News Security operations Microsoft Defender

7 min read

Get end-to-end protection with Microsoft's unified security operations platform, now in public preview

By Rob Lefferts, Corporate Vice President, Microsoft Threat Protection

April 3, 2024

AI and machine learning SIEM and XDR Microsoft Copilot for Security more

Today, I am excited to announce the public preview of our unified security operations platform. When we announced a limited preview in November 2023, it was one of the first security operations center platforms that brought together the full capabilities of an industry-leading cloud-native security information and event management (SIEM), comprehensive extended detection and response (XDR), and generative AI built specifically for cybersecurity. This powerful combination of capabilities delivers a truly unified analyst experience in the security operations center (SOC).

And last month at Microsoft Secure, we added unified exposure management capabilities that provide continuous, proactive end-to-end visibility of assets and cyberattack paths. Together, these fully integrated, comprehensive capabilities give security leaders and SOC teams what they need to manage cyberthreats across their organization—from prevention to detection and response.

After gaining insights from the initial customer feedback, we are excited to expand the platform's availability to public preview. Customers with a single Microsoft Sentinel workspace and at least one Defender XDR workload deployed can start enjoying the benefits of a unified experience, in a production environment, now. Onboarding a Microsoft Sentinel workspace only takes a few minutes, and customers can continue to use their Microsoft Sentinel in Azure. Need another reason to get started today? Microsoft Sentinel customers using Microsoft Copilot for Security can now leverage the embedded experience in the Defender portal, helping them to level up their security practice further.

Unified security operations platform

The new platform brings together the capabilities of XDR and SIEM. Learn how to onboard your Microsoft Sentinel workspace to the Microsoft Defender portal.

Get started today >

Knock down security silos and drive better security outcomes

SOCs are buried under mountains of alerts, security signals, and initiatives. Analysts are spending too much time sifting through low-level alerts, jumping between portals, and navigating complex workflows to understand what happened, how to resolve it, and how to prevent it from happening again. This leaves little time for analysts to focus on high-value tasks—like remediating multistage incidents fully or even decreasing the likelihood of future attacks by reducing the attack surface. With an ever-growing gap in supply and demand of talent—in fact, there are only enough cybersecurity professionals to meet 82% of the United States demand—something must change.[1]

At the heart of this challenge is siloed data—SOCs have too much security data stored in too many places and most SOC teams lack the tools to effectively bring it all together, normalize it, apply advanced analytics, enrich with threat intelligence, and act on the insights across the entire digital estate. This is why we built the security operations platform—by bringing together the full capabilities of SIEM, XDR, exposure management, generative AI, and threat intelligence together, security teams will be empowered with unified, comprehensive features that work across use cases, not security tool siloes.

The new analyst experience is built to create a more intuitive workflow for the SOC, with unified views of incidents, exposure, threat intelligence, assets, and security reporting. This is a true single pane of glass for security across your entire digital estate. Beyond delivering a single experience, unifying these features all on one platform delivers more robust capabilities across the entire cyberattack lifecycle.

"Security teams need a single pane of glass to manage today's IT environments. Long gone are the days when teams could operate in silos and protect their environments. With today's announcement Microsoft is moving another step forward in helping businesses protect their systems, customers and reputations," said Chris Kissel, IDC Research Vice President, Security and Trust. "Microsoft combining the full capabilities of an industry-leading cloud-native SIEM and XDR with the first generative AI built specifically for cybersecurity is a game changer for the industry."

Capabilities across Microsoft Sentinel and Microsoft Defender XDR products are now extending, making both Microsoft Sentinel and Defender XDR more valuable. XDR customers can now enjoy more flexibility in their reporting, their ability to deploy automations, and greater insight across data sources. With the new ability to run custom security orchestration, automation, and response (SOAR) playbooks on an incident provided by Microsoft Sentinel, Defender XDR customers can reduce repetitive processes and further optimize the SOC. They can also now hunt across their XDR and SIEM data in one place. Further, XDR detection and incident creation will now open to data from SIEM. SIEM customers can now get more out of the box value, improving their ability to focus on the tasks at hand and gain more proactive protection against threats, freeing them to spend more time on novel threats and the unique needs of their environment.

Prevent breaches with end-to-end visibility of your attack surface

During the past 10 years, the enterprise attack surfaces have expanded exponentially with the adoption of cloud services, bring-your-own device, increasingly complex supply chains, Internet of Things (IoT), and more. Approximately 98% of attacks can be prevented with basic cybersecurity hygiene, highlighting the importance of hardening all systems.[2] Security silos make it more difficult and time-consuming to uncover, prioritize, and eliminate exposures.

