Microsoft Security

Secure employee access in the age of AI

The road towards identity and network unification

Introduction

The rise of cloud, distributed workloads, and SaaS applications made it easier for employees to work from anywhere and connect. Now, generative AI is once again reshaping work and collaboration, creating even more access points, workload identities, and access permissions.

The number of identities and endpoints has proliferated, expanding the attack surface area. Today, there are over 300 billion passwords in use by humans and machines,[1] making identity the most popular attack vector and the first line of defense for organizations.

Password attacks make up more than 99% of the identity attacks we see. Microsoft blocks over 7,000 password attacks per second.[1] As more organizations enforce MFA, attackers are pivoting to more sophisticated attacks. For example, while token theft still accounts for fewer than 5% of all identity compromises, incidents are growing. Microsoft detected 147,000 token replay attacks, an 111% increase year-over-year.[2]

This world demands a new security approach beyond traditional security technologies. To learn how organizations can improve security and user experience for their employees, Microsoft partnered with Hypothesis Group, an insights, design, and strategy agency, on a two-stage research project:

Phase 1: Quantitative Survey

In November 2024, a survey was conducted in the United States among 300 professionals at enterprise organizations with decision-making authority over Identity Management and/or Network Access Management. They were surveyed about their current approach to identity and network access security as well as their planned investments for the future.

Phase 2: Qualitative Interviews

In December 2024, Hypothesis Group conducted qualitative interviews with 4 senior level US Security Decision Makers to gain further insight into the quantitative results.

This paper explores the evolution of work and the complexity of securing identity and network access for all applications and resources in an evolving threat landscape. It delves into the attitudes towards stronger collaboration between identity and network access teams.

1. "Microsoft Digital Defense Report 2024." Microsoft.
2. "How to break the token theft cyber-attack chain." Microsoft.

Key Findings

1

In today's complex modern work environment, organizations face numerous identity and network security challenges.

% Find it challenging to...

50%
Simplify employee identity lifecycle

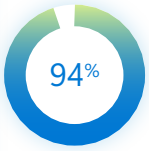
46%
Implement least privilege access

37%
Secure hybrid work (employees working both in-office and remote)

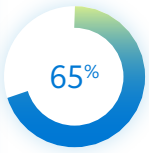
32%
Secure access to AI applications

2

These challenges lead to incidents impacting all organizations. To address them, security leaders deploy multiple solutions that are often managed by siloed teams and result in fragmented workflows:



Experienced an identity/network access incident in the past year



Incidents resulted in loss of customer trust

IDENTITY

5 Identity access solutions from **3** Vendors on average

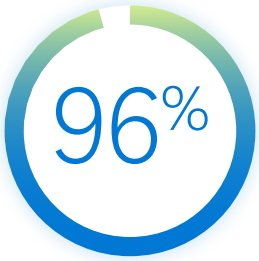
NETWORK

4 Network access solutions from **3** Vendors on average

3

Ultimately, to better protect employees, enhance the user experience, and make security teams more efficient, organizations overwhelmingly want to:

Increase collaboration between identity and network teams



Unify identity and network access controls

1

Complexity of modern work

The rise in identities and applications, varied work models (in-person, remote, hybrid), and rapid AI adoption have transformed the workplace, offering unprecedented flexibility. But legacy security approaches like manual identity lifecycle management didn't catch up, creating complexity and challenges for identity and network decision-makers.

