

Search the blog

[Best practices Identity and access management Microsoft Entra](#)

9 min read

## 5 ways to secure identity and access for 2024

By [Joy Chik](#), President, Identity & Network Access**January 10, 2024**

AI and machine learning

Multifactor authentication

Microsoft Copilot for Security

Microsoft Entra ID Governance

Microsoft Entra ID Protection

Microsoft Entra Internet Access

Microsoft Entra Permissions Management

Microsoft Entra Private Access

Microsoft Entra Verified ID

Security strategies

The security landscape is changing fast. In 2023, we saw a record-high 30 billion attempted password attacks per month, a 35% increase in demand for cybersecurity experts, and a 23% annual rise in cases processed by the Microsoft Security Response Center and Security Operations Center teams.<sup>1</sup> This increase is due in part to the rise of generative AI and large language models, which bring new opportunities and challenges for security professionals while affecting what we must do to secure access effectively.

Generative AI will empower individuals and organizations to increase productivity and accelerate their work, but these tools can also be susceptible to internal and external risk. Attackers are already using AI to launch, scale, and even automate new and sophisticated cyberattacks, all without writing a single line of code. Machine learning demands have increased as well, leading to an abundance of workload identities across corporate multicloud environments. This makes it more complex for identity and access professionals to secure, permission, and track a growing set of human and machine identities.

Adopting a comprehensive defense-in-depth strategy that spans identity, endpoint, and network can help your organization be better prepared for the opportunities and challenges we face in 2024 and beyond. To confidently [secure identity and access](#) at your organization, here are five areas worth prioritizing in the new year:

1. Empower your workforce with Microsoft Security Copilot.
2. Enforce least privilege access everywhere, including AI apps.
3. Get prepared for more sophisticated attacks.
4. Unify access policies across identity, endpoint, and network security.
5. Control identities and access for multicloud.

Our recommendations come from serving thousands of customers, collaborating with the industry, and continuously protecting the

digital economy from a rapidly evolving threat landscape.

## Microsoft Entra

Learn how unified multicloud identity and network access help you protect and verify identities, manage permissions, and enforce intelligent access policies, all in one place.

[Explore Microsoft Entra](#) >

### Priority 1: Empower your workforce with Microsoft Security Copilot

This year generative AI will become deeply infused into cybersecurity solutions and play a critical role in securing access. Identities, both human and machine, are multiplying at a faster rate than ever—as are identity-based attacks. Sifting through sign-in logs to investigate or remediate identity risks does not scale to the realities of cybersecurity talent shortages when there are more than 4,000 identity attacks per second.<sup>1</sup> To stay ahead of malicious actors, identity professionals need all the help they can get. Here's where [Microsoft Security Copilot](#) can make a big difference at your organization and help cut through today's noisy security landscape. Generative AI can meaningfully augment the talent and ingenuity of your identity experts with automations that work at machine-speed and intelligence.

Based on the latest Work Trend Index, business leaders are empowering workers with AI to increase productivity and help employees with repetitive and low value tasks.<sup>2</sup> Early adopters of Microsoft Security Copilot, our AI companion for cybersecurity teams, have seen a 44% increase in efficiency and 86% increase in quality of work.<sup>3</sup> Identity teams can use natural language prompts in Copilot to reduce time spent on common tasks, such as troubleshooting sign-ins and minimizing gaps in identity lifecycle workflows. It can also strengthen and uplevel expertise in the team with more advanced capabilities like investigating users and sign-ins associated with security incidents while taking immediate corrective action.

To get the most out of your AI investments, identity teams will need to build a consistent habit of using their AI companions. Once your workforce becomes comfortable using these tools, it is time to start building a company prompt library that outlines the specific queries commonly used for various company tasks, projects, and business processes. This will equip all current and future workers with an index of shortcuts that they can use to be productive immediately.

**How to get started:** Check out this Microsoft Learn training on the [fundamentals of generative AI](#), and [subscribe for updates on Microsoft Security Copilot](#) to be the first to hear about new product innovations, the latest generative AI tips, and upcoming events.

