Microsoft

hypothesis

Data Security Index

Trends, insights, and strategies
to secure data

Foreword

In a time being defined by a surge of data, it has become increasingly clear that an organization's data is nothing less than its lifeblood. The wealth of data created and used by organizations powers critical operations, informs strategic and global decision-making, and shapes the possibilities for their futures. Data is not merely a resource – it is the beating heart of modern enterprises.

Yet, with this increased reliance on data comes the stark reality that vulnerabilities in the digital shadows are real and quickly expanding. Cyber threats, data breaches, and insider risk incidents are no longer rare occurrences; they are pervasive and escalating, posing risks to organizations that depend on data. Of the decision makers we surveyed recently, 89% said they view their data security posture as critical to their overall success.

In this white paper, we embark on an exploration of that fundamental imperative: the protection of your organization's data. My team and I are excited to share our findings with you – and hopefully start a dialogue around how to continue to push data security forward collectively toward excellence. Our learnings exemplify how data security is at a critical juncture – while security decision makers agree it's essential to the safety of their data, and most say they're confident in what they're doing, they're simultaneously experiencing a plethora of data security incidents and challenges. And, 80% of the leaders we spoke to recognize that a best-in-suite, integrated approach is superior to point-solutions, but most companies are still using a fragmented, multi-tool system to protect their data – which is often resulting in more security incidents instead of fewer.

We welcome you to read and share this latest report and treat it as the beginning of new conversations with our teams on how we can best help secure our collective future.

Rudra Mitra
Corporate Vice President
Microsoft Data Security and Compliance

Introduction

Preventing data breaches and other security incidents continue to be a constant concern for security and risk decision makers – and a cornerstone of any cybersecurity program – because a single breach can cause significant reputational and financial damage. Organizations are tasked with protecting a wide range of sensitive data – including employee and customer information, intellectual property, financial forecasts, and operational data.

To understand current data security practices and trends as well as identify opportunities for organizations to enhance data security, Microsoft commissioned an independent research agency, Hypothesis Group, to conduct a multi-national survey among over 800 data security professionals. This report presents five key findings from the research including trends, insights, and strategies to secure data.

Key Findings

1

Decision makers think they're protected, but reality doesn't match perceptions.

While most decision makers say they are satisfied and confident with their data security solutions, they're still experiencing an average of 59 data security incidents a year, with costly impacts.

2

Having more tools does not mean greater data security or efficiency – it's the opposite.

80% of decision makers agree that comprehensive, integrated solutions are superior to manual, best-of-breed solutions – and yet organizations' approach to tools continues to be fragmented, using an average of 10+ data security tools. But those with the most tools also experience more data security incidents, suggesting that the greater the tool proliferation, the weaker the security.

3

Organizations continue to be plagued by the stress of external and internal data security incidents, especially in business data.

50% of organizations surveyed have experienced a ransomware or malware attack in the past year – and many decision makers don't believe their organization is fully prepared to prevent and address future ones. Internally, malicious insiders are a top concern. Additionally, organizations are highly concerned about the vulnerability of their business data. This again underscores the need for a security platform that addresses risks comprehensively.

Key Findings

4

Organizations need Cloud and AI to drive digital transformation – but they're also the most vulnerable data locations.

Cloud applications and AI technology have become essential for organizations' collaboration and productivity – however, this evolution has also created more dynamic and multifaceted risks. As organizations embrace AI, enhancing data security to enable responsible and safe use becomes critical.

5

Automation and AI are promising avenues of greater protection.

Organizations want their teams to spend less time on detection and more time on prevention. Automation can allow teams to focus more on proactive measures, while using AI for data security helps organizations be more strategic and get smarter about future threats.

1

Decision makers think they're protected, but reality doesn't match perceptions.

Decision makers think they're protected, but reality doesn't match perceptions.

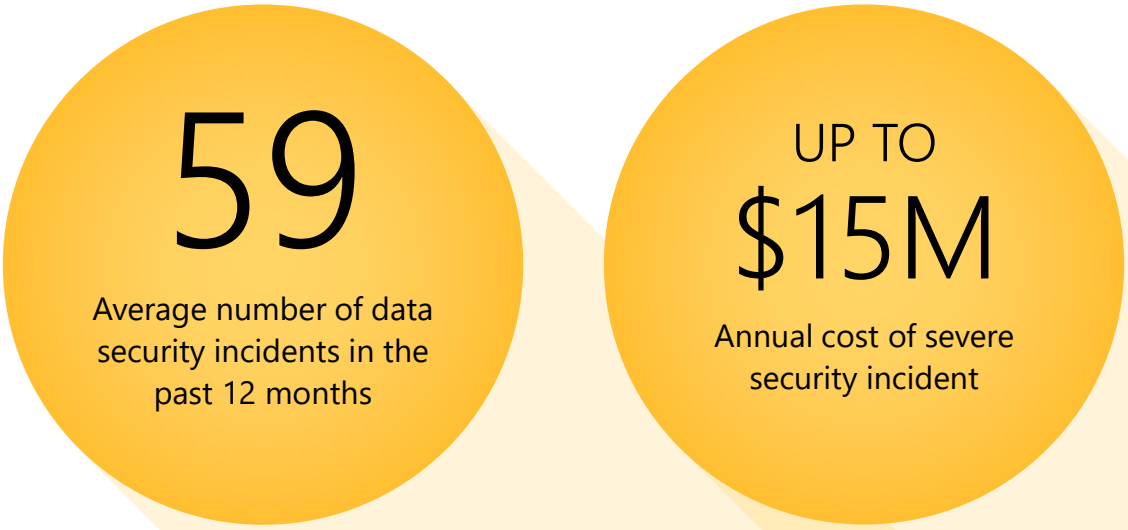
On the surface, decision makers project high levels of confidence and satisfaction with their data security solutions, The majority of organizations agree their data security controls are sufficient in preventing data from being breached, they feel they know where most of their data resides, and that they can detect a majority of risks around data.

