



METADATA FRAMEWORK 6.2.85

Release Notes

Publishing Information

Software version	6.2.85
Document version	46
Publication date	March 29, 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.

INTRODUCTION

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 6.2.85

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

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

What's New in 6.2.80

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

- DataPrivilege
 - Migration is now supported for the DataPrivilege Web Application.
- Data Transport Engine
 - This version enables cloning Data Transport Engine rules.

What's New in 6.2.74

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

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

What's New in 6.2.73

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

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

What's New in 6.2.72

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

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

What's New in 6.2.71

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

- Data Transport Engine
 - A new option, *Display virtual entities in Work Area prior to executing rules*, enables displaying the virtual entities to be created at the destination in the Work Area.
- Reports
 - The *Assigned Owner SAM Account Name* column is now available in report 4f.
 - New filters
 - *Exclude files with hits on these rules*
 - In this version, the new *ShouldAlwaysLimitReportServerExportOutputRows* configuration key enables setting how report subscriptions will be generated.
- Core and infrastructure
 - *Mailbox permission added* and *Mailbox permission removed* PowerShell events are now supported on Exchange 2013.

What's New in 6.2.66

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

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

What's New in 6.2.63

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

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

What's New in 6.2.62

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

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

What's New in 6.2.61

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

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

What's New in 6.2.60

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

The version contains the following new features:

- Data Transport Engine
 - In this version, Data Transport Engine mirror rules can copy stub files that were created by regular rules.
- DCF
 - The new DCF predefined rule, *Security Certificate File Types*, detects security certificate files.
- Core and infrastructure
 - A log collection program gives customers the opportunity to help improve the Metadata Framework.
 - SQL Server credentials are now cached when a file server is added, so that the credentials are automatically entered if another file server is added during the same session.

What's New in 6.2.53

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

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

What's New in 6.2.52

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

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

What's New in 6.2.51

This version of the Metadata Framework is declared generally available. This includes DatAlert Analytics.

- DatAdvantage
 - 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.
- Data Transport Engine
 - With this version, the Data Transport Engine now copies unique as well as inherited permission entries from the source to the destination.
- DCF
 - With this version, a match is considered valid even though the pattern is enclosed in parentheses or square brackets.
- DatAlert
 - A new DatAlert Analytics threat model has been introduced, *Immediate pattern detected: user actions resemble ransomware*.
- Reports
 - 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.
- Core
 - Ubuntu-14.04-SMP-3.13.0-74-x86-64 is now supported.
- Upgrade
 - DatAdvantage can now be upgraded to a separate version from DataPrivilege; ownership synchronization and IDU Analytics recommendations are retained.

What's New in 6.2.38

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

What's New in 6.2.37

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

What's New in 6.2.36

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

What's New in 6.2.35

- DatAdvantage
 - The Dictionaries tab has been moved from the DCF and DW Configuration window to a window of its own, accessible through the Tools menu.
 - In the log, times are now normalized to UTC.
- Management Console
 - This version enables identifying *executive accounts* during discovery of privileged accounts.
 - The following jobs have been added to the new *DatAlert Analytics* jobs category in the Management Console:
 - *DatAlert Analytics Trigger Publisher*
 - *DatAlert Analytics Calculate Entities*
 - *DatAlert Analytics Calc Stats*
 - *DatAlert Analytics Windows service rules*
 - *DatAlert Analytics Exchange rules*
 - *DatAlert Analytics Lockout rules*
 - *DatAlert Analytics Extensions rules*
 - *DatAlert Analytics Crypto rules*
- DatAlert
 - In this version, a number of enhancements and changes have been made to the DatAlert scope configuration.
 - This version enables running a custom or built-in executable script for each DatAlert rule. In addition, placeholders can now be applied as environment variables in executable scripts.
 - With this version, Varonis introduces the DatAlert web interface, which enables monitoring and analyzing the various alerts generated by DatAlert and DatAlert Analytics.
 - With this version, Varonis now supports the integration of DatAlert with the following Security Information and Event Management (SIEM) systems:
 - HP ArcSight
 - FireEye TAP
 - LogRhythm
 - The names of the following predefined rules and threat models were changed in this version:
 - *Abnormal behavior: access to sensitive data* was renamed to *Abnormal behavior: unusual amount of access to sensitive data*
 - *Abnormal behavior: unusual amount of access to stale data* was renamed to *Abnormal behavior: unusual amount of access to idle data*
 - *Abnormal behavior: unusual amount of activity on script files* was renamed to *Abnormal behavior: unusual amount of script file creations*
 - The following predefined rules and threat models were added in this version:
 - *Abnormal admin behavior: unusual amount of lockouts across admin accounts*
 - *Abnormal behavior: accumulative create and delete actions resemble ransomware*
 - *Abnormal behavior: accumulative increase in access to idle data*
 - *Abnormal behavior: accumulative increase in access to sensitive data*
 - *Abnormal behavior: accumulative increase in lockouts across end-user accounts*

- *Abnormal behavior: accumulative increase of lockouts for individual end-user accounts*
- *Abnormal behavior: accumulative user rename and modify actions resemble ransomware*
- *Abnormal behavior: unusual amounts of lockout across end-user accounts*
- *Abnormal behavior: unusual number of file deletions*
- *Abnormal behavior: unusual number of sensitive file deletions*
- *Abnormal behavior: user create and delete actions resemble ransomware*
- *Abnormal behavior: user rename and modify actions resemble ransomware*
- *Abnormal executive behavior: accumulative increase in access-denied events across executive accounts*
- *Abnormal executive behavior: accumulative increase in access to script, configuration and backup files across executive accounts*
- *Abnormal executive behavior: unusual amounts of access-denied events across executive accounts*
- *Abnormal executive behavior: unusual amounts of access to script, configuration and backup files across executive accounts*
- *Abnormal service behavior: accumulative increase in lockouts across service accounts*
- *Abnormal service behavior: accumulative increase in lockouts for individual service accounts*
- *Abnormal service behavior: unusual amounts of lockouts across service accounts*
- *Executive account locked-out/disabled/deleted/password reset*
- *Membership Changes: Service Accounts*
- *Modification: Critical Organizational Units*
- *Modification: GPO Security Settings*
- *Permission changes on OU*
- *Permissions granted directly to user in directory services*
- *Permissions granted directly to user in windows file system*
- *Suspicious access activity: service account access to file containing credentials*
- The following predefined rule was removed in this version:
 - *Possible asset exposure: permissions granted to user in local/unmonitored/abstract domain*
- Reports
 - The following filters have been added in this version:
 - *Alert category*
 - *Alert ID*
 - *Alert severity*
 - *Asset*
 - *Excluded file name and extension*
 - *Excluded file name and extension dictionary*
 - *File name and extension*
 - *File name and extension dictionary*
 - *Only alerted events*

- *Show DatAlert details*
 - *Number of alerts*
 - *Number of events*
- DatAnswers
- Core and Infrastructure
 - This version provides increased support for the source IP in events.
- Upgrade
 - This version supports the upgrade of DatAlert exclusion scopes (that is, scopes configured prior to this version) to a new scope.

What's New in 6.2.15

- DatAdvantage
 - CNAME aliases for file servers are now supported in DFS management.
- DatAlert User Behavior Analysis now requires a separate license from standard DatAlert.
- Reports
 - The DatAdvantage Reporting API provides customers with restful APIs that enable accessing and extracting data from DatAdvantage.
 - 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 queries have been optimized.
- Columns have been added to the database views for CIFS events.

What's New in 6.2.10

- DataPrivilege
 - The Bulk Upload Utility is now supported.
- Core
 - In this version, it is possible to configure Probe proxies on NetApp clusters.
 - This version provides support for IBM Storwize v7000 version 1.6 and higher.
 - The Probe database provides two new views for retrieving and resolving CIFS and Exchange events, regardless of whether they were gathered directly by the Probe or by a Collector.

What's New in 6.2.6

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

What's New in 6.2.5

- DatAlert
 - In this version, DatAlert provides a number of predefined rules. These rules are categorized as follows:
 - User Behavior Analysis rules
 - Threshold
 - Standard alert rules
 - DatAlert now provides filters that enable *excluding* entities from a rule scope.
- Management Console
 - This version provides automatic discovery of *privileged* accounts, such as administrative users, testing and service accounts.
- New filters
 - *Acting privileged accounts*
 - *Affected privileged accounts*
 - *Included access paths*
 - *Excluded access paths*
 - *Directory Services access paths*
 - *EMC access paths*
 - *Exchange access paths*
 - *Hitachi NAS access paths*
 - *HP NAS access paths*
 - *NetApp access paths*
 - *SharePoint access paths*
 - *Unix access paths*
 - *Unix SMB access paths*
- Changes to Existing Filters
 - The inner filters of the *File properties* compound filter have been changed. They are now:
 - *File name and extension*
 - *Excluded file name and extension*Both these filters permit adding a list of values (semicolon-separated).
 - The *Affected object path* filter is now available in report 6b, under *Affected objects > Directory objects*.

What's New in 6.2.3

- DatAdvantage
 - The DatAdvantage user interface can be installed on Windows 10.
 - It is now possible to filter directories and files in the Directories pane according to one or more classification rules. The *Classification Rules* submenu has been added to the Filters menu in the Directories pane to enable this option.
 - This version provides the *Classification Analysis for Unix Files* user role for DatAdvantage. Users with this role will be able to view the classification analysis of all sensitive files on a Unix file server from the Work Area.

- Integrated - With this version, Varonis now provides complete visibility into directory service events. Several new events related to authentication, permission and GPO setting changes have been added to support this enhancement. In addition, enhancements have been made to existing directory service events.
- Integrated - DatAdvantage now provides complete visibility into Group Policy Object (GPO) changes. It includes support for several new events related to GPO changes.
- Integrated - Varonis now provides complete visibility into permission changes on directory service objects.
- Integrated - The commit process has been optimized to enable managing changes and commit processes. All commit operations can now be performed through the **Change Management and Commit** window. In addition, this window enables viewing commit actions and processes that are both pending and historical.
- Integrated - The Archive option on the Tools menu now enables administrators to archive committed processes.
- DataPrivilege
 - Integrated - Broad support for on-premises SharePoint
 - Integrated - Changes to application settings
 - Integrated - Additional DataPrivilege jobs
- Management Console
 - With this version, it is now possible to decommission a file server that no longer exists. When a file server is decommissioned, historical data is saved. The **Set file server as decommissioned** option has been added to the **Editing file server** window of the Management Console to enable this configuration.
 - The Management Console now enables configuring elevated privileges for DatAnswers users. To enable this configuration, the Elevated search mode drop-down list has been added to the Administration tab on the **DatAnswers Setup** page.
 - For DatAnswers, it is now possible to select whether suggestions are displayed in the menu under the My Folders search box while typing the name or path of a folder. The *Show suggestions in My Folders search box menu* option has been added to the Display Layout Attributes area of the Page Layout tab to support this configuration.
 - The *Sync SharePoint* job has been added to the *Synchronization* jobs category.
 - The *IDU Analytics* job now runs every Saturday at 08:00.
 - Integrated - With this version, the Management Console enables adding and editing Azure Active Directory domains from the **Domains** pane.
 - Integrated - It is now possible to add Exchange Online and SharePoint Online file servers from the File Server wizard. For SharePoint Online, the Sites tab of the wizard now enables selecting site collections, public sites as well as OneDrive for Business personal sites.
 - Integrated - In this version, it is now possible to configure the lifetime of changes and committed processes before they are archived or deleted. The Pending Changes and Commit area has been added to the Archive Policy tab to enables this option.
 - Integrated - The Management Console now enables storing the credentials used for the commit process. The Commit Credentials area has been added to the DatAdvantage Security tab to enables this option.

- Integrated - It is now possible to view failed synchronizations from the Failed Syncs tab. In addition, the following Synchronization jobs have been added to the *Synchronization* jobs category:
 - *Re-run Failed Sync jobs*
 - *Sync Domains*
 - *Sync EMC Controller*
 - *Sync Exchange Configuration*
 - *Sync Filer*
 - *Sync Filer Deleted*
 - *Sync Filtered Users*
 - *Sync Monitored Mailboxes*
 - *Sync Probe Configuration*
 - *Sync Probe Licences*
 - *Sync Probe Proxy*
 - *Sync Pruned Dirs*
 - *Sync Pruned Users*
 - *Sync Volumes*
- Integrated - It is now possible to install a local database (LocalDB) on a Collector. To support this enhancement, the *Use LocalDB on this Collector (advanced)* option is now available when adding a new Collector through the Management Console or the Enterprise Installer.
- Integrated - The following jobs have been added to the *DataPrivilege* jobs category:
 - *DataPrivilege Sanity Check*
 - *DataPrivilege Objects Maintenance*
 - *DataPrivilege Incremental Synchronization*
 - *DataPrivilege Entitlement Review*
 - *DataPrivilege Full synchronization*
 - *DataPrivilege Sync Owners*
- Integrated - A notification mechanism that continually reminds users to address file server upgrade failures has been introduced.
- Integrated - A **Repair** button has been added to the Resource toolbar on the main File Server tab of the Management Console.
- Integrated - In this version, data sync shares and web servers can now be edited from the DatAnswers General tab of the Management menu.
- Integrated - It is now possible to edit DatAnswers, API and SOLR Admin access accounts from the DatAnswers Accounts tab of the Management menu.
- DCF
 - This version introduces various thresholds to predefined rules, to reduce the number of false positives (rules will be rescanned during upgrade). In particular, the **Sarbanes-Oxley** rule has been restored to the DCF.
 - Dictionaries can now be used to find file names.
 - It is now possible to designate negative keywords that must *not* be found within the specified proximity to a potential match in order for that match to be valid. The Negative Keywords area has been added to the **New Pattern** dialog box to enable this option.

- The following pattern has been added:
 - *Korean Resident Registration Number*
- Integrated - The DCF now supports SharePoint Online items, such as document libraries, sites, items, and lists.
- Integrated - With this version, the DCF supports Unix out of the box; that is, without the installation of Samba.
- Integrated - Keywords and excluded values are no longer predefined parameters of regular expressions. Instead, they are now configurable as needed through the UI.
- Integrated - In this version, multiple RSA connections can be defined in the database. However, they cannot be displayed or edited in the UI.
- Integrated - The *UK Vehicle Registration Number* pattern was added.
- Integrated - The *UK Electoral Roll Number* pattern was removed.
- Integrated - The **Save** and **Refresh** buttons have been removed from the Patterns tab. Instead, changes are saved in the dialog box in which they are actually made.
- Integrated - A new column, *Country*, enables filtering available and selected patterns by country.
- DatAlert
 - Starting with this version, all DatAlert mail has two parts - HTML and plain text.
 - In this version, DatAlert includes a predefined alert template that complies with the CEF format, to enable sending DatAlerts to HP ArcSight via Syslog.
 - Integrated - DatAlert now supports all new directory service events.
 - Integrated - Support is now provided for several Exchange admin events.
 - Integrated - DatAlert now provides support for all directory service object creation events, including custom types.
- Reports
 - In this version, it is possible to set owners for report templates and subscriptions. Ownership enables restricting template visibility, so that users only see the relevant templates.
 - The trend reports now store and display trends for each classification rule, in addition to the total number of classification results displayed in previous versions.
- New Reports
 - Report 12.l.02, Open Access on Sensitive Data
 - Report 14.a.04, Open Access on Sensitive Data Statistics
 - Integrated - Report 1.a.05, Events Committed Through DatAdvantage
 - Integrated - Report 1.a.06, Directory Service Permission Change Events
 - Integrated - Report 1.a.07, After Hours Authentication Events
 - Integrated - Report 1.b.01, GPO Setting Changes
 - Integrated - Report 2.a.02, Statistics by Event Operation
 - Integrated - Report 2.a.03, Users with Failed Events
 - Integrated - Report 2.e.01, Most Active Users per Folder
 - Integrated - Report 2.e.02, Users with Most Failed Events per Folder
 - Integrated - Report 2.f.01, Event Type Distribution on File Server
 - Integrated - Report 2.f.02, Event Type Distribution per User

- Integrated - Report 16.a.01, Authentication Statistics per Hour or Day
- Integrated - Report 16.b.01, Users with Failed Authentications
- New Filters
 - *Windows access paths*
 - *% change in hit count (selected rule)*
 - *% change in hit count on files with open access (selected rule)*
 - *% change in no. of files with hits (selected rule)*
 - *% change in no. of files with hits and open access (selected rule)*
 - *% change in no. of folders with hits (selected rule)*
 - *% change in no. of folders with hits and open access (selected rule)*
 - *% change in size of files with hits and open access (selected rule)*
 - *% change in size of all hits (GB) – selected rule*
 - *Display assigned owner*
 - *Elevated mode*
 - *Elevated user*
 - *Elevated user's domain*
 - *Email*
 - *Hit count (selected rule)*
 - *Hit count on files with open access (selected rule)*
 - *Hit count on files with open access (selected rules)*
 - *Mail-enabled*
 - *No. of files with hits (selected rule)*
 - *No. of files with hits and open access (selected rule)*
 - *No. of files with hits and open access (selected rules)*
 - *No. of folders with hits (selected rule)*
 - *No. of folders with hits and open access (selected rule)*
 - *Physical size of this folder (in MB)*
 - *Physical size of folder and subfolders (in MB)*
 - *Physical size of subfolders (in MB)*
 - *Public folder type*
 - *Size of all hits (GB) – selected rule*
 - *Size of files with hits and open access (selected rule)*
 - *Show group members in sub report*
 - Integrated - *Azure blockCredential*
 - Integrated - *Azure isBlackberryUser*
 - Integrated - *Azure isLicensed*
 - Integrated - *Azure isSystem*
 - Integrated - *Azure lastDirSyncTime*
 - Integrated - *Azure liveId*
 - Integrated - *Azure ObjectID*
 - Integrated - *Azure passwordResetNotRequiredDuringActivate*
 - Integrated - *Azure preferredLanguage*

- Integrated - *Azure userType*
- Integrated - *Changed GPO settings*
- Integrated - *Commit process ID*
- Integrated - *Date/time interval*
- Integrated - *Event ID*
- Integrated - *GPO name*
- Integrated - *GPO setting name*
- Integrated - *GPO version*
- Integrated - *IP/hostname*
- Integrated - *New setting value*
- Integrated - *Old setting value*
- Integrated - *Permission changes (Directory Services)*
- Integrated - *Policy name*
- Integrated - *Policy path*
- Integrated - *Protected folders only*
- Integrated - *User/computer configuration*
- Integrated - *% change in no. of folders with open access (inc. inherited)*
- Integrated - *Calculate current permissions*
- Integrated - *Calculate effective permissions*
- Integrated - *Calculate recommended permissions*
- Integrated - *Count events on*
- Integrated - *Display affected share paths*
- Integrated - *Display assigned owner*
- Integrated - *Display share path*
- Integrated - *Event count on folder and subfolders*
- Integrated - *iPhone*
- Integrated - *Most active users*
- Integrated - *No. of folders with open access (inc. inherited)*
- Integrated - *Primary user address*
- Integrated - *Recommended file system permissions*
- Integrated - *Telephone number*
- Integrated - *title*
- Changes to Existing Reports
 - The following additional columns have been added to report 4f:
 - *Email*
 - *Mail-Enabled*
 - *Public Folder Type*
 - The following additional columns have been added to report 12l:
 - *Classification Results with Open Access (Selected Rules)*
 - *Hit Count on Files with Open Access (Selected Rules)*
 - *Management Status*
 - *No. of Files with Hits and Open Access (Selected Rules)*

- *Owner Name*
- *Uniqueness*
- The following additional columns have been added to report 14a:
 - *Hit Count (Selected Rules)*
 - *Hit Count on Files with Open Access (Selected Rule)*
 - *No. of Files with Hits (Selected Rule)*
 - *No. of Files with Hits and Open Access (Selected Rule)*
 - *No. of Folders with Hits (Selected Rule)*
 - *No. of Folders with Hits and Open Access (Selected Rule)*
 - *Size of All Hits (GB) – Selected Rule*
 - *Size of Files with Hits and Open Access (Selected Rule)*
- The following additional columns have been added to report 14b:
 - *% Change in Hit Count (Selected Rule)*
 - *% Change in Hit Count on Files with Open Access (Selected Rule)*
 - *% Change in No. of Files with Hits (Selected Rule)*
 - *% Change in No. of Files with Hits and Open Access (Selected Rule)*
 - *% Change in No. of Folders with Hits (Selected Rule)*
 - *% Change in No. of Folders with Hits and Open Access (Selected Rule)*
 - *% Change in Size of All Hits (GB) – Selected Rule*
 - *% Change in Size of Files with Hits and Open Access (Selected Rule)*
- The following trends have been added to report 14c:
 - *Hit count (selected rules)*
 - *Hit count on files with open access (selected rules)*
 - *No. of files with hits (selected rules)*
 - *No. of files with hits and open access (selected rules)*
 - *No. of folders with hits (selected rules)*
 - *Size of all hits (GB) – selected rules*
 - *No. of folders with hits and open access (selected rules)*
 - *Size of files with hits and open access (selected rules)*
- The following changes have been made to report 15a:
 - The Folder selection category has been added to the Event type filter. The following event types are now available:
 - *Add file's parent folder to My Folders*
 - *Folder added*
 - The Search Scope column has been added.
 - The following additional columns have been added:
 - *Elevated Mode*
 - *Elevated User*
 - *Elevated User's Domain*
- Report 9h and Trend reports - Columns and filters that show folder size now show the logical size.

- Integrated - Report 8.b.01, DatAdvantage Operational Log - The *Date* filter now enables selecting the relevant unit of time (days, minutes or hours) from a drop-down list. The drop-down list is displayed only if *Relative Mode* is selected.
- Integrated - Report 2.a.01, Access Statistics - The **Event Types** and **Event Count on Folder and Subfolders** columns have been added.
- Integrated - Report 2a - The **Effective File System Permissions** and **Recommended File System Permissions** columns have been added.
- Changed filters
 - Integrated - The *Interval* filter is now part of both the *Trend Interval* and *Date/time interval* compound filters.
 - Integrated - The following filters are now part of both the *Permission changes (Windows)* and *Permission changes (Directory Services)* compound filters:
 - *Changed permission*
 - *Permission after change*
 - *Permission before change*
 - *Permission type*
 - *Trustee*
 - *Trustee account type*
 - Integrated - The *Show data from* filter can now retrieve *History of differences - commit only* events. This filter enables users to quickly and easily find events on commit actions performed in DatAdvantage.
 - Integrated - The *Permission changes for global access groups only* filter now supports Directory Service permission events.
 - Integrated - The *% change in no. of folders with global access* filter was renamed to *% change in no. of folders with open access*.
 - Integrated - The *% change in no. of sensitive files accessible by global access groups* filter was renamed to *% change in no. of sensitive files with open access*.
 - Integrated - The *% change in no. of sensitive folders accessible by global access groups* filter was renamed to *% change in no. of sensitive folders with open access*.
 - Integrated - The *Affected users from group* filter was renamed to *Affected objects from group*. Now filters according to the users, computers and groups who are members of the selected group(s), including derived members.
 - Integrated - The *No. of folders with global access* filter was renamed to *No. of folders with open access*.
 - Integrated - The *No. of sensitive files accessible by global access groups* filter was renamed to *No. of sensitive files with open access*.
 - Integrated - The *No. of sensitive folders accessible by global access groups* filter was renamed to *No. of sensitive folders with open access*.
- Report subscriptions
 - Integrated - With this version, it is now possible to run report subscriptions immediately from the subscription form and the My Subscriptions pane. The *Run immediately* option

in the subscription form and the **Run** button on the toolbar of the My Subscriptions pane have been added to enable this option.

