80 to 443.
447442	In the DCF, pattern matching improvements were made that enabled quicker scanning of files 20 MB and larger.
449242	The Not contained in operator was added to the Rule Name filter in various reports.
452827	Added to main body of release notes.
453663	Improvements to DatAlert's predefined rules help to prevent false positives.
454316	File event types were added to the "Encryption of multiple files" predefined rule.
454552	When committing on folders with broken ACLs, the dialog box now contains a clear message emphasizing the results of the operation.
455807	The Encrypted Files and Exploitation Tools dictionaries no longer include the .mp3 item. In addition, *canvas.py was changed to runcanvas.py.
457566	In the Management Console, the "Use file name as Office document title" option was changed to the more general, "Use file name as a document title".
458362	In DatAlert, the *cred*. value was changed to *credential*.*.

Issue ID	Description
459152	Added to main body of release notes.
461182	In this version, PowerShell 3.0 or higher must be installed on SharePoint Online file servers to enable event collection.
461271	The error message regarding Azure AccessToken retrieval failre was improved.
465662	Improvements to DatAlert's predefined rules help to prevent false positives.
467332	In the Support Assistant Tool, the Base folders cannot be defined as managed folders error message now includes the name of the base folder.
467455	When a NetApp Cluster Mode file server was manually selected during installation in the Management Console, the NetApp shares were not correctly displayed and events from the file server were not collected.
468820	Events done locally or via RDP are now registered with their IP addresses as 127.0.0.1 to reflect the local origin.
469037	An Alert Category placeholder was added to the DatAlert template's optional fields.
469531	Extensions were added to crypto files and encrypted file dictionaries, to prevent malware infection.
471691	The license names in the 6.3 license site were broadened, indicating visibility only or requires Lite.
473382	The labels in the DataPrivilege Conversion Assessment Tool were updated for clarity.
475272	On an Exchange Online file server with new group types, the ADWalk job failed with errors.
483150	The subfolders under the MSI folder were renamed to exclude the word "Beta".

6.3.50

Issue ID	Description
323147	Users with the Logs View role can now run Sync Latest Events.
366915	A new validation algorithm for the tenth digit of the German driver's license number (Führerscheinnummer) was implemented.
370480	DatAnswers now works with HTTPS.
381064	Dell's .clusterConfig folder is filtered by the FileWalk job.
393558	The results of the Broken Inheritance Repair utility are only reflected in the DatAdvantage Work Area following the next FileWalk (either incremental or full).
398581	The upgrade to Metadata Framework 6.3 includes an upgrade to the Solr software, which is used by DatAnswers. Following upgrade to 6.3, all existing files must be reindexed to ensure continued use of DatAnswers.
405068	On clean installation of DatAnswers, the following file types are no longer indexed by default (upgrade is not affected): • CSV • RAR • MOV • MP3 • MP4 • MKV • MPG • MSG • SRT • SUB • LOG • WAV • WMA • WMV • XML • TXT Adding additional file types to the default list might impact performance and hardware requirements.
407507	In DataPrivilege, the ReportExportPath key enables setting the path to which a report is exported if the report results pass the limit that defined by the ReportLimit setting.

Issue ID	Description
411739	In Windows environments, NT ACL extraction is always used. If only DataPrivilege is installed, all crawled shares of CIFS file servers (Windows, NAS) must be defined as NTFS-crawled in the Management Console and not Mixed or NFS. Otherwise, DataPrivilege cannot crawl or manage them.
413549	In DatAnswers, a user that is part of one domain will be able to search on other domains only if there is a trust between the two domains and both domains are monitored in DatAdvantage.
413889	Dell FluidFS does not support local accounts.
419360	In order to run FileWalk on SharePoint Online, the SharePoint Online/OneDrive user can have SharePoint administrator permissions instead of the Global administrator permissions.
436880	Following schema conversion, the path format for managed folders is changed from <file_server_name.domain_name\share_name to <file_server_name>\share_name. Use this format when configuring file servers in the Management Console.
439622	DatAnswers now provides an option to search a term that appears in a document's file name. The new option is available in the Occurrences drop-down list, under Advanced Search.

Resolved Issues

6.3.190

Issue ID	Description
598107	Depending on the time zone in which events occurred, the following issues occurred: - West of UTC - Due to faulty event management, events were discarded and the rule's threshold was never met. - East of UTC - Events that triggered an alert were stored properly. However, older events were not deleted and alerts were delayed for the duration of the defined threshold.
599034	An internal filter related to Hitachi NAS was missing. As a result, no DatAlerts were triggered for this file server.

6.3.189

Issue ID	Description
589997	The DCF did not work after upgrade from 5.8.
590112	When a file server was not configured to collect events, changes made to other file servers on the same Probe or Collector were not synchronized.
590930	DataPrivilege website configuration reverted from HTTPS to HTTP following refresh and Management Console restart.
592114	The DCF generated errors when it could not find database tables.
592141	In the DCF, Oracle could not find matches for XML files.
592143	A timeout occurred in the DCF export process.
592215	Files were deleted before they were processed due to an error in the processing flow. As a result, an error was written to the event log.
592935	The Windows agent stopped responding while attempting to load Volume Shadow Copy Service (VSS) volumes.
593998	A data transport engine mirror rule stopped functioning due to an error that occurred during the DryRun execution.

6.3.188

Issue ID	Description
590481	In DatAlert, errors occurred when any filter related to users or groups or their properties was used in the Where scope.

6.3.187

Issue ID	Description
579066	Running the flattening job simultaneously with UBA aggregation and the flat report resulted in either deadlocks or a data movement error.

Issue ID	Description
588069	When a Broken Inheritance Repair module rule was run using the <i>Directory name</i> filter and a database table was simultaneously being recalculated, an error was returned stating that the rule scope was empty even though it was not.
588074	In the Broken Inheritance Repair module, rule closure failed if the same access path appeared twice in the database and the path was remediated.
588076	When running the Broken Inheritance Repair Utility, a timeout exception occurred.
588081	In the Broken Inheritance Repair module, the commit process did not merge inherited permissions correctly.
588087	The report capping function terminated Global Access Group module rules that ran for a long time.
588151	In DatAlert Analytics, a rule having a global flag as a filter stopped responding.
588458	The Broken Inheritance Repair and Global Access Groups modules did not unregister selections made in the directory picker.
589082	Unnecessary API requests per NetApp CM session registration were made, resulting in endless reconnections.
589862	A primary key violation occurred when the DumpEvents_UpdateAlertData stored procedure was run.
589954	An exception was thrown when UBA_ManagementService was run.
589968	Multiple alerts were triggered on the same day for the same user due to faulty handling of alert rules.

6.3.186

Issue ID	Description
585882	The DatAlert Analytics Export job re-exports messages that were already exported.

Issue ID	Description
582389	Following upgrade from 6.0.70 or lower, old predefined pattern data that were not password-encrypted could not be opened.
582390	The event viewer showed several errors when the Probe was not set to monitor a particular file server and DCF user synchronization was run.
583274	The ability to save matches in the Category 19 report was disabled even if there were content-related conditions.
583551	Errors occurred during DatAlert Engine export on access paths having TABs.
584172	The Save Matches checkbox was always checked in the UI, regardless of whether a rule was new.

6.3.185

Issue ID	Description
454120	Error messages were displayed on the DCF monitor regarding index ranges.
501849	DCF Lite results were deleted following source failures.
536578	The job history cleanup procedure was optimized.
537072	When a File Server was installed without automatic detection, the UUID was not set.
539266	After a site collection on a SharePoint File Server was removed, the domain did not exist in the ResourceDetected table, but was still marked as monitored in the Domains table.
539920	In the Bulk Upload Utility, after uploading an Excel file with an existing Automatic Rule, a message was received, "A rule with that name already exists."
541969	The DatAlert Alert Delivery job waited a long time in the general queue before being executed.
542738	In DatAnswers, in My Folders mode, the main page was not loaded when using the small zoom option.

Issue ID	Description
543393	In the Management Console, in Management > IDU > Service Components > Reports > Report Configuration , the Report CSV Export Path is now available for manual editing, and users are now able to enter a UNC path.
543773	In the DCF, when there were many DCF Dictionary hits, the DCF Allocate DirID Job would run for days causing performance issues.
544354	When the default domain settings were removed and added again (hence no longer default), and when upgrading from versions 6.0.X to 6.3.X, the data migration would crash with an error message.
546391	The current status of the RTA Scopes life cycle caused situations where calculated scopes were not delivered to the Collector because PullWalk invalidated the calculation results.
550068	The Management Console did not validate Probe proxy credentials when admin credentials were used.
556220	FileWalk ceased to function due to deadlocks, due to MS SQL intra-query parallelism issues.
556802	Setting an expiration date on an entitlement review report caused all reports to have unintended expiration dates as well.
558391	When an account was being unlocked, the acting object was overridden by the affected object.
558391	When the account was being unlocked, the action object was overridden by the affected object.
558668	The stored procedures "spBrokenAcls_LoadRunResultsParams" and "spBrokenAcls_ResolveRunResults" ran for a long time and failed upon timeout.
558941	The stored procedure "spAutomation_GetRelevantScopesForGAGRemediation" name should be changed to: "spAutomation_GetScopesForRemediation".
558944	The name of the Save and Calculate button was changed to Save & Calculate Expected Results .
558946	In the Expected Global Permission Removal tab, the column name "IsCausingAccessErrors" was replaced with "Permission in use".

