

From Risk To Resilience:

A Buyer's Guide to Data Loss Prevention

Insights That Demand Action

\$4.88M

Average Cost
of a Breach

73%

Rise In Ransomware
Attacks

3,205

Publicly Reported
Data Compromises

Introduction

The Growing Complexity of Data Security

As an IT or Security leader, you face the critical challenge of protecting sensitive data in an environment that grows more complex by the day. Today, 40% of data breaches impact multiple platforms¹ — cloud, on-premises, and mobile, highlighting the need for a robust Data Loss Prevention (DLP) strategy.

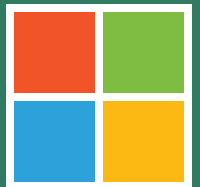
Rising Cyber Threats and Financial Impact

Cyber threats are escalating; ransomware attacks rose by 73% in 2023², and the average data breach cost surged to \$4.88 million in 2024¹. The speed of attacks is also increasing, with the period an attacker is on a system from compromise to detection dropping from 101 days in 2017 to just 10 days in 2023³. To address this rapid evolution in threats, organizations need a proactive data security strategy that both mitigates risks and enables swift threat detection.

The Double-Edged Sword of AI in Security

The integration of AI into security frameworks presents new challenges. While AI enhances threat detection and response, its rapid integration has nearly doubled AI-related security incidents in the past year⁴. A balanced approach to AI implementation is critical, ensuring that the benefits outweigh the risks.

“ **While remarkable in its reach and potential, AI is only the latest transformational wave sweeping across enterprises, like hybrid work, cloud, and mobility, that in recent years underscored the timeless need for visibility in their use to mitigate risk and maximize impact. Informed by these learnings, properly securing data used in AI, as well as using AI to enhance data security measures, will enable greater productivity, resilience, and agility as teams navigate future challenges.**”



- Rudra Mitra, Corporate Vice President-Data Security and Compliance, Microsoft

Long View's Buyer's Guide: Expert Insights for Effective DLP Implementation

This buyer's guide, developed with insights from Long View Systems' defense experts, offers a clear pathway to integrating DLP into your security strategy. Covering emerging trends, essential features, and cost considerations, it equips you with the knowledge needed to build a resilient data security framework tailored to your organization's needs.

Strengthening Your Security Posture

By prioritizing DLP alongside other security measures, you're enhancing your organization's defenses and ensuring compliance with critical regulations like:

GDPR

HIPAA

CCPA

More than just protecting data, you're safeguarding your organization's stability, reputation, and future success in an increasingly high-stakes digital landscape.



154

Annual Data Security Incidents on Average per Organization⁴



The Urgent Need To Fortify Your Data Defense

With an increased need to focus on data security, organizations must address the rapidly evolving threat landscape — from rising data breaches, third-party vulnerabilities, and AI-driven attacks. The necessity for stringent data protection laws, coupled with the significant financial repercussions of breaches and disruptions from data loss, calls for a proactive security strategy.

As cloud adoption and remote work gain prevalence, prioritizing robust data defense not only offers a competitive edge but also ensures compliance and prepares your organization for future threats.

“Data security is a cornerstone of effective cybersecurity programs. Notably, of the security decision-makers we spoke to, the vast majority (89%) consider their data security posture critical to their overall success in protecting their data.”

