

Defend against   
cybersecurity threats   
Partner Messaging and Positioning Framework



# Purpose of this framework

This messaging framework provides clarity and consistency for developing messaging for external and   
internal use for the Microsoft defend against cybersecurity threats campaign. You can use the information within this document in all forms—analyst meetings, public relations, events, web social, and conversations with stakeholders.

**This is an internal document only.** It is intended only for use by your sales and marketing representatives who need to explain and communicate this solution story to create customer-facing copy for websites, social media, promotional materials, and so on. In addition to sales and marketing, this messaging information can be used in the field by vendors, for PR, by events teams, by product teams, by social teams, and for corporate communications. If unsure of usage in a particular situation, please check with your Microsoft representative.

**Do NOT give this document directly to customers**. Instead, use it as a reference to align materials and customer messaging. These messages can be constructed using the customer-facing topline message, benefits, and proof points.

# Market context and research

## The partner story

The partner opportunity to deliver services and solutions related to Microsoft security grew in fiscal year (FY) 2024 by 10 percent for enterprise customers and by 19 percent for small and medium-sized business (SMB) customers. This growth was driven by several factors, including customers getting ready for generative AI, customers’ desire to reduce costs while improving IT security, and partners expanding into new solution areas in response to the increased investments Microsoft made in its security-related offerings.

Many factors have contributed to the increased partner opportunities to assist customers with their security and compliance needs. First and foremost, the meteoric rise in customer interest to use generative AI (gen AI) solutions in the workplace and the launch of Copilot for Microsoft 365 mean organizations that previously deferred security and compliance work must now make up for years of underinvestment. Second, cyberthreats continue to increase in terms of complexity, volume, and velocity. In part, this is due to bad actors using gen AI to increase speed, scale, and perceived believability of attacks across existing and new threat channels. Third, ongoing economic uncertainty has spurred companies to look for ways to reduce costs. In many cases, companies are double paying for security solutions in the form of Microsoft premium SKUs.

The analyst story

We consistently hear how the day-to-day workflow of analysts involves spending significant time filling the gaps left by their current tools. Many of the security teams we talk to use many cybersecurity tools. This leaves them with a patchwork of tools to defend their digital estate. As a result, they’re defending in siloes and thinking in lists. Meanwhile, attackers are thinking in graphs, expertly traversing across the network by moving between the seams of the organization’s security siloes. This forces the security teams to manually translate their lists of alerts into an incident map, while under pressure from potentially in-progress attacks. All 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.

## The cybersecurity story

Cybersecurity is a complex problem that needs to be addressed holistically. Strong prevention or the ability to capture and analyze a wide variety of logs alone isn’t enough. Attacks happen in minutes and hours; security teams don’t have days or months to respond. And as long as defenders are stuck working in siloes, attackers will have an edge being able to move between all the seams. Security leaders need to shift towards a comprehensive approach that better integrates their threat protection capabilities across a unified security platform to deliver real value and impact across the entire lifecycle of threats.

# Aligned Scenarios

* Unify your security tools.
* Build new cloud-native apps and be ready for the era of AI.
* Add AI capabilities to security.
* Modernize security and take advantage of cloud capabilities.
* Simplify IT and security operations.
* Protect a hybrid workforce.
* Enhance threat protection.
* Get a comprehensive view of your entire digital estate.

# Aligned Products

|  |  |
| --- | --- |
| Products | * Microsoft Sentinel * Microsoft Defender XDR * Microsoft Defender for cloud * Microsoft Threat Intelligence * Security Exposure management |
| AI | * Security Copilot |

# Audience

|  |  |
| --- | --- |
| Decision maker | C-Suite (CSO, CTO)/VP/Director of Development, Architecture |
| Influencers | SOC Teams, IT |

