News Identity and access management Microsoft Entra
5 min read

XDR meets IAM: Comprehensive identity threat detection and response with Microsoft

By Rob Lefferts, Corporate Vice President, Microsoft Threat Protection
Alex Weinert, Vice President, Identity Security

May 31, 2023

AI and machine learning
Multifactor authentication
Security operations
SIEM and XDR
Threat trends
Zero Trust
Security strategies

Identity has become the corporate security perimeter. The average organization used 130 different cloud applications in 2022. That's up 18 percent from 2021 alone.[1] And as organizations continue to embrace digital transformation and enable remote work, they look to identity and access management solutions to ensure that the right people have access to the files, data, and apps they need to do their job without putting those same resources at risk.

As you might imagine, the more identities become integral to how we work, the more they become a target. With just a single compromised account, attackers can quickly bypass existing security protocols and move laterally to increasingly sensitive accounts or resources. Privilege misuse and credential compromise have been two of the most common and damaging attack vectors organizations face, but identity threats are becoming increasingly sophisticated. Cybercriminals have evolved from brute force and password spray tactics to targeting the underlying identity infrastructure in an effort to slip through even the smallest gaps in protection.

Beyond the complexity of these attacks is their sheer volume. It's estimated that more than 80 percent of breaches can be attributed to identity-based attacks, and as more and more cybercrime groups join nation-state actors in executing these types of attacks, that number is only going to grow.[2] To counter these ever-growing identity threats, a new security category has emerged: identity threat detection and response (ITDR).

What is ITDR?

At Microsoft, we see ITDR as an integrated partnership between two historically separate, but critically important, disciplines: identity and access management (IAM) and extended detection and response (XDR).

IAM is a foundational element of any organization's security strategy, providing a baseline for identity security and helping IT departments control what company resources users can and cannot access. By using IAM best practices such as strong

authentication, Conditional Access, and identity governance, organizations can reduce their overall attack surface area while also providing the information and context needed to detect breaches.

XDR solutions are designed to deliver a holistic, simplified, and efficient approach to protect organizations against advanced attacks. These solutions correlate identity signals with telemetry from other domains like endpoints, cloud applications, and collaboration tools, giving security operations center (SOC) teams a more complete view of the cyberattack kill chain. With this enhanced visibility, they can more effectively investigate threats and provide automated remediation across multiple domains using vast sets of intelligence and built-in AI.

IAM and XDR each provide immense benefits to organizations, but when working together in concert, they provide a robust and comprehensive ITDR solution.

Whether you are just starting on your ITDR journey or are already well on your way, Microsoft can help. In this blog post, we'll talk through the critical areas of ITDR and bring insights from our leadership in both identity and security.

Prevent identity attacks before they happen with secure adaptive access

The best-case scenario in any attack is that the bad actors are stopped before they can breach your security. When working with customers, we recommend they implement granular Conditional Access policies as a powerful first step in thwarting cybercriminals and keeping their organization safe.

Multifactor authentication, for instance, has been shown to reduce the risk of compromise from identity attacks by 99.9 percent. This is one of the most important steps and organization can take. Attackers are constantly evolving their tactics, looking for the smallest crack they can exploit, whether that be a human or workload identity they can compromise or misconfigured policies and identity infrastructure that let them gain even more control. That's why we recommend you also use Conditional Access policies to protect non-human identities, whether applications, services, or containers. It's critical to create more secure access policies and manage the lifecycles of different workload identities to prevent an attack.

IT and identity practitioners need to analyze relevant risk signals from across their unique landscape and enforce universal Conditional Access policies in real time. The deep integration of our IAM and XDR platforms helps organizations do just that. Leveraging insights from the more than 65 trillion signals daily across Microsoft's ecosystem, our identity protection capabilities detect things like atypical travel, unfamiliar sign-in properties, and leaked credentials. These capabilities then assign each sign-in attempt a risk score, which in turn can trigger pre-defined remediation efforts or block access entirely until an administrator can review.

Detect advanced attacks with threat-level intelligence.

