Best practices Data security Microsoft Purview
6 min read

Top insights and best practices from the new Microsoft Data Security Index report

By Herain Oberoi, General Manager, Data Security, Compliance, and Privacy, Microsoft

October 25, 2023

A whopping 74 percent of organizations recently surveyed experienced at least one data security incident with their business data exposed in the previous year. That's just one of our interesting insights from Microsoft's new Data Security Index: Trends, insights, and strategies to secure data report, released today.

Data security is a cornerstone of effective cybersecurity programs. Notably, of the security decision-makers we spoke to, the vast majority (89 percent) consider their data security posture critical to their overall success in protecting their data. Safeguarding sensitive information, spanning from employee and customer data to intellectual property, financial projections, and operational records, against an array of cyberthreats, data breaches, and insider risks, is a top priority for these organizations.

Every chief information security officer (CISO) I've spoken with has shared a daunting data security experience and expressed a desire to explore the best practices and technological innovations that can help them overcome these challenges. At Microsoft, we're keen to help organizations navigate the complexity of data security and implement effective comprehensive strategies for strengthening their data security posture.

To facilitate this dialogue and learn more from our customers and peers, we partnered with the independent research agency Hypothesis Group to conduct a multinational survey involving more than 800 data security professionals. Our collaborative effort has resulted in the publication of the Data Security Index report, designed to offer valuable insights into current data security practices and trends. Moreover, it aims to identify practical opportunities for organizations to enhance their data security efforts.

In this blog post, I'll dive into some of the key findings from the report, including:

- Data security incidents remain frequent.
- Vulnerabilities manifest in various dimensions due to a diverse set of factors.
- How a fragmented solution landscape can weaken an organization's data security posture.

Data security incidents remain frequent

Data security incidents continue to occur frequently with an average of 59 incidents occurring in the past 12 months, 20 percent considered severe, resulting in potential annual costs of up to USD15 million.

While decision-makers are attempting to make the best use of the tools they currently employ, it's not enough to mitigate the continued frequency of data security incidents.

> *I can't go tell my board of directors "I secured the data, I just didn't protect it"… the last thing we want to see is our bank failing to deliver on the front page of the* Wall Street Journal.
>
> —Chief information security officer in the financial services industry

Vulnerabilities manifest in various dimensions due to a diverse set of factors

One of the primary reasons data security incidents occur more commonly than desired is the expanding diversity and complexity of risks associated with data. These encompass a variety of factors such as the causes of the incidents, the need to safeguard different types of data and the challenges presented by data processed and stored across various locations and workloads.

Among all causes of data security incidents, decision-makers expressed their least preparedness in preventing malware, ransomware attacks, and malicious insider incidents. When considering the types of sensitive data at risk of exposure—business data, such as intellectual property, is at a higher risk compared to operational and personal data. Additionally, as cloud and AI become imperative for organizations to drive digital transformation—security teams need to deal with the complexities of protecting data across a variety of locations and application types.

A fragmented solution landscape can weaken data security posture

How can organizations effectively navigate the multifaceted landscape of data security risks? Often, various use cases within different aspects of data security efforts may necessitate the adoption of distinct solutions. In the physical realm, adding more locks to a door typically enhances security. However, in the context of cybersecurity tools designed to safeguard data, the situation is quite the opposite. Organizations employing more than 16 tools to secure data face a staggering 2.8 times more data security incidents compared to those who use fewer tools. Moreover, the severity of these incidents tends to be higher as well.

For each tool an organization adopts, it necessitates dedicated staff and processes, primarily because each vendor provides its distinct portal with varying technological foundations. Take data classification as an example; when organizations use siloed solutions, each solution might have its own classification service, resulting in data being classified multiple times based on specific use cases.

The proliferation of tools also leads to an increase in the number of alerts, and at times, these alerts may be duplicated, creating more noise in the system. According to the report, organizations using a greater number of tools receive more than double the volume of alerts compared to those with fewer tools. However, they can only review a smaller percentage of these alerts.

Now, imagine a scenario where an incident occurs—each administrator of each tool must initiate their own investigations within their respective areas of expertise. Subsequently, they convene to deduplicate alerts, correlate insights, and determine the nature of the incident. Unfortunately, insights may occasionally get lost in translation because they originate from disparate systems, ultimately resulting in longer time to conclude an investigation.

Decision-makers seem to have the correct intuition about this, with 80 percent agreeing that a comprehensive data security platform with integrated solutions is superior to multiple and disjointed point solutions. Despite this understanding, practical implementation remains fragmented, as organizations on average, still utilize more than 10 different tools to manage data security.

