

Rethinking Security from the Inside Out

March 2024



Foreword

The technological advances enabling and evolving businesses are the same technological advances that could expose you and your team to threats from data breaches, insider risks, ransomware, and more potential harm. It's this paradox that set our teams at Microsoft out to learn more about internal threats as well as standard data security practices being adopted worldwide that may actually be creating potential harm alongside this once-in-a-generation innovation. Add in AI and machine learning, and the ecosystem gets more complex, and more difficult to cover.

Read on to learn about what we found in our survey of more than 500 data security and identity and access management professionals. What you will find is a deep analysis of the need for different approaches, forward thinking, and adequate staffing across teams of all sizes. As always, we welcome your insights and feedback on what comprehensive solutions look like to you and your peers and discussions about needs for your own industries.

Rudra Mitra

Corporate Vice President
Microsoft Data Security and Compliance

Introduction

In today's landscape, every company is a tech company. That's because technology plays a critical role in nearly every aspect of every business, offering more ways to connect with customers and drive revenue — but also with more risks for your data to get stolen, compromised, or misused.

The rise of remote work has created a broader attack surface to exploit. Both insider risks and external threats like ransomware and zero-day exploits get more sophisticated by the day. And if you're attacked, the costs associated with legal fees, regulatory fines, and reputational damage can be devastating.

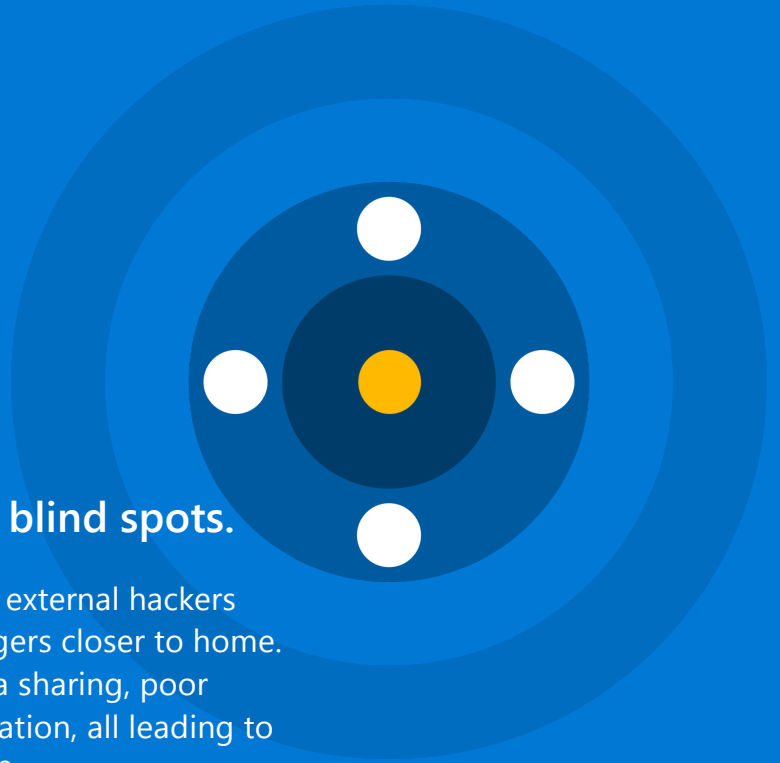
It should come as no surprise then that data breaches are more widespread than ever, but too many companies don't have enough bandwidth to fight back. Even with adequate support, security teams often find themselves focused on tracking external threats that they overlook the potential risks posed by their own staff.

In this paper, we'll discuss why these internal risks matter and what you can do about them. We'll look at standard practices that may be putting your organization in danger. Finally, we'll explore what a comprehensive solution might look like — and what you'll need to turn that vision into a reality.

To help organizations understand the need for a different approach to internal risks, Microsoft commissioned an independent research agency, Hypothesis Group, to conduct a multinational survey of more than 500 data security and identity and access management (IAM) professionals across a wide range of industries.



The need to protect from insider risk



Conventional data security is full of blind spots.

Today's security leaders are so intent on fighting external hackers that they forget to protect themselves from dangers closer to home. These insider risks can include unintentional data sharing, poor password practices, and theft of sensitive information, all leading to data breaches which can cost millions to clean up.

Manual processes are part of the problem.