58%

Expect number of identities to grow in the next year

61%

See an increase in incidents due to remote/hybrid work

84%

Say employee use of GenAI apps will increase in the next year

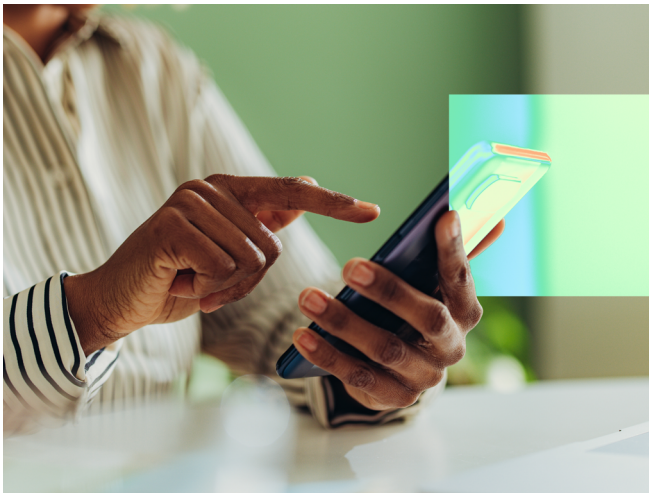
57%

Anticipate a rise in incidents due to increasing employee GenAI use

Identity and application sprawl is making it harder to manage and secure access

As organizations adopt new ways of working, managing secure access across diverse environments becomes increasingly complex.

The first challenge is simplifying the **employee access lifecycle**, including onboarding new employees and automating join-move-leave processes. Once employees are in, **ensuring proper least privilege access** is another top priority.



This challenge is expected to grow, with **58% of those surveyed anticipating an increase in the number of identities** at their organization in the next 12 months.

> **"A key challenge we face is working with developers and app owners to simplify the role-based access control."**
>
> CISO, Legal & Professional Services

Top challenges in securing and governing employee access

Managing employee access lifecycle (NET)	**50%**
Reinforcing security of employee self-service access management with identity verification	23%
Simplifying the onboarding of new employees	21%
Automating the join-move-leave processes	16%

Ensuring least privilege access (NET)	**46%**
Advancing Zero Trust security strategy	29%
Ensuring least privilege access for all employees	23%

Adding to the complexity of securing employee access is the vast amount of application sprawl. Decision-makers reported that their **organizations use over 2,500 applications on average**, including both SaaS/cloud-based and on-premise, which adds to the complexity. Additionally, 71% expect the number of cloud-based applications to increase in the next year.

2,500+

Applications on average used in organizations

71%

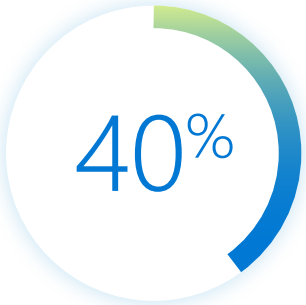
Anticipate cloud-based applications used to increase in next 12 months

"Our core applications number several hundred. If I look in my Cloud access security broker, I will see about 6,000 SaaS apps. Sprawl is a big issue. You get new apps that are getting more complex, there's more differentiation in needs, which means even more apps."

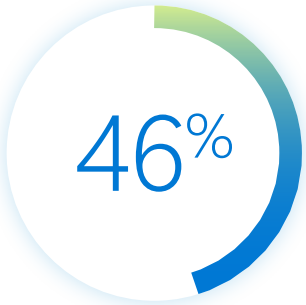
CISO, Legal & Professional Services

Remote and hybrid work is forcing organizations to rethink their access strategy

Organizations continue to have a large part of their workforce off-site, making it even more challenging to secure access. While this flexibility is preferred by employees, it creates challenges in providing seamless sign-in experiences and securing all access points. Additionally, **61% report that remote/hybrid work leads to more identity and security incidents.**



Say that sign-in experience when working remotely is complex and inconsistent



Find it difficult to secure access to all apps for remote and hybrid workers

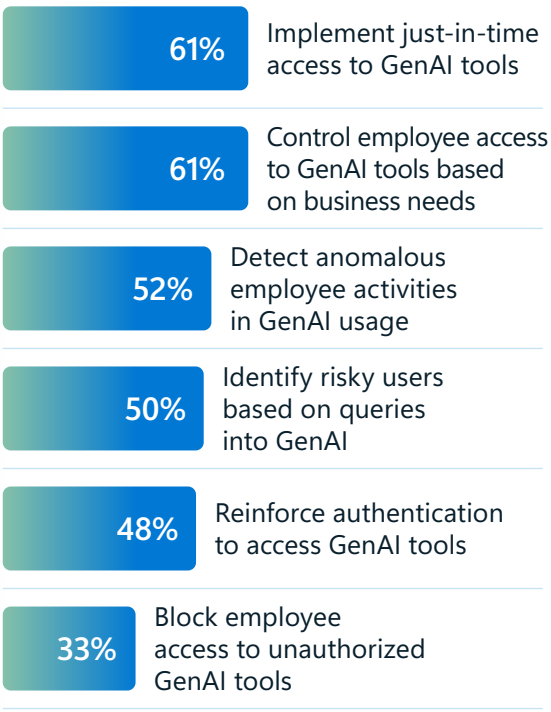
> **"Identity is the new perimeter, like network used to be. Hybrid or remote work has been a catalyst to pushing that, so that's where the bad actors are going."**
>
> CISO, Legal & Professional Services

