Symantec™ Data Loss Prevention for Network

Monitor and protect data leaving your network over mobile devices, the cloud, and Web 2.0

Overview


Data Loss Prevention for Network monitors network communications and detects sensitive data that is being sent in violation of your security policy. When a policy is violated, it routes messages to an encryption gateway, removes confidential information from web posts, quarantines messages to a secure server, or blocks email and web communications.

Monitor your network without disrupting business

Network Monitor passively inspects network traffic for confidential data that is being sent in violation of security policy. It is deployed at egress points in the network demilitarized zone (DMZ) with a network tap or Switched Port Analyzer (SPAN).

Network Monitor performs deep content inspection of all network communications with no packet loss, unlike other data loss prevention (DLP) solutions which may only sample packets during peak loads and put you at greater risk for data loss.

Key features

- Monitors high-risk protocols: email (SMTP/TLS), Web (HTTP/HTTPS), IM, and FTP.
- Monitors non-standard and proprietary protocols including BitTorrent and FastTrack®.
- Scales to hundreds of thousands of global network users.

How it works

A leading fitness center chain uses Network Monitor to protect their intellectual property and comply with the Payment Card Industry Data Security Standard (PCI DSS). They inspect network traffic for membership pricing plans and members’ personally identifiable information (PII), including check routing numbers and credit card numbers.

Prevent data loss over outbound email

Network Prevent for Email redirects, quarantines, or blocks outbound messages containing sensitive data. It is deployed at egress points in the network DMZ and integrates with your existing on-premise, public or private cloud messaging infrastructure.

Network Prevent for Email provides comprehensive protection for managed and unmanaged endpoints, including mobile devices that access your corporate email systems.

Key features

- **Corporate email protection for smartphones and tablets** running Google® Android™, Apple® iOS, BlackBerry®, and Windows® Mobile.
- **Redirects unencrypted messages** to an encryption gateway for secure delivery.
- **Quarantines or relocates email** containing sensitive data to a secure location for end-user review and release.
- **Broad integration support** for enterprise messaging gateways, Mail Transfer Agents (MTAs), and hosted email solutions such as Microsoft® Online Services.
How it works

A large education services company uses Network Prevent for Email to protect their students’ PII. They monitor email traffic and block or route messages containing United States social security numbers to an encryption gateway for secure delivery.

Prevent data loss over the Web

Network Prevent for Web blocks or removes sensitive data from outbound web communications if they violate security policy. It is deployed at egress points in the network DMZ and integrates with your on-premise, public or private cloud messaging infrastructure.

Network Prevent for Web provides comprehensive protection for managed and unmanaged endpoints, including mobile devices, that access the Web through your corporate network.

Key features

- Corporate web protection for smartphones and tablets running Google Android, Apple iOS, BlackBerry, Windows Mobile.
- Cloud and social media protection for Salesforce.com™, Facebook®, Twitter®, YouTube™, and LinkedIn®.
- Hosted web and security services support for Symantec.cloud, Google Apps™, and Microsoft® Online Services.
- Exclusive enhanced web blocking seamlessly strips sensitive data from web posts.
- Broad integration support for existing enterprise web proxies and gateways.

How it works

A major financial services company uses Network Prevent for Web to protect their customers’ PII. It monitors web traffic and blocks communications containing proprietary information, such as pricing and financial results.

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 Network 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.

Technical Specifications

System Architecture
Data Sheet: Data Loss Prevention
Symantec™ Data Loss Prevention for Network

System Requirements

|------------------|---------------------------------------------------|
|                  | Microsoft® Windows Server® 2008 R2, Enterprise Edition (64-bit)  
|                  | Red Hat® Enterprise Linux® 5 (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: 8-16 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 only)  
| Virtual Support  | VMware® ESX Server 3.5  
|                  | VMware® ESX Server 4.0  

| MTA | Network Prevent for Email integrates with any SMTP-compliant MTA  
| Web Proxy | Network Prevent for Web integrates with the following certified web proxies:  
|          | - Blue Coat® ProxySG, NetCache®  
|          | - Cisco® IronPort® S-Series  
|          | - Microsoft® ISA  
|          | - McAfee® Web Gateway  
|          | - Squid  
|          | - Symantec® Web Gateway  

Additional Symantec Data Loss Prevention products

Data Loss Prevention delivers a unified solution suite to discover, monitor, protect, and manage sensitive data wherever it is stored or used.

Symantec™ Data Loss Prevention for Endpoint

- **Symantec™ Data Loss Prevention Endpoint Discover** scans for sensitive data stored on laptops and desktops in order to inventory, secure, or relocate the data.

- **Symantec™ Data Loss Prevention Endpoint Prevent** monitors and blocks confidential data from being transferred, sent, copied, or printed by desktop or laptop users.

Symantec™ Data Loss Prevention for Storage

- **Symantec™ Data Loss Prevention Network Discover** identifies sensitive data exposed on file servers, collaboration platforms, websites, desktops, laptops, and other data repositories.

- **Symantec Data Loss Prevention Data Insight** is for governance of unstructured data.

- **Symantec™ Data Loss Prevention Network Protect** remediates exposure of sensitive data.

How to learn more about Data Loss Prevention

**Visit our website**


**Speak with a Data Loss Prevention Product Specialist in the U.S.**

Call (415) 829-5013

**Speak with a Data Loss Prevention 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.

**Symantec World Headquarters**

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

Copyright © 2011 Symantec Corporation. All rights reserved. Symantec and the Symantec 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.

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