Many organizations rely on manual processes to manage user access to sensitive corporate data. These processes are resource-intensive and prone to human error, leaving you vulnerable to attack. By taking an automated approach to IAM, you can manage risk profiles, detect potentially risky activity, and enforce access policies without hampering the productivity of your most trusted users.



Organizations want a comprehensive solution — without overextending IT

Security teams are managing too many tools.

As new risks continue to emerge and evolve, many companies have invested in a growing array of point solutions. That can make it difficult to see the big picture, and it may even create security gaps that can be exploited.

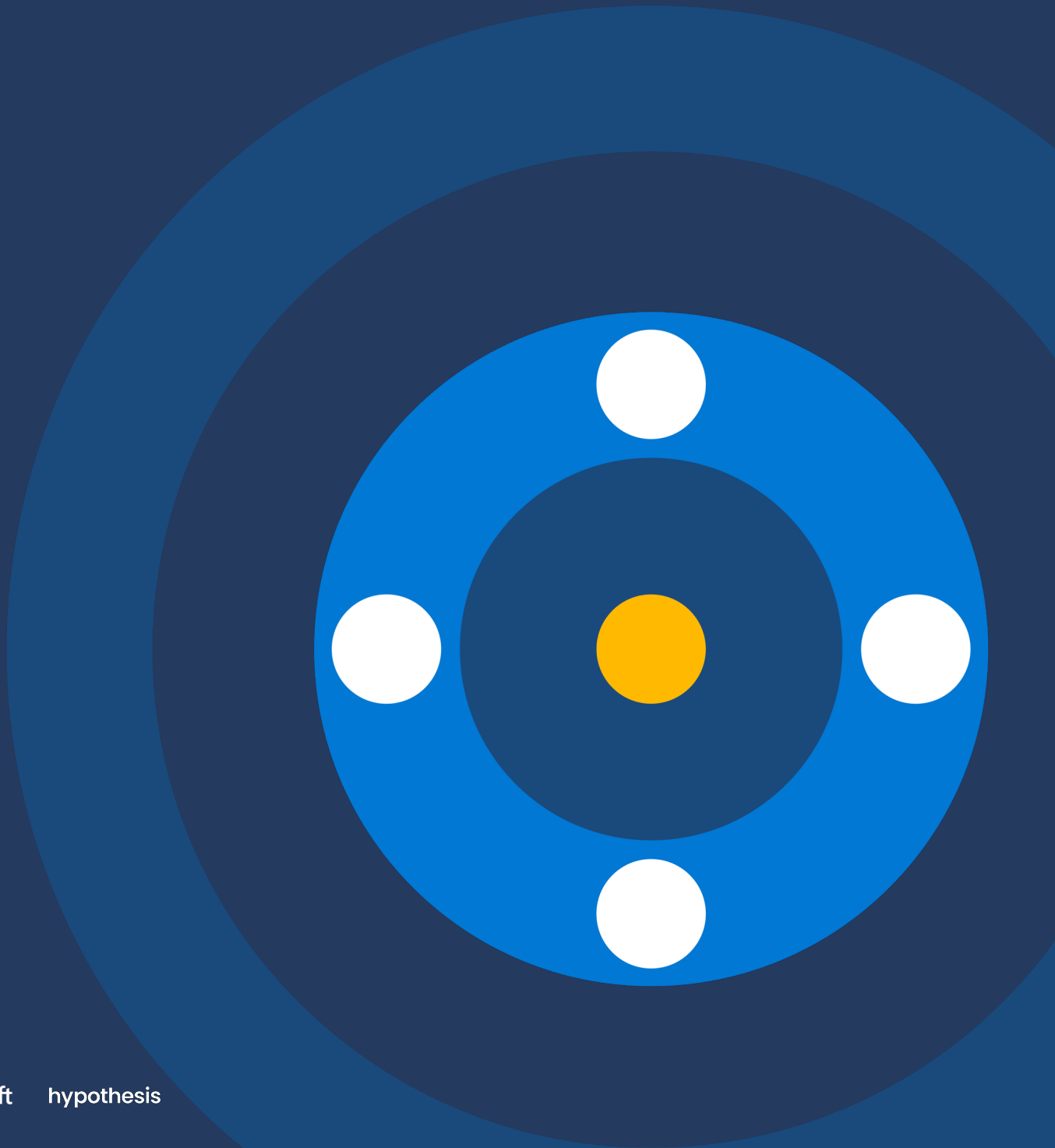
Consolidation with a dynamic, comprehensive solution is the right approach.

