WHITE PAPER

When *Good Enough* Isn’t Good Enough

Data Protection Where It Matters

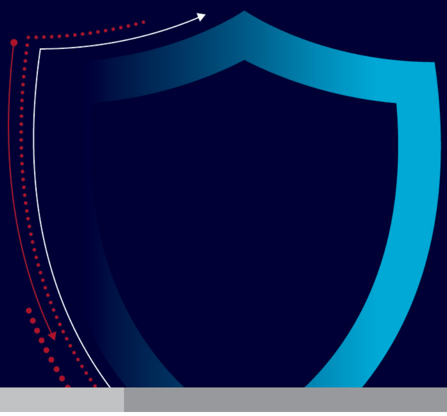


TABLE OF CONTENTS

Introduction

Organizations should evaluate data protection solutions considering the total cost of ownership, not just the purchase price. This paper guides the reader through the relevant factors in this evaluation process, and is based on the understanding of Microsoft product capabilities as of April 2023.

This paper is intended for data owners: CFOs, Data Protection Officers (DPOs), HR managers, PR specialists, risk and compliance managers, and engineering leaders who are responsible for protecting their organizations’ critical data. Data protection specialists, such as information, operational, and information/communication technology professionals who implement and manage data protection technologies and processes will also find value in this paper, as it will prove beneficial for communicating with data owners.

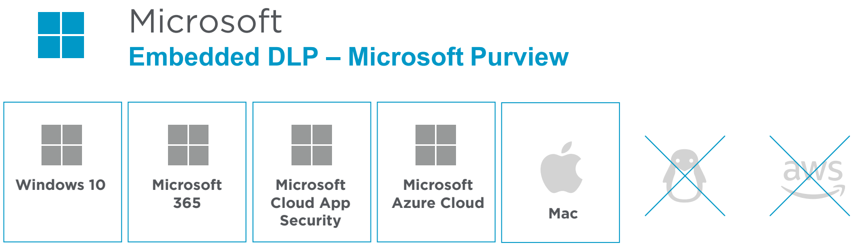
Two Philosophies of Data Protection

Microsoft and Symantec® data loss prevention (DLP) solutions are each in pursuit of fundamentally different goals. The differences ripple through every feature offered by the two solutions, and define the difference between good enough and enterprise-grade data protection.

Microsoft

Microsoft embeds data protection features into its authoring tools (tagging), platforms, and services, specifically Windows 10, Microsoft (Office) 365, Microsoft Cloud App Security (MCAS), and Azure Cloud. Collectively, the company calls these features Microsoft Purview Information Protection (MPIP).

This Microsoft approach offers basic protection for unstructured content created predominantly using Microsoft tools, with some support for non-Microsoft file formats. It is an acceptable choice for first-time DLP users whose sensitive data is maintained entirely within Microsoft environments, and for non-enterprise organizations for which data loss is not a strategic concern.

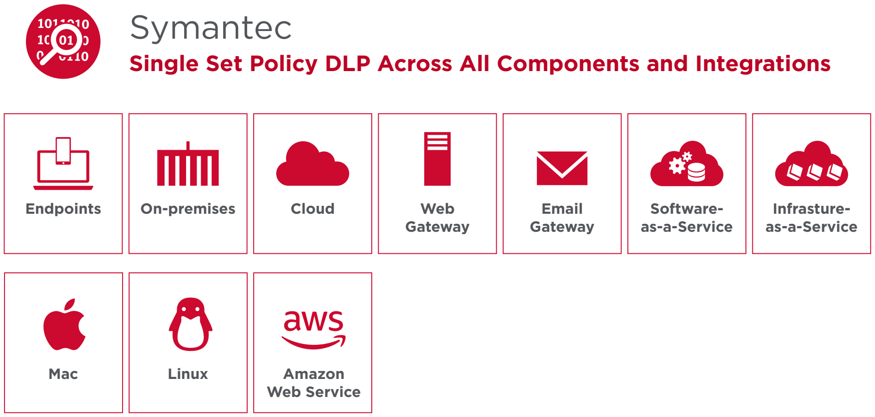

Microsoft
Embedded DLP – Microsoft Purview

Symantec

The Symantec portfolio of purpose-built solutions protects endpoints and on-premises and Cloud data, with integrations that apply DLP protection to other control points: web and email gateways, and cloud applications in both software as a service (SaaS) and infrastructure as a service (IaaS) environments. It is an agnostic data protection solution for data in use, in motion, or at rest in any channel or environment.