At the same time, organizations continue to experience a substantial volume of data security incidents – an average of 59 in the past 12 months, with a fifth of those being considered 'severe'. The impact of these incidents is widespread as on average, organizations estimate that the total financial cost of their most severe data security incident is around $244K – meaning annual incidents can cost up to $15 million. On top of these costs, four in 10 decision makers also say the operational cost to recover for a data security incident and loss of business from reputational damage is of high concern.

In addition, 92% face challenges, primarily in the areas of cost, integration, and time to implement, which inhibit their ability to further invest in data security, underscoring the need for more budget-friendly and labor-efficient solutions.

The perception of confidence in data security readiness differs from the reality of incidents organizations are experiencing. Even though it is important for organizations to know where data is located and detect risks, these measures individually, or separately, are not enough to help organizations prevent the incidents that keep data security and risk decision makers up at night.

As one CISO (Chief Information Security Officer) in financial services puts it, "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."



2

Having more tools does not mean greater data security or efficiency – it's the opposite.

Having more tools does not mean greater data security or efficiency – it's the opposite.

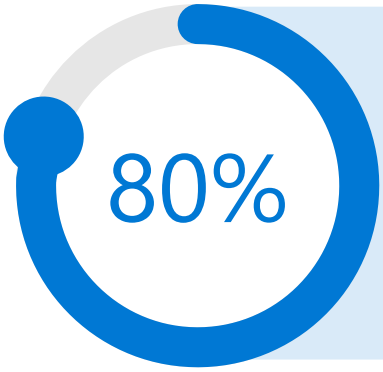
Organizations are coming to realize that years of a point solution approach has created gaps in visibility and efficiency due to siloed data security tools. That trend is now giving way to a desire to have an integrated solution for data security with 80% agreeing that a comprehensive data security platform with integrated solutions is superior to using multiple best-of-breed solutions that have to be manually integrated and managed.

Yet even though the vast majority consider integrated solutions superior, data security tool usage is prolific and fragmented.

As a result, organizations report using 10 data security tools on average to address data security risks, including Data Loss Prevention, Information Protection, Insider Risk Management, Security Information & Event Management (SIEM), Cloud Access Security Broker, and more. For organizations with over 5,000 employees, the average number of tools is even greater.

Having more tools may be creating a false sense of security, as those who use more tools (16+) are more confident in their data security posture compared to those who use fewer tools (61% vs. 56%).

However, research contradicts that sense of security, as organizations with 16 or more tools, also experienced more data security incidents in the past year – an average of 133 – compared to 48 incidents for organizations with fewer tools.

