What's New and What's Changed in Symantec™ Data Loss Prevention 14

What's New and What's Changed in Symantec Data Loss Prevention 14

Documentation version: 14.0c

Last updated: 28 April 2015

Legal Notice

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.com

Technical Support

Symantec Technical Support maintains support centers globally. Technical Support's primary role is to respond to specific queries about product features and functionality. The Technical Support group also creates content for our online Knowledge Base. The Technical Support group works collaboratively with the other functional areas within Symantec to answer your questions in a timely fashion. For example, the Technical Support group works with Product Engineering and Symantec Security Response to provide alerting services and virus definition updates.

Symantec's support offerings include the following:

- A range of support options that give you the flexibility to select the right amount of service for any size organization
- Telephone and/or Web-based support that provides rapid response and up-to-the-minute information
- Upgrade assurance that delivers software upgrades
- Global support purchased on a regional business hours or 24 hours a day, 7 days a week basis
- Premium service offerings that include Account Management Services

For information about Symantec's support offerings, you can visit our website at the following URL:

www.symantec.com/business/support/

All support services will be delivered in accordance with your support agreement and the then-current enterprise technical support policy.

Contacting Technical Support

Customers with a current support agreement may access Technical Support information at the following URL:

www.symantec.com/business/support/

Before contacting Technical Support, make sure you have satisfied the system requirements that are listed in your product documentation. Also, you should be at the computer on which the problem occurred, in case it is necessary to replicate the problem.

When you contact Technical Support, please have the following information available:

- Product release level
- Hardware information

- Available memory, disk space, and NIC information
- Operating system
- Version and patch level
- Network topology
- Router, gateway, and IP address information
- Problem description:
  - Error messages and log files
  - Troubleshooting that was performed before contacting Symantec
  - Recent software configuration changes and network changes

Licensing and registration

If your Symantec product requires registration or a license key, access our technical support Web page at the following URL:

www.symantec.com/business/support/

Customer service

Customer service information is available at the following URL:

www.symantec.com/business/support/

Customer Service is available to assist with non-technical questions, such as the following types of issues:

- Questions regarding product licensing or serialization
- Product registration updates, such as address or name changes
- General product information (features, language availability, local dealers)
- Latest information about product updates and upgrades
- Information about upgrade assurance and support contracts
- Information about the Symantec Buying Programs
- Advice about Symantec's technical support options
- Nontechnical presales questions
- Issues that are related to CD-ROMs, DVDs, or manuals

Support agreement resources

If you want to contact Symantec regarding an existing support agreement, please contact the support agreement administration team for your region as follows:

Asia-Pacific and Japan	customercare_apj@symantec.com
Europe, Middle-East, and Africa	semea@symantec.com
North America and Latin America	supportsolutions@symantec.com

Contents

Chapter 1

Introducing Symantec Data Loss Prevention 14

This chapter includes the following topics:

About this guide

The *What's New and What's Changed* guide describes new features and changed capabilities in the version 14 release of Symantec Data Loss Prevention.

This guide does not contain implementation or configuration details for these features. It provides an overview of each new feature in Symantec Data Loss Prevention 14, including, where appropriate, enough detail to help you understand how this feature can be used. It also includes deployment information to help you plan for rolling out these new features to your organization.

Where possible, the guide provides pointers to further information about new and changed functionality.

Summary of new and changed features in Symantec Data Loss Prevention

The following tables summarize the new and changed features in Symantec Data Loss Prevention 14.

