Symantec Data Loss Prevention Solution

Discover, monitor and protect your sensitive corporate information

Data Sheet: Data Loss Prevention

Protecting Your Information in a Mobile, Cloud-Centered World

Keeping sensitive corporate information safe and compliant has never been easy. But today, you're faced with a totally new set of data protection challenges. Sensitive information is leaving the safety of your corporate network as more employees share files over consumer cloud storage services and access those files on their own mobile devices. The number of targeted cyber attacks continues to grow, as cybercriminals develop effective new methods for defeating traditional security measures and stealing corporate information. And as all of these factors converge, it becomes increasingly difficult to manage corporate information and protect it against loss and theft.

So how do you manage and protect your information in this challenging environment? And what does a complete, successful data protection strategy look like in the face of eroding security perimeters, increasing targeted attacks, and evolving user habits and expectations?

Symantec Data Loss Prevention (DLP) answers these questions with a comprehensive approach to information protection that embraces today's cloud- and mobile-centered realities. With DLP, you can:

- **Discover** where data is stored across all of your cloud, mobile, network, endpoint, and storage systems
- **Monitor** how data is being used, whether your employees are on or off the network
- **Protect** data from being leaked or stolen—no matter where it's stored or how it's used

Symantec's market-leading approach and technology expands the reach of your DLP capabilities to the cloud and mobile devices. It gives you the ability to extend security and compliance policies beyond the borders of your own network. And 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 More Data with Content-Aware Detection

Symantec DLP starts with a combination of advanced technologies that can accurately detect all of the confidential data in your organization—whether it's at rest, in motion, or in use. The detection technologies in Symantec DLP include:

- **Exact Data Matching (EDM)** detects content by fingerprinting structured data sources, including databases, directory servers, or other structured data files.
- **Indexed Document Matching (IDM)** applies fingerprinting methods to detect confidential data stored in unstructured data, 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.
- **Vector Machine Learning (VML)** protects intellectual property that has subtle characteristics that may be rare or difficult to describe, such as financial reports and source code. It detects this type of content by performing statistical analysis on unstructured data and comparing it to similar content or documents. Unlike other detection technologies, VML does not require you to locate, describe, or fingerprint the data you need to protect.
- **Described Content Matching (DCM)** detects content by looking for matches on specific keywords, regular expressions or patterns, and file properties. Symantec DLP provides more than 30 data identifiers out-of-the-box, which are pre-defined algorithms that combine pattern matching with built-in intelligence to prevent false positives. For example, the "credit card number" data identifier detects 16-digit patterns and validates them with a "Luhn check".

Symantec™

- **File type detection r**ecognizes and detects more than 330 different file types such as email, graphics, and encapsulated formats. You can configure Symantec DLP to recognize virtually any custom file type, and it also allows you to extract content from specific file formats—including encrypted formats—using the Content Extraction API.

Working together, these content-aware detection technologies make it possible to reduce false positives, minimize the impact of your DLP efforts on end users, and find confidential information stored in virtually any location and file format.

Define and Enforce Policies Consistently across Your Entire Environment

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 features a unified management console, the DLP Enforce Platform, and a business intelligence reporting tool, IT Analytics for DLP, which allows you to write policies once and then enforce them everywhere, and measurably reduce information risks. With **DLP Enforce and IT Analytics**, you can:

- Use a **single web-based console** to define data loss policies, review and 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 **60 pre-built policy templates** and a convenient **policy builder** to get your DLP solution up and running quickly.
- Leverage robust **workflow and remediation capabilities** to streamline and automate incident response processes.
- Apply **business intelligence** to your DLP efforts with **a sophisticated analytics tool** that provides advanced reporting and ad-hoc analysis capabilities. This includes the ability to extract and summarize system data into multi-dimensional cubes—and then create relevant reports, dashboards, and scorecards for different stakeholders in your organization.

Symantec DLP is ready to help you find and monitor all of the confidential data in your diverse environment. But with the Enforce Platform, it will also make sure you can apply consistent policies and take appropriate actions to keep that information safe and protected.

Monitor and Protect Your Cloud-Based Email and Storage

For many enterprises, moving on-premise applications to the cloud is a smart way to increase agility and cut costs. But how do you take advantage of the cloud without losing visibility and giving up control of your sensitive corporate information? **Symantec DLP Cloud Service for Email, Cloud Prevent for Microsoft Office 365 and Cloud Storage for Box** solve this problem by providing robust discovery, monitoring and protection capabilities for your cloud-based email and storage.

The **Symantec DLP Cloud Service for Email** combines industry-leading, content-aware data loss prevention and email security into a single, easy-to-deploy solution so you can move quickly to cloud-based email without compromising security. This convenient cloud service – which is hosted by Symantec - gives you the essential layers of security needed to protect popular cloud email systems such as Microsoft Exchange Online and Gmail for Business. It includes accurate, real-time monitoring and analysis of data in motion; robust incident remediation; and sophisticated data loss policy authoring.