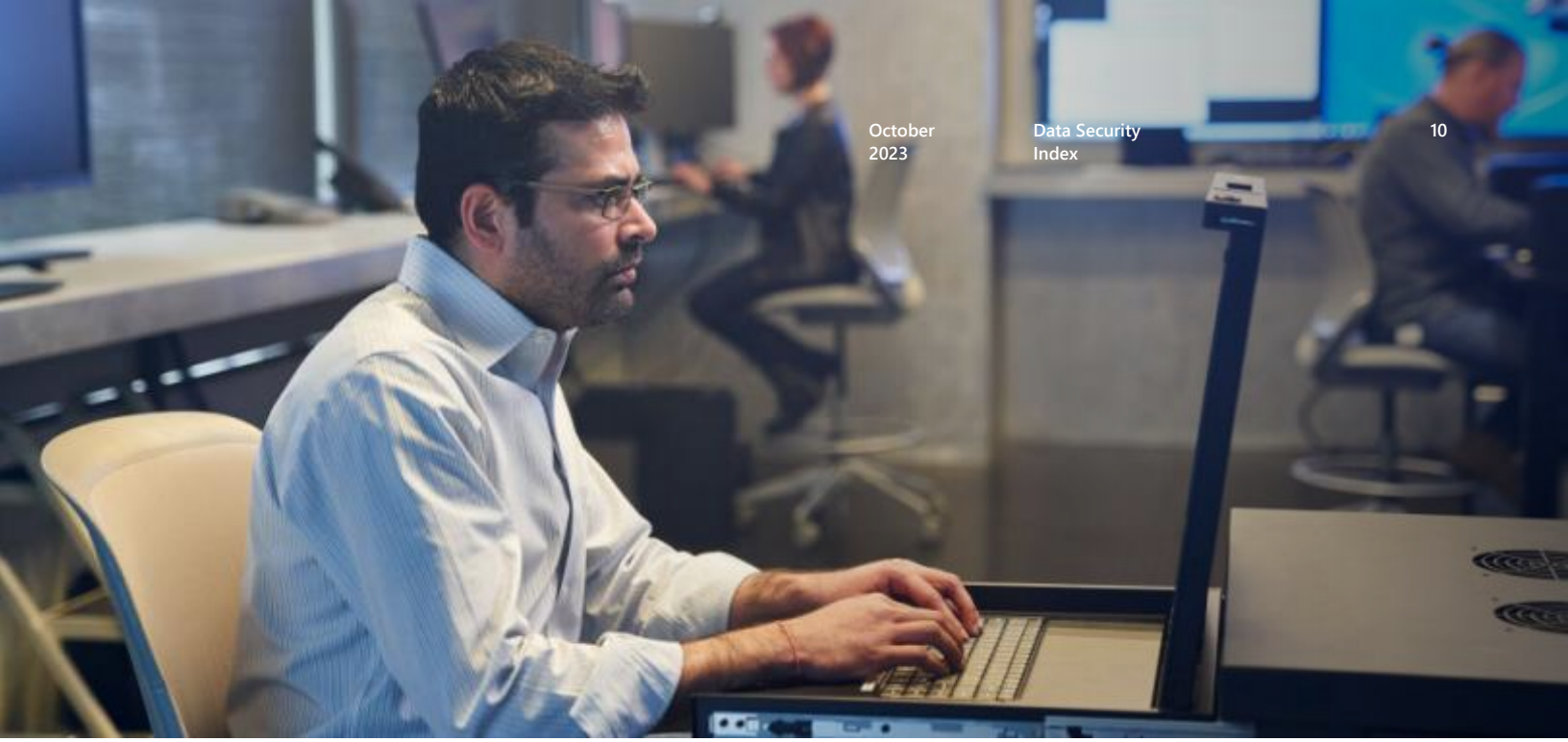


Agree that a comprehensive security platform with integrated solutions is superior to using multiple best-of-breed solutions that have to be manually integrated and managed.

2.8x

More data security incidents in the past year

For organizations with 16 or more tools (compared to organizations with fewer tools)



The case for greater data security through more integrated solutions and fewer tools becomes even stronger when looking at the sentiments and practices of those who prefer best-of-breed solutions or more tools.

"How is data going to be gathered, aggregated, and used from quite a few systems? A lot of different data points need to be put together in one ecosystem for it to really work. Or else you really have a Swiss cheese version of data security."

VP of IT
Manufacturing/Production

First, multiple disparate data security tools can lead to gaps in visibility and more shadow data. In fact, those who are concerned about shadow data are more likely to prefer best-of-breed solutions. This is most likely because organizations with a best-of-breed approach need to take more effort to gain a comprehensive visibility into their data security posture.

Second, managing siloed solutions brings more complexity to data security teams, as each disparate solution requires dedicated staff, endpoint agent installation and maintenance, and various new processes. Take alerts review and triage, one of the tasks that need staff and resources, as an example. An increasing number of alerts means extra efforts required of data security teams when managing isolated solutions. Organizations with more tools receive an average of 96 data security alerts per day, while teams with fewer tools receive less than half that amount, with 44. In addition, they aren't able to review as many of these alerts as teams with fewer tools can (61%, compared with 68%). This often also results in organizations with more tools being more reactive compared to organizations who use a lower volume of tools.

Lastly, more tools also indicate that organizations must exert extensive effort to integrate insights and remediation plans, and information can become lost in translation. When asked about the top data security challenges, the cost of implementing or maintaining data security solutions and challenges integrating data security solutions are ranked as the top two.

This translates to longer, slower processes, with 37% of those who use 16 or more tools reporting needing one month or longer to complete a data security investigation compared to only 21% of those with fewer tools.

"Right now, we're crawling. Every one of the systems that we have, they all have their own portals, their own tools, their own ways of dealing with things. Each person goes their own way, where they're the expert. Then they all get back together and decide what is going on, and we address it from there. So, it's a bit of manual work at this point," stated a Director of Infrastructure & Operations in manufacturing and production.

Ultimately, by choosing to continue with multiple solutions, organizations are ignoring their own talk of understanding that integrated solutions are superior and walking in the opposite direction – costing them time and money.

