

When *Good Enough* Isn't Good Enough: Data Protection Where It Matters

TABLE OF CONTENTS

Introduction

Two Philosophies of Data Protection

Microsoft

Symantec

Critical Choices in DLP

Comprehensive

Policy-Driven

Practical

Informative

Affordable

Conclusion

Appendix A: What's at Risk: The Costs of Good Enough DLP

Appendix B: A Taxonomy of Threats

Introduction

This paper is intended for data owners: individuals including CFOs, DPOs^a, 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.

This paper recommends that organizations evaluate data protection solutions considering the total cost of ownership, not just the purchase price, and guides the reader through the relevant factors in this evaluation process.

Two Philosophies of Data Protection

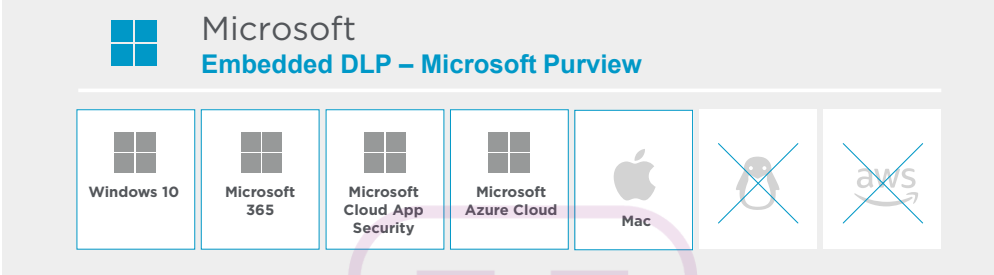
Microsoft and Symantec both offer Data Loss Prevention (DLP) solutions, but in pursuit of fundamentally different goals. The differences ripple through every solution and feature offered by the two companies, and define the difference between *good enough* and enterprise-grade data protection.

This paper is based on the Symantec understanding of Microsoft product capabilities as of April 2023.

Microsoft

Microsoft embeds data protection features into its authoring tools (e.g., tagging), platforms, and services, specifically Windows 10, Microsoft (formerly 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.



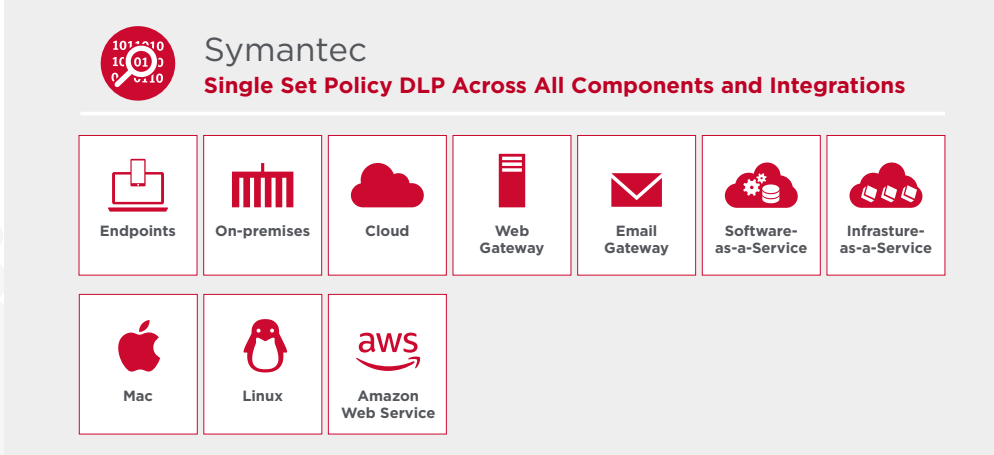
The diagram shows the Microsoft logo and the title "Microsoft Embedded DLP – Microsoft Purview". Below this, there are seven boxes representing different environments. The first four boxes, labeled "Windows 10", "Microsoft 365", "Microsoft Cloud App Security", and "Microsoft Azure Cloud", are highlighted with a blue border. The remaining three boxes, labeled "Mac", "Google", and "AWS", are crossed out with a blue 'X', indicating that the Microsoft approach does not provide protection for these environments.

