




3 Tips for Comprehensive Data Security



Contents

- Introduction 3
-  Tip 1: Discover and protect sensitive data 5
-  Tip 2: Understand user context and detect critical risks 7
-  Tip 3: Prevent data loss 9
- Conclusion 11

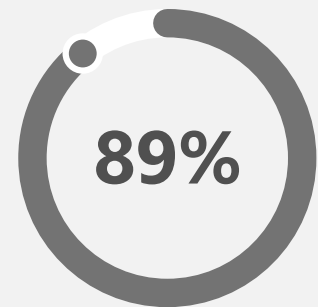
Introduction

Data is a driving force for modern organizations. Its contributions to operations, innovation, and forward momentum are immeasurable, and its obvious value makes it a top priority for security teams, which must keep it safe from cyberthreats and insider incidents.

Safeguarding sensitive information, spanning from employee and customer data to intellectual property, financial projections, and operational records, against an array of cyber threats, data breaches, and insider risks, is a top priority for CIOs and CISOs around the globe.

In fact, of more than 800 data security professionals recently polled in a multi-national survey¹, **the vast majority (89%) consider their data security posture critical to their overall success.**

IT and security teams are looking for better ways to manage the entire data lifecycle, across multicloud, hybrid cloud, and on-premises environments, especially since years of point solutions have left critical gaps.



Of surveyed data security professionals say data security posture is critical to their business success.

¹Microsoft Data Security Index: Trends, insights, and strategies to secure data," October 2023.



This paper shows how an end-to-end approach can help. That approach involves three key tips:



Tip 1: Discover and protect sensitive data:

Determine where your data lives, what kind of data it is, and how it's being used or shared.



Tip 2: Understand user context and detect critical risks:

Detect critical risk around data, highlighting the importance of insider risk management.



Tip 3: Prevent data loss:

Leverage data loss prevention (DLP) solutions and Adaptive Protection, to dynamically enforce effective policies.

The goal of this approach? To provide the kind of comprehensive data security that protects data with a multi-layered approach, minimizing risk without sacrificing productivity.



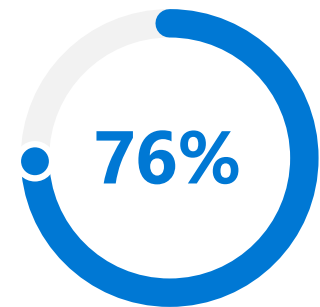
Tip 1:

Discover and protect sensitive data

For an organization to apply the right policies or protections for its data, it must know what it is, where it lives, how it's used, and how it travels around the organization.

Identifying all this data can be difficult. In fact, three in four (76%²) security professionals worry about proliferating shadow data and the vulnerability of the unknown, especially in the face of expanding rates of enterprise data generation, which are expected to more than double by 2026³.

Artificial intelligence (AI) and machine learning (ML) can help, by discovering sensitive data (such as intellectual property and trade secrets) and classifying it automatically. This classification technology can span your entire data estate—scanning, labeling, and protecting data anywhere it lives, from on-premises to cloud-based repositories, from software-as-a-service (SaaS) to OS-native apps.



Of surveyed data security professionals worry about proliferating shadow data.

²"[Microsoft Data Security Index: Trends, insights, and strategies to secure data](#)," October 2023.

³"Worldwide IDC Global DataSphere Forecast, 2022–2026: Enterprise Organizations Driving Most of the Data Growth," John Rydning. IDC. May 2022.

Once the data is classified, proper data protection controls, such as encryption and watermarking, help ensure data isn't accidentally or intentionally misused or accessed without authorization. The protection controls are persistent no matter where the data travels to, securing it throughout its lifecycle.

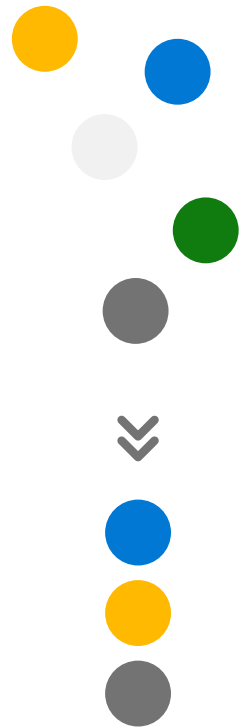
Additionally, unified, high-fidelity classification services allow organizations to classify their data once and use that classification in various security and compliance use cases—including preventing data loss and detecting critical data security risks.

Whereas traditional classification approaches involve considerable manual work and inaccuracy, running the risk of errors or inadvertently overlooking critical data, ready-to-use, trainable classifiers can help automate this process. An integrated data solution allows administrators to manage classification centrally, across all systems.



Want to better manage and protect sensitive data across your environment?

Learn about data classification and protection in Microsoft Purview at Microsoft.com.



 Tip 2:

Understand user context and detect critical risks

Data doesn't move itself. People move data. It's just as important for your organization to identify and classify its data, as it is to understand the critical risks surrounding it.

Organizations must take measures to safeguard their data, both by preventing unauthorized access from external threats and by mitigating the risk of insider theft or accidental data exposure. Malicious insider incidents, **is one of the incident types security decision makers feel least prepared to prevent**⁴. These findings are aligned with research from Forrester, which indicates that insider risks accounted for 26% of the security breaches reported in the past year. What's even more significant is that over half of these incidents were intentional⁵.