OUTCOMES OF THOSE WHO USE FEWER (<16) VERSUS MORE (16+) DATA SECURITY TOOLS

	Low Volume of Tools	High Volume of Tools
Number of **data security incidents** in the past 12 months	48	133
Proportion of **severe** data security incidents	19%	26%
Our current data security strategy is more **reactive**	31%	40%
Challenged with **integrating** solutions	24%	39%
Data security team spends most time on **response**	19%	26%
We are **confident** with our data security posture	56%	61%
Number of alerts **received** per day on average	44	96
Proportion of alerts we can **review** per day	68%	61%
One month or longer needed to complete a data security investigation	21%	37%

3

Organizations continue to be plagued by the stress of external and internal data security incidents, especially in business data.

Organizations continue to be plagued by the stress of external and internal data security incidents, especially on business data.

As factors around data – including the people who interact with data, activities around data, and devices and apps used to process data – are constantly evolving, data security incidents and data breaches can happen anytime and anywhere. And, these threats come from both external attackers as well as trusted personnel, including employees, contractors, and partners. Whether maliciously or inadvertently, all players can cause data security incidents – which means there's a constant need to protect across a multitude of areas.

A VP of IT in financial services said, "What you are trying to protect against is always changing. It's a moving target. It's always going to be evolving, changing, and flexible. What you are protecting and where it lives is only going to get more varied."

While data security incidents can come from various sources, the external threat of malware or ransomware incidents - instances where malicious software infiltrates a system, providing attackers with unauthorized access to systems or networks - are far and away the most common, with 50% of organizations surveyed having experienced at least one in the past year.

In addition, these attacks are where organizations feel the most vulnerable, with 41% saying they feel least prepared to handle future malware or ransomware attacks in the next year. This sense of vulnerability is even higher among those that prefer a best-of-breed approach – 44% feel unprepared for an attack of this nature, compared to only 36% of those who prefer an integrated solution.

Securing against and preventing insider risk is also top of mind for decision makers. 35% say they need to shore up defenses against malicious insiders and compromised accounts, and a third are concerned with inadvertent insider incidents. Although malicious insider incidents may not be the leading cause of data security breaches, they are the second most common type of incident decision makers feel least prepared to prevent.

"At least once a month, I get a call from a panicked director... 'we've had an event, I've uncovered an event, or the threat team has uncovered an event.' Some of them are unintentional, some are people not knowing or understanding what their privileges allow."

US Government CISO

Insiders are trusted individuals who typically have been granted access to, or possess knowledge of, company resources, data, or systems that are not generally available to the public. Consequently, the data security risks associated with insiders tend to be more elusive and difficult to detect. As Bret Arsenault, the CISO of Microsoft, indicated "Ultimately, it doesn't matter if the breach was intentional or accidental. Insider risk programs should be part of every company's security strategy."

DATA SECURITY INCIDENTS SUMMARY

Causes of data security incidents	Most common incidents in the past 12 months	Least prepared to prevent in the next 12 months
Malware or ransomware	50%	41%
Compromised accounts	38%	35%
Denial-of-service (DoS) attacks	35%	33%
Negligent insiders	32%	29%
Inadvertent insiders	31%	32%
Malicious insiders	31%	35%
Physical property	29%	29%

The data security solutions that organizations choose must also work for a variety of sensitive data, including high-value business data, operational data, and personal data. During data security incidents in the past 12 months, 74% of organizations have had business data exposed, 65% saw operational data compromised and 58% experienced personal data being made vulnerable. Among the various types of data, intellectual property, IT and network design, and PII has been compromised or exposed most often.

Looking ahead, 77% of organizations perceive business data, such as intellectual property and source code, as the most vulnerable. This is primarily because business data plays a crucial role in establishing competitive advantages and revenue generation. However, identifying and classifying such data can be challenging, as traditional pattern recognition, regular expression, or function match technology may not effectively identify content that lacks specific string formats or keywords. In turn, organizations need more advanced technologies to help discover and protect those vulnerable sensitive data.

TYPES OF DATA MOST AT RISK IN THE NEXT 12 MONTHS

77% **Business Data**		64% **Operational Data**		63% **Personal Data**	
Intellectual property	**30%**	IT and network design	**29%**	Personal Identifiable Information (PII)	**31%**
Source code	**28%**	Financial statements	**18%**	Human resources information (payroll, resume, etc.)	**21%**
Business plans	**27%**	Sales and revenue reports	**15%**	Payment card industry (PCI) data	**18%**
Trade secrets	**24%**	Procurement & invoice	**12%**	Protected Health Information (PHI)	**18%**
Merger & acquisition files	**20%**	Legal documents/ agreements	**12%**	Credentials	**17%**
Construction specifications	**18%**	Manufacturing processes/batch files	**11%**		

4

Organizations need Cloud and AI to drive digital transformation – but they're also the most vulnerable data locations.

Organizations need Cloud and AI to drive digital transformation – but they're also the most vulnerable data locations.