A robust identity posture is the first step toward identity security, helping to thwart the majority of attacks. Effective breach detection and response completes the story. Ever-evolving attack strategies and the impact of human error from multifactor authentication fatigue or social engineering attacks mean we must always "assume breach." A recent survey found that 76 percent of businesses expect a successful attack to be executed within the next 12 months, highlighting why it is imperative to detect a breach quickly and accurately.[3] To do this, you need powerful detections both at the identity level and across the entire cyber kill chain.

Our customers benefit from robust identity detections out of the box, each prioritized by potential impact and augmented with additional signals and insights into the latest attack strategies. By ingesting signals from on-premises Active Directory, Microsoft Azure Active Directory, and other third-party identity providers as well as the underlying identity infrastructure, like Active Directory Federation Services and Active Directory Certificate Services, SOC teams gain a comprehensive view of their identity landscape, user activities, and risk.

We help you harness the power of our best-of-breed identity detections by integrating our identity security capabilities directly into our XDR platform so SOC teams can see identity alerts and data within the context of broader security incidents. By correlating identity data with signals from across other security domains, not only is each individual alert increasingly more accurate but analysts also gain unprecedented insight into the entirety of an attack and its progression.

Learn more about how to empower your SOC team to spot even the most advanced identity attacks.

Respond and remediate attacks faster with automatic attack disruption

Detecting a breach and remediating an attack are two very different things. The final piece of a successful ITDR strategy is the ability to stop in-progress attacks and limit lateral movement. At Microsoft, we have infused AI and machine learning into our security capabilities to help empower the SOC with intelligent automation that can disrupt attacks at machine speed.

Analysts can confidently automate workflows and remediation tactics thanks to the high level of accuracy our correlated incidents provide. This effectively shifts the response time from hours or days to minutes or seconds. When a breach occurs, every second matters, and costs can soar to 80 percent higher when security AI and automation aren't fully deployed.[4]

Human efficiency is also critical, so we have designed our portals with the needs of each unique persona in mind while enabling a seamless flow of information and workflow processes. By prioritizing everything from alerts to configurations and posture management, users can focus better on what is most important to them.

Find out how to stop advanced attacks at machine speed.

Get started today

As the sophistication and prevalence of identity-based attacks continue to grow, identity protection and ITDR are becoming increasingly critical to modern cybersecurity. Partner with a proven leader in both identity and security to streamline your identity protection and deploy a successful ITDR strategy.

Learn more about Microsoft's Identity Threat Detection and Response solution.

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 Twitter (@MSFTSecurity) for the latest news and updates on cybersecurity.

---

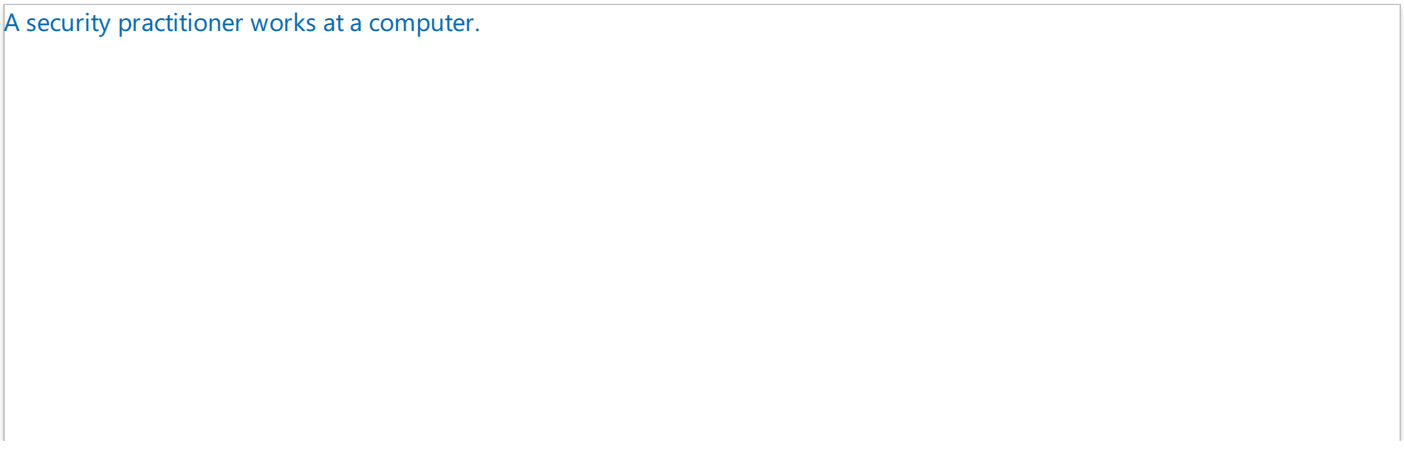
[1] 2023 State of SaaSOps study, BetterCloud. 2023.