Consolidating tools could help protect your organization against new risks, both internal and external, by better leveraging insights across solutions. Limiting the number of tools can help streamline the IT workflow and reduce operational costs.

But, consolidation requires commitment.

Adopting a new solution across your entire infrastructure is challenging, since most IT teams are already overextended, but can be done well with the right support in place. Many security leaders believe that starting with outside support from a third-party provider or MSP can help them navigate the initial complexities of implementation, training, and change management without overburdening internal staff.

The need to protect from insider risk

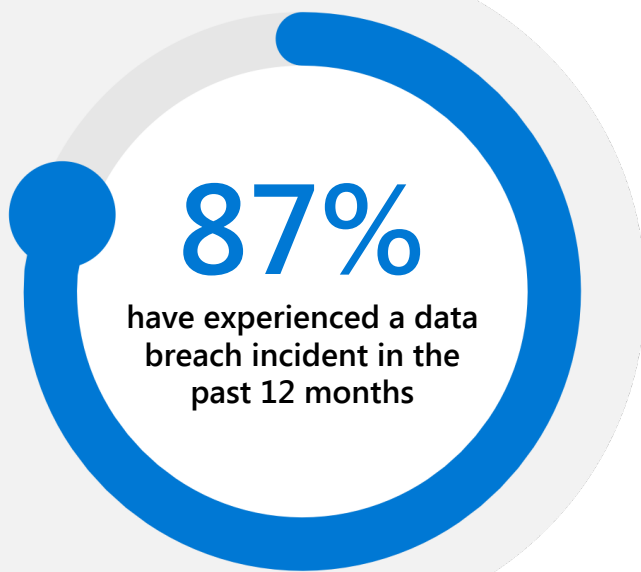


Data breaches are on the rise — and taking a heavy toll

If your organization didn't suffer a data breach last year, consider yourself very lucky.

According to our survey, 87% of security leaders report having experienced a data breach in the past 12 months. This points to a staggering loss of revenue, as organizations report that annual incidents could cost up to \$15 million. And those numbers don't take into account indirect costs like customer attrition and loss of reputation, either of which could haunt a company for years.

Worse yet, the problem doesn't appear to be going away. Our research indicates that 61% of organizations are just as, or even more, vulnerable to data breach incidents as in 2020. 26% of organizations have experienced an increase in data breach incidents, while 35% have seen the same number of incidents.



"It was estimated that the intellectual property theft cost upwards of a billion dollars in potential loss in the lifecycle of the product."

Global Head of Information
Security, Agriculture



Insider risks are a top cause of breaches, but a lower priority, leaving organizations at risk

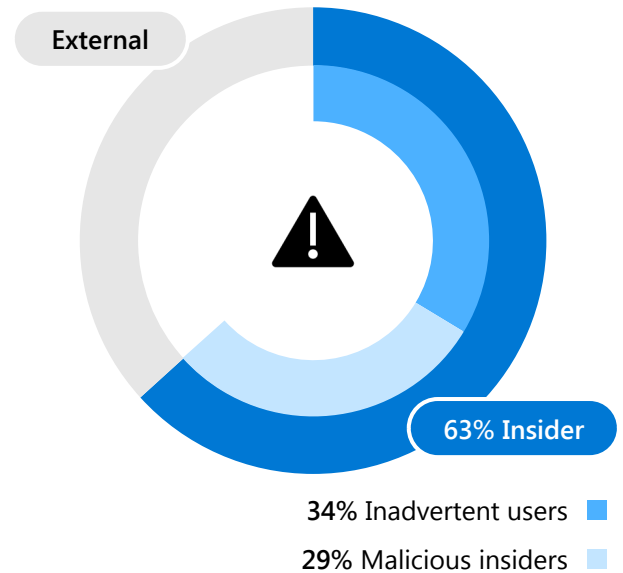
In asking security leaders to name the number-one cause of data breach incidents, many say that external threats top the list. Hackers, phishing scams, and advanced persistent threats are often cited as the prime culprits behind the compromise of data integrity.

However, the reality is that nearly two-thirds (63%) of data breach incidents originate with insiders, while only 37% stem from external threats like stolen credentials. These insiders are not necessarily malicious actors; they often include well-meaning employees who accidentally use unsecured networks or share sensitive information.