Collaboration through cloud applications and platforms, combined with new AI technology, significantly enhances employee productivity and enables flexible work arrangements, making cloud applications and AI technology essential for organizations. On average, organizations now utilize 147 public cloud services spanning SaaS, PaaS, and IaaS.[1] And, 66% of organizations have developed an AI strategy, with 36% already implementing it.[2] However, this evolution has created more dynamic and multifaceted risks, due to the difficulty of clearly defining data boundaries across various environments.

1. Measuring Risk and Risk Governance, Cloud Security Alliance (CSA), 2022
2. Microsoft data security AI research, Hypothesis, Mar 2023

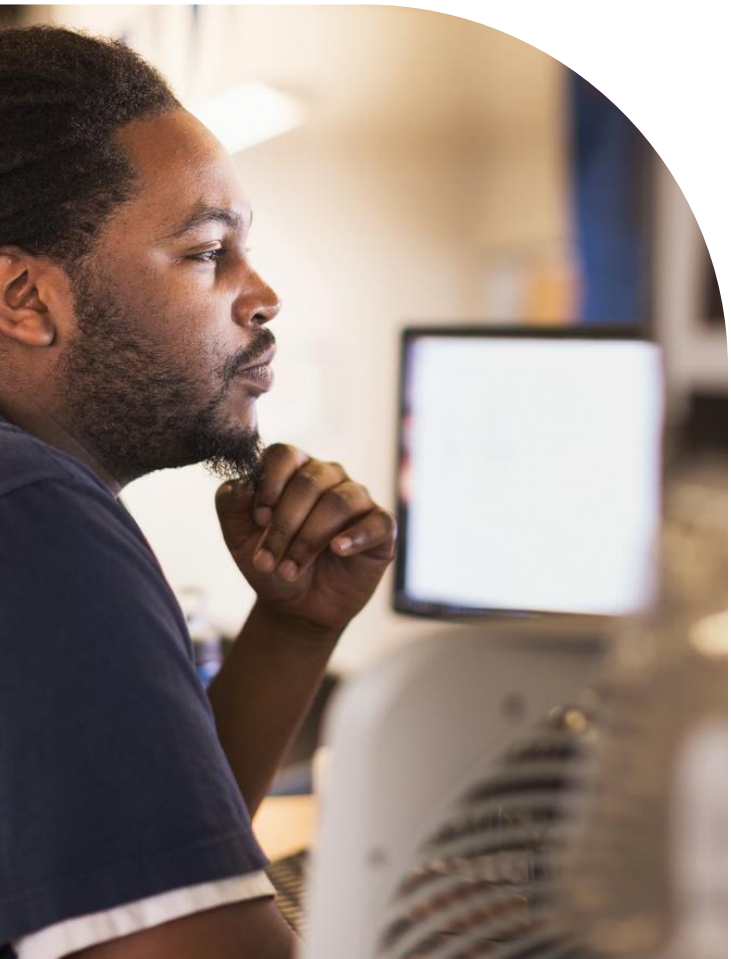
It's now even more crucial to have the right data security solution for these high-productivity data locations. In the past 12 months, 42% of organizations reported security incidents in cloud storage and 31% in emails, instant messaging, or online meeting tools. Incidents seem to be most common where the most productivity and collaboration happen.

Managing these types of incidents takes resources, and 79% of organizations report that their data security team needs more people to effectively manage critical data security responsibilities. However, among the organizations who claim to need more people, the majority (57%) prefer a best-in-breed approach. This preference highlights that organizations that use more solutions may struggle more to identify the true risks among the myriad user activities.

DATA LOCATIONS SUMMARY

Data Locations	Compromised in past 12 months	Most at risk
Cloud storage (e.g., Box, OneDrive, Google Drive)	42%	54%
Emails/Instant messaging/Online meeting tools	31%	39%
Platform-as-a-service (PaaS)	29%	34%
Infrastructure-as-a-service (IaaS)	28%	36%
AI (e.g., ChatGPT, Bard, etc.)	27%	38%
SaaS-based databases/data lakes	27%	41%
Endpoints/devices	25%	36%
On-prem repositories/file shares/databases	24%	28%
Shadow data	21%	23%
Line-of-business applications	17%	25%
Developer tools	16%	23%

With over a third of organizations implementing AI strategy, and more on the way, AI is being adopted at an unprecedented rate, much speedier than cloud and email adoption in the past. As organizations embrace AI, enhancing data security to enable responsible use and prevent risk becomes essential. AI is considered a top at-risk location for data security incidents, compared to other locations, and 27% of organizations have experienced an AI data security breach. Organization's concerns around the risks of using AI center around a lack of control over data shared with AI, lack of controls to detect and mitigate risky use of AI, lack of transparency around how generative AI models are trained, and leak of confidential information through AI.



"AI is good for productivity and efficiency, but it has potential security and data risks." An enterprise a Security Decision Maker stated.

While concerns around AI exist, decision makers can also see the potential, especially as vendors in the market are developing innovations to help empower businesses through responsible AI use. To further utilize AI, however, organizations report top controls they need are to detect malicious or risky content in AI, encrypt, mask, or anonymize data before it can be uploaded to AI, and identify sensitive data generated by AI.