Issue ID	Description
558947	In the Remaining Access Errors/Prevented Access Errors tabs, the "User" column was repositioned to the first column on the left.
558948	The "Expected Impact on Token" tab did not mention that the actual token size is not taken into account. This tab only listed the users who exceeded the warning and limitation thresholds, as configured in the Method tab.
559299	When SharePoint Online auditing was used, no events were received, and the event log displayed too many requests.
560176	When old/late Events for PrunedUsers were pulled and the Shadowpartition was archived, the error message was unclear. It is now more informative. In addition, the code was changed for an illegally implemented self-join for the PartitionView.
562856	In DataPrivilege, migration failed when the "Converting Report Subscriptions" step was executed for customer subscriptions in which the owner was removed from Active Directory.
563044	After changing the Active Directory property in DataPrivilege settings, the migration failed with the error, "The multi-part identifier 's.sidID' could not be found."
563046	In DataPrivilege, migration failed upon theme conversion when the active theme to be migrated had the same theme ID as the default theme.
563047	In DataPrivilege, modified names of permissions types and names in the Navigation menu panel were not migrated.
563245	The stored procedures "spBrokenAcls_LoadRunResultsParams" and "spBrokenAcls_ResolveRunResults" ran for a long time and increased the timeout from 5 minutes to 1 day.
563844	In DatAlert Engine, the DatAlert Analytics Export/Import/Execute Learning jobs were runnable via the Management Console, but should not have been.
563882	DataPrivilege migration failed at step <name of step> when it contained OUs that belonged to a domain which was removed.
564458	An invalid filterXml scope was created and the canned rule was not updated upon merge from a DatAdvantage version lower than 6.3.185.

Issue ID	Description
565001	The following warning message was missing before rollback and has now been added: "Please note that you are about to roll back all of your changes from the last execution. All of the global groups permissions will be returned to the file system and any new groups that were created will be removed."
565851	Upgrade to 6.3.150 failed when the spCreateFilegroup stored procedure was executed during database restoration and backup.
565893	The @tableName parameter in the spGetDeliveryEngineCascaseConvertors stored procedure was erroneously wrapped in QUOTENAME.
565903	Certain links to DFS root shares were not displayed in the DatAdvantage UI when the file servers' DFS share paths were identical.
565907	While adding a file server, the Sync Pruned Users job runs synchronously and takes a long time to complete.
565925	Performance issues occurred while calculating the closest share for TMP_SortedDirectoryTree during the execution of the spPostPullingCalculation stored procedure.
565926	A deadlock occurred during the run of the DFSWalk job.
567219	The DatAlert Alert Delivery job failed due to a conflict between an INSERT statement and a CHECK constraint.
567384	A Data Transport Engine mirror rule stopped running after destination folders were removed.
568402	The DatAlert Analytics Engine detected the wrong IDU Working directory. As a result, alerts were not discovered by the database.
568452	Following the run of the DatAlert Analytics Trigger Publisher job, not all DatAlerts were published.
568527	The DataPrivilege Migration checker failed to detect the operating system type of specific file servers.
569340	The VaronisServerMonitor stopped responding after the IDU Server was restarted.

Issue ID	Description
569760	While running a data transport rule that created more than 100K folders and then running the FileWalk and PullWalk jobs on the destination file server, the PullWalk job failed with a publishing error (on ALTER SWITCH).
569810	In the Bulk Upload utility, the file selection function displayed .xlsx files, even though this file type is not supported by the utility.
571321	A deadlock occurred when the PullAD and PullEvents jobs were run simultaneously.
571836	A Collector threw an exception when it failed to execute a step during a repair operation. The exception was returned to the IDU Server, which failed to display an error message to the user.
571838	The spJOB_SyncRtaScopes_MergeDataOnProbe stored procedure failed to execute during the repair of the Collector LocalDB.
572193	A duplicate "S" permission line appeared in a report for the Users group.
573016	In the DCF, when a pattern within a compound pattern was modified, the UI failed to display the Pattern Modified dialog box.
573489	A conflict occurred when both the PullWalk Publishing and DCF Pull: Processing jobs were run at the same time.
578441	If an environment had more than one Active Directory file server, the export job failed to construct.

6.3.173

Issue ID	Description
434461	The "Home" tab cannot be configured to be hidden for different roles. It is always shown for all roles.
438311	Report 9.h.01, Changes in Folder Size, was not supported in DatAdvantage Light, since this report is not event-based. Authorization is only permitted for users with ReportsView AND (StatisticsView or WorkAreaView) roles.

Issue ID	Description
438965	Report 4.o.01, Directory Service Delegated Tasks, execution took a significant amount of time, regardless of the object type and number of users. On the client environment, execution took up to several hours.
443359	When Report 4.b was exported to a Microsoft Excel file, the report was displayed as expanded, but with no '+' to expand and minimize a group.
444878	Errors resulted when running data-driven subscriptions that were created with the "All recipients" option and one or more users were deleted.
449561	Report 8.d, Potential User Count/List by Platform, ran for an excessive amount of time due to a combination of a large amount of global group deny Access Control Entries(ACEs) and Active Directory users.
457012	When running a data transport rule to copy files from SharePoint to Windows, where some of the SharePoint column values were null, errors occurred and extended file attributes were not copied.
466701	Support was added for "AccessDenied" events in Hitachi NAS.
469566	In Microsoft Exchange Server 2013, the value of the "InternalRpcHttpServer" attribute could not be changed.
471581	The "LastAccess Date" calculation was changed to MAX (create date, modify date, access date).
472894	The installer crashed when the wrong information was inserted in the license registration. This occurred, for example, when there was a mismatch between the license key and the version being installed.
476524	The Publisher was stuck in a deadlock with many pending tasks until all historical raw alerts were processed.
498657	A file system had a "ModifyDate" attribute with a future value.
500038	The working directory contained a double slash when the root drive was selected.
501013	In an environment without MS Visual C++ runtime, the event collection agent was unable to start.

Issue ID	Description
501309	An unexplained, unclear error occurred in the Database/Server view in the installer when a server with a disabled administrative share was selected.
501634	FileWalk terminated before "Max Idle Timeout" was reached. Therefore, volumes were marked as deleted.
502157	In Events and Alerts pages, the refinement terms were not clear. Values are now displayed in full, and binary values are shown as percentages.
502701	Health Check job clashed with the Delete Old Events job causing deadlock when the patch was installed. Also the Health Check job ran out of server resources on certain conditions even without the patch.
502844	Failures occurred when connecting to Azure. Therefore, the Azure tenant ID detection was changed to work without the resource account, but with the Azure file server account.
504357	The sync service failed for a migrated file server whose alias equaled a decommissioned file server.
504522	In DataAlert, the Publisher now sends messages every hour to accurately report the alert count.
504523	Due to a faulty Windows API call, ADWalk stopped responding.
504675	A Distributed File System (DFS) path filter and column were added to reports 4a, 4b, and 4c. * If the Old "DFSPaths" filter is used, the "Access Path" column shows the DFSpath, and the "DFS Access Path" column shows the DFS Path. * If only the new "DFS Access Path" filter is used, the "Access Path" column shows the Physical access path, and the "DFS Access Path" column shows the DFSPath. * If none is used, the "DFSAccess Path" column is NULL.
505497	The Classification results filter now allows positive and negative selections for rule names.
506736	LDAP user properties were displayed incorrectly after Encana was upgraded with patch 63591.
506988	Data-driven report names that contained "Pending" were considered to be in pending state, even though the subscriptions had already finished.
507063	In FileWalk, the folder ID was duplicated in the Microsoft Exchange Extended properties table.

Issue ID	Description
508047	In the Data Transport Engine, commands were run without proper parameters. This occurred since the rule had previously crashed when parameters were being inserted into the commands.
508276	In DatAlert, the mail provider kept the connection open to the mail server. When the number of emails exceeded the limit, the emails were not sent and error messages were displayed.
508853	Dynamic ports (high ports) for Directory Services were added to the port list.
509196	The upgrade script "20150730-V6.3-Reattached_Schedules_jobID.sql" did not remove duplicated FileWalk schedules when InitArguments were absent.
510627	The Publisher got multiple instances on multiple ServerOperation callbacks.
511228	Notifications about system errors were emailed as zipped file attachments when the contents exceeded the maximum message size limit.
512426	File names with case differences were missed by data transport rules with event-based file filters. This occurred when some of the events had file names that differed in case from the file names on the file server.
512517	Microsoft Exchange 2013 events were not displayed as expected. For example, when adding additional users to a shared folder, changing permissions to previously added users, and so on, sometimes an event was missing or the user was wrong.
512527	In the Management Console, when a subscription owner was changed to a group, then all group members lost access to the subscription.
512870	A subscription of Report 12.L.1 became stuck after DatAdvantage was upgraded from 6.0 to 6.2.
513118	A warning message that connection to port 4972 was blocked was erroneously displayed when adding a file server to the ManagementConsole.
513537	Access path validation failed for the Suspicious access activity: non-admin access to startup files and scripts threat model. An error message indicated that an asterisk is not supported between letters, however it should be supported between 2 slashes.

Issue ID	Description
513594	The Active Directory attributes were not displayed as expected in the work area for Deny Permissions when properties (such as AccountExpires, LastLogonTime, PwdLastSet) were added for users and groups.
514712	AD Walk jobs hung on call ldap_bind_s() and did not run as expected.
514926	Report 10.a erroneously displayed a folder that was deleted.
515100	ADWalk crashed when it ran a large number of monitored domains.
515184	In the Recommended Users and Groups pane, the manager name was erroneously displayed in LDAP format.
515970	When scheduled to run at high frequency, the Data Transport Engine suffered from memory leaks.
516512	Due to a high number of false positives, the File Open event has been removed from the Event type filter in the What (Event Details) page for the following rule: Security certificate activity by non-administrators.
516635	The LDAP Bind (ldap_bind_s) timeout error message has been improved.
517011	It was not possible to select public folders for monitoring in an active Exchange file server when public folders were selected for monitoring in a decommissioned file server from the same domain.
517223	The Reporting API tool could not be installed using the credentials provided for Windows authentication in the Installation wizard.
517351	When Incremental FileWalk failed to access all folders with events, the Pull FileWalk job also failed with errors.
517392	A deadlock occurred during the run of the Pull Events job.
517507	The Data Transport Engine mistakenly added domain users to local built-in groups when folder owners were transferred.
517513	On an Exchange Online file server, the ADWalk job failed to retrieve certain mailboxes and permissions. As a result, the ADWalk job stopped to crawl other mailboxes.