AI at work—the next frontier for identity and network access security

Generative AI (GenAI) is transforming enterprise operations, promising unprecedented productivity and efficiency. According to the 2024 Microsoft Work Trend Index, 75% of knowledge workers use AI at work today, with 46% starting in the last six months. Our research shows that **84% of identity and network security leaders have seen an increase in AI usage over the past year**, and 48% are willing to implement embedded GenAI skills for productivity benefits.[4]

While organizations recognize the productivity benefits of AI for both employees and security teams, **57% also report an increase in security incidents from AI usage.** Securing AI is a new challenge for identity and network leaders. Although most organizations are working on implementing AI controls, 60% have not yet started. Those that have are focusing on just-in-time access for AI apps (61%) and controlling employee access to AI apps based on business needs (61%).

Identity and network access controls in place around employee GenAI usage



"We're using GenAI a lot. We have chosen to selectively implement some licenses from a few different providers. And we're working on models within one of our security tools to govern that. But meaningful controls to limit AI is hard to do right now, but it really is much needed investment."

CISO, Legal & Professional Services

4. "2024 Microsoft Work Trend Index." Microsoft and LinkedIn.

2

Expanding attack surface and tool proliferation

Despite security teams' efforts, incidents and breaches remain widespread. To address vulnerabilities and gain better visibility, organizations have accumulated numerous access management solutions across various security teams, with mixed results on their security posture.

94%

Experienced an identity or network access incident in the past 12 months

26%

of incidents resulted in a breach or have direct business impact

5 Identity access solutions from **3** Vendors on average

4 Network access solutions from **3** Vendors on average

79%

of those with 6+ solutions say significant breaches have increased in past year

(vs. 45% of those with <6)

Organizations are overwhelmed with increasing and more sophisticated attacks

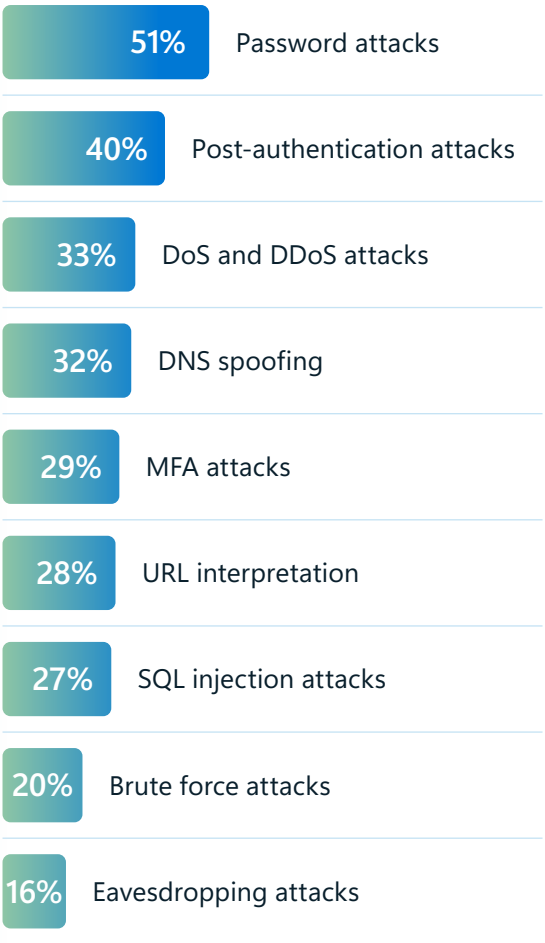
Nearly all organizations (94%) have recently faced access management security incidents, with a quarter leading to breaches that directly impact business, disrupt operations, and pose significant financial and reputational risks.

