Microsoft Security

March 2025

Building a cyberthreat-resilient organization

A crash course in Microsoft Defender XDR and Microsoft Sentinel

Introduction—secure your multiplatform, multicloud organization

Microsoft observes more than 600 million ransomware, phishing, and identity attacks each day. One major theme from our analysis of these attacks is clear: organizations with integrated tools have better visibility and a more holistic defense than those using a diverse portfolio of point solutions. The data, visibility, and organizational silos created by these tools are creating gaps in security and contributing to the overwhelming workload faced by your SOC team.

Analysts are buried under a mountain of manual work—leaving little time for them to focus on high-value, proactive tasks. Every false positive, messaging ping, portal jump, context-searching, and complex workflows navigation increases the time it takes to understand what happened, resolve it, and prevent it from ever happening again. The gaps between tools, security signals, and functional teams (identity security admins, SOC analysts, threat hunters, and network managers, to name a few) makes it difficult to identify and remediate multistage incidents fully or decrease the likelihood of future attacks.

This is why we built the Microsoft unified security operations platform. It brings together the security data, capabilities, and workflows, delivering a true end-to-end experience for preventing, detecting, investigating, and responding to cyberthreats. Our security operations platform combines our global threat intel with all of the capabilities of our SIEM, XDR, cloud security, exposure management and generative AI solutions into a single experience.

In this e-book, we will share how our unified security operations platform can help you knock down silos and better protect your organization across the entire lifecycle of threats.

Table of contents

Chapter 1

Gain clarity and expanded visibility

> "Malicious actors can strike from anywhere in the world. I honestly believe that the visibility possible with Microsoft 365 E5 is a must for any organization, regardless of size."
>
> **Neil Natic**
> Chief Information Officer, Georgia Banking Company

Threat actors thrive off the boundaries created by your technical debt and traditional security tools. They force defenders think in silos—like working through lists of unorganized alerts from multiple sources or only having context in a single domain like identities. Conversely, attackers are thinking in graphs—like how they can chain together multiple vulnerabilities to traverse your network undetected. This makes it extremely difficult for even the best security teams to understand the full scope of an attack when they're working out of multiple portals and having to correlate at least some alerts manually. When only part of the attack kill chain is uncovered, the likelihood of an attacker maintaining a foothold and continuing their attack is at an unreasonable level. To counteract these cyberthreats, your team needs to see across your entire environment, examine a particular event or cyberthreat actor, and make correlations across disparate security data.

The unified security operations platform brings together data and insights from across your multicloud, multiplatform environment to provide your SOC with end-to-end visibility and the tools to dig into alerts, entities, and cyberthreat actors as needed. It's a unified incident experience that streamlines triage and provides a complete view of threats across the entire digital estate.

Multiple data sources, just one portal

Today's organizations run on multiple clouds with employees accessing resources from various locations using a mix of devices. It's made the workplace more flexible and productive, but it's also created many more opportunities for bad actors to gain unauthorized access.

Our platform combines the native signal from Defender XDR—which includes all of the platforms and cloud protected by our Defender suite—with our cloud-native SIEM, Sentinel, into a single portal. Get the depth of signal and incident-correlation of XDR with the flexibility and customization of a SIEM. Sentinel offers more than 300 connectors to platforms such as Microsoft Azure, Google Cloud Platform, AWS, CrowdStrike, Oracle, and SAP. From a single portal, your team can monitor all your devices, cloud apps, and active and inactive identities.

Put cyberthreats in context

A typical SOC is inundated with security data and alerts that don't always identify true security threats. Analysts end up losing valuable time to sifting through false positives or, worse, missing something important. With alerts automatically combined into a list of prioritized incidents, your team will save time and focus on the most important threats. And with Microsoft Security Copilot built-in, analysts can move even faster with incident summaries, code analysis, KQL query generation, and guided response, eliminating historically time-consuming tasks during the investigation and response.