Issue ID	Description
517658	Temp tables on VrmsDomainDB were not removed during the run of the HealthCheck job.
517700	Errors were received during the run of the Events-Pull job.
517709	When the Probe failed to activate the Unix agent monitor, the received error message did not provide the cause of failure. The cause is now provided in the error message.
517833	The Could not load XML from the DynamicFilters column error message did not include the XML string which the parser failed to load.
517997	The performance of DTE folder and file scope was improved when using filters "Classification Results"-> "Rule names" and "Classification Results"->"Excluded files with rule names".
518971	Out-of-memory exceptions occurred during SharePoint Online FileWalk due to environments with large numbers of files, lists, and lists attachments.
519184	The Resource Monitor, which succeeded to retrieve partial data only, removed the rest of the file server shares.
520317	The Commit engine failed to commit changes made to a CIFS folder on a NetApp Cluster Mode file server.
520982	The upgrade from 6.2.62 (with DatAnswers installed) to 6.3.153 failed to complete.
521184	Warning messages were written to the Event Log about a database connection issue even though the IDU Service successfully started.
521283	During the run of the DataAlert Analytics Work Hours job, warning messages were received in the log.
521469	In the DataAlert Analytics working directory, the conversion from Unicode to wchar in the AGE.exe file triggered a warning message.
521638	Multiple permission requests took a long time to be create din DataPrivilege.
521767	When a large number of historical (raw) alerts were displayed in the Event Viewer, the DataAlert Publisher failed to start.

Issue ID	Description
522066	The Probe failed to connect to a NetApp file server with a large number of FPolicies and VServers when FPolicyDisable was issued, followed immediately by FPolicyEnable.
522225	The database script "20151207-v6215-UTCProbeColumns.sql" performed poorly due to a heavy load with many tables on the Probe.
522252	Even though the Probe proxy password was updated, it was not used when the Domain Controller was monitored using the proxy.
522367	Two different threads attempted to add a new resolver in the CoreResolver.
522627	In report 1.a.08, the Alert severity filter displayed the severity "Waiting" instead of "Warning".
522693	False positives were returned when the DatAlert Management Service failed to monitor one or more days.
522744	Report 8b failed to display the Operator role for a user who inherited permissions from a group.
523008	When a web application contained a host named "site collection" with a managed path, an enumeration error occurred. As a result, FileWalk failed to run.
523022	The Privileged Accounts Notification email failed to display changes. Instead, errors were received in the mail queue.
523045	On an Exchange file server with more than one volume, the calculation of DatAlert rules failed to complete.
523121	When the Shadow database did not contain events, the export process failed to return any events.
523263	It is now possible to abort the run of the DatAlert Engine historical tool.
523264	A progress bar has been added to the DatAlert Engine historical tool.
523357	During the run of the Pull Events job, a deadlock occurred when the spGetEventsStats stored procedure was called.

Issue ID	Description
527052	The key value was erroneously duplicated when adding protection with copy for Create Owner.
527172	A guest link erroneously appeared in the Directory Services navigation tree in the DatAdvantage Directories pane.
527348	When a Data Transport Mirror rule was run several times and then suddenly aborted, an error was received and written to the log.
527359	The Potential past ransomware activity indicated by a suspected a residual ransomware note threat model is no longer available.
527517	A deadlock occurred between two stored procedures.
527596	It was not possible to edit the file server in the Management Console when the domain ID was manually updated; another domain was detected as the affiliated domain.
527662	For an on-premises SharePoint file server, a Null Reference exception was thrown while host-named sites were enumerated. As a result, detection failed.
527795	The UK postal code pattern has been renamed to UK post code.
527883	Warning messages were written to the event log when the Application configuration file (Office365Agent.exe.Config), used to store the latest collected events, could not be resaved without reloading.
527956	An exception occurred when a new resolver was added on CoreResolver.
527970	Errors in the mail queue and in the notification tables were received following the run of the DatAlert Analytics Calculate Entities job.
528108	Report 12m performance was improved when using the "Starting Directory Name/Depth" filters.
528265	In DatAdvantage, due to privacy checks for each template, the reports window opened unusually slowly for non-Enterprise admin users.
528307	An exception was thrown when the AddIpAddressToCache() function was invoked on an on-premises SharePoint file server.

Issue ID	Description
528330	In the Management Console, in SharePoint's Claim-Based Authentication, when SamAccountName was added, the SID mapping mapped to a different site collection instead of to the Active Directory account.
528410	In the Bulk Upload Utility, uploading a CSV file containing at least 3500 rows failed to complete.
528682	When DatAnswers indexed a large number of files, the indexing ceased to function until the service restarted.
528684	In DataAlert, when editing rules in bulk, the previously-defined settings were overridden.
528744	In DataAdvantage, if a mount point directory was shared and added, FileWalk could not crawl it successfully.
529052	
529054	In DataAdvantage's Work Area, shared folders were marked yellow, not green.
529101	When an exception occurred in the child task of a broken ACL, the rule's execution ceases to function.
529103	In the Broken Inheritance Repair Utility, when running a rule and using the Stop button, the utility ceases to function.
529104	In the Broken Inheritance Repair Utility, the delivery engine failed to connect to the target file server.
529146	In DataAlert Analytics, when using decimal commas (where numbers are formatted as "1,23" instead of "1.23"), the bulk insert process failed.
529315	If the name of a volume was different from the root directory in DirectoryServices, the relation DirID volumeID was not found, and so the volume's dirID and Access path were not available.
529389	When a web server was changed to work with HTTP instead of HTTPS, the previous URL protocol continued to work.
529593	In the Broken Inheritance Repair Utility, during the Health Check job, the table's rows are deleted.

Issue ID	Description
529938	In DatAlert, when a rule contains more than one access path filter, at least one filter is ignored.
530650	The Events Archive job for Directory Services performed slowly when loading large inputs of data.
530784	After editing Data Transformation Engine rules, DataAdvantage ceases to function.
531312	Selecting a filter hit count in a Real Time Alert rule caused performance issues in the Real Time Alert rule prepare job.
531656	In the French installation, the DatAlert Analytics Export job failed due to date format issues where the month and day are reversed (for example, March 12 becomes December 3).
531698	The ChangedActiveDirectoryProperties filter had string values in the dynamic XML filters instead of numbers.
531707	The DatAlert scope delivery job for real-time alerts takes an unusually long time to run and consumes a high amount of CPU resources.
531723	Owners were not synchronized from DatAdvantage to DataPrivilege for regular hidden shares (marked with a \$ sign).
531759	Errors occurred when alert method command line credentials were cached in the credentials picker component.
532084	When only logon events were received for a certain day, the events statistics for this day were not calculated.
532131	The DatAlert aggregation job, when run from the Management Console, failed with an error. As a result, it was impossible to search for alerts in DatAdvantage.
532193	In the installer, in License Configuration, when selecting automatic registration, the Copy License key to clipboard button does not work.
532423	An error message was displayed when expanding an Exchange MailboxStore with Dynamic Grouping enabled.

Issue ID	Description
532439	If DataPrivilege emails were configured to have no image and no text in the header-left area, they were sent with the default Varonis header-left logo.
532489	A DatAlert stored procedure failed due to a primary key violation.
532534	There were performance issues with the DatAlert delivery jobs (Alert/Scope).
532934	In DataPrivilege, in Application Settings > Mail, when Send mail for auto-created and auto-approved requests was defined as true, emails were not sent.
533011	The Logs Collector job failed when the get upload URL action is not done with special user credentials.
533502	In DatAdvantage, it was impossible to create a new group on a domain with transitive trust.
533504	Incremental FileWalk was repeatedly cancelled because FileWalk would wait for PullWalk to complete.
534430	A DatAlert stored procedure failed due to a primary key violation.
534453	FPolicy was automatically re-enabled on a NetApp file server after it was disabled.
534617	DataPrivilege did not send emails when the value of "Retry attempts" was set to zero (in the Management Console).
534941	Performance issues occurred when using the object_id(table_name) function inline on spDeleteOldRTAlertedEvents.
535022	A string was changed in the license message when the user license enforcement was turned OFF.
535050	In the Alerts dashboard, in the resource picker, the Apply button ceased to function correctly and loaded indefinitely.
535198	In the Automation Engine, the term license was limited to three executions.
535357	The DatAlert Web UI no longer requires Internet Information Services (IIS).

Issue ID	Description
535404	When running the Broken Inheritance Repair Utility, a timeout exception occurred.
535869	The logs collection job failed if a proxy was defined.
536483	When there were a large number of installed file servers, and when trying to deploy a VIP patch for a file server component, the multi-page function that displays the number of file servers per page did not work.
536599	The connection string was wrong when installing the Reporting API Adapter. There was a double "exe.exe" in the string suffix. Therefore, the installation of "Varonis.ReportingApi.Adapter.Setup.msi" failed.
536611	Repair/upgrade to 6.3.15x failed on attempt to change the compatibility level of read-only databases.
536759	In the Management Console, filtering by name/type/status relevant components did not work.
536848	The JOB_Commands table did not include a clustered index.
537084	Since the Data Transport Engine does not support mapping of shared permissions in Windows (only NTFS permissions are mapped), there were incorrect permissions on shared ACLs after running a Data Transport Engine rule.
537238	The list of Active Directory properties in the user/group picker included a property not defined within Active Directory. When trying to search for users or groups according to this property, an error message was displayed.
539252	Errors occurred in Linux when host file locations were marked with an asterisk (*).
539335	Events occurred for IPs in IPv6 address format. IPv6 addresses are now supported.
539505	An error occurred when loading the Domains list when there was a large number of domains.
539508	Due to no Directory Services, the DatAnalytics job had no files to export.