But most security leaders simply don't see the dangers within their own doors, and insider risks are an even lower priority among larger enterprises. That's why many prioritize protecting compromised users (44%) and fewer prioritize protecting against insider risk (33%). This skewed perception can lead to gaps in security protocols and an underestimation of the true risks facing an organization from within its own ranks.

TOP CAUSES OF DATA BREACH INCIDENTS

37% Lost/stolen credentials



USER RISK PRIORITIES

Prioritize compromised users	44%
Equal priorities	23%
Prioritize insider risk	33%



Organizations are overlooking the full range of risky activities that contribute to insider risk

Organizations today tend to focus on a few early indicators of insider risk: poor security practices and suspicious data access patterns that could be precursors to data compromise.

Meanwhile, security leaders often miss more active and malicious activity like deliberate sabotage or theft of sensitive data by disgruntled employees. They also neglect to look at access creep, a security risk that occurs when individuals gradually accumulate access or privileges over time without proper oversight.

That’s why more organizations are starting to implement comprehensive security education and robust security measures that address a broad spectrum of potential risk — not just the most visible or familiar activity. In the words of one CIO, “There’s not enough phishing training. People make mistakes. They’re not paying attention, they’re rushing, or something just looks real. You have to have as many layers of defense as possible to mitigate risk.”



TOP INDICATORS OF USER RISK

Internal Risk
External Threat

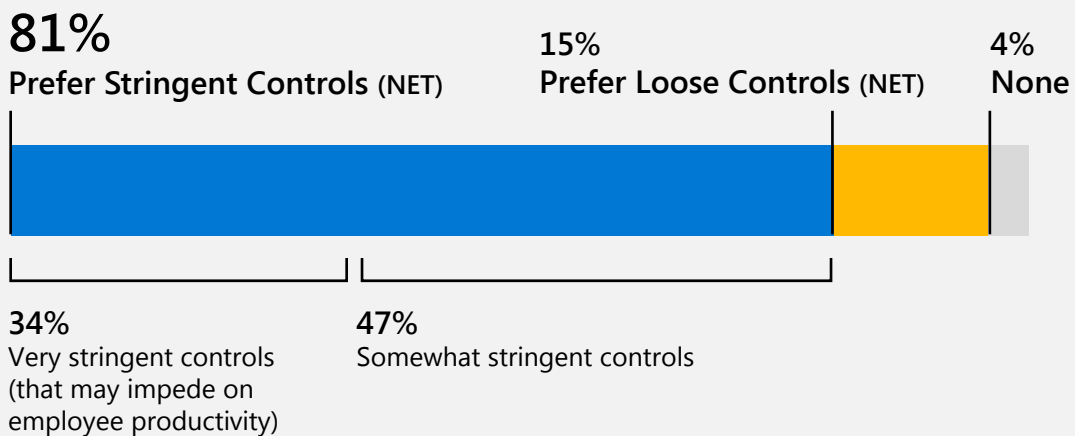
1	Risky browsing activities (like visiting sites known to host malware)
2	Using unauthorized applications
3	Clicking on phishing emails
4	Weak password practices
5	Working on a highly confidential project
6	Suspicious data access patterns
7	Uploading data to USB or personal drive
8	Data exfiltration attempts
9	Unusual IP addresses
10	Violated corporate or regulatory policy
11	Renaming files for concealed exfiltration
12	Recent changes in job role or responsibilities
13	Increasing access permissions over time
14	Recent resignation submission
15	Failed login attempts

Finding the right balance between strict controls and optimal productivity is more challenging than ever

When it comes to managing user access, the vast majority of organizations (81%) opt for stringent controls. But nearly two-thirds (64%) see a clear downside to that approach and indicate that stringent controls can have a negative impact on employee productivity.

While one-size-fits-all policies aren't working, that doesn't mean looser controls are the answer either. In fact, according to our survey, those who prefer looser controls are 3 times more likely to experience data breach incidents.

It all comes down to finding the right balance between appropriate oversight and keeping pace with the day-to-day demands of the business. That's why many organizations are opting for smarter, more dynamic controls that can adapt to the specific user's risk levels without hindering the flow of work. A Director of IT Security claims, "Dynamic access is much more secure because the access control policy can be much more intelligent and less disruptive than what we have now, which is based on static information."



Managing insider risk requires a combination of automation and provider support

What’s the best way to manage insider risk while optimizing for user productivity — especially when many IT and security teams are already overextended? Organizations utilize a combination of tactics to manage insider risk, many of which combine third-party provider support with more dynamic and automated access controls.