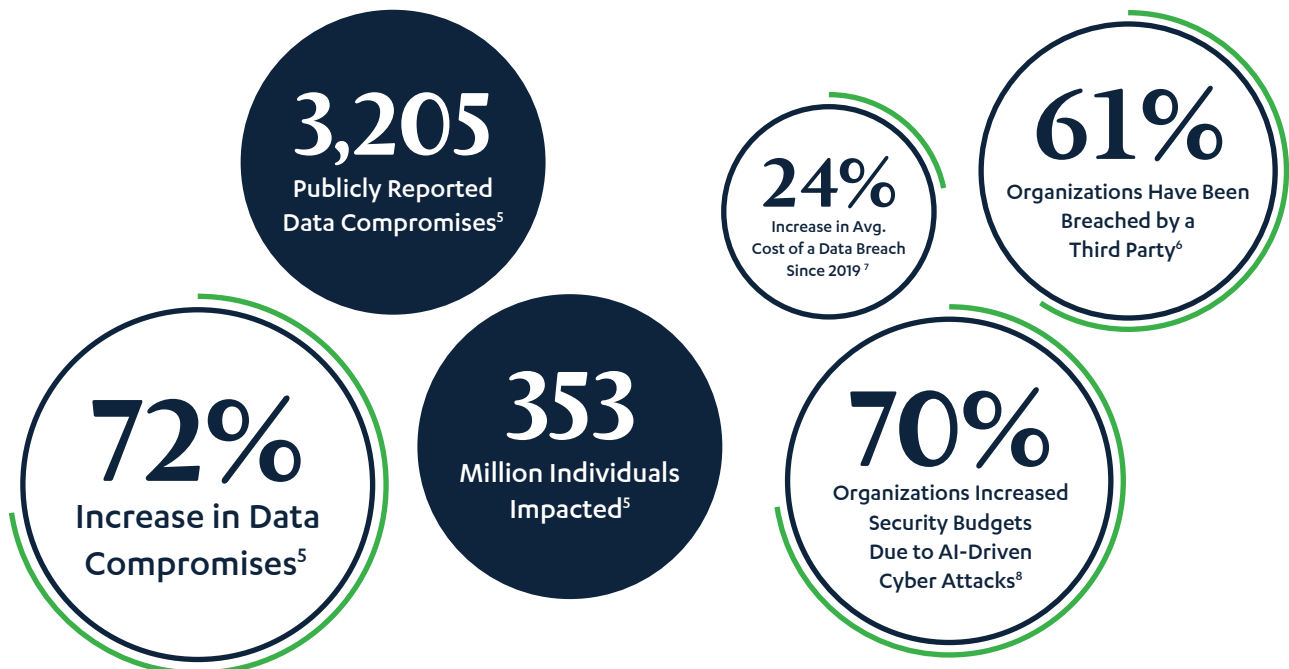
- Herain Oberoi, General Manager for Data Security, Compliance, and Privacy, Microsoft



Decisive Action Required

The time to strengthen your data security is now. By deploying comprehensive solutions to safeguard sensitive data, you enhance your organization's resilience. Recent statistics confirm the urgency and complexity of today's data security challenges:

Escalating Cyber Threats



Regulatory Compliance and Financial Implications

\$1.6

Billion in GDPR
Fines Imposed⁹

\$10.5

Trillion Projected in
Annual Global Cybercrime
Cost by 2025¹⁰

Operational Continuity and Business Resilience

292

Days on Average to
Identify and Contain
a Data Breach¹

65%

Consumers Cite
Misuse of Personal Data
as Top Reason for
Losing Brand Trust¹¹

Facilitating Secure Digital Transformation

21%

Breaches Originated
from Attacks on
Remote Work
Environments¹²

85%

Cybersecurity Leaders
Report Recent Attacks
Powered by AI¹³

Investing in advanced data protection solutions now is crucial for securing your digital infrastructure, maintaining customer trust, and ensuring long-term business viability.

Building a Strong DLP Framework

Establishing Your Data Protection Strategy

Building an effective data strategy begins with a comprehensive assessment of your organization's specific security and business needs. Central to this is DLP, which involves identifying sensitive data, reviewing existing protections, and aligning security policies with organizational objectives to boost data security, compliance, and resilience.

Conducting a Thorough Security Audit

A structured security audit should focus on several critical areas, including evaluating security policies to ensure alignment with industry standards, verifying that access controls are justified and secure, and assessing incident response preparedness to effectively detect, respond to, and recover from potential breaches.







Transitioning to DLP Strategy Implementation

Transitioning from a security audit to actionable DLP steps focuses on implementing a comprehensive strategy that enhances data security, ensures compliance, and bolsters resilience.

