Defense and intelligence Thought leadership · 4 min read

Defend against cyber threats with AI solutions from Microsoft

By Alvaro Vitta, Microsoft Worldwide Cybersecurity Lead for Public Sector

Government AI Copilot more

cyber-attacks attributed to nefarious actors.

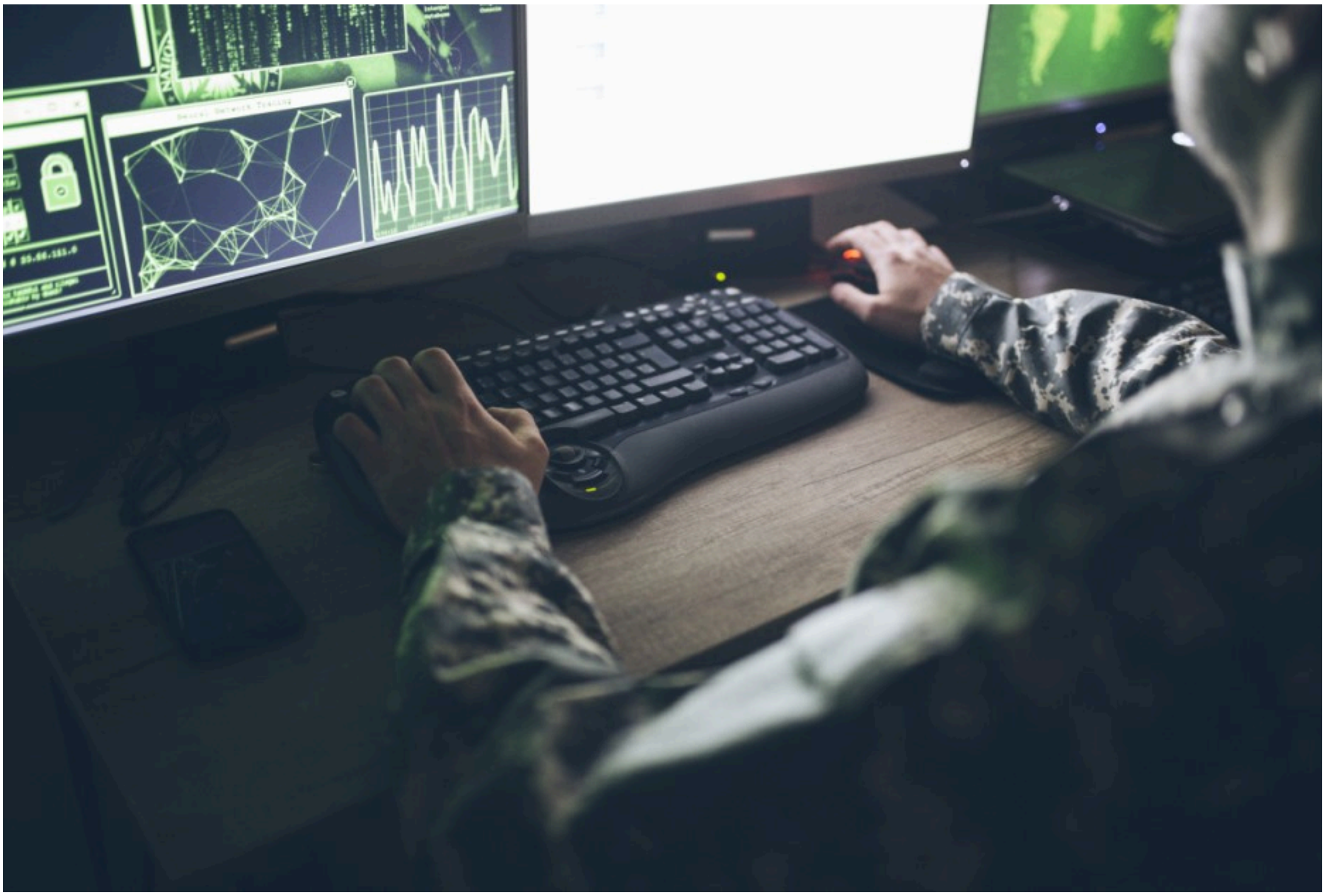
Historically, a nation's security and sovereignty depended on its ability to defend its interests in the land, air, sea, and space domains. However, with the growing reliance of nations on the digital ecosystem, the "cyber domain" has become as crucial to national security as the traditional domains. The number of cyber incidents targeting government agencies worldwide from December 2022 to August 2023 rose by an astonishing 150%—our adversaries are increasing their volume of attacks.

The Defense and Intelligence team at Microsoft understands defending a nation's interests requires a comprehensive national strategy that covers both the physical and digital domains. Accordingly, a reliable and secure digital backbone is the foundation, and a prerequisite for a national cybersecurity system.

Microsoft for Defense and Intelligence

Learn how to promote stability and security with Microsoft Cloud solutions

Explore capabilities >



The cybersecurity gap

Cyber offensive adversaries have a substantial advantage over national security agencies across four key areas