Issue ID	Description
539783	Changes have been made to the VrmsDomainDB code to improve the dispatcher performance in critical areas.
539785	The license check was called every time the spGetFilers was called, regardless of the parameters.
539786	The performance of the Management Console jobs screen has been improved.
539857	The File encrypted by ransomware has been removed from the dictionary and is no longer available.
541782	In order to support delete file operations over SMB3, by FPolicyregistration to open and close events, an extra open directory event was generated.
542578	When the account was being unlocked, the action object was overridden by the affected object.
542680	An error occurred upon converting data type vnarchar to bigint when running spLog_CleanupLogTables.
542846	A number of terms have been removed from the Crypto Files dictionary.
542849	Errors occurred when running a flattening job. A report execution failed with an error. The schema was changed after the target table was created after running spRunReportSQL.
542930	The user "VaronisSystem" does not exist in Active Directory, and cannot be viewed in reports. The user "VaronisSystem" can be seen in DataPrivilege.
543317	The executive accumulative behavior alerted on non-executive users.
543869	When creating a new "Dell Fluid Access path", the dynamic XML filtering the "Where" scope was missing the "fluidfsAccessPath".
544281	The rule summary included default warning/preventions limitations, even when the limitations were not selected and should not have been applied.
546473	When a search service ran on a machine that was localized for a language other than English, the float number was incorrectly converted.

Issue ID	Description
546622	An execution time error/exception occurred, the CollisionBehavior parameter was missing when the command parameters were fetched from theCommandLoader.
548056	Report 1a8 failed to report events for Directory Services and Microsoft Exchange, even though alerts were generated.
550721	Alert descriptions were missing in notification emails for real-time alerts.

6.3.164

Issue ID	Description
578849	The DatAlert Analytics Export Job failed to initiate when the environment comprised multiple Directory Service containers.

6.3.163

Issue ID	Description
568948	The DatAlert web UI stopped responding when it received alerts on Exchange file servers.
569884	In the DTE, after running a rule which creates more than 100,000 folders, PullWalk failed.
569935	A string was changed in the license message when the user license enforcement was turned OFF.
569937	When inserting a user to a group of unmonitored users but this user had previously performed events, pull events might cause errors.

Issue ID	Description
559621	When the DCF scanned a large number of small files, an out-of-memory exception occurred.

6.3.162

Issue ID	Description
562844	Upgrade from 6.2.6x to 6.3.x failed because the installation order of scripts for the repair/upgrade flow was incorrect.
562872	The multi-part identifier <i>s.sidID</i> could not be bound when changing an Active Directory property in DataPrivilege.
563015	DataPrivilege migration failed on theme conversion when the active theme (to be migrated) had same theme ID as the default theme.
563033	In DataPrivilege migration, the customized names of permission types and names in the navigation menu were not migrated.
563504	The DatAlert Engine took the first IduWorkingDirectory path it found in the database, even though the path had been deleted and was invalid.
563710	New FileWalk requests in the "pending" state remained pending for a long period of time, until the current run of full FW was completed.
563824	The update schedule screen threw an exception following upgrade to 6.3.x.
564946	Repair/upgrade to 6.3.15x failed on attempt to change the compatibility level of read-only databases.

Issue ID	Description
559621	When the DCF scanned a large number of small files, an out-of-memory exception occurred.

6.3.161

Issue ID	Description
559621	When the DCF scanned a large number of small files, an out-of-memory exception occurred.

6.3.160

Issue ID	Description
536913	While shutting down a node on a Windows 2012 RN file server (with CSV), a blue screen of death was displayed.
536914	The dependency of the delivery engine was removed from the host machine regional settings, in particular, a decimal separator can be either a dot or a comma.
536919	Changes have been made to the VrmsDomainDB code to improve the dispatcher performance in critical areas.
536920	The license check was called every time the spGetFilers was called, regardless of the parameters.
536931	The performance of the Management Console jobs screen has been improved.
536936	Following upgrade to 6.2.72 or 6.2.73, high CPU utilization on a Collector caused it to stop functioning. The Collector crashed due to an excessive number of wild cards inserted in the Real-Time Alerts internal map.
536937	The ADWalk job stopped responding due to an unresponsive RegconnectRegistry WinApi.
536939	The Collector FileWalk Data Delivery job failed with errors.
536940	The GPO unique ID was not available.
536977	Synchronization did not work correctly in some Probes and Collectors. Therefore, recovery jobs ceased to function properly.
536978	After the server restarted, the jobs that were not finished from the previous run took too much memory and the server crashed.
537092	The connection string was wrong when installing theReporting API Adapter. There was a double "exe.exe" in the string suffix. Therefore, the installation of "Varonis.ReportingApi.Adapter.Setup.msi" failed.
537093	The term license was limited to 3 executions for the Automation Engine. This limitation has now been removed.

Issue ID	Description
537095	Incremental FileWalk was not run when Full FileWalk data was pending the PullWalk job.
537146	An SQL exception occurred when a report with session ID 10299 was run.
537237	The list of Active Directory properties in the user/group picker included a property not defined within Active Directory. When trying to search for users or groups according to this property, an error message was displayed.
537279	In the DatAlert Engine, log levels were high for several DatAlert Analytics components.
537303	Since the Data Transport Engine does not support mapping of shared permissions in Windows (only NTFS permissions are mapped), there were incorrect permissions on shared ACLs after running a Data Transport Engine rule.
537440	The JOB_Commands table did not include a clustered index.
539501	When the Shadow database did not contain events, the export process failed to return any events.
539745	The DatAlert aggregation job, when run from the Management Console, failed with an error. As a result, it was impossible to search for alerts in DataAdvantage.
539765	When running the Broken Inheritance Repair Utility, a timeout exception occurred.
542020	When the account was being unlocked, the action object was overridden by the affected object.
542674	The user "VaronisSystem" does not exist in Active Directory, and cannot be viewed in reports. The user "VaronisSystem" can be seen in DataPrivilege.
543220	The schema was changed after the target table was created after running spRunReportSQ.
543706	If DataPrivilege emails were configured to have no image and no text in the header-left area, they were sent with the default Varonis header-left logo.

6.3.157

Issue ID	Description
513796	A typo in a message from the Probe CryptoDetector was corrected.
521199	DataPrivilege direct permission requests failed on clustered NetApp file servers.
521833	An incorrect MSI was used by the Enterprise Installer for the DatAlert Analytics Engine.
521934	The web UI was not installed properly on upgrade from 6.3.102 to 6.3.153.
523324	If Microsoft KBs were missing, the DatAlert Engine was installed with a warning instead of an error.
527776	The DatAlert Analytics Execute Learning job failed.
529243	Broken Inheritance Remediation rule scopes were removed when the cleanup job was run.
530249	The Event Flattening job failed due to a primary key violation.
530585	Errors occurred in the mail queue after the DatAlert Calc Entities job was run.
530603	If the name of a volume was different from the root directory in DirectoryServices, the relation DirID volumeID was not found; therefore, the volume's dirID and Access path were not available.
531338	The Probe service failed on Exchange Servers when writing to the CLIENTHOSTNAME field.
531681	A DCF disk space error was edited for clarity.
532074	Some database tables were created with an incorrect naming convention, which resulted in an error in converting nvarchar data types to bigint data types.
532461	The DatAlert Alert Delivery job failed to insert alerts that were more than six months old into the database.
532488	A DatAlert stored procedure failed due to a primary key violation.

Issue ID	Description
534301	There was potential credential exposure on Support Assistant output.

6.3.154

Issue ID	Description
484909	When editing a file server failed, the Shadow database was dropped.
520981	Upgrade from 6.2.6x failed.
521300	Pull FileWalk failed in incremental mode when it was run after Full FileWalk.
521622	An incorrect MSI was used by the Enterprise Installer for the DatAlert Analytics Engine.
523172	A guest link erroneously appeared in the Directory Services navigation tree in the DatAdvantage Directories pane.
527516	A deadlock occurred between two stored procedures.

6.3.153

Issue ID	Description
328138	The FileWalk Remote Procedure call (RPC) used NTLM instead of Kerberos authentication, resulting in FileWalk failing with an access is denied error message.
377974	AD filters in the DatAlert Where scope were not marked as DS ONLY.
437884	When the file server's SID changed, no message was displayed in the Edit File Server dialog box.
445246	Subscriptions that were configured to not be sent without data, generated errors while running.
452308	In DataPrivilege, groups could not be created in organizational units whose names included a plus (+) character.

Issue ID	Description
462149	Report 4f failed to generate results when the <i>Global flag on access path</i> filter was set with the <i>not equal</i> operator.
462206	The user "VaronisSystem" did not exist in Active Directory, and could not be viewed in reports. The user "VaronisSystem" could be seen in DataPrivilege.
466437	Report subscriptions where the email addresses in the To/CC/BCC fields that began with an exclamation mark (!) and a dash (-) or capital letters afterwards were allowed to be saved.
471705	The Event Status parameter was added to the default reports template.
474160	A domain user or group could not be added to a local group on a NetApp Cluster Mode file server when the user name was different than the SAM account name.
474631	DatAdvantage upgrade failed due to missing SearchPriority and DBColumnDefinition columns in the ADPropConfig table.
474908	In the Bulk Upload utility, the file selection function displayed .xlsx files, even though this file type is not supported by the utility.
475690	The <i>SAM Account Name</i> filter did not function correctly for historical reports.
476083	When running FileWalk via spRunFileWalkJob, the job failed with the error: "Error Cannot define FW mode".
476327	The Group Policy Object (GPO) alert was not identified correctly by the Publisher.
476796	During the "Pull Events" job, a primary key violation was detected for alerted events pulled from the Probe database to the Shadow database.
476962	There was an inconsistency between the type of ChangedAceMask in the code (Unsigned long) and in the database (int). The code cast is now set to "long" to match the type in the database.
477614	Selecting a value greater than 15 in the Report 16b <i>Number of top users</i> filter returned only 15 results.