To provide these capabilities, the Cloud Service for Email combines a flexible, cloud-based content detection service with a centralized on-premise management console, the DLP Enforce Platform. It also integrates with a cloud-based email security service, Symantec Email Security.cloud [1], to provide always-on inbound and outbound email security and guaranteed mail delivery. This holistic approach to cloud email protection, which goes far beyond basic compliance, provides the advanced

[1] Symantec DLP Cloud Service for Email includes the Symantec Email Security.cloud Email Safeguard service plan

capabilities you need to keep sensitive information safe from well-meaning and malicious insiders—and keep your organization safe from email-borne threats, including phishing campaigns and targeted attacks.

Symantec DLP Cloud Prevent for Microsoft Office 365 brings content-aware data loss prevention capabilities to Microsoft Exchange Online so you can move to cloud-based email - quickly and securely. It includes accurate, real-time monitoring and analysis of data in motion, robust incident remediation, and sophisticated data loss policy authoring. To provide these capabilities, Cloud Prevent for Microsoft Office 365 combines a cloud-based content detection server, called Cloud Prevent, with a centralized on-premise management console, the DLP Enforce Platform. It also integrates with a cloud-based email security service, Symantec Email Security.cloud [2], to provide guaranteed mail delivery. Unlike the DLP Cloud Service for Email, which delivers content detection as a service hosted by Symantec, the Cloud Prevent server is designed to be hosted in a customer-managed public, cloud IaaS environment, such as Microsoft Azure or Rackspace.

Symantec DLP for Cloud Storage enables secure collaboration and gives you deep visibility into all of the corporate files that users are storing and sharing on Box. It provides powerful content discovery capabilities so you can easily scan Box Business and Enterprise accounts and understand what sensitive data is being stored, how it's being used, and with whom it's being shared. Cloud Storage even engages users to self-remediate policy violations by placing visual tags on Box files and enabling incident remediation from an intuitive online portal, the Symantec DLP Self-Service Portal.

Keep Data Safe on Traditional Endpoints

Although mobile devices and cloud storage are becoming more popular and widespread, endpoints continue to serve as a major repository for confidential corporate information. **Symantec DLP Endpoint Discover and Endpoint Prevent** will make sure you can keep all that information safe and protected—by giving you the ability to discover, monitor, and protect confidential data on traditional and virtual desktops, whether users are on or off your corporate network.

With Symantec DLP, a single highly scalable agent enables both the Endpoint Discover and Endpoint Prevent modules. Working together, they allow you to:

- **Perform local scanning, detection, and real-time monitoring** for a wide range of events on Windows 7, Windows 8, Windows 8.1, and Mac OS X machines.
- **Monitor confidential data** that is being downloaded, copied, or transmitted to or from laptops and desktops. This includes:
  - **Applications**: Outlook
  - **Cloud Storage**: Box, Dropbox, Google Drive, Microsoft OneDrive
  - **Email**: Outlook, Lotus Notes
  - **Network Protocols**: HTTP/HTTPS, FTP
  - **Removable Storage**: USB, MTP, CF and SD cards, eSATA, FireWire
  - **Virtual Desktops**: Citrix, Microsoft Hyper-V, VMware
- **Notify users with an an-screen, pop-up window** or block specific actions when a policy violation is detected.
- **Scan local drives on laptops and desktops** to provide a complete inventory of confidential data, so you can secure or relocate exposed files.
- Use **multiple scanning options**, such as idle scanning and differential scanning, to enable high-performance, parallel scanning of thousands of endpoints with minimal impact to your systems.
- **Deploy a highly scalable, multi-tiered architecture** that can protect hundreds of thousands of endpoint users.

[2] Symantec DLP Cloud Service for Email includes the Symantec Email Security.cloud Email Safeguard service plan

Extend Complete Data Protection to Your Mobile Devices

BYOD is erasing the lines between work and personal life. Today, users simply expect the ability to access sensitive corporate data any time, from any device, using any type of connection. In fact, 2 out of 5 employees admit to downloading work files to their personal phones and tablets. **Symantec DLP for Mobile** gives you the visibility and control you need to embrace this trend and provide the flexible mobile access users want—without putting your information at risk. With Symantec DLP for Mobile, you can:

- **Extend DLP monitoring and protection capabilities** to all of your iOS and Android devices—no matter who owns them.
- Take advantage of an advanced **Mobile Email Monitor** module to detect when users download confidential email to their Android and iOS devices over the Microsoft Exchange ActiveSync protocol. These monitoring capabilities are deployed at your network egress point, and they integrate with your reverse Web proxy for seamless mobile email monitoring.
- Use the **Mobile Prevent** module to monitor users' activities and prevents the transmission of confidential data via the native iOS mail client, browser, and other apps like Dropbox and Facebook. Mobile Prevent connects to your enterprise network through 3G and 4G cellular networks, Wi-Fi networks, and iOS VPN On Demand. Outbound mobile traffic is routed through a VPN to your Web proxy and then to Mobile Prevent**,** which analyzes the information and automatically redacts or blocks confidential data.

