FAMILY DATA SHEET

Symantec Data Loss Prevention

Drive total protection of your sensitive data

At a glance

Highest level of data protection

- Broadest data protection for communication channels: cloud, email, web, endpoints, and storage.
- Fewer false positives with comprehensive detection technologies.

Single pane of glass

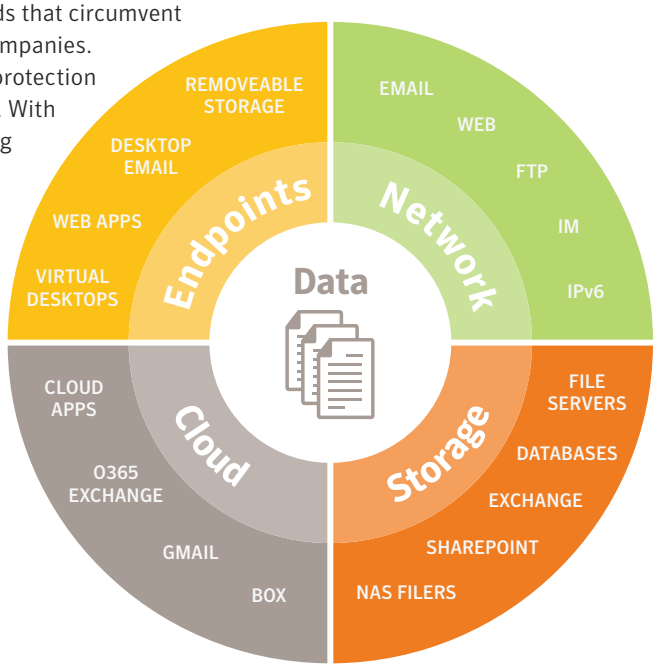
- Single console for policy management, incident response, reporting and administration.
- One set of policies and workflow for all communication channels: cloud, email, web, endpoints, and storage.

Wide range of integrations

- Integrates with Symantec Information Centric Security and the Integrated Cyber Defense Platform.
- Broad integration support for user behavior, third-party encryption, data classification and rights management products.

Stop data loss with the highest level of protection

Keeping information safe and compliant has never been easy. But today, enterprises face new and unexpected security problems. As more companies unplug their on-premises systems and move to cloud-based services, company data becomes more vulnerable to accidental exposure by inexperienced cloud users and configuration errors. Cloud security isn't the only concern for enterprises. Targeted cyber-attacks have become all too common as cybercriminals develop effective new methods that circumvent traditional security measures and exploit users to steal valuable data from companies. Symantec's Data Loss Prevention (DLP) solution delivers the highest level of protection you need to prevent data breaches and safeguard your company's reputation. With our industry-leading technology, you get comprehensive discovery, monitoring and protection capabilities that give you total visibility and control over your confidential data.



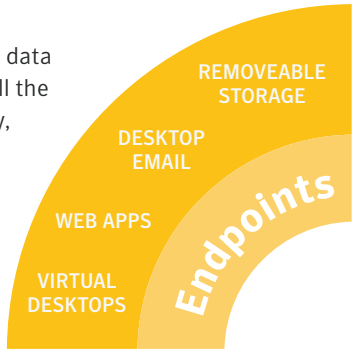
Discover where data lives across every channel: cloud, email, web, endpoints, and storage

Monitor how data is being used on and off the corporate network

Protect data from being exposed or stolen in real-time

Keep data safe while in use on endpoints

As employees become more mobile through the use of laptops, company data becomes more vulnerable to data leaks and thefts – on and off the corporate network. The **Symantec DLP for Endpoint** solution provides all the protection you need to keep sensitive data safe and protected on endpoints. It provides complete discovery, monitoring and protection capabilities for data in use across a broad range of channels: email, cloud apps, network protocols, external storage, and virtual desktops and servers. With Symantec DLP, a single lightweight endpoint agent enables two modules: DLP Endpoint Discover and DLP Endpoint Prevent.