- Integrated - Report subscriptions can now be scheduled to run at a time in the past. This can be used to overcome time zone differences.
- Integrated - Reports 2.e.01, 2.e.02, 2.f.01 and 2.f.02 - These reports support data-driven subscriptions.
- Integrated - Several changes were made to enhance the performance of DatAdvantage reports.
- DatAnswers
 - This version enables specified users to run searches with elevated privileges. Users with the *DatAnswers Elevated Search* user role can run elevated searches, either by seeing unfiltered results or by impersonating a different user.
 - In this version, it is now possible to narrow the result set by limiting the search scope to a specific folder or a set of folders. A number of changes have been made to the DatAnswers UI to support this enhancement.
 - The Advanced link, which enables performing advanced enterprise searches, is now displayed on the initial DatAnswers page and the search results page.
 - Integrated - With this version, DatAnswers enables viewing the metadata for each item displayed in the search results. The Metadata pane, which is displayed to the right of the search result, has been added to enable this option. Additionally, it is now possible to view the information of a contact displayed in the Metadata pane.
 - Integrated - DatAnswers API
 - In this version, new API methods are now available, which enable retrieving a document's metadata and the contact information of document authors, business owners and users who performed Create or Modify events on the document.
 - New API methods:
 - *GetDocumentMetaData*
 - *GetContactsData*
- Core and Infrastructure
 - The Metadata Framework supports data deduplication on Windows 2012.
 - New Linux flavors
 - Red Hat 6 Kernel 2.6.32
 - SMP - X86 32 bit
 - 2.6.32-504
 - Red Hat 7

- SUSE SLES 11.3 Kernel 3.0.76 - Supported types:
 - SMP - 64 bit
 - 3.0.76-0
- SUSE SLES 12.0 Kernel 3.12.28 - Supported types:
 - SMP - 64 bit
 - 3.12.28-4
- Ubuntu 12.04.4 LTS Kernel 3.2.0
 - SMP - 64 bit
 - 3.2.0-58-virtual
- Ubuntu 14.04 LTS Kernel 3.13.0
 - SMP - 64 bit
 - 3.13.0-24
- This version provides support for AIX 7.1.
- Exchange On-Premises - The following information is now collected for mail-enabled public folders (in addition to existing support for these events on mailboxes):
 - Message created
 - Message received
- Integrated - This version introduces some changes to the architecture of the Metadata Framework, to support the tight integration between DatAdvantage and DataPrivilege.
- Integrated - In this version, Varonis provides actionable insight into Azure Active Directory users and groups and the information residing on Exchange Online and SharePoint Online. This includes bi-directional visibility into Active Directory Domain Service permissions (on-premises) as well as Azure Active Directory permissions on the cloud. New icons are presented throughout the DatAdvantage user interface to support this enhancement.
 - DatAdvantage now provides bi-directional visibility into Exchange Online and SharePoint Online permissions.
 - Varonis now monitors three types of SharePoint Online site collections:
 - Site collections
 - Public websites
 - OneDrive for Business personal sites
- Integrated - This version provides Distributed Exchange FileWalk (DEF), which enables choosing any Collector from which to run FileWalk on Exchange Storage Group servers.
- Integrated - The names of some services have been changed.
- Integrated - The Metadata Framework now supports SQL Server *AlwaysOn* availability groups.
- Integrated - The Metadata Framework now supports Isilon 7.2 or higher for NFS events.
- Integrated - Support for the following NetApp versions:
 - 8.3 RC, GA
 - 8.3.1 RC
 - 8.3 P1 - Also supported for cluster mode
- Integrated - This version provides support (both visibility and auditing) for NetApp shares on which the *nobrowse* option is enabled.
- Integrated - The Exchange 2013 agent is now generally available.

- Integrated - This version provides support for Nexenta 3.1.3.5.
- Integrated - FileWalk
 - Full FileWalk has been restored as the default mode.
 - If incremental FileWalk is enabled, events made by filtered and unmonitored users are now collected and used in calculating the scope of the incremental FileWalk. These events are not saved anywhere afterward.
- Integrated - Several changes have been made aimed at reducing the number of inessential notifications sent by the Metadata Framework.
- Licensing
 - With this version, the SharePoint Online and Exchange Online licenses are separate from the on-premises licenses. SharePoint Online and Exchange Online file servers can now be installed only if there are valid SharePoint Online and Exchange Online licenses.
 - Integrated - In this version, the behavior of the permanent software license changes when the licensed users and data counters exceed their configured limit.
 - Integrated - Evaluation licenses:
 - The grace period for evaluation licenses has now been extended to 30 days.
 - The behavior of the evaluation license changes when the number of days set for a particular platform's license is reached.
 - The behavior of the evaluation license changes when the grace period for a particular platform has finished.
- Upgrade
 - Upgrade to 6.2.3 is *only* available for installations that have always included *only* DatAdvantage. DataPrivilege cannot be upgraded to this version at all; nor can installations that include both DatAdvantage and DataPrivilege. Only clean installation of 6.2.3 is possible for these environments.
 - In consolidated environments, in which DatAdvantage and DataPrivilege share a working account, the working account must remain the same for both products even if one of them is upgraded to 6.2.3.
 - During the upgrade process, recommendations are now provided to decommission servers that are no longer monitored and for which events are not collected. The **Set Servers as Decommissioned** page has been added to the Enterprise Installer to enable decommissioning one or more of these file servers.
 - Integrated - In this version, it is now possible to upgrade Collectors through the Enterprise Installer. The **Collector Upgrade** page has been added to the Varonis Setup Wizard to enable this option.
- Documentation
 - Integrated - A number of structural changes have been made to the documentation that accompanies the Metadata Framework.
- Noteworthy or Changed Behavior
- Resolved Issues
- Known Issues

2

NEW ENHANCEMENTS

DatAdvantage

Editing Existing Permission Entries

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

6.2.35

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

6.2.35

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

6.2.15

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.

Support for Windows 10

6.2.3

With this version, it is possible to install the DatAdvantage user interface on Windows 10.

Filtering Directories by Classification Rule

6.2.3

In this version, it is now possible to filter directories and files in the Directories pane according to one or more classification rules. The *Classification Rules* submenu has been added to the Filters menu in the Directories pane to enable this option.

The files and directories in the Directories pane are filtered to show only files with a hit count greater than zero on the selected rule(s).

Note: Only rules that were run on files on which hits were detected are displayed in the submenu.

Classification Analysis for Unix Files

6.2.3

This version provides the *Classification Analysis for Unix Files* user role for DatAdvantage. Users with this role will be able to view the classification analysis of all sensitive files on a Unix file server from the Work Area (in the **File Results Analysis** window).

Only the Enterprise Manager can assign this role to users.

Important: This role allows the user to access the files regardless of the user's permissions.

Visibility into Directory Service Events

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

With this version, Varonis now provides complete visibility into directory service events.

It includes support for several new events related to authentication, permission and GPO setting changes, as well as new report templates and filters to identify such changes.

New Events

- Account authentication
- Access request
- GPO settings modified
- GPO link created
- GPO link deleted
- GPO link modified
- Owner changed

Note: Account authentication and access request events are collected from the domain controller. The collection of logon and logoff events from file servers are not supported.

Enhancements to Existing Events

The following enhancements have been made to existing directory service events:

- *DS object permission added (hist. of differences only)* and *DS object permission removed (hist. of differences only)* - In addition to the history of differences, audit events are now supported for both event types. These event types have been renamed to *DS object permission added* and *DS object permission removed* to enable this change.
- *DS object modified* - The event description has been optimized to include the property's old value as well as its new value.

DatAlert

DatAlert now supports all new directory service events. For example, it is possible to receive a notification if GPO settings were modified, or if a GPO link was changed, deleted or created.

Report Templates

See [New Reports in This Version](#).

New Filters

See [Changes to Filters](#).

Visibility into Group Policy Changes

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

With this version, Varonis provides complete visibility into Group Policy Object (GPO) changes. It includes support for several new events related to GPO changes, as well as a new report template and filters to identify such changes.

The following events have been added to enable visibility into GPO changes:

- GPO settings modified
- GPO link created
- GPO link deleted
- GPO link modified

The Log view now displays event log data for every change made to the GPO version number. It is also possible to view GPO setting changes for a single event. To enable this visibility, the **Event Details** window now includes the GPO Changes tab. The GPO Changes tab is displayed only if GPO setting changes were made.

Reports

To support visibility into Group Policy changes, changes have been made to several reports. In addition, [report 1.b.01](#) provides information about changes made to GPO settings. The information in this report can be used to identify the GPO version number, who made the changes, what changes were made as well as prior and current values.

Visibility into Directory Service Permission Changes

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

With this version, Varonis provides complete visibility into permission changes on directory service objects. It includes support for a new report template and filters to identify such changes.

DatAlert

The **What (Event Details)** page now includes the *Permission changes* filter category, which enables adding filters that identify changes made to permissions. For example, a DatAlert can be generated for changes made to Directory Service permissions or permissions on Windows machines.

Report Templates

See [New Reports in This Version](#).

New Filters

See [Changes to Filters](#).

Change Management and Commit

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

With this version, the commit process has been optimized to enable managing changes and commit processes. All commit operations can now be performed through the **Change**

Management and Commit window. It is possible to view commit actions and processes that are both pending and historical.

In addition, the **Change Management and Commit** window enables performing the following operations:

- View pending or invalid changes
- Search for specific changes and commit processes
- View the prerequisites of changes prior to committing, scheduling or discarding
- Commit a single change or a bulk of changes
- Discard selected changes
- Run a commit process immediately or at a scheduled time
- View, edit, abort, cancel or roll back required processes
- View the progress and status of commit processes
- Export changes and processes to CSV

An email notification is sent when a commit process successfully completes, fails or changes are rolled back.

Note:

- Users must have the *Commit/Edit* role to perform operations in the **Change Management and Commit** window. Users with the *Edit* role can only view changes and commit processes and discard changes.
- Commit processes are executed asynchronously.

Supported Rollback Operations

The following DatAdvantage operations can be rolled back:

- Group membership changes
 - Group member added
 - Group member removed
 - Group member edited
- Permission changes (SharePoint, Exchange, CIFS and NFS)
 - Permission added
 - Permission removed
 - Permission edited
- Group created

Note:

- The rollback process can only be performed for terminated or completed commit processes that have not yet been rolled back.
- The rollback reverses changes and may not restore permissions to their original state.

Report Templates

This version also includes a new report template and filters to identify events created as a result of commit operations in DatAdvantage. For more information, see [New Reports in This Version](#) and [Changes to Filters](#).

Archiving Committed Processes

The Archive option on the Tools menu now enables administrators to archive committed processes.

Event Statistics Enhancements

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

Until this version, event statistics were stored without differentiating between event types. With this version, event statistics are now stored and displayed according to the type of event. This enhancement includes support for several new report templates, as well as a new report related to the distribution of events according to event type.

Statistics per event type are not available for events that occurred prior to the upgrade of this version.

The following reports have been added to support this enhancement:

- *Report 2.a.02, Statistics by Event Operation*
- *Report 2.a.03, Users with Failed Events*
- *Report 2.e.01, Most Active Users per Folder*
- *Report 2.e.02, Users with Most Failed Events per Folder*
- *Report 2.f.01, Event Type Distribution on File Server*
- *Report 2.f.02, Event Type Distribution per User*

In report 2a, it is now possible to view the permissions of users who performed the events displayed in the report.

DataPrivilege

DataPrivilege Migration

6.2.80

Migration is now supported for the DataPrivilege Web Application.

DataPrivilege Bulk Upload Utility

6.2.10

The Bulk Upload Utility is now supported.

DataPrivilege Support for SharePoint

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

With this version, DataPrivilege introduces broad support for on-premises SharePoint entities, including:

- Managing SharePoint site collections, protected sites and folders
- Defining SharePoint permission levels and their inheritance structure
- Managing SharePoint groups
- Configuring and managing entitlement reviews for SharePoint entities
- Ownership synchronization - Logical folder owners added through DataPrivilege are synchronized to the mapped physical folder in DataAdvantage.

Since this version of DataPrivilege is based on 5.9.22, features and functionality that were developed after that version's release are not available in 6.2.3. These features and functions will be reintroduced at a later date.

Configuration and Management

The following items are now configured and managed through the Management Console; they are not managed directly in DataPrivilege:

- Domains
- File servers

Many application settings that were available in the most recent versions of 5.9 and 6.0 are not available in 6.2.3. See [Changes to Application Settings](#).

Upgrade and Migration

- DataPrivilege cannot be upgraded to 6.2.3 at all; nor can installations that include both DataAdvantage and DataPrivilege. Only clean installation of 6.1.33 is possible for these environments.
- For a similar reason, migration is not supported at all in 6.2.3.

Bulk Upload Utility

The Bulk Upload Utility is not supported in 6.2.3.

Web Farms

Web farms are not supported in 6.2.3.

DataPrivilege API

The DataPrivilege API is not supported in 6.2.3.

Report Deployment Tool

DataPrivilege does not support the Report Deployment Tool in 6.2.3.

Changes to Application Settings

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

Many changes have been made to the DataPrivilege application settings. A number of the application settings introduced in the latest versions of 5.9 and 6.0 are not available in this version. Other settings are available under different categories, or have reverted to their original names.

Setting	Change
<i>"From" email address for email sent by Varonis</i>	Not available in this version
<i>"From" name for email sent by Varonis</i>	Not available in this version
<i>Account for processed email</i>	Not available in this version
<i>Account password for processed email</i>	Not available in this version
<i>Active Directory property used for displaying images</i>	Not available in this version
<i>Allow folder owners to edit names of new groups</i>	Not available in this version
<i>Allow owner to authorize requests pending to requestee's manager</i>	Not available in this version
<i>Default number of days from the start date to the end date in the date filter used in searches</i>	Not available in this version
<i>Default number of days from the start to end dates displayed in the Request Date filter</i>	Not available in this version
<i>Default search mode for users & groups</i>	Not available in this version
<i>Default value (IsBypassData) for created groups</i>	Moved to the File System and Active Directory category.
<i>Directory of CSV reporting created files</i>	Not available in this version

Setting	Change
<i>Enable emulation of direct permissions on folders, to groups which are members in the directly permitted groups</i>	Not available in this version
<i>Enable management authorization</i>	Moved to the File System and Active Directory category
<i>Hide all real direct permissions on folders</i>	Not available in this version
<i>Hide users, built-in groups and local computer groups with real direct permissions on folders</i>	Not available in this version
<i>Maximum number of emails to process at once</i>	Not available in this version
<i>Maximum number of rows displayed in the report. If the number of rows exceeds this value, the report is exported to a CSV file and 10 rows are displayed in the browser.</i>	Not available in this version
<i>Number of attempts to send email</i>	Not available in this version
<i>Number of emails that can be sent in bulk</i>	Not available in this version
<i>Number of FileWalk threads</i>	Not available in this version
<i>Number of users allowed in group membership requests</i>	Now called <i>A limit on the amount of users allowed in multiuser group membership requests</i>
<i>Number of users allowed in permission requests</i>	Now called <i>A limit on the amount of users allowed in multiuser permission requests</i>
<i>Port for processed email</i>	Not available in this version
<i>Protocol for processed email</i>	Not available in this version
<i>Remove folders from DataPrivilege that were not found in the last nightly synchronization</i>	Not available in this version

Setting	Change
<i>Send email for auto-approved requests</i>	Not available in this version
<i>Server for processed email</i>	Not available in this version
<i>Set default owners for unmanaged groups</i>	Not available in this version
<i>Set the membership level at which groups that are members of the directly permitted groups will be emulated with direct permissions on folders (level 1 means direct members of the directly permitted groups; groups at other levels won't be emulated with direct permissions on folders)</i>	Not available in this version
<i>Set the types of the directly permitted groups for which their members of type group be emulated with direct permissions on folders (all member group types will be emulated)</i>	Not available in this version
<i>Set whether or not the user who creates the create folder request is the authorizer of the new folder</i>	Not available in this version
<i>Show column names in tooltips on mouseover</i>	Not available in this version
<i>SMTP address</i>	Not available in this version
<i>SMTP password</i>	Not available in this version
<i>SMTP port</i>	Not available in this version
<i>SMTP user</i>	Not available in this version
<i>Support recipient's email address</i>	Not available in this version
<i>Synchronize group owners with Active Directory</i>	Not available in this version
<i>Synchronize unmonitored domains</i>	Not available in this version

Setting	Change
<i>The ADProperties column containing the manager value</i>	Moved to the File System and Active Directory category
<i>The ADProperties column to which the manager value is compared</i>	Moved to the File System and Active Directory category
<i>The height of the printed page in pixels (excluding printed reports)</i>	Now called Page size for printing (excluding reports)
<i>Use SSL encryption for email</i>	Not available in this version
<i>Use SSL for SMTP connections</i>	Not available in this version

DataPrivilege Jobs

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

For a list of new DataPrivilege jobs, see [New Jobs](#).

Data Transport Engine

Ability to Clone Rules

6.2.80

The new Clone Rule button enables you to clone Data Transport Engine rules. Cloned rules will be identical in all aspects (settings, scopes) to the original rule, except for rule name and destination.

Display of Virtual Entities

6.2.70

A new option, *Display virtual entities in Work Area prior to executing rules*, enables displaying the virtual entities to be created at the destination in the Work Area. This includes recommendations from IDU Analytics and manual user editing. Clearing this option might significantly reduce rule calculation time.

Copy of Stub Files in Mirror Rules

6.2.60

In this version, Data Transport Engine mirror rules can copy stub files that were created by regular rules. Note that mirror rules themselves do not create stub files.

Data Transport Engine Configuration Enhancements

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.

Management Console

New Jobs

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.

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

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

- *DataPrivilege Sanity Check* - Performs a sanity check on the system and displays errors in the event viewer (if any).
- *DataPrivilege Objects Maintenance* - Cancels requests for objects that are excluded.
- *DataPrivilege Incremental Synchronization* - Synchronizes existing data in DatAdvantage to DataPrivilege.
- *DataPrivilege Entitlement Review* - Creates entitlement review requests.
- *DataPrivilege Full synchronization* - Executes the following operations:
 - Enforces automatic rules for managed groups
 - Enforces automatic rules for base and managed folders
 - Resolves expired relations (groups to members)

- Sends a notification regarding expired requests
- Synchronizes the Active Directory settings that are related to users and managers
- *DataPrivilege Sync Owners* - Synchronizes owners in DatAdvantage to DataPrivilege.

In addition, the following jobs have been added to the *Synchronization* jobs category:

- *Re-run Failed Sync jobs* - Reruns all failed synchronization jobs.
- *Sync Domains* - Synchronizes the entire contents of the Domains and IDU_hosts table.
- *Sync EMC Controller* - Synchronizes only relevant contents of the EMC_Control_Station and EMC_Filer_Controller tables.
- *Sync Exchange Configuration* - Synchronizes Exchange configuration information.
- *Sync Filer* - Synchronizes relevant file server data.
- *Sync Filer Deleted* - Synchronizes the removal state of the file server and removes it from the related Probe or Collector.
- *Sync Filtered Users* - Synchronizes the entire contents of the AD_FilteredUsers table.
- *Sync Monitored Mailboxes* - Synchronizes relevant contents of the EX_MonitoredMailboxes table.
- *Sync Probe Configuration* - Synchronizes contents of the vwConf table according to command and defined configuration.
- *Sync Probe Licences* - Synchronizes all license-related information in the KeyValue table.
- *Sync Probe Proxy* - Synchronizes only relevant contents of the ProbeProxy and Filers_Proxy tables.
- *Sync Pruned Dirs* - Synchronizes the entire contents of the PrunedDirs table.
- *Sync Pruned Users* - Synchronizes the entire contents of the PrunedUsers table.
- *Sync Volumes* - Synchronizes only relevant contents of the Volumes table.

Designation of Executive Accounts

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.

Decommissioning File Servers

6.2.3

With this version, it is now possible to decommission a file server that no longer exists. When a file server is decommissioned, historical data is saved. Event collection and crawling are disabled for decommissioned file servers.

The **Set file server as decommissioned** option has been added to the **Editing file server** window of the Management Console to enable this configuration.

The following occurs when a file server is decommissioned:

- FileWalk will cease to run on the decommissioned file server. It will no longer be possible to manually run FileWalk or edit its schedule.
- No events will be collected.
- Events and statistics will continue to be archived.
- The DFS Walk and SHS FileWalk jobs will continue to run on the decommissioned file server.
- DataPrivilege and DatAdvantage (including reports) will continue to display the decommissioned file server and its historical data.
- The DCF and DatAnswers will cease to scan decommissioned servers. No new data will be indexed for DatAnswers. However, the decommissioned server's historical data will continue to be available.
- Decommissioned servers will be excluded from the DTE source and DatAlert scopes and from the calculation. No indication of this change will be displayed in the UI.
- It will be possible to edit the Probe or Collector to which the decommissioned server is connected.

New Synchronization Job

6.2.3

In this version, the *Sync SharePoint* job has been added to the *Synchronization* jobs category.

This job executes the following operations:

- Configures audit settings for on-premises SharePoint
- Designates the FileWalk user (who is granted the Office 365 Global administrator role) as the administrator for all monitored site collections

Automatic Discovery of Privileged Accounts

6.2.5

Certain types of users, such as administrators, service and testing accounts, typically behave differently than regular end users. In this version, the Management Console enables automatic discovery of these *privileged* accounts, so that DatAlert rules can be tailored to exclude them if preferred.

Automatic discovery of privileged accounts is only available with a DatAlert license; privileged accounts can be added manually with a regular DatAdvantage license.

Configuring Folder Suggestions for DatAnswers

6.2.3

With this version, the Management Console enables selecting whether suggestions are displayed in the menu under the My Folders search box while typing the name or path of a folder. The *Show suggestions in My Folders search box menu* option has been added to the Display Layout Attributes area of the Page Layout tab to support this configuration. By default, this option is selected.

Adding Azure Active Directory Domains

6.2.3

With this version, the Management Console enables adding and editing Azure Active Directory domains (tenants) from the **Domains** pane.

Important: The IDU Server must reside on Windows Server 2008 R2 or above in order to add this domain type.

Adding Exchange and SharePoint Online File Servers

6.2.3

In this version, the Management Console enables adding Exchange Online and SharePoint Online file servers from the File Server wizard.

For SharePoint Online, the Sites tab of the wizard now enables selecting site collections, public sites as well as OneDrive for Business personal sites.

Important: The Probe or Collector connected to Online file server must reside on Windows Server 2008 R2 or above.

Archive Policy Enhancements

6.2.3

With this version, it is now possible to configure the lifetime of changes and committed processes before they are archived or deleted. The Pending Changes and Commit area has been added to the Archive Policy tab to enable this option.

DatAdvantage Security Enhancements

6.2.3

The Management Console now enables storing the credentials used for the commit process so that they do not need to be entered again during the commit. The Commit Credentials area has been added to the DatAdvantage Security tab to enable this option.

Selecting this option saves the credentials for each commit operator.

Viewing Failed Synchronizations

6.2.3

With this version, the Management Console now enables viewing failed synchronizations. The Failed Syncs tab displays a list of failed synchronization jobs, the date and time at which the job last ran, as well as the target server and component. Until they successfully complete their run, the jobs listed in the grid are automatically rerun every hour. It is also possible to rerun a specific Synchronization job manually.

Synchronization jobs are responsible for synchronizing configuration information from the IDU Server to the Probes or Collectors with a local database (LocalDB).

The *Synchronization* jobs category has been added to **All Jobs** pane to support this enhancement. For a list of jobs included in the *Synchronization* category, see [New Jobs](#).

Installing LocalDB on Collectors

6.2.3

With this version, it is now possible to install a local database (LocalDB) on a Collector. To support this enhancement, the *Use LocalDB on this Collector (advanced)* option is now available when adding a new Collector through the Management Console or the Enterprise Installer.

Note: This option is only available if advanced features have been enabled.

By default, this option is selected. If this option is cleared, the LocalDB is not installed on the Collector. Existing Collectors are reconfigured by the Installer so that they use the LocalDB.

This option is only available if the relevant advanced configuration setting is enabled. Contact Varonis Support for more information.

Note: Collectors installed on Windows Server 2003 to 2008 are configured so that the configuration data is stored in memory. Collectors installed on Windows Server 2008 R2 and above are configured to use Microsoft's LocalDB feature.

Notification of File Server Upgrade Failure

6.2.3

This version introduces a notification mechanism that continually reminds users to address file server upgrade failures, to ensure all file servers are properly handled during Metadata Framework upgrade. The mechanism provides a popup notice in the Management Console at a configurable interval, requiring users to resolve upgrade errors.

Ability to Repair File Servers from Main Screen

6.2.3

In this version, a **Repair** button has been added to the Resource toolbar on the main File Server tab of the Management Console. This button enables easy repair of selected file servers.

Editing DatAnswers Management Components

6.2.3

With this version, the Management Console enables editing DatAnswers data sync shares and web servers from the DatAnswers General tab of the Management menu. Additionally, it is now possible to edit DatAnswers, API and SOLR Admin access accounts from the DatAnswers Accounts tab of the Management menu.

DCF

New Predefined Rule for DCF

6.2.60

This version provides a new predefined rule for the DCF. The rule, *Security Certificate File Types*, detects security certificate files with the following extensions:

- cer
- crt
- der
- pfx
- pem
- key
- p7b
- p7c
- p12

Enhancements to Patterns and Regular Expressions

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]

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

This version introduces a number of enhancements to DCF patterns:

- The **New Pattern** and **Edit Pattern** dialog boxes now include tabs for defining general parameters, keywords and terms to be excluded from the pattern. Because they can now be configured in the UI, these parameters are no longer predefined in regular expressions for predefined patterns. (Negative lookahead characters cannot be configured by users). Following upgrade, all existing rules that use predefined patterns will be rescanned.
- A new column, *Country*, has been added to the Pattern Repository window, to enable filtering available and selected patterns by country.