Table 1-1 New features for Endpoint for Symantec Data Loss Prevention 14

Feature	Description
Endpoint Prevent for cloud storage applications	Popular cloud sync applications, such as Box, Dropbox, and Google Drive, are now available on the Application Monitoring page, making it easy to monitor those specific applications. See "Endpoint Prevent for cloud storage applications" on page 15.
Mac Endpoint Prevent for removable storage	Monitor and prevent confidential data transfer between Mac endpoints and removable storage devices, including USB drives, Secure Digital (SD) memory cards, and Thunderbolt storage devices. See "Mac Endpoint Prevent for removable storage" on page 17.
Mac Endpoint Prevent for browser-based uploads	Monitor and prevent confidential data uploads using browsers on Mac endpoints. See "Mac Endpoint Prevent for browser-based uploads" on page 18.
Monitoring the Upload Multiple Files option in SharePoint	Support for monitoring files uploaded using the **Upload Multiple Files** option in SharePoint. See "Monitoring the Upload Multiple Files option in SharePoint" on page 19.
Preventing data loss to HTTPS websites from Google Chrome	Monitor and prevent sensitive data transfer over HTTPS from the Google Chrome browser. See "Preventing data loss to HTTPS websites from Google Chrome" on page 19.
Enhanced support for Microsoft Windows 8.1	Enhanced support for Microsoft Windows 8.1, including Microsoft Store application monitoring, and monitoring in Enhanced Protection Mode in Internet Explorer 11. See "Enhanced support for Microsoft Windows 8.1" on page 19.
Preventing data loss to mobile devices using the Media Transfer Protocol (MTP)	Support for monitoring data transfer between Windows 8 systems and mobile devices using MTP. Monitoring of Windows 7 systems and mobile devices that use MTP was introduced in Data Loss Prevention 12.5. See "Preventing data loss to the mobile devices that use the Media Transfer Protocol (MTP)" on page 20.
Disabling SPDY protocol in endpoint browsers	The SPDY protocol, which is used by certain websites but can affect monitoring for data loss, can be disabled on Internet Explorer and Firefox browsers used by endpoints in your organization. Once SPDY is disabled, Symantec Data Loss Prevention can monitor the standard HTTPS traffic that browsers use to communicate with the websites. See "Disabling SPDY protocol in endpoint browsers" on page 20.

Table 1-1 New features for Endpoint for Symantec Data Loss Prevention 14 *(continued)*

Feature	Description
Clipboard Paste monitoring	You can monitor data being pasted from the clipboard to specific applications, such as the Windows Store Mail app, Google Chrome, Microsoft Lync, Microsoft Communicator, and Skype. See "Clipboard Paste monitoring" on page 20.
Endpoint support for Microsoft Windows Server 2012 R2	The DLP Agent can be deployed on Microsoft Windows Server 2012 systems. See "Endpoint support for Microsoft Windows Server 2012 R2" on page 21.
Support for VMware Fusion 7 monitoring	Support for monitoring VMware Fusion 7 on Mac endpoints. Data is monitored that resides on or moves from Windows VMs or the Mac host file system. See "Support for VMware Fusion 7" on page 21.
Disabling the Print Screen function	You can prevent users from copying their screen using the Print Screen function. See "Disabling the Print Screen function" on page 21.
Endpoint notification pop-ups appear in a user's display language	Support for displaying notification pop-ups in the end user's selected display language. See "Endpoint notification pop-ups appear in a user's display language" on page 21.
Simplified process for monitoring CD/DVD applications	The selection for CD/DVD applications is now conveniently grouped with other application types on the **Application Monitoring** screen. See "Simplified process for monitoring CD/DVD applications" on page 21.

Table 1-2 New features for cloud support for Symantec Data Loss Prevention 14

Feature	Description
Data Loss Prevention for Box cloud storage	You can run Network Discover/Cloud Storage Discover scans to find sensitive information on your employees' corporate Box cloud storage accounts. See "Data Loss Prevention for Box cloud storage" on page 22.
Cloud Prevent for Microsoft Office 365	You can deploy a Cloud Prevent for Email Server in the cloud and manage it from your on-premises Enforce Server administration console. Symantec Email Security.cloud is used as the MTA to direct mails that have passed detection from Data Loss Prevention to their final destination. (Supported beginning with Symantec Data Loss Prevention 12.5.x.) See "Cloud Prevent for Microsoft Office 365" on page 22.

Table 1-2 New features for cloud support for Symantec Data Loss Prevention 14 *(continued)*

Feature	Description
Detection servers on Amazon Web Services (AWS) infrastructure	Hybrid cloud support for deploying detection servers on AWS infrastructure and connecting to on-premises Enforce Server. (Supported beginning with Symantec Data Loss Prevention 12.5.) See "Detection servers on Amazon Web Services (AWS) infrastructure" on page 23.

Table 1-3 New features for Network Prevent for Symantec Data Loss Prevention 14

Feature	Description
Associating a Network Prevent for Web incident with an end user	You can use the IP address in a Web Prevent incident to determine the user name associated with that incident. See "Associating a Network Prevent for Web incident with an end user" on page 23.

Table 1-4 New and changed features for Detection for Symantec Data Loss Prevention 14

Feature	Description
EDM incident highlighting style	Ability to choose to highlight all incident matches in the proximity window (including duplicates) or the minimum number of matches required by the EDM condition. See "EDM incident highlighting style" on page 24.
EDM enhancements: improved accuracy, faster detection, and larger indexes	EDM enhancements include reducing the chance of false positives, which significantly improves detection accuracy. Other improvements include significantly faster detection times and support for much larger index sizes. See "EDM enhancements: improved accuracy, faster detection, and larger indexes" on page 24.
Natural language processing for Chinese, Japanese, and Korean for EDM policies	Detection servers now support natural language processing for Chinese, Japanese, and Korean (CJK) in policies that use EDM detection. When natural language processing for CJK languages in enabled, the detection server validates CJK tokens before reporting a match, which improves matching accuracy. See "Natural language processing for Chinese, Japanese, and Korean for EDM policies" on page 25.