Find and Protect Your Elusive Unstructured Data

Unstructured data is growing at an alarming rate of 70 percent per year, so it's not surprising that many organizations struggle to manage and protect it effectively. Working together, **Symantec DLP Network Discover, Network Protect, Data Insight and the Data Insight Self-Service Portal** allow you to take control of all your unstructured data, so it never becomes vulnerable to careless employees and malicious attackers.

First, **Symantec DLP Network Discover** finds and exposes 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. Network Discover deploys inside your corporate LAN environment and communicates policy and incident information directly through the centralized Enforce Platform.

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-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, Microsoft Rights Management Services, Liquid Machines, GigaTrust, and Adobe LiveCycle.

Finally, **Symantec Data Insight** collects and analyzes user events from network-attached storage (NAS) filers, Windows servers, and SharePoint. This data governance solution—designed specifically for unstructured data environments—provides rich, actionable intelligence into data ownership, usage, and access controls. Data Insight also integrates with Network Discover to discover confidential files, identify data owners, understand file permissions and access history, and alert you to anomalous user activity. With Symantec Data Insight, you can finally shine a light on elusive 'dark data' by understanding exactly what data exists in your environment, how it is being used, who owns it, and who has access to it.

Symantec Data Insight also features a **Self-Service Portal** that adds efficient incident remediation workflow capabilities by giving data owners the ability to review and remediate network file incidents. With the Data Insight Self-Service portal, data owners are automatically notified via email whenever a policy violation occurs, and then directed to an intuitive web-based porta**l** to remediate the violation. The IT security team can also view and track the incident's activity through the Enforce Platform's management console.

Together, these four essential DLP modules make it possible to discover, protect, and manage confidential data across virtually any storage system and keep all of your unstructured data safe—no matter how quickly it grows.

Monitor and Protect Your Data in Motion

Studies show that about half of all employees regularly email work files to their own personal accounts, so it's no wonder that email and web are the most common channels for data loss. **Symantec DLP Network Monitor, Network Prevent for Email, and Network Prevent for Web** can help eliminate this nearly universal problem—by giving you the ability to monitor a wide range of network protocols and prevent both authorized and unauthorized network users from mishandling confidential data.

First, **Network Monitor** detects confidential data sent over a wide range of network protocols—including SMTP, HTTP, FTP, IM, NNTP, custom port-specific protocols, and Internet Protocol Version 6 (IPv6). It 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. Network Monitor is deployed at network egress points and integrates with your network tap or Switched Port Analyzer (SPAN).

Next, **Symantec DLP Network Prevent for Email** inspects corporate email for confidential data, notifies users of policy violations, and blocks or routes email to encryption gateways for secure delivery. Network Prevent is also deployed at your network egress point and integrates with your SMTP-compliant Mail Transfer Agent (MTA) and cloud services such as Symantec Email Security.cloud.

Finally, **Symantec DLP Network Prevent for Web** inspects outbound traffic sent over HTTP and HTTPS, notifies users of policy violations, and blocks or conditionally removes data from web posts. Like the other two modules, Network Prevent for Web is deployed at your network egress point, and it integrates with ICAP-compliant Web proxies and cloud services such as Google Apps and Symantec Web Security.cloud.

Start Building Your Unified Information Protection Solution Today

Symantec is ready to help you extend data loss prevention to the cloud and across all of your high-risk data loss channels, so you can discover, monitor, and protect your information more completely and effectively—whether it's at rest, in motion, or in use.

Visit Symantec.com/data-loss-prevention to learn more—and discover the advantages of a unified approach to data loss prevention foundation that's built for today's mobile, cloud-centered world.

System Requirements

Symantec DLP consists of a unified management platform, content-aware detection servers, and lightweight endpoint agents. It also offers you a variety of flexible deployment options, including on-premise, hybrid cloud, and as a managed service (through a Symantec DLP Specialized Partner). Unlike other DLP solutions, Symantec has proven its ability to work in highly distributed environments and scale up to hundreds of thousands of users and devices.

DLP Servers

Operating System	Microsoft Windows Server 2008, 2012 Red Hat Enterprise Linux VMware ESX and ESXi
Processor	2 X 3.0 GHz CPU
Memory	6 to 8GB
Storage	140GB
Network	1 Copper or Fiber 1GB/100MB Ethernet NIC
Database	Oracle 11g Standard Edition

DLP Endpoint Agents

Operating System	Apple Mac OS X Microsoft Windows Microsoft Windows Server 2003, 2008 Citrix XenApp and XenDesktop Microsoft Hyper-V VMware Workstation and View
Memory	25 to 30MB
Storage	70 to 80MB

More Information

Visit our website

http://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 an information protection expert that helps people, businesses, and governments seeking the freedom to unlock the opportunities technology brings—anytime, anywhere. Founded in April 1982, Symantec, a Fortune 500 company operating one of the largest global data intelligence networks, has provided leading security, backup, and availability solutions for where vital information is stored, accessed, and shared. The company's more than 20,000 employees reside in more than 50 countries. Ninety-nine percent of Fortune 500 companies are Symantec customers. In fiscal 2014, it recorded revenue of $6.7 billion. To learn more go to www.symantec.com or connect with Symantec at: go.symantec.com/socialmedia.

Symantec World Headquarters

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