The approach comprises four pivotal steps designed to protect sensitive information effectively and align data protection policies with business objectives, creating a robust foundation for managing and safeguarding critical data:







STEP 1

Identify And Classify Sensitive Data

 Key Considerations	Critical for Protection: Identifying and categorizing data like Personally Identifiable Information (PII), intellectual property, and financial records is essential to address compliance requirements.
 Actions	Map and Categorize Data: Utilize discovery and classification tools to efficiently map, categorize, and automate the tracking of sensitive data, enhancing accuracy and mitigating risks from cloud migration.
 Outcomes	 Focused Protection  Defined Scope of Risk  Aligned Policies





STEP 2

Evaluate Your Current Security Posture

 Key Considerations	Regular Assessments: Ongoing evaluations of your security posture are vital to understanding the effectiveness of your security measures, especially as cloud and hybrid environments become more common.
 Actions	Evaluate Your Security Environment with Key Questions: <ul style="list-style-type: none">• What does “normal” look like?• Who controls privileged access points?• How visible are connected devices and applications?
 Outcomes	 Clearer Insights  Refined Policies  Enhanced Resilience







STEP 3

Align Data Security Policies With Business Objectives

 Key Considerations	Tailored for Effectiveness: Aligning policies to business goals ensures your data security is both effective and efficient, avoiding a one-size-fits-all approach that can hinder productivity.
 Actions	Collaborate Across Departments: Engage stakeholders to customize policies, considering the specific needs of small businesses or the complex structures of large enterprises.
 Outcomes	 Strengthened Protection  Enhanced Productivity  Supported Growth

STEP 4

Strengthen Incident Response Preparedness

 Key Considerations	Critical for Recovery: Effective incident response minimizes the impact of data breaches by enabling swift detection, response, and recovery—key elements of a strong data protection strategy.
 Actions	Prepared for Threats: Test your incident response plan regularly, equip your team with real-time monitoring tools, and conduct post-incident reviews to enhance detection, containment, and recovery.
 Outcomes	 Faster Threat Detection  Reduced Downtime  Improved Organizational Resilience

Securing Success

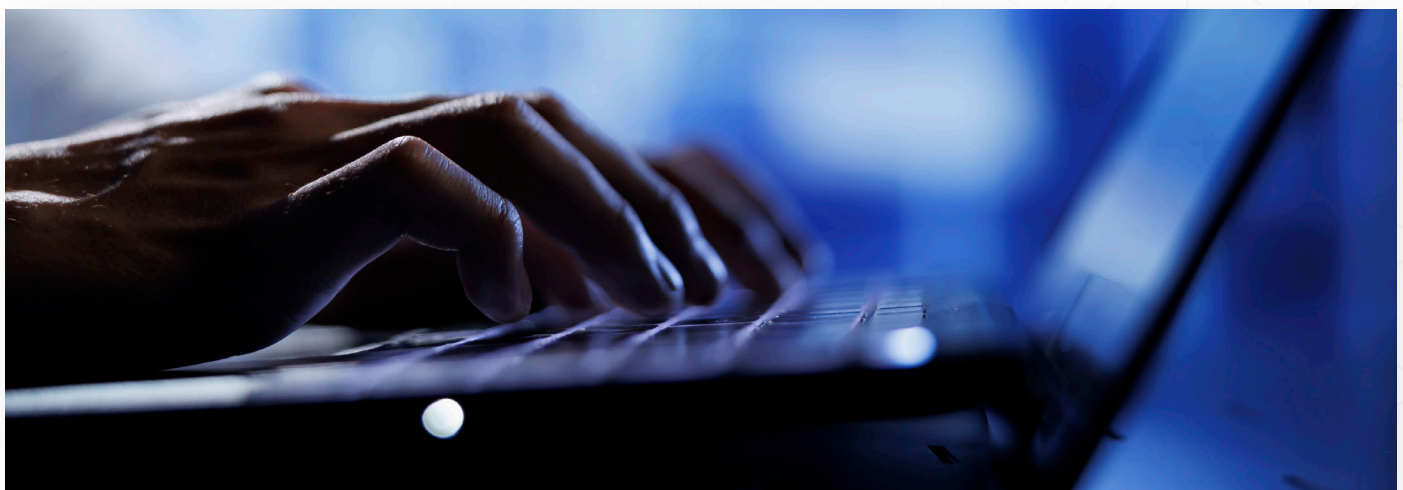
Implementing a DLP strategy tailored to your specific needs not only helps prevent data breaches but also strengthens your overall security posture, ensures compliance, and protects your organization's most valuable assets.