Fortunately, the Microsoft Security Exposure Management solution, built right into the new unified platform experience, consolidates silos into a contextual and risk-based view. Within the unified platform, security teams gain comprehensive visibility across a myriad of exposures, including software vulnerabilities, control misconfigurations, overprivileged access, and evolving threats leading to sensitive data exposure. Organizations can leverage a single source of truth with unified exposure insights to proactively manage their asset risk across the entire digital estate. In addition, attack path modeling helps security professionals of all skill levels predict the potential steps adversaries may take to infiltrate your critical assets and reach your sensitive data.

Shut down in-progress attacks with automatic attack disruption

In today's threat landscape, where multistage attacks are the new normal, automation is no longer optional, but a necessity. We've seen entire ransomware campaigns that only needed two hours to complete, with attackers moving laterally in as little as five minutes after initial compromise—the median time for attackers to access sensitive data is only 72 minutes.[3] This capability is essential to counter the rapid, persistent attack methods like an AKIRA ransomware attack. Even the best security teams need to take breaks and with mere seconds separating thousands versus millions of dollars spent on an attack, the speed of response becomes critical.

This platform harnesses the power of XDR and AI to disrupt advanced attacks like ransomware, business email compromise, and adversary-in-the-middle attacks at machine speed with automatic attack disruption, a game-changing technology for the SOC that remains exclusive to Microsoft Security. Attack disruption is a powerful, out-of-the-box capability that automatically stops the progression and limits the impact of the most sophisticated attacks in near real-time. By stopping the attack progression, precious time is given back to the SOC to triage and resolve the incident.

Attack disruption works by taking a wide breadth of signals across endpoints and IoT, hybrid identities, email and collaboration tools, software as a service (SaaS) apps, data, and cloud workloads and applying AI-driven, researcher-backed analytics to detect and disrupt in-progress attacks with 99% confidence.[3] With more than 78 trillion signals fueling our AI and machine learning models, we can rapidly detect and disrupt prominent attacks like ransomware in **only three minutes,** saving thousands of devices from encryption and recovery costs. Using our unique ability to recognize the intention of the attacker, meaning accurately predict their next move, Microsoft Defender XDR takes an automated response such as disabling a user account or isolating a device from connecting to any other resource in the network.

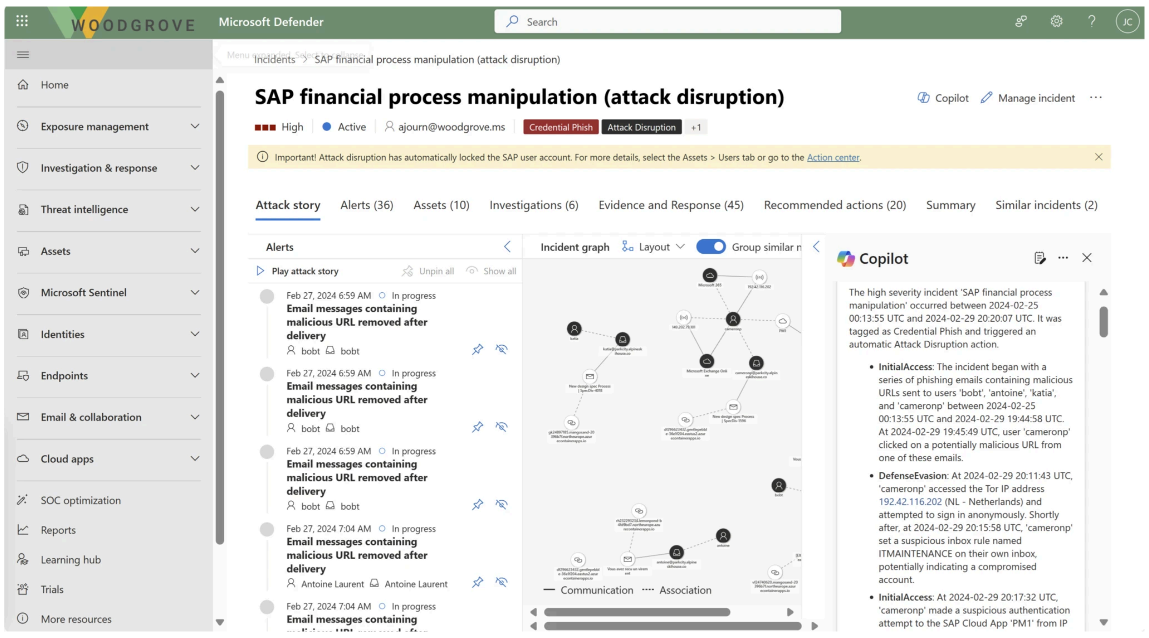
Built on the attack disruption technology in our Defender XDR solution, our unified platform now extends this dynamic protection to new solutions through Microsoft Sentinel—starting with SAP. When an SAP account attack is detected, our platform will **automatically respond to cut off access in SAP.** This means unprecedented protection for a platform that houses incredibly sensitive data, making it a prime target for attackers.