Breaking this inertia to better protect data requires strong collaboration among security teams, prioritizing the overall data security posture of the organization over individual and departmental security use cases. It also calls for better-integrated solutions to bring this collaborative approach to life.

Fortifying data security with integrated solutions

An integrated data security solution set should empower security teams to do all these critical tasks seamlessly:

- **Automatically discover, classify, and protect your sensitive data throughout its lifecycle by leveraging a unified and intelligent data classification service.** Detecting sensitive data, such as intellectual property and trade secrets, can be challenging. Traditional methods like pattern recognition, regular expressions, or function matching may fall short in identifying content without specific string formats or keywords. By harnessing a single AI-powered classification service, you can classify your data once, and this classification can be applied across multiple solutions, facilitating secure and compliant data use.
- **Understand user and data usage context and identify risks around your sensitive data, such as intellectual property theft and data leakage.** Data doesn't move itself, people move data and that's where the risks stem from. Organizations need solutions that can help parse through both content and user signals to detect critical data security risks before they evolve into incidents.
- **Proactively prevent data security incidents with security and compliance controls built into the cloud apps, services, and devices users use every day.** Solutions that natively integrate with your modern work environment can effectively educate, influence, and prevent users from causing accidental or intentional data security incidents.
- **Tailor security and compliance controls based on user's risk level dynamically.** All of the aforementioned capabilities should seamlessly integrate with each other to assist organizations in establishing adaptive security. For example, security teams can dynamically apply strict data loss prevention policies on users assessed as high risks for potential data security incidents, accelerating incident response and mitigating emerging risks proactively.

Enabling security teams to do all these critical tasks seamlessly has been the primary focus for Microsoft Purview. These solutions leverage the same industry-leading,[1] AI-powered data classification technology, data map, extensive audit logs and signals, and management experience. As a result, the data security solutions seamlessly integrate with each other, aiding organizations in protecting their data with lower complexity and better outcomes.

To give you a real-world example, we dissected a corporate espionage incident inspired by a true story to demonstrate how taking an integrated approach can help detect and prevent such incidents that may otherwise have gone unnoticed.

Learn if other professionals' experiences match yours—and about comprehensive security from Microsoft

Explore Data Security Index: Trends, insights, and strategies to secure data to learn best practices and recommended strategies based on data security professionals' experience, and listen to the podcast episode "Unveil Data Security Paradoxes" on Uncovering Hidden Risks, where I share deeper insights on why an integrated set of solutions can help enhance security. To learn more, you also can:

- Watch our series of videos, introducing and demonstrating Microsoft Purview Information Protection, Insider Risk Management, Data Loss Prevention, and Adaptive Protection.
- Try our E5 Purview trial if you are an organization using Microsoft 365 E3 and want to see data security solutions in Microsoft Purview in action for yourself.
- Check out our Cybersecurity Awareness Month website for more ways to educate and protect your organizations against cyber threats.

To learn more about Microsoft Security solutions, visit our website. Bookmark the Security blog to keep up with our expert coverage on security matters. Also, follow us on LinkedIn (Microsoft Security) and X (formerly known as "Twitter") (@MSFTSecurity) for the latest news and updates on cybersecurity.

---

[1] Microsoft recognized as a Leader in The Forrester Wave™: Data Security Platforms, Q1 2023, Rudra Mitra. March 22, 2023.

Get started with Microsoft Security

Microsoft is a leader in cybersecurity, and we embrace our responsibility to make the world a safer place.

Learn more

Connect with us on social

What's new

Surface Laptop Studio 2

Surface Laptop Go 3

Surface Pro 9

Surface Laptop 5

Microsoft Copilot

Copilot in Windows

Explore Microsoft products

Windows 11 apps

Microsoft Store

Account profile

Download Center

Microsoft Store support

Returns

Order tracking

Certified Refurbished

Microsoft Store Promise

Flexible Payments

Education

Microsoft in education

Devices for education

Microsoft Teams for Education

Microsoft 365 Education

How to buy for your school

Educator training and development

Deals for students and parents

Azure for students

Business

Microsoft Cloud

Microsoft Security

Dynamics 365

Microsoft 365

Microsoft Power Platform

Microsoft Teams

Copilot for Microsoft 365

Small Business

Developer & IT

Azure

Developer Center

Documentation

Microsoft Learn

Microsoft Tech Community

Azure Marketplace

AppSource

Visual Studio

Company

Careers

About Microsoft

Company news

Privacy at Microsoft

Investors

Diversity and inclusion

Accessibility

Sustainability

English (United States)

Your Privacy Choices

Consumer Health Privacy