TOP 5 DATA SECURITY CONTROLS NEEDED FOR AI

1. **Detect malicious or risky content** in AI
2. **Encrypt, mask, or anonymized data** before it can be uploaded to AI
3. **Identify sensitive data** generated by AI
4. **Prevent sensitive data from being uploaded** to AI
5. **Detect model or data manipulation** in AI

5

Automation and AI are promising avenues of greater protection.

Automation and AI are promising avenues of greater protection.

In an ideal world, without constraints based on organizational priorities or budget, half of organizations would like to be more proactive around data security management, spending more time on things like discovery of sensitive data and associated risks around it and prevention of data security incidents. Currently though, more than half of organizations spend the most time focusing on reactive measures like detection of incidents, response, and investigations. And this detection and response to data security incidents is time-intensive – it takes most organizations about a month to resolve a data security incident and for some, resolution can take up to six months.

The benefit of adopting a more proactive strategy is evident, as the organizations surveyed that are more proactive already experience less costly data security incidents, are more likely to be able to investigate those incidents in less than a month, and are more likely to believe their defense controls are sufficient in preventing data breaches.

While organizations are aware that proactive data security measures can help reduce data security risks, they are not making progress in implementing those measures. For example, those seeking to be more proactive by allocating more time to prevention are more likely to choose best-of-breed solutions, which actually demand greater efforts in handling reactive measures when bringing in detection signals and response controls together.

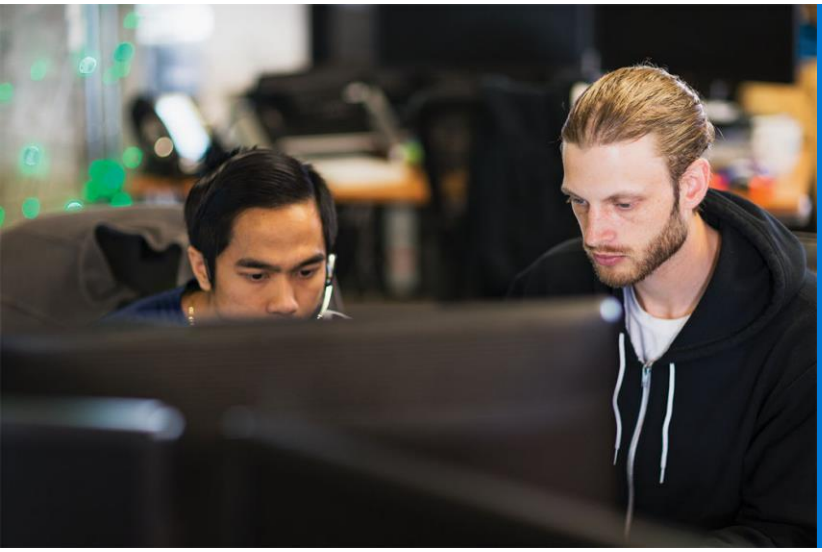
OUTCOMES OF ORGANIZATIONS THAT ARE MORE PROACTIVE VS. REACTIVE

	More Proactive	More Reactive
Average cost impact of a data security incident in the past 12 months	**$207k**	**$330k**
Complete a data security investigation in less than a month on average	**80%**	**68%**
Our defense controls are sufficient in preventing data breaches	**77%**	**68%**

As resources and staff are limited and the allocation of effort between activities might not be ideal, organizations are looking for technology to help them to set aside more time for proactive activities. Automation is one way for organizations to make time for a more proactive approach to data security. 74% of organizations surveyed would prefer semi or fully-automated risk mitigation, which allows security teams to minimize the impact of potential data security incidents ahead of time over manual reviews. Furthermore, organizations recognize many other tasks that could benefit from automation, such as creation of data security reports, automation of incident management workflow, and the response to and investigation of incidents. Most of the top tasks that security teams want to automate are reactive measures. By automating these tasks, organizations can alleviate the burden on their data security teams, enabling them to embrace a more proactive stance.