- Save and Refresh
 - Changes to patterns are now saved when the **Save** button in the **New Pattern** or **Edit Pattern** dialog box is clicked.
 - Patterns that are added from the Repository dialog box are saved when the **OK** button in that dialog box is clicked.
 - Accordingly, the **Save** and **Refresh** buttons have been removed from the Patterns tab.
- The following pattern has been added:
 - *UK Vehicle Registration Number*
- The following pattern has been removed:
 - *UK Electoral Roll Number*

Thresholds for DCF Rules and Regular Expressions

6.2.3

This version introduces various thresholds to predefined rules, to reduce the number of false positives (rules will be rescanned during upgrade):

- The *Sarbanes-Oxley* rule has been restored to the DCF, no longer returning a large number of false positives. In addition, the following change has been made to this rule:
 - For the following, at least five different matches are now required for each dictionary:
 - *SEC filing terms*
 - *Financial reporting*
 - *Stock analysis and terms*
- *HIPAA PHI Data - US* - For each of the following, at least five different matches are required for each dictionary:
 - *Proprietary drug names*
 - *Medical conditions*
 - *Medical procedures*
- *PCI Data Security Standards (PCI-DSS) -Strict* - At least five credit card numbers must exist in the document for this rule to be detected.
- The following pattern has been added:
 - *Korean Resident Registration Number*

The following changes have been made to rule configuration when creating a new rule:

- The *Minimum number of hits required* option has been added to the **New Rule** dialog box to enable selecting the minimum number of hits required in order for the rule to be a match.
- The *Hit Count* option on the File Scope toolbar has been replaced by an **Advanced** link to the right of each condition. When selected, the new **Advanced Condition Settings** dialog box enables setting the following advanced settings for each condition:
 - *Minimum no. of matches* - Enables setting the minimum number of matches to the condition.
 - *Matches must be distinct* - Enables selecting whether matches to the condition must be distinct.
 - *Hit count configuration* - Determines how matches to the condition are calculated in the total hit count.

Use of Dictionaries to Find File Names

6.2.3

The *File names (dictionary)* condition has been added to the File Scope area, which enables defining more than one file name to search.

Defining Negative Keywords for Patterns

With this version, it is now possible to designate negative keywords that must *not* be found within the specified proximity to a potential match in order for that match to be valid.

For example, if a regular expression searches for 9-digit numbers, along with the negative keyword *Phone*:

- "123456789" is a valid match
- "My phone number is 123456789" is *not* a valid match

The Negative Keywords area has been added to the **New Pattern** dialog box to enable this option.

DCF Support for SharePoint Online

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

The Varonis Data Classification Framework (DCF) now supports SharePoint Online items, such as document libraries, sites, items, and lists. DatAdvantage enables viewing the items which have the most exposed permissions and contain the most sensitive data.

Upgrading Predefined DCF Content

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

With this version, it is possible to set how the upgrade process handles existing results of prior DCF scans when predefined DCF content is upgraded. During the upgrade process, a page is displayed that includes the following options:

- *Delete all existing results for these rules and patterns and rescan using the most updated version* - This option deletes all existing results and rescan all rule scopes.
- *Keep existing results and scan only new or modified files with the updated version* - This option uses the upgraded rules to scan only new or modified files. Existing results are retained. If this option is selected:
 - Files that have already been scanned by a rule are not rescanned with the new version of the rule unless the files are modified.
 - There is no way to know whether a file was scanned by the old or the new version of the rule.

- The only way to rescan all files with the new rule is to disable and then enable the rule. This action deletes existing results.
- These caveats apply to both predefined rules and user-defined rules that contain predefined patterns.

The page appears during upgrade from any of the following versions:

- 5.8.81
- 5.9.63
- 5.9.72
- 6.0.52
- 6.0.60
- 6.0.82

It may appear in different locations in the upgrade flow, depending on the initial version.

DCF Support for Unix

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

With this version, the DCF supports Unix out of the box; that is, without the installation of Samba.

Important: During upgrade to this version (or higher versions supporting DCF for Unix), the Unix agent must also be upgraded.

The following restrictions and limitations apply:

- The DCF supports file servers that support NFS3 (including NetApp and Celerra).
- Only files having extensions can be scanned by DCF, just as with Windows.
- Hard file links are not distinguished. Each such link is processed as a distinct file.
- Unix extended file properties are not supported.
- Classification analysis is not supported.

The *Open Access* priority factor is supported for Unix and prioritizes all files with permissions for Other.

Multiple RSA Connections

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

In this version, multiple RSA connections can be defined in the database. However, they cannot be displayed or edited in the UI.

DatAlert

Changes to Threat Models

6.2.70

The following threat models are new in this version:

- Ransomware
 - *File encrypted by ransomware* - A file with a known encrypted ransomware extension was created or renamed.
 - *Past ransomware activity indicated by a residual ransomware note* - A file with a known crypto tool or ransom note file name was accessed.
 - *Potential past ransomware activity indicated by a suspected a residual ransomware note* - Multiple files with a suspected crypto tool or ransom note file name were accessed.
 - *Suspected crypto intrusion activity* - Multiple files were created with, opened or renamed to a suspected crypto tool or ransom note file name.
- Tools
 - *Exploitation software created or modified* - A file commonly associated with exploitation software was created or modified.
 - *Abnormal service behavior: a dormant service account was reactivated* - A service account became active again after being dormant for a long period of time compared to its previous behavior.
 - *Operation on an exploitation tool failed* - An attempt to create, modify or access a file commonly associated with exploitation software failed.
 - *Operation on a penetration testing or hacking tool failed* - An attempt to create, modify or access a file commonly associated with a tool used by penetration testers or hackers failed.
 - *Operation on a security tool failed* - An attempt to create, modify or access a file commonly associated with a tool used by security professionals failed.
 - *Operation on a system administration tool failed* - An attempt to create, modify or access a file commonly associated with a system administration tool failed.
 - *Penetration testing and hacking tools accessed* - A file commonly associated with a tool used by penetration testers or hackers was accessed.
 - *Penetration testing and hacking tools created or modified* - A file commonly associated with a tool used by penetration testers or hackers was created or modified.
 - *Security tools accessed* - A file commonly associated with a tool used by security professionals was accessed.
 - *Security tools created or modified* - A file commonly associated with a tool used by security professionals was created or modified.
 - *System administration tools accessed* - A file commonly associated with a system administration tool was accessed.
 - *System administration tools created or modified* - A file commonly associated with a system administration tool was created or modified.

The following changes have been made to threat models:

- *Crypto intrusion activity*
 - New category - Denial of Service
 - New severity level - 0 - Emergency
- *Encryption of multiple files*
 - New severity level - 1 - Alert
- *Recon tools detected*
 - New severity level - 4 - Warning
- *Suspicious mailbox activity: multiple messages marked as unread by user other than the mailbox owner*
 - New name - *Abnormal behavior: unusual number of messages marked as unread by a user other than the mailbox owner*
- *Exploitation tools detected*
 - New name - *Exploitation software accessed*
 - New severity level - 1 - Alert

The following threat models have been removed:

- *Multiple open events on files likely to contain credentials*

New DatAlert Analytics Threat Model

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 Web Interface

6.2.35

With this version, Varonis introduces the DatAlert web interface, which enables monitoring and analyzing the various alerts generated by DatAlert and DatAlert Analytics.

The web interface enables viewing the status of all alerts in an organization through different views.

In addition, the following tasks can be performed with the DatAlert web interface:

- View the top alerted users, assets and threat models
- Search for alerts and alerted events using advanced search capabilities
- View a graphical or tabular display of all alerts and alerted events for the selected time period
- View context cards of entities, categories and specific days throughout the user interface
- View a kill chain analysis of the alerts matching the defined search criteria
- Switch between different views of the same data

DatAlert's web interface is comprised of the following options:

- *Dashboard* - Displays a stacked bar chart illustrating the dispersion of alerts over the specified timeframe. This pane also presents the top five alerted users, assets and threat models as well as a kill chain analysis.
- *Alerts* - An "in depth" view of the alert data in tabular form.
- *Alerted Events* - A bar chart illustrating the dispersion of alerted events over the specified timeframe. This pane also displays the event information in the form of a table.

Context cards are presented throughout the DatAlert web interface as a means to provide detailed information about a specific entity, category or day on which alerts were generated. It provides a quick and easy way to drill down and view the alert information.

Context cards can be opened for the following entities:

- *Users*
- *Assets*
- *Threat models*
- *Category*
- *Day*

DatAlert Integration with Security Management Systems

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](#).

Predefined DatAlert Rules

6.2.35

The names of the following predefined rules and threat models were changed in this version:

- *Abnormal behavior: access to sensitive data* was renamed to *Abnormal behavior: unusual amount of access to sensitive data*
- *Abnormal behavior: unusual amount of access to stale data* was renamed to *Abnormal behavior: unusual amount of access to idle data*
- *Abnormal behavior: unusual amount of activity on script files* was renamed to *Abnormal behavior: unusual amount of script file creations*

The following predefined rules and threat models were added in this version:

Rule Name	Description	Category	Severity	Rule Type	Product
Abnormal admin behavior: unusual amount of lockouts across admin accounts	May indicate misconfiguration, a brute-force attempt to exploit admin privileges, or a denial-of-service attack. Admin account's lockout events are compared to a behavioral profile for all admin accounts, and an alert is created when a deviation is discovered	Lateral movement	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: accumulative create and delete actions resemble ransomware	User create and delete actions over time may indicate that a ransomware attack is underway	Denial of service	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: accumulative increase in access to idle data	May indicate a gradual scan of or attempt to gain access to data assets. User's actions over time are compared to his behavioral profile and an alert is created when an increase is discovered	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics

Rule Name	Description	Category	Severity	Rule Type	Product
Abnormal behavior: accumulative increase in access to sensitive data	This may indicate a gradual scan of or attempt to gain access to sensitive data. User's actions over time are compared to his behavioral profile and an alert is created when an increase is discovered.	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: accumulative increase in lockouts across end-user accounts	May indicate misconfiguration, a brute-force attempt to gain access to accounts, or a denial-of-service attack. End-user account's lock-out events over time are compared to a behavioral profile for all end-user accounts, and an alert is created when an unusual increase is discovered.	Lateral movement	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: accumulative increase of lockouts for individual end-user accounts	May indicate an attempt to gain access to the user's account using brute-force, or a denial-of-service attack. End-user account's lockout events are compared to his behavioral profiles and an alert is created when an increase is discovered.	Lateral movement	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: accumulative user rename and modify actions resemble ransomware	User rename and modify actions over time may indicate that a ransomware attack is underway	Denial of service	1 - Alert	DatAlert Analytics	DatAlert Analytics

Rule Name	Description	Category	Severity	Rule Type	Product
Abnormal behavior: unusual amounts of lockout across end-user accounts	May indicate misconfiguration, a brute-force attempt to gain access to accounts, or a denial-of-service attack. End-user accounts lockout events are compared to a behavioral profile for all end-users accounts, and an alert is created when a deviation is discovered	Lateral movement	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: unusual number of file deletions	May indicate an unauthorized attempt to damage or destroy data assets, or a denial of service attack. The user's delete actions are compared to his behavioral profile and an alert is generated when a deviation is discovered.	Denial of service	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: unusual number of sensitive file deletions	May indicate an unauthorized attempt to damage or destroy sensitive data assets, or a denial of service attack. The user's delete actions are compared to his behavioral profile and an alert is generated when a deviation is discovered	Denial of service	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: user create and delete actions resemble ransomware	User create and delete actions may indicate that a ransomware attack is underway	Denial of service	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: user rename and modify actions resemble ransomware	User rename and modify actions may indicate that a ransomware attack is underway.	Denial of service	1 - Alert	DatAlert Analytics	DatAlert Analytics

Rule Name	Description	Category	Severity	Rule Type	Product
Abnormal executive behavior: accumulative increase in access-denied events across executive accounts	May indicate an unauthorized attempt to gain access to data assets using executive accounts. Executive accounts access-denied events over time are compared to the behavioral profile of all executive accounts, and an alert is created when an increase is discovered.	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal executive behavior: accumulative increase in access to script, configuration and backup files across executive accounts	May indicate an unauthorized attempt to extract credentials using executive accounts. Executive accounts events over time are compared to the behavioral profile of all executive accounts, and an alert is created when an increase is discovered.	Privilege escalation	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal executive behavior: unusual amounts of access-denied events across executive accounts	May indicate an unauthorized attempt to gain access to data assets using executive accounts. Executive accounts access-denied events are compared to the behavioral profile of all executive accounts and an alert is created when a deviation is discovered.	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal executive behavior: unusual amounts of access to script, configuration and backup files across executive accounts	May indicate an unauthorized attempt to extract credentials using executive accounts. Executive accounts events are compared to the behavioral profile of all executive accounts and an alert is created when a deviation is discovered.	Privilege escalation	1 - Alert	DatAlert Analytics	DatAlert Analytics

Rule Name	Description	Category	Severity	Rule Type	Product
Abnormal service behavior: accumulative increase in lockouts across service accounts	May indicate an attempt to exploit service privileges using brute-force, or a denial-of-service attack. Service account's lockout events over time are compared to a behavioral profile for all service accounts, and an alert is created when an increase is discovered.	Lateral movement	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal service behavior: accumulative increase in lockouts for individual service accounts	May indicate an attempt to exploit service privileges using brute-force, or a denial-of-service attack. Service account's lockout events over time are compared to a behavioral profile for all service accounts, and an alert is created when an increase is discovered	Lateral movement	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal service behavior: unusual amounts of lockouts across service accounts	May indicate misconfiguration, a brute-force attempt to exploit service privileges, or a denial-of-service attack. Service account's lockout events are compared to the service account's behavioral profile and an alert is created when a deviation is discovered.	Lateral movement	1 - Alert	DatAlert Analytics	DatAlert Analytics
Executive account locked-out/ disabled/deleted/password reset	May indicate a misconfigured account	Other	5 - Notice	Standard	DatAlert Analytics

Rule Name	Description	Category	Severity	Rule Type	Product
Membership Changes: Service Accounts	May indicate a misconfiguration or unauthorized attempt to damage the infrastructure and deny users access to systems, especially if performed outside of established change control processes.	Privilege escalation	4 - Warning	Standard	DatAlert
Modification: Critical Organizational Units	May indicate unauthorized attempts to gain access by changing policies, or using privileged groups. May also indicate attempts to deny users access to systems, especially if performed without regard for established change control processes.	Privilege escalation	4 - Warning	Standard	DatAlert
Modification: GPO Security Settings	May indicate a misconfiguration or unauthorized attempt to gain access to data or system by changing policies. May also indicate attempts to deny users access to systems, especially if performed without regard for established change control processes.	Privilege escalation	4 - Warning	Standard	DatAlert
Permission changes on OU	May indicate a misconfiguration or unauthorized attempt to gain access to data by granting broad access. May also indicate attempts to deny users access to systems, especially if performed without regard for established change control processes.	Privilege escalation	4 - Warning	Standard	DatAlert
Permissions granted directly to user in directory services	May indicate a misconfiguration or unauthorized attempt to gain access to data	Privilege escalation	4 - Warning	Standard	DatAlert

Rule Name	Description	Category	Severity	Rule Type	Product
Permissions granted directly to user in windows file system	May indicate a misconfiguration or unauthorized attempt to gain access to data	Privilege escalation	4 - Warning	Standard	DatAlert
Suspicious access activity: service account access to file containing credentials	May indicate unauthorized attempt of access or modify/etc/passwd	Exploitation	4 - Warning	Standard	DatAlert Analytics

6.2.5

The following table lists predefined rules for DatAlert. These rules can be run as is, with no additional configuration needed.

There are three types of rules:

- Standard rules - Rules designed to send real-time notification that a particular event has occurred, or a particular user or computer account has performed a certain action.
- Threshold rules - Rules designed to send notification that a large number of events has occurred, if the configured threshold of events has been exceeded.
- DatAlert Analytics rules - Rules designed to send notification that user behavior is atypical, in comparison to the user's behavioral profile. DatAlert Analytics rules send alerts once a day, not in real-time as with standard or threshold rules. Moreover, user data must be gathered for several months (at least three) to build an effective behavioral profile on which to base alerts.

Rules are displayed according to the existing license. For example, if only a DatAlert license exists, only DatAlert rules are displayed. If both DatAlert Analytics and DatAlert licenses exist, rules for DatAlert and DatAlert Analytics are displayed.

Note: For more information, see the [DatAlert Analytics Overview](#) on Varonis Connect.

Rule Name	Description	Category	Severity	Rule Type	Product
Abnormal admin behavior: access to atypical mailboxes	May indicate unauthorized attempt to exploit admin privileges to gain access to data assets. The user's actions are compared to his behavioral profile and an alert is created when a deviation is discovered.	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: access to sensitive data	May indicate an unusual amount of unauthorized attempts to gain access to sensitive data assets. The user's actions are compared to his behavioral profile and an alert is created when a deviation is discovered.	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: unusual amount of access-denied events	May indicate an unauthorized attempt to gain access to data assets. The user's actions are compared to his behavioral profile and an alert is created when a deviation is discovered.	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: unusual amount of access to configuration and backup files	May indicate an unauthorized attempt to extract credentials. The user's actions are compared to his behavioral profile and an alert is created when a deviation is discovered.	Privilege escalation	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: unusual amount of access to stale data	May indicate an unauthorized attempt to gain access to data assets. The user's actions are compared to his behavioral profile and an alert is created when a deviation is discovered.	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics

Rule Name	Description	Category	Severity	Rule Type	Product
Abnormal behavior: unusual amount of access to system files	May indicate an unauthorized attempt to extract credentials. The user's actions are compared to his behavioral profile and an alert is created when a deviation is discovered.	Privilege escalation	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal behavior: unusual amount of activity on script files	May indicate an unauthorized attempt to gain access to data assets. The user's script file creation actions are compared to his behavioral profile and an alert is created when a deviation is discovered.	Exploitation	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal service behavior: access to atypical files	May indicate unauthorized attempt to exploit service privileges to gain access to data assets. The user's actions are compared to his behavioral profile and an alert is created when a deviation is discovered.	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal service behavior: access to atypical folders	May indicate unauthorized attempt to exploit service privileges to gain access to data assets. The user's actions are compared to his behavioral profile and an alert is created when a deviation is discovered.	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics
Abnormal service behavior: access to atypical mailboxes	May indicate unauthorized attempt to exploit service privileges to gain access to data assets. The user's actions are compared to his behavioral profile and an alert is created when a deviation is discovered.	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics

Rule Name	Description	Category	Severity	Rule Type	Product
Abnormal service behavior: atypical failure to access data	May indicate unauthorized attempt to exploit service privileges to gain access to data assets. The user's actions are compared to his behavioral profile and an alert is created when a deviation is discovered.	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics
Administrative or service account disabled, deleted, or reset	May indicate unauthorized attempt to damage the infrastructure, deny users access to systems, or to obfuscate, especially if performed outside of established change control processes	Exploitation	1 - Alert	Standard	DatAlert Analytics
Crypto intrusion activity	May indicate presence of ransomware	Intrusion	1 - Alert	Standard	DatAlert
Deletion: Active Directory containers, Foreign Security Principal, or GPO	May indicate unauthorized attempt to damage or destroy operational forest structure, denying users access to systems	Denial of service	1 - Alert	Standard	DatAlert
Deletion: Multiple directory service objects	May indicate unauthorized attempt to damage or destroy operational forest structure, denying users access to systems	Denial of service	0 - Emergency	Threshold	DatAlert
Encryption of multiple files	May indicate a ransomware attack underway	Denial of service	0 - Emergency	Threshold	DatAlert
Exploitation tools detected	May indicate attempt to install or use known hacking tools	Exploitation	1 - Alert	Standard	DatAlert

Rule Name	Description	Category	Severity	Rule Type	Product
Lockout: Multiple accounts locked-out	May indicate misconfiguration, brute force attempt to gain access or denial of service attack	Lateral movement	0 - Emergency	Threshold	DatAlert
Membership changes: admin groups	May indicate unauthorized attempt to gain access via privileged groups or prevent administrators from responding to the attack, especially if performed outside of established change control processes	Exploitation	1 - Alert	Standard	DatAlert Analytics
Modification: Critical GPOs	May indicate unauthorized attempts to gain access by changing policies, or using privileged groups. May also indicate attempts to deny users access to systems, especially if performed without regard for established change control processes	Exploitation	4 - Warning	Standard	DatAlert
Modification: Hosts file	May indicate unauthorized attempt to redirect data out of the organization to attackers' servers, especially if performed without regard for established change control processes	Exfiltration	1 - Alert	Standard	DatAlert
Multiple open events on files likely to contain credentials	May indicate unauthorized attempt to extract credentials	Privilege escalation	1 - Alert	Threshold	DatAlert
Permission changes: global access groups added/removed	May indicate a misconfiguration or unauthorized attempt to gain access to data by granting broad access	Privilege escalation	3 - Error	Standard	DatAlert

Rule Name	Description	Category	Severity	Rule Type	Product
Potential masked intrusion: system binaries found in unusual locations	It is unusual for system binaries to appear in non-system directories. Malware often masks itself by using common services in uncommon locations, to seem as innocuous as possible	Intrusion	1 - Alert	Standard	DatAlert
Recon tools detected	May indicate unauthorized presence of reconnaissance tools that could be used to scan the corporate network or to search for vulnerabilities	Reconnaissance	1 - Alert	Standard	DatAlert
Security certificate activity by non-administrators	May indicate unauthorized attempt to access or modify the security certificates of various systems in the organization	Exploitation	1 - Alert	Standard	DatAlert Analytics
Suspicious access activity: non-admin access to files containing credentials	May indicate an unauthorized attempt to extract credentials, or deny access to systems	Privilege escalation	1 - Alert	Standard	DatAlert Analytics
Suspicious access activity: non-admin access to startup files and scripts	May indicate an unauthorized attempt to install or tamper with software, extract credentials or deny access to systems	Privilege escalation	1 - Alert	Standard	DatAlert Analytics
Suspicious mailbox activity: multiple messages marked as unread by user other than the mailbox owner	May indicate unauthorized mail access, exfiltration, and obfuscation.	Exfiltration	1 - Alert	DatAlert Analytics	DatAlert Analytics

DatAlert Scope Configuration Enhancements

6.2.35

With this version, the following enhancements have been made to the DatAlert scope configuration:

- The **Who (Acting Object)**, **Where (Affected Object)**, **What (Event Details)** and **When (Event Time)** pages of the **Add Rule** window now enable adding filters to define scopes for predefined DatAlert rules. Filters can be added to define alerts on specific objects or to exclude entities from the rule scope. For example, it is now possible to configure rules that generate alerts on a single user only or users with a red flag on a specific rule.

Note: This option is only available for DatAlert standard and threshold rules. It is not possible to add filters to define scopes for DatAlert Analytics rules.

- This version now supports importing filters to be applied to a rule on an affected object. Alternatively, it is possible to export the current list of filters to a CSV file. Only user-defined filters will be exported. The *Import/Export Filter* option has been added to the Advanced Search toolbar of the **Where (Affected Object)** page to support this configuration.

In addition, the following changes have been made to support the new configuration options:

- Entities can now be excluded from a rule scope by using the available filters. The Excluded Affected Objects area in the **Where (Affected Object)** page and the Excluded Acting Objects area in the **Who (Acting Object)** page have been removed to enable this change.
- It is only possible to bulk edit information that is common to all selected rules.
- Exclusion scopes can be defined for DatAlert Analytics rules only.
- It is no longer possible to configure global conditions, or exclusion scopes, for both affected objects and acting objects. The Exclusion Scopes tab in the left pane of the **DatAlert** window has been removed.
- The following audit event types are no longer available:
 - *DatAlert global exclusion scope created*
 - *DatAlert global exclusion scope deleted*
 - *DatAlert global exclusion scope edited*

This version supports the upgrade of exclusion scopes (that is, scopes configured prior to this version) to a new scope. For more information, see [DatAlert Exclusion Scope Upgrade](#).

Executable Script Enhancements for DatAlert Rules

6.2.35

This version enables running a custom or built-in executable script for each DatAlert rule.

To support this enhancement, the Executable Script area has been moved from the Configuration tab of the **DatAlerts** window to the **Alert Method** page of the **Add Rule** window. The Executable Script area enables defining script settings.

Placeholders can now be applied as environment variables in executable scripts. For a list of supported placeholders, see the *DatAlert User Guide*. It is possible to select an executable script without defining a template for it.

DatAlert Analytics License

6.2.15

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.

The DatAlert Analytics license includes the following:

- Auto-detection of privileged accounts
- The following canned rules:
 - All rules with the *User behavior analysis* type
 - Administrative or service account disabled or deleted
 - Membership changes to administrative groups
 - Security certificate activity by non-administrators
 - Suspicious access activity: non-admin access to files containing credentials
 - Suspicious access activity: non-admin access to startup files and scripts
 - Service account access to credentials stored in files

Exclusion Filters

6.2.5

DatAlert now provides filters that enable *excluding* entities from a rule scope. Such *exclusion* filters can be useful in designing alerts that exclude items of low interest, such as cookies and temporary files and folders. Alerts to address other issues can be designed as needed. See [Changes to Filters](#) for a list of the filters that have been added to support this feature.

DatAlert Email in Plain Text

6.2.3

Starting with this version, all DatAlert mail has two parts - HTML and plain text. The mail client of the customer processes the mail in the supported format. This applies to regular mail, threshold mail and aggregated mail.

HP ArcSight Alert Template

6.2.35

The HP ArcSight template now uses `<Event Type ID>` in the header instead of `<rule id>`.

6.2.3

In this version, DatAlert includes a predefined alert template that complies with the CEF format, to enable sending DatAlerts to HP ArcSight via Syslog. The template is read-only.