Our research shows that most security teams (84%) are burdened with manually approving access every few hours (or more often). Ongoing support from a trusted provider could ease that burden, ensuring that access control remains both efficient and effective without constant manual effort.

Meanwhile, an even larger majority (90%) say that additional investment in AI-powered data security tools is a top priority, potentially freeing up internal teams to focus on more complex and strategic tasks. This pivot toward automation and AI reflects a significant shift in how some organizations are thinking about insider risk — prioritizing the detection of internal risks in a way that supports, rather than hinders, operational efficiency.

% OF ORGS DESIRE EACH TACTIC TO MANAGE INSIDER RISK

Provider Support	Provider support to navigate legacy systems	38%
Access Controls	More dynamic controls to manage different levels of user risk	38%
Provider Support	Provider support to navigate incomplete policies	37%
Solutions/Strategy	More automation/less manual processes	37%
Solutions/Strategy	Improved incident response plan	37%
Provider Support	Provider support to navigate complexity of infrastructure	36%
Training/Resources	Better communication between security teams	36%
Access Controls	Right-sizing access (e.g., role change, resignation)	31%
Solutions/Strategy	Consolidating with a single solution	31%
Training/Resources	More end user training	28%
Access Controls	Just-in-time access	26%
Training/Resources	More resources	25%

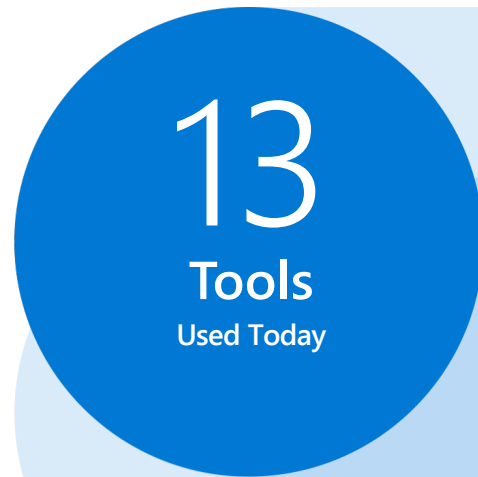
Organizations want
a comprehensive solution
— without overextending IT



The danger of relying on too many tools

The vast landscape of data security tools is highly fragmented. Our research shows that organizations use around 13 different solutions to manage discrete aspects of data security. These may include data loss prevention (DLP), identity and access management (IAM), user activity monitoring (UAM), compliance management, insider risk management (IRM), security information management (SIM), and many more.

The data indicates that consolidation should be an especially high priority for larger enterprises, which are more likely to use a broader range of tools. The reason is simple: the more tools you use, the more likely you are to experience data breach incidents (91% of organizations with a high volume of tools experience a data breach incident vs. 81% of orgs with a low volume of tools).



"We use a number of tools to look at different things — managing file shares, trending, patch management. We have DLP, SIM, and a SOC that will alert us to anything that looks like a strange trend or someone trying to exfiltrate data."

CIO, Human Resources Services



Managing both data security and IAM tools can be too much for one team

While some larger organizations rely on separate teams to manage data security and IAM, the most common practice is to manage both under a single team. As one CISO puts it, "I'm responsible for the P&L of information security that rolls up to the CIO. It's important to note that both data security and access management are under my umbrella."

Organizations with two separate teams are more likely to use a broader range of tools — and therefore experience more data breach incidents. Meanwhile, the single team approach often results in departments that are under-resourced and unable to oversee the full tool stack.

Organizations are choosing to integrate teams and solutions, often with help from a third-party provider, as they work towards alleviating their operational burden without compromising security.

"I'm responsible for the P&L of information security that rolls up to the CIO. Both data security and access management are under my umbrella."