> "The biggest benefit in our eyes is the increased and holistic visibility we get across the entire Campari Group thanks to the fusion of the Defender solutions and Sentinel."
>
> **Andrea Mazzetti**
> Cybersecurity Global IT Manager, Campari Group

Chapter 2

Proactively prevent multidomain cyberattacks

Many of the traditional point solutions used by security teams today are limited to prevention or detection and, sometimes, response capabilities. This makes it hard for organizations to understand and implement policies that can help prevent attacks. Additionally, many were never designed for today's large, distributed and complex environment. As a result, organizations face significant risk exposure security teams just aren't equipped to manage effectively.

If we look at a common type of ransomware attack—we can see how the attacker will work across email, endpoints, identities, network, data stores, and sometimes even the cloud. Gone are the days of commodity ransomware that mostly targeted your endpoints. Today's attacks are targeted and typically focus on getting access to mission critical systems or your most sensitive data.

Protecting your organization in this reality requires a multidomain approach to prevention that focuses on hardening against the attacker's tactics. The unified security operations platform is designed to prevent attacks with multiple pre-breach capabilities, including looking for suspicious activity at each stage outlined by the cyberattack chain and correlating data across endpoints, hybrid identities, email, collaboration tools, cloud apps, cloud workloads, and data to uncover serious cyberthreats. The platform can proactively improve your security risk posture by:

Hardening your defenses with tailored recommendations

Prioritize your prevention efforts across identities, endpoints, email, apps, data and cloud with threat-intel driven insights and Microsoft research-backed best practices.

Monitoring security controls and model potential attack paths

Connect the dots between isolated security findings, providing teams with an attacker's perspective for more effective prioritization and proactively prevent attacks reaching critical assets—such as cloud workloads and data storage.

In the 2023 MITRE Engenuity ATT&CK® Evaluations, Microsoft Defender XDR demonstrated visibility and analytics across all stages of the cyberattack chain.

Chapter 3

Dynamically stop attackers with real-time, defense in-depth protection

While preventing attacks is always the priority, even the best security teams won't be able to fully out-patch every threat actor. Post-breach disruption capabilities are critical to limiting the impact of a breach. Our AI-powered automated attack disruption capabilities provide built-in, self-defense capabilities that dynamically respond to in-progress, hands-on-keyboard attacks. When an intruder is detected, built-in automated response actions in Defender XDR are utilized to isolate compromised assets and suspend users, stopping the attacker in their tracks.

Unlike traditional solutions that periodically scan for known malware and solely rely on endpoint signals, attack disruption uses AI and cross-domain signals to predict an attacker's next move and adapt its response. This means Defender XDR can dynamically block lateral movement early in the kill chain and stop the attacker from progressing.

Think of attack disruption as a series of adaptive playbooks that come built-in and are constantly updated with the latest and greatest threat intel. This autonomous process ensures real-time response to an attack, no matter how busy your security team is.

3 minutes

is the average amount of time it takes to disrupt ransomware attacks[1]

2,000

incidents are disrupted each month[2]

3.5k

disabled user accounts in the last month[2]

100k+

devices saved from an attack in the last six months[2]

[1]Microsoft internal research
[2]Microsoft multicloud risk report

Chapter 4

Streamline investigation and accelerate response

Security teams are using an average of over fourteen[2] security tools to detect and respond to threats—making it hard to correlate alerts into incidents and coordinate response in a timely fashion. The result is analysts are spending significant amounts of time manually filling the gaps left by siloed tools.

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.

Once a cyberattack has been confirmed, the unified platform's investigation and response tools empower analysts to determine what happened and take decisive action quickly. Rather than analysts piecing together insights from unconnected alerts, the platform correlates low-level alerts into a single incident to help analysts focus their time effectively.

Graphs and detailed information about each incident help your SOC understand:

- The timeline of the cyberattack
- Which anomalies and suspicious activities triggered the incident
- How entities involved in the incident are impacted
- What connections were made to other security domains
- How the attacker could use compromised assets to move laterally

When the platform is used with Security Copilot, teams get guidance, recommendations, and explanations in natural language to help them limit the impact of a cyberattack. SOAR capabilities built into Sentinel allow multiple team members to coordinate response activities quickly. And remediation playbooks automate key activities such as isolating malware, disabling compromised accounts, and deploying antivirus capabilities.