Table 1-4 New and changed features for Detection for Symantec Data Loss Prevention 14 *(continued)*

Feature	Description
Keyword matching performance improvements	Faster detection times for keyword matching conditions, on the server and the endpoint, both whole and partial word matching. See "Keyword matching performance improvements" on page 25.
Detecting custom metadata tags in PDF documents	Server and agent support for detecting custom metadata tags in PDF documents. See "Detecting custom metadata tags in PDF documents" on page 25.
Remote IDM Indexer	Standalone tool that lets you index confidential documents and files locally and securely on the systems where these files are stored; frees you from having to copy confidential documents to the Enforce Server host. See "Remote IDM Indexer" on page 26.
New international data identifiers	Forty new system-defined international data identifiers detect personally identifiable information (PII) based on common data patterns for various countries. See "New international data identifiers" on page 26.

Table 1-5 New and changed features for the Enforce Server for Symantec Data Loss Prevention 14

Feature	Description
Improved Enforce Server administration console usability	Modernized Enforce Server administration console look and feel. See "Improved Enforce Server administration console usability" on page 27.
Role-based access control improvements	Creation of a new Auditor role for DLP policy management. You can now use separate roles for Author and Auditor (policy viewer). See "Role-based access control improvements" on page 27.
External storage for incident attachments	You can now choose to store attachments for new incidents on a file server rather than in the Symantec Data Loss Prevention Oracle database, lowering your expense for storage and increasing your database performance. See "External storage for incident attachments" on page 27.
Support for Microsoft Internet Explorer 11 for Enforce Server access	Ability to use Microsoft Internet Explorer 11 to access the Enforce Server. See "Support for Microsoft Internet Explorer 11 for Enforce Server access" on page 28.

Table 1-5 New and changed features for the Enforce Server for Symantec Data Loss Prevention 14 *(continued)*

Feature	Description
Upgrade data pre-checker tool	The upgrade data pre-checker tool checks your Symantec Data Loss Prevention database for some types of corrupted data before you upgrade your installation. See "Upgrade data pre-checker tool" on page 28.
Database diagnostics	Ability to view diagnostic information about your Symantec Data Loss Prevention database, such as tablespace allocation and table details, from the Enforce Server administration console. See "Database diagnostics" on page 28.
Automatic upgrade patch distribution	When you upgrade from Symantec Data Loss Prevention 12.5 or later, the new upgrader patch distribution system automatically distributes upgrade patches to all detection servers that are connected to your Enforce Server. See "Automatic upgrade patch distribution" on page 28.

Table 1-6 Removed and unsupported features for Symantec Data Loss Prevention 14

Feature	Description
Removed and unsupported features	The following items are not supported in Symantec Data Loss Prevention 14: ■ Oracle Database 11.2.0.3. ■ Reporting API; superseded by the Incident Reporting and Update API. For more information, refer to the *Symantec Data Loss Prevention Incident Reporting and Update API Developers Guide*. ■ DLP Agent running on Microsoft Windows Server 2003. ■ Monitoring AOL Instant Messenger (**AIM**) from the **Agent Configuration** screen. ■ Monitoring Windows Messenger (**MSN**) from the **Agent Configuration** screen. ■ Network Discover scanning of Microsoft Exchange Server 2007 SP1 and older. ■ Microsoft Threat Management Gateway (TMG). See "Removed and unsupported features" on page 29.

Chapter 2

New and Changed Features in Symantec Data Loss Prevention 14

This chapter includes the following topics:

Endpoint features

The following features are new or improved in Symantec Data Loss Prevention 14.

Endpoint Prevent for cloud storage applications

You can monitor and prevent sensitive data from being synced to cloud storage sites from Windows endpoints.

Most of the popular cloud storage sites are already monitored, but you can easily add applications you want to monitor. The applications monitored by default include the following:

- Box

- Dropbox
- Google Drive
- Hightail
- iCloud
- Microsoft OneDrive
- Microsoft Skydrive

This feature also monitors and blocks sensitive files that a user attempts to save from Microsoft Office 2007 and 2012 applications (Windows Excel, and PowerPoint) to the OneDrive cloud storage application. You enable this feature using the **Hooking.CLOUD_STORAGE_HOOKING** advanced agent setting. Refer to the "Advanced agent settings" topic in the "Discovering and preventing data loss on endpoints" section of the *Symantec Data Loss Prevention Administration Guide* for more information.