# Elevator pitch

|  |
| --- |
| PARTNER SOLUTION and The Microsoft unified security operations platform integrates Microsoft Sentinel, Defender XDR, Security Exposure Management, Security Copilot, and Threat Intelligence into one unified experience. Customers receive a unified incident queue, single data model, guided investigations and response, continuous risk assessments and attack path modeling, and automated protection and remediation. The platform starts with a foundation of global threat intelligence that delivers the industry’s broadest view of the threat landscape. Next is a posture layer that applies security controls at every layer to help prevent threats from happening. The solution also makes it easier to implement improvements with simple step-by-step guidance—or even single-click actions. In addition, there’s threat detection and response layers powered by leading XDR and SIEM solutions. Using the depth of XDR, the breadth of SIEM, and the context of threat intelligence, PARTNER SOLUTION and Microsoft unified security operations also delivers unparalleled visibility into threats, improves prioritization and drives rapid, holistic responses—even across multiple security layers and domains. Lastly, the platform uses cybersecurity-specific AI, delivering automation that can disrupt threats before they can impact an organization, guide analysts through incident investigations, and cut down tasks that turn hours into minutes or seconds. |

# Solution copy blocks

|  |  |
| --- | --- |
| Short elevator pitch (25 words) | Unify security operations across prevention, detection, and response with a comprehensive, gen-AI powered platform that centralizes security data, capabilities, and threat intelligence to empower defenders. |
| Medium elevator pitch (50 words) | PARTNER SOLUTION and the Microsoft unified security operations platform brings together all the security data, intelligence, and SOC tooling capabilities security teams need to dynamically defend their organization against today’s threats. This comprehensive, AI-powered unified platform knocks down security siloes and empowers defenders with intel-driven recommendations, real-time attack disruption, and powerful automated response capabilities. |
| Long  elevator pitch (100 words) | Today, defenders are fighting asymmetric battles against relentless, well-resourced attackers. A diverse portfolio of disparate legacy tools is simply not able to protect organizations from the speed, scale, and sophistication of today’s cyberthreats. PARTNER SOLUTION and The Microsoft unified security operations brings together all the security data, intelligence, and SOC tooling capabilities security teams need to dynamically defend their organization in today’s threat landscape. This comprehensive, AI-powered unified platform empowers defenders with intel-driven recommendations on how to reduce their attack surface and harden defenses, actively disrupts attackers that breach the perimeter, and enables rapid remediation with a powerful AI-powered investigation experience and automated response actions. |

# Value pillars—customer outcomes

|  |  |
| --- | --- |
| 1 | Prevent breaches across your multiple-platform,  multicloud environment Proactively improve your security posture with unified exposure management that continuously discovers, learns, and responds to risks in all connected systems, powered by Microsoft global threat intel and security experts. |
| Core pain points | * Preventing repeat attacks and identity compromises * Attackers taking advantage of overworked security teams * Large digital footprints having a ton of exposure * Understanding and implementing effective security policies |
| Customer benefits | * Continuously measure, manage, and improve a security posture across devices, identity, applications, data, and multi-cloud infrastructure * Harden defense with tailored recommendations * Monitor security controls and model potential attack paths * Improve security posture with faster mean-time-to-detect * Prevent repeat attacks by limiting vulnerability to similar attacks in the future |
| Proof points | * 80–90% of compromise originates from unmanaged devices.[[1]](#footnote-2) * Basic security hygiene still protects against 99% of attacks.1 |

|  |  |
| --- | --- |
| 2 | Detect and defend against threats with real-time protection Coordinate defense across security layers and prevent attackers from reaching critical assets with AI-generated decoys and lures, disrupting the kill chain in the early stages, and automating response to significantly reduce dwell time. |
| Core pain points | * Limiting damage from breaches * Gaining visibility into the entire kill chain * Little margin to detect and respond to in-progress attacks |
| Customer benefits | * Detect and disrupt in-progress advanced persistent threats like ransomware, business email compromise, and adversary-in-the-middle with Automatic Attack Disruption * Deceive attackers and protect critical outlets with AI-generated decoys and lures * Detect and defend across the entire kill chain with full visibility and protection * Get end-to-end visibility all in one place, streamlining triage and views of threats across the digital estate |
| Proof points | * Disrupt ransomware attacks in an average of 3 minutes.[[2]](#footnote-3) * Lower the risk of a material breach by 60% with XDR + SIEM.[[3]](#footnote-4) * Reduce average time-to-respond by 88%.3 * Improve SOC productivity by redeploying up to 75% of analyst time by moving away from basic triage and alert correlation.3 |

