7 REASONS TO UPGRADE TO DLP 14

Enterprises are undergoing major transformation as they move their information from on-premises systems to the public cloud such as Office 365, Box and Amazon Web Services to increase mobile workforce productivity, improve operational agility, and lower costs. But as information moves out of your hands and into the cloud, it raises concerns about security, privacy and compliance. Symantec Data Loss Prevention (DLP) addresses these issues so you can take advantage of the cloud with control and visibility. It discovers, monitors and protects your confidential data across cloud, mobile and on-premises environments. Unlike other solutions, Symantec DLP is available as an on-premises and hybrid cloud solution enabling flexible deployment and seamless management from a unified platform.

1 Visibility and Control for Cloud Storage

+ DLP Cloud Storage is a new cloud discovery product that gives you deep visibility into the sensitive files that business users are storing and sharing on Box. DLP seamlessly integrates with Box to scan employees' accounts and discover what information is being stored, how it's being used, and with whom it's being shared. When sensitive files are detected, DLP places visual tags on them and engages users to self-remediate them on Box.

+ The Cloud File Sync and Share feature monitors and prevents users from syncing sensitive files from their desktop to cloud storage sites including Box, DropBox, Google Drive, Hightail, iCloud and Microsoft OneDrive.

2 Visibility and Control for Cloud Email

DLP Cloud Prevent for Microsoft Office 365[1] seamlessly integrates with Microsoft's hosted email service, Exchange Online, to give you deep visibility and control of sensitive messages sent by business users. Unlike other products, it provides advanced, content-aware detection and incident remediation capabilities from a unified management console, DLP Enforce. Cloud Prevent can be easily deployed in a hybrid cloud environment, and integrated with your on-premises DLP Enforce Server and Symantec Email Security.cloud.

3 Easy to Deploy in the Cloud and On-premises

+ Amazon Web Services (AWS) support[2] enables fast out-of-the-box deployment of DLP content detection servers in the AWS Cloud. Once deployed, you can easily discover, monitor and protect sensitive data stored in AWS-hosted instances of Microsoft Exchange and SharePoint.

+ **Single server installation support**[3] enables fast out-of-the-box deployment of the DLP management server, content detection servers, and Oracle database on a single physical server for branch offices or small organizations, and lowers hardware and maintenance costs.

4 Improved Content Detection Capabilities

+ The Keyword Matching technology significantly reduces the time it takes to detect content matches against complex keyword-based policies.

+ The Exact Data Matching technology delivers faster detection and improved accuracy so you can easily fingerprint extremely large, structured data sources such as databases and detect a single field or combinations of fields from a record.

21299912 - 2 04/15

Symantec

+ The Indexed Document Matching technology significantly reduces the size of the server index footprint so you can efficiently fingerprint and detect unstructured data in documents such as Microsoft Office, PDF, and CAD.

+ The Remote Indexed Document Matching Indexer is a new out-of-the-box tool that protects business users' privacy by enabling them to directly fingerprint highly sensitive files instead of providing your DLP Administrator and DLP Enforce server direct access to them.

5 New Look and Feel

The improved UI modernizes the overall look and feel of the DLP Enforce management console, simplifies navigation and optimizes performance for mobile devices.

6 Improved Mac Agent

+ Removable Storage support monitors and prevents unauthorized file transfers to removable storage devices connected to Mac desktops and laptops.

+ Google Chrome, Firefox and Safari support monitors and prevents users from uploading sensitive files via their Mac web browsers.

+ VMware Fusion support monitors data in use on a virtual Windows machine running on Mac OS and prevents unauthorized file transfers to network shares and resources.

7 Improved Windows Agent

+ Google Chrome support monitors and prevents users from transmitting sensitive data from their Chrome browsers. The Agent also supports Firefox and Internet Explorer.

+ Microsoft Hyper-V support protects data in use on virtual Windows machines residing on a Hyper-V Server. The Agent also monitors virtual desktops and applications hosted by Citrix XenApp and VMware.

+ Media Transfer Protocol (MTP) support monitors and prevents data transfer between Windows 8 desktops and mobile devices using MTP.

[1] Support added in DLP 12.5
[2] Support added in DLP 12.5
[3] Support added in DLP 12.5

Symantec DLP provides a comprehensive suite of products to protect your information anywhere, anytime. For more information, *visit go.symantec.com/dlp*

21299912 - 2 04/15

Symantec