Issue ID	Description
478008	When running a search in the Log screen after removing and adding columns, a fatal error message was displayed instead of a dialog box with event details.
478554	New GPO Object events were collected as Rename DS Object events.
478609	Pulling bounded synchronization ran for days and consumed CPU resources.
479060	DataPrivilege canceled requests on unmanaged groups.
479514	The Data Transport Engine rule sync failed for rules that took over a month to execute.
480279	Changes done in VrnExplorer.dll.user.config prior to upgrading or repairing the installation were overwritten.
480449	FileWalk failed when an editing command had a CMD_ID longer than 16 characters.
481017	In DatAdvantage, Russian display settings in the GUI caused the "Flags" context menu to be missing flag items.
481275	In NetApp Cluster Mode, all NFS exports are now detected.
481926	The Data Transport Engine failed when a rule having approximately 20M commands was run.
482176	Files copied to EMC VNX storage lost their original timestamp and received the copy time instead.
482715	In DatAdvantage, ADWalk failed to find the domain when there was a container with the exact same name as the domain.
482843	Indexes of the table JOB_Execution table (in the vrndomaindb DB) were unnecessarily rebuilt upon upgrade.
482851	The results of the DFS path on the Windows NetApp file server displayed "mixed" back and forward slashes '/' and '\'.
482852	It was not possible to save report templates if they had Active Directory attributes that contained numbers in their names.

Issue ID	Description
482857	The upgrade failed due to a conflict between an INSERT statement and a CHECK constraint.
482858	It was not possible to apply a license in the Management Console, since it was a server version and not an MC version.
483113	smg_DataMoving contained a table to be delivered even though the rule was deleted and the table did not exist.
483437	Due to a faulty Windows API call, ADWalk stopped responding.
483438	NetApp Cluster Mode shares could not be detected or scanned if they exposed only HTTPS (no HTTP at all) when installing DatAdvantage.
483679	Deduplication and Probe upgrade failed if a file server was connected via several Collectors.
483876	The GetCurrentToken procedure call used the permission set from the "Process Token" instead of the "Thread Token" which resulted in missing administrative permissions, and therefore caused "Access Denied" errors during Data Transport Engine runtime.
484002	DFSWalk did not return an error when it timed out. This occurred when a DFS tree had a lot of links to a target server on which the async calls were failing, the system kept retrying each link instead of timing out.
484169	In DatAlert, the "command line" alert method mishandled paths with spaces and quotes, and created log errors.
484362	The recycle bin was excluded from the <i>Permissions granted directly to user in Windows</i> threat model. An alert was erroneously received when files and folders were moved to the recycle bin.
484393	In DataPrivilege, an Active Directory search did not find users or groups from a different trusted domain, when the user credentials in the Management Console were the same for both trusted domains and the user had access to both domains.
484474	During DatAdvantage installation, the DatAlert Publisher ignored working directory updates.
484525	The working share could not be defined on the same location as the installation path of the Collector/Probe.

Issue ID	Description
484607	In DataPrivilege, it was not possible to right-click "DataPrivilege Windows Explorer Add-on" on mapped network drives with long paths.
484715	Following upgrade, AD Properties within a data-driven subscription were no longer available.
484783	The French IBAN number regular expression was erroneously associated with Switzerland instead of France.
484785	In report 9.h.01 (Changes in Folder Size), the <i>Access path</i> filter returned incorrect path names.
484798	The Events Archive job failed to respond while aggregating Windows events.
484843	The DatAlert Delivery job failed if *.rta files were loaded more than once.
484909	When editing a file server failed, the Shadow database was dropped.
484972	Performance issues occurred while starting DatAdvantage and the Management Console.
485349	In the DatAdvantage log, it was not possible to export filters to report 1.a.01 while in Simple view.
485435	The "Excluded access path" filter did not function correctly in the DatAlert Where scope.
485525	Upon upgrade, the transaction log for the Varonis database was full and an error message was retrieved. The size of the Inode table in the script file was too large.
485744	In DatAlert, if one email recipient in a list did not exist, an exception was thrown and no email was sent to the valid addresses in the list.
485790	The database stopped responding when the GetTagetComponentHostname stored procedure was called.
485803	DatAlerts were not triggered properly, due to a faulty hash function.
485958	For a Windows file server, duplicate shares were displayed in the list of available shares in the Management Console.

Issue ID	Description
485964	In DatAdvantage, a performance issue occurred while filtering in the Work Area.
486010	False access-denied CIFS events occurred on EMC-Celerra using CEPA on successfully created folders.
486135	A performance issue occurred when a data-driven subscription for report 4b was sent to a number of owners.
486578	When the CSV delivery option was selected for a data-driven subscription, two output files were created instead of one.
486638	In events alerted by the <i>Immediate pattern detected: user actions resemble ransomware</i> threat model, the UTC timestamp and local timestamp were switched.
486790	When copying files using the Data Transport Engine, the modified time of the copied file was set up correctly but changed a few seconds later to Now.
490064	When the CSV delivery option was selected for a data-driven subscription, two output files were created instead of one.
490405	For reporting purposes, only the following languages are supported for the SQL Server: English, German, Russian, and Chinese.
490571	In large environments, the deduplication Probe upgrade script ran for a very long time.
490896	A FIPS error occurred during detection of SharePoint site collections.
490968	In DatAdvantage, the server crashed when using Windows Server 2012 cluster with a CSV file system due to driver incompatibility issues.
491101	The DCF failed to retrieve hits on files with no attribute value.
494077	The Collector Service stopped responding when a large number of Group Policy Objects (GPOs) were being loaded.
494080	To enhance security in the DatAnswers UI, the encrypted SID for each search request is now validated. In addition, it is now possible to disable the DatAnswers API.

Issue ID	Description
494151	For Isilon, events with timestamps older than 7 days can now be written to the database.
494178	The DatAlert Scope Delivery job ran for an unusually long time.
494345	The root step of the Collector's data transfer procedure ran with RCID=1, instead of -1.
494399	Report 4b displayed incorrect share paths for a CIFS share when similar shares were defined for a folder and its subfolder in a mixed file server.
494525	The DCF User Sync job has been optimized so that classification priorities are not calculated for file servers outside the DCF scope.
494584	The AddLegacyExchangeDNMapping stored procedure now allows configuring a value for LegacyExchangeDN that is longer than 330 characters.
494586	When the <i>File properties</i> filter was used with both sub-filters, <i>File name and extension dictionary</i> and <i>Excluded file name and extension dictionary</i> , report 1.a.08 was empty.
494880	Multiple domains were displayed in the work area.
494942	The PullWalk job failed due to a duplicate key error.
495158	The Data Transport Engine finished with an error when copying built-in roles from Windows to SharePoint and the target file server was configured in a different language.
495218	The timeout for the publisher pull configuration from the database was increased.
495225	When a file server was added, an error occurred due to a faulty stored procedure.
495283	Folders that were managed in DataPrivilege that had duplicate rows in the sdt_accesspath table became undetected.
495539	Some changes to GPO settings were not collected.

Issue ID	Description
495540	GPO fetching was carried out per domain controller, not per domain.
495678	Obsolete report performance monitoring was removed.
495698	Errors occurred during Data Transport Engine rule preparation when source groups were merged from different file servers.
495705	If there were many Active Directory objects and relations, the Data Transport Engine's Next Run screen stopped responding while calculating lost permissions.
495719	The function <code>fnExportBcpReplaceNonLetter</code> changed the numbers of the <code>DBCcolumn</code> name to '_' (for example, 'extendedAttribute_4', 'extendedAttribute_5').
496238	Syslog identity has been removed from SIEM-oriented templates.
496935	IDU migration rollback tried to roll back changes on a non-existing database (<code>VrnsUI</code>).
497105	When DFS shares were added as base folders in <code>DataPrivilege</code> and the DFS link pointed to C\$, an error message was received.
497107	The Pull AD job did not include <code>AD_SidHistory</code> in the logic to insert into <code>ActiveDirectory_sid_relations</code> , so not all permissions were calculated and displayed.
497109	It was not possible to edit or request permission on mount point folders that were defined as base folders in <code>DataPrivilege</code> .
497110	In <code>DataPrivilege</code> , in organizations with a huge amount of shared folders, the tree view or the user interface that displays a folder hierarchy was timed out and shared folders were not displayed.
497111	When a single quotation mark was added to a folder name, the Sync Owner job failed.
497147	The Missing Events notification ran using an incorrect <code>NoEventsPeriod</code> value.
497148	The Pull AD Events job failed if two domains had the same configuration and events required special resolution.

Issue ID	Description
497152	The stored procedure that updates the IsParent column consumed too much CPU.
497167	FileWalk failed due to an arithmetic overflow in the Probe database.
497169	The list of database jobs was not properly displayed in the Management Console.
497540	The DCF and DatAnswers Monitor file counts did not include files that were skipped due to their size.
497673	The spgRunLog job failed due to an additional schema with vwADroperties views.
498012	It is now possible to view via Permission Sources from which groups a user's permissions are granted.
498087	When a Collector was installed to a non-default location, the installation path reverted to the default following upgrade.
498113	All Access Paths that contained 'ForeignSecurityPrincipals' were deleted from sdt_dirMapping.
498352	When no DataAlert rule was configured for a Probe or Collector's file server, an error message was displayed in the Event Viewer.
498416	The PullWalks Publishing job sent unwanted notifications during timeouts or deadlocks.
498453	When Data Transport Engine stubs were created, performance issues occurred for MS Excel files in Russian.
498524	In DataPrivilege, when adding a SharePoint file server after 100 file servers were defined, adding SharePoint sites from that file server resulted in invalid paths.
498706	An exception occurred when a directory was selected in an environment in which the domain ID in the database was at least 32,768.
498822	Report subscriptions failed if AD properties were added to the report columns.