DatAlert Support for Exchange Admin Events

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

With this version, DatAlert provides support for Exchange admin events. The following events are supported:

- Mailbox permission added
- Mailbox permission removed
- Public folder administrative permission added
- Public folder administrative permission removed

DatAlert Support for Directory Service Object Creation Events

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

DatAlert now provides support for all directory service object creation events, including custom types. Support is provided as follows:

- The *Event type* filter includes a value of *DS object created*.
- *Directory name* filter:
 - If it is used with the *Search in child objects* option, a DatAlert is sent for any object created either directly or indirectly under the specified folder.
 - If it is used without the *Search in child objects* option, a DatAlert is sent for any object created directly in the specified folder.

Reports

Changes to Filters

6.2.71

New Filters

The following filters have 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.

6.2.35**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
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.

Filter Name	Description
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.

6.2.5

New Filters

The following filters have been added in this version:

Filter Name	Description
Acting privileged accounts	Filters according to the specified type of privileged account.
Affected privileged accounts	Filters according to the specified type of privileged account.
Included access paths	A compound filter which includes all specified access paths for the selected resource types. Comprised of the following filters: • Directory Services access paths • EMC access paths • Exchange access paths • Hitachi NAS access paths • HP NAS access paths • NetApp access paths • SharePoint access paths • Unix access paths • Unix SMB access paths • Windows access paths

Filter Name	Description
Excluded access paths	A compound filter which excludes all specified access paths for the selected resource types. Comprised of the following filters: • Directory Services access paths • EMC access paths • Exchange access paths • Hitachi NAS access paths • HP NAS access paths • NetApp access paths • SharePoint access paths • Unix access paths • Unix SMB access paths • Windows access paths
Directory Services 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 directory service file servers.
EMC 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 directory service file servers.
Exchange 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 directory service file servers.
Hitachi NAS 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 directory service file servers.
HP NAS 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 directory service file servers.
NetApp 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 directory service file servers.

Filter Name	Description
SharePoint 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 directory service file servers.
Unix 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 directory service file servers.
Unix SMB 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 directory service file servers.
Windows 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 directory service file servers.

Changes to Existing Filters

- The inner filters of the *File properties* compound filter have been changed. They are now:
 - File name and extension*
 - Excluded file name and extension*
 Both these filters permit adding a list of values (semicolon-separated).
- The *Affected object path* filter is now available in report 6b, under *Affected objects > Directory objects*.

6.2.3

New Filters

The following filters have been added in this version:

Filter Name	Description
% change in hit count (selected rule)	Filters according to the percentage change in the specified number of hits on the selected rule.
% change in hit count on files with open access (selected rule)	Filters according to the percentage change in the specified number of hits on files with open access for the selected rule. Calculated according to the method defined in the Change percent calculation method filter.

Filter Name	Description
% change in no. of files with hits (selected rule)	Filters according to the percentage change in the specified number of files with hits on the selected rule.
% change in no. of files with hits and open access (selected rule)	Filters according to the percentage change in the specified number of files with hits and open access for the selected rule. Calculated according to the method defined in the Change percent calculation method filter.
% change in no. of folders with hits (selected rule)	Filters according to the percentage change in the specified number of folders that directly contain files with hits on the selected rule.
% change in no. of folders with hits and open access (selected rule)	Filters according to the percentage change in the specified number of folders with open access that directly contain files with hits on the selected rule. Calculated according to the method defined in the Change percent calculation method filter.
% change in size of files with hits and open access (selected rule)	Filters according to the percentage change in the specified size of files with hits and open access for the selected rule. Calculated according to the method defined in the Change percent calculation method filter.
% change in size of all hits (GB) – selected rule	Filters according to the percentage change in the specified size of all files (in GB) with hits for the selected rule.
Display assigned owner	Filters to display the names of owners assigned to the object in DatAdvantage (i.e., the "Varonis owner").
Elevated mode	Filters according to searches that were run in one of the following elevated modes: • <i>Run as a different user</i> • <i>Show unfiltered results</i>
Elevated user	Filters according to the user that was impersonated while running a search as a different user in DatAnswers.
Elevated user's domain	Filters according to the domain of the user that was impersonated while running a search as a different user in DatAnswers.
Hit count (selected rule)	Filters according to the total hit count on the selected rule.

Filter Name	Description
Hit count on files with open access (selected rule)	For the selected rule, this filter returns the total number of hits on files with open access. If the <i>Filter by percentage</i> option is selected, the value entered must be between 0 and 100.
Hit count on files with open access (selected rules)	Part of the Classification results compound filter. For the selected rules, this filter returns the total number of hits on files with open access.
Mail-enabled	Indicates whether the Microsoft Exchange object is mail-enabled.
No. of files with hits (selected rule)	Filters according to the number of files with hits on the selected rule.
No. of files with hits and open access (selected rule)	Filters according to the number of files with hits and open access for the selected rule. If the <i>Filter by percentage</i> option is selected, the value entered must be between 0 and 100.
No. of files with hits and open access (selected rules)	Part of the Classification results compound filter. For the selected rules, this filter returns the number of files with hits and open access.
No. of folders with hits (selected rule)	Filters according to the number of folders that directly contain files with hits on the selected rule.
No. of folders with hits and open access (selected rule)	Filters according to the number of folders with open access that directly contain files with hits on the selected rule. If the <i>Filter by percentage</i> option is selected, the value entered must be between 0 and 100.
Public folder type	Filters according to the public folder class
Size of all hits (GB) – selected rule	Filters according to the specified size of all files (in GB) with hits for the selected rule.
Size of files with hits and open access (selected rule)	Filters according to the specified size of files with hits and open access for the selected rule. If the <i>Filter by percentage</i> option is selected, the value entered must be between 0 and 100.
Show group members in sub report	When this filter is used, an additional sub-report is generated that displays direct and indirect members of groups that appear in the original report. Users having direct permissions (i.e., not through a group) are not displayed in the sub-report.

Changes to Existing Filters

- The *Email* filter is now available under the *Exchange objects* filter category.

The following changes are now available, integrated from 6.1.33:

- The *Interval* filter is now part of both the *Trend Interval* and *Date/time interval* compound filters.
- The following filters are now part of both the *Permission changes (Windows)* and *Permission changes (Directory Services)* compound filters:
 - *Changed permission*
 - *Permission after change*
 - *Permission before change*
 - *Permission type*
 - *Trustee*
 - *Trustee account type*
- The *Show data from* filter can now retrieve *History of differences - commit only* events. This filter enables users to quickly and easily find events on commit actions performed in DatAdvantage.
- The *Permission changes for global access groups only* filter now supports Directory Service permission events.
- The FS property date filters now include *Before* and *After* operators.

Integrated from 6.1.33

The following filters are now available, integrated from 6.1.33:

Filter Name	Description
Azure blockCredential	Filters according to whether or not the user can log on to Azure Active Directory using the user ID. This is an Azure AD property.
Azure isBlackberryUser	Filters according to whether or not the user has a BlackBerry device. This is an Azure AD property.
Azure isLicensed	Filters according to whether or not the user has licenses assigned. This is an Azure AD property.
Azure isSystem	Filters according to the <i>Azure isSystem</i> Azure AD property.
Azure lastDirSyncTime	Filters according to the <i>Azure lastDirSyncTime</i> Azure AD property, which indicates the date and time of the last directory synchronization (returned from users synced through Active Directory Domain Services synchronization).
Azure liveld	Filters according to the <i>Azure liveld</i> Azure AD property, which is the user's unique login ID.

Filter Name	Description
Azure ObjectID	Filters according to the <i>Azure ObjectID</i> Azure AD property, which is the user's unique ID.
Azure passwordResetNotRequired	Filters according to whether or not a password must be reset when activated.
Azure preferredLanguage	Filters according to the <i>Azure preferredLanguage</i> Azure AD property, which is the user's preferred language.
Azure userType	Filters according to the <i>Azure userType</i> Azure AD property, which is the type of user.
Changed GPO settings	Compound filter that returns changes made to GPO settings. Includes the following filter: • GPO setting name
Commit process ID	Filters according to ID of the commit process, which includes the selected change(s) to be committed.
Date/time interval	Filters according to the specified period of time and the interval (hourly/daily) at which the authentication event count is displayed. This is a compound filter, comprised of the following: • Date • Interval
Event ID	Filters according to the unique ID of the event in the log in which the policy setting was changed. For report 1.b.01, GPO changes performed for the same event share the same event ID.
GPO name	Filters according to the name of the GPO that was changed. Select the required GPOs from the Group Policy Objects dialog box. Note that the GPO Structure tab enables you to select GPOs from one or more domains, while the History tab enables you to select GPOs that have been deleted.
GPO setting name	Part of the Changed GPO settings compound filter. When used, filters according to the name of the GPO setting that was changed.
GPO version	Filters according to the version number of the GPO in which the change was made.
IP/hostname	Filters according to the machine from which the event was initiated (IP address or host name).

Filter Name	Description
New setting value	Filters according to the value of the policy setting after the change.
Old setting value	Filters according to the the value of the policy setting before the change.
Permission changes (Directory Services)	Compound filter that returns changes made to Directory Service permissions. Includes the following filters: • <i>Changed permission</i> • <i>Permission after change</i> • <i>Permission before change</i> • <i>Permission type</i> • <i>Trustee</i> • <i>Trustee account type</i>
Policy name	Filters according to the name of the changed policy setting.
Policy path	Filters according to the path of the changed policy setting.
Protected folders only	Filters according to folders and special files with protected permissions. Cannot be applied in any template in which two dates are selected.
User/computer configuration	Filters according to the object to which the changed policy setting applies. Options are: • User configuration • Computer configuration

Changes to Existing Reports

6.2.71

- The *Assigned Owner SAM Account Name* column is now available in report 4f.

6.2.3

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

- The following additional columns have been added to report 4f:
 - *Email*
 - *Mail-Enabled*
 - *Public Folder Type*
- The following additional columns have been added to report 12l, to help users to evaluate which folders with open access should be remediated first. Folders without owners and folders with many classification hits are riskier and require attention. Columns:
 - *Classification Results with Open Access (Selected Rules)*
 - *Hit Count on Files with Open Access (Selected Rules)*
 - *Management Status*
 - *No. of Files with Hits and Open Access (Selected Rules)*
 - *Owner Name*
 - *Uniqueness*
- The following additional columns have been added to report 14a:
 - *Hit Count (Selected Rules)*
 - *Hit Count on Files with Open Access (Selected Rule)*
 - *No. of Files with Hits (Selected Rule)*
 - *No. of Files with Hits and Open Access (Selected Rule)*
 - *No. of Folders with Hits (Selected Rule)*
 - *No. of Folders with Hits and Open Access (Selected Rule)*
 - *Size of All Hits (GB) – Selected Rule*
 - *Size of Files with Hits and Open Access (Selected Rule)*
- The following additional columns have been added to report 14b:
 - *% Change in Hit Count (Selected Rule)*
 - *% Change in Hit Count on Files with Open Access (Selected Rule)*
 - *% Change in No. of Files with Hits (Selected Rule)*
 - *% Change in No. of Files with Hits and Open Access (Selected Rule)*
 - *% Change in No. of Folders with Hits (Selected Rule)*
 - *% Change in No. of Folders with Hits and Open Access (Selected Rule)*
 - *% Change in Size of All Hits (GB) – Selected Rule*
 - *% Change in Size of Files with Hits and Open Access (Selected Rule)*
- The following trends have been added to report 14c:
 - *Hit count (selected rules)*
 - *Hit count on files with open access (selected rules)*
 - *No. of files with hits (selected rules)*
 - *No. of files with hits and open access (selected rules)*

- *No. of folders with hits (selected rules)*
- *Size of all hits (GB) – selected rules*
- *No. of folders with hits and open access (selected rules)*
- *Size of files with hits and open access (selected rules)*
- The following changes have been made to report 15a:
 - The Folder selection category has been added to the Event type filter. The following event types are now available:
 - *Add file's parent folder to My Folders*
 - *Folder added*
 - The *Search Scope* column has been added.
 - The following additional columns have been added:
 - *Elevated Mode*
 - *Elevated User*
 - *Elevated User's Domain*

Accessing SharePoint Objects via URL in Reports

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.

Reporting API

6.2.15

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 Reporting 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.

6.2.15

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.

Template and Subscription Ownership

6.2.3

In this version, it is possible to set owners for report templates. Ownership enables restricting template visibility, so that users only see the relevant templates.

- In the template:
 - The owner is set on the Display Options tab.
 - The users and groups that can see the template are selected on the Privacy Settings tab.
- In the Management Console:
 - The Enterprise Manager can be configured to see all templates if required.
 - The owner can be replaced for all templates at once.

Trends per Rule

6.2.3

The trend reports now store and display trends for each classification rule, in addition to the total number of classification results displayed in previous versions. Users can select classification rules in trend reports to view the following trends on the rule per resource:

- No. of hits on the rule
- No. of files with hits on the rule
- No. of folders with hits on the rule
- Size of all hits (GB) on the rule
- No. of folders with hits and open access on the rule
- No. of files with hits with open access on the rule
- Hit count on files with hits and open access on the rule
- Size of files with hits and open access on the rule

See [New Reports in This Version](#) for more information.

New Reports in This Version

6.2

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

- *Report 12.1.02, Open Access on Sensitive Data* - This report displays the folders with open access that contain files with hits on the selected classification rules. It is ordered according to the total number of hits on the files in the folders.
- *Report 14.a.04, Open Access on Sensitive Data Statistics* - For the selected rule, this report displays classification metrics on each file server.

The following report templates are now available in 6.2.3, integrated from 6.1.33:

- *Report 1.a.05, Events Committed Through DatAdvantage* - This report displays events created as a result of commit operations in DatAdvantage.
- *Report 1.a.06, Directory Service Permission Change Events* - This report is a template based on report 1a and provides information about Directory Service permission change events. Calculated according to audit events and the history of differences, it displays data about changes in permissions, as well as the trustees affected by such changes.
- *Report 1.a.07, After Hours Authentication Events* - This report is a template based on report 1a and provides information about authentication events that occurred during non-standard working hours. The events are collected from the domain controller.
- *Report 1.b.01, GPO Setting Changes* - This report provides information about changes made to Group Policy Object (GPO) settings. Each row in the report displays a policy setting that was changed during the specified time period. The information in this report can be used to identify the GPO version number, recent password policy changes, and so on.
- *Report 16.a.01, Authentication Statistics per Hour or Day* - This report displays a line chart which represents the distribution of authentication events that occurred during the defined time period. It can be used to identify the time of day with the most authentication events. It also

enables monitoring the distribution of authentication events from a specific user or computer or the number of failed authentication events during a given period of time.

- *Report 16.b.01, Users with Failed Authentications* - This report provides a bar chart which displays the users with the most failed authentication events on a specific domain during the selected time period.

Report Performance Enhancements

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

In this version, the following changes were made to enhance the performance of DatAdvantage reports:

- Improved performance in data-driven subscriptions for folder owners
- Queries are now restricted to only file servers on which the owner has managed objects
- Enhanced performance for queries with a large result set

Changes to Report Subscriptions

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

With this version, it is now possible to run report subscriptions immediately from the subscription form and the My Subscriptions pane. The *Run immediately* option in the subscription form and the **Run** button on the toolbar of the My Subscriptions pane have been added to enable this option. If a report subscription is already running, selecting the *Run* or *Run immediately* options will not rerun the subscription.

Additionally, report subscriptions can now be scheduled to run at a time in the past. This can be used to overcome time zone differences.

DatAnswers

Configuring Elevated Privileges for DatAnswers

6.2.3

With this version, the Management Console enables configuring elevated privileges for DatAnswers users. Elevated privileges allow users with the *DatAnswers Elevated Search user* role to perform advanced DatAnswers operations that ordinary users are not authorized to perform.

The following elevated search modes are available:

- *Run as a different user* - Enables impersonating another user and viewing results according to that user's permissions.
- *Show unfiltered results* - Enables viewing all results for a searched term without permission or classification filtering.

To enable this configuration, the Elevated search mode drop-down list has been added to the Administration tab on the **DatAnswers Setup** page.

Note: Elevated mode enables accessing only the search results that the user is permitted to view. While a user in unfiltered mode can view search results for which he has no permissions, he cannot open the files themselves. All operations performed during elevated searches are logged.

Limiting the Search Scope to Selected Folders

6.2.3

By default, DatAnswers searches the contents of all files and folders on which the user has permissions. In this version, it is now possible to narrow the result set by limiting the search scope to a specific folder or a set of folders.

A number of changes have been made to the DatAnswers UI to support this enhancement:

- A drop-down list has been added to the right of the search box on the initial DatAnswers page and the search results page. This option enables selecting one of the following search scopes:
 - *All contents* - Searches the contents of all files and folders on which the user has permissions.
 - *My folders* - Searches only the folder(s) listed in My Folders.
- The *Edit My Folders* option has been added to the search results page, which enables editing My Folders.
- The My Folders dialog box enables selecting the folders that should be included in the search scope. This dialog box is displayed when selecting *My folders* on the initial DatAnswers page or when selecting *Edit My Folders* on the search results page. It is possible to edit My Folders at any time by simply adding or removing one or more folders. The list of folders in My Folders is automatically saved until the next time the list is edited.
- The *Add to My Folders* option has been added to the list of menu options for each search result. This option enables adding a folder that is displayed for a particular search result to the My Folders list.

New DatAnswers Facet

In addition to the changes described above, the Folder facet has been added to the list of facets on the search results page. This facet narrows the results to files directly under the selected folder. To display the Folder facet, the DatAnswers scope must be reindexed.

Reports

To support this enhancement, several *changes have been made* to report 15a.

Viewing Metadata for Search Results

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

With this version, DatAnswers now enables viewing the metadata for each item displayed in the search results. For example, for a particular document, it is possible to view the dates on which it was created and last modified, the events performed on the file, and the document's file system permissions. The Metadata pane, which is displayed to the right of the search result, has been added to enable this option.

The file properties that are displayed in the Metadata pane depend on the options selected during configuration in the Management Console. Additionally, properties are displayed according to the following factors:

- To view classification results, flags, tags, notes and business owners, a valid DatAdvantage license is required.
- The *Work Area user* role is required to view flags, tags, notes and business owners.
- The *Classification Results View user* role is required to view the classification results in the Metadata pane.

Additionally, the Metadata pane enables viewing the details of contacts displayed in the pane. For example, it is possible to view the contact information of document authors, business owners and users who performed Create or Modify events on the document. The contact details that are displayed depend on the Active Directory properties defined in the configuration. It is only possible to view the contact information of Active Directory users.

DatAnswers API

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

In this version, new API methods are now available, which enable retrieving a document's metadata and the contact information of document authors, business owners and users who performed Create or Modify events on the document.

The following methods have been added to the DatAnswers API:

- *GetDocumentMetaData*
- *GetContactsData*

The following API classes have been added:

- *ContactRequest*
- *ContactResponse*
- *EventType*
- *Flag*
- *MetadataRequest*
- *MetadataResponse*
- *User*
- *UserEvent*
- *UserPermission*

Core and Infrastructure

Additional Events for On-Premises Exchange

6.2.70

Mailbox permission added and *Mailbox permission removed* PowerShell events are now supported on Exchange 2013.

6.2.3

This version adds support for the following events on public folders (in addition to existing support for these events on mailboxes):

- Message created
- Message received

In the log, the path of the public folder is recorded as the recipient.

Log Collection to Improve the Metadata Framework

6.2.60

With this version, Varonis introduces an improvement program. Customers who wish to participate can help to improve the quality, reliability, and performance of the Varonis Metadata Framework. Such customers' contribution would include automatically sending their Metadata Framework logs to Varonis; software performance will not be affected in any way. Customers may end participation at any time.

Varonis will collect:

- Information from the environment about Varonis software and configuration.
- Varonis event logs, which might include the names of servers, folders, files and users.

The logs are saved in the working directory on the IDU Server. From there, they are sent to a Varonis server located in the USA.

Varonis will not collect:

- File content
- Passwords

Caching SQL Credentials

6.2.60

In this version, the admin credentials entered for the SQL Server are cached when a file server is added; these credentials are then filled in automatically if another file server is added during the same session.,

New Linux Flavors

6.2.51

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

6.2

- Red Hat 6 Kernel 2.6.32
 - SMP - X86 32 bit
 - 2.6.32-504
- Red Hat 7
- SUSE SLES 11.3 Kernel 3.0.76 - Supported types:
 - SMP - 64 bit
 - 3.0.76-0
- SUSE SLES 12.0 Kernel 3.12.28 - Supported types:
 - SMP - 64 bit
 - 3.12.28-4
- Ubuntu 12.04.4 LTS Kernel 3.2.0
 - SMP - 64 bit
 - 3.2.0-58-virtual
- Ubuntu 14.04 LTS Kernel 3.13.0
 - SMP - 64 bit
 - 3.13.0-24

Increased Support for Source IP in Events

6.2.35

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	

Platform	IP Support	Comments
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	
Directory Services	Yes	

New Views in Probe Database

6.2.15

The following changes have been made to the new database views:

- New columns have been added for *User*, *Trustee*, *Previous Owner* and *SAM Account Name*.
- If the user SID is not resolved, the *UserSIDName* columns show the SID.
- The *AceMask&etc* column is translated to permission names.

6.2.10

In this version, the Probe database provides two new views:

- A view to retrieve and resolve daily Exchange events. This view shows resolved Exchange events that were collected, either directly by the Probe or via the Collector's files. Only events occurring on mailboxes that have already been crawled by FileWalk are resolved and shown in the view. It can take up to four hours for these events to show up in the new view.
- A view in the Probe database that shows all CIFS events that were collected, either directly by the Probe or via the Collector's files. The view shows events from the past three hours (including events from Collectors). These events are available for query until the *CIFS Events Delete Old Table* job is executed (usually at night).

Support for Probe Proxies on NetApp Clusters

6.2.10

In this version, it is possible to configure Probe proxies on NetApp clusters.

Support for IBM Storwize

6.2.10

This version provides support for IBM Storwize v7000 version 1.6 and higher. A document has been added to the standard documentation package providing configuration instructions.

Deduplication Support

6.2.3

Data deduplication involves finding and removing duplication within data without compromising its fidelity or integrity. If deduplication is enabled on a Windows Server, an indication is displayed in the Work Area that dedup is enabled on the volume. For each deduped file, both the physical and logical sizes are displayed.

- The Metadata Framework supports data deduplication on Windows 2012.

Important: During upgrade to 6.2, the FileWalk agent *must* be upgraded. Without this, deduplication support is not functional.

- Directories pane
 - A new *Deduplication* indicator is available under the **View** menu. If this option is selected, an icon is displayed next to the volumes on which deduplication is enabled.
 - The **Size** column now indicates the logical size of folders and subfolders.
 - A new column, *Physical Size (After Deduplication)*, is available. It is hidden by default.

- Report columns and filters
 - The *FS properties* filter category and column type now include the following filter:
 - *Physical size of this folder (in MB)*
 - *Physical size of folder and subfolders (in MB)*
 - *Physical size of subfolders (in MB)*
 - Throughout DatAdvantage and its subproducts, *Size* now indicates logical size. This affects report columns and filters, and the DCF Size priority factor.

Support for AIX 7.1

6.2.3

This version provides support for AIX 7.1.

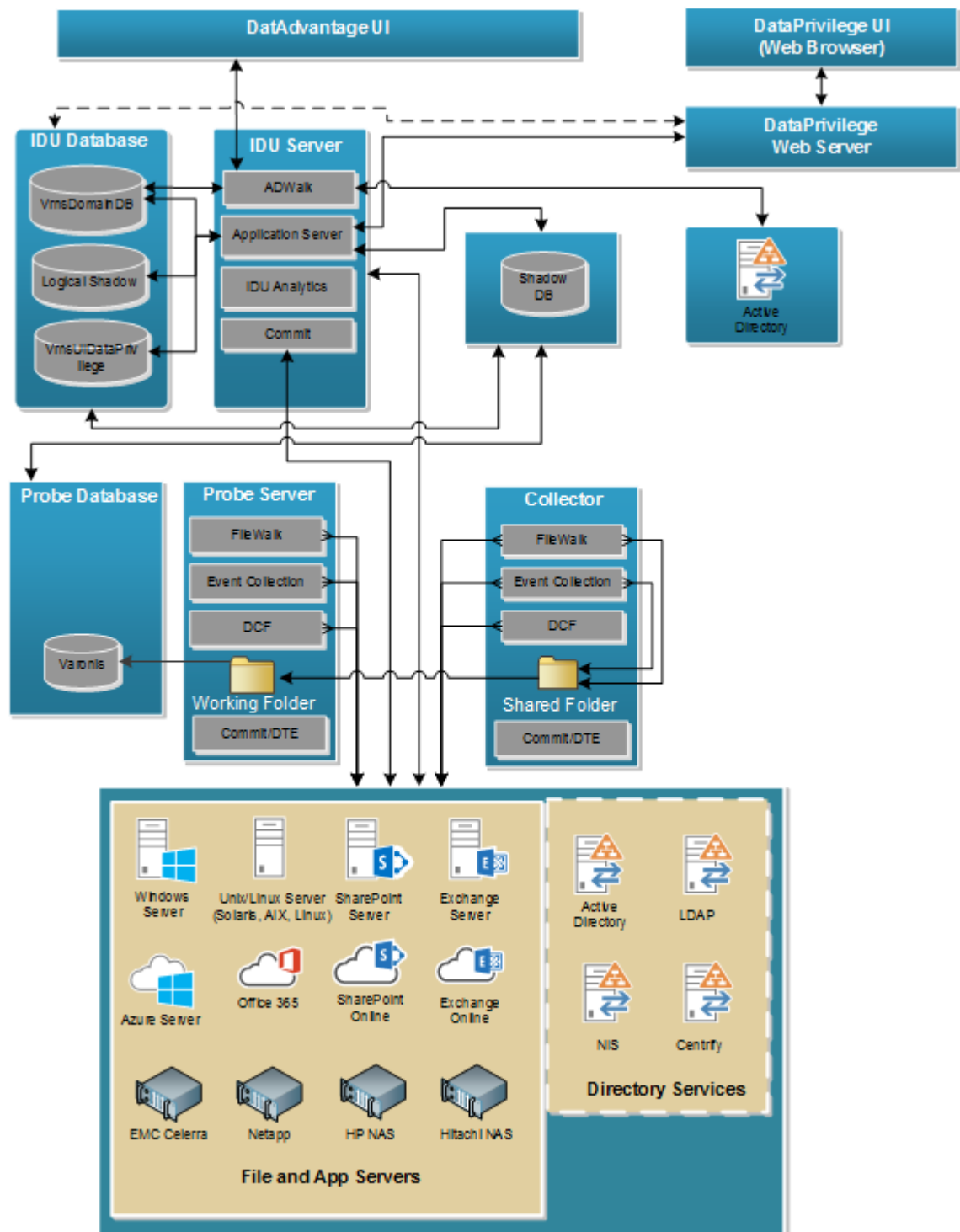
Architecture

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

The following changes have been made to the architecture of the Metadata Framework:

- DataPrivilege is now integrated tightly with DatAdvantage and IDU Analytics.
 - The DataPrivilege services (synchronization, scheduler, searcher and commit) have been removed. Their functionality now resides in other components.
 - The DataPrivilege Web Server communicates directly with the VrnUIDataPrivilege database.
- LogicalShadowDB - The new DataPrivilege database, LogicalShadowDB replaces the DataPrivilegeShadow and DataPrivilegeDomain databases.
- The Commit service now resides on the Probe/Collector and is used by the entire Metadata Framework.



