What's New in Data Loss Prevention 14.5

New capabilities let you work more securely with confidential data

Data Sheet: Data Loss Prevention

Symantec Data Loss Prevention 14.5 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.

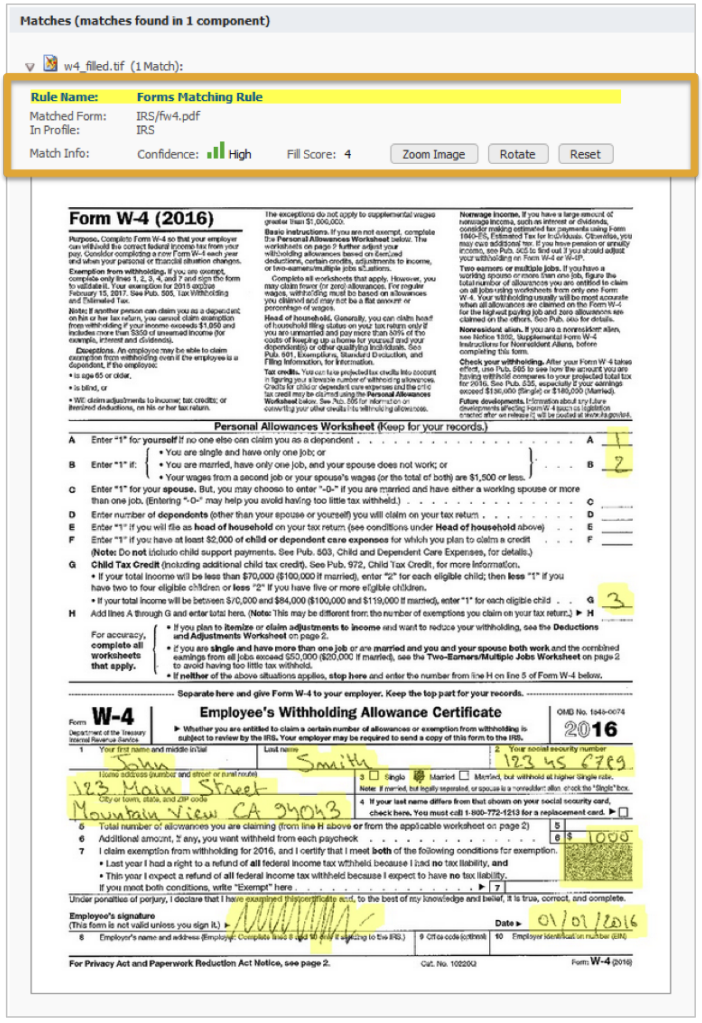
Data Loss Prevention 14.5 includes:

- **Advanced data detection** – Lets you catch personally identifiable information and intellectual property in more types of documents, across more channels
- **Enhanced cloud discovery** – Provides added file protection for sensitive documents that are stored and shared on Box
- **Stronger endpoint monitoring** – Gives you more control over confidential data in use on Macs and PCs
- **Better visibility into encrypted communications** – Allows you to uncover and eliminate security blind spots created by encrypted web traffic

Protect sensitive forms

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).

With Symantec **DLP Form Recognition**, you can protect data stored in images of handwritten and typed forms such as tax returns, insurance claims, patient forms or any form that might contain PII. DLP Form Recognition is a new content detection technology that leverages intelligent image processing to catch and stop confidential data that would otherwise go undetected in scanned or photographed forms.



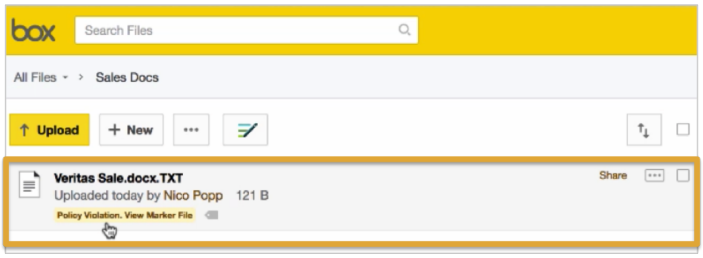
Current DLP users can easily add on Form Recognition with a single enterprise-wide license that enables you to leverage the product across one or more of these detection servers: Network Monitor, Network Prevent for Email, Network Prevent for Web, Network Discover and Network Protect.

Protect confidential data in the cloud

You can enable employees to work freely and safely on cloud apps, such as Box, Gmail and Microsoft Office 365, with the Symantec DLP Endpoint Agent for Windows, DLP Cloud Storage, and the DLP Cloud Service for Email.

