# What's New in Data Loss Prevention 15.5

## New and enhanced data security and compliance controls

Symantec Data Loss Prevention 15.5 introduces new information protection capabilities, powered by the industry's leading data loss prevention technology, to give you greater visibility and security over your confidential data.

- **New integration with Symantec Endpoint Protection (SEP) secures data against malicious applications:** Together, Symantec Data Loss Prevention and Symantec Endpoint Protection can now stop malicious, suspicious or unknown apps from seizing control of users' endpoints and stealing sensitive corporate data like intellectual property and PII.
- **Detect more data, more accurately with new Exact Matching Data Identifier (EMDI):** Effective data protection always starts with good detection. DLP 15.5 features EMDI, a new powerful data fingerprinting detection engine providing accuracy, security and performance for discovery of indexed data. EMDI completes the already broad set of data detection engines included with Symantec DLP and is available on all DLP detection channels.
- **Improved detection on endpoints with Data Classification controls:** DLP policies can now suggest a classification tag to the end users as they classify newly created content with Symantec Information Centric Tagging (ICT). Additionally, DLP 15.5 has the innovative ability of being able to classify existing data on endpoints. Data Loss Prevention can scan endpoints and apply an appropriate classification tag as a response to a policy violation.
- **Expanded integration with Information Centric Encryption (ICE):** DLP 15.5 expands protection of sensitive data leaving endpoints via browser uploads.
- **Extended application coverage with DLP:** DLP 15.5 includes support for more cloud applications through cloud access security broker and for Skype for Business on premises.

## New integration with Symantec Endpoint Protection (SEP) secures data against malicious applications

Protecting sensitive data against cyber threats is increasingly difficult as threats arise daily. DLP can detect and protect sensitive data in many formats, yet DLP doesn't understand cyber threats and malicious processes. Symantec DLP 15.5 makes DLP threat aware thanks to its integration with leading-edge Symantec Endpoint Protection. Now DLP can stop endpoint data exfiltration based on application risk.

- **SEP Intensive Protection feature:** In Symantec DLP 15.5, you can now automatically prevent exfiltration of sensitive data by apps running on endpoints that are unknown or malicious based on reputation-based application profiling. In fact, the SEP agent dynamically instructs the DLP endpoint agent to monitor applications that are malicious, suspicious or have unknown reputation. By leveraging such information about the application reputation from SEP, DLP is now able to generate incidents when a non-legit application is trying to access files that are sensitive, thus effectively allowing DLP to block sensitive data from being accessed and exfiltrated by those processes.

# Detect more data, more accurately

Symantec Data Loss Prevention 15.5 provides enhanced data detection and compliance controls. In fact, DLP 15.5 features new powerful and secure data fingerprinting engine supporting all DLP detection channels.

- **New Exact Matching Data Identifier (EMDI):** EMDI is a new fingerprinting detection engine supporting all DLP detection channels, including detection servers, appliances, cloud services, and DLP endpoint agents. It provides the ability to detect more data via a new memory-efficient fingerprinting technology. EMDI can detect structured data, especially PII, with a high degree of accuracy and a low false positive ratio, virtually eliminating certain false positive matches that Data Identifiers and regex can periodically generate. Additionally, EMDI has a stringent security model that makes it suitable for profile deployment on endpoints and in the cloud.
- **More built-in detection intelligence:** In DLP 15.5, you get over 75 new and updated data identifiers and policy templates including General Data Protection Regulation (GDPR) to reflect the new European Personal Identity data identifiers.

# Improved detection on endpoints with Data Classification controls

DLP 15.5 further broadens the data classification capabilities enabled via integration with Symantec Information Centric Tagging (ICT).

- **DLP assists user in the classification decision process:** DLP policies can now be used, instead of built-in rules of Information Centric Tagging (ICT), to suggest classification tags to the user. End users automatically receive the suggested classification based on DLP defined policies and can optionally override the DLP suggested classification.
- **Ability to scan and tag existing data on endpoints:** DLP can use endpoint classification scans to detect and apply a data classification tag based on content and context. Such classification tag labels the data for protection everywhere it goes.

# Expanded integration with Information Centric Encryption (ICE)

DLP 15.5 expands protection for endpoint channels to automatically apply ICE encryption and digital rights to file and folder browser uploads.

- **DLP applies ICE to data shared via browser upload:** Data encryption capabilities for DLP Endpoint Prevent have been expanded to cover more egress methods on Windows endpoints. In fact, files or folders that are uploaded with browsers using HTTPS such as Chrome, Edge, Firefox and Internet Explorer can be now automatically encrypted with Symantec Information Centric Encryption (ICE). You can ensure data is protected with encryption and digital rights when uploaded from a local disk, network share, or a removable storage device using a browser.

# Extended application coverage with DLP

With DLP 15.5 you can extend DLP coverage to protect data on more applications in the cloud and on premises.

- **DLP covers more cloud applications via integration with Symantec CloudSOC:** DLP 15.5 provides support for the following Symantec CloudSOC securlets through the DLP Cloud Detection Service in addition to several other securlets and gatelets included in previous versions.
    - Amazon S3
    - Cisco Spark
    - Slack

- **New and updated smart response rules for CloudSOC securlets:** Symantec Data Loss Prevention includes the following new smart response rules: Encrypt, Remove collaborators and Remove shared links.
- **Protect sensitive content shared on Skype for Business:** Now you can extend DLP protection to Skype for Business, a Microsoft messaging and collaboration application for business users. This protection is obtained via integration of Symantec DLP API Detection for SkypeShield, a new REST API virtual appliance, and AGAT SkypeShield.

## More DLP enhancements

Symantec Data Loss Prevention 15.5 also introduces several performance enhancement and new capabilities such as:

- **Larger inspection file sizes:** Data Loss Prevention now supports larger file sizes – up to 2 GB.
- **Server Message Block (SMB) 2 protocol support for Network Discover and Network Protect:** Symantec Data Loss Prevention now supports SMB2 for Network Discover detection and Network Protect incident response.

**To learn more about Symantec Data Loss Prevention visit go.symantec.com/DLP**

**About Symantec**
Symantec Corporation (NASDAQ: SYMC), the world's leading cyber security company, helps organizations, governments and people secure their most important data wherever it lives. Organizations across the world look to Symantec for strategic, integrated solutions to defend against sophisticated attacks across endpoints, cloud and infrastructure. Likewise, a global community of more than 50 million people and families rely on Symantec's Norton and LifeLock product suites to protect their digital lives at home and across their devices. Symantec operates one of the world's largest civilian cyber intelligence networks, allowing it to see and protect against the most advanced threats. For additional information, please visit www.symantec.com or connect with us on Facebook, Twitter, and LinkedIn.

Symantec

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