Issue ID	Description
499041	When adding a file server, prerequisites for IRPStackSize that were not case sensitive were able to pass without problems.
499356	Primary key errors in the errCalcDomain table prevented data from displaying.
499654	Samba servers disrupted basic DataPrivilege functionality such as adding base folders and creating new permissions for managed folders.
500153	Loading time in DatAlert has been reduced.
500161	The Dictionaries window in DatAdvantage was not restricted according to user.
500195	Installation of DatAlert Analytics failed when FTP was present in IIS.
500196	Logging of the crypto algorithm was improved.
500197	The suspected time and suspected events were missing from the raw alert data.
500199	The DatAlert crypto algorithm did not consider delete events that followed read events.
500201	DatAlert's crypto algorithm considered Create Directory events as if it were the parent directory that was created when rolling back counters.
500207	An exception occurred during execution of Data Transport Engine rule, so that directories were not deleted and/or stubs were not created.
500208	Several issues with FileWalk scheduling occurred, including the creation of duplicate schedules, removal of schedules from FileWalk, and faulty InitArguments.
500212	In the Data Transport Engine, when files and folders containing special characters were migrated from Windows to SharePoint, the special characters were automatically converted to hyphens (-).
500215	The presence of the <i>Affected object type</i> filter had a negative impact on the performance of certain rules.

Issue ID	Description
500216	After upgrade, Incremental FileWalk was enabled unexpectedly.
500217	On VM machines with low resources, the UBA statistics calculation job ran for a very long time.
500219	Events were filtered for Isilon file servers because their ID was reported incorrectly.
500220	The Probe service stopped responding while printing to the log.
500221	After upgrade, Incremental FileWalk lost its schedule and next run values.
500515	Incremental FileWalk overwrote full FileWalk data.
500668	When DatAlert rules included privileged accounts in the Where scope, changes to the scope were only updated after the nightly jobs were run.
501344	When there were few events per file server, a false missing events notification was sent hourly.
501929	The merge of published Exchanged data failed.
501932	The Who scope was deleted from DatAlert rules when Scope Delivery ran after PullAD/PullWalk.
501933	The Events - Pull job did not include updating statistics for the relevant partitioned tables.
501992	When the HTTPS connection failed on the Exchange Server, it reverted to a plain text HTTP connection.
502017	The DiscoverShares All command retrieved only Unix shares.
502426	In report 4j, in the permissions row, there were numbers instead of the actual permissions' names.
502964	A deadlock occurred on two PullAD events.
503022	In DataPrivilege, when a new administrator was added, the remove button in the Authorizer tab was disabled.

Issue ID	Description
503051	In DataPrivilege, when a folder owner was also an authorizer, the checkbox for removal did not work.
503058	After deleting a DatAlert rule, its scopes were not deleted from the RTA_Scopes share folder.
503092	If a DatAlert rule used a predefined scope and it was changed to a regular scope, the data of the predefined scope was not deleted.
503440	The DataPrivilege evaluation license removed the DatAdvantage permanent license when DataPrivilege was installed over an existing installation of DatAdvantage.
503682	An error occurred while publishing a DatAlert lockout alert.
504121	After upgrade, report 12.L did not work properly.
504322	Upgrading from 6.2 failed after computer accounts were added to the IDU Analytics list of filtered accounts in the Management Console.
504506	Group Policy Object fetching errors occurred when Group Policy Objects HTML reports contained a bullet symbol.
505013	Following an upgrade, events from mounts were not collected.
505336	The Data Transform Engine checked for Path length instead of Filename length, which caused the prefix to be partially or completely removed.
505616	In the DCF, performance issues and rare instances of data loss occurred on results found by dictionaries.
505663	If a database was manually copied to the target, Probe migration was unable to proceed.
505920	When replication existed between two domain controllers, and the main domain controller was powered off, then users were unable to log in to DataPrivilege.
506084	Duplications were prevented for the ADproperty field in table DS_PropertyIDs, by removing the Checksum function used for row validation. This occurred using the existing row validation by the GUID.

Issue ID	Description
506469	UBA peers crashed when the aggregation files contained spaces in the middle of the access paths.
506728	In the Report API, the export to CSV function failed.
506829	When adding a Host Named Site Collection (HSNC), DataPrivilege failed to find the relevant domain.
508496	If events arrive the next day to the domain from the Probe or Collector, DataAlert triggered the same alerts again, causing alerts redundancy issues.
508848	A DataAlert notification email contained 0 events.
509177	User Behavior Analysis error ML algorithms now write to the event viewer.
509765	The Job History in the Management Console for the FileWalk job did not contain the FileWalk type specifier.
510893	In the DataAlert web UI, the Event by User > Member of group filter did not display the selected value.
513064	DataAlert rules with multiple file servers defined in the Where scope were duplicated per file server.
513375	Following upgrade, the old IP/Hostname placeholder for DataAlert templates was not replaced by the Device IP Address and Device Name placeholders.
513388	Access path validation failed for the Suspicious access activity: non-admin access to startup files and scripts threat model.
513446	The domain picker did not return the correct domains.

6.3.102

Issue ID	Description
420290	DCF scans ran longer than the defined scheduling times.
425333	The default port used for license verification has been changed from 80 to 443.

Issue ID	Description
442284	The Collector Events Delivery job now transfers a maximum of 1,000 files from the Collector to the Probe each time it runs. This fix was implemented to avoid out-of-memory errors.
445332	In the DCF, The UK Vehicle Registration Number is listed under the Phones category instead of Driver's Licenses.
447222	In DatAlert, configuration data was missing, resulting in DatAlert crashing and did not recover.
447234	The temporary tables on the Shadow database were not removed, even though the event statistics were already pulled to the IDU database.
447236	The Client sent localized dates to server requests.
447442	In the DCF, pattern matching improvements were made that enabled quicker scanning of files 20 MB and larger.
447756	When FileWalk ran in debug mode, it crashed because while printing a string that was referenced as an integer.
448181	DatAnswers erroneously displayed results to users in a group whose share permissions included Deny access permissions.
448644	Out of memory error messages were received due to the large number of folders containing special files and Incremental FileWalk inputs. To fix this issue, the number of folders containing special files and Incremental FileWalk inputs cannot exceed the allowed limit.
449187	Some domain users' display names contained a new-line character, resulting in SOLR caches failed to load and no returned results.
449242	The Not contained in operator was added to the Rule Name filter in various reports.
450632	When new tables were created after a month, creating new permissions tables failed.
451450	The DCF dictionary experienced two problems: * The total number of dictionaries did not get updated when a single dictionary was updated or deleted * When the number of dictionaries reached its defined limit, the dictionaries were unable to find matches

Issue ID	Description
451607	Filewalk did not support SharePoint custom list types.
452017	In the DCF, predefined email patterns have possible backtracking and are not up-to-date.
452641	After DatAdvantage was installed using a sys admin user, and then the user was deleted, then SQL procedures containing "WITH execute as owner" did not work.
453122	File Servers weren't added successfully upon startup and were therefore not monitored.
453663	Improvements to DatAlert's predefined rules help to prevent false positives.
454296	In DataADvantage, after Traverse permissions were selected, they were given without list permissions.
454316	File event types were added to the "Encryption of multiple files" predefined rule.
454552	When committing on folders with broken ACLs, the dialog box now contains a clear message emphasizing the results of the operation.
455807	The Encrypted Files and Exploitation Tools dictionaries no longer include the .mp3 item. In addition, *canvas.py was changed to runcanvas.py.
457566	In the Management Console, the "Use file name as Office document title" option was changed to the more general, "Use file name as a document title".
458362	In DatAlert, the *cred*.* value was changed to *credential*.*.
458536	In GPO settings, certain events on rules were not displayed.
460224	In DatAdvantage Core, in SharePoint 0365 Auditing, the EventViewer printed unnecessary messages.
461182	In this version, PowerShell 3.0 or higher must be installed on SharePoint Online file servers to enable event collection.
461271	The error message regarding Azure AccessToken retrieval failre was improved.

Issue ID	Description
463373	Folders which include broken inheritance cannot be edited. Configuration of the commit process prevents performing commit on these folders. All edits made to the folders will be invalid. It is possible to change the configuration in the Management Console, or use the Broken Inheritance Repair Tool (Tools > Automation Engine) to fix the folder's permissions.
463448	In the Unmonitored Users tab in the Management Console, the Last Unmonitored column was changed to Last Monitored.
463864	When a Directory Service proxy agent was used, the Probe failed to properly connect to the domain controller.
464322	When a Real Time Alert rule was created with many (approximately 3000) File Servers on a WHERE scope, a timeout error occurred.
464804	The Collector FileWalk Data delivery job failed to run and deliver the data to the database. To fix this issue, this job now supports the encryption and decryption of ZIP files if the Use ZIP encryption option is enabled.
465285	The UI changed the names of FileWalk schedules, resulting in problematic behavior, including duplications.
465519	The Dell FluidFS file server experienced connectivity problems.
465523	The Dell FluidFS file server experienced connectivity problems.
465662	Improvements to DatAlert's predefined rules help to prevent false positives.
466069	When the Reconnaissance tools rule was run, alerts were generated when certification, graphic and text files were accessed. The Reconnaissance tools dictionary was improved to reduce the number of false positives.
466070	When the Exploitation tools rule was run, alerts were generated when certification, graphic and text files were accessed. The Exploitation tools dictionary was improved to reduce the number of false positives.
467070	Upon upgrade from 6.0.112 to 6.2.53, temporary tables were not created after executing FileWalk on decommissioned file servers. As a result, several jobs failed to complete.
467333	In the Domains grid of the Management Console, the value displayed for the eDirectory domain (which uses TLS) in the Server Type column was incorrect.