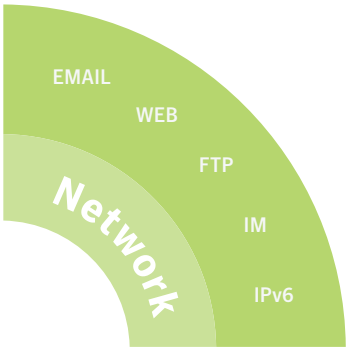
Symantec DLP Endpoint Discover scans local hard drives and gives you deep visibility into sensitive files that users are storing on their laptops and desktops. It provides a wide range of responses including local and remote file quarantining, and policy-based encryption and digital rights management enabled by the DLP Endpoint FlexResponse API.

Symantec DLP Endpoint Prevent monitors users' activities and gives you fine-grained control over a wide range of applications, devices and platforms. It provides a wide range of responses including identity-based encryption and digital rights for files transferred to USB. With Endpoint Prevent, you can alert users to incidents using on-screen popups or email notifications. Users can also override policies by providing a business justification or canceling the action (in the case of a false positive).

Browsers	Chrome | Safari | Firefox | IE & Edge
Cloud Apps	Box | Dropbox | Google Drive | Microsoft OneDrive
Email Apps	Outlook | Lotus Notes
Network Protocols	HTTP | HTTPS | FTP
Removable Storage	MSC devices | MTP devices
Virtual Desktops	Citrix | Microsoft Hyper-V | VMware
Others	Print | Fax | Network Share | Clipboard

Protect data in motion over the network

The widespread adoption of collaboration tools and cloud apps, coupled with risky employee behavior that companies may not even be aware of, increases the risk of data exposure over business communications. The **Symantec DLP for Network** solution monitors and prevents sensitive data from being leaked over a wide range of communication protocols across your network.



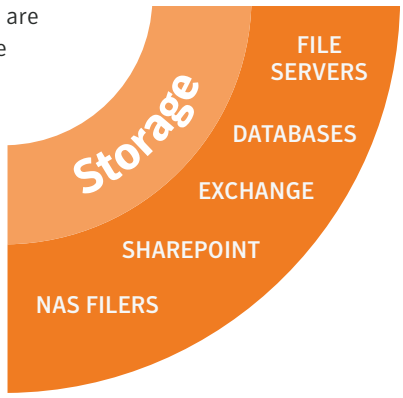
DLP Network Monitor captures and analyzes outbound traffic on your corporate network, and detects sensitive content and metadata over standard, non-standard and proprietary protocols. It is deployed at network egress points and integrates with your network tap or Switched Port Analyzer (SPAN). Network Monitor performs deep content inspection of all network communications with zero packet loss, unlike other solutions that sample packets during peak loads and put you at high risk for false negatives.

DLP Network Prevent for Email protects sensitive messages from being leaked or stolen by employees, contractors and partners. It monitors and analyzes all corporate email traffic, and optionally modifies, redirects, or blocks messages based on sensitive content or other message attributes. Network Prevent for Email is deployed at network egress points and integrates with mail transfer agents (MTAs) and cloud-based email including Microsoft® Office 365 Exchange. Network Prevent for Email is available as software or virtual appliance.

DLP Network Prevent for Web protects sensitive data from being leaked to the Web. It monitors and analyzes all corporate web traffic, and optionally removes sensitive HTML content or blocks requests. Network Prevent for Web is deployed at network egress points and integrates with your HTTP, HTTPS or FTP proxy server using ICAP. Network Prevent for Web is available as software, hardware appliance, or virtual appliance.

Protect data at rest across storage repositories

Digital data is growing significantly, largely due to internally generated documents, yet few companies are focused on governing and protecting it. With **Symantec DLP for Storage**, you can discover and secure sensitive data at rest – the data stored on file servers, endpoints, cloud storage, network file shares, databases, SharePoint and other data repositories.



First, **Symantec DLP Network Discover** finds confidential data by scanning network file shares, databases, and other enterprise data repositories. This includes local file systems on Windows, Linux, AIX, and Solaris servers; Lotus Notes and SQL databases; and Microsoft Exchange and SharePoint servers. DLP Network Discover recognizes more than 330 different file types—including custom file types—based on the binary signature of the file. It also provides high-speed scanning for large, distributed environments, and it optimizes performance by scanning only new or modified files.