> **"We've had financial hits—fake invoices that we've paid, fines in certain countries for our lack of role-based access control, and more."**
>
> CISO, Legal & Professional Services

"One incident we had, an outside actor got access onto a server, and, from a kernel of information, they were able to execute commands and do account enumeration on there."

Global IT Operations Manager
Chemical Manufacturing

Identity and network incidents or attacks organizations have experienced in the past 12 months

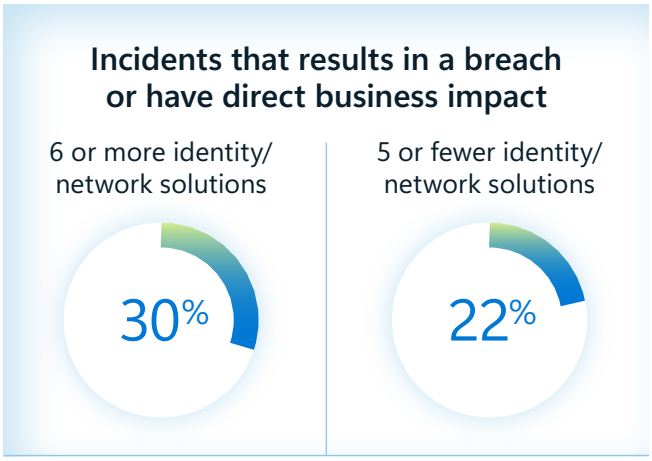


Organizations are accumulating tools—with mixed results on their security posture

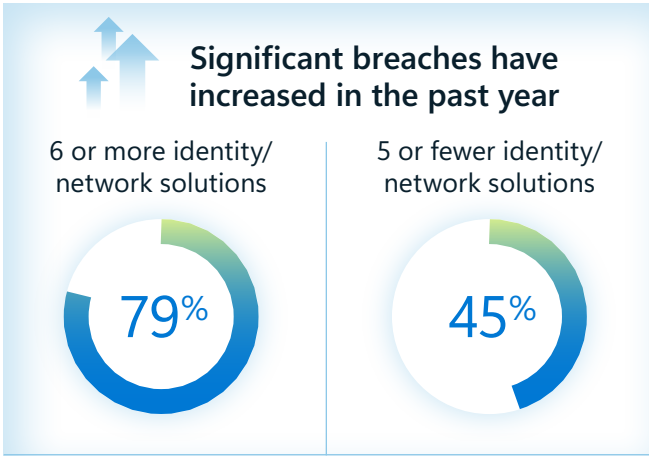
Most organizations use an average of 5 identity solutions and at least 4 network solutions, which are part of a larger security stack. These solutions often come from multiple vendors—typically 3 for identity and 3 for network access. However, using so many solutions hinders cross-team collaboration needed to prevent cyberattacks. In fact, organizations with fewer identity and network tools experience fewer breaches and direct business impacts. This shows that sometimes, less is more.

> **"I need to not have 6 panes of glass that people have to look at. This needs to be streamlined and well-structured. I need to keep all of my IT groups at the various sites using the same tools in the same way."**
>
> Global IT Operations Manager, Chemical Manufacturing

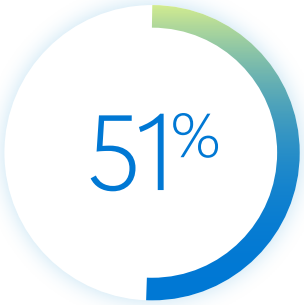
Incidents that results in a breach or have direct business impact



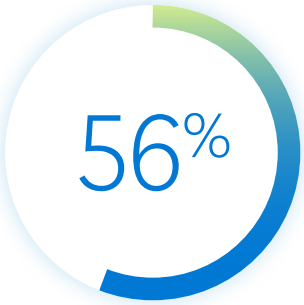
Significant breaches have increased in the past year



Organizations often feel compelled to maintain multiple solutions because they don't believe a single solution can meet all their needs. Despite the complexities, many continue to keep identity and network silos and expect to use even more solutions in the future due to legacy app requirements, mergers and acquisitions, and technological changes. With so many solutions spread across teams, communication and collaboration can suffer, ultimately compromising the organization's security.