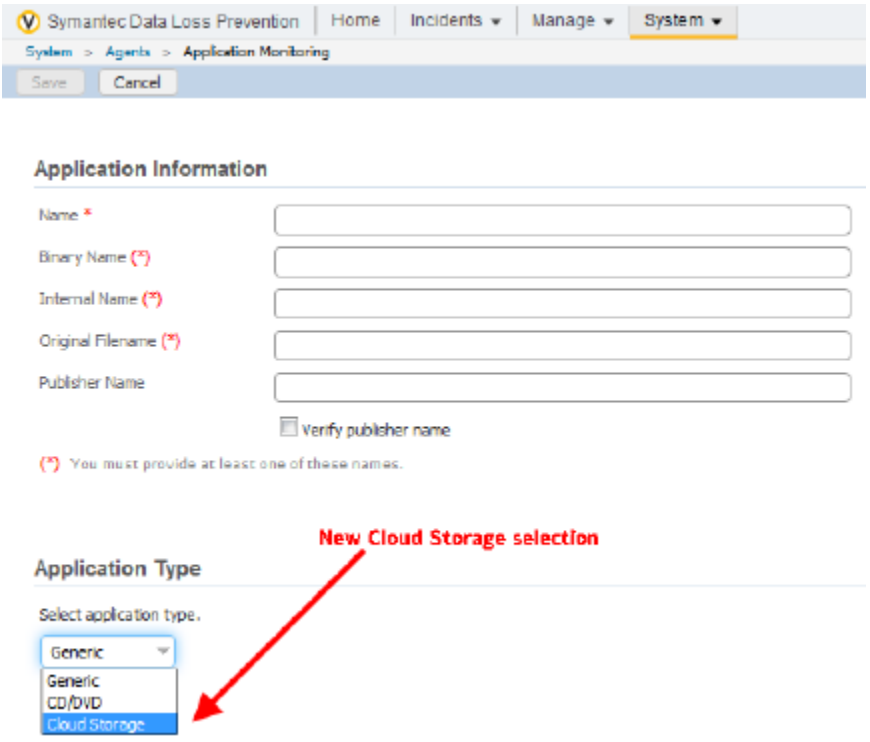
In previous versions of Symantec Data Loss Prevention, you could add these cloud storage applications to the **Application Monitoring** screen. However, multiple incidents were created for a violation of a block response rule because the endpoint would make multiple attempts to synchronize the file with the cloud version. In Symantec Data Loss Prevention 14, the sensitive file is quarantined, and only one incident is created for a violation of a block rule. By default the file is quarantined to `%USERPROFILE%\My Recovered Files`. You can designate another location on the **Agent Configuration** tab on the **Agent Configuration** screen.

If sensitive content is added to files that are to be synced to the cloud application, Symantec Data Loss Prevention creates a new *Cloud Storage* incident.

You can add cloud storage applications not listed on the **Application Monitoring** screen as you normally would. However, you select **Cloud Storage** in the new **Application Type** section. Refer to the "Using application monitoring" topic in the "Discovering and preventing data loss on endpoints" section of the *Symantec Data Loss Prevention Administration Guide* for more information.

The following figure shows the new **Cloud Storage** selection.

Figure 2-1 Selecting Cloud Storage



Mac Endpoint Prevent for removable storage

You can now monitor and prevent confidential data transfer between Mac endpoints and removable storage devices. This feature is enabled by default using the **Removable Storage** selection on the **Agent Configuration** screen.

This feature includes monitor and prevent support for the following:

- Save-as operations, which include support for these applications: Microsoft Office, iWork 9, TextEdit, Preview, Archive Utility, and Acrobat Reader.
- File copy operations, which include support for these applications: Finder, Terminal, Browsers (Safari, Firefox, and Google Chrome), CopyQueue, and CyberDuck.
- Response rules, which include Block, Notify, Data Retention, and Set Severity.

Note: This feature supports USB 2.0 and greater devices.

The following device types were tested and are supported:

- USB flash drives and memory sticks
- Memory cards, including SDXC and SDHC cards
- Removable hard drives
- FireWire storage devices
- Thunderbolt storage devices

Endpoint incidents for Mac removable storage display the removable storage device ID in the following format: *Vendor&Model&Serial&No*.

You can set Symantec Data Loss Prevention to ignore company-provided removable storage devices using the new Mac-specific DeviceID tool. You can also set Symantec Data Loss Prevention to ignore a range of device types, like FireWire devices, USB drives, and so on, using the **Filesystem.ignore_storage_bus_type** advanced agent setting.