### Priority 2: Enforce least privilege access everywhere, including AI apps

One of the most common questions we hear is how to secure access to AI apps—especially those in corporate (sanctioned) and third-party (unsanctioned) environments. Insider risks like data leakage or spoilage can lead to tainted large language models, confidential data being shared in apps that are not monitored, or the creation of rogue user accounts that are easily compromised. The consequences of excessively permissioned users are especially damaging within sanctioned AI apps where users who are incorrectly permissioned can quickly gain access to and manipulate company data that was never meant for them.

Ultimately, organizations must secure their AI applications with the same identity and access governance rules they apply to the rest of their corporate resources. This can be done with an identity governance solution, which lets you define and roll out granular access policies for all your users and company resources, including the generative AI apps your organization decides to adopt. As a result, only the right people will have the right level of access to the right resources. The access lifecycle can be automated at scale through controls like identity verification, entitlement management, lifecycle workflows, access requests, reviews, and expirations.

To enforce least privilege access, make sure that all sanctioned apps and services, including generative AI apps, are managed by your identity and access solution. Then, define or update your access policies with a tool like [Microsoft Entra ID Governance](#) that controls who, when, why, and how long users retain access to company resources. Use lifecycle workflows to automate user access policies so that any time a user's status changes, they still maintain the correct level of access. Where applicable, extend custom governance rules and user experiences to any customer, vendor, contractor, or partner by integrating [Microsoft Entra External ID](#), a customer identity and access management (CIAM) solution. For high-risk actions, require proof of identity in real-time using [Microsoft Entra Verified ID](#). Microsoft Security Copilot also comes with built-in governance policies, tailored specifically for generative AI applications, to prevent misuse.

**How to get started:** Read the guide to [securely govern AI](#) and other business-critical applications in your environment. Make sure your governance strategy abides by [least privilege access principles](#).

## Priority 3: Get prepared for more sophisticated attacks

Not only are known attacks like password spray increasing in intensity, speed, and scale, but new attack techniques are being developed rapidly that pose a serious threat to unprepared teams. Multifactor authentication adds a layer of security, but cybercriminals can still find ways around it. More sophisticated attacks like token theft, cookie replay, and AI-powered phishing campaigns are also becoming more prevalent. Identity teams need to adapt to a new cyberthreat landscape where bad actors can automate the full lifecycle of a threat campaign—all without writing a single line of code.

To stay safe in today's relentless identity threat landscape, we recommend taking a multi-layered approach. Start by implementing phishing-resistant multifactor authentication that is based on cryptography or biometrics such as Windows Hello, FIDO2 security keys, certificate-based authentication, and passkeys (both roaming and device-bound). These methods can help you combat more than 99% of identity attacks as well as advanced phishing and social engineering schemes.<sup>4</sup>

For sophisticated attacks like token theft and cookie replay, have in place a machine learning-powered identity protection tool and Secure Web Gateway (SWG) to detect a wide range of risk signals that flag unusual user behavior. Then use continuous access evaluation (CAE) with token protection features to respond to risk signals in real-time and block, challenge, limit, revoke, or allow user access. For new attacks like one-time password (OTP) bots that take advantage of multifactor authentication fatigue, educate employees about common social engineering tactics and use the Microsoft Authenticator app to suppress sign-in prompts when a multifactor authentication fatigue attack is detected. Finally, for high assurance scenarios, consider using verifiable credentials—digital identity claims from authoritative sources—to quickly verify an individual's credentials and grant least privilege access with confidence.

Customize your policies in the Microsoft Entra admin center to mandate strong, phishing resistant authentication for any scenario, including step up authentication with Microsoft Entra Verified ID. Make sure to implement an identity protection tool like [Microsoft Entra ID Protection](#), which now has token protection capabilities, to detect and flag risky user signals that your risk-based CAE engine can actively respond to. Lastly, secure all internet traffic, including all software as a service (SaaS) apps, with [Microsoft Entra Internet Access](#), an identity-centric SWG that shields users against malicious internet traffic and unsafe content.

**How to get started:** To quick start your defense-in-depth campaign, we've developed [default access policies](#) that make it easy to implement security best practices, such as requiring multifactor authentication for all users. Check out these guides on requiring [phishing-resistant multifactor authentication](#) and planning your [conditional access deployment](#). Finally, read up on our [token protection](#), [continuous access evaluation](#), and [multifactor authentication fatigue suppression](#) capabilities.