CISO, Agriculture

A single team that manages/oversees both data security and IAM

64%

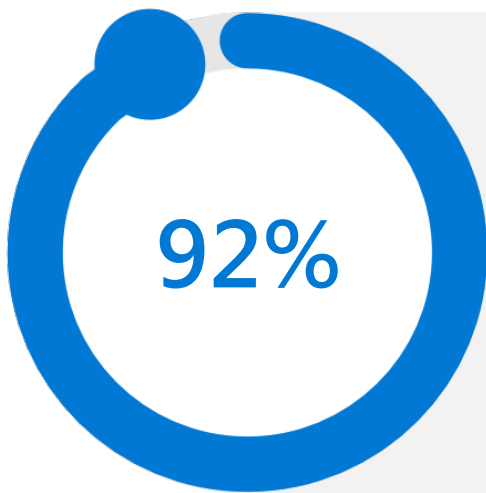
Different teams for data security and IAM management

36%

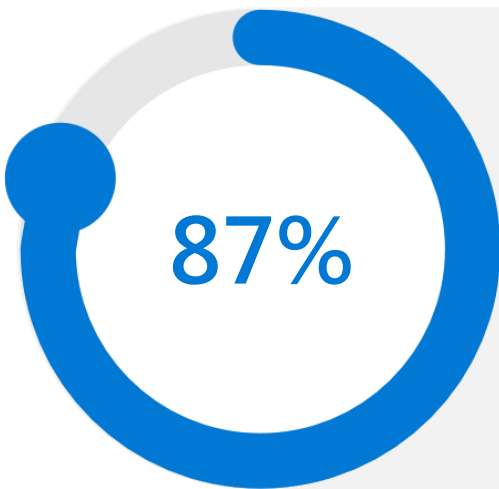
Consolidation is the right approach

If fragmentation is the problem, then consolidation is the solution. But that's easier said than done. Our survey shows that an overwhelming 92% of respondents would prefer to consolidate their data security and IAM tools. Nearly as many (87%) believe that a comprehensive data security and IAM platform with integrated solutions would be superior to using multiple point solutions that must be manually integrated and managed.

In particular, many security leaders say they clearly understand the value of dynamically adjusting data security and access policies based on a user's perceived risk level — especially if that is possible within a consolidated platform. As one CTO observes, "From an IT standpoint, if this is under one policy engine, it's a whole lot easier to manage and detect potentially risky activity. If we could do that with one policy engine, it would reduce our attack surface."



Our preference would be to **consolidate** the number of data security and IAM tools we use



A **comprehensive** data security and IAM platform with integrated solutions is superior to using multiple best in breed solutions that have to be manually integrated and managed



A comprehensive platform would unlock real business value

When we ask security leaders to consider the potential benefits of consolidation, the consensus is clear: an adaptive, comprehensive solution would enable them to jump on problems faster, with a third foreseeing quicker response times. Keeping up with regulations and maintaining compliance would also be less of a headache according to a third of respondents. Additionally, they see the potential of real cost savings by proactively stopping attackers in real time and automating access policies.

“I see value in the automated workflow, policy assignment based on risk scoring, early warning triggering, and the ability to catch an outlying risky event and block it before it happens,” noted one respondent, a Global Head of Information Security in the agriculture industry. “That’s the difference between a four-year, \$1 billion potential loss of revenue because one file made it out the door — or turning the same situation into a non-event.”

TOP 5 REASONS TO ADOPT A CONSOLIDATED SOLUTION

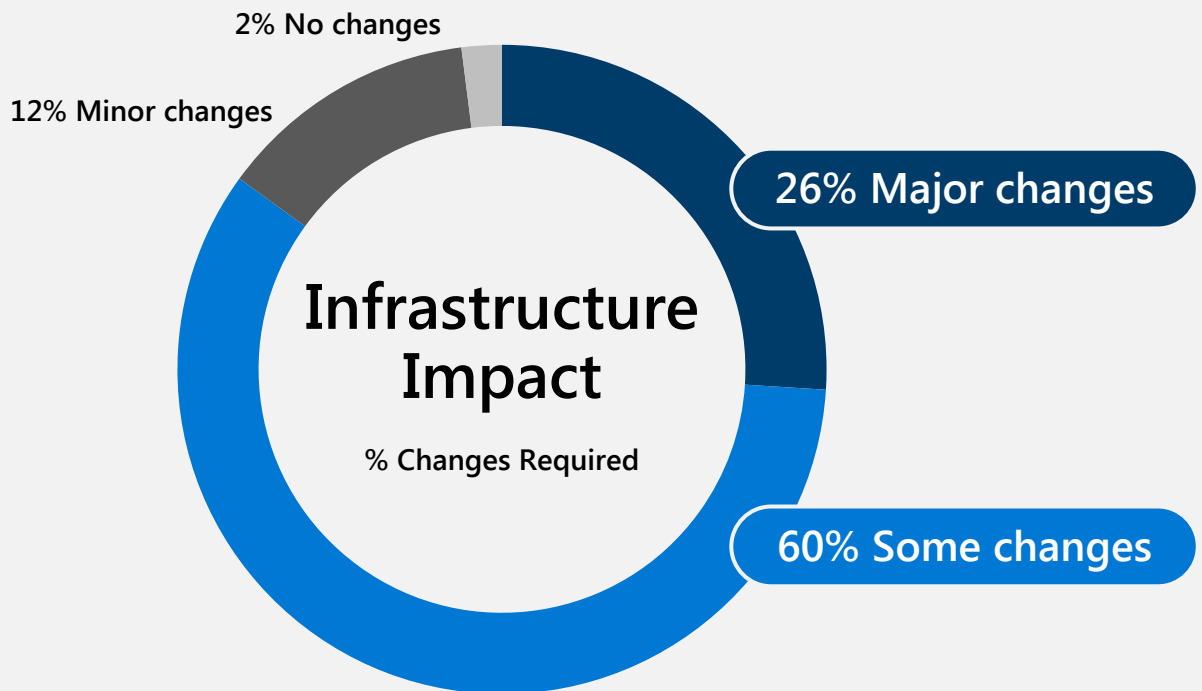
- 1 Improved **response time** to security incidents
- 2 Adherence to **compliance** and regulatory obligations
- 3 **Cost savings** from more efficient access management
- 4 **Real-time reactions** to proactively stop attackers
- 5 **Automation** around putting users in and out of policy