|  |  |
| --- | --- |
| 3 | Rapidly remediate threats with generative AI Improve SOC responsiveness with a unified analyst experience that reduces context-switching and delivers a streamlined threat-intel enriched investigation experience with step-by-step guidance and automation. |
| Core pain points | * Investigating and responding to threats efficiently. * A wide range of security expertise needed. * Collaborating across business functions. |
| Customer benefits | * Respond to incidents at the speed of generative AI * Gain step-by-step guidance automation that turns complex, multi-stage incidents into manageable investigations * Supercharge SOC productivity with a unified, incident-focused investigation and response experience * Get security reporting without the heavy lifting |
| Proof points | * Across all tasks, participants using Microsoft Security Copilot were22% faster.4 * 97% of security professionals said they want Copilot next time they do the same task.[[4]](#footnote-5) * 93% reported Copilot helped them improve the quality of their work.4 * 19% were faster at writing incident reports.4 * 39% were faster at summarizing an incident.4 * Analysts using Copilot created incident summaries with 49% more incident facts.4 |

# Use cases

For most businesses, unified security is most compelling when sold through a relevant use case. Use cases connect the value of AI and of a unified security solution.

|  |  |
| --- | --- |
| Device management | Generate policies and simulate their outcomes, gather device information for forensics, and configure devices with best practices from similar deployments. |
| Data security and compliance | Identify data impacted by security incidents, generate comprehensive summaries of data security and compliance risks, and surface risks that may violate regulatory compliance obligations. |
| Incident response | Quickly analyze and respond to security incidents with AI-driven insights and recommendations. |
| Security reporting | Generate comprehensive reports that provide clear visibility into your security landscape, aiding in decision-making, threat assessment, compliance, and management/board-level briefs. |
| Security posture management | Assess and improve your organization’s security posture with actionable insights based on your unique organization. |
| Threat hunting | Use natural language to search for and isolate advanced threats across the environment. |
| Cloud security | Discover attack paths impacting workloads and summarize cloud CVEs to proactively prevent threats and manage cloud security posture more efficiently. |
| Incident summarization | Gain context for incidents and improve communication across your organization by taking advantage of gen AI to swiftly distill complex security alerts into concise, actionable summaries, which then enable quicker response times and streamlined decision-making. |
| Impact analysis | Utilize AI-driven analytics to assess the potential impact of security incidents, offering insights into affected systems and data to prioritize response efforts effectively. |
| Reverse engineering  of scripts | Eliminate the need to manually reverse engineer malware and enable every analyst to understand the actions executed by attackers. Analyze complex command line scripts and translate them into natural language with clear explanations of actions. Efficiently extract and link indicators found in the script to their respective entities in your environment. |
| Guided response | Receive actionable step-by-step guidance for incident response, including directions for triage, investigation, containment, and remediation. Relevant deep links to recommended actions allow for quicker response. |

1. Microsoft Digital Defense Report 2023 [↑](#footnote-ref-2)
2. Microsoft Internal Statistics [↑](#footnote-ref-3)
3. [Forrester Consulting, “The Total Economic Impact™ Of Microsoft SIEM And XDR,”](https://go.microsoft.com/fwlink/?linkid=2245543&clcid=0x409&culture=en-us&country=us) August 2022, commissioned by Microsoft [↑](#footnote-ref-4)
4. Source: Microsoft Copilot for Security randomized controlled trial conducted by Microsoft Office of the Chief Economist, January 2024 [↑](#footnote-ref-5)