[2] Verizon Data Breach Investigation Report, Verizon. 2022.

[3] Cyber Risk Index (CRI), Trend Micro. 2023.

[4] Cost of a Data Breach Report, Ponemon Institute. 2021.

Related Posts

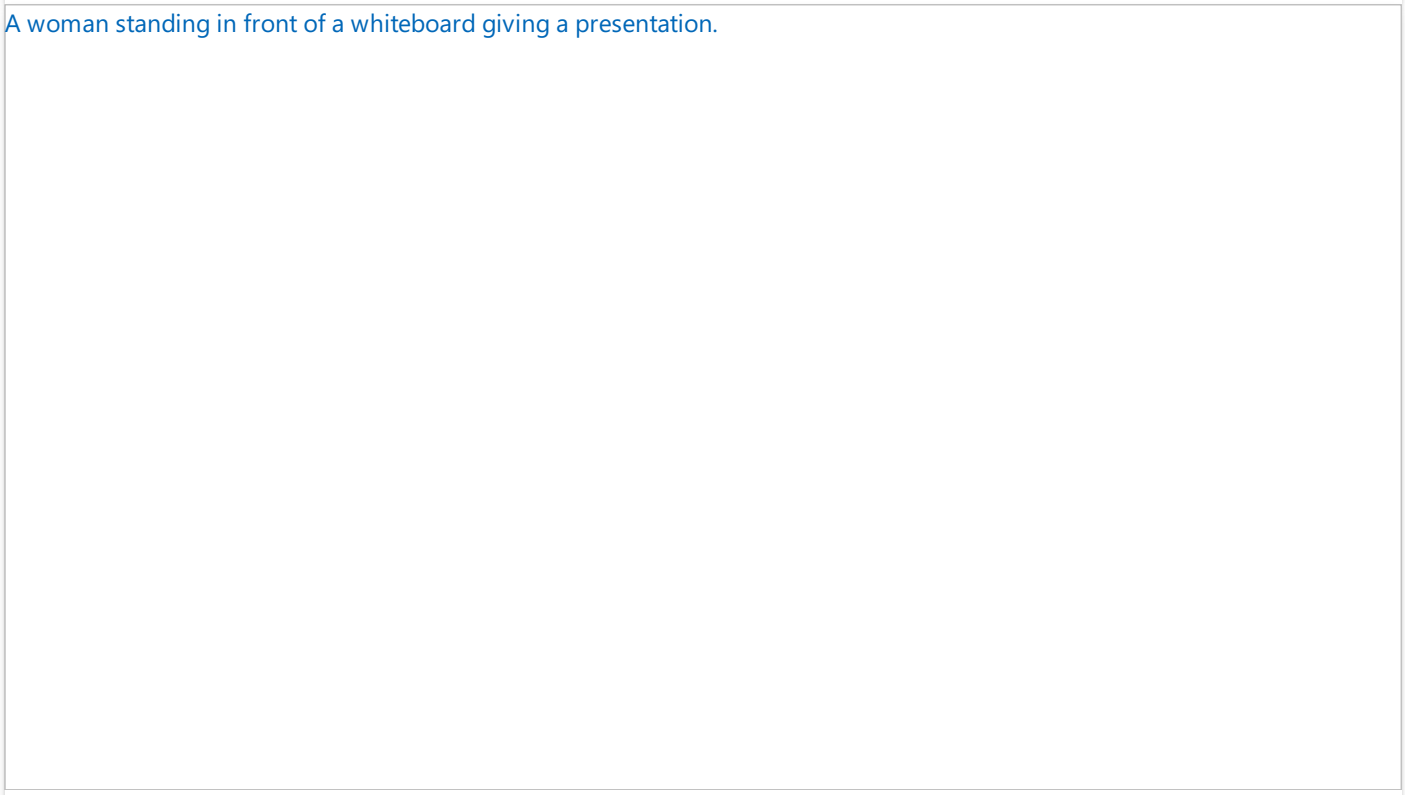


News
Endpoint security
Microsoft Intune

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.