Sensitive files that are blocked from being moved from the endpoint to removable storage are moved to a non-configurable local path on the Mac endpoint: `$HOME/My Recovered Files`, where `$HOME` is the endpoint user's home directory.

Mac Endpoint Prevent for browser-based uploads

You can now monitor and prevent confidential data uploads using browsers on Mac endpoints. This feature allows the DLP Agent to monitor and prevent data from moving from Mac endpoints to web applications like email and cloud storage.

You enable this feature using the **Application File Access** selection on the **Agent Configuration** screen. You add the browser you want to monitor to the **Application Monitoring** screen. You must also add browser child processes you want to monitor to the **Application Monitoring** screen. Refer to the "About monitoring browser-based file uploads on Mac endpoints" topic in the "Discovering and preventing data loss on endpoints" section of *Symantec Data Loss Prevention Administration Guide* for implementation information.

This feature supports the following Mac browsers:

- Google Chrome
- Mozilla Firefox
- Safari

This feature supports the following response rules:

- Endpoint Prevent: Block
- Endpoint Prevent: Notify

You can use DCM detection with this feature. If a file violates a policy, a Mac application monitoring incident is generated.

Note: You can adjust the agent configuration settings to improve monitoring performance. Refer to the "Working with agent configurations" topic in the "Discovering and preventing data loss on endpoints" section of the *Symantec Data Loss Prevention Administration Guide* for more information.

Monitoring the Upload Multiple Files option in SharePoint

Endpoint Prevent now monitors and blocks sensitive information being uploaded to SharePoint when the **Upload Multiple Files** option is selected. This update supports monitoring files uploaded from the Internet Explorer, Firefox, and Chrome browsers. Support includes monitoring and preventing of single and multiple file uploads using Windows Explorer drag and drop, and copy and paste.

Preventing data loss to HTTPS websites from Google Chrome

Symantec Data Loss Prevention can now monitor and prevent sensitive data transfer over HTTPS from the Google Chrome browser. Also, Google Chrome is now a default application on the **Application Monitoring** screen, which means you are no longer required to add it to monitor sensitive information.

You can do the following with this feature:

- Prevent sensitive files from being uploaded using Chrome. You can also indicate sites where sensitive information is allowed to be uploaded.
- Prevent sensitive information from being pasted into Chrome. You can also indicate sites where sensitive information is allowed to be pasted.
- Prevent sensitive information from being printed from Chrome.
- Monitor Chrome in Windows Metro mode.

Enhanced support for Microsoft Windows 8.1

Symantec Data Loss Prevention 14 includes enhanced support for Microsoft Windows 8.1:

- Clipboard paste monitoring
- Support for Windows Store applications in Microsoft Internet Explorer 11
- Ability to whitelist Windows Store applications
- Support for Microsoft Internet Explorer 11 in Enhanced Protection Mode

Preventing data loss to the mobile devices that use the Media Transfer Protocol (MTP)

Symantec Data Loss Prevention monitors and prevents data transfer between Windows 8 and 8.1 64-bit systems and mobile devices using MTP. Monitoring and preventing of data transfers between Windows 7 systems and mobile devices using MTP was introduced in Symantec Data Loss Prevention 12.5. If a user moves sensitive information from an endpoint to an external device that uses MTP, Symantec Data Loss Prevention creates a removable device incident.

Disabling SPDY protocol in endpoint browsers

The SPDY protocol, which is used by certain websites but can affect monitoring for data loss, is now automatically disabled on Internet Explorer and Firefox running on endpoints in your organization.

When SPDY is disabled, Symantec Data Loss Prevention can monitor the standard HTTPS traffic that browsers use to communicate with the websites. If an endpoint user enables the SPDY protocol, the setting does not take effect and the protocol remains disabled.

Note: The SPDY protocol can be enabled and disabled using the **NetworkMonitor.DISABLE_SPDY_PROTOCOL.int** setting on the **Advanced Agent Settings** screen.

Clipboard Paste monitoring

You can now monitor data being copied and pasted from the Clipboard, letting you prevent sensitive data from being pasted to specific applications. Incidents generated from both copy and paste actions display as Clipboard incidents.

The following applications are configured by default for Clipboard Paste monitoring:

- Windows Store Mail app
- Google Chrome
- Microsoft Lync
- Microsoft Communicator
- Skype

Note: To enable this feature for additional applications, you add them to the **Application Monitoring** screen.

Endpoint support for Microsoft Windows Server 2012 R2

You can now install the DLP Agent on computers running the Microsoft Windows Server 2012 R2 operating system.

(Support added in Symantec Data Loss Prevention 12.5.x.)

Support for VMware Fusion 7

Symantec Data Loss Prevention now monitors Windows virtual machines that run on VMware Fusion 7.