Planning to expand the number of **identity** access solutions



Planning to expand the number of **network** access solutions

> **"I want to mature a platform. I don't want a dozen vendors, but a lot of times we feel like we have to go with best in breed because the market reality may not be there yet."**
>
> CISO, Legal & Professional Services

> **"The most scarce resource I've got is the time and attention of my people, and if they're thinking about how to get different solutions to talk to another, that's taking them away from other important tasks."**
>
> Global IT Operations Manager
> Chemical Manufacturing

3

Breaking silos between identity and network

Given the challenges organizations face, effective collaboration between identity and network teams is crucial for managing today's complex threat landscape. Organizations aim for consolidation to enhance collaboration.

4

Different teams, on average, are managing and securing employee access across identity and network

98%

Believe closer collaboration between teams would improve security and organization efficiency

70%

Say consolidating identity and network access solutions would improve teams' efficiency

96%

Prefer to have an integrated identity and network access management approach

Benefits of closer collaboration between identity and network teams

While 30% report exceptional collaboration and 57% report strong collaboration between teams, most organizations still divide security responsibilities across four or more teams.

4 Different teams on average are managing and securing employee access across identity and network

"The identity team is broken into 3 groups. There's a governance group. There's a privileged access group, and there's a provisioning group. On the network side it's part of our overall cybersecurity operations team. So, we have the incident response team, which is separate. And then I have a network team."

EVP & CISO, Financial Services & Banking

This separation often fractures communication and information sharing, leading to time and resources loss, as well as exploited vulnerabilities.

"One employee was leading and could have collaborated with others to bring a solution but didn't and now we've got a big security vulnerability. Bad stuff happens when we're not working together towards the goal, and good things can happen when we do."

Global IT Operations Manager, Chemical Manufacturing

Nearly all (98%) agree that closer collaboration would enhance both security and organizational efficiency. By sharing insights and data, organizations could also reduce the number of solutions they use.

The road towards tool unification

70% of leaders say that consolidating identity management and network access security solutions would improve their teams' efficiency.

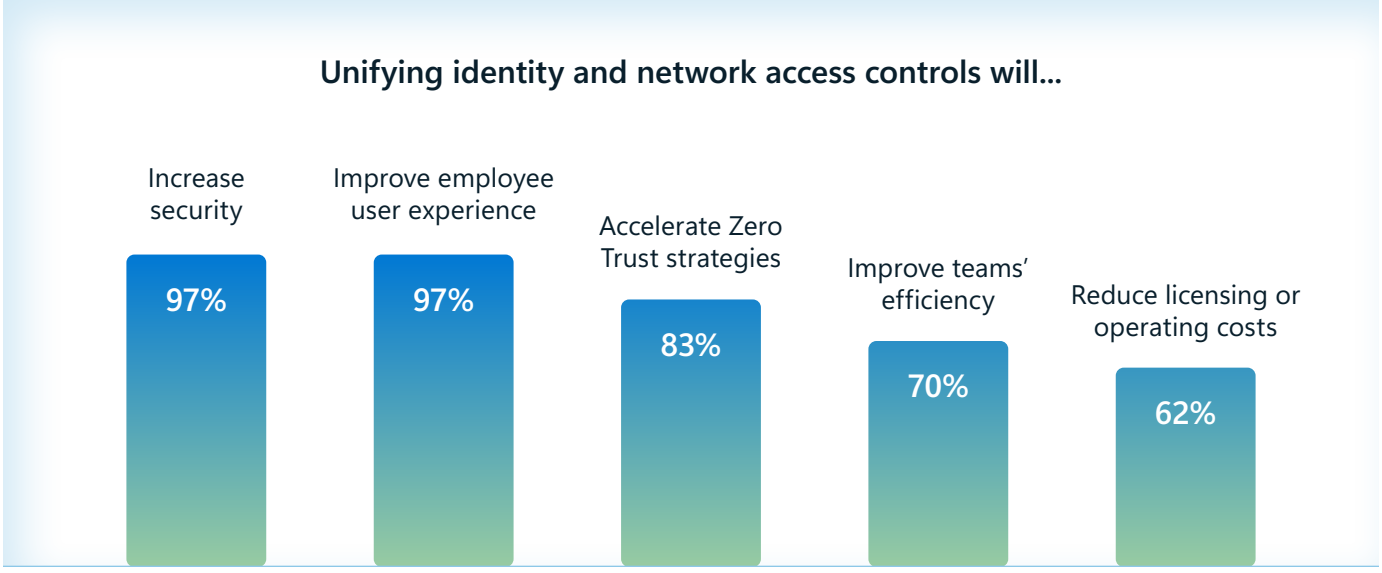
> **"I really do think complexity is the enemy. With a unified solution, my employees could collaborate and it would facilitate them learning a little bit more about what the other person is doing. And it is all within the platform. You can light up a little bit more permissions for each person to poke into other's territory a little bit. And I think I can do more with less people in a consolidated way."**
>
> Global IT Operations Manager, Chemical Manufacturing

