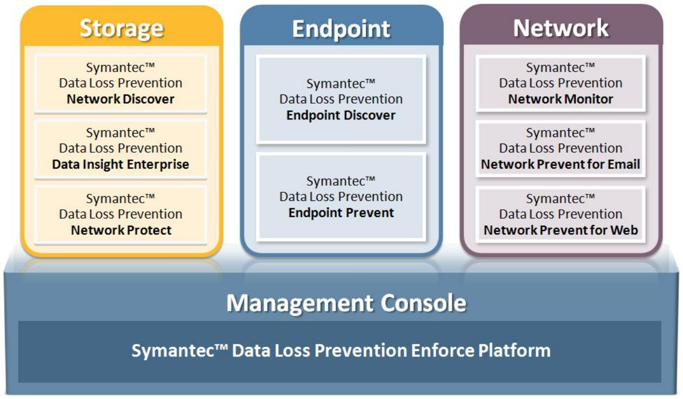
Data Sheet: Data Loss Prevention

Symantec™ Data Loss Prevention for Endpoint

Discover, monitor, and protect sensitive data on laptops and desktops. Anytime. Anywhere.


Storage
Symantec™ Data Loss Prevention Network Discover
Symantec™ Data Loss Prevention Data Insight Enterprise
Symantec™ Data Loss Prevention Network Protect
Endpoint
Symantec™ Data Loss Prevention Endpoint Discover
Symantec™ Data Loss Prevention Endpoint Prevent
Network
Symantec™ Data Loss Prevention Network Monitor
Symantec™ Data Loss Prevention Network Prevent for Email
Symantec™ Data Loss Prevention Network Prevent for Web
Management Console
Symantec™ Data Loss Prevention Enforce Platform

Overview

Symantec™ Data Loss Prevention for Endpoint addresses the risks associated with the storage and use of confidential data on laptops and desktops across your organization. Data Loss Prevention for Endpoint discovers confidential data wherever it resides and identifies those endpoints with the highest risk. It also actively monitors the many ways confidential data can be used on the endpoint and flags any activity not in accordance with policy.

This software-based solution consists of two products operating off of the same endpoint agent: ***Symantec™ Data Loss Prevention Endpoint Discover*** and ***Symantec™ Data Loss Prevention Endpoint Prevent***. Together, these products:

- Allow organizations to monitor and protect more endpoint activity than other solutions.
- Provide more choices in how to address and remediate incidents.
- Use technology specifically designed to operate in the most efficient and unobtrusive manner possible.

Discover data on endpoints

Endpoint Discover scans laptop and desktop hard drives for confidential data in order to inventory, secure or relocate it. Over 60 templates are provided to enable out-of-the-box discovery of sensitive data mapped to different industry and regulatory directives. Initial scans for confidential data are run when the endpoint is idle. Subsequent scans are run on only those things that have changed since the previous scan. Endpoint Discover provides three different detection technologies to address different types of data:

Describe looks for data matching keywords, expressions or patterns, file type recognition, and other signature-based detection technologies.

Fingerprinting looks for exact matches of whole or partial files, coming from structured sources (e.g., databases) and unstructured sources (e.g., design documents) that are fingerprinted with a hashing algorithm.

Learning looks for unstructured data such as source code, Intellectual Property (IP), or legal contracts that it is able to identify by building a statistical model based on uploading positive and negative example documents.

Key features

- *Accurate Discovery* - Accurately identify the confidential data and IP that exists on your endpoints while minimizing the false positives (incorrect identification) and false negatives (missed identification).
- *Actionable Discovery* - Automatically quarantine (or move) files containing specific confidential data upon discovery and rank your endpoints with the most confidential data in order to prioritize your protection efforts.
- *Efficient Discovery* – Scan only when idle, scan only what has changed, and limit the resources used for the scan.

How it works

- ***For compliance*** - employees on a retail sales analysis team were careless in saving unencrypted cardholder data onto their laptops. Endpoint Discover automatically discovered the inappropriately exposed cardholder data along with information about the data. Documentation provides forensic evidence for the Payment Card Industry Data Security Standard (PCI DSS) audit.

- ***For protecting business secrets*** – a technology company that allows developers to work remotely must be able to inventory where their proprietary source code exists in order to prioritize their full-disk encryption deployment. Endpoint Discover used the Learning detection method to identify the endpoints that had proprietary source code on them and ranked the endpoints according to risk so they could be secured first.

Monitor and protect data on endpoints

Endpoint Prevent provides the most extensive coverage of end user activity in the market, and it does so in a "context-aware" manner. This means that how the data is being used is as important as what data is being used in determining whether to allow the action or not. For example, an organization could allow customer data to be exchanged as part of an authorized application, but would prevent it from being copied to a USB or CD/DVD device (the WikiLeaks method).

Endpoint Prevent provides broad event coverage over the many ways that data loss can happen on the endpoint and matches that coverage with a broad set of remediation capabilities to properly respond to incidents. It is deployed in a scalable, multi-tiered architecture and provides protection against data loss whether the user is connected to the network or not.

Key features

- Event coverage includes downloading files, copying files to CD/DVD/USB/iPod®/Bluetooth®, and other removable media; communications over email, Instant Messaging (IM), and the Web; and support for virtual Citrix® environments.
- Trusted Device support enables organizations to define specific removable media devices that can be used with confidential data, providing a more granular level of protection while still enabling required business functions.
- Application File Access Control secures the use of confidential data in endpoint applications such as Facebook®, LinkedIn®, Cisco® WebEx, IM, and Twitter®.
- Broad remediation capabilities: onscreen pop-up notifications; quarantining or relocating data to a secure location; blocking endpoint events; and applying custom responses via the FlexResponse feature, such as applying encryption to a file using the Symantec™ Endpoint Encryption FlexResponse.