Issue ID	Description
467455	When a NetApp Cluster Mode file server was manually selected during installation in the Management Console, the NetApp shares were not correctly displayed and events from the file server were not collected.
467563	In the DCF, predefined email patterns have possible backtracking and are not up-to-date.
467596	While attempting to add a domain through the Installer, the eDirectory domain type was not available for selection. The eDirectory option is available only if a Novell key is provided.
468197	While attempting to parse the license counters XML, an exception was thrown. Insufficient data was provided in the exception.
468415	During upgrade to 6.2.35, an error occurred when DatAlert rules were created, updated, deleted or disabled, triggering the DatAlert Sync Dictionaries job.
468421	When DFS shares were added as base folders in DataPrivilege and the DFS link pointed to C\$, an error message was received.
468655	A primary key violation occurred while running the Pull Alerts job.
468704	When a folder was selected through the Directory name filter in the DatAlert Where scope, the name of the folder was only partially displayed.
468714	The Mail Recipient field in the Management Console failed to display an error message when the maximum number of characters was reached.
468801	DatAlert scopes were delivered to the Collector with no file server attached. As a result, the same scopes were delivered to the Collector every time the DatAlert Scope Delivery job ran.
468976	While adding a new Collector in the Management Console, the Failed to resolve host IP error message failed to display the host name.
469530	The Glamour value in the crypto file dictionary caused a high rate of false positives. This value was removed.
469531	Extensions were added to crypto files and encrypted file dictionaries, to prevent malware infection.

Issue ID	Description
471492	Following upgrade to 6.2.53, the FileWalk job failed to initiate on SharePoint file servers.
471543	VaronisFilterHandler.exe stopped responding when an attempt was made to terminate the process.
471598	The upgrade process triggered a rescan of predefined threshold rules.
471790	The VaronisFilterHandler.exe process failed to respond while attempting to terminate it.
471841	It was not possible to edit or request permission on mount point folders that were defined as base folders in DataPrivilege.
471944	The Pull DCF job failed to pull the DCF_Files table to the Shadow when there was a valid license for DatAnswers but not for DCF or DCF Lite.
471984	A warning message was erroneously displayed when a DatAlert rule was created and the DatAlert Scope Delivery job was run.
472275	While attempting to add a SharePoint site to DataPrivilege, an Invalid path error message was received.
472583	The DCF failed to scan a root share on a NetApp Cluster Mode file server.
472896	In the Management Console, an Exchange file server was added without a Crawled By value, even though a value was selected during configuration.
473234	In DataPrivilege, the name of a button was displayed in English even though the language selected for the interface was Dutch.
473276	Following a DatAdvantage upgrade to 6.2.15.68 and on clean installation of DataPrivilege, the system administrator account no longer appeared in the list of user roles in the Management Console.
473592	On clean installation of DatAdvantage, the Installer stopped responding when the user originated from a different domain.
474160	A domain user or group could not be added to a local group on a NetApp Cluster Mode file server when the user name was different than the SAM account name.

Issue ID	Description
474828	The New Value column in report 9.h.01 displayed an incorrect value.
475272	On an Exchange Online file server with new group types, the ADWalk job failed with errors.
476124	To reduce the number of false positives, the item *.enc was removed from the Encrypted Files dictionary.
476156	In the DatAlert Web UI, the Alerts Over Time bar chart failed to clearly indicate that alerts were generated for several of the days presented in the chart. In the chart, dates which are now marked in bold contain alerts.
476287	Upon upgrade, the transaction log for the Varonis database was full, resulting in an error.
476359	An error occurred while configuring the archive policy options in the Management Console.
476644	In Trend reports, when Unicode characters were used in the department name, a duplicate key error occurred.
476655	In Trend reports, when Unicode characters were used in the department name, a duplicate key error occurred.
477547	Upon upgrade to 6.2.53, DCF rule conditions which had a Russian pattern or string were corrupted.
477575	Although the syslog method was configured and selected in the DatAlert UI, DatAlerts were not sent to the relevant server via syslog.
478249	An Out-of-Memory error occurred while verifying a very large number of data transport rules.
478324	When French was the displayed language in an SQL lab, DatAlert jobs failed to respond.
478510	It was not possible to add a DFS share to the list of base folders in DataPrivilege.
478529	The DCF Service stopped responding while allocating space for additional results.

Issue ID	Description
478803	The Access path filter did not work in SharePoint when a URL was displayed in the Access Path column in report 4f.
479204	Predefined rules triggered alerts on events that were not included in the dictionary.
479223	The DatAlert historical tool deleted old alerted events from environments on which it ran.
480399	When the IDU Suite Probe and the domain were consolidated, and the host was being restarted, the vrnsdomaindb database started faster than the Probe, resulting in inconsistencies.
481774	A major slowdown in event collection occurred.
482354	A primary key constraint violation occurred when a global access group rule was calculated.

6.3.50

Issue ID	Description
209847	Directory service events (Create, Rename and Move) were filtered when the Active Directory domain was configured with a NetBIOS name.
315011	When the IP address of a Search Node was changed, the cluster failed to respond.
317037	DataPrivilege synchronization took a long time due to an incorrect datatype for the SID parameter.
323147	Users with the Logs View role can now run Sync Latest Events.
326038	The Affected user/group filter in report 1a and the log failed to retrieve events which occurred before the user was moved to a different organizational unit.
331433	The search box label in the DatAnswers UI displayed an ellipsis when the text was too long.

Issue ID	Description
335185	The Events - Pull job failed to complete and a CHECK constraint violation was received. This occurred because the statistics tables were prematurely archived.
355163	Host-named site collections with one or more characters following the name of the host caused the DCF to fail.
366915	A large number of false positives were returned when the DE Driver's License Number pattern was used. A new validation algorithm for the tenth digit of the German driver's license number (Führerscheinnummer) was implemented.
370480	DatAnswers now works with HTTPS.
373232	A user with permissions to assign global flags and tags did not have the rights to remove global flags and tags from an object.
374148	CID images in email templates were not displayed in OWA.
374332	When the default domain was removed in the Management Console, no other domain was defined for the Varonis system user. As a result, DataPrivilege requests failed to complete and error messages were received in the UI.
375217	In DatAdvantage, when the Group Policy Management Console (GPMC) was not installed (or disabled), and events were added to the domain services, starting the Probe resulted in errors in the Event Viewer.
382409	A network error occurred and DataPrivilege failed to log the exception.
392812	It was not possible to add a domain with the same SID as the existing file server.
393792	When a customized logo was set through the Management Console, DatAnswers displayed the default Varonis logo until the user was fully loggedon. Only then was the customized logo displayed.
394894	An error occurred when full FileWalk was run and the session ID was over one billion.
404592	While checking the status of a running DTE rule, the progress bar displayed only folder commands and not file commands.

Issue ID	Description
404593	It was not possible to check the status of a newly created DTE rule.
404597	Upon upgrade to 6.2.3, the options to add SharePoint or Exchange Online file servers were not available.
405630	The value of the AffiliatedDomainID was incorrect. The file servers table displayed the old domain ID instead of the new one.
407828	The China Union Pay card pattern did not cover all credit card ranges.
410670	In DatAdvantage, it was not possible to maximize the Change Management and Commit window.
412136	It was possible to install licenses for DatAdvantage Lite and Data Transport Engine (DTE).
412274	A timeout occurred while waiting for the Varonis Filer Monitor service to connect.
413549	In DatAnswers, a user that is part of one domain will be able to search on other domains only if there is a trust between the two domains and both domains are monitored in DatAdvantage.
413857	Report 4f displayed incorrect date and time format in the File Modify Date column.
418741	A primary key violation occurred on the RTAlertedEvents table while running the Events - Pull job.
419348	A NetApp cluster mode file server disconnected from the Varonis FPolicy server because the size of the TCP socket receive buffer was insufficient. As a result, the Probe did not receive all data from the file server.
419360	In order to run FileWalk on SharePoint Online, the SharePoint Online/ OneDrive user can have SharePoint administrator permissions instead of the Global administrator permissions.
419363	When a synced domain user was defined as the ADWalk user, ADWalk failed to run on the Azure Active Directory domain.
420365	The "Failed to identify Domain identity for filer xxx" error message displayed the wrong file server details.

Issue ID	Description
420594	An exception was thrown and FileWalk failed to complete when WrapperException() was called without UTF-8 characters.
421187	A performance issue occurred while event archive jobs were running on NFS directories.
421627	In Directory Services, no errors were printed to corrupted domain controller security logs.
422638	When DatAdvantage was installed in an environment that used SQL Server Enterprise edition, the Partition table was improperly created and the Partition View could not be updated. Therefore the Events-Pull job failed.
423123	Following the migration of the IDU database to another server, the Trustworthy attribute on the VrmsDomainDB database was no longer selected.
423816	A mount point was not crawled when another mount point was defined on the same path in the volumes list.
425524	A different name was displayed for the spVerification_FixFilerIdentity stored procedure in the catch block. As a result, the wrong notification was received.
426097	ADWalk failed to crawl a local administrator's account on an EMC file server. As a result, the permissions could not be resolved.
427001	ADWalk failed to crawl a local administrator's account on an EMC file server. As a result, the permissions could not be resolved.
428671	A performance issue occurred while running the FileWalk Collector Data Processing job. This occurred because the file servers contained a large number of folders.
429307	The Detect OS method failed to retrieve a file server's data.
429748	An error occurred while migrating mail auditing data in DataPrivilege.
429905	Poor performance followed by a timeout occurred when RDLs or templates were uploaded to the Reports site.