Support for Azure Active Directory and Office 365

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

In this version, Varonis provides actionable insight into Azure Active Directory users and groups and the information residing on Exchange Online and SharePoint Online, Microsoft's Office 365 cloud-based services. In addition, DatAdvantage's user interface enables bi-directional visibility into Active Directory Domain Service permissions (on-premises) as well as Azure Active Directory permissions on the cloud.

The Active Directory Sync tool (DirSync) synchronizes on-premises Active Directory users and groups to the Azure Active Directory on the cloud. In terms of permissions visibility, a synchronized object is displayed as a domain user or group in the DatAdvantage UI.

DatAdvantage also presents new icons throughout the user interface to support this enhancement. These new icons can be viewed in the DatAdvantage legend.

Reports

To support Azure Active Directory and Office 365, changes have been made to various permission reports. For example, report 4.a.01 (Effective Permissions for User or Group) can now display the permissions of domain users on SharePoint or Exchange Online.

In addition, a large number of Azure Active Directory properties have been added in this version. These properties can be used as filters or columns in the log. For a list of default Azure Active Directory properties, see [Changes to Filters](#). Additional Azure Active Directory properties are available for selection in the Active Directory Properties tab of the Management Console.

Azure Active Directory

Varonis Installation Requirements

- The IDU Server must reside on Windows Server 2008 R2 or above
- Microsoft .Net Framework 4.5 or above

Security Requirements

- The ADWalk user account must have a sign-in status of *Allowed* in the Office 365 portal

DataPrivilege

DataPrivilege does *not* support Azure Active Directory or Office 365 in this version.

Visibility into Exchange Online Permissions

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

With this version, DatAdvantage provides bi-directional visibility into Exchange Online permissions. It is now possible to view user or group permissions as well as mailbox and folder permissions on Exchange Online.

For Exchange Online, FileWalk is executed through Exchange Web Services (EWS). The following is retrieved:

- Mailboxes and mailbox folders
- Public folders
- Mailbox permissions (Full Access, Send As, Send on Behalf)
- Mailbox folder permissions

Hybrid Deployment

In a hybrid deployment, on-premises and cloud-based Exchange mailboxes are represented and monitored as two different resources. To view report results for either resource, both the Exchange Online and on-premises Exchange file servers must be selected.

Varonis Installation and Requirements

- The Probe or Collector connected to Exchange Online must reside on Windows Server 2008 R2 or above
- Microsoft .Net Framework 4.5 or above

Security Requirements

- The FileWalk user must be assigned the following Office 365 roles:
 - *ApplicationImpersonation*
 - *Exchange administrator*
- The FileWalk user must be mailbox-enabled
- The FileWalk user must have a dedicated user account. That is, the user account must be different than the one used for SharePoint Online.

Supported Features

- DatAdvantage UI Visibility
- DatAdvantage ownership

Visibility into SharePoint Online Permissions

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

In this version, DatAdvantage enables viewing SharePoint Online permissions, such as the permissions of users and groups on SharePoint sites or lists. It also enables viewing the permissions of local SharePoint groups.

For SharePoint Online, FileWalk is executed through the client-side object model (CSOM). The following is retrieved:

- SharePoint items, such as document libraries, sites and lists
- SharePoint Online permissions

DataPrivilege

DataPrivilege does *not* support SharePoint Online in this version.

DCF Support

The Varonis Data Classification Framework (DCF) now supports SharePoint Online items, such as document libraries, sites, items, and lists. DatAdvantage enables viewing the items which have the most exposed permissions and contain the most sensitive data.

Varonis Installation and Requirements

- The Probe or Collector connected to SharePoint Online must reside on Windows Server 2008 R2 or above
- Microsoft .Net Framework 4.5 or above

Security Requirements

- The FileWalk user must be assigned the Office 365 *Global administrator* role
- The FileWalk user must have a dedicated user account. That is, the user account must be different than the one used for Exchange Online.

Supported Features

- DatAdvantage UI Visibility
- DCF
- DatAdvantage ownership

SharePoint Online Site Collections

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

With this version, Varonis now monitors three types of SharePoint Online site collections:

- Site collections - Non-public sites to which users require access permissions
- Public websites - Public-facing sites to which users do not require access permissions
- OneDrive for Business personal sites - Personal sites used for storing a user's business documents and files.

DatAdvantage displays the above site collection types as separate SharePoint Online file servers.

Distributed Exchange FileWalk

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

It is not unusual for organizations to install Exchange servers on multiple sites in differing LANs, yet belonging to the same domain. This sort of topology can have a negative effect on FileWalk performance due to latency issues arising from the physical distance between the Exchange servers (mailbox servers and public folders) and the Metadata Framework components.

To overcome these issues, Distributed Exchange FileWalk (DEF) enables choosing any Collector from which to run FileWalk on Exchange Storage Groups. To enable this feature, the Exchange

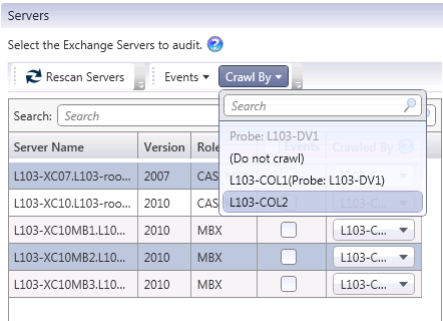
storage group should be connected to a Collector. Any Collector can be used, even a Collector that was previously configured to work with a different Probe.

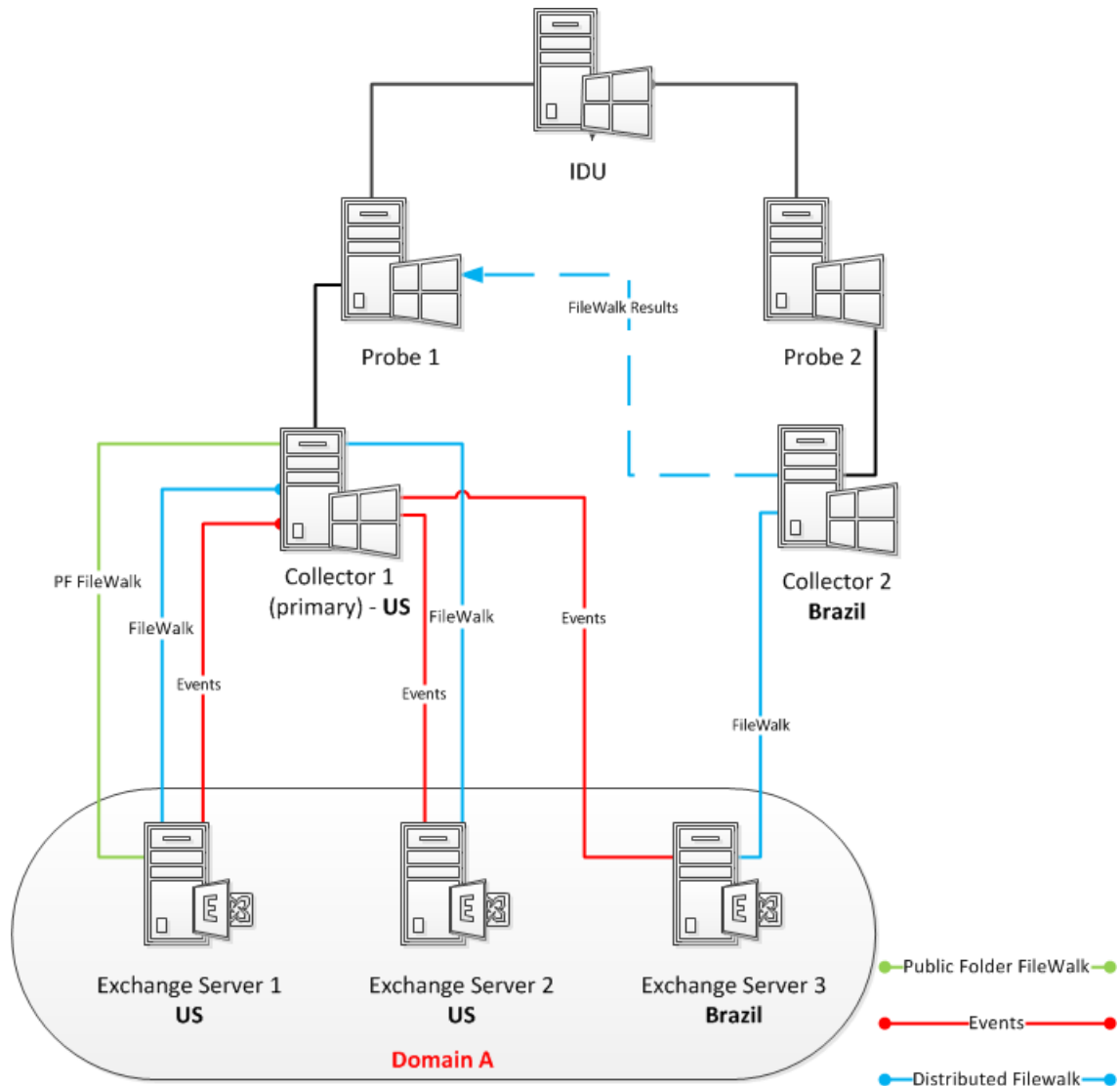
Event Collection and Crawling

This version enables configuring different settings for event collection and crawling, for every Exchange server in the storage group.

Crawling

Each Exchange Server can be configured separately, so that it is crawled by the default Probe or Collector (that is, the one linked to the Exchange storage group), a remote Collector, or is not crawled at all. At least one server must be crawled when public folders or a domain are selected from the Domains tab.



Sample Topology**Changes to Service Names****6.2.3**

Note: Now available in 6.2.3, integrated from 6.1.33.

In this version, the names of the following services have been changed:

- Varonis Filer Logger > Changed to Varonis Audit Event service
- Varonis Filer Monitor > Changed to Varonis Audit Event Collection service

Support for SQL Server AlwaysOn Availability Groups**6.2.3**

Note: Now available in 6.2.3, integrated from 6.0.x.

In this version, the Metadata Framework supports SQL Server *AlwaysOn* availability groups. Configuration is supported on SQL Server 2012 and 2014, and only for clean installations. Contact Varonis Support for assistance with configuration.

Enhanced Support for EMC Isilon

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

In this version, the Metadata Framework supports Isilon 7.2 or higher for NFS events. Access Denied events are not supported.

Support for NetApp

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

With this version, the Metadata Framework provides support for the following NetApp versions:

- 8.3 RC, GA
- 8.3.1 RC
- 8.3 P1 - Also supported for cluster mode

Monitoring of NetApp Shares Set to "Nobrowse"

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

This version provides support (both visibility and auditing) for NetApp shares on which the *nobrowse* option is enabled. These are shares that cannot be accessed or detected through their parent, or through a search function. They can only be access by using their full path.

Exchange 2013 Agent

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

In this version, the new agent is generally available (GA).

Note: With regard to BlackBerry, only BlackBerry Enterprise Server 10 and higher are supported.

Nexenta Support

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

This version provides support for Nexenta 3.1.3.5, as a Unix SMB file server.

Incremental FileWalk

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

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

- Full FileWalk has been restored as the default mode.
- If incremental FileWalk is enabled, events are now collected temporarily for filtered and unmonitored users and calculated in the scope of the incremental FileWalk.
 - These events are added only to the scope of incremental FileWalk; they do not appear in statistics or reports, nor are they stored in the database.
 - If incremental FileWalk is disabled on a particular file server, these events can be filtered.

Reduction in System Notifications

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

This version includes the following, aimed at reducing the number of inessential notifications sent by the Metadata Framework:

- Redundant notifications about locked mutexes are either suppressed or removed completely.
- Database messages regarding similar errors are now aggregated to a single notification.
- Performance has been improved in the following:
 - Data-driven report subscriptions for folder owners
 - Queries are now performed only on file servers on which the owner has owned objects
 - General performance of queries with a large result set

Licensing

Changes to the SharePoint Online and Exchange Online Licenses

6.2.3

Prior to this version, SharePoint Online and Exchange Online licenses were not required in order to install SharePoint Online and Exchange Online file servers.

With this version, the SharePoint Online and Exchange Online licenses are separate from the on-premises licenses. SharePoint Online and Exchange Online file servers can now be installed only if there are valid SharePoint Online and Exchange Online licenses.

In addition, the following changes were made with regard to the expiration of the online licenses:

- During the grace period, the ADWalk job will continue to run on Azure Active Directory.
- Upon license expiration, local ADWalk will cease to run on the expired platform.

Changes to Permanent Software Licenses

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

With this version, the behavior of the permanent software license 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.
- During the grace period, the Metadata Framework will remain as it was prior to the grace period. Mail alerts will be sent regarding pending license expiration.
- Following the grace period, the behavior of the license changes as follows:
 - Crawling and event collection - Will continue on all file servers and all volumes of mixed file servers.

Note: The folder structure and event data will only be presented in the user interface once the current license is extended or a permanent license is purchased. If a platform is purchased during the grace period, all events from the relevant platform will be available in the DatAdvantage UI and in the Reports view.

- Jobs - Will continue to run on all on all file servers and all volumes of mixed file servers.
- DatAdvantage UI
 - Will continue to be available, provided that at least one platform remains licensed.
 - For expired file servers or individual volumes of mixed file servers, folder structure is not available in the DatAdvantage UI. In addition, the option to select an expired file server will no longer be available from all Resources pickers and File server filters in the DatAdvantage UI.
- Reports
 - Historical data collected from expired file servers will cease to be available in all reports.
 - Mixed file servers - Report and log data will continue to be retrieved for all volumes of mixed file servers, provided that at least one platform is valid.
 - Reports 8a, 8c and 8d will continue to be available when the licenses for all platforms are expired.
- Indications of expired licenses will appear for the relevant file servers throughout the DatAdvantage and Management Console UIs.

- DatAlert - Alerts will not be sent for expired resources.
- DCF
 - Will continue to run on file servers or folders with an expired license.
 - Will continue to scan and index data for DatAnswers
- DatAnswers
 - Windows and SharePoint - Will continue to display search results for the expired file servers in the DatAnswers UI.
 - Mail alerts will be sent regarding pending license expiration.
- 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.

Changes to Evaluation Licenses

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

With this version, the grace period for evaluation licenses has been extended to 30 days. In addition, the behavior of the evaluation license changes as follows when the number of days set for a particular platform's license is reached (and the grace period begins):

- Crawling and event collection - Will continue on all file servers and all volumes of mixed file servers.

Note: The folder structure and event data will only be presented in the user interface if the current license is extended or a permanent license is purchased. If a platform is purchased during the grace period, all events from the relevant platform will be available in the DatAdvantage UI and in the Reports view.

- Jobs - Will continue to run on all on all file servers and all volumes of mixed file servers.
- DatAdvantage UI
 - Will continue to be available, provided that at least one platform remains licensed.
 - For expired file servers or individual volumes of mixed file servers, folder structure is not available in the DatAdvantage UI. In addition, the option to select an expired file server will no longer be available from all Resources pickers and File server filters in the DatAdvantage UI.

- Reports
 - Historical data collected from expired file servers will cease to be available in all reports.
 - Mixed file servers - Report and log data will continue to be retrieved for all volumes of mixed file servers, provided that at least one platform is valid.
 - Reports 8a, 8c and 8d will continue to be available when the licenses for all platforms are expired.
 - Indications of expired licenses will appear for the relevant file servers throughout the DatAdvantage and Management Console UIs.
- DatAlert - Alerts will not be sent for expired resources.
- DCF
 - Will continue to run on file servers or folders with an expired license.
 - Will continue to scan and index data for DatAnswers
- DatAnswers - Windows and SharePoint - Will continue to display search results for the expired file servers in the DatAnswers UI.
- Email notifications will be sent to the system administrator regarding pending license expiration.

The behavior of the evaluation license changes as follows when the grace period for a particular platform has finished:

- Crawling and event collection
 - Will cease on all file servers and on all volumes of the relevant protocol for mixed file servers.
 - If a platform is purchased after the grace period, all events performed following license expiration will be lost.
- Jobs - No data will be retrieved for expired file servers and volumes of mixed file servers.
- DatAnswers
 - Windows and SharePoint - Will cease to display search results for the expired file servers in the DatAnswers UI.
- Automatic share detection will continue running on volumes of mixed file servers with expired licenses, provided that there is a valid Windows license.

Upgrade

Upgrade Flows

6.2.85

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.x directly to 6.2.85.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.85. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership

synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.

- Version 6.0.101 and higher may be upgraded to 6.2.85. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
- Version 6.1.30 or higher may be upgraded directly to 6.2.85. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.80

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.x directly to 6.2.80.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.80. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.0.101 and higher may be upgraded to 6.2.80. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.80. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.74

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.x directly to 6.2.74.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.74. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.0.101 and higher may be upgraded to 6.2.74. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.74. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.73

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.x directly to 6.2.73.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.73. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.0.101 and higher may be upgraded to 6.2.73. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.73. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.72

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.x directly to 6.2.72.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.72. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.0.101 and higher may be upgraded to 6.2.72. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.72. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.71

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.x directly to 6.2.71.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.71. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership

synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.

- Version 6.0.101 and higher may be upgraded to 6.2.71. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
- Version 6.1.30 or higher may be upgraded directly to 6.2.71. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.66

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.x directly to 6.2.66.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.66. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.0.101 and higher may be upgraded to 6.2.66. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.66. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.63

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.x directly to 6.2.63.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.63. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.0.101 and higher may be upgraded to 6.2.63. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.63. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.62

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.x directly to 6.2.62.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.62. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.0.101 and higher may be upgraded to 6.2.62. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.62. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.61

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.x directly to 6.2.61.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.61. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.0.101 and higher may be upgraded to 6.2.61. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.61. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.60

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.x directly to 6.2.60.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.60. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership

synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.

- Version 6.0.101 and higher may be upgraded to 6.2.60. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
- Version 6.1.30 or higher may be upgraded directly to 6.2.60. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.53

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.x directly to 6.2.53.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.53. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.0.101 and higher may be upgraded to 6.2.53. DatAdvantage is upgraded, while DataPrivilege remains on 6.0.101. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.53. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.52

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.x directly to 6.2.52.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.52. DatAdvantage is upgraded, while DataPrivilege retains the original version. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.0.101 and higher may be upgraded to 6.2.52. DatAdvantage is upgraded, while DataPrivilege retains the original version. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.52. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.51

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.x directly to 6.2.51.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.51. DatAdvantage is upgraded, while DataPrivilege retains the original version. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.0.101 and higher may be upgraded to 6.2.51. DatAdvantage is upgraded, while DataPrivilege retains the original version. Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade. However, the Log and Statistics screens in DataPrivilege are not functional.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.51. Both DatAdvantage and DataPrivilege are upgraded.

See [Installing or Upgrading DatAdvantage and DataPrivilege Separately](#) for more information.

6.2.38

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.x directly to 6.2.38.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.38. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.0.101 and higher may be upgraded to 6.2.38. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.38. Both DatAdvantage and DataPrivilege are upgraded.

6.2.37

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.x directly to 6.2.37.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.37. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.0.101 and higher may be upgraded to 6.2.37. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.1.30 or higher may be upgraded directly to 6.2.37. Both DatAdvantage and DataPrivilege are upgraded.

6.2.36

Due to critical issues that were discovered, upgrade is no longer available to this version. Instead, customers who want to upgrade may do so to version 6.2.37, as described above. All features and functionality included in this version are available in 6.2.37 as well.

6.2.35

Due to critical issues that were discovered, upgrade is no longer available to this version. Instead, customers who want to upgrade may do so to version 6.2.37, as described above. All features and functionality included in this version are available in 6.2.37 as well.

6.2.15

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.x directly to 6.2.15.
- DataPrivilege-only installations may *not* be upgraded to 6.2.15 at all. Only clean installation is possible.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.15. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.0.101 and higher may be upgraded to 6.2.15. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.1.30 may be upgraded directly to 6.2.15. Both DatAdvantage and DataPrivilege are upgraded.

6.2.10

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.x directly to 6.2.10.
- DataPrivilege-only installations may *not* be upgraded to 6.2.10 at all. Only clean installation is possible.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.10. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.0.101 and higher may be upgraded to 6.2.10. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.1.30 may be upgraded directly to 6.2.10. Both DatAdvantage and DataPrivilege are upgraded.

6.2.6

Customers who want to upgrade may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x and 6.1.x directly to 6.2.6.
- DataPrivilege-only installations may *not* be upgraded to 6.2.6 at all. Only clean installation is possible.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.6. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.0.101 and higher may be upgraded to 6.2.6. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.1.30 may be upgraded directly to 6.2.6. Both DatAdvantage and DataPrivilege are upgraded.

6.2.5

Customers who want to upgrade DatAdvantage alone may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x and 6.1.x directly to 6.2.5.
- DataPrivilege-only installations may *not* be upgraded to 6.2.5 at all. Only clean installation is possible.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.5. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.0.101 and higher may be upgraded to 6.2.5. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.1.30 may be upgraded directly to 6.2.5. Both DatAdvantage and DataPrivilege are upgraded.

6.2.3

Customers who want to upgrade DatAdvantage alone may do so as follows:

- DatAdvantage-only installations may be upgraded from 6.0.x and 6.1.x directly to 6.2.3.
- DataPrivilege-only installations may *not* be upgraded to 6.2.3 at all. Only clean installation is possible.
- DatAdvantage+DataPrivilege installations may be upgraded as follows:
 - Versions lower than 6.0.101 must first be upgraded to 6.0.101 or higher, and then to 6.2.3. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.0.101 and higher may be upgraded to 6.2.3. DatAdvantage is upgraded, while DataPrivilege retains the original version. Synchronization between DatAdvantage and DataPrivilege ceases following upgrade.
 - Version 6.1.30 may be upgraded directly to 6.2.3. Both DatAdvantage and DataPrivilege are upgraded.

Installing or Upgrading DatAdvantage and DataPrivilege Separately

6.2.51

In this version, it is possible to upgrade only DatAdvantage in an environment that includes both DatAdvantage and DataPrivilege, as long as the source version of both products is 6.0.10x. In this case:

- Ownership synchronization between DatAdvantage and DataPrivilege *is retained* following upgrade, and IDU Analytics recommendations are functional for both.
- With the exception of the synchronization service, DatAdvantage jobs run without taking DataPrivilege into consideration.
- DataPrivilege data is not affected, but the Log and Statistics screens in DataPrivilege are hidden by default and not functional if an administrator configures them to be visible.

If DataPrivilege 6.0.10x is already installed and a new installation of DatAdvantage 6.2.51 is required, DatAdvantage 6.0.10x must first be installed, and then upgraded to 6.2.51. Otherwise, ownership synchronization and IDU Analytics recommendations will not be available.

6.2.3

In consolidated environments, in which DatAdvantage and DataPrivilege share a working account, the working account must remain the same for both products even if one of them is upgraded to 6.2.

For example: DatAdvantage 6.0.100 and DataPrivilege 6.0.100 share a working account. Only DatAdvantage is upgraded to 6.2. If the working account is changed in any way (user name or password), DataPrivilege will cease to function. Therefore, the working account must either remain the same for both products, or any change to it must be made for both products.