Outmaneuver bad actors with advanced threat-hunting capabilities

The cyberthreat landscape is never static. Nation-state actors and cybercriminals of all sizes continuously gain access to new tactics that help them evade detection.

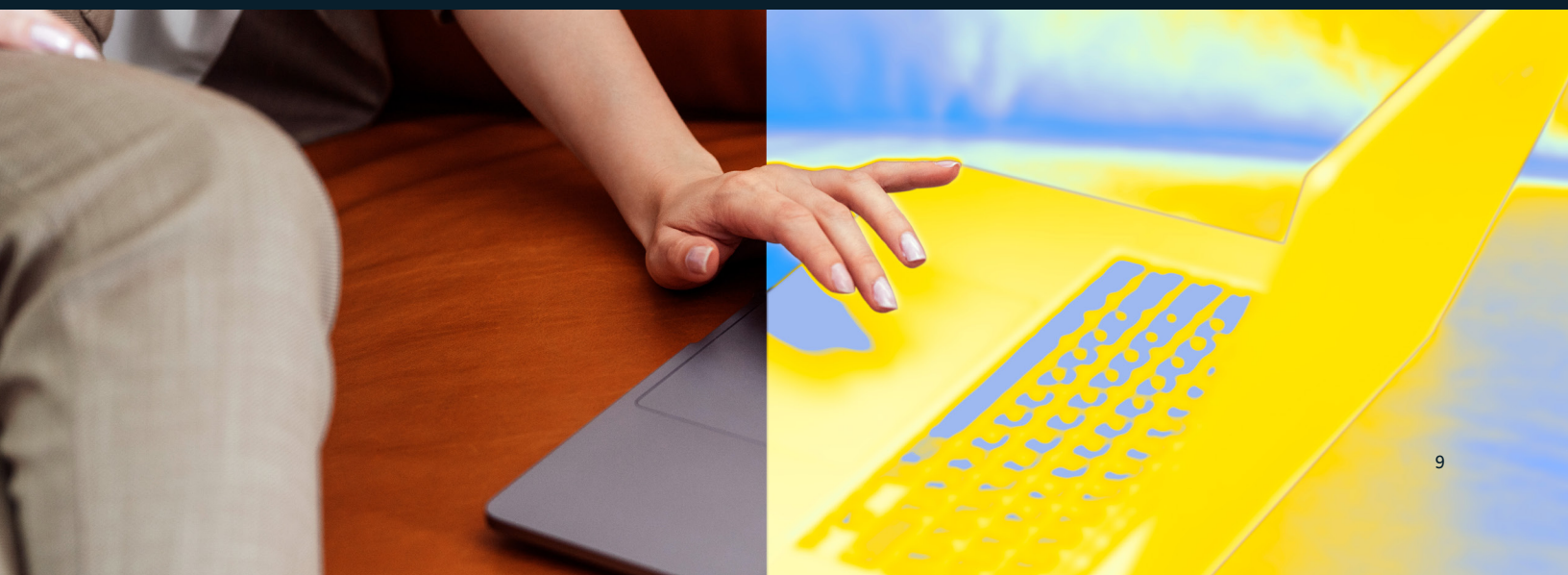
To uncover these stealth cyberthreats, Defender XDR provides advanced hunting, a query-based investigation tool that lets security professionals explore up to 30 days of raw data. Microsoft teams can root out hidden adversaries using two modes:

- With **guided mode,** prebuilt queries make it easy to start looking for signs of a new cyberattack without writing any code.
- In **advanced mode,** teams create custom queries using Kusto Query Language (KQL) to further refine their search based on their expertise and knowledge of the organization.

Analysts who don't know KQL but need to develop a custom query can ask Security Copilot to do it for them. Security Copilot can turn a natural-language request into a custom query using the advanced hunting data schema.

Teams can also build custom detection rules that automatically check for and respond to findings such as suspected breach activity or misconfigured machines.

> "We consider it a game-changer that Defender XDR combines signals for threat hunting because it connects data from the identity and endpoint perspectives to pinpoint truly malicious events."
>
> **Krzysztof Kuźnik**
> Product Owner, ING



Chapter 5

Supercharge SOC productivity with GenAI

Supercharge SOC productivity

The integrated analyst experience helps improve mean time-to-respond (MTTR) on multistage attacks that cross identities, endpoints, apps, email and documents, workloads, IoT, on-premises and cloud infrastructure, and more. And with the addition of Security Copilot, security teams can optimize their time and impact.

