Government Thought leadership · 5 min read

Microsoft Copilot for Security: The great equalizer for government security

By Alvaro Vitta, Microsoft Worldwide Cybersecurity Lead for Public Sector

February 14, 2024

Copilot

Generative AI

Cybersecurity for government organizations is a game of speed, with cyberattackers working to compromise networks and steal

data as swiftly as possible before defenders can detect and deter them. In this ongoing battle, cyberattackers have traditionally had an asymmetrical advantage.

From the moment a user clicks on a bad hyperlink in a malicious email, it can take as little as *72 minutes* before an attacker begins to exfiltrate data. By contrast, it takes an average of 277 days for organizations to identify and contain a data breach.[1] The advantage gap is widening, as nation-state-actors and cybercriminals are actively employing AI to step up their attacks. To cite just one measure: in 2023, password attacks globally increased from three billion to 30 billion per month.[2]

HOW GOVERNMENTS ARE LEVELING THE CYBERSECURITY PLAYING FIELD WITH CLOUD AND AI

Read the blog ›

The good news is that advances in hyperscale cloud and AI technology promise to help shift the balance of cybersecurity power to the defenders. In my previous blog, I examined the strategies governments can take to minimize cybersecurity risk and advance security effectiveness with Microsoft technology. Now, I'd like to explain how Microsoft Copilot for Security offers one of the most powerful new opportunities for governments to make dramatic improvements in cybersecurity, thanks to the power of generative AI.

The unique cybersecurity challenges facing governments

Government agencies and critical infrastructure organizations are prime targets for cybercrime, for obvious reasons: the vast amounts of valuable data they hold, the importance of the assets they oversee, and economics involved. Cybercriminals target the public sector for ransomware attacks more than any other sector, and nation-state actors are ramping up their attacks on critical infrastructure and government.

Making the challenge even more difficult for governments is the growing demand for skilled cybersecurity staff. Worldwide, there is a shortage of 3.4 million cybersecurity professionals, and the problem is especially problematic for governments, who often struggle to attract and retain top talent.[2]

Add to this the liabilities of legacy systems, legacy mindsets, and legacy approaches to technology (any of which can hamper governments, despite their most sincere efforts), and the advantage can easily tilt in the direction of cyber adversaries.

How Microsoft Copilot for Security advances government cybersecurity

Cybercriminals have been quick to embrace generative AI. In underground, gated internet forums—the so-called dark web—attackers share the latest innovations built on ChatGPT, effectively accelerating the ability of bad people and organizations to do bad things. A recent report attributed 85% of the rise in cyberattacks over the past 12 months to bad actors using generative AI.[3] The good news is that Microsoft and other technology providers are responding with AI-powered innovations to counter the threat.

Microsoft Copilot for Security is the first generative AI security product that will help defend organizations at machine speed and scale. It combines the most advanced GPT4 model from OpenAI with a Microsoft-developed security model, powered by Microsoft Security's unique expertise, global threat intelligence, and comprehensive security products.

Microsoft Copilot for Security is designed to work seamlessly with the systems and tools used by modern governments, specifically the security operations center (SOC) for managing security on an organizational and technical level, and the security information and event management (SIEM) solution for detecting, analyzing, and responding to threats.

Imagine an analyst investigating a potential breach in the network. Today, this person would use scripts and manual queries to correlate information from across multiple screens and disparate systems with terabytes and petabytes of data, in an attempt to evaluate security signals and draw valuable conclusions—a "needle-in-the-haystack" exercise that is both slow and unreliable.

MICROSOFT COPILOT FOR SECURITY PROVIDES IMMEDIATE IMPACT FOR THE MICROSOFT DEFENDER EXPERTS TEAM

Read the blog ↗

By contrast, Copilot for Security enables analysts to use natural language to ask questions, such as, "Can you identify indicators of compromise?" "Where are we seeing suspicious logon attempts?" and so on, to rapidly assess an organization's security posture. By analyzing and interpreting massive amounts of security data from across heterogenous environments and platforms in real-time, copilot assists the cybersecurity analyst to find detailed, actionable insights and solutions at a speed and reliability that are simply unachievable today using legacy technology. Moreover, Copilot for Security can then easily translate hunting insights or incident responses into PowerPoint slides or emails to quickly inform colleagues or leadership.