DatAlert Exclusion Scope Upgrade

6.2.35

This version supports the upgrade of exclusion scopes (that is, scopes configured prior to this version) to a new scope.

The following table describes the logic:

Scope	Excluded By	New Exclusion Filter and Operator
Where	File server	File server; not equals
Who	User/Group	• For users: User; not equals • For groups: Acting users from group; not contained in
	Organizational units	OU path (acting object); not equals
	Admin accounts	Acting privileged accounts; not equals admin accounts

Scope	Excluded By	New Exclusion Filter and Operator
	Service accounts	Acting privileged accounts; not equals service accounts
	Test accounts	Acting privileged accounts; not equals test accounts

The following changes will be made upon upgrade:

- Global exclusion scopes will be added as user-defined filters to all DataAlert rules.
- Global exclusion scopes will be added as user-defined exclusion conditions to all DataAlert Analytics rules.
- Report 8b will continue to display old audit events regarding the creation, editing or deletion of global exclusions.

Decommissioning File Servers During Upgrade

6.2.3

During the upgrade process, recommendations are now provided to decommission servers that are no longer monitored and for which events are not collected. The **Set Servers as Decommissioned** page has been added to the Enterprise Installer to enable decommissioning one or more of these file servers.

When a file server is decommissioned, historical data is saved. Event collection and crawling are disabled for decommissioned file servers.

During upgrade and repair, only the Shadow database will be upgraded. No other operations will be performed for decommissioned servers. In addition, no error messages will be displayed for decommissioned servers during the Repair/Upgrade flow.

Upgrading Collectors

6.2.3

Note: Now available in 6.2.3, integrated from 6.1.33.

In this version, it is now possible to upgrade Collectors through the Enterprise Installer. The **Collector Upgrade** page has been added to the Varonis Setup Wizard to enable this option.

Documentation

6.2.51

In this version, the *Management Console User Guide* has been rearranged. The following topics are now located under *Managing the Metadata Framework*:

- *Running and Scheduling Database Jobs*
- *Viewing Failed Synchronizations*

- *Setting Database Credentials*
- *Helping to Improve the Metadata Framework*

6.2.3

Note: Now available in 6.2.3, integrated from 6.0.x.

With this version, a number of structural changes have been made to the documentation that accompanies the Metadata Framework:

- The DCF and DatAnswers configuration material has been removed from the *DatAdvantage User Guide*. It is now found in the *DCF and DatAnswers Configuration Guide*.
- The DatAlert documentation has been removed from the *DatAdvantage User Guide*. It is now found in the *DatAlert User Guide*.
- The Data Transport Engine documentation has been removed from the *DatAdvantage User Guide*. It is now found in the *Data Transport Engine User Guide*.
- The filter documentation has been removed from the *DatAdvantage User Guide* and the *Metadata Framework Report Guide*. It is now found in the *Metadata Framework Filter Reference Guide*.
- The PowerShell information has been removed from the *Management Console User Guide*. It is now found in the *Metadata Framework Powershell Reference Guide*, which has been updated to include new PowerShell commands.
- The database job descriptions have been removed from the *Management Console User Guide*. They are now found in the *Metadata Framework Database Job Reference Guide*.

Noteworthy or Changed Behavior

6.2.85

Issue ID	Description
527358	The <i>Potential past ransomware activity indicated by a suspected a residual ransomware note</i> threat model is no longer available.
528805	Solr now stops indexing and processing files when there is less than 20 GB of free disk space.

6.2.80

Issue ID	Description
501586	A clone rule was added to the Data Transport Engine.

Issue ID	Description
503696	Following migration of the VrmsDomainDB database to a new SQL instance and running the Report Deployment Tool, friendly names were no longer displayed for report columns.
504882	In DataPrivilege, creating a request for ten or more simultaneous users is now faster.
510921	The Management Console's performance on large environments was enhanced.
511170	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.
514029	The retention policy no longer blocks the executions table.
520785	The Encrypted Files dictionary has been expanded to include new values.
520786	The Crypto Files dictionary has been expanded to include new values.

6.2.74

N/A

6.2.73

N/A

6.2.72

Issue ID	Description
505051	The scheduling of the DatAlert Rule Prepare job has been changed, so that it now runs every 10 minutes.

6.2.71

Issue ID	Description
479395	Improvements to DatAlert's predefined rules help to prevent false positives.

Issue ID	Description
479985	When reports are exported to CSV through a subscription, column headers containing non-alphanumeric characters are replaced by underscores.
480859	A number of terms were added to the Encrypted files dictionary.
481065	A check was added to ensure the Probe is online raising DoSyncProbe.
485194	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 (-).
485210	"Mailbox permission added" and "Mailbox permission removed" PowerShell events are now supported on Exchange 2013.
486411	An Alert Category placeholder was added to the DatAlert template's optional fields.
486794	It is now possible to disable VSS in the Windows agent.
494418	The DCF and DW Send Workload job has been optimized for resource cooperation efficiency.
494845	Solr now stops indexing and processing files when there is less than 50 GB of free disk space.
496236	Syslog identity has been removed from SIEM-oriented templates.
501124	Exchange upgrade failed because the machine account was used instead of the installation account.

6.2.66

Issue ID	Description
496007	Several issues with FileWalk scheduling were fixed: • Duplicate schedules were removed. • The FileWalk job was reattached to the correct schedule. • Invalid FilerIDs in FileWalk schedules were fixed.

6.2.63

N/A

6.2.62

N/A

6.2.61

N/A

6.2.60

Issue ID	Description
392031	The Security Certificate File Types rule, which detects security certificate files, now searches for additional file types for the DCF and DatAnswers.
439934	When a Data Transport rule was created and the Files Activity filter was added to the file scope, newly created files with no events were erroneously moved to the destination. To fix this issue, when the Files Activity filter is added to a file scope, a default filter (Date created < 1 week) will also be applied to the scope.
450204	To enable full NTFS permission support on Samba, set the /etc/samba/smb.conf configuration file with the following values: * vfs objects = acl_xattr * store dos attributes = yes * inherit acls = yes * inherit permissions = yes * map acl inherit = yes * admin users = "Domain Admins"
453070	The subfolders under the MSI folder were renamed to exclude the word "Beta".
457476	New crypto extensions were added to the Encrypted Files dictionary.
457818	In the DatAlert Web UI, customers can now go from the object widgets at the top of the dashboard straight to the alerts drill down data, without opening the context card.
465329	Values were added to the crypto files dictionaries to improve ransomware detection capabilities.

6.2.53

Issue ID	Description
463376, 463380	Extensions were added to crypto files and encrypted file dictionaries, to prevent malware infection. The following extensions have been added: • *.cryptz • *.ded • *.crypt38 • *.epic The term *GLAMOUR*.* has been removed, as its inclusion resulted in false positives.

6.2.52

N/A

6.2.51

Issue ID	Description
368306	Multiple files created by the subscriptions CSV files were put in the same location.
419446	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.
433942	Servers must be defined with the same name in both the Varonis Management Console and in DFS Management. Otherwise, the mapping of file server to its CNAME must be provided via the DFS Shares tab in the Management Console.
437649	The Events Deletion job was optimized to accommodate a large amount of tables.
438214	In the DCF, pattern matching improvements were made that enabled quicker scanning of files 20 MB and larger.
438746	The Analytics Engine was modified to work faster.
440647	In reports 4.g.1 and 4.f.1, it is possible to display a valid SharePoint URL.
446784	In DatAlert Analytics, in the exploitation tools dictionary, the value canvase.* was changed to canvas.bat and *canvas.py in order to eliminate false positives.

Issue ID	Description
448449	In DatAlert Analytics, for non-CIFS resources (such as SharePoint, Unix and Exchange), mixed CIFS environments and NFS platforms, events retrieved from unresolved folders will not be displayed even if the unresolved folder is a child of a resolved folder.
449352	DatAlert currently supports up to 150 filters per rule.
449955	The DatAdvantage UI only supports text at a zoom level of 100%.
450451	In the recon tools dictionary, the term *SET* was replaced by a list of more specific and detailed terms.
450687	IP address resolution in Windows relies on the way in which the user logged in. The IP address is resolved when login is performed with the following methods: • Network logon – accessing a computer from elsewhere on the network • NetworkClearText – similar to the above, when password was sent in clear text The IP address is not resolved when login is performed through any of the following methods: • Interactive logon – logon at the console of a computer • RemoteInteractive – when accessing a computer through Terminal Services, Remote Desktop (RDP) or Remote Assistance • Batch logon – done by the scheduled task service for scheduled tasks • Service logon – done by services on start • CacheInteractive – used by mobile devices For additional information, see: http://www.windowsecurity.com/articles-tutorials/misc_network_security/Logon-Types.html
451122	Metabase 6 compatibility must be configured to enable use of IIS on Windows 2003.
453631	In the DatAlert web interface, in the Alerted Events screen, the default columns were changed.
454160	The Encrypted Files dictionary has been expanded in order to include new values.
455804	To monitor GPO change events, the primary language of the Probe server's operating system should be English (GPMC report output must be in English).

6.2.38

N/A

6.2.37

N/A

6.2.36

Issue ID	Description
449319	When the DatAlert web UI is run on Internet Explorer, a new error message indicates that Compatibility mode is not supported.

6.2.35

Issue ID	Description
401971	In DatAlert Analytics, test accounts are now known as other accounts.
405023	The alert email template did not retain any customizations following upgrade.
405030	In DatAlert Analytics, long SAM account names were cut off in the notification emails and Details column in the View History window.
419100	The Possible asset exposure: permissions granted to user in local/unmonitored/abstract domain predefined rule has been deprecated.
420267	In DatAlert Analytics, personal accounts are now called employee accounts.
422833	In DatAlert Analytics, duplicate events arriving from different domain controllers are now aggregated.
439418	Additional values were added to the DatAlert Analytics dictionaries.
439967	For Windows 2000 file servers, the Enterprise Installer installs an older version of the Varonis Windows Agent. A separate MSI is also provided, for manual installation of the older agent.

6.2.15

Issue ID	Description
393239	In DatAdvantage, report subscriptions now support exporting to the XLSX format, in addition to XLS.
397918	Statistics tables are now updated during the Maintenance job.
412281	The list of products that are not supported by license was added to the licensing error message.
418246	Report 9i now calculates stale data based on physical size rather than logical size.
393888	It is now possible to define aliases for each CIFS file server defined in the Management Console.
410464	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.
430393	A new configuration option has been added to varonis.config. The DfsEnableDfsFolderCrawl option can now be set to show DFS folders that link to other DFS folders that reside at a different root.
425215	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 Adding additional file types to the default list might impact performance and hardware requirements.

6.2.10

Issue ID	Description
358843	In DatAdvantage, the Probe database restoration message is now more detailed.
383343	In DatAdvantage, the GPO report generation failure notification is now more detailed, mentioning that the GPMC might not be installed.
387809	In the Management Console, a distinguishedName error message now includes more details.
392295	In DatAnswers, the search function has been improved. When searching for <i>filename:<word></i> , all filenames with <word> in it are returned. For example, a search for the word may will generate both <i>AutoMay</i> and <i>Auto May</i> .
392355	In DatAdvantage report 9e, files without extensions are no longer labelled as <i>other</i> . They are now labelled as <i>Files without Extension</i> .
393012	In DatAdvantage, in the Collector, the sending, checking, and recovery of jobs is now executed three times in the event of a timeout exception.
393048	In DatAdvantage, the default value in the WinNTLDAP field in the Domains table was changed to <i>AutoDetect</i> .
393158	In DatAdvantage, a new database view displays resolved Exchange events from the last two days.
395619	The DCF no longer scans TMP files (files that begin with ~\$).
395623	In the DCF, the following keywords were removed from predefined patterns: • DE Driver's License Number - <i>DL</i> was removed • ACT Driver Licence Number - <i>DL</i> and <i>ACT</i> were removed • WA (AU) Driver Licence Number - <i>DL</i> and <i>WA</i> were removed
401261	In DatAdvantage, the CSV format for uploading follow-up indicators now use the DomainName\SAM account name format.
401344	In the DatAlerts Publisher, cache size has been increased to reduce network traffic from the Publisher to Active Directory.

Issue ID	Description
401679	In the Data Transport Engine, performance improvements have been made to command selection to avoid memory consumption problems and slow response time.
402186	In DatAdvantage, during Shadow migration, the validation logic of the file server's SID is no longer executed.
405754	To avoid negative performance impact, the scopes of disabled DatAlert rules are no longer calculated during FileWalk. (Note: If many DatAlert rules are enabled, performance will be affected.)
409283	In DatAdvantage, for systems running Unix or Linux, all privileged accounts must be added manually.

6.2.6

N/A

6.2.5

N/A

6.2.3

Issue ID	Description
209646	The port used by the DCF Monitor has been changed from 55555 to 2907, since the range 49152–65535 is dynamic and port 55555 might already be in use.
322447	FPolicy was automatically re-enabled on a NetApp file server after it was disabled.
335176	In the configuration of the incremental FileWalk job (General settings in the Management Console), it is no longer necessary to set the number of objects (files and folders) that can be stored in the scanning queue.
336295	The downgrade patch now accesses sys.sql_expression_dependencies only on SQL Server 2008 and higher.
355174	Subvolumes are not treated as available mount points and are not visible in the list of shares in the Enterprise Installer or the Management Console.

Issue ID	Description
367829	The schedule of IDU Analytics has been changed to "weekly". The change is made during both clean installation and upgrade.
374267	GPO installation instructions have been updated.
374798	A prerequisite check was added to DatAnswers installation to ensure the target website is running.
383314	During upgrade, the FileWalk agent <i>must</i> be upgraded to support deduplication.
383848	The prerequisites for Exchange Online have changed as follows: • The IDU Server and Collector that monitor Exchange Online must both have access to the following URLs: • https://ps.outlook.com/powershell • http://schemas.microsoft.com/powershell/Microsoft.Exchange • To enable FileWalk to run successfully, the Make this person change their password the next time they sign in option must be cleared for the FileWalk user.
383880	An index was added to the daily table to improve performance of CIFS archiving.
387427	If a filtered user created files, incremental FileWalk scanned the parent folder instead of the folder in which the file was created.
392955	The FileWalk user for Exchange Online has been changed to the Exchange administrator role instead of the Global administrator role.
393258	Performance of event archiving for Active Directory has been improved.

Resolved Issues

6.2.85

Issue ID	Description
520962	The DatAlert Analytics Extensions job stopped responding.
522368	An exception occurred when a new resolver was added on CoreResolver.

Issue ID	Description
522682	DatAlert's Exploitation tools and Recon tools dictionaries were not fully updated with new values.
523021	There were errors in the mail queue and notification tables after the DatAlert Calc Entities job was run.
523044	DatAlert rules on Exchange did not complete their calculations because the Where scope did not reach the Probe. Following this error, the database had duplicate rows and there were duplicate entries in the UI for the alert.
523393	There was a typographical error in DatAlert severities, whereby the severity was listed as Waiting instead of Warning.
528490	In DatAlert rules, the Where scope sent files to the Probe for SharePoint file servers.
529311	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.
529937	Filters in DatAlert rules were not converted to dynamic filters if the rules contained more than one Access path filter.
529589	The Commit option was missing from the context menu in DatAdvantage mixed Exchange Servers.
531484	The EventsStats table in the vrnsDomain database could not be updated if there were simultaneous calls for the Hist_PrepareHistoryTable with different request times from different file servers.

6.2.80

Issue ID	Description
467663	Descriptions were not displayed in reports using the RDL TableBasedContainSubReportRdlTemplate RDL file (for example, report 4.b.x).
469319	Report 4f did not return results for folders that contained multiple flags.

Issue ID	Description
472052	When an Exchange file server from a mixed environment was added to the Management Console, the wrong volume version was defined. As a result, Exchange permission changes could not be committed.
484796	The Events Archive job got stuck on a specific subset of events on aggregating windows events.
486846	When a data-driven subscription was emailed to a user-owner that had been deleted from Active Directory, the subscription completed with the status "finished with errors".
494954	The DataPrivilege Request and Authorization report did not display pending entitlement reviews correctly.
501443	When implementing Windows Authentication, the Bulk Upload Utility installation failed.
502891	In the Data Transport Engine, when a rule was deleted before the Rule Prepare operation finishing running, the operation crashed but the commands were not deleted for the deleted rule.
503016	When there were clones of a SharePoint's domain, it was impossible to add a SharePoint site to DataPrivilege.
503126	An error occurred in fetching GPOs.
504119	After upgrade, report 12.L did not work properly.
504321	After adding a computer account to the IDU Analytics list of filtered accounts, upgrade failed.
505614	In DCF, performance issues and rare instances of data loss occurred on results found by dictionaries.
505662	Probe migration with a manual database copy was unable to be performed.
506094	For the Pull AD job, the system user entry in the AD_SidIDs table was not displayed in DatAdvantage.
506330	Numbers were displayed instead of permission levels in the permissions row in report 4j for the SharePoint file server.

Issue ID	Description
506475	Rename and move events were not reported correctly. The "rename_DirPath" did not include the destination path for the "move operation" for files and folders.
506716	Following a rule's deletion, its accompanying four scopes were not likewise deleted.
506969	"IDU" was not displayed in the File Server tab in reports and thus could not be selected. The report tab now displays File Server/Domain, so that IDU can be selected.
507100	The ADWalk job stopped responding due to an unresponsive RegconnectRegistry WinApi.
507164	ADWalk thread management was improved for better handling of local accounts.
507243	The Enterprise Installer sent multiple start commands to PublishingManagement, resulting in multiple standard DataAlerts on the same events and threshold alerts with the same alerted events.
507484	Reports could not be exported to CSV.
507503	In DataPrivilege, when a new administrator was added, the remove button in the Authorizer tab was disabled.
507505	When replication existed between two domain controllers, and the main domain controller was powered off, users were unable to log in to DataPrivilege.
507611	The ADWalk job failed to scan Exchange mailboxes and the Autodiscover service couldn't be located error message was retrieved.
508251	DataAlert failed to initialize on the Probe. As a result, no alerts were generated.
509757	In the Management Console, Job history was missing the FileWalk job type that was running.
510281	Following upgrade to 6.2.53, the FileWalk job failed to initiate on SharePoint file servers.

Issue ID	Description
510632	Multiple start commands sent by the installer to PublishingManagement resulted in multiple alerts on the same events and threshold alerts with the same alerted events.
511077	While shutting down a node on a Windows 2012 RN file server (with CSV), a blue screen of death was displayed.
513066	DatAlert rules with multiple file servers defined in the Where scope were duplicated per file server.
513140	Synchronization did not work correctly in some Probes and Collectors. Therefore, recovery jobs ceased to function properly.
513157	Following upgrade to 6.2.72 or 6.2.73, high CPU utilization on a Collector caused it to stop functioning.
513467	The DatAlert AnalyticsExtensions rules job crashed when there were two alerts for the same user for the same rule for more than one day.
513510	Access path validation failed for the Suspicious access activity: non-admin access to startup files and scripts threat model.
513547	The DCF failed to scan keywords that contained the following delimiters: # ; .
514031	Changes have been made to the VrmsDomainDB code to improve the dispatcher performance in critical areas.
514033	The license check was called every time the spGetFiles was called, regardless of the parameters.
514036	New diagnostics were added to the Event lifecycle, DCF, DCF progress, FileWalk, and FileWalk execution statistics.
514038	The performance of the Management Console jobs screen has been improved.
515415	After the server restarted, the jobs that were not finished from the previous run took too much memory and the server crashed.
516056	The Collector FileWalk Data Delivery job failed with errors.

Issue ID	Description
517359	The installation of SQL Server 2005 failed. A default value could not be assigned to a local variable.
517652	Temporary tables were not properly deleted from the database.
520785	The Encrypted Files dictionary has been expanded to include new values.
520786	The Crypto Files dictionary has been expanded to include new values.

6.2.74

Issue ID	Description
513065	DatAlert rules that had multiple file servers defined in the Where scope were duplicated for each file server.
513411	The DatAlert Analytics Extensions rules job did not function correctly.

6.2.73

Issue ID	Description
509254	Existing email recipients for DatAlert Analytics rules were deleted on upgrade.
509341	After DatAlert Analytics rules were created, standard DatAlert rules were not published and pv_RTAlertedEvents could not read from the Probe to the Shadow database.

6.2.72

Issue ID	Description
502695	The incremental FileWalk job overwrote data from the full FileWalk job.
505050	The DatAlert Rule Prepare job ran during upgrade, which caused a number of problems.

Issue ID	Description
505312	When several rules used the same What scope, only one rule was calculated and sent.
505612	The spFixfileWalk stored procedure stopped responding, resulting in poor performance on Unix and NetApp file servers with NFS shares.

6.2.71

Issue ID	Description
430169	DatAlert resolved well-known SIDs in the wrong domain when nested domains were configured.
454847	SharePoint frontend servers that had been previously added to the IDU could not be re-added.
459136	In DataPrivilege, 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.
461508	The Pull AD job did not include AD_SidHistory in the logic to insert into ActiveDirectory_sid_relations, so not all permissions were calculated and displayed.
466018	Probe upgrade failed if several file servers were connected via several Collectors.
469012	The Dictionaries window in DatAdvantage was not restricted according to user.
469072	Access was sometimes denied during execution of Data Transport Engine rules due to a faulty stored procedure.
469261	The JOB_Executions indexes were unnecessarily rebuilt during upgrade.
469417	It was not possible to save report templates if they Active Directory attributes that contained numbers in their names.
471487	DFS paths on Windows and NetApp file servers included both forward slashes and back slashes.

Issue ID	Description
472391	An exception occurred during execution of Data Transport Engine rule, so that directories were not deleted and/or stubs were not created.
472897	When applying licenses, the Management Console displays mistaken license version warnings, rendering license application impossible.
473307	The recycle bin was included in the Permissions granted directly to user in Windows file system DatAlert rule, causing alerts to be generated on files and folders that were moved to it.
474159	Domain users could not be added to a group in NetApp CM.
474628	DatAdvantage upgrade failed due to missing columns in the ADPropConfig table.
474827	The FS history table was updated incorrectly, resulting in erroneous results for report 9.h.01.
476056	On an Exchange Online file server with new group types, the ADWalk job failed with errors.
476286	During upgrade, the transaction log for the Varonis database was completely filled if there was insufficient disk space and the Inodes table was very large.
476704	FileWalk failed with an arithmetic overflow recorded in the Event Log.
476775	Clean installation on SQL Server 2005 failed with an error in the Environment-sp.sql script.
477345	The Data Transport Engine failed when a rule having approximately 20M commands was run.
477429	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.
477546	DCF conditions became corrupted during upgrade.
477796	In the DCF, when DirIds were created for new results, it added entries into the Sorted Directory Tree tables of the wrong file servers.

Issue ID	Description
477807	GPO fetching was carried out per domain controller, not per domain.
478004	Known issue: As a result of architectural changes made by Microsoft in Exchange Server 2013, Delete Public Folder events are no longer supported by the Varonis agent.
478509	DFS shares could not be added to DataPrivilege as base folders.
478528	The DCF serviced stopped responding while trying to allocate more space in the dictionary matcher.
478605	The DCF Pulling Bounded Sync job ran for an inordinately long time, consuming CPU.
478732	When DFS shares were added as base folders in DataPrivilege and the DFS link pointed to C\$, an error message was received.
479082	Folders from temporary shares could not be added to DataPrivilege.
479205	Predefined rules triggered alerts on events that were not included in the dictionary.
479224	The DatAlert historical tool deleted old alerted events from environments on which it ran.
479385	Improvements to DatAlert's predefined rules help to prevent false positives.
479395	Improvements to DatAlert's predefined rules help to prevent false positives.
479529	The check constraint was removed from the ClickType column in the Click Audit tables.
479754	In the Management Console, an Exchange file server was added without a Crawled By value, even though a value was selected during configuration.
479779	Although the syslog method was configured and selected in the DatAlert UI, DatAlerts were not sent to the relevant server via syslog.
479985	When reports are exported to CSV through a subscription, column headers containing non-alphanumeric characters are replaced by underscores.

Issue ID	Description
480146	The upgrade failed due to a faulty stored procedure.
480503	NetApp CM shares could not be detected or scanned when the HTTPS protocol was configured.
480640	Duplicate column names were returned from a query in the DatAlert web interface.
481065	A check was added to ensure the Probe is online raising DoSyncProbe.
481078	Performance improvements were made to statistics calculation in DatAlert.
481243	It was not possible to edit or request permission on mount point folders that were defined as base folders in DataPrivilege.
481522	When the File properties filter was used with both sub-filters, File name and extension dictionary and Excluded file name and extension dictionary, report 1.a.08 was empty.
481772	A major slowdown in event collection occurred.
481987	Due to a faulty Windows API call, ADWalk stopped responding.
482679	A collation error occurred during upgrade.
482957	When editing a file server failed, the Shadow database was dropped.
483750	The AddLegacyExchangeDNMapping stored procedure now allows configuring a value for LegacyExchangeDN that is longer than 330 characters.
484407	The DatAlert publisher ignored updates to the working directory.
484710	The DatAlert Rule Prepare job stopped responding due to an issue with filters in the Where scope.
484761	The Missing Events notification ran using an incorrect NoEventsPeriod value.
484772	In DatAlert, GPO alerts were not identified correctly by the Publisher.