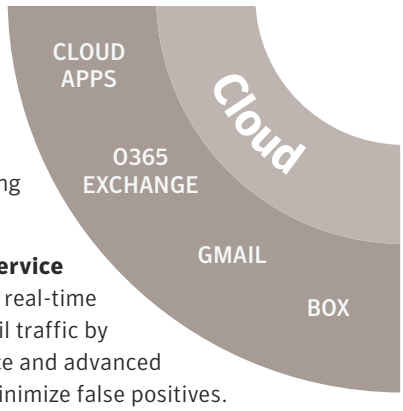
Next, **Symantec DLP Network Protect** adds robust file protection capabilities on top of Network Discover. Network Protect automatically cleans up and secures all of the exposed files Network Discover detects, and it offers a broad range of remediation options, including quarantining or moving files, copying files to a quarantine area, or applying policy identity-based encryption and digital rights to specific files. Network Protect even educates business users about policy violations by leaving a marker text file in the file's original location to explain why it was quarantined.

Symantec DLP also includes a **FlexResponse API Platform** that allows you to build custom file remediation actions. FlexResponse provides easy turnkey integration with other Symantec and third-party file security solutions—including Symantec File Share Encryption and Adobe LiveCycle.

File Servers	Windows via CIFS and DFS | Unix via NFS | Local Windows | Local Unix (Linux, AIX and Solaris) | NAS Filers
Distributed Machines	Laptops | Desktops
Document and Email Repositories	SharePoint | LiveLink | Documentum | Lotus Notes | Microsoft Exchange | PST
Web Content and Applications	Corporate Web Sites | Intranet | Extranet | Custom Applications
Databases	Oracle | Microsoft | IBM DB2

Protect data in the cloud

Security concerns persist as companies continue to migrate legacy IT applications to public cloud services where it's difficult to get the same level of visibility and control of sensitive data as on their own private servers. With Symantec's DLP Cloud Services, you can extend powerful data protection controls to the cloud with the convenience of cloud-delivered DLP. They provide rich discovery, monitoring and protection capabilities for a wide range of cloud applications as well as on-premises applications.



The **Symantec DLP Cloud Detection Service** inspects content extracted from cloud app and web traffic, and automatically enforces sensitive data policies. It offers enhanced cloud-to-cloud integration with Symantec CloudSOC, our industry leading cloud access security broker solution, to protect data in motion and data at rest across more than 100 in sanctioned and unsanctioned cloud apps such as Office 365, G-Suite, Box, Dropbox, and Salesforce. The integration allows to extend existing policies and robust detection to cloud applications and manage all incidents from the DLP console. Controls include un-share sensitive files, quarantine, block them from leaving the application, and also apply identity-based encryption and digital rights automatically to specific files shared with third parties. The DLP Cloud Detection Service also offers enhanced integration with Symantec's Web Security Service to monitor web traffic - even when it's encrypted - and protect roaming and mobile users.

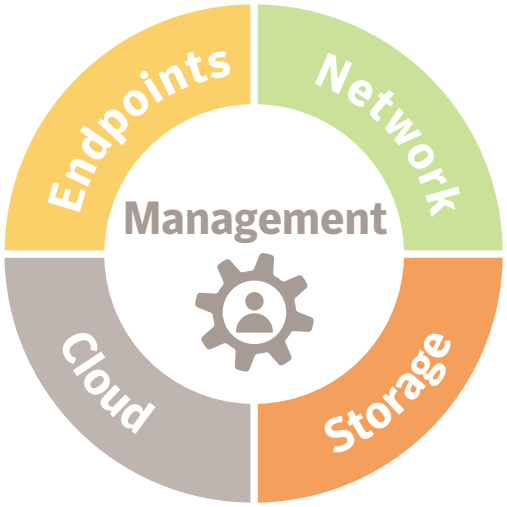
The **Symantec DLP Cloud Service for Email** provides accurate, real-time monitoring of corporate email traffic by leveraging built-in intelligence and advanced detection capabilities that minimize false positives. It also provides real-time protection against data leaks with automated messaging blocking, or message modification to enforce downstream encryption or quarantining. When data is shared with third parties it can automatically enable identity-based encryption and digital rights for email bodies and attachments. The DLP Cloud Service for Email supports Gmail for Work, Microsoft Office 365 Exchange Online as well as Microsoft Exchange Server. It is available standalone or bundled with the superior email threat protection capabilities of Symantec's Email Security.cloud service.