By unifying access controls across identities and network, they believe it would increase security (97%) and accelerate Zero Trust strategies (83%).

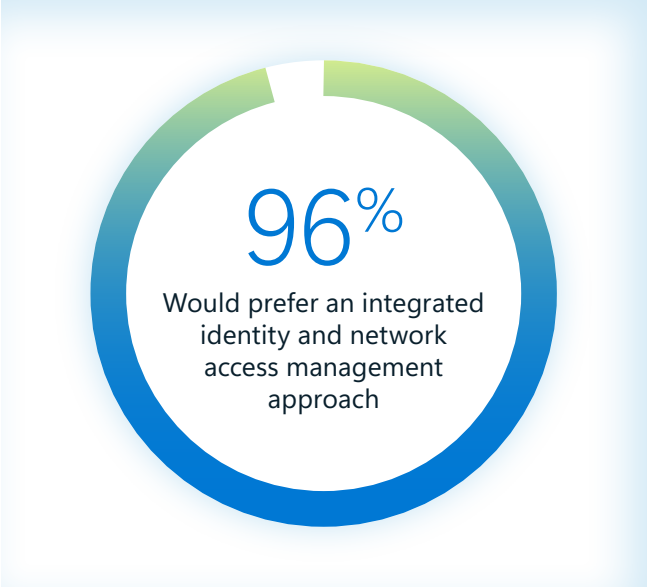
Consolidation is also seen as beneficial for reducing licensing and operational costs (62%) and improving user experience (97%).

> **"We have it in our roadmap to look at where we can have platform consolidation. There's a lot of complexity. And I think that one of the criteria for our 2025 planning is looking at the interoperability of the platform and where we see disconnects."**
>
> EVP & CISO, Financial Services & Banking

> **"A secondary goal [for consolidating], but still an important one is cost. Just negotiating power of buying 5 products from one platform hopefully will reduce the sprawl of having to go to 5 different vendors."**
>
> EVP & CISO, Financial Services & Banking