The **DLP Endpoint Agent for Windows** provides new monitoring and blocking capabilities for file uploads to Box through the Box Sync and Box for Office applications. It allows users to upload all kinds of files to company-sanctioned Box accounts while preventing them from uploading files to unsanctioned personal Box accounts through Box Sync.

DLP Cloud Storage tracks sensitive data that users are storing and sharing on Box, and identifies risky practices such as using shared links that could give open access to unauthorized users. When users violate a policy, you can automatically move exposed files and folders a protected quarantine folder on Box and leave behind a marker file in its place to notify users by leveraging the new File Quarantine feature of DLP Cloud Storage. Not only can you secure unprotected files, but also visually tag files to alert users to self-remediate sensitive files and folders.



The **DLP Cloud Service for Email** monitors and protects your corporate email regardless of whether it's hosted in a conventional on-premise email application, public or private cloud email service, or a hybrid mix of on-premise and cloud environments. This cloud-powered detection service provides deep integration with Gmail, Microsoft Office 365 Exchange Online, and now Microsoft Exchange Server, and can be easily plugged into your existing DLP Enforce Server.

Enable safer data use on endpoints

Employees face countless dangers 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 applications, file types and operating systems commonly used by employees to share sensitive data:

- Mac OS 10.11
- Microsoft Office 2016 file types
- Microsoft Outlook 2011 email client
- Chrome, Firefox and Safari browsers (via HTTP and HTTPS)
- Copy to network shares
- Paste from the clipboard
- Skype instant messaging client

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 applications and file types:

- Microsoft Office 2016 file types
- Box for Office and Box Sync applications
- Cisco Jabber and Skype for Business instant messaging clients

Manage policies across environments the easy way

When it comes to moving your data loss policies between environments – such as from development or test to production – simplifying and automating the process can help you avoid mistakes and save time. With the policy import and export feature, you can easily migrate policies between instances of the DLP Enforce Server. Policies are exported to a file that contains full policy details, including policy groups and response rules, and are imported error-free.

Protect document snippets on endpoints

Employees readily cut, copy and paste snippets of information from sensitive documents across different files and applications – some of which may be unsanctioned and unsafe to use. Symantec DLP makes it easy to spot these fragments with a powerful data fingerprinting capability called Endpoint Indexed Document Matching, which can detect confidential data in its derivative and original forms. Endpoint Indexed Document Matching is especially helpful for organizations with mobile or remote employees who routinely

work with unstructured data – i.e., information that doesn't readily fit into a database.

Take more control of web communications

Most companies rely on a few key web protocols – HTTPS, HTTP, and FTP – to communicate with customers, partners and contractors. But when employees send confidential data over these encrypted and unencrypted channels, it creates blind spots and vulnerabilities for IT. In DLP 14.5, you get advanced web monitoring and prevention capabilities for HTTPS, HTTP and FTP by leveraging new integrations between DLP Network Prevent for Web and these web gateways and cloud proxies:

- A10 Networks Application Delivery Controller, SSL Insight and Thunder Convergent Firewall
- Zscaler Web Security Service

Get better visibility into encrypted communications

As more and more of the world's internet traffic becomes encrypted, you lose visibility of the confidential data that your company is leaking over encrypted communication protocols. DLP gives you back control by letting you inspect encrypted traffic before it leaves the safety of your network. Through deep integration with the leading SSL decryption appliances, DLP can analyze decrypted traffic and prevent confidential data from being posted or sent by users. In DLP 14.5, you get new SSL monitoring capabilities for web, email, FTP and IM communications by leveraging integrations between DLP Network Monitor and these SSL decryption products:

- Blue Coat SSL Visibility
- Palo Alto Networks Next Generation Firewalls

More Information

Visit our website

go.symantec.com/dlp

To speak with a Product Specialist in the U.S.

Call toll-free 1 (800) 745 6054

To speak with a Product Specialist outside the U.S.

For specific country offices and contact numbers, please visit our website.

About Symantec

Symantec Corporation (NASDAQ: SYMC) is the global leader in cybersecurity. Operating one of the world's largest cyber intelligence networks, we see more threats, and protect more customers from the next generation of attacks. We help companies, governments and individuals secure their most important data wherever it lives.

Symantec World Headquarters

350 Ellis St.
Mountain View, CA 94043 USA
+1 (650) 527 8000
1 (800) 721 3934
www.symantec.com

21299912 - 2 06/16