For enhanced support, partnering with a trusted advisor like Long View can offload your team's burden. Their **data defense experts** offer certified expertise and predictable spending models to ensure your investments in data protection are effective and efficient.



59%

IT Leaders Say DLP Should be Part of a Holistic Data Protection Strategy¹⁴



Critical Factors for Choosing a Data Security Platform and Partnership

Selecting a DLP solution goes beyond data loss prevention; it's about enhancing your entire security strategy. When choosing a DLP solution, focus on these critical factors to ensure it complements and strengthens your security goals:

1

Types Of Data To Protect

- Identify Sensitive Data:** Pinpoint data needing protection, such as personal, financial, or intellectual property, and verify robust classification and management tools are included.
- Protect the Entire Data Lifecycle:** Ensure solutions cover data at rest, in transit, and in use.

2

Compliance and Regulatory Requirements

- Industry-Specific Compliance:** Confirm platform compliance with regulatory standards like HIPAA and PCI-DSS, and check for helpful features like templates and audit tools.
- Global and Local Laws:** Ensure compliance with regulations, such as GDPR and CCPA.
- Audit Tools:** Seek platforms with comprehensive audit logs and reporting for easier regulatory compliance.

3

Deployment Options and Scalability

- Flexible Deployment:** Choose between on-premises, cloud-based, or hybrid solutions.
- Built-in Scalability:** Opt for solutions that can grow with your data and user base, particularly those offering cloud scalability.

4

Integration with Existing Systems

- Seamless Compatibility:** Select a platform that integrates easily with your existing IT infrastructure, such as security tools, cloud platforms, and endpoints.
- API and Customization:** Look for robust API support and customization options.
- Cost Efficiency:** Prioritize solutions that leverage existing investments, like Microsoft, to reduce costs, streamline training, and minimize administrative overhead.

5

Ease of Use and Manageability

- User-Friendly Interface:** Choose platforms that are easy for IT teams to manage.
- Simplified Policy Management:** Seek solutions that make it easy to create, enforce, and manage data protection policies.

6

Threat Detection and Response Capabilities

- Real-Time Threat Monitoring:** Evaluate platforms for immediate breach detection and alerts.
- Automated Remediation:** Prioritize platforms that can autonomously secure sensitive files during threats.

7

Endpoint and Network Coverage

- Comprehensive Coverage:** Ensure all access points are covered, from desktops to mobile and network connections.
- Remote Work Support:** Select solutions that cater to hybrid work environments without compromising security.

8

Cost and Licensing Models

- Transparent Pricing:** Look for clear, upfront pricing structures covering licensing, implementation, and ongoing support costs.
- Flexible Licensing Options:** Choose models that align with your operational scale and budget.
- ROI and Long-Term Value:** Focus on solutions that reduce costs through seamless integration with your environment.

9

Customizability and Flexibility

- Tailored Security Policies:** Choose platforms that allow policy customization to meet compliance, risk tolerance, and department-specific needs.
- Growth Adaptability:** Confirm the solution can adjust to evolving risks and regulatory changes.

10

DLP Support and Training

- Proven Expertise:** Partner with a DLP services provider known for effective data protection and comprehensive advisory services.
- Customer Service:** Ensure the partner offers fast, dependable support and training.

11

Implementation and Maintenance

- Deployment Efficiency:** Assess the rollout timeline and the resources required for minimal disruption.
- Continuous Optimization:** Engage a partner that provides ongoing maintenance and updates to keep the solution effective.

Data Defense Powered by Microsoft & Long View

Through this guide, we've addressed today's top security challenges, provided steps for assessing your needs, and offered a checklist for selecting your DLP solution. Partnering with data defense specialists like Long View, who bring over 75 years of combined expertise, can enhance your data protection strategy. Together, Microsoft Purview and Long View offer a streamlined and effective DLP solution, ideal for small and medium-sized businesses aiming for strong security with minimal operational impact.