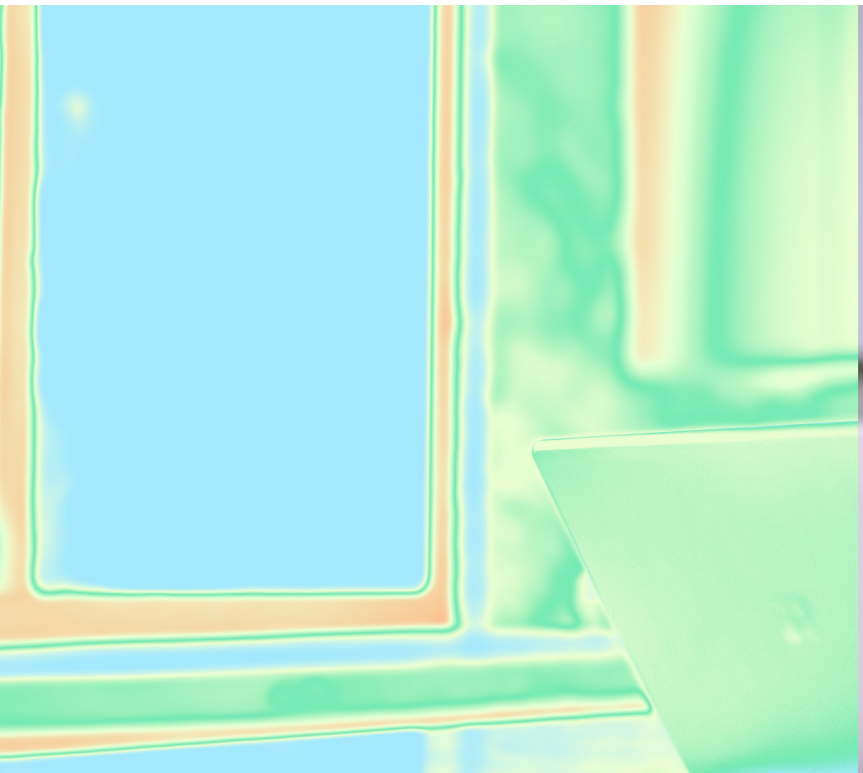
Ultimately, leaders want to consolidate and improve collaboration—96% of leaders say that they would prefer to have a comprehensive and integrated approach versus multiple standalone solutions.



> **"We're going to consolidate whenever possible, but it's hard to consolidate these things. When you're trying to consolidate the solutions, not everything lines up. Some hard decisions have to be made at the end of the day."**
>
> Global IT Operations Manager, Chemical Manufacturing

They also know it'll take time to get there. While 43% are "somewhat likely," only 25% are "very likely" to consolidate in the future, indicating that organizations will need help along their journey to make consolidation a reality.

Read on for how your organization can begin the journey towards unification



Final Recommendations

The path forward is clear: organizations must proactively secure identity and network access by embracing innovation, integration, and collaboration. By addressing today's pressing security challenges with forward-thinking strategies, leaders can build a foundation that empowers resilience, adaptability, and growth.

1 **Unify identity and network access controls**

Simplify Zero Trust security strategy by breaking silos and implementing consistent access controls across identities, networks, and endpoints for stronger security and better user experience.

2 **Foster greater collaboration between identity and network security teams**

Encourage teams to share overall access responsibility to enhance efficiency and security in an ever-evolving threat landscape.

3 **Reduce complexity and consolidate access solutions**

Consolidate and reduce the number of access solutions to strengthen security posture, enhance collaboration, and potentially reduce costs.

4 **Secure access to AI**

Move past experimentation to transforming your business with AI by ensuring secure access to AI apps. This will help drive growth and reduce risks.

Learn more

Discover how Microsoft Entra can help to secure access for your employees with the Microsoft Entra Suite. Read more on our website.

Research Objectives

The objectives of the research included:

1. Understand workforce evolution, including GenAI use and remote/hybrid work.
2. Gauge organizational reactions to these changes from an identity and network access perspective.

Methodology

The research was conducted in two phases:

Phase 1: A 15-minute quantitative online survey (November 18–27, 2024) among 300 enterprise access management decision-makers.

Questions focused on identity and network access, incidents, trends, and securing AI use.

To meet the screening criteria, access management decision-makers needed to be:

- CISO and adjacent decision-makers (C-2 and above) with authority over Zero Trust Network Access and/or Secure Web Gateway, and/or Identity Governance and Administration, Identity and Management, and/or Identity Verification
- Work at enterprise organizations (1,000+ employees; range of sizes)
- Mix of regulated and non-regulated industries (no education, government, or non-profit)

Phase 2: Four 60-minute web-enabled in-depth interviews (December 17–18, 2024) with CISO decision-makers with authority over access management. These interviews explored the survey results in detail.