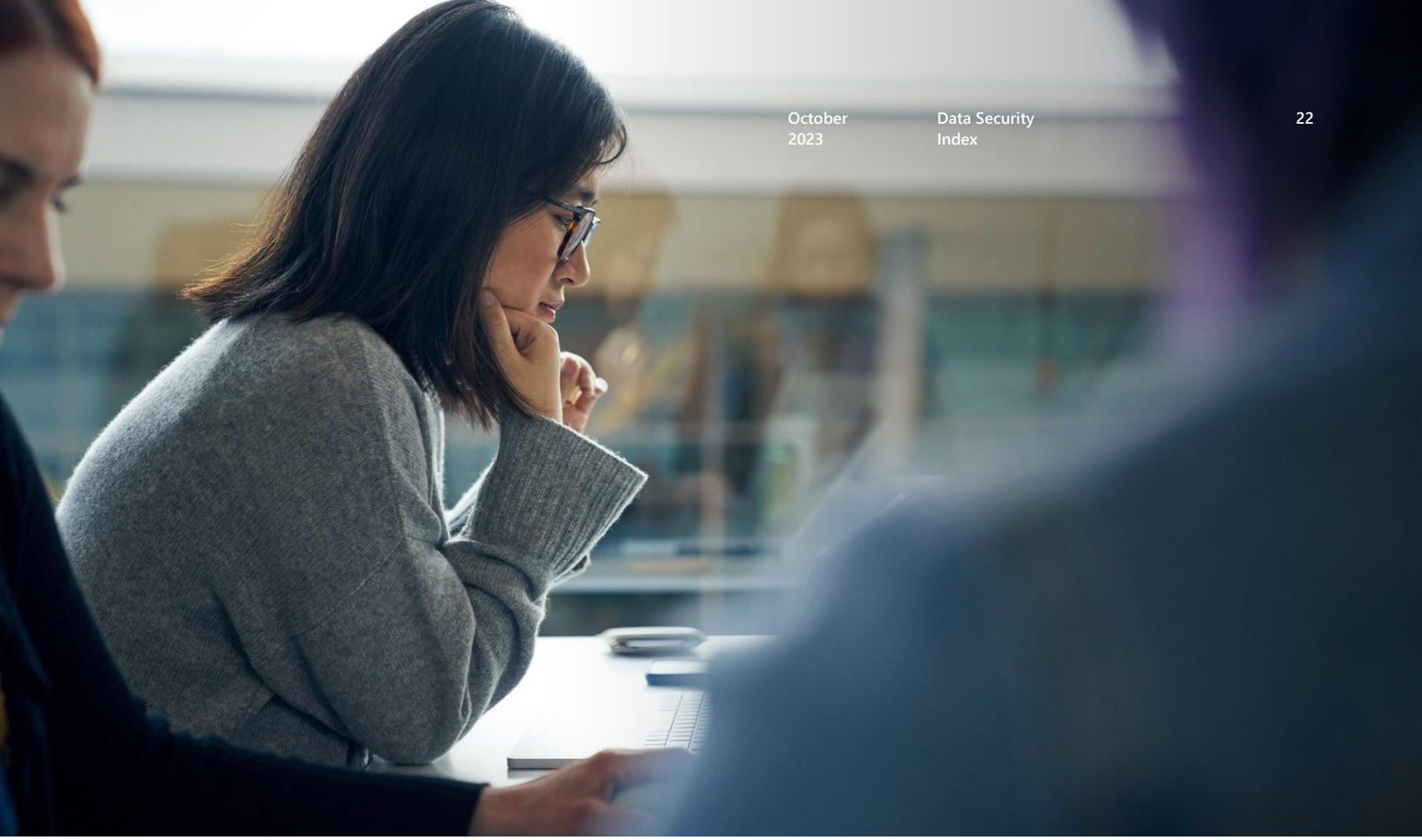
TOP 5 AREAS DATA SECURITY TEAMS PREFER TO AUTOMATE/ALLEVIATE

Reactive	1	Creating automated workflows for incident management and response
	2	Creating data security reports
Reactive	3	Responding to and containing data security incidents
	4	Routing incidents to the right teams (e.g., SOC, legal, HR) during investigations
	5	Investigating data security incidents



"There is so much risky data to manually evaluate. AI can help in speeding up our team's response times and protect data as we are under-resourced."

UK Security Decision Maker



Using AI for data security can also help organizations be more strategic and get smarter about future threats. The technology speeds up the response to detected incidents, buying data security professionals time to investigate further. Similar to automation, organizations cite many scenarios where AI can help provide stronger security, **thus saving their team's time**. Top scenarios for AI use include automatically blocking inappropriate sharing of data, detecting critical data security risks/ anomalous data activities, and investigating potential data security incidents.

By leveraging the benefits of AI and automation and moving towards more integrated solutions, organizations can embrace a more proactive data security strategy, and set themselves up for a more secure future.

TOP SCENARIOS WHERE AI IS USED

Automatically block inappropriate sharing of data

Detect critical data security risks/anomalous data activities

Recommendations to better secure your data environment

Investigate potential data security incidents

Finetune data security policies

Final Recommendations

- Adopt an integrated platform to strengthen data security posture
- Guard against data security incidents from both outside in and inside out with a defense-in-depth approach
- Upgrade your data security strategies with AI and automation

Adopt an integrated platform to strengthen data security posture

According to the findings in this research, fewer solutions can bring more security. It may seem counterintuitive, but organizations must combat the false sense of confidence that arises from a multitude of isolated solutions. Vendor consolidation offers a strategic approach that not only reduces costs but also enhances security.

Data security decision makers can initiate this transformation by empowering their teams to dedicate more time to strategic work like researching and planning for new security controls and optimizing security policies – something 84% of decision makers agree they want to be doing. This process involves replacing legacy siloed solutions, which are often considered 'best-of-breed' but fail to integrate effectively with other tools.