This new support allows Symantec Data Loss Prevention to monitor data residing on or moving from the Windows VM or the Mac host file system. You can configure the monitor coverage when you implement Windows virtual machines. Refer to the *Symantec Data Loss Prevention Administrator Guide* for more information.

Disabling the Print Screen function

Symantec Data Loss Prevention administrators can disable the ability of endpoint users to copy their screen using the Print Screen function. Enabling this feature prevents users from recording an image of the desktop using the `Print Screen` keyboard key as well as key combinations, like `Shift + Print Screen`. This feature applies to Window 7 and 8 endpoints.

Endpoint notification pop-ups appear in a user's display language

Endpoint notification pop-ups now use the user's selected display language instead of the language in the system locale. For example, if the system locale is set to English and the user sets the display language to German, the pop-up appears in German.

Simplified process for monitoring CD/DVD applications

The selection for CD/DVD applications is now conveniently grouped with other application types on the **Application Monitoring** screen. Now when you add a CD/DVD application to the **Application Monitoring** screen, you select **CD/DVD** under the new **Application Type** section. In previous versions of Symantec Data Loss Prevention, the selection was located in a list of selections at the bottom of the screen.

You do not have to reconfigure CD/DVD settings made in previous versions. The table Endpoint Prevent for cloud storage applications lists previous versions configurations and what they are updated to in Symantec Data Loss Prevention 14.

Table 2-1 Previous versions and Symantec Data Loss Prevention 14 Application Monitoring configuration

Previous version configuration	Symantec Data Loss Prevention 14 configuration
Applications with neither **Monitor Application File Access** nor **Monitor writing to CD/DVD** enabled.	**Generic Applications** enabled.
Applications with only **Monitor Application File Access** enabled.	**Generic Applications** enabled.
Applications with only **Monitor writing to CD/DVD** enabled.	**CD/DVD** enabled.

Data Loss Prevention for cloud features

The following features are new or improved for Symantec Data Loss Prevention 14.

Data Loss Prevention for Box cloud storage

You can create Network Discover/Cloud Storage Discover scans to scan files that are stored in employee Box accounts. Network Discover/Cloud Storage Discover scans of Box targets show you:

- What sensitive information is stored in your employees' accounts
- With whom your employees have shared that sensitive information, including external parties
- How that sensitive information is shared: for example, you can see if sensitive files are password protected, or if they are accessible through links that are available to unauthorized users

Cloud Prevent for Microsoft Office 365

Symantec Data Loss Prevention Cloud Prevent for Microsoft Office 365 detects confidential data in corporate email sent from Microsoft Office 365 Exchange. It monitors and analyzes outbound Microsoft 365 Exchange email traffic and can block, redirect, or modify email messages as specified in your enterprise's policies. It integrates seamlessly with your existing on-premises Enforce Server administration console and enables your enterprise to leverage its existing investment in policy definition and administration as well as incident remediation processes. This solution

integrates with the separate Symantec Email Security.cloud email service, which provides email delivery.

(Support added in Symantec Data Loss Prevention 12.5.x.)

Detection servers on Amazon Web Services (AWS) infrastructure

Symantec Data Loss Prevention supports the deployment of specific detection servers on Amazon Web Services (AWS) infrastructure. Data Loss Prevention support for AWS is based on a hybrid cloud model: a supported detection server deployed to AWS connects to an on-premises Enforce Server using a registered TCP port. You do not have to modify a detection server or perform any special configurations to deploy Data Loss Prevention on AWS.

Starting with Symantec Data Loss Prevention 12.5.x, you can deploy a Network Discover detection server on AWS to discover sensitive data on Microsoft SharePoint, Microsoft Exchange, and CIFS-compliant file share servers residing in the cloud. In addition, you can deploy a Network Prevent for Email detection server on AWS to control the transmission of sensitive email from a Microsoft Exchange mail server residing in the cloud.

For more information, see the Symantec Solutions for Amazon Web Services page at the following URL: http://www.symantec.com/page.jsp?id=amazon. To download the documentation for deploying Data Loss Prevention detection servers on AWS, go to the Support knowledge base at the following URL: http://www.symantec.com/docs/TECH225947.

Network Prevent features

The following features are new or improved for Symantec Data Loss Prevention 14.

Associating a Network Prevent for Web incident with an end user

You can use the IP address in a Network Prevent for Web incident to determine the user name associated with that incident. Using the new domain controller agent, Symantec Data Loss Prevention collects Windows Events from the Security event log on the Microsoft Active Directory domain controller server. These events are stored in the Symantec Data Loss Prevention database, where a look-up service can resolve the IP address to its associated user name.

