# What's New in Data Loss Prevention 14.6

## New capabilities let you work more securely with sensitive information

Symantec Data Loss Prevention 14.6 introduces a new set of information protection capabilities, powered by the industry's leading data loss prevention technology, to give you greater visibility and control over your confidential data. It includes:

- **Expanded cloud app security integrations –** Allow you to extend DLP coverage to cloud apps with Symantec Cloud Access Security Broker and Symantec Blue Coat Web Security Service[1].

- **Stronger endpoint monitoring –** Gives you more control over sensitive data in use on Macs and PCs including Mac OS 10.12 and Windows 10 Anniversary Update.

- **Expanded data discovery –** Gives you visibility into sensitive documents stored in SharePoint 2016.

- **Improved content detection –** Lets you catch more types of sensitive data, across more types of documents such as files encrypted by Microsoft RMS.

- **Easier system management –** Lets you manage policies, respond to incidents, and deploy our software more easily.

## Protect data in cloud apps

Security is the biggest challenge faced by enterprises adopting cloud apps – especially with popular business apps like Office 365 and Salesforce where all kinds of sensitive company data will be stored and shared. With Symantec DLP, you can enable employees to work freely and safely in the cloud.

We've extended DLP coverage to sanctioned and unsanctioned cloud apps by leveraging integrations between Symantec's DLP Cloud Service Connector[2], a new cloud-based detection service powered by the same leading technology as our on-premises software, and Symantec Cloud Access Security Broker and Symantec Blue Coat Web Security Service[3]. You can uncover data blind spots in over 60 cloud apps including Office 365, Box, Dropbox, Google Apps, or Salesforce - all from the same management console, DLP Enforce.

**✔Symantec.**™

# Enable safer data use on endpoints

Employees face countless vulnerabilities on and off the network. With the **DLP Endpoint Agent for Mac OS**, you can protect data in use across a wide range of events including downloading to removable storage; copying and pasting within documents; and sending over the web. To help you stay ahead of potential leaks, we've added support for new platforms and applications:

- Mac OS 10.12

- Microsoft Outlook 2016

- More granular monitoring for applications via Application Monitoring

The **DLP Endpoint Agent for Windows** packs in many of the same powerful features as our Mac Agent and now has added protection for data in use across these platforms and applications:

- Microsoft Windows 10 Anniversary Update Enterprise

- Citrix 7.9 XenApp / XenDesktop

- Microsoft Edge

- More granular monitoring for applications via Application Monitoring

### Application Monitoring Configuration

Select the channels to monitor:

For 14.5.x and earlier agents, selecting any of Removable Storage, Local Drive, Copy to Network Share, or Application File Access enables monitoring for all of the following channels: Removable Storage, Local Drive, and Copy to Network Share.

Likewise, for 14.5.x and earlier agents, selecting either HTTP or FTP enables monitoring for both HTTP and FTP channels.

**Destinations**
- ☑ Removable Storage
- ☑ Printer/Fax
- ☑ Local Drive

**Application File Access**
- ☐ Application File Access
  - ○ Open
  - ○ Read

**Clipboard**
- ☑ Clipboard
  - ● Copy
  - ○ Paste

**Network Shares**
- ☑ Copy to Network Share

**Web**
- ☑ HTTP
- ☑ FTP

# Get visibility into SharePoint 2016

Unstructured data in enterprises is growing significantly, largely due to internally generated documents, yet few companies are focused on governing and protecting it. With DLP Network Discover, you can get visibility into where your most sensitive data lives and prevent it from being exposed by careless employees or malicious attackers. By leveraging high-speed scanning capabilities, DLP Network Discover quickly finds sensitive data stored across network file shares, databases, and other data repositories – now including Microsoft SharePoint 2016.

# Find sensitive data anywhere

Content-aware detection techniques make it possible to find sensitive data stored in virtually any location and file format. Symantec DLP offers the most comprehensive data detection

by leveraging advanced describing, fingerprinting and machine learning technologies that accurately detect data so you don't have to worry about false positives impacting business users.

In DLP 14.6, we've improved content detection so you can catch more types of data across more types of documents:

- **Microsoft RMS-encrypted files:** You can now detect sensitive content in files encrypted by Microsoft Rights Management Services (RMS).

- **Improved regex detection:** The DLP detection engine can evaluate regular expressions significantly faster – up to 40X – and more consistently across the DLP endpoint agent and detection servers.

- **More built-in detection intelligence:** DLP 14.6 provides new and updated policy templates for the new European General Data Protection Regulation (GDPR) and U.S. HIPAA and HITECH; it also provides new and updated Data Identifiers for China, France, India, Japan, Korea, Mexico, Spain, Sweden and the U.S.

✓Symantec. | **p. 2**

# Protect form documents

More than ever, companies are relying on imaged documents – from scanners and phones – to digitize their business processes. Doing so makes it easier to exchange information with customers and partners, but it also makes it harder to track and control sensitive data, especially scanned forms which are often rife with personally identifiable information (PII).

Introduced in DLP 14.5, Symantec DLP Form Recognition[4] leverages intelligent image processing to catch sensitive data that would otherwise go undetected in rasterized forms, such as scanned or imaged forms that have been typed or filled out by hand. With DLP 14.6, you can now detect sensitive data in electronically fillable PDF files.

# Manage the system more easily

In DLP 14.6, we've made it easier to manage policies, respond to incidents, and deploy our software with enhancements to the DLP Enforce Server and Console.

- **Windows Server 2016:** You can now deploy the DLP Enforce Server and detection servers Windows Server 2016 in addition to Windows Server 2008 and 2012.

- **Improved policy management:** The DLP Policy List page supports filtering the policy list as well as applying bulk operations such as Activate/Suspend policies, Export, Download and Delete multiple policies at the same time.

- **Expanded access to incident variables:** Admins get access to more incident field variables – such as application name, application user – allowing for more meaningful context in syslog messages and email notifications.

# About Symantec

Symantec Corporation World Headquarters

350 Ellis Street
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934

www.symantec.com

12/16     Part # 21366644