Effective integration is challenging but necessary and calls for a different approach to infrastructure

The excitement around consolidation is real. While a quarter (26%) of security leaders say that implementing a consolidated solution would require major changes to existing security infrastructure and processes, the majority wouldn't expect the changes to be so impactful. 60% acknowledge there would be some changes required and another 12% think only minor changes would be necessary. 2% indicate that a consolidated solution would require no changes to infrastructure at all.

So, what does that mean in practice? As one might expect, the more complex the system, the harder it may be to switch. Security leaders who believe major changes would be necessary are also more likely to be managing a broader range of tools (10+) (30% vs. 20%) — and thus more likely to be hit by a data breach (31% vs. 24%).

For such organizations, the right approach to consolidation would not only protect their most sensitive data, but also mitigate any potential impact on productivity.



IT will bear the brunt of any infrastructure change — so they'll need support to make it happen

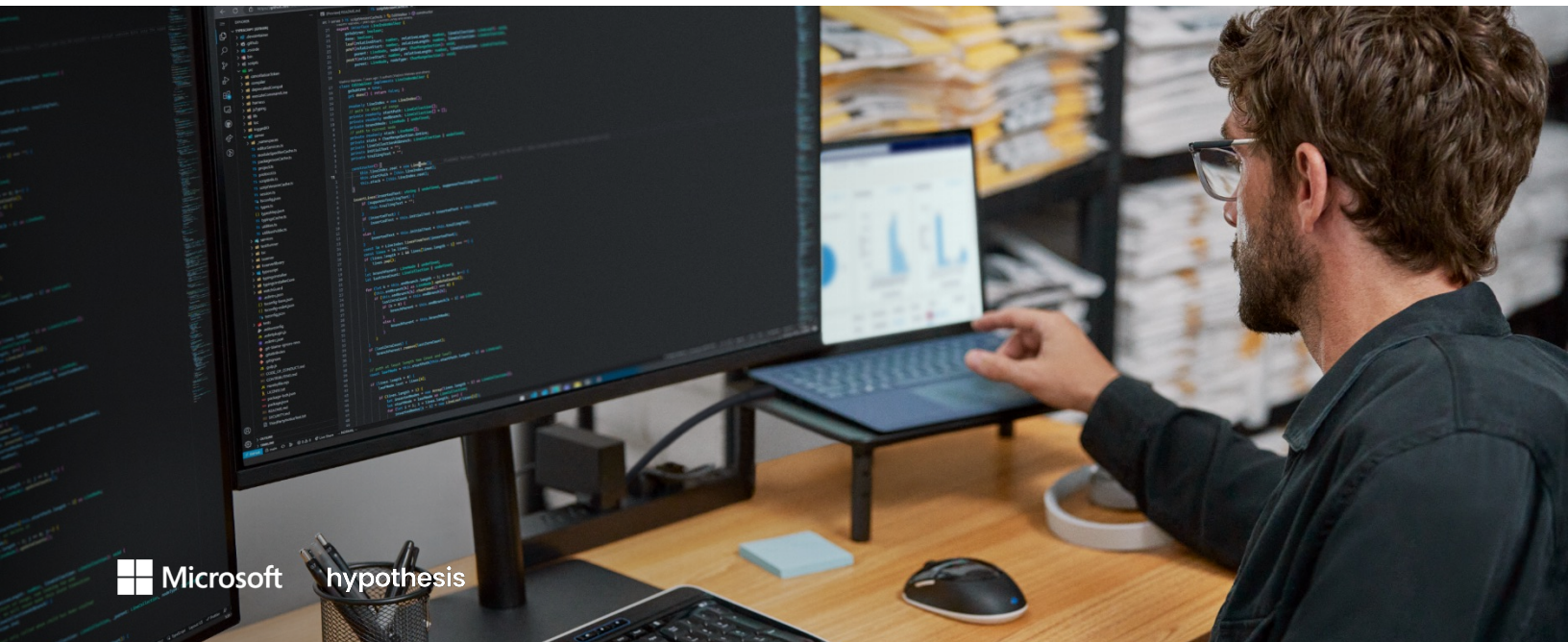
Given the potential impact on infrastructure, IT would most likely be responsible for implementing a comprehensive data security and IAM solution, with security teams and CISOs providing critical leadership and strategic direction along the way.