Symantec DLP protects data in Microsoft and non-Microsoft environments, applications, and files, including structured data and images. Symantec DLP applies a single set of policies across all components and integrations. Designed for and widely adopted by large enterprises, Symantec DLP offers a comprehensive risk-based solution that meets the needs of large enterprises who place a high priority on data protection.

SYMANTEC DLP IS AN AGNOSTIC DATA PROTECTION SOLUTION FOR DATA IN USE, IN MOTION, OR AT REST IN ANY CHANNEL OR ENVIRONMENT


Symantec
Single Set Policy DLP Across All Components and Integrations

Critical Choices in DLP

Robust enterprise-grade DLP meets the following criteria:

Comprehensive

Covers all sensitive information no matter how old, wherever it is stored, and however it is transmitted

Policy-Driven

Consistently enforces every regulatory requirement, industry-standard, and organizational policy across all covered applications, devices, and environments

Practical

Links configuration and management to established operational processes to save time, money, and personnel

Informative

Connects policy noncompliance and exfiltration events with all necessary context, for measured and effective response and escalation.

Affordable

End-to-end lifetime cost of ownership aligns with the value of the protections it confers

Applying these criteria to Microsoft and Symantec solutions in the following sections illustrates the difference between good enough feature-based protection and enterprise-grade DLP.

WHAT DATA WILL YOU PROTECT, OR CONVERSELY, WHAT DATA ARE YOU PREPARED TO OVERLOOK?

Comprehensive

The most important decision in data loss prevention is comprehensive coverage:

- What data will you protect, or conversely, what data are you prepared to overlook?

Coverage applies to the first step in DLP discovery, as data is everywhere in the modern enterprise:

- What servers, endpoints, data stores, etc. will you scan for sensitive information?
- What file types and sizes?
- Will you include both structured (database) and unstructured (e.g., text or spreadsheet) information?
- What about obsolete formats like Lotus 1-2-3, WordStar, or Microsoft Works?
- Have you considered images and email attachments?

The second part of coverage involves monitoring:

- What data paths, environments, and endpoints will you watch for sensitive data in motion, at rest, or in use?

A SIDE-BY-SIDE COMPARISON OF COVERAGE AND MONITORING REVEALS CRITICAL GAPS

Consistent with the Microsoft philosophy of protecting data created using its own tools, MPIP identifies and monitors a small subset of the sensitive information organizations need to safeguard. The Symantec vendor-agnostic approach applies consistent data protection policies over the entire range of enterprise data.

A side-by-side comparison of coverage and monitoring reveals critical gaps:

Coverage	Microsoft	Symantec
Data Channels and Pathways		
On-Premises Servers and Storage	*Limited scan speed and scan targets*	*Up to 2 TB per hour speed and rich scan support*
IaaS Cloud Data Storage	*AWS, S3 buckets, Google*	*AWS, S3 buckets, Google*
Web Gateways, On Premises and Off Premises	*No*	*Yes*
Email Archives and Attachments	*Microsoft 365*	*Microsoft 365, Gmail, and more*
Endpoint-Attached Storage	*No*	*Yes*
Bring Your Own Device Storage	*No*	*Yes*
Content Inspection of Unsanctioned Applications	*No*	*More than 200 applications*
Environments		
OS Platforms	*Windows 10, 11, and three latest Mac releases*	*Current and legacy Windows, Mac, Linux*
Web, Using Browsers	*Chrome, Firefox, Edge, Safari, etc.*	*Chrome, Firefox, Edge, Safari, etc.*
Structured Databases: Oracle, MS SQL, IBM Db2, etc.	*Yes*	*Yes*
Loss/Exfiltration Vectors		
Upload to Web or Cloud	*Yes*	*Yes*
Copy to Clipboard	*Yes*	*Yes*
Copy to Removable Media (USB), Local Drive, or Share	*Yes*	*Yes*
Print	*Yes*	*Yes*
Images: Print Screen, Photo, Scan, etc.	*No*	*Yes, plus optical character recognition*
File Characteristics		
File Types, Including Legacy and Obsolete Files	*Fewer than 50 file types*	*More than 375 file types*
Large Files and Attachments	*No, 1 MB extracted text limit*	*Yes*
Scanning, Applies Primarily to Cloud		
Continuous	*Yes, with a longer SLA*	*Yes*
Exhaustive	*No*	*Yes*