Detect hidden patterns and behaviors

Security Copilot uses the end-to-end visibility of the unified platform to surface cyberthreats in real-time.

Build up security talent

Top security tradecraft, delivered through natural language, makes advanced investigation techniques available to every member of the security team, even junior analysts.

Quickly make sense of complex situations

Security-trained generative AI models transform cyberthreat data into insights delivered in natural language, saving teams precious time when every minute counts.

Accelerate investigations

Security Copilot delivers clear recommendations and deep context relating to any security event, including internal data about the environment and external information about known threats.

Get comprehensive reports

Security Copilot creates custom reports in seconds, making it easier for security teams to communicate efficiently with all their stakeholders.

Generative AI is already proving to be a game-changer in security, amplifying team effectiveness and accelerating investigation and response. Because this new technology can interpret natural human language and synthesize complex data into easy-to-digest information, it gives security teams the tools they need to take down threats faster and even predict future cyberattacks.

Security Copilot helps organizations defend at machine speed and scale, empowering security professionals to respond to cyberthreats in minutes instead of hours or days.

Already, teams participating in the Security Copilot early access program are seeing positive results:

Across all tasks, participants were

44% more accurate and **26%** faster.[3]

86% reported that Security Copilot helped them improve the quality of their work.[3]

83% stated that Security Copilot reduced the effort needed to complete the task.[3]

86% said that Security Copilot made them more productive.[3]

90% expressed their desire to use Security Copilot next time they do the same task.[3]

"We are excited about what we have seen from Security Copilot. These capabilities can help companies stay ahead of future threats."

Jeremy J. Hyland
Director of Cyber Defense, Dow Inc.

[3]Microsoft Security Copilot randomized contolled trial conducted by Microsoft Office of the Chief Economist, November 2023

Chapter 6

Improve visibility into cloud-based threats and secure applications

Cloud computing has revolutionized the way organizations develop and deploy applications, offering increased scalability, agility, and innovation. However, this rapid shift also poses significant security challenges. Organizations want to embrace the benefits of the cloud, without compromising on the highest levels of security, resilience or performance. Microsoft Defender for Cloud is a full cloud-native application platform (CNAPP) delivering comprehensive security and compliance from code-to-runtime enhanced by generative AI to help you secure your hybrid and multicloud environments, across the entire lifecycle. Organizations can develop and deploy applications securely, minimize risks with continuous posture management, and protect workloads and applications from modern threats in an industry-first unified SecOps experience.

Defender for Cloud is fully integrated into the unified security operations platform—enabling your SOC team to have full visibility into cloud threats within the context of your broader threat landscape and active incidents. This includes automatic incident correlation with non-cloud security alerts and built-in response actions that make remediating easy. Your SOC and cloud security teams can efficiently collaborate on responding to incidents and hardening defenses.

Defender for Cloud also helps your cloud security team adopt a full CNAPP strategy, enabling them to achieve a higher level of security and resilience for their cloud native applications, while also accelerating innovation and business agility. A CNAPP enables organizations to embrace the benefits of cloud computing, without compromising on security or performance.

82%

of breaches involved data stored in the cloud.[4]

74%

of orgs have had business data exposed in an incident.[5]

42%

of data security incidents happen in the cloud.[5]

10 minutes

Cloud attackers spend less than 10 minutes to execute an attack.[6]

[4]Microsoft Enterprise DevOps Report
[5]Microsoft 2024 State of Multicloud Security Report
[6]The Need for Speed: When Cloud Attacks Take Only 10 minutes, Darkreading, October 9, 2023

Chapter 7

Get the most out of your security platform

The Microsoft unified security operations platform makes optimizing your SOC easier and faster. With the platform and related Microsoft services like Microsoft Defender Experts for XDR, organizations can increase SOC efficiency and save up to 50% on additional headcount. You can also realize up to a 50% reduction in employee downtime, and correlate incidents 50% faster—reducing singleton alerts to quickly get a full view of the early stages of any attack. And the projected return on investment (ROI) for organizations who unify their SIEM and XDR operations is between 43%-254% over a three-year period.[7]

To help CISOs and SOC leaders get the most out of their SIEM and/or XDR solution, we announced a new feature called SOC optimizations. We know data ingestion isn't free and even if you do ingest everything, it doesn't automatically make everything better—your coverage is only as good as your detection rules. SOC optimizations provides recommendations on how to fine-tune your data ingestion, detection rules, and more—based on your unique threat exposure and security toolset.