Investigate and respond faster

Multiple dashboards and siloed hunting experiences can really slow down the meantime to acknowledge and respond. The effectiveness of the SOC is measured by these critical metrics. Microsoft delivers a single incident queue, equipped with robust out-of-the-box rules, that saves time, reduces alert noise, and improves alert correlation, ultimately delivering a full view of an attack. During our private preview, **customers saw up to an 80% reduction in incidents**, with improved correlation of alerts to incidents across Microsoft Sentinel data sources, accelerating triage and response.[4] Further, unified hunting helps customers to reduce investigation time by eliminating the need to know where data is stored or to run multiple queries on different tables.

We're not stopping at automatic attack disruption and unified incident queues—we're on a mission to uplevel analysts of all experience levels. Microsoft Copilot for Security helps security analysts accelerate their triage with comprehensive incident summaries that map to the MITRE framework, reverse-engineer malware, translate complex code to native language insights, and even complete multistage attack remediation actions with a single click.

Copilot for Security is embedded in the analyst experience, providing analysts with an intuitive, intelligent assistant than can guide response and even create incident reports automatically—saving analysts significant time. Early adopters are seeing their analysts move an average of 22% faster and accelerate time to resolution.[5] Copilot for Security is more than a chatbot—it's a true intelligent assistant built right into their workflow, helping them use their tools better, level up their skills, and get recommendations relevant to their work at hand.



Incidents > SAP financial process manipulation (attack disruption)

SAP financial process manipulation (attack disruption)

High | Active | ajourn@woodgrove.ms | Credential Phish | Attack Disruption | +1

Important! Attack disruption has automatically locked the SAP user account. For more details, select the Assets > Users tab or go to the Action center.

Feb 27, 2024 6:59 AM ○ In progress
Email messages containing malicious URL removed after delivery
bobt bobt

Feb 27, 2024 6:59 AM ○ In progress
Email messages containing malicious URL removed after delivery
bobt bobt

Feb 27, 2024 6:59 AM ○ In progress
Email messages containing malicious URL removed after delivery
bobt bobt

Feb 27, 2024 7:04 AM ○ In progress
Email messages containing malicious URL removed after delivery
Antoine Laurent Antoine Laurent

Feb 27, 2024 7:04 AM ○ In progress
Email messages containing

The high severity incident 'SAP financial process manipulation' occurred between 2024-02-25 00:13:55 UTC and 2024-02-29 20:20:07 UTC. It was tagged as Credential Phish and triggered an automatic Attack Disruption action.

- **InitialAccess**: The incident began with a series of phishing emails containing malicious URLs sent to users 'bobt', 'antoine', 'katia', and 'cameronp' between 2024-02-25 00:13:55 UTC and 2024-02-29 19:44:58 UTC. At 2024-02-29 19:45:49 UTC, user 'cameronp' clicked on a potentially malicious URL from one of these emails.
- **DefenseEvasion**: At 2024-02-29 20:11:43 UTC, 'cameronp' accessed the Tor IP address 192.42.116.202 (NL - Netherlands) and attempted to sign in anonymously. Shortly after, at 2024-02-29 20:15:58 UTC, 'cameronp' set a suspicious inbox rule named ITMAINTENANCE on their own inbox, potentially indicating a compromised account.
- **InitialAccess**: At 2024-02-29 20:17:32 UTC, 'cameronp' made a suspicious authentication attempt to the SAP Cloud App 'PM1' from IP

If you'd like to join the public preview, view the prerequisites and how to connect your Microsoft Sentinel workplace.

Learn more

Learn more about Microsoft SIEM and XDR solutions.

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.

[1] Cybersecurity Supply and Demand Heat Map, CyberSeek. 2024.

[2] Microsoft Digital Defense Report, Microsoft. 2023.

[3] Microsoft Digital Defense Report, Microsoft. 2022.

[4] Microsoft Internal Research.

[5] Microsoft Copilot for Security randomized controlled trial (RCT) with experienced security analysts conducted by Microsoft Office of the Chief Economist, January 2024.

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