Decision makers can foster close collaboration with their teams to establish data security program goals and key performance indicators (KPIs). They can then progress by defining solution requirements and identifying non-negotiable features. This approach empowers them to pinpoint vendors capable of providing tools that align with their overarching objectives. Crucially, it promotes a forward-thinking mindset and helps teams avoid becoming overly fixated on existing practices or isolated use cases, allowing them to implement necessary changes towards a more integrated approach.

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

1. Discover and protect sensitive data within their digital landscape.
2. Detect critical risks associated with this data.
3. Prevent unauthorized use of sensitive data while not impacting legitimate business activities.

By implementing an integrated data security strategy, organizations can achieve a higher level of protection while simultaneously simplifying their security infrastructure.

Guard against data security incidents from both outside in and inside out with a defense-in-depth approach

Data security incidents commonly result from external attackers, malicious insiders, or inadvertent insiders. 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.

To tackle these challenges, organizations can adopt a defense-in-depth approach to data security. This strategy is analogous to a museum's protection of priceless artworks: cutting-edge security cameras equipped with threat intelligence monitor visitors, ticketing systems manage identity and access to the museum, and stringent security measures around the artworks operate similarly to data security controls protecting your valuable data. These measures discourage potential incidents, whether it originates from external bad actors or individuals already within the organization's environment.

Combating evolving data security risks requires a concerted effort across the organization to implement this defense-in-depth strategy. Data security team's collaboration with other departments, such as Security Operations Center (SOC), can optimize data security investment. Notably, 66% of organizations that consider themselves proactive interact with their SOC team, compared to 54% who do not.

Like teamwork across security teams, data security solutions should also seamlessly integrate with other systems, such as Extended Detection and Response (XDR) or Identity and Access Management (IAM) solutions, to effectively prevent data security incidents from both external and internal sources. These integrations enable organizations to conduct comprehensive investigations and responses to security incidents, gaining a thorough understanding of the affected data, actors, and activities, and responding with multiple mitigation controls. Consequently, this empowers them to make informed, precise, and prompt responses to minimize the impact of potential security incidents.

Upgrade your data security strategies with AI and automation

Automation and AI can help organizations be more proactive in data security. Here are some recommendations for your organization to embark on the automation and AI journey:

- Discover sensitive data: Utilize AI to assist in identifying sensitive data and applying protection policies, including encryption and rights management. This is particularly valuable for business data that may pose challenges for detection through traditional pattern recognition technologies. Organizations can leverage classification technology, such as machine learning or AI-powered classifiers, known for their intelligence and ability to swiftly locate sensitive content based on data context or business category. Alternatively, organizations can employ exact data matching technology to discover operational or personal data.

  Furthermore, as industry regulations evolve (e.g., GDPR, HIPAA, or PCI DSS) and data landscape become more dynamic, it is crucial to possess advanced classification technology that is customizable and easily adaptable to identify new categories of sensitive data.

- Detect critical data security risks: Harness the power of AI to pinpoint critical risks associated with your sensitive data and allocate resources strategically to address potential high-risk incidents. AI technologies can generate high-fidelity alerts, allowing security teams to save valuable time that would otherwise be spent sifting through an abundance of false-positive alerts. Moreover, AI can assist organizations in identifying elusive risks, particularly when malicious actors attempt to evade detection. It is imperative to utilize machine speed to outpace these threat actors.

- Prevent data security incidents dynamically: Use AI and automation to tailor your prevention and mitigation controls automatically based on assessed risks, enabling a more adaptable and proactive data security strategy. When AI-powered solutions detect and evaluate risks, automated prevention controls can swiftly engage to safeguard the data, applying mitigation controls precisely to the high-risk areas. For instance, in cases where early indicators of data exfiltration intent are detected by high-risk users, organizations can apply more stringent Data Loss Prevention (DLP) policies, proactively staying ahead of potential data security incidents.

We hope you find the insights and recommendations in this report helpful to enhance your data security posture and fortify your organization against evolving risks.

To learn more about Microsoft Data Security, visit https://aka.ms/DataSecurityNews

Detailed Research Objectives, Methodology, and Audience Recruit

The objectives of the research included:

1. Understand the data security landscape, including priorities, mindsets, and challenges
2. Map the cause and effect of data security incidents and identify actions that data security teams can take to enhance data security posture
3. Explore the future of data security, including emerging strategies and innovations around using AI for data security

Methodology was:

A 15-minute multi-national online survey was conducted July 28-August 9, 2023, among 822 data security decision makers.

Questions centered around the data security landscape, how data security teams allocate their resources, data security incidents, and attitudes toward and use of artificial intelligence (AI) for data security.

To meet the screening criteria, Data Security Decision Makers needed to be:

CISO and adjacent decision makers (C-2 and above) with purview over data security

Work at Enterprise organizations (500+ employees; range of sizes)

Mix of regulated and non-regulated industries (no education, government, or non-profit)

Of the 822 Data Security Decision Makers surveyed for the research, completes by country were:

US	329
UK	322
Australia	171