Symantec

Symantec by Broadcom® offers a portfolio of purpose-built solutions that protect endpoints, 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.



The diagram shows the Symantec logo and the title "Symantec Single Set Policy DLP Across All Components and Integrations". Below this, there are ten boxes representing different components and environments. The first seven boxes, labeled "Endpoints", "On-premises", "Cloud", "Web Gateway", "Email Gateway", "Software-as-a-Service", and "Infrastructure-as-a-Service", are highlighted with a red border. The remaining three boxes, labeled "Mac", "Linux", and "Amazon Web Service", are also highlighted with a red border, indicating that Symantec provides protection for these environments as well.


Critical Choices in DLP

Robust enterprise-grade DLP meets the following criteria:

	<p>Comprehensive</p> <p>Covers all sensitive information no matter how old, wherever it is stored, and however it is transmitted</p>
	<p>Policy-Driven</p> <p>Consistently enforces every regulatory requirement, industry standard, and organizational policy across all covered applications, devices, and environments</p>
	<p>Practical</p> <p>Links configuration and management to established operational processes to save time, money, and personnel</p>
	<p>Informative</p> <p>Connects policy noncompliance and exfiltration events with all necessary context, for measured and effective response and escalation</p>
	<p>Affordable</p> <p>End-to-end lifetime cost of ownership aligns with the value of the protections it confers</p>

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?

Consistent with the Microsoft philosophy of protecting data created using its own tools, Microsoft Purview Information Protection 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^b:

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

^b Analysis based on the Symantec understanding of Microsoft product capabilities as of April 2023.

COVERAGE ESTABLISHES WHERE YOUR DATA LOSS PREVENTION SOLUTION WILL LOOK; POLICIES ESTABLISH WHAT IT WILL LOOK FOR.



Policy-Driven

Coverage establishes where your data loss prevention solution will look; policies establish what it will look for. Policy choices are determined primarily by the regulations and standards you wish to meet: DLP solutions may include pre-built policies labeled as US Regulatory Enforcement or General Data Protection Regulation. But out-of-box policies won't examine data for compliance with industry standards and company policies, cover proprietary data formats and file-transfer models, or impose higher standards than regulations alone require. Customized authoring and editing tools can accomplish all of these tasks.

Just as regulations and standards apply to the entire organization, data protection policies should be consistent across devices, applications, on-premises and cloud, etc. Fully effective DLP solutions should adapt and extend policies, considering context as well as content, using machine learning to discover new patterns in sensitive content, and leveraging user and entity behavior analytics to discover risky behavior by devices or personnel. These techniques are especially critical when users can access data in the public cloud from any location. Assessing both the risk of user access and the sensitivity of the data being accessed enables risk-adaptive controls such as restricting data downloads to unmanaged devices.

DATA PROTECTION POLICIES SHOULD BE CONSISTENT ACROSS DEVICES, APPLICATIONS, ON-PREMISES AND CLOUD, ETC.

Policies	Microsoft	Symantec
Granularity		
Logical Combinations (AND, OR) Permitted	Yes	Yes
Limits, Exceptions, Thresholds, Accepted, for example the number of SSN?	Yes	Yes
Identical Policy Framework		
On-Premises and Cloud	No	Yes
Email	No	Yes
Web Applications	No	Yes
At Secure Web Gateways, Mirror Gateways, etc.	No, reverse-proxy solutions only	Yes
Pre-built and Customizable Policies		
Pre-built Policies Are Available	Yes	Yes
Pre-built Policies Can Be Customized	Yes	Yes
Custom Policies Can Be Built From Scratch	Yes	Yes
Policies Extensible Using Machine Learning	Yes	Yes
Context-Dependent Policies and Behavior Analysis		
Context-Dependent DLP	Yes, public preview only	Yes
User Behavior (UEBA) Analytics	Yes, public preview only	Yes

**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.**



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.