Practical

Awareness of DLP policy exceptions is not enough. Organizations must also act to remediate any damage and prevent future incidents or false alarms. Integrating incident response, remediation, and other actions into practical workflows can make the difference between a data protection program that operates smoothly and effectively, and a reactive, expensive, and ultimately unsustainable program.

The different Microsoft and Symantec approaches have important consequences for the practical administration of DLP programs at the enterprise level. Symantec DLP automates processes as much as possible, and integrates administrative decision-making into established workflows, avoiding reactive fire drills in favor of smooth, efficient operations.

SYMANTEC DLP AUTOMATES PROCESSES AS MUCH AS POSSIBLE, AND INTEGRATES ADMINISTRATIVE DECISION-MAKING INTO ESTABLISHED WORKFLOWS, AVOIDING REACTIVE FIRE DRILLS IN FAVOR OF SMOOTH, EFFICIENT OPERATIONS

Management and Workflow	Microsoft	Symantec
Policies		
One Set of Policies Across All Applications, Platforms, and Environments	*No*	*Yes*
Single Management Console for End-to-End DLP	*No*	*Yes*
Alerts		
Automated Warnings for Low-Level Alerts	*Yes*	*Yes*
Automated Blocking at Exit Points	*Selective, for example to Azure*	*Yes*
Remediation of Low-Level Incidents by Data Owners.	*No*	*Yes*
Prioritization		
Full Alert Context on One Page	*No*	*Yes*
Tools to Manage False Alarms	*No*	*Yes*

Policies: Microsoft data protection policies are managed individually for each application, platform, or environment. For example, even though MCAS protects several different cloud applications, policies are administered separately for each.

Symantec DLP applies a single set of policies across all on-premises and cloud environments, including their endpoints and Web and email exit points, and manages them from a single administrative console.

Alerts: DLP policy exceptions trigger alerts, which may or not rise to the level of actionable incidents. Alert response tells you how much work the DLP solution needs to do to confirm, prioritize, and escalate them, and how much of it will fall to administrative staff. Automated responses may range from pop-up user warnings to encryption of files transferred to printers, the clipboard, USB devices, or other portable storage media. Network traffic is typically redirected or blocked at network egress points or mail transfer agents.

Microsoft alerts block traffic selectively, for example, only to Azure. And data owners can't fix low-level incidents themselves, increasing the burden on administrative teams.

With Symantec DLP, alerts block data exfiltration at every exit point, and users can remediate low-level incidents without involving data protection administrators.

Prioritization: Determining which alerts constitute actionable incidents requires human judgment backed by context, and the following essential context is simply missing from Microsoft's collection of DLP features:

- Which policy was violated?
- What activity caused the violation?
- What content was involved?
- What file was involved, and where is it located?
- What user was involved; whom do you call?
- Machine name, application, Active Directory attributes, and much more.

The Symantec solution offers this contextual information and more on a single screen, ready for effective escalation and response.

DETERMINING WHICH ALERTS CONSTITUTE ACTIONABLE INCIDENTS REQUIRES HUMAN JUDGEMENT BACKED BY ESSENTIAL CONTEXT

Data protection solutions are deliberately tuned to minimize misses—undetected instances of data exfiltration—because of their potentially disastrous consequences. Most real-life alerts will be false alarms triggered by harmless activities. Without an efficient method to deal with them, false alarms will quickly overwhelm management staff and create incentives to make the system less sensitive. Microsoft offers no tools for managing false alarms or prioritizing incidents; the Symantec solution includes them on its central management console.

Escalation and Reporting: Most large organizations already have effective tools for incident escalation and reporting; ServiceNow is a leading solution. Integration with an established trouble-ticketing system vastly simplifies incident response and reduces workloads. Microsoft offers no such integration; the Symantec solution includes robust integration with ServiceNow.