Notably, Copilot for Security empowers analysts to become more effective hunters and responders without specialized technical training. Our early private preview customer research data shows that it saves analysts up to 40 percent of their time on foundational tasks like threat intelligence assessments, and up to 63 percent of their time preparing reports. These efficiency gains free up analysts to focus more on high value tasks to secure the organization, with Tier 1 and Tier 2 analysts potentially performing tasks that would otherwise be reserved for more experienced Tier 3 or Tier 4 professionals.

Preparing your environment for Microsoft Copilot for Security

Microsoft Copilot for Security is currently available through our Early Access Program and is expected to be released broadly later this year.

However, now is the time to prepare so that your environment is optimized to take full advantage of Copilot for Security when it becomes available.

The most impactful move you can make in the near term is to adopt Microsoft Defender XDR (for extended XDR, or extended detection and response), Microsoft Sentinel (a cloud-native SIEM solution), and Microsoft Intune (for endpoint management) as soon as possible. These tools deliver a unified security operations platform that complements most existing environments and investments, and they provide a strong security foundation that leverages Microsoft's vast security data and expertise.

Beyond this, it's important to build a strong partnership between your public sector organization and trusted companies in the private sector. At Microsoft for Government, we are committed to partnering with government customers and our global partner ecosystem to ensure long-term success. With our leading cloud and AI capabilities, our battle-tested understanding of the digital threat landscape, and the wisdom of our more than 10,000 security professionals globally, we are excited to help shift the balance of cybersecurity power from the side of the criminal over to the side of governments.

Improve cybersecurity with Microsoft technologies

To learn more and get ready for Microsoft Copilot for Security in your organization, work with your Microsoft representative or solutions provider partner to explore an envisioning workshop or plan a national cybersecurity modernization journey roadmap.

Visit theMicrosoft for Government page to learn more about how we're helping governments secure critical environments, protect data, and achieve compliance. For United States customers, see Preparing for Security Copilot in US Government Clouds.

---

[1]Cost of Data Breach Report 2023, IBM.

[2]Microsoft issued annual Digital Defense Report: Espionage fuels global cyberattacks, Microsoft.

[3]Study finds increase in cybersecurity attacks fueled by generative AI, Security Magazine.

Alvaro Vitta

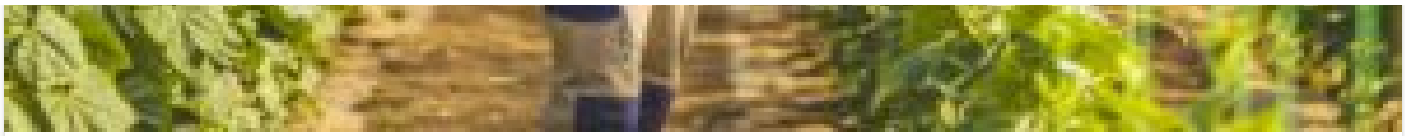
Microsoft Worldwide Cybersecurity Lead for Public Sector

Alvaro leads the Global Cybersecurity Strategy for Public Sector at Microsoft. He helps government organizations implement cybersecurity strategies, enabling the modernization of cybersecurity capabilities using an AI-centric approach. He has over 18 years of experience and holds several industry certifications in security and cloud architecture.

See more articles from this author ›

Related posts

Apr 2
7 min read read
Threefold revolution: The influence of generative AI on retail and consumer goods ›



Apr 2
4 min read read
World Agri-Tech 2024: Pioneering agriculture resilience with AI ›

Apr 1
6 min read read
How responsible AI helps financial services manage risk and assure compliance ›

Mar 28
5 min read read
Use natural language and generative AI to create calculation models, streamline data collection, and improve reporting ›

Explore Microsoft industry solutions

Transcend boundaries with tailored industry solutions. Accelerate time to value, speed up innovation, and drive benefits for your customers, employees, and organization.

Learn more

Follow us:

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