A woman standing in front of a whiteboard giving a presentation.

Best practices
Identity and access management
Microsoft Entra

Jan 10
9 min read

5 ways to secure identity and access for 2024

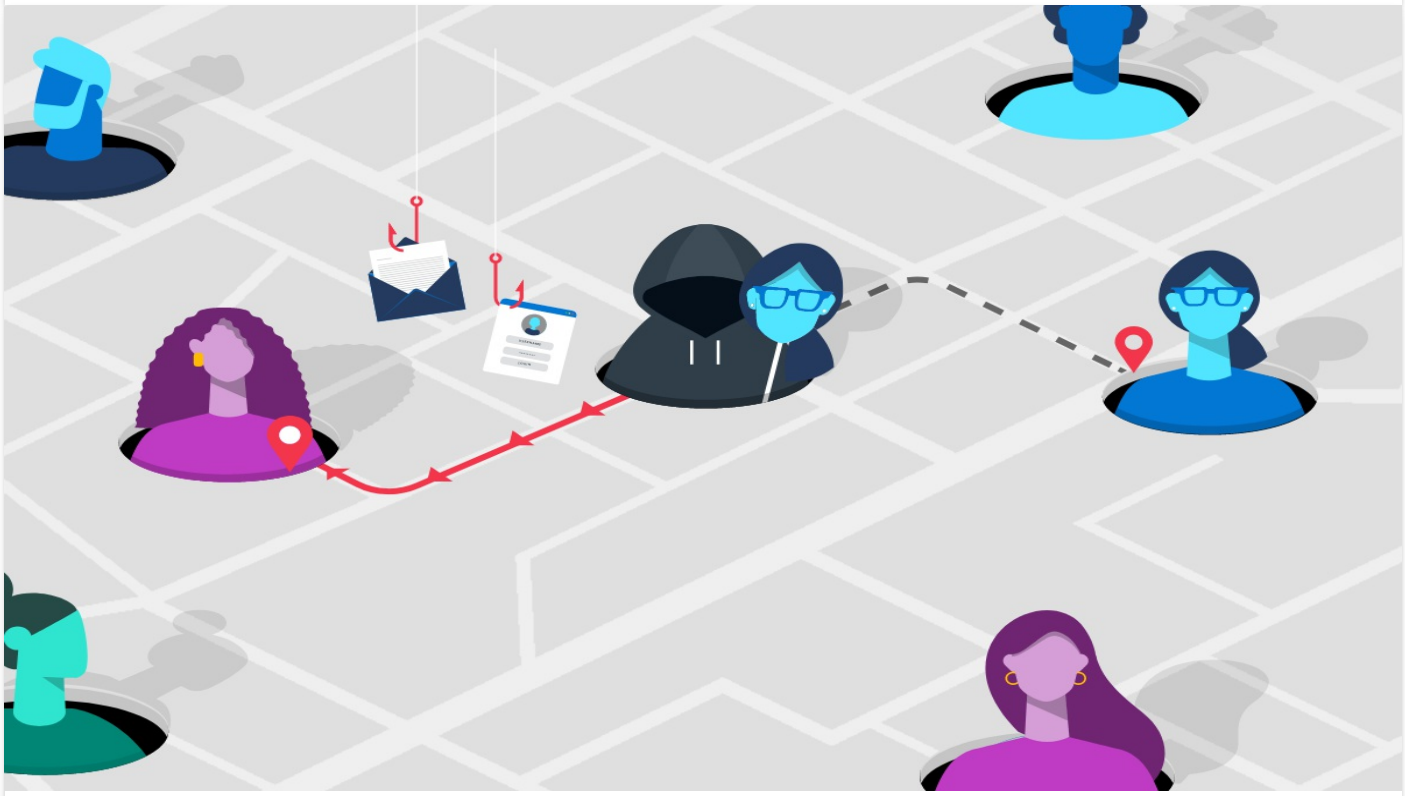
To confidently secure identity and access at your organization, here are five areas Microsoft recommends prioritizing in the new year.

[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]
[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

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