Manage from a single pane of glass

As your data spreads across a wider range of devices and storage environments, the ability to consistently define and enforce policies becomes even more critical. Symantec DLP gives you a unified management console, the DLP Enforce Platform, which allows you to write policies once and then enforce them everywhere – across all data loss channels.

With the **DLP Enforce Platform**, you can:

- Use a **single web-based console** to author data loss policies, remediate incidents, and perform system administration across all of your endpoints, mobile devices, cloud-based services, and on-premise network and storage systems.
- Take advantage of more than **70 pre-built policy templates** and a convenient **policy builder** to get your system up and running quickly.
- Leverage robust **workflow and remediation capabilities** to streamline and automate incident response processes for high traffic environments.
- Apply business intelligence to your risk reduction efforts with **a sophisticated analytics tool**, **Symantec IT Analytics for DLP**, which provides advanced reporting and ad-hoc analysis capabilities.



Get unmatched visibility into confidential data

At the core of any DLP solution is content-aware detection. 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 detection with advanced machine learning, image recognition, fingerprinting and describing technologies that accurately classify data so you don't have to worry about false positives and impacting business users.

DESCRIBED CONTENT MATCHING

DESCRIBED DATA

Non-indexable data

EXACT DATA MATCHING

STRUCTURED DATA

Account Numbers, Credit Cards, Government IDs

INDEXED DOCUMENT MATCHING

UNSTRUCTURED DATA

Financial Reports, Marketing Plans

MACHINE LEARNING

UNSTRUCTURED TEXT

Source Code, Product

SENSITIVE IMAGE RECOGNITION

IMAGES

Scanned or Electronically-Filled Forms, Images

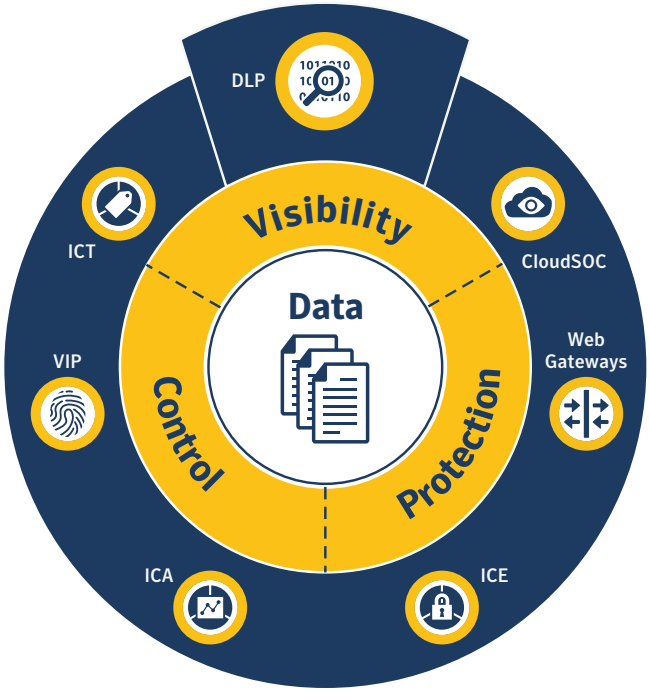
- **Described Content Matching** detects content by looking for matches on specific keywords, regular expressions or patterns, and file properties. Symantec DLP provides more than 130 Data Identifiers out-of-the-box, which are pre-defined algorithms that combine pattern matching with built-in intelligence to prevent false positives.
- **Exact Data Matching** detects data by fingerprinting or indexing structured data sources such as databases, directory servers, and other structured data files.
- **Indexed Document Matching** applies fingerprinting methods to detect data stored in unstructured documents, including Microsoft Office documents; PDFs; and binary files such as JPEGs, CAD designs, and multimedia files. IDM also detects "derived" content, such as text that has been copied from a source document to another file.
- **Sensitive Image Recognition** detects text embedded in images such as scanned forms, documents, screenshots, pictures and PDFs by leveraging our proprietary Form Recognition technology and built-in Optical Character Recognition (OCR) engine.
- **Vector Machine Learning** protects intellectual property with nuanced characteristics that are rare or difficult to describe such as financial reports and source code. Unlike other detection technologies, Vector Machine Learning does not require you to locate, describe, or fingerprint the data you need to protect.

