Solution Brief

Symantec® Data Loss Prevention Core Solution

Use Cases

- Gain greater visibility and understanding of your organization's sensitive data.
- Discover where data lives and monitor how it is being used as it moves across all channels.
- Protect critical data with targeted controls and policies based on user risk and sensitivity level.
- Pinpoint risky behavior so you can stop careless, compromised or malicious users in their tracks.
- Protect data in use on endpoints on and off network, and enable secure remote work.
- Scan and remediate data at rest stored across file servers, endpoints, file shares, databases, SharePoint, and more.
- Monitor email and web channels in real-time and take immediate action to prevent accidental exposure and sharing.
- Meet compliance requirements for global data protection regulations and standards.
- Seamlessly extend data loss prevention to the cloud without disjointed policies.

10X Gartner Magic Quadrant Leader for DLP

Symantec Data Loss Prevention is a proven solution that analyst firms including Gartner, Forrester, IDC, and others recognize as a global market leader.

Extends data loss prevention across the enterprise, detects insider risks, and protects critical information from exfiltration

Solution Benefits

- Protects brand reputation, intellectual property, regulated data, and other sensitive information
- Provides visibility into where sensitive data lives and moves at the endpoint, in storage, and over networks
- Provides comprehensive channel coverage and advanced content inspection
- Simplifies incident triage, streamlines remediation, and detects risky behaviors and insider threats
- Reduces complexity with a single unified platform for on-premises and hybrid cloud environments

Establish a Zero-Trust Foundation with Core Data Security Capabilities

Keeping information safe and remaining compliant has never been easy. Today we face complex and evolving data security challenges that often translate into barriers for organizations, their employees, and the customers they serve. The COVID-19 pandemic has created a sudden and lasting shift to remote work and accelerated digital transformation agendas. The perimeter-less, zero-trust world is forcing security leaders to rethink their data protection programs to improve business productivity while mitigating new threats and reducing the risk of costly data breaches.

In addition, constantly changing standards and regulations around data protection are putting pressure on security and risk teams to keep pace with a myriad of compliance obligations—many of which require translating complex national, regional, and industry requirements into specific technical controls and organizational measures.

Symantec Data Loss Prevention Core solution expands your data security foundation and puts your organization on the path to Zero Trust. By combining our industry-leading enterprise Data Loss Prevention (DLP) with integrated User and Entity Behavior Analytics (UEBA), we provide visibility and control for sensitive information wherever it lives and travels across devices and on-premises environments so you can prevent accidental sharing of data, stop insider risks, and enforce compliance requirements.

Solution Differentiators

Extensive Visibility and Control for Data In Use, At Rest, and In Motion
Through deep content inspection and contextual analysis, DLP provides a comprehensive understanding of where sensitive data lives, how it moves across users, devices and networks, and when it is at most risk for exposure so that you can prevent data leaks and data exfiltration attempts.

Full Incident Details and Context of Data at Risk Speeds Up Investigation
Our intuitive management console makes it easy for you to rapidly investigate incidents and fully understand data loss risks. It provides all the enriched incident data that you need at your fingertips such as policies violated, response actions, matches detected, custom attributes, attribute correlations, incident history, and more.

Automated and Manual Actions Remediate Critical Incidents Quickly
Advanced incident remediation capabilities enable you to automatically respond to incidents as they arise without user intervention, manually intervene for more serious incidents with one-click SmartResponses, and distribute incidents to data owners for review. Enforcement actions include escalate, notify, redirect, quarantine/restore, and block.

Change User Behavior with Coaching and Education
Empower your employees to make smart decisions about handling sensitive data and lower organizational risk—rather than circumventing security controls—by using real-time notifications that guide their actions and educate on data protection policies as they interact with the data.

Unrivaled Content Detection Follows Your Data Everywhere
Go beyond regex pattern matching that can lead to high false positive rates and protect your data with sophisticated detection algorithms and techniques such as Exact Data Matching, Indexed Document Matching, Vector Machine Learning, and Sensitive Image Recognition.

Centralized Policies and Granular Controls Ensure Safe Data Usage Without Slowing Down Employees
Our powerful policy engine gives you fine-grained control over how users and applications can share, transfer and interact with sensitive data. In a single policy, you can combine multiple detection methods for precision, compound matching conditions for accuracy, and group rules and exceptions for individualization. Prevent risky and careless behavior that might compromise data while enabling employees to get their job done both online and off.

User and Entity Behavior Analytics Pinpoints and Prioritizes Problems into Actionable Insights
Backed by patented machine learning, our user and entity behavior analytics platform continuously baselines your users' normal activities and flags risky behavior and bad actors via comparative risk scoring. Its adaptive risk models, customizable dashboards, and point-and-click interface provides advanced investigation capabilities and response workflows so security analysts can address the users and risks that matter most to your organization.

Product	Details
DLP for Endpoints	**DLP Endpoint Discover** scans local hard drives and gives you visibility into any sensitive data stored by users on laptops and desktops and establishes a baseline inventory. It provides a number of responses including quarantining files, flagging files for Symantec Endpoint Protection, as well as custom response actions such as encryption, DRM, or redacting confidential information enabled by the Endpoint FlexResponse API. **DLP Endpoint Prevent** monitors users' activities and enables fine-grained control over a wide range of applications, devices, and platforms. It provides a wide range of responses including identity-based encryption and DRM for files transferred to USB. With Endpoint Prevent, alert users to incidents using on-screen pop-ups or email notifications. Users can also override policies by providing a business justification or canceling the action (in the case of a false positive).
DLP for Storage	**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. It provides high-speed scanning for large, distributed environments, and optimizes performance by scanning only new or modified files. **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 DRM 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.
DLP for 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). **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. **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.
User and Entity Behavior Analytics	**Information Centric Analytics** is a user and entity behavior analytics (UEBA) platform that provides an integrated, contextually enriched view of cyber risks in your enterprise. It collects, correlates, and analyzes large amounts of security event data from across diverse sources, including all data exfiltration channels (data telemetry), user access (identity telemetry), corporate asset data, and alerts from other security systems (threat telemetry). Backed by patented machine learning, ICA delivers rapid identification and prioritization of user and entity-based risks.
Sensitive Image Recognition	**Optical Character Recognition** provides the capability to extract text from images (scanned documents, screen shots, pictures, and so on). **Form Recognition** detects form images that contain sensitive data in a wide variety of image formats including Microsoft Office documents, PDF and JPEG.

Symantec™
A Division of Broadcom

For product information and a complete list of distributors, visit our website at: broadcom.com

DLP-Core-Pkg-SB100 December 18, 2020