For more information about user name resolution and the domain controller agent, see the topic "Resolving user names from IP addresses in web incidents" in the "Working with user risk" chapter of the *Symantec Data Loss Prevention*

Administration Guide, and the "Installing the Domain Controller Agent" chapter in the *Symantec Data Loss Prevention Installation Guide*.

Detection features

The following features are new or improved for Symantec Data Loss Prevention 14.

EDM incident highlighting style

For Exact Data Matching (EDM) policies, you can choose to highlight all incident matches in the proximity window (including duplicates) or the minimum number of matches required by the EDM condition. (Introduced in Symantec Data Loss Prevention 12.5.1.)

EDM enhancements: improved accuracy, faster detection, and larger indexes

Symantec Data Loss Prevention 14 provides significant enhancements to Exact Data Matching (EDM), including improved detection accuracy, faster detection times, and support for larger indexes.

Table 2-2 describes each enhancement.

To take advantage of these EDM enhancements, you must reindex your data sources using Symantec Data Loss Prevention 14 indexers (Enforce Server or Remote EDM Indexer). In addition, for large indexes, you must verify that you have allocated sufficient memory to index, load, and process each index.

For more information about EDM memory requirements, see the topic "EDM memory requirements" in the *Symantec Data Loss Prevention Administration Guide*.

Table 2-2 EDM enhancements in Symantec Data Loss Prevention 14

Enhancement	Description
Improved detection accuracy	For large indexes, the chance of a false positive caused by a hash collision is greatly reduced, resulting in more accurate detection.
Faster detection times	EDM detection performs, on average, approximately seven times faster than previous releases.
Support for larger indexes	You can index a data source with up to six billion cells. Previously the limit was two billion cells.

Natural language processing for Chinese, Japanese, and Korean for EDM policies

Symantec Data Loss Prevention detection servers support natural language processing for Chinese, Japanese, and Korean (CJK) in policies that use Exact Data Matching (EDM) detection. When natural language processing for CJK languages is enabled, the detection server validates CJK tokens before reporting a match, which improves matching accuracy.

Token validation for CJK is disabled by default. You must enable token validation for each detection server by setting the Advanced Server Setting **EDM.TokenVerifierEnabled** to true. You must match on whole words for token validation to apply.

For more information, see the topic “Configuring natural language processing for Chinese, Japanese, and Korean for EDM policies” in the *Symantec Data Loss Prevention Administration Guide*.

Keyword matching performance improvements

Performance improvements for keyword matching conditions significantly reduce detection time for both full and partial keyword matching on the server and on the endpoint. Functionality has not changed, and you do not need to change or update your existing keyword conditions to take advantage of the performance improvements. The performance improvements take effect when you upgrade your detection servers and agents to version 14.

These performance improvements cause the DLP Agent to consume more RAM compared to previous versions of the DLP Agent. The amount of increase depends upon the complexity and the number of policies. However, even with a complex policy set, the total memory consumed is low compared to the total memory available on the endpoint.

Detecting custom metadata tags in PDF documents

You can now detect custom metadata tags in PDF documents when you enable metadata detection on the server or on the endpoint. Symantec Data Loss Prevention now supports extraction of custom metadata that have been added using the Document Information Dictionary.

Symantec Data Loss Prevention has supported the detection of certain document metadata for several releases now, including Microsoft Office metadata fields and standard Adobe PDF metadata tags. Data Loss Prevention 14 adds detection support for custom PDF metadata tags.

Table 2-3 lists and describes the types of PDF metadata tags now supported by Data Loss Prevention.

Table 2-3 Supported PDF metadata tags

Metadata type	Technical name	Description	DLP support
Standard PDF metadata tags	Document Information Dictionary (DID)	DID metadata includes fields such as Author, Title, Subject, Creation, and Update. Adobe Acrobat automatically creates DID metadata by default.	Server version 11.0 and later Endpoint version 11.5 and later
Custom PDF metadata tags	Document Information Dictionary (DID)	Custom metadata added using the DID.	Server and Endpoint version 14.0

Remote IDM Indexer

The Remote IDM Indexer is a standalone tool that lets you index your confidential documents and files locally on the systems where these files are stored, or from a shared network resource that is easier or preferable to access from a remote host. Using the Remote IDM Indexer greatly simplifies the IDM indexing process because it frees you from having to collect and copy all the files you want to protect to the Enforce Server.

The Remote IDM Indexer generates a secure (encrypted) pre-index file that you upload to the Enforce Server for final indexing and deployment to servers and endpoints. The Remote IDM Indexer is supported on Windows and Linux platforms and provides three configuration options: properties file, command-line interface (CLI), and user interface (Windows only).