It's crucial to understand your user activity and context around data to identify risks. However, parsing through and reasoning over multitudes of signals can be time-consuming, resource-draining, and ineffective. Ready-to-use machine learning models and insider risk indicators can help security teams detect critical risks more effortlessly and effectively and thus accelerate time to action, getting ahead of data security risks before it evolves into incidents.



Security decision makers feel least prepared to prevent malicious insider incidents."⁴

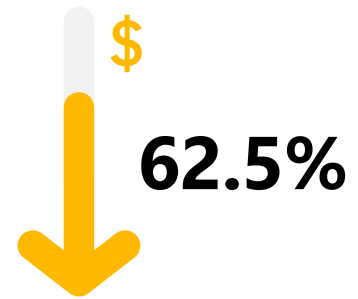
⁴"[Microsoft Data Security Index: Trends, insights, and strategies to secure data](#)," October 2023.

⁵"[Internal incidents cause roughly a quarter of breaches, with more than half intentional](#)," Forrester, July 2023.

The solution should also respect user privacy. Addressing security concerns must be balanced with taking a user privacy-centric approach to ensure a strong security culture across your organization. In fact, in a recent survey⁶ of 300 United States-based security experts, 94% of those surveyed noted that a key element to program success is finding a balance between employee privacy and company security.

Research shows that organizations with fully deployed AI/ML and automation security technologies experienced almost 65.2% less cost, compared to those with no AI/ML and automation deployed when a data breach happened⁷

By combining human expertise with powerful data security tools, you can work toward a safer digital future.



Fully deployed AI/ML and automation security technologies experienced almost 65.2% less cost.



Want better insight into user context and critical risks to your most sensitive data?

Learn about activity exploration in Microsoft Purview at [Microsoft.com](https://www.microsoft.com).

⁶["Building a Holistic Insider Risk Management Program: 5 elements that help companies have stronger data protection and security while protecting user trust,"](#) October 2022.

⁷["Cost of a Data Breach,"](#) IBM, 2022.

Tip 3:

Prevent data loss

Why invest the resources and energy to properly identify and classify your data, if that data isn't adequately protected from loss? **More than 80 percent of organizations rate theft or loss of personal data and intellectual property as high-impact insider risks**⁸. Data loss prevention (DLP) solutions can educate, influence, and prevent users from sharing, exposing, or transferring sensitive data without authorization—intentionally or inadvertently.

DLP policy can prevent accidental or intentional loss of data—without slowing down your teams. Security doesn't have to come at the expense of productivity. Proactively mitigate the loss of sensitive data across your apps, services, and devices by adding built-in protection, wherever your users work. Create and manage multi-scoped policies from a single location, and empower your users to better handle sensitive information.

Often the risk stems from organizations making do with one-size-fits-all, content-centric data-protection policies that end up creating alert noise. This signal overload leaves admins scrambling as they manually adjust policy scope and triage alerts to identify critical risks. Fine-tuning broad, static policies can become a never-ending project that overwhelms security teams.



Of surveyed data security professionals rate theft and data loss as high-impact risks.

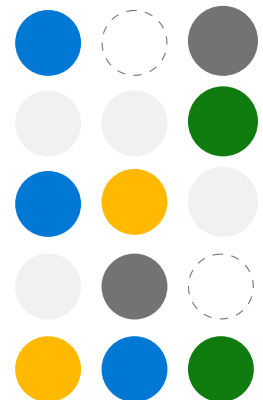
⁸["2022 State of Data Governance and Empowerment Report,"](#) Enterprise Strategy Group, July 2022.

What's needed is a more adaptive data security solution to help organizations address the most critical risks dynamically, efficiently prioritizing their limited security resources on the highest risks and minimizing the impact of potential data security incidents. For example, with more adaptive data security controls, organizations can automatically apply strict DLP policies, such as blocking them from exfiltrating data, on high-risk users while allowing low-risk users to work as usual.



Want intelligent detection and control of sensitive information?

Learn about adaptive data loss prevention in Microsoft Purview at Microsoft.com.



Conclusion

After years of acquiring multiple best-of-breed solutions, many organizations are recognizing the 'paradox of plenty' through gaps in visibility and growing inefficiencies.

Research shows that organizations using more than 16 tools to secure data experienced nearly three times **more** data security incidents than those who used fewer⁹.

The point solution approach of the past has become unwieldy, giving way to the desire for a more comprehensive, platform-based approach that seamlessly and without dependencies integrates Information Protection, Data Loss Prevention, Insider Risk Management, and Adaptive Protection.

3x

Organizations with 16 or more tools receive an average of 96 data security alerts per day compared to 44 alerts for teams with fewer tools.

⁹["Microsoft Data Security Index: Trends, insights, and strategies to secure data"](#), October 2023.



A simple, integrated, and intelligent solution: Microsoft Purview

Microsoft Purview provides comprehensive and AI-powered data security capabilities that enable organizations to secure data with a defense-in-depth approach across your digital landscape.

Data security that keeps you moving forward fearlessly
[Learn more about securing your data with Microsoft Purview >](#)

Interested in a specific area of data security? Get more detailed information on how Microsoft Purview can help you with:

[Data Security >](#)

[Information protection >](#)

[Data loss prevention >](#)

[Insider risk management >](#)



©2024 Microsoft Corporation. All rights reserved. This document is provided "as-is." Information and views expressed in this document, including URL and other Internet website references, may change without notice. You bear the risk of using it. This document does not provide you with any legal rights to any intellectual property in any Microsoft product. You may copy and use this document for your internal, reference purposes.