Seamless Integration with Existing Microsoft Environments

For organizations already using Microsoft solutions, Purview offers a cloud-native DLP solution that integrates seamlessly, enhancing data protection and compliance while avoiding costly add-ons. This deep integration delivers consistent security across all users, devices, and applications, simplifying the expansion of DLP capabilities in a cost-effective manner.

Minimize Disruption, Maximize Customization, and Insightful Data Management

Together, Microsoft Purview and Long View enhance standard DLP features by providing automated remediation, detailed alerts, custom policy templates, and powerful investigative tools. Flexible licensing and expert guidance from Long View ensure your policies align with both your security needs and budget, offering deep insights into your data activities and security posture without compromising productivity.

DLP in 30: Rapid Deployment for Immediate ROI

The beginning of every digital transformation journey is unique, but the objective for all organizations is the same: to transition smoothly into a secure, digital enterprise. Drawing on decades of experience helping organizations navigate complex security challenges, Long View developed [Data Loss Prevention in 30 Days \(DLP in 30\)](#) as a streamlined solution tailored to meet the urgent need for robust data protection.

Powered by Microsoft Purview, [DLP in 30](#) is designed to deliver fast, comprehensive data security in just 30 business days. Long View's experts streamline the implementation process through an eight (8)-stage process, ensuring quick deployment and immediate effectiveness.

This rapid setup minimizes downtime, boosts ROI, and prevents data leaks to secure sensitive information, ensuring compliance right from the start. With AI-powered security, organizations gain substantial cost savings and proactive protection, allowing them to stay ahead of vulnerabilities without disrupting daily operations.



64% of Organizations Plan to Increase Their IT Budgets in 2025¹⁵

Move Your Business Forward with Long View

With over 25 years as a Microsoft Partner and accolades including Partner of the Year, Long View offers proven, reliable solutions and services for your data security needs.

Technology is our means, but your empowered workforce is our end. We support the world's dynamic businesses by bringing agility, simplicity, and insight to your people, so they can serve your clients. We can do it because our offices are home to a team of the best and brightest business technologists from across the continent, united by a common mandate — we're using technology to help the world work.

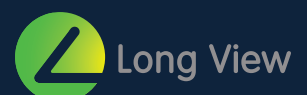
We have successfully helped clients navigate complex security challenges, enhance data protection controls, streamline tools for efficiency, and improve existing technology controls and processes. Our end-to-end support, from proactive maintenance to strategic long-term planning, ensures your organization is protected, resilient, and equipped to evolve with the changing security landscape.

Ready to Secure Your Data with Confidence?

Data security is essential for every business. Through our partnership with Microsoft, Long View provides a scalable, compliant data protection framework tailored to grow with your organization. With our **DLP in 30** service, you'll benefit from cutting-edge technology and expert support, ensuring your data is protected by top-tier professionals using the latest tools.

Contact Long View today to enhance your data security and ensure your organization's future resilience.

People, forward.



References

- ¹IBM (2024) Cost of a Data Breach Report
- ²Sans Institute (2024) Ransomware Blog
- ³Mandiant (2024) M Trends Report
- ⁴Microsoft (2024) Data Security Index Report
- ⁵ITRC (2024) Annual Data Breach Report
- ⁶Prevalent (2024) Third-Party Risk Management Study
- ⁷statista (2024) Avg. Cost of a Data Breach Worldwide
- ⁸Investopedia (2024) Fears About AI Blog
- ⁹statista (2024) EU Protection Fines Blog
- ¹⁰Cybercrime Magazine (2020) Cybercrime Annual World Cost Blog
- ¹¹MediaMath (2023) Consumer Privacy Survey
- ¹²Forrester (2024) The State of Data Security
- ¹³CFO (2023) Cybersecurity and AI Blog
- ¹⁴Microsoft (2023) Data Loss Prevention: From On-premises to Cloud
- ¹⁵Spiceworks (2024) The 2025 State of IT