New international data identifiers

There are 40 new international data identifiers for detecting personally identifiable information (PII) that are commonly used in various countries, including Argentina, Australia, Austria, Belgium, Brazil, Bulgaria, Chile, Czech Republic, England, France, Germany, Greece, Hungary, India, Indonesia, Ireland, Israel, Japan, Luxembourg, Malaysia, Mexico, Norway, Poland, Romania, Russia, South Africa, Spain, Sweden, Switzerland, Thailand, United Arab Emirates, and Venezuela.

Enforce Server platform features

The following features are new or improved for Symantec Data Loss Prevention 14.

Improved Enforce Server administration console usability

The Enforce Server administration console user interface has been updated. The top navigation has been simplified and the overall appearance has been improved.

The user interface includes the following improvements:

- Section 508 compliance
- Simplified menus
- Modernized look and feel
- Improved use of space
- Redesigned to allow for better responsiveness on tablets and handheld devices
- Updated display settings to better adapt to various screen sizes and resolutions

The **Incidents** screen has a number of updates in addition to the style updates mentioned above. The incident badges at the top of the screen display incidents by severity and count. The screen automatically adjusts the navigation bar if you use larger fonts.

Role-based access control improvements

A new Auditor role for Data Loss Prevention policy management is available. The Auditor role is restricted to read-only privileges for policy groups for which the Auditor role is enabled. Users with the Auditor role cannot manage or remediate incidents.

This new role enables you to efficiently divide up the policy management workflow, so that any employee with an Auditor role can monitor specific policies. This capability can be particularly helpful to use when you experience a large volume of incidents that must be monitored for a policy group and have to bring on more staff to deal with these incidents.

External storage for incident attachments

You can now choose to store attachments for incidents on a file server rather than in the Symantec Data Loss Prevention Oracle database, lowering your expense for storage and increasing your database performance. Existing incident attachments in your database are migrated to the external storage directory. Be aware that you cannot migrate externally stored incidents into the database.

For more information about external storage for incident attachments, see the topic "About external storage for incident attachments" in chapter 1 of the *Symantec Data Loss Prevention Upgrade Guide*.

Support for Microsoft Internet Explorer 11 for Enforce Server access

You can now use Microsoft Internet Explorer 11 to access the Enforce Server administration console.

Upgrade data pre-checker tool

You can use the upgrade data pre-checker tool to check your Symantec Data Loss Prevention database for some types of corrupted data before you upgrade your installation. If the tool returns an error, you can contact Symantec Technical Support to resolve your data corruption issues before upgrading.

For more information about the upgrade data pre-checker tool, see the topic "Preparing the Oracle database for a Symantec Data Loss Prevention upgrade" in chapter 1 of the *Symantec Data Loss Prevention Upgrade Guide*.

Database diagnostics

You can now view diagnostic information about the Symantec Data Loss Prevention database from the Enforce Server administration console. To view a summary of tablespace allocations and files within specific tablespaces, navigate to **System > Database > Tablespaces Summary**. To view database table details, navigate to **System > Database > Table Details**.

For more information about database diagnostics, see the "Managing the Symantec Data Loss Prevention database" chapter in the *Symantec Data Loss Prevention Administration Guide*.

Automatic upgrade patch distribution

Symantec Data Loss Prevention 12.5.x introduced a new framework for automatically distributing patch files to detection servers before or during the upgrade process. This new approach to patch distribution shortens and simplifies the upgrade process. To begin this automated distribution process, download and extract the upgrade software. The Enforce Server automatically detects the upgrade packages and begins distributing the patches to your detection servers. When you choose to upgrade your system, you can view the patch distribution status in the Upgrade Wizard.

For more information about upgrading your detection servers, see chapter 2 in the *Symantec Data Loss Prevention Upgrade Guide*.

Removed and unsupported features

The following items are not supported in Symantec Data Loss Prevention 14:

- Oracle Database 11.2.0.3.
- The Reporting API; superseded by the Incident Reporting and Update API. For more information, refer to the *Symantec Data Loss Prevention Incident Reporting and Update API Developers Guide*.
- DLP Agent running on Microsoft Windows Server 2003.
- Monitoring AOL Instant Messenger (**AIM**) from the **Agent Configuration** screen. Sensitive information accessed using this application is monitored using the Clipboard monitoring and application file access features.
- Monitoring Windows Live Messenger (**MSN**) from the **Agent Configuration** screen.
- Network Discover scanning of Microsoft Exchange Server 2007 SP1 and older using the Exchange Web Store connector.
- Microsoft Threat Management Gateway (TMG).