## Priority 4: Unify access policies across identity, endpoint, and network security

In most organizations, the identity, endpoint, and network security functions are siloed, with teams using different technologies for managing access. This is problematic because it requires conditional access changes to be made in multiple places, increasing the chance of security holes, redundancies, and inconsistent access policies between teams. Identity, endpoint, and network tools need to be integrated under one policy engine, as neither category alone can protect all access points.

By adopting a [Zero Trust security model](#) that spans identity, endpoint, and network security, you can easily manage and enforce granular access policies in one place. This helps reduce operational complexity and can eliminate gaps in policy coverage. Plus, by enforcing universal conditional access policies from a single location, your policy engine can analyze a more diverse set of signals such as network, identity, endpoint, and application conditions before granting access to any resource—without making any code changes.

Microsoft's Security Service Edge (SSE) solution is identity-aware and is delivering a unique innovation to the SSE category by bringing together identity, endpoint, and network security access policies. The solution includes Microsoft Entra Internet Access, an SWG for safeguarding SaaS apps and internet traffic, as well as [Microsoft Entra Private Access](#), a Zero Trust Network Access (ZTNA) solution for securing access to all applications and resources. When you unify your network and identity access policies, it is easier to secure access and manage your organization's conditional access lifecycle.

**How to get started:** Read these blogs to learn why their identity-aware designs make [Microsoft Entra Internet Access](#) and [Microsoft Entra Private Access](#) unique to the SSE category. To learn about the different use cases and scenarios, configuration prerequisites, and how to enable secure access, go to the [Microsoft Entra admin center](#).

## Priority 5: Control identities and access for multicloud

Today, as multicloud adoption increases, it is harder than ever to gain full visibility over which identities, human or machine, have access to what resources across your various clouds. Plus, with the massive increase in AI-driven workloads, the number of machine identities being used in multicloud environments is quickly rising, outnumbering human identities 10 to 1.<sup>5</sup> Many of these identities are created with excessive permissions and little to no governance, with less than 5% of permissions granted actually used, suggesting that a vast majority of machine identities are not abiding by least privilege access principles. As a result, attackers have shifted their attention to apps, homing in on workload identities as a vulnerable new threat vector. Organizations need a unified control center for managing workload identities and permissions across all their clouds.

Securing access to your multicloud infrastructure across all identity types starts with selecting the methodology that makes sense for your organization. Zero Trust provides an excellent, customizable framework that applies just as well to workload identities as it does to human identities. You can effectively apply these principles with a cloud infrastructure entitlement management (CIEM) platform, which provides deep insights into the permissions granted across your multicloud, how they are used, and the ability to right size those permissions. Extending these controls to your machine identities will require a purpose-built tool for workload identities that uses strong credentials, conditional access policies, anomaly and risk signal monitoring, access reviews, and location restrictions.

Unifying and streamlining the management of your organization's multicloud starts with diagnosing the health of your multicloud infrastructure with [Microsoft Entra Permissions Management](#), which will help you discover, detect, right-size, and govern your organization's multicloud identities. Then, using [Microsoft Entra Workload ID](#), migrate your workload identities to managed identities where possible and apply strong Zero Trust principles and conditional access controls to them.

**How to get started:** Start a [Microsoft Entra Permissions Management free trial](#) to assess the state of your organization's multicloud environment, then take the recommended actions to remediate any access right risks. Also, use Microsoft Entra Workload ID to assign conditional access policies to all of your apps, services, and machine identities based on least privilege principles.

## Our commitment to continued partnership with you

It is our hope that the strategies in this blog help you form an actionable roadmap for securing access at your organization—for everyone, to everything.

But access security is not a one-way street, it is your continuous feedback that enables us to provide truly customer-centric solutions to the identity and access problems we face in 2024 and beyond. We are grateful for the continued partnership and dialogue with you—from day-to-day interactions, to joint deployment planning, to the [direct feedback](#) that informs our strategy. As always, we remain committed to building the products and tools you need to defend your organization throughout 2024 and beyond.

Learn more about [Microsoft Entra](#), or recap the [identity at Microsoft Ignite blog](#).

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 ([@MSFTSecurity](#)) for the latest news and updates on cybersecurity.

---

<sup>1</sup>[Microsoft Digital Defense Report](#), Microsoft. October 2023.