Issue ID	Description
484819	The DatAlert Delivery job failed if *.rta files were loaded more than once.
484836	The Pull AD Events job failed if two domains had the same configuration and events required special resolution.
484911	When French was the displayed language in an SQL lab, DatAlert jobs failed to respond.
484944	DatAlerts were not triggered properly, due to a faulty hash function.
485194	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 (-).
485210	"Mailbox permission added" and "Mailbox permission removed" PowerShell events are now supported on Exchange 2013.
485266	The "Excluded access path" filter did not function correctly in the DatAlert Where scope.
485272	A FIPS error occurred during detection of SharePoint site collections.
485338	DatAlert Analytics alerts were generated after the evaluation license expired.
485656	The grid could not be resized in the DatAlert web interface.
485780	The database stopped responding when the GetTargetComponentHostname stored procedure was called.
485840	The DataPrivilege searcher did not work with an impersonation user account from a different trusted domain.
486024	The Sync Owner job failed.
486104	Installation of DatAlert Analytics failed when FTP was present in IIS.
486450	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.

Issue ID	Description
486631	In an .rta file created from a CryptoRTA alert, the timestamp and UTC timestamp fields were mixed.
486794	It is now possible to disable VSS in the Windows agent.
490098	A FileWalk processing query in the spCollectorFWDDataTransformations stored procedure failed to complete its processing.
490107	The Data Transport Engine rule synchronization failed for rules that took over a month to execute.
490568	In large environments, the Probe upgrade took a very long time due to the deduplication script.
490963	Windows Server 2012 with Cluster Shared Volumes (CSV) crashes due to driver incompatibility.
491480	In DatAlert, the Where scope ran on decommissioned file servers.
491581	Incremental FileWalk was enabled unexpectedly after repair/upgrade.
493661	On VM machines with low resources, the UBA statistics calculation job ran for a very long time.
494177	The DatAlert Scope Delivery job ran for a very long time.
494279	The stored procedure that updates the IsParent column consumed too much CPU.
494344	The root step of the Collector's data transfer procedure ran with RCID=1, instead of -1.
494418	The DCF and DW Send Workload job has been optimized for resource cooperation efficiency.
494527	The DCF and DW Allocate DirId job is now run only by schedule and not by spDCF_SyncService.
494540	FileWalk failed due to an arithmetic overflow in the Probe database.

Issue ID	Description
494629	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.
494672	The Probe service stopped responding while printing to the log.
494746	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.
494845	Solr now stops indexing and processing files when there is less than 50 GB of free disk space.
495009	Events were filtered for Isilon file servers because their ID was reported incorrectly.
495088	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.
495159	DatAlert's crypto algorithm considered Create Directory events as if it were the parent directory that was created when rolling back counters.
495162	The DatAlert crypto algorithm did not consider delete events that followed read events.
495182	An Out-of-Memory error occurred while verifying a very large number of data transport rules.
495188	The suspected time and suspected events were missing from the raw alert data.
495189	An error occurred when a file server was added, due to a faulty stored procedure.
495193	Logging of the crypto algorithm was improved.
495195	Some changes to GPO settings were not collected.
495217	The timeout for the publisher pull configuration from the database was increased.

Issue ID	Description
495581	A faulty stored procedure did not allow processing of FileWalk data when an Exchange mailbox was deleted.
495594	The presence of the Affected object type filter had a negative impact on the performance of certain rules.
495632	Several issues with FileWalk scheduling occurred, including the creation of duplicate schedules, removal of schedules from FileWalk, and faulty InitArguments.
495694	Errors occurred during Data Transport Engine rule preparation when source groups were merged from different file servers.
495697	If there are many Active Directory objects and relations, the Data Transport Engine's Next Run screen might stop responding while calculating lost permissions.
495927	Following a successful upgrade, the incremental FileWalk lost its Next Run and schedule values.
496119	The list of database jobs was not properly displayed in the Management Console.
496179	The first-read and first-write filters were erroneously included in the documentation of NFS configuration for NetApp CM.
496236	Syslog identity has been removed from SIEM-oriented templates.
497539	The DCF and DatAnswers Monitor file counts did not include files that were skipped due to their size.
497681	Report 14a could not be generated for external rules imported with a CSV file.
498050	A primary key violation occurred while running the Pull Alerts job.
498071	When a Collector was installed to a non-default location, the installation path reverted to the default following upgrade.
498318	DatAlert performance was improved.

Issue ID	Description
498402	The DataPrivilege evaluation license removed the DatAdvantage permanent license when DataPrivilege was installed over an existing installation of DatAdvantage.
498509	Site collections were not identified when SharePoint sites were added.
498686	For the DatAlert web UI, Windows Server Update Services must be disabled for IIS.
498808	The Enterprise Installer sent multiple start commands to PublishingManagement, resulting in multiple standard DatAlerts on the same events and threshold alerts with the same alerted events.
498821	Report subscriptions failed if AD properties were added to the report columns.
498831	The Event Viewer raised an error even though no DatAlert rule was configured for any file server connected to the Probe/Collector.
499655	When a Unix Samba file server was added, DataPrivilege ceased to function correctly.
499868	DataPrivilege's subscriptionTest log was mistakenly placed in the wrong location.
500024	The DatAlert web UI displayed a browser error briefly at startup.
500044	An executable path that included quotation marks (") was not removed from the run queue because the quotation marks were treated as illegal characters.
500434	When DatAlert rules included privileged accounts in the Where scope, changes to the scope were only updated after the nightly jobs were run.
501473	The merge of published Exchanged data failed.
501641	The Events - Pull job did not include updating statistics for the relevant partitioned tables.
501795	The Who scope was deleted from DatAlert rules when Scope Delivery ran after PullAD/PullWalk.

Issue ID	Description
503681	An error occurred while publishing a DatAlert lockout alert.

6.2.66

Issue ID	Description
495797	The number of fetched GPOs listed in the Varonis event log equalled the number of monitored GCs, not the number GPOs in the domain.
495798	Some GPO setting modifications were not collected.
498440	Installation failed with an error due to a faulty SQL script.
498651	New GPO Object events were collected as Rename DS Object events.

6.2.63

Issue ID	Description
484471	The DatAlert Rule Prepare job stopped responding due to an issue with filters in the Where scope.
484544	When a file server was edited and deployment failed, the definition of the Shadow database was deleted.
484545	The DatAlert Publisher was triggered to begin working during installation, before the Working Directory registry value was set to the correct final value.
484550	Although the syslog method was configured and selected in the DatAlert UI, DatAlerts were not sent to the relevant server via syslog.
484551	Predefined rules triggered alerts on events that were not included in the dictionary.
484777	Improvements to DatAlert's predefined rules help to prevent false positives.
484905	When French was the displayed language in an SQL lab, DatAlert jobs failed to respond.

Issue ID	Description
486376	DatAlerts were not triggered properly, due to a faulty hash function.
486378	The "Excluded access path" filter did not function correctly in the DatAlert Where scope.
486629	In events alerted by the "Immediate pattern detected: user actions resemble ransomware" rule, the UTC timestamp and local timestamp were switched.
490092	A FileWalk processing query in the spCollectorFWDDataTransformations stored procedure failed to complete its processing.
490530	In large environments, the deduplication Probe upgrade script ran for a very long time.

6.2.62

Issue ID	Description
481771	A major slowdown in event collection occurred.

6.2.61

Issue ID	Description
477381	During upgrade to either 6.2.53 or 6.2.60, any user-defined DCF rule containing non-Latin characters was corrupted.

6.2.60

Issue ID	Description
447821	A DatAlert rule failed to run when the pathname of the folder in which the event occurred (in the Where (Affected Object) scope) included an upper case letter in Russian.
459153	A deadlock occurred during the Events - Archive job on an Exchange file server.

Issue ID	Description
455285	After changing a user's accountExpiry attribute to never expires, the Domain Controller's agent crashes.
458223	After security log events were collected in large volumes, the Varonis Agent caused the server to cease functioning.
458210	After the Remote Registry service was disabled on a DatAnswers server, upgrade failed.
459143	An error occurred in the DatAlert Analytics scope delivery job.
472324	An internal server error occurred and the DatAlert Web UI stopped functioning. The search session ID was generated using an encryption provider that was not FIPS-compliant.
452850	A performance issue occurred when the Archive job was run on a Unix file server with a large number of events.
463413	Dictionaries could be edited by users with the minimum role of "User."
454560	During upgrade to 6.2.35, an error occurred when DatAlert rules were created, updated, deleted or disabled, triggering the DatAlert Sync Dictionaries job.
468564	File event types were added to the "Encryption of multiple files" predefined rule.
461532	Following upgrade, the Users/Groups panes in the Work Area could not be loaded.
459719	In DatAlert, the Resource Type filter was removed from the Where scope for Shadow databases.
456809	In DataPrivilege, after a SharePoint site was added, the URL would wrongly include an extra backslash ("/") at the end, resulting in an inability to add SharePoint sites to DataPrivilege.
456810	In DataPrivilege, extra spaces at the start and at the end of a SharePoint URL were not removed, resulting an inability to add SharePoint sites to DataPrivilege.

Issue ID	Description
459136	In DataPrivilege, 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.
454766	In environments with many filtered users and SharePoint file servers with a large site collection, the The Sync Filtered users job took too much time.
455075	In report 13c, when merging source folders, the wrong source paths were displayed.
458627	In Report 2A, the Only Protected Folders and Distinguished Uniques filters caused the report to fail.
456528	In Report 4J, when the Share Name filter was selected, the report was displayed with Share Permission Sources column empty.
456333	In Reports, subscriptions with to/cc/bcc e-mail addresses with '!' as the first character were not saved.
457818	In the DatAlert Web UI, customers can now go from the object widgets at the top of the dashboard straight to the alerts drill down data, without opening the context card.
456708	In the Data Transport Engine, stub files were not copied from the Source folder to the Destination folder.
467420	In the Management Console, job schedules could not be edited in bulk.
450838	It took a long time to calculate the DatAlert scope when the Management status filter was selected from the Where (Affected Object) page.
466233	It was not possible to change the name of a permission type when the UI was set to French.
457476	New crypto extensions were added to the Encrypted Files dictionary.
454588	Report 4.g.02 failed to display several of the filters and values.
464897	Some reports did not function in French.

Issue ID	Description
455212	The ability to repull FileWalk data from the Probe to the Shadow database was disabled.
463483	The Access path filter did not work in SharePoint when a URL was displayed in the Access Path column in report 4f.
456307	The Alias feature did not resolve DFS links.
456739	The CAS Exchange Server was not monitored by the Probe or Collector.
460244	The Collector Events Delivery job did not compress file data prior to network delivery.
460547	The Collector Events Delivery job failed to load event files from the Collector.
446534	The Commit Engine failed to commit changes on a root directory in a NetApp Cluster-Mode file server.
459471	The crypto file dictionary was improved with additional values, and the removal of values that caused a high rate of false positives.
446915	The DatAlert Publisher Engine failed to resolve missing information.
474727	The DatAnswers Click Audit Import job failed in the month following upgrade.
446945	The DCF failed to scan a root share on a NetApp Cluster-Mode file server.
454572	The DFS Walk job failed to retrieve DFS links even though a DFS root was defined in the Management Console.
427270	The DP ADWalk job failed for local accounts on NetApp file servers.
450009	The Events Archive job failed to process temporary data for Active Directory Domain Services. Group Policy Objects on the site were not scanned by FileWalk.
472034	The Events - Collector Events Delivery job failed while transferring a file using the Varonis Service on the Collector.

Issue ID	Description
445178	The Event Type filter in the What (Event Details) page of the Add Rule dialog box can be used only once.
429583	The ExpiredRelationsJob failed and an error message was received.
459895	The file server picker returned different file servers than those that were selected.
467416	The FileWalk job continued to run on a Collector after the Probe failed over.
460156	The hour was missing from the Alerted Events grid, at the event level.
457153	The jump action from the Alerts page to the Alerted Events page was missing from the DatAlert Analytics Web UI.
457783	The latest events with a future timestamp were not displayed for file servers in a (future) time zone.
458942	The performance of the Management Console job display was improved.
463636	The PullWalk job did not correctly rename tables before pulling them to the Shadow.
463712	The report documentation erroneously included some column names in report 3.d.01.
459956	There was no global date format available for the @startDate and @endDate parameters in the DataPrivilege advanced search.
451553	The rule publisher service wrote events of the same threshold rule to one .rta file, even though the events originated from different file servers.
392031	The Security Certificate File Types rule, which detects security certificate files, now searches for additional file types for the DCF and DatAnswers.
453070	The subfolders under the MSI folder were renamed to exclude the word "Beta".
463388	The upgrade process triggered a rescan of predefined threshold rules.

Issue ID	Description
465963	To reduce the number of false positives, the terms "account" and "license" were removed from the Credentials Files dictionary.
440030	Upon upgrade from 6.0.112 to 6.2.15, the Collector failed to connect to the NetApp Cluster-Mode file server.
453091	Upon upgrade from 6.1.112 to 6.2.35, the RTA Notify job failed and an error message was received.
465329	Values were added to the crypto files dictionaries to improve ransomware detection capabilities.
463489	Values were added to the DatAlert Analytics dictionaries to improve the effectiveness of the user behavior analysis.
450560	VaronisFilterHandler.exe stopped responding when an attempt was made to terminate the process.
449605	When a DatAlert rule was created and the Directory Name filter was applied, it took a long time for the Rule Prepare job to calculate the folders. The performance of the Rule Prepare job is now improved, no longer calculating historical folders.
439934	When a Data Transport rule was created and the Files Activity filter was added to the file scope, newly created files with no events were erroneously moved to the destination. To fix this issue, when the Files Activity filter is added to a file scope, a default filter (Date created < 1 week) will also be applied to the scope.
457621	When AdWalk was run on a domain using ADSI, it did not display the same results as LDAP.
460583	When a file was opened for read/write on an EMC server, only a "file open write" event was generated.
465348	When a folder was added to DataPrivilege with a DFS path, the folder synchronization stopped responding at the Pending stage.
455434	When loading real-time alerts, an error was displayed.
450631	When new tables were created after a month, creating new permissions tables failed.

Issue ID	Description
455747	When the KeyTable was used by several database processes simultaneously, it caused those processes to slow down and cease functioning.
454663	When the tempdb filled up from a huge amount of events, the PullCIFS, PullWalk, and PullDCF jobs ran for days.
454398	While attempting to delete events from the Filtered Users window in the Management Console, an error was received when the Purge Existing Data option was selected.
434497	While DataPrivilege was unavailable in some environments, the error messages seemed to be unrelated to its availability.
454102	While installing SharePoint Online and adding sites through the File Server Wizard, an exception was thrown and the wrong error message was displayed.

6.2.53

Issue ID	Description
463383	The Collector's Event Delivery job did not compress file data prior to network delivery.
463177	Upgrading from version 6.2.50 or higher triggered a rescan of predefined threshold rules.

6.2.52

Issue ID	Description
463082	The PullAD job failed with an error on directory service events because some default event tables were not created during installation.

6.2.51

Issue ID	Description
329400	After a subscription was created in reports, if the report had special characters (i.e. single quote, double quotes, comma, etc.), the subscription generated a file with incorrect data.
368306	Multiple files created by the subscriptions CSV files were put in the same location.
402475	In cases where Exchange was a cluster server, the Exchange Agent automatic instalaltion failed.
411317	The ADWalk job failed on a DataPrivilege domain update when the domain does not exist.
414673	In DataADvantage, after selecting a NetApp CM local host as the domain, the commit operation failed.
419446	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.
420373	When the DCF received a directory from SharePoint whose path name was more than 260 characters, the scan stopped functioning.
423700	In the DCF, duplicated file entries from the same directory caused memory problems.
429533	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.
430155	When there were more than 2147483647 files on one file server, an SQL error occurred during calculation of the files count, and the trend reports displayed the wrong data.
433222	In the DCF, using the user/group filters generated the wrong results.
434164	A performance issue occurred while event archive jobs were running on NFS directories.
434502	In DatAnywhere, Pull Events, Exchange DN or email identifiers longer than 324 characters caused instability.

Issue ID	Description
435825	A DCF Service error occurred when a Null value was inserted as the SSH file user name and password.
437323	Report 4d.01 failed with an error message after selecting filters "File server" and "Trustee account type".
437453	The tempdb fills up when the PullCIFS, PullWalk, and PullDCF jobs ran for days calculating SDT Stack.
437649	The Events Deletion job was optimized to accommodate a large amount of tables.
438054	In DatAdvantage, when many events accumulated in a file from more than one day, the Events Collection job failed with a deadlock.
438101	After running report 12j as a folder or group owner, a database error message was displayed.
438214	In the DCF, pattern matching improvements were made that enabled quicker scanning of files 20 MB and larger.
438308	When the Events - Archive job executed simultaneously with the Events - Rename Hourly (RT) Tables job, view creation in the latest CIFS tables was updated.
438746	The Analytics Engine was modified to work faster.
439125	DataPrivilege failed to retrieve the list of file servers when a NetApp cluster was configured.
439938	During Repair/Upgrade, FileWalk 's schedule was able to be duplicated and therefore caused scheduling inconsistencies.
440613	In report 7.b.1, after the file server and object type contained in site filters were added, the report did not generate results.
440647	In reports 4.g.1 and 4.f.1, it is possible to display a valid SharePoint URL.
440650	In the Managed Folder User Level Permissions report, after the Expiration Date filter was added, the permissions set to expire are no longer displayed in the report.

Issue ID	Description
440883	The Sync Probe Proxy job was not synchronized with the changes in the Filer Proxy table, and caused performance issues in the events collection and crawling functions.
441338	The Sync Probe Proxy job was not synchronized with the changes in the Filer Proxy table, and caused performance issues in the events collection and crawling functions.
442599	In DA Security in the Management Console's Configuration screen, after a local user from an unmonitored domain was added and saved, the added user disappeared.
442646	When upgrading DatAnswers to version 6.2, the ZK service got stuck while in "stopping" status.
442911	In DataAdvantage, the Collector FileWalk Data Processing job failed due to unique constraint violations in related tables.
443058	In report 12h, if the Group Name filter was selected, an error message was displayed after running the report.
443826	The Subscription DateTime format ID was wrong, thereby preventing any format changes.
444082	In DataAdvantage, the Events – Pull job took an excessively long time to run.
444650	DataPrivilege reports did not work when using customized themes.
444995	In DataPrivilege, when there were no authorizers for emails, mail was sent to the folder's owner only when the folder was a base folder.
445110	Report 6.b.01 failed to generate when using the non-USA date format (dd.mm.yyyy).
445203	In an environment without MS Visual C++ runtime, the event collection agent was unable to start.
445550	In DataAlert, after creating a rule from the Log tab, the What scope remained empty, or the application crashed.

Issue ID	Description
445792	After installing version 6.2.15, viewing the license information in Help > About resulted in an error message. After the error, the Help > About screen displayed a blank serial, no products, and an incorrect email address.
446784	In DatAlert Analytics, in the exploitation tools dictionary, the value canvase.* was changed to canvas.bat and *canvas.py in order to eliminate false positives.
447180	DatAdvantage failed to commit group creation operations in an environment where there are shut-down file servers.
447496	On file servers with names of more than 32 characters, the commit process didn't work.
447667	After the Management Console was installed, and the folder to which %temp% is pointed was deleted, the Management Console displayed error messages.
447861	FileWalk stopped functioning when the special files input was too large.
448959	When running DatAlert with Exchange 2013, the Exchange resource mailboxes in the Review Area were unable to expand.
449186	In DatAnswers, some domain users' display names contained a new-line character, resulting in Solr caches failing to load and DatAnswers not returning results.
449282	DatAnywhere ignored deny and share permissions, resulting in invalid search results.
449872	On an upgrade from a version that contained the LogicalShadow database, the installer was unable to recreate it and so failed as a result.
449955	The DatAdvantage UI only supports text at a zoom level of 100%.
450002	When copying from Windows to Sharepoint file servers, inherited permissions on the unique folders were not copied.
450076	Commit operations on Exchange file servers failed if UAC was enabled.
450427	In reports 2.e.1 and 2f, when either the Acting Object Type or Acting Users From Group filters were selected, no results were generated.

Issue ID	Description
450451	In the recon tools dictionary, the term *SET* was replaced by a list of more specific and detailed terms.
450559	When an unsupported Unix file server was added via PowerShell, the Filewalk method stayed Varonis instead of switching to NFS.
450581	When the jobs' execution overlapped with the retention policy, the jobs were displayed in the Management Console as never run, and the jobs failed without any error notification.
450631	When new tables were created after a month, creating new permissions tables failed.
450884	During upgrade, an upgrade script added column UTCTimestamp to all events tables.
450994	In DatAlert, when the Real-Time Alerts ran at the same times as RW Publishing, some Where scopes could not be calculated and an error message was displayed.
451122	Metabase 6 compatibility must be configured to enable use of IIS on Windows 2003.
451125	The characters () and [] in regex patterns prevented the patterns from being counted as hits.
451452	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
451515	The Reporting API msi files were not able to be installed together with the DatAlert.Web msi files since they both use the same upgrade code.
451552	The Publisher wrote all events of the same threshold rule to the same .rta file even if they originated in different file servers.
451758	In DatAdvantage or DataPrivilege, after clicking the IDU database in Existing Products, there was no error message that indicated the application was already installed.
451940	DatAlert Analytics failed to be installed or upgrade to 6.2.35 or 6.2.36 when MS SQL 2005 was in use.

Issue ID	Description
453334	Installed versions of the Bulk Upload Utility did not match the version of DataPrivilege.
453357	In DataAlert Analytics crashed on versions prior to 6.0.100 when lockout tables did not exist.
453431	Opening the security.config.cch files created an alert.
453492	In DataAlert Analytics, after much renaming was performed in a single day, the excessive data in the database caused calculations to stop working.
453631	In the DataAlert web interface, in the Alerted Events screen, the default columns were changed.
453655	In DataPrivilege, groups could not be created in organizational units whose names included a plus (+) character.
453848	After upgrade, the Events-Archive job failed when the daily events table exists in the Varonis database but not in the CIFS_Archive metadata table.
454160	The Encrypted Files dictionary has been expanded in order to include new values.
454293	In DataADvantage, after Traverse permissions were selected, they were given without list permissions.
455117	In DataPrivilege, in Configuration, when reviewing a folder permission request, the Custom ADProperty value was empty.
455519	When trying to scan sites in the SharePoint file server, an error message was displayed.
455804	To monitor GPO change events, the primary language of the Probe server's operating system should be English (GPMC report output must be in English).
456376	In the Data Transport Engine, copying data from a SharePoint site to a Windows folder was extremely slow.
456538	A long authorization token made the request header too big for the server to work with, resulting in a failed request and a blank UI.

Issue ID	Description
456772	In the Data Transport Engine, after creating a rule that copies several Sharepoint file servers into a single destination, the document directories became "roots" and some folders were not able to be copied.
457032	In DatAlert, when there were a lot of site collections and mapped local SharePoint objects, the RTA Rule Prepare stopped functioning when the Who scope was calculated.
457617	The wrong IP address information was displayed on log reports.
457640	The VrmsCifsQueue stopped functioning when performing a large amount of Change Security events.

6.2.38

Issue ID	Description
453250	Several DatAlert Analytics dictionary values were likely to create false positives. The following values have been removed from the dictionaries: • Crypto files • ReadMe.txt • README1.txt • README2.txt • README3.txt • README4.txt • README5.txt • README6.txt • README7.txt • README8.txt • README9.txt • README10.txt • recovery*.* • _ReCoVeRy_*.* • message.txt • Reconnaissance tools • *SET*.* • Exploitation tools • SET.* • ps.exe • canvas.*
454599	Installed versions of the Bulk Upload Utility did not match the version of DataPrivilege.

Issue ID	Description
454615	The AIX agent's event daemon failed to start, resulting in the inability to monitor events on AIX servers.

6.2.37

Issue ID	Description
451939	DatAdvantage failed to be installed or upgrade to 6.2.35 or 6.2.36 when MS SQL 2005 was in use.
452652	During installation of DatAdvantage or DataPrivilege, no validation of existing products was performed. As a result, installation was able to continue for an already-installed product and the existing installation stopped functioning.

6.2.36

N/A

6.2.35

Issue ID	Description
358554	In DatAdvantage, in the Log tab, out-of-memory exceptions were caused when large amounts of log search data was exported.
371986	Different SQL versions on the Probe (2005) and Shadow (2008\R2) caused an "ARITHABORT" message during the DCF's pull job.
391175	The Events - Archive job on Exchange occasionally caused duplication between similar folders, if the only difference between the folders was an extra space.
403114	In DatAlert, the <i>Modification: Hosts</i> file path in the <i>included access paths</i> filter contained a backslash ("\") at the end.
403209	In SharePoint, hostnamed site collections were not grouped by host.
403969	In DatAdvantage, the email sent by the <i>Administrative or service account disabled or deleted</i> rule did not specify the account which was disabled/deleted.