How it works

- ***For compliance*** - employees on a retail sales analysis team were careless in saving unencrypted cardholder data on their laptops. Endpoint Prevent automatically encrypted the data and notified data owners of this policy violation. Documentation provides evidence of remediation for the PCI DSS audit.
- ***For protecting business secrets*** - a rogue employee tried to steal business intellectual property by copying it to a USB storage stick. Endpoint Prevent automatically disabled the device to prevent copying and the data owners were notified of the incident. Documentation provides evidence of remediation for internal audit.

Supported Endpoint Event Coverage

Endpoint Events	Network File Transfer (HTTP, IM, FT)
	Email (Microsoft® Outlook® , IBM® Lotus Notes®)
	HTTPS (Microsoft® Internet Explorer®, Mozilla® Firefox®)
	Copy/Paste
	Print/Fax
	Internal Drive(s)
	USB, Apple® FireWire® , SD/CF Cards, SCSI Storage
	CD/DVD
	Network Shares
	Application File Access Control

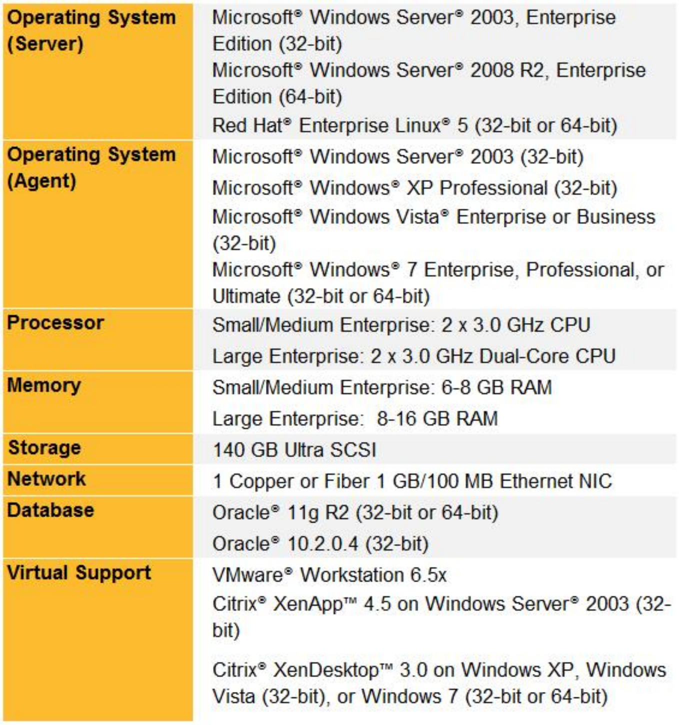
Manage network policies and incidents

The Symantec™Data Loss Prevention Enforce Platform is the central web-based management console and incident repository that is included with Data Loss Prevention for Endpoint and is used across all Symantec Data Loss Prevention products. It is where you define, deploy, and enforce data loss policies, respond to incidents, analyze and report policy violations, and perform system administration.

The Enforce Platform is deployed on a single server and is supported by an Oracle® database, which stores historical incident and system information.

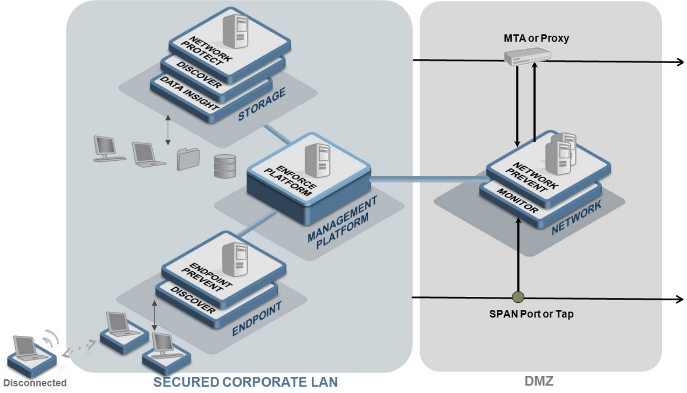
For more information, please download the Enforce Platform data sheet.

System Requirements



Operating System (Server)	Microsoft® Windows Server® 2003, Enterprise Edition (32-bit) Microsoft® Windows Server® 2008 R2, Enterprise Edition (64-bit) Red Hat® Enterprise Linux® 5 (32-bit or 64-bit)
Operating System (Agent)	Microsoft® Windows Server® 2003 (32-bit) Microsoft® Windows® XP Professional (32-bit) Microsoft® Windows Vista® Enterprise or Business (32-bit) Microsoft® Windows® 7 Enterprise, Professional, or Ultimate (32-bit or 64-bit)
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
Network	1 Copper or Fiber 1 GB/100 MB Ethernet NIC
Database	Oracle® 11g R2 (32-bit or 64-bit) Oracle® 10.2.0.4 (32-bit)
Virtual Support	VMware® Workstation 6.5x Citrix® XenApp™ 4.5 on Windows Server® 2003 (32-bit) Citrix® XenDesktop™ 3.0 on Windows XP, Windows Vista (32-bit), or Windows 7 (32-bit or 64-bit)

System Architecture



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. 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.

Confidence in a connected world. Symantec.