Issue ID	Description
430361	In report 1a and in the log, when the Affected user/group filter was used, not all results were returned.
431435	The column headers in the subscription CSV files now match those of reports generated in the UI.
432447	The Owner SID was missing from the FileWalk data on directory service file servers.
432650	When the "Apply object limitation for users that own both directory objects and file system objects" option was selected and then saved, the Management Console failed to save the change.
432662	In DataPrivilege, the Requests and Authorizations report did not work properly.
433844	The Collector Events Delivery job failed to load event files from the Collector.
434127	In DataPrivilege, the Disabled and Deleted Owners report failed to display data regarding users that have been added as owners or authorizers after being disabled.
435154	After changes were made on a SharePoint site, the INodes table failed to remove older INode values.
435826	A DCF Service error occurred when a Null value was inserted as the SSH file user name and password.
436266	The AD_SidIDs table displayed the wrong checksum value in the Varonis System User row, causing the Pull AD job to fail.
436920	While creating a data-driven subscription, a schedule was set before Delivery parameters were set. As a result, the schedule settings were not saved.
437210	The Reports view displayed no results even though a CSV file was created and contained results.
439230	In DataPrivilege, the calculation of an automatic rule failed.
440153	During repair and upgrade, the FileWalk schedule was duplicated, resulting in inconsistencies.

Issue ID	Description
441337	The Sync Probe Proxy job failed to synchronize flag setting changes in the Filers_Proxy table from the IDU to the Probe. As a result, event collection was not properly executed.
441571	The fixDomainIDent stored procedure was missing after a Windows file server was added.
443399	The IDU Server stopped responding in large environments while deleting file servers or stopping jobs.
443422	The "IsDecommissioned" property for a file server was not transferred to the Probe database.
443698	The CifsQueue failed to deliver events on a mount which was not logged, even though another mount on the same device was logged.
445658	A deadlock occurred while running the Events - Pull and Events - Archive jobs on an Exchange file server.
445924	When events were created on a file server on which incremental FileWalk was disabled, the relevant tables were not removed.

Known Issues

6.3.190

N/A

6.3.189

N/A

6.3.188

N/A

6.3.187

N/A

6.3.186

N/A

6.3.185

ID	Documentation
559236	When all platform licenses are expired, only report 8b is available.
572193	A duplicate "S" permission line appears in a report for the Users group.

6.3.173

ID	Documentation
502617	The automatic detection of Windows Server 2016 by simple users (i.e., users with backup operator and power user privileges) is possible <i>only</i> if the Active Directory (AD) role is installed on Windows Server 2016.
508865	The DCF scans the entire contents of compressed files using the same provider that begins the analysis. This means that if the contents include a different type, such as a .zip file, that type will not be scanned.
519282	In the DataPrivilege API, the reqID output parameter of the AddNewPermissionToFolder method is not the actual request ID of the created permission group.
531960	When resolving a hybrid dual-stack Ipv4/Ipv6, the IpResolver does not recognize it as a valid Ipv6 address (and convert it to Ipv4).
535929	In the DataAlert web UI, if directory service events that occurred on accounts are filtered by "Event on user" with flags, tags or notes, the filter functions correctly but the corresponding column does not display the flags linked to the user account; rather, it displays the flags linked to the directory service object of the account.
538062	DataPrivilege users are accustomed to searching for users by their CN value in the Active Directory. However, in DataPrivilege 6.1 and higher, the actual CN value is the user display name taken from Active Directory. Therefore, DataPrivilege users cannot do the following: • See the CN value of a user in the UI (even if the 'Active Directory property for display name of users and groups' option is set to CN) • Search users via pickers by their CN value • See the CN value reports. Customers whose CN value is identical to the display name value are not affected by this issue.

ID	Documentation
543618	During DataPrivilege migration, Dell FluidFS folders are not migrated properly to the new database. This results in an incorrect warning message during the Database Conversion process. The Database Conversion process is unable to properly detect the Dell FluidFS file server, since the Dell SDK does not expose this information.
562582	In DatAlert, when an alerted event is received, the publisher service rounds the event time up rather than allowing the SQL Server to round it down. As a result, related alerts may not be included in reports. This only affects Exchange alerts.

6.3.163

N/A

6.3.162

Issue ID	Description
563541	If the DataPrivilege conversion process fails to disable a migrated report subscription, an internal Reporting Services exception message is displayed to the user rather than a Varonis message.
563802	During the mail template conversion step of the DataPrivilege migration, the conversion process uses SQL authentication by default; it does not use the authentication method chosen by the user.

Issue ID	Description
559621	When the DCF scanned a large number of small files, an out-of-memory exception occurred.

6.3.161

N/A

6.3.160

N/A

6.3.157

N/A

6.3.154

N/A

6.3.153

Issue ID	Description
473791	While the Users and Groups panes indicate that editing was initiated by the Automation Engine, the changes themselves are not visible and cannot be changed through Change Management; in addition, the folder does not indicate that there is an active Automation Engine rule that affects its editing.
482726	The following filter combination is not allowed. It will be handled as if the operator is AND and not OR: • Rule name contained in (rule X, rule Y) • Hit count equals 0 OR • Is sensitive equals No
486327	Migrating users and groups between domains requires redefining their direct permissions on the managed folders (to use the new SID).
490539	DataPrivilege does not support DFS links that point to other DFS links. Folders defined this way in DataPrivilege 6.0.x are no longer synchronized following upgrade to 6.3.x.
500078	This version does not provide a graphic view of the distribution of alerts over users, devices or data.
502765	In NetApp, since the root folder has only GAG permissions, the default advanced exclusion filter (Exclude folders with only global access group NTFS permissions) must be removed from the GAG remediation rule in order to generate results when calculating the rule scope.
504896	Following migration of the VrnDomainDB database to a new SQL instance and running the Report Deployment Tool, friendly names are no longer displayed for report columns.
514344	EMC Unity currently supports only CIFS events.
516760	In 6.3.153 and higher, the Review Area is only available for users having the Review Area user role.

6.3.102

Issue ID	Description
423048	In DatAdvantage, if the Remove protection without unique permissions and Add protection with copy permissions from parent commands are created on a folder together, only the remove permission commands related to actual removed permissions are displayed. The add permission commands that result from the add protection action are not seen. The error is calculated only if the total effective permissions resulting from the add and remove protection commands are not enough based on the events.
476868	In the Data Classification Framework, the process of extracting content from Office documents that contains linked embedded files fails.
413820	In the UI, reports and subscriptions might fail to load if more than approximately 600 filters are configured. If this occurs, it is recommended to reduce the number of filters used in a single report.
453766	The Share Discovery job does not detect shares on the CIFS connector.

6.3.50

Issue ID	Description
386094	If a broken inheritance rule is set to run on a specific resource and the upgrade process is started while the rule is running, the rule is not stopped. This results in an execution error for the rule. However, the rule will be executed successfully for resources that were not part of the upgrade.
385434	Due to a NetApp known issue (NetApp ID 738251), local NetApp groups cannot be found during a search in the DataPrivilege UI, even if the groups exist on the file server.
387711	In the Azure AD domain properties, if an AD attribute other than the default is used for ImmutableId, contact Varonis Support to update the value in the database.
393168	If the parent share of a monitored share is not monitored, the details of the monitored share's permission inheritance will not be available since the parent folder is not scanned. It is recommended that shares monitored in the Management Console be for protected folders.

Issue ID	Description
395892	In the Broken Inheritance Repair utility, if the Only apply these permissions on objects and/or containers within this container option is selected for the Creator-Owner permission, the utility does not propagate the owner to nested objects; however, it reports as if it does propagate the owner.
411287	In monitoring Access Denied events on EMC (or Windows), right-clicking a folder without access rights and selecting Properties creates false Access Denied Open Folder events.
411294	In EMC CIFS Access Denied events, some pattern filter cases may not function as expected.
411553	In DataPrivilege, the width of report columns is fixed to enable printing at A4 size.
414938	The DCF only allows inserting integers into the text field, not properties of the Decimal type. When extracting decimal properties from a file, the decimal number is rounded to the closest integer and compared to the number that the user inserted in the rule condition.
423693	A custom SharePoint permission appears approximately 1 minute after it is added, while a custom Windows permission appears right away.
424342	If an older version of DataPrivilege has managed a DFS path of a folder and a local machine group was permitted to it, the permissions of the group appears as added outside DataPrivilege following schema conversion to 6.3.x.
428516	Windows 2003 only supports the required crypto algorithm if the following hotfix is installed: https://support.microsoft.com/en-us/kb/968730
433801	If an attachment is added to an object in SharePoint Online (in either a list item or a task), the Create event includes only the file name, not the object name.
434799	No path is presented in the log for users who are deleted before ADWalk and PullWalk.
442737	Subscriptions to the DataPrivilege <i>Managed Folder User Level Permissions</i> report might not be sent due to their size, if the Render Format option was set to Web Archive.

Issue ID	Description
443848	When DataPrivilege is used in a Windows 2003 environment and Windows Authentication is configured, an error may be displayed in the browser when the DataPrivilege website is accessed. The issue does not arise if SQL authentication is used, or a Windows version higher than 2003 is used.
444143	Alerts on permission changes are not received in Dell.
444626	In DataPrivilege, the mechanism that triggers the Incremental FileWalk upon addition of a folder to DataPrivilege while FileWalk is running is disabled. Therefore, folders that are added from DataPrivilege must wait for the next FileWalk run. This might take up to 24 hours, depending on FileWalk scheduling.