Informative

Information is essential to managing and refining policies, and both automated and human response to alerts. Full contextual information helps organizations do the following:

- Determine the full extent of a breach to reduce dwell time and guide recovery, public relations, and reimbursement activities where necessary.

- Reconstruct the pattern of events that preceded the breach, to improve policies and processes to guard against another one.

- Perform forensic analysis going back well before a breach, to identify suspicious patterns of behavior and possible bad actors that contributed to it.

- Document the breach, its antecedents, and remediation measures to satisfy regulators that appropriate measures have been taken.

The full context Symantec DLP solutions provide with every alert, maintained in detailed, searchable logs, support the steady refinement of enterprise data protection for ever stronger protection.

Affordable

Determining Total Cost of Ownership (TCO) is a complex task, and software license costs are only the start. A capability as important as DLP should not be evaluated on the basis of cost alone, but total cost of ownership is essential to any calculation of risks and benefits. Effective TCO estimation tools include software, personnel, and downstream effect cost considerations:

TOTAL COST OF OWNERSHIP IS ESSENTIAL TO ANY CALCULATION OF RISKS AND BENEFITS

- **Software cost considerations** include the costs of the core DLP solution or feature set. For MPIP, these charges will be embedded in application, platform, or environment licenses; for Symantec DLP, they will be explicit:
  - Price or annual license fee
  - Upgrades
  - Vendor support charges

  Be sure to include the costs of solutions to fill coverage aps, if any, left by the core solution:

  - Critical non-Microsoft platforms and environments
  - High-risk exfiltration vectors: printers, USB drives, .txt files, images
  - Shadow IT: phones, BYO devices, Web apps, etc.
  - Web channels such as Secure Web Gateways, on-premises, and in the cloud
  - Email gateways, on-premises and in the cloud
  - Cloud-Access Security Brokers (CASB)
  - Isolation channels for quarantine of suspect traffic
  - Zero Trust Network Access portals
  - Custom solutions to protect unique brand or intellectual property
  - Support, upgrade, and maintenance costs for all the above
- **Personnel cost considerations** include staffing to implement, integrate, and manage the core and gap-filling solutions, and to perform administrative tasks manually where automated solutions are not available:
  - Costs to hire, train, and maintain a highly mobile, in-demand workforce salary premiums for highly skilled employees for required scripts or custom integrations
  - Service and consulting fees
  - Staffing to respond to alerts with poor contextual information, and manage false alarms
  - Staffing to compensate for manual discovery, policy management, prioritization, and escalation processes
  - Staffing to meet compliance and reporting requirements
  - Staffing to administer and manage multiple consoles, platforms, and tools
- **Downstream effect cost considerations** include the direct and indirect operational costs of sub-optimal DLP:
  - Inefficiencies from gap-filling solutions poorly integrated with core DLP
  - Impacts on end-user efficiency, including responses to false alarms
  - Impacts of workload from manual processes and alert storms on security operations morale and turnover

Conclusion

Microsoft Purview Information Protection offers basic DLP across a range of popular products and services. Mature organizations will go further, with a solution that encompasses five crucial criteria:

- **Comprehensive**, identifying and monitoring sensitive information across data channels, environments, exfiltration vectors, and file characteristics—including but not limited to those offered by Microsoft.
- **Policy-Driven**, with a single set of granular policies that enforce every regulatory requirement, industry standard, and organizational policy consistently across all covered applications, devices, and environments.
- **Practical**, with policies, alerts, and processes including prioritization, escalation, and reporting, linked to established tools and processes to save time, money, and personnel.
- **Informative**, presenting administrative teams with the full context they need to deliver a measured response and escalation to alerts and incidents.
- **Affordable**, with end-to-end lifetime cost of ownership aligned to the value of the protections it provides.

SYMANTEC DLP OFFERS A COMPREHENSIVE RISK-BASED SOLUTION THAT MEETS THE NEEDS OF LARGE ENTERPRISES WHO PLACE A HIGH PRIORITY ON DATA PROTECTION

BROADCOM®
connecting everything®

For more information, visit our website at: www.broadcom.com

SYM-DLP-WP104 March 10, 2025