Symantec DLP also offers a rich set of out-of-the-box and add-on APIs to allow you to customize and integrate with a wide range of third-party security products, cloud and proprietary applications: DLP REST API, DLP FlexResponse API, DLP Content Extraction API, DLP Incident Reporting and Update API, and DLP API Detection Virtual Appliance.

Extend data protection beyond DLP

As sensitive data is shared with external users or travels to the cloud and goes outside of your managed environment, it becomes vulnerable to unwanted exposure. Symantec's **Information Centric Security** solution provides comprehensive protection for your data throughout its lifecycle beyond your managed premises, with policy driven cloud access security, classification, encryption, user analytics, and web gateways.

- **Extend DLP policies to cloud applications**: Extend DLP detection, policies and workflows to cloud apps through integration with Symantec CloudSOC (CASB), and manage incidents on a single console.
- **Classify data based on sensitivity**: Enable users to classify and label sensitive files and protect them based on sensitivity by leveraging Symantec's data classification solution, Information Centric Tagging (ICT).
- **Protect data when it's shared outside the company**: Automatically apply persistent encryption and digital rights to data when it leaves the managed premises, control who can use it, track it everywhere, and revoke access if necessary with Information Centric Encryption (ICE).
- **Simplify incident triage and policy management**: Reduce time and efforts for incident remediation and policy management, and mitigate data risk with Symantec Information Centric Analytics (ICA), a User and Entity Behavior Analytics.
- **Share data more securely with others**: Prevent unauthorized access to sensitive data via strong authentication when data is shared with business partners with Symantec VIP Identity and Access Management.



- **Prevent data from going to unwanted sites**: Ensure sensitive data doesn't get leaked over untrusted web traffic, even encrypted traffic, by leveraging DLP integration with Symantec Secure Web Gateways: Symantec ProxySG and Web Security Service.

System Requirements

The Symantec DLP solution comprises a single unified management platform, lightweight endpoint agent, and powerful content-aware detection products. We offer the most deployment flexibility with a wide range of options for any type of environment: on-premises software; virtual and physical appliances; public, private and hybrid cloud services; and managed services delivered by Symantec Partners. Unlike other solutions, Symantec DLP is proven to work in highly distributed environments and scale up to hundreds of thousands of users.

For complete system requirements of Symantec Data Loss Prevention visit our **support page**.

Start protecting your information today

Symantec is ready to help you extend your security and compliance polices beyond the borders of your firewall, so you can discover, monitor, and protect your information more completely and effectively. It offers you the lowest total cost of ownership—with proven deployment methodologies, intuitive policy and incident management tools, and comprehensive coverage across all of your high-risk channels.

Discover the advantages of a comprehensive information protection solution that's built for today's mobile, cloud-centered world.

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

To learn more about Symantec Information Centric Security visit **go.symantec.com/ICS**

To learn more about Symantec User and Entity Behavior Analytics visit **go.symantec.com/UEBA**

To learn more about Symantec Encryption products visit **go.symantec.com/encryption**

To learn more about Symantec Identity and Access Management visit **go.symantec.com/VIP**

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 | **www.symantec.com**

Copyright ©2018 Symantec Corporation. All rights reserved. Symantec, the Symantec Logo, and the Checkmark Logo are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

19B191255_ds_DLP_EN