Our internal research shows that customers using SOC optimizations increased their data utilization by 30% and improved protection by 17%—all while reducing the workload on SOC engineers.[2]

[7]Total Economic Impact™ of Microsoft SIEM and XDR

Conclusion—be ready to defend against AI-driven cyberthreats

Advancements in AI are already changing cybersecurity. Cybercriminals are stepping up their game, using AI to automate cyberattacks and rapidly creating sophisticated malware and credible-sounding phishing emails. Fortunately, the security community is also moving quickly to incorporate the latest AI advancements into solutions that make identifying and responding to cyberthreats more efficient and effective.

To give your organization an edge, start by simplifying your security stack. The Microsoft unified security operations platform together with Security Copilot provides visibility across your entire digital ecosystem and powerful tools to stop cyberattacks quickly—no matter where they start.

And for those with smaller teams or hiring challenges, Microsoft Defender Experts for XDR is a managed service to augment your SOC with experts that triage, investigate, and respond to incidents on your behalf.

Build a cyberthreat-resilient organization with a unified security operations platform that integrates XDR, SIEM, and generative AI.

"There aren't too many vendors on the planet that can create a solution capable of providing consolidated insights into large, complex environments like ours. That's why we chose Microsoft."

Thomas Mueller-Lynch
Service Owner Lead for Digital Identity, Siemens

A unified platform with industry-leading solutions

Microsoft named a Leader in the Forrester Wave: Extended Detection and Response (XDR) platforms, Q2, 2024[8]

Microsoft Defender XDR is an extended detection and response (XDR) solution that helps protect devices, email, collaboration tools, hybrid identities, and multicloud apps with automatic attack disruption capabilities and effective tools for investigating and remediating complex security incidents.

Microsoft named a Leader in the 2024 Gartner® Magic Quadrant™ for Security Information and Event Management.[9]

Microsoft Sentinel is a cloud-native security information and event management (SIEM) solution that empowers teams to detect and resolve critical cyberthreats quickly with built-in security orchestration, automation, and response (SOAR) capabilities, user and entity behavior analytics (UEBA), and threat intelligence.

With the unified security operations platform, Microsoft leads the industry in individual workloads with recognition in nine Forrester Wave™ reports[10] from Enterprise email security and Zero Trust to data security platforms, endpoint security and more.

Combining the most advanced GPT-4 model from OpenAI with a Microsoft-developed, security-specific model, Microsoft Security Copilot is a generative AI security solution that automates query development, analyzes code, and offers guidance and recommendations in natural language.

60%
reduction in the risk of a material breach[1]

$1.6M
annual savings from vendor consolidation[4]

207%
return on three-year investment[4]

68,000
hours saved annually in improved productivity[4]

[8]Forrester Wave: Extended Detection and Response (XDR) platforms, Q2, 2024
[9]Gartner, Magic Quadrant for Security Information and Event Management, By Andrew Davies, Mitchell Schneider, Rustam Malik, Eric Ahlm, 8 May 2024.
Gartner does not endorse any vendor, product or service depicted in its research publications and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose. GARTNER is a registered trademark and service mark of Gartner, Inc. and/or its affiliates in the U.S. and internationally, Magic Quadrant is a registered trademark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved.
[10]The Forrester Wave™: Extended Detection and Response Platforms, Q2 2024, Allie Mellen, June 2024.

Resources and references

Explore your deployment options

Learn about the unified security operations platform

Learn about Microsoft XDR

Learn about Microsoft Sentinel

Learn about Microsoft Security Copilot

Augment your team

Learn about Microsoft Security Experts