Issue ID	Description
404096	The SHS walk on the NetApp file server did not retrieve “no browse” shares.
405362	DatAdvantage reports stopped responding when a filter value contained special characters.
406011	Installation failed if the cluster had no disk resources.
410470	ToolTips were not displayed on mouse-over for DatAlert rule filters.
412376	It took FileWalk took several hours to complete scanning file server directories with millions of symbolic links, to be terminated by the FileWalk monitor which interpreted it as “stuck”.
413636	The Skip database file copy option was missing from the shadow migration process.
421626	In Directory Services, no errors were printed to corrupted domain controller security logs.
422168	The uninstallation process failed if recab was done to a build before release.
425453	The DatAlert Analytics Calc Stats job stopped responding when it ran on a very large number of events (~54 million).
432085	The license key was not displayed in the license key area after installing 6.0.107 and then upgrading to 6.2.3.
432387	In DatAlert, the defined limitation for email notifications was ignored.
434498	In DatAdvantage, after Data Driven Reports Subscription was set to <i>save output to file share</i> , owner-created folders were missing permissions for the owner's user.
436872	Syslog alerts were not filtered from the logger.
437003	An error message is displayed after editing binding for a SharePoint site and then opening the actual site.
439418	Additional values were added to the DatAlert Analytics dictionaries.

Issue ID	Description
439662	DataPrivilege failed to retrieve the list of file servers when a NetApp cluster was configured.
439799	The DatAlert Analytics Calc Stats failed when a new events_stats table was created after a month.
439967	For Windows 2000 file servers, the Enterprise Installer installs an older version of the Varonis Windows Agent. A separate MSI is also provided, for manual installation of the older agent.
440500	A duplicate key was inserted in the session and notifications database tables.
441570	The fixDomainIDent stored procedure was missing after a Windows file server was added.
443247	The IDU Server stopped responding in large environments while deleting file servers or stopping jobs.
443421	The "IsDecommissioned" property for a file server was not transferred to the Probe database.
443715	A primary key constraint could not be created due to a faulty stored procedure.
444361	"Missing events" notification was not sent for directory services resources.
447060	The insertion of a huge number of Create events into the database exploded the SQL Server transaction log.

6.2.15

Issue ID	Description
316146	DataPrivilege reports failed when they were run from within the application.
358941	Unnecessary SSH connection attempts were made.
382277	Groups were able to inherit permissions from abstract groups.
383642	Site detection failed due to special IIS binding.

Issue ID	Description
393239	In DatAdvantage, report subscriptions now support exporting to the XLSX format, in addition to XLS.
393544	A search for archived data did not return results for the specified dates.
393888	It is now possible to define aliases for each CIFS file server defined in the Management Console.
394489	Poor performance followed by a timeout occurred when RDLs or templates were uploaded to the Reports site.
396873	The status of a CSV volume was changed to restricted access when the volume was moved to a different node and then moved back again.
397918	Statistics tables are now updated during the Maintenance job.
397933	SSH connections failed when event collection was enabled.
398305	SIDs were not resolved during OS detection when the Explorer SDK was in use.
398706	During event resolution, a new connection was unnecessarily opened from the core resolver to the DC.
403098	DFSWalk did not support DFS roots that point to DFS logical folders.
403179	Setting LogMaxSize in the logging.config file of the Probe/Collector to a value larger than 32767 (short) caused it to use the maximum value of 256MB on service restart.
403457	An error message was improved in the Varonis Support Assistant.
404610	The temporary report subscriptions that are created when a data-driven report is run were included in the operational logs.
405142	The Remove Permissions option was not present for all relevant users.
405416	Users whose accounts were locked out were not included in reports.
406329	Logon events were not retrieved for the Archive window in DatAdvantage.

Issue ID	Description
406332	The FileWalk job failed while processing an Active Directory server due object duplication.
406649	A duplicate key was found in the 'dbo.DA_AuthorizerDIR' table.
407815	SharePoint Office 365 groups were not resolved in the Azure domain.
409179	The DCF Lite license was converted to a full license on upgrade.
409598	When the DatAdvantage UI was opened by a user that had no permissions, a null reference exception was logged in the event viewer along with an Access Denied error.
409647	Azure users who were mapped to Active Directory had no effective permissions on SharePoint Online objects, even though permission levels were assigned to them on the site.
410266	Shares were detected as NFS even though they were NT.
410956	An invalid column name was encountered by the Events - Archive job following upgrade.
411823	DatAlert rules ran only on parent domains, not child domains.
412281	The list of products that are not supported by license was added to the licensing error message.
412507	FileWalk stopped responding when it encountered snapshot folders.
413370	A deadlock error occurred in the spDCF_GetClassificationDataDone stored procedure.
415029	Report 8d failed to execute due to a faulty internal procedure.
418246	Report 9i now calculates stale data based on physical size rather than logical size.
419489	ADWalk stopped responding with a Max Recursion error.
423062	FileWalk incorrectly identified NTFS shares on a NetApp cluster as NFS.

Issue ID	Description
423814	The Data Transport Engine did not delete source files although the rule was configured to do so.
424112	In the Data Transport Engine, the merge of a very large number of files (250K) that already existed at the target took a very long time because a warning was written to the event log regarding each existing file.
424250	The performance of report 3a was negatively affected in very large environments (1 million users, 1 million relations).
424558	No results were returned for the parent Folder User Access Log.
427432	Migration of a directory service container to a SQL Alwayson database failed.
428378	The local database was not installed during upgrade from versions older than 6.1.30 to 6.2.x.
429012	An integer overflow occurred in the spAddSuspiciousUser stored procedure.
430393	A new configuration option has been added to varonis.config. The <i>DfsEnableDfsFolderCrawl</i> option can now be set to show DFS folders that link to other DFS folders that reside at a different root.
431554	Report 1a failed when the 'Affected group type' filter was used.
434408	Migration failed on the ALTER DATABASE command because the instance name was added before [vrnsDomainDB]
435553	The Dispatcher lost asynchronous jobs on recovery when there was no access to the database.
436280	If DataAdvantage was upgraded to 6.2.x and then DataPrivilege was later installed and there were owners defined in DatAdvantage, the PullWalks and DataPrivilege Sync Owners jobs failed.

6.2.10

Issue ID	Description
366934	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.
380674	In DatAdvantage, after resolved issues with corrupt FileWalk data, previously-defined flags were missing.
381289	In DatAdvantage, a new Azure AD domain name with the same name as the local Active Directory domain name was allowed to be saved.
391319	In DatAnswers, events arrived with both regular filenames and with upper-case filenames for the same file, even if the file had not been renamed.
392148	In DatAdvantage, PullAD crashed when trying to insert an SID as new in history for the same SID of a pruned and deleted user that had history records.
393254	In DatAdvantage, when report 7b (Inactive Directories by Size) was run with the <i>Display Inactive Folders Only if all Their Subfolders are Inactive</i> filter, the report took a long time to generate.
393743	In the DCF, information about the UK electoral pattern incorrectly included information about the French national identification number.
394735	In DatAdvantage, a lack of synchronization between event collection processes and the Probe missing events check caused a false missing events notification to be sent by email.
395133	CIFS FileWalk still checked the CheckCycleGuard parameter in filewalk.exe.varonis.config even after the parameter was disabled.
395885	Using the <i>ResolveHostIp</i> setting in Data Transport Engine caused rules to fail if copying shares.
396657	In DatAdvantage, the resource monitor automatic detection added deleted or inaccessible volumes to the ResourceDetected database table.
397242	In DatAdvantage, an error in the Event Viewer was received when running a search in the Log tab, and then adding and grouping the Classification Results column.

Issue ID	Description
398600	The DatAlert Publisher used an older and non-updated dll that caused faulty and unexpected behavior.
399332	In DatAdvantage, in the DCF Monitor tab, the screen indicated that a large percentage of DCF rules were still pending even after all file servers with enable schedule completed.
399986	In DatAdvantage, the Probe did not reconnect to a disconnected NetApp Cluster Mode file server.
400417	After upgrading DatAdvantage, the Collector failed to connect to one or more file servers.
401507	In DatAdvantage, in report 2c, the FileType column contained both upper-case and lower-case file extensions and the results were separated by case.
403553	In the Data Transport Engine, export to CSV failed when the source folder scope contained a lot of entries.
404759	In DatAdvantage, after an SQL downgrade, a missing corresponding table in <i>Hist__Archive</i> caused the related Partition View to be improperly created, and so the Events-Pull job failed.
407838	After DatAnswers was uninstalled, a general slowdown in FileWalk occurred due to not removing the <i>Admin_Unique_Read_Perm_Files</i> key, which brings unique file permissions used by FileWalk.
407881	The DCF service did not run after .NET Framework was installed.
408272	In the Data Transport Engine, rules got stuck after running, and commands failed.
408712	In DatAdvantage, the Probe did not use the proxy to connect to NetApp.
410629	In DatAdvantage, in the organizational unit whose name contains <i>service</i> , most of the users were detected as <i>service</i> , instead of <i>personal</i> , therefore harming the results.
412390	In DatAdvantage version 6.1.33, after the time was changed, upgrading to version 6.2.6 failed.
413033	DatAnswer data remained in the database tables after uninstalling.

Issue ID	Description
414787	In the DCF, when DirIds were created for new results, it added entries into the Sorted Directory Tree tables of the wrong file servers.
421115	In DatAdvantage, in environments that used MS-SQL standard edition, a crash occurred due to faulty table structure.
421170	In DataAlert, UBA statistics did not calculate Velocity events on clean installation.
421565	Upgrade failed due to a faulty SQL script.
423056	The PullWalk job failed with error messages.
424305	Distributed FileWalk Exchange was not configured following upgrade.

6.2.6

Issue ID	Description
408576	The Varonis Customer Support Assistant Tool did not function correctly after upgrading from 6.2.3.

6.2.5

Issue ID	Description
399662	Following upgrade from 6.1.30, the Autodetect Resources job disabled crawling of existing volumes.

6.2.3

Issue ID	Description
211802	The Shadow database file was created in the IDU database location even though the default location was changed.
213596	Only the first line of a migration token could be pasted when its text contained multiple lines.

Issue ID	Description
316616	It was not possible to terminate a report that was already running.
317051	When the Where scope of a DataAlert rule was set to Folder, DataAlerts were generated for both files and folders.
322447	FPolicy was automatically re-enabled on a NetApp file server after it was disabled.
324871	It was not possible to install a Windows file server using Windows SQL credentials.
324881	When the IDU Server was restarted and the database was busy, a timeout occurred and the spJob_LoadRunningExecutions stored procedure failed to recover jobs.
325499	When a web application contained 100,000 site collections, the automatic detection of sites failed.
326258	While trying to access a SharePoint site collection, the Open events module generated an error.
330503	The Installer failed to upgrade the Probe database when the Varonis service account was used.
332958	An error occurred while migrating a file server to another Probe.
333282	A Windows file server could not be added to the list of monitored file servers. As a result, the Probe service stopped functioning.
333875	The upgrade of a NFS file server failed due to a duplicate key error.
334780	Exchange mailbox names were not resolved properly in the Exchange DataAlert.
335180	IDU Analytics discarded events occurring below the fifth level of the file system, instead of assigning them to level 5.
335545	False access denied events were recorded on a Windows Server 2003 with NetApp iSCSI drives.
335768	Upon upgrade, the link on the License Upgrade screen was incorrect.

Issue ID	Description
336295	The downgrade patch now accesses sys.sql_expression_dependencies only on SQL Server 2008 and higher.
354057	The Collector service stopped functioning when the affected object added to a DataAlert rule contained a large amount of shares.
354979	FileWalk required a long time to run due to a large number of snapshot directories that could not be pruned directly through the Management Console.
358276	A performance issue occurred while expanding a file server and its folders in the Work Area. This occurred due to the large size of a data transport rule.
358410	An error occurred while exporting a report to CSV because the SAM Account Name column appeared twice.
358488	Events were printed to the AD_EVENTS table in the Collector with line breaks, which resulted in failure to insert data to the database.
358608	No error was returned when the deployment process failed to start for a file server.
359249	The AIX Varonis driver succeeded to load only if it was reinstalled after being rebooted.
359694	The Management Console failed to display the updated IP address of a SharePoint file server.
359696	A performance issue occurred during the migration of a file server from one Collector to another.
369996	The Redistribute script tool erroneously replaced VrmsDomainDB with the name of the server entered during authentication.
370027	The builders for the Delivery Engine Task Type relied on the IP address supplied by DatAdvantage instead of the hostname.
371144	When the name of a indexed file is capitalized, DatAnswers fails to retrieve results containing this document.
371205	The spJob_FileWalkExecutionBuilder stored procedure returned an error when the Session ID contained more than 10 digits.

Issue ID	Description
371824	When the Logs folder was removed, the DatAnswers UI could not be uninstalled.
371994	No error was returned by the Pull AD job when the DataPrivilege system user could not be created.
372352	A stub file created by the Data Transport Engine failed to include Creator Owner permissions.
373196	For Isilon, local accounts could not be resolved.
374267	GPO installation instructions have been updated.
374798	A prerequisite check was added to DatAnswers installation to ensure the target website is running.
375181	If the name of an organizational unit contained a pound character (#), a backslash character (\) was prefixed to the name.
375220	The first run of the file server synchronization process failed with a timeout.
377500	The New Jersey Driver's License DCF pattern was corrected.
377942	In trying to add a folder to the Unmonitored Folders list, an error was returned stating the folder was already listed in the database.
378687	Report processes that were run on remote Shadow databases were not terminated, although their reports were.
378951	The Delivery Engine relied on the IP address provided by DatAdvantage, not the host name.
379783	A performance issue occurred when the DCF scanned a particular file.
380269	Custom FileWalk schedules were reset to "None" after a new file server was added.
380474	The Probe failed to remain connected to the DS Proxy (installed on the DC).

Issue ID	Description
381092	Consideration of Active Directory and Exchange containers has been removed from the pulling of logon events.
381093	Poor performance occurred during authentication and access requests.
382402	A primary key violation occurred while adding new Active Directory attributes in the Management Console.
382756	The DCF failed to extract text or metadata.
382982	Detection of an Isilon server failed when the HTTP web service could not be accessed.
383880	An index was added to the daily table to improve performance of CIFS archiving.
384061	If a target folder already had an owner who was assigned by someone other than the user running the Data Transport Engine, and a rule was executed that included copying ownership, the Rule Sync job stopped responding due to a duplicate key violation.
385296	Report 9.h.01 failed to run when Relative mode was selected for the Date filter.
386510	The presence of duplicate site IDs in SharePoint Online resulted in problems scanning the folder structure.
386814	A primary key violation occurred on the SecSearch_Shares table.
386874	The Exchange agent caused the store service to stop responding during multiple dump creation.
392689	The Data Transport Engine experienced performance degradation while copying a very large number of folders.
393258	Performance of event archiving for Active Directory has been improved.
395557	Related to Varonis Production. No docsummary needed.
395727	The DatAnswers Import Click Audit job failed repeatedly while attempting to insert a Null value into the database.

Known Issues

6.2.85

Issue ID	Description
523384	In SharePoint On Premises, SharePoint Online and OneDrive, the maximum number of site collections that can be detected by the Management Console or the Enterprise Installer is 12,000.

6.2.80

Issue ID	Description
481394	In reports 16.b, 14.i, and 6.c, when the report runs as a subscription and is sent either as a Web page or PDF, some user names are not displayed in the results.

6.2.74

N/A

6.2.73

N/A

6.2.72

N/A

6.2.71

Issue ID	Description
478004	As a result of architectural changes made by Microsoft in Exchange Server 2013, Delete Public Folder events are no longer supported by the Varonis agent.
503632	DataPrivilege reports are not deployed when the Report Deployment Tool is set to <i>All</i> and then used to deploy reports on a different reporting server. In this scenario, DatAdvantage reports are deployed as expected.
503673	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.

6.2.66

N/A

6.2.63

N/A

6.2.62

N/A

6.2.61

N/A

6.2.60

Issue ID	Description
395414	As a result of architectural changes made by Microsoft in Exchange Server 2013, Delete Public Folder events are no longer supported by the Varonis agent.
455328	Local (Windows) account permission visibility and commit are not supported on Unix SMB servers.
465428	When DatAdvantage and DataPrivilege 6.0.112 are both installed, and only DatAdvantage is upgraded to 6.2.60, DataPrivilege is not available in the list of products. Users who want to uninstall DataPrivilege must navigate back and then forward in the Enterprise Installer to enable selection of DataPrivilege.
469522	When the value in the Access path field is set to a URL, the Log view contains the following: * Simple mode - Shows the Display Name in the Path column * Advanced mode - Shows the URL in the Path column
469528	The "Or" operation between Access path fields and other fields is no longer available in the following reports: 1a, log, 4a, 4d, 4j, 4k, 4o, 5a, 5c, 6b, 8b, 9h, 12k, 12j. Note: Users can still create "OR" queries between access paths.
469534	When the value in the Access path field for SharePoint objects is set to a URL, the user must enter the full URL (and not only part of it as in other cases) when using the "Like" or "Starts With" operator in the Access Path filter.
474697	After importing report subscriptions to DataPrivilege using the Report Subscription tool, the web browser should be reopened.

6.2.53

N/A

6.2.52

N/A

6.2.51

Issue ID	Description
435536	When a trusted domain that had a base folder in DataPrivilege is removed, the base folder that was added is still managed as if the domain were not removed. Automatic and authorization rules are deleted for those folders.
439135	In NetApp CM, the Account Management > Delete Group operation has not been implemented.
445384	In this version, DataPrivilege does not support local groups.
450046	When a new user is added through the Enterprise Installer (Configuration > Database Users), the user's SID might be displayed instead of the user name in the Management Console DatAdvantage Security tab until the next run of ADWalk.
451393	If there is no valid URL, the display name will always be presented in the Access Path column in reports.
453927	In the following scenario, ownership synchronization between DatAdvantage and DataPrivilege will not work: * Install DatAdvantage and DataPrivilege 6.0.112. * Log in as Administrator and add <Folder1> with <Owner1>. * Wait for Owner Synchronization to finish. * Upgrade only DatAdvantage to 6.2.50. * Uninstall DataPrivilege. * Install DataPrivilege 6.2.50.
454093	Events generated in very short (fractions of seconds) SSH sessions may not include the IP address.
456163	In the Data Transport Engine, copying from Windows to SharePoint does not copy permissions that apply only to files. This will be fixed in a coming version.
456327	The ability to display source IP in events is only available with the agent provided in 6.2.50. It is not available if a lower-version agent is used.
456754	Following upgrade from 6.0.x or lower, if FileWalk has not yet run on SharePoint 2013, the Edit permission is set only to be visible in DataPrivilege. It is not configured with the "monitored," "can be committed" and "visible" attributes. The issue is resolved following the first run of both FileWalk and PullWalk.

Issue ID	Description
458947	During clean installation with a distributed Probe, if the user proceeds through the wizard up to the Install button, and then clicks Back to change the location of the Probe server, and then proceeds with the installation, the installation finishes with an error. However, the error is only reported in the Event Viewer; the installation appears to finish successfully.
454368	When there are more than 10,000 folders on a file server, the UI might stop responding when a new base folder is added to DataPrivilege through the folder picker.
332873	Following clean installation, the "Edit Permission" option is missing from the context menu in the Work Area Directories pane. The UI must be closed and reopened to enable this option.

6.2.38

N/A

6.2.37

N/A

6.2.36

N/A

6.2.35

Issue ID	Description
404947	In DatAlert, changes on many objects may result in several alerts.
426405	In Linux, events done directly on the terminal display an unknown IP address.
427522	If a user was once detected as having a privileged account and then manually changed to having no type of privileged account, neither the user nor its history is visible on the Privileged Account Discovery screen. To view its history, the user may be assigned a privileged account temporarily for the purposes of detection, and then lose the privileged status (through manual removal) after its history has been viewed.
430137	The first event after the SharePoint server is restarted will not have an IP address.
432337	DatAlert Analytics does not currently support IP addresses for events from XenDesktop.

Issue ID	Description
432387	Configuration changes, including rule changes, reset all counting regarding threshold type alerts and the <i>suppress mail message</i> setting.
434131	On Probe startup, SMTP info is sent to the Probe. A failure message is sent, even though the operation succeeds.
437206	When Windows IPV6 and IPV4 are enabled, the IP address is retrieved inconsistently in SharePoint on-premises environments.
438612	EMC Celerra folders cannot be synchronized to DataPrivilege until the next execution of the nightly jobs (FileWalk and PullWalk) if the folders are added while the full FileWalk is running.
441231	On Probe startup, SMTP info is sent to the Probe. A failure message is sent, even though the operation succeeds.
441506	Rolled-up grouping values for cells with multiple entries are empty.
442496	In the DatAlert web UI, context cards are not available for deleted items.
442868	In the DatAlert web UI, it is not possible to open a user context card from the Manager or FS Owner columns in the Alerted Events grid.
445223	Report 1a shows several lines for aggregated events when displaying alert details.

6.2.15

Issue ID	Description
435105	When a trusted domain that had a base folder in DataPrivilege is removed, the base folder that was added is still managed as if the domain were not removed. Automatic and authorization rules are deleted for those folders.
413989	Incremental File Walk on DataPrivilege is not supported for any share that is part of a file server that has at least one share for which the crawling method is defined as Mixed or NFS. Such managed folders are only scanned as part of the full FileWalk execution.

Issue ID	Description
436716	After installing DatAdvantage alone, upgrading it to 6.2.15.68 and then installing that version of DataPrivilege, incremental synchronization fails. This occurs because the Sync Probe configuration job is not run after DataPrivilege is installed. To avoid the issue, run the job manually after installation.
436718	After upgrading a DatAdvantage-only installation to 6.2.15.68 and then performing a clean installation of DataPrivilege to the same version, the DataPrivilege Administrator user is lacking the DatAdvantage System Administrator user role. It must be added manually to the DatAdvantage security settings in the Management Console.

6.2.10

Issue ID	Description
410231	The <i>Possible asset exposure</i> UBA rule only alerts on adding permissions to new users or groups. It does not alert when existing permissions are increased.
417281	In DataPrivilege, if the owner of a local group was added in previous versions, it will not be removed.
422448	On Probe startup, SMTP info is sent to the Probe. A failure message is sent, even though the operation succeeds.

6.2.6

N/A

6.2.5

Issue ID	Description
394773	The Access paths filter should only be used to filter folders, notfiles. The File properties filter can be used to filter file names andtypes. This applies to special files as well.

Issue ID	Description
395204	All types of alerts depend upon the data DatAdvantage collects for the relevant objects. This means alerts are not generated for: • Filtered users and unmonitored users on which events are not collected (this includes filtered users for whom the Allow event collection option is selected) • Unmonitored folders or objects on which events are not collected Users from unmonitored domain (not unmonitored users) are displayed in the alert with available user data (name and/or SID).
400108	Selecting deleted groups in the Acting users from groups filter does not return data.
403869	The Access path and File properties filters currently support up to 50 values for DatAlerts. Defining more than 50 will cause performance issues.
403896	The Administrative or service account disabled or deleted DatAlert UBA rule does not specify the account which was disabled or deleted.
404589	Privileged account discovery is not available for LDAP and NIS domains.
404893	Following upgrade to 6.2.5, customized logos in DatAlert email templates must be reapplied.
405753	Since DatAlert rule scope is recalculated after every PullWalk, having a topology with several (16) rules with different scopes causes severe performance degradation.
406084	Following upgrade of DatAnswers, the browser cache must be cleared to ensure use of updated Javascript sources.

6.2.3

Issue ID	Description
224386	When the user credentials provided at logon cannot be resolved, the message displays "Nobody" instead of the entered user name.
326742	The FileWalk user account is added as an owner all all crawled site collections (both regular and personal sites), either in the Management Console when the sites are added, or by FileWalk itself during its run. Site collections that were added by the site auto-detection feature are not crawled until the next run of FileWalk.

Issue ID	Description
326743	The FileWalk user account is added as an owner to all site collections in SharePoint Online, to enable running FileWalk on them. However, this user is not removed when the SharePoint Online file server is removed or DatAdvantage is uninstalled.
329633	If a file is created in a source folder from which the Data Transport Engine already copied a file with the same name and left stub for it, the second rule execution to copy the new file will fail to delete the new file from the source and create a stub for it, since a stub with the same name already exists. The system will not rename the new stub, since that would cause users to lose context.
333899	If, following the commit process in DataPrivilege, an opposite editing command is created in DatAdvantage before FileWalk and PullWalk, it is not possible to commit the change since the commands cancel each other out. (For example, an Add Permission command existed in DatAdvantage, was committed through DataPrivilege and then a Remove Permission command for the same permission is created in DatAdvantage.) Following FileWalk and PullWalk, the Add command is invalid so the Remove command can be created again and committed.
358214	Due to a Windows issue, the deduplication process returns the wrong physical file size on rare occasion.
367630	When Windows servers are accessed via CIFS, the INHERITED ACE flag is not returned.
372854	Changes made in DatAdvantage Security only take effect in DatAnswers after the browser window is closed and reopened.
374263	Due to a Microsoft issue, some event IDs do not appear in the event log in Windows Server 2012 R2.
378365	In some cases, NFS clients might cache small files. When the files are accessed several times, there is no request to the server; therefore, those events are not collected.