In our survey, the majority of security leaders (56%) say that a consolidated solution would require increased dependency on data security and IAM protocols. Another 43% note that more IT training would be required to implement the solution, highlighting the need to elevate the skillsets of IT personnel to match the complexity of emerging security technologies.

Meanwhile, 38% of respondents predict that an infrastructure-wide implementation would result in a larger IT workload. In other words, organizations may need to brace for a period of increased demand on their IT resources — or perhaps enlist the help of a third-party provider to help them navigate the transition to a more comprehensive and adaptive platform.

TOP 5 NEEDED CHANGES TO INFRASTRUCTURE

Increased dependency on data security and IAM	56%
More IT training needed to implement the solution	43%
Increased IT workload	38%
Evaluate and address impact to end user productivity	35%
Time needed for the solution to learn	32%



Final Thoughts

Final Thoughts

A secure data environment doesn't happen by accident. It calls for a proactive strategy, an adaptable infrastructure, and a well-equipped IT and security team. Here's how to make that happen.


● Hedge against data breach incidents by reinforcing security best practices and protecting yourself from insider risk.

In a fast-evolving risk landscape, the goal of every organization should be to maintain a robust defense against the risk of data breaches from any and all sources. That's why forward-thinking organizations are reinforcing their security apparatus with vigilant, responsive systems that preemptively identify and mitigate insider risks.

● Bolster your data security strategy with dynamic access controls.

This means implementing a system that not only adjusts data security based on the user's risk level as it fluctuates over time but also adapts to changing conditions in real time. A truly adaptable system should proactively identify user activity, flagging and responding to abnormal patterns that could indicate a breach — thereby ensuring that only the right people have the right access at the right time.





Give your teams adequate resources to navigate the implementation and management of a comprehensive, adaptive solution.

Supporting your IT and security teams isn't just about providing them with the latest tools. It's about acknowledging the complexity of the task at hand and offering them the necessary resources to get it done — whether that be training to sharpen their skills, additional personnel to manage the increased workload, or expert guidance from solution providers to streamline the transition process. Above all, it's important to foster an environment where your teams feel empowered to suggest improvements and lead the charge in adopting new, more effective security measures to guard against every kind of risk.



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 Adaptive Protection integrated with Conditional Access, visit:

aka.ms/adaptiveprotection/conditionalaccess

Detailed Research Objectives, Methodology, and Audience Recruit

The objectives of the research included:

- 1 Understand the current user risk landscape including areas of investment, approaches, and challenges
- 2 Identify the interest, benefits, and barriers to implementing a consolidated, dynamic solution

The methodology was:

A 20-minute multi-national online survey conducted from Dec 19 - Dec 29, 2023, among 502 data security decision makers.

Questions centered around the data Security/IAM landscape, how organizations manage data security and IAM solutions, 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 at least one of: data visibility, data risk management, data loss prevention, insider risk management, data classification, AND IAM

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

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

Of the 502 Data Security Decision Makers surveyed for the research, completes by county were:

US	254
UK	248