<sup>2</sup>[Work Trend Index Annual Report: Will AI Fix Work?](#) Microsoft. May 9, 2023.

<sup>3</sup>[Microsoft unveils expansion of AI for security and security for AI at Microsoft Ignite](#), Vasu Jakkal. November 15, 2023.

<sup>4</sup>[How effective is multifactor authentication at deterring cyberattacks?](#) Microsoft.

<sup>5</sup>[2023 State of Cloud Permissions Risks report now published](#), Alex Simons. March 28, 2023.

## Related Posts

A security practitioner works at a computer.

[News](#)

[Endpoint security](#)

[Microsoft Intune](#)

Feb 1

8 min read

**3 new ways the Microsoft Intune Suite offers security, simplification, and savings** > >

The main components of the Microsoft Intune Suite are now generally available. Read about how consolidated endpoint management adds value and functionality for security teams.



[Best practices](#)

[Incident response](#)

[Microsoft Security Experts](#)

Jun 6

6 min read

## [Why a proactive detection and incident response plan is crucial for your organization > >](#)

Matt Suiche of Magnet Forensics talks about top security threats for organizations and strategies for effective incident response.



[News](#)

[Identity and access management](#)

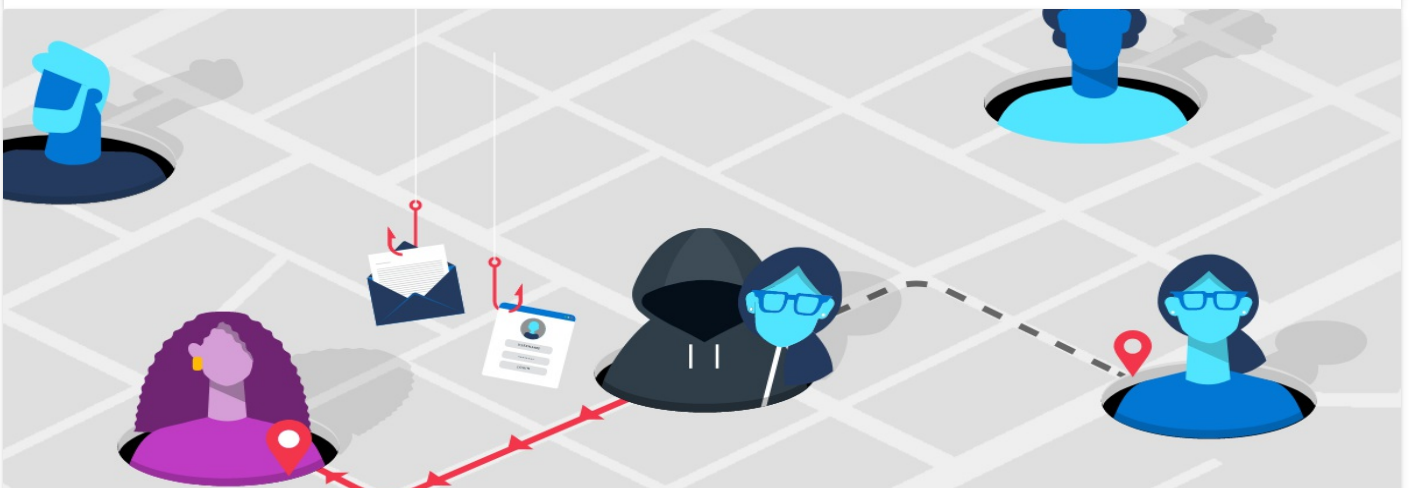
[Microsoft Entra](#)

May 31

5 min read

## [XDR meets IAM: Comprehensive identity threat detection and response with Microsoft > >](#)

Identity-based attacks are on the rise, making identity protection more important than ever. Explore our blog post to learn how Microsoft's Identity Threat Detection and Response can help.





[News](#)

[Email security](#)

**May 19**

**3 min read**

## [Cyber Signals: Shifting tactics fuel surge in business email compromise > >](#)

Business email operators seek to exploit the daily sea of email traffic to lure victims into providing financial and other sensitive business information.

## 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](#)

[Sitemap](#) [Contact Microsoft](#) [Privacy](#) [Terms of use](#) [Trademarks](#) [Safety & eco](#) [Recycling](#) [About our ads](#) [© Microsoft 2024](#)