Microsoft and Symantec each have different 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.

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.

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

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.

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

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; Symantec 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; Symantec 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:

- 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:

Software cost considerations include the costs of the core DLP solution or feature set. For Microsoft Purview Information Protection, 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 gaps, 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

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

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.



HAUMOUN
www.haumoun.com

Appendix A: What's at Risk: The Costs of Good Enough DLP

Information is a strategic asset for most enterprise-scale organizations, especially:

- Financial services firms, where data and data transactions are the product itself
- Pharmaceutical and technology firms, whose value is concentrated in proprietary information
- High-visibility consumer firms whose reputation is essential to their brand
- Healthcare and government organizations with obligations to protect client and citizen privacy
- Any organization that does business in jurisdictions with strong privacy and data protection laws

For such companies, data loss is a growing threat with rising impacts. IBM Security reports the 2021 global average at a record \$4.24 million, but “breakout” cases at British Airways and Marriott have touched \$100 million. A full accounting of breach costs includes:

- Forensic investigation, crisis management, assessment and audit.
- Lost business, including reputational losses and loss of shareholder value.
- Notification of and reparations for victims, including discounts and free services.
- Fines and legal expenditures

Confidential customer information, business intellectual property, and employee records are the top categories of information exposed in these breaches. So governments, industry groups, and advocacy organizations have stepped forward to protect the data assets of their constituents with:

- Regulations such as Europe’s General Data Protection Regulation and the California Consumer Privacy Act of 2018.
- International standards such as ISO 27701 for data privacy and ISO 27018 for data security.
- Industry standards such as the Payment Card Industry Data Security Standard (PCI-DSS), and best practices advocated by the Financial Services Information Sharing and Analysis Center (ISAC).
- Company policies developed by Legal, PR, Engineering, HR, Finance, and Risk Management teams to keep essential company information assets protected.

Paradoxically, regulatory and standards requirements add to the costs and risks of data protection, by raising the complexity and therefore the cost of compliance, as

well as the reputational damage and remediation cost of any breach. For example, GDPR requires organizations to report a breach within 72 hours and can impose fines of up to 4% of global turnover.

Appendix B: A Taxonomy of Threats

Verizon’s Data Breach Investigations Report (DBIR) is an annual summary of potential and confirmed data disclosures—almost 30,000 of them in 2020—classified according to who did what:

Outside threats typically originate from financially-motivated criminal gangs operating outside Western jurisdictional reach. Sophisticated “advanced persistent threats” get the most press, but most outsider attacks are short and simple:

Phishing attacks use fraudulent emails to trick targets into disclosing sensitive data or credentials, or installing malicious software that does the same.

Stolen credentials are used to loot client accounts directly, deployed in Web application attacks (below), or increasingly, sold in black markets on the Dark Web.

Web application attacks use stolen, purchased, or computer-generated credentials to break into online applications, typically financial portals.

Ransomware encrypts data in place, exfiltrates it, or both. Attackers then extort payment in exchange for the decryption key or promise not to publish.

Insider threats include IT staff and end users who make mistakes—sometimes innocent, but sometimes attempts to work around a policy for a perceived greater or more immediate good.

Errors include users’ misdelivered email and lost devices from thumb drives to laptops; and IT staff’s misconfigured databases and unprotected data stores.

Workarounds include password sharing, privilege escalation, and other “just this once” good-faith/poor-judgement violations of data protection policies.

Supply-chain threats originate with credentialed partners. They figured in the gigantic 2013 data theft from Target Stores, and the 2021 ransomware attacks on customers of Kaseya software—reminders that partners who share your networks share a responsibility for protecting the data they hold.

Regulators aren’t traditional “bad actors,” but they nonetheless impose costs of compliance and audit, reputational damage, and remediation expense if data protection is noncompliant.