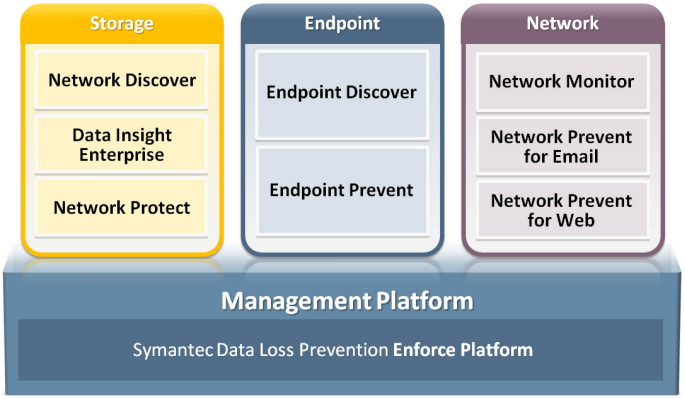
Symantec Data Loss Prevention for Storage

Discover, monitor, and protect sensitive data stored throughout your organization



Overview

Symantec™ Data Loss Prevention for Storage helps you find and protect sensitive information stored throughout your organization. The challenge entails finding information that can be stored almost anywhere and owned by almost anyone. Compounding the problem, unstructured data is growing at an annual rate of 60%. The full Data Loss Prevention for Storage solution taps three products, which discover stored confidential data throughout the enterprise; monitor the ownership and use of stored data; and protect sensitive data according to centrally administered policies. Data Loss Prevention for Storage products can be used individually or together as a complete solution to reduce the risk of data loss.

Discover stored data

Symantec™ Data Loss Prevention Network Discover finds sensitive data stored throughout the organization. It discovers sensitive data using one or more policy-based Symantec detection technologies:

Describe looks for data matching keywords, expressions or pattern or file type recognition.

Fingerprinting looks for exact matches of whole or partial files, usually in highly specific and centralized sources of data.

Learning looks for sensitive data using Symantec's exclusive Vector Machine Learning technology that develops detection policies based on sample documents such as source code, confidential reports, legal contracts, and other sensitive data.

Network Discover recognizes over 330 file types. It can be configured to recognize any custom file type, and a content extraction API accommodates creation of plug-ins for extracting text from almost any file format.

Key features

- *Scan essentially any data repository*, including file servers, databases, and web sites. Comprehensive coverage means you get visibility of all sensitive data, so you can take measures to reduce the risk of data loss.
- *When a sensitive file is found, a rich set of incident data* is provided to the information security team about exposed confidential information, including file owner and location, file content, and file permissions.
- *Fast and efficient scanning,* with minimal impact on the network, is managed by scan filters, schedule windows, scan throttling, and incremental scanning.

How it works

- *For compliance*, the audit team was able to prepare for the Payment Card Industry Data Security Standard (PCI DSS) Qualified Security Assessor's audit by using Network Discover to automatically locate exposed cardholder data throughout the enterprise.
- *For protecting business secrets,* Network Discover automatically locates inappropriately exposed sensitive data throughout the enterprise so that it can be moved to a secure location.

Monitor stored data

Symantec™ Data Loss Prevention Data Insight Enterprise tracks network file usage and can tell you who owns the files stored on network file servers. It also tells you who is accessing sensitive files and how often the files are being accessed. Data Insight Enterprise provides valuable storage

management features: It identifies files that are no longer accessed and can track storage consumption trends by department and organization.

Key features

- *Identifies who* is looking at confidential data and how often they are looking at it.
- *Scans the file system* to identify files and folders with broad access permissions.
- *Triggers policy-based alarms* for unusual events, such as when someone accesses sensitive data for the first time, downloads a confidential file, or downloads an unusual number of files in a particular duration of time.
- Monitors Microsoft Windows®, NetApp®, and EMC® network attached storage systems.

How it works

- *For compliance*, the audit team used Data Insight Enterprise to find out who accessed files and folders that contained inappropriately exposed cardholder data and to review access history and access permissions.
- *For protecting business secrets,* the security team used Data Insight Enterprise to identify owners of inappropriately exposed, pre-released, financial files in order to notify owners of how to take steps to secure their information.

Protect stored data

Symantec™ Data Loss Prevention Network Protect remediates exposure of sensitive data. It does this by automatically informing owners of exposed data and lets them know how they can secure it. In addition, Symantec Network Protect FlexResponse™ can automatically encrypt, quarantine, copy, remove, or apply enterprise rights management policies to exposed sensitive data.

Key features

- *Automatic data owner notification* of a policy violation, including instructions on how to secure and protect sensitive files.
- *FlexResponse* support for file encryption and digital rights management solutions from PGP™, Oracle®, GigaTrust™ and Microsoft®.

How it works

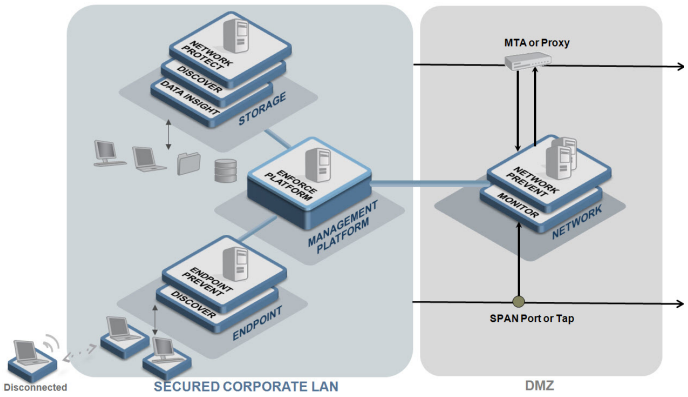
- *For compliance*, the audit team used Network Protect to automatically move files containing inappropriately exposed cardholder and other regulated data into protected locations in order to comply with regulations.
- *For protecting business secrets,* the security team used Network Protect FlexResponse to automatically encrypt inappropriately exposed sensitive data with PGP™ NetShare from Symantec™.

Manage network policies and incidents

Symantec™ Data Loss Prevention Enforce Platform is an included web-based solution that serves as the central management console for Symantec Data Loss Prevention for Storage. With the Enforce Platform, users create policies to automatically detect and protect sensitive data, perform incident workflow and remediation, generate reports, and configure role-based access and system management options. The Enforce Platform unifies the Symantec Data Loss Prevention solution suite with universal policies and reporting. A single data loss policy can be deployed across all products, and reports include unified dashboards that can combine information from all products on a single page. For more information, see the Enforce Platform data sheet.

Technical Specifications

System Architecture



System Requirements

Operating System - Network Discover and Network Protect	Microsoft Windows Server® 2003, Enterprise Edition (32-bit) SP2 or higher Microsoft Windows Server® 2008, Enterprise Edition (64-bit) R2 or higher Red Hat Enterprise Linux® 5 (32-bit or 64-bit), update 2 or higher
Operating System - Data Insight	Microsoft Windows Server 2003, Enterprise Edition (32-bit) with SP2 or higher
Processor	Small/Medium Enterprise: 2 x 3.0 GHz CPU Large Enterprise: 2 x 3.0 GHz Dual-Core CPU
Memory	Small/Medium Enterprise: 6-8 GB RAM Large Enterprise: 8-16 GB RAM
Storage	140 GB Ultra SCSI; 500 GB (Data Insight)
Network	1 Copper or Fiber 1 GB/100 MB Ethernet NIC
Virtual Support - Network Discover and Network Protect	VMware® ESX Server 3.5 (32-bit or 64-bit hardware) VMware® ESX Server 4.0 (64-bit hardware)
Virtual Support - Data Insight	VMware ESX Server 3.5 or higher
Supported Data Repositories - Network Discover	Databases: Oracle®, Microsoft SQL Server®, IBM DB2®, etc. Collaboration platforms: Lotus Notes®, Microsoft® Exchange, Microsoft Outlook® .pst, Microsoft SharePoint®, Documentum®, LiveLink®, etc. Websites: public, intranets, extranets, wikis, web- based applications Storage on desktops and laptops
Supported File Servers - Data Insight	NetApp Data ONTAP® 7 or later EMC Celerra® DART version 5.6.45 or later Microsoft Windows Storage Server® 2003 SP1 or later (both 32- and 64-bit) Microsoft Windows Server 2008 R2(64-bit using the CIFS protocol, including DFS)
Integration with Data Protection Solutions - Network Protect	PGP™ NetShare from Symantec™, Microsoft® Windows Rights Management Services, Oracle® Information Rights Management, Liquid Machines™, and GigaTrust™

More Information

Visit our website

http://enterprise.symantec.com

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 is a global leader in providing security, storage, and systems management solutions to help consumers and organizations secure and manage their information-driven world. Our software and services protect against more risks at more points, more completely and efficiently, enabling confidence wherever information is used or stored. Headquartered in Mountain View, Calif., Symantec has operations in 40 countries. More information is available at www.symantec.com.

Symantec World Headquarters

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

Symantec helps organizations secure and manage their information-driven world with **IT Compliance**, **discovery and retention management**, **data loss prevention**, and **messaging security** solutions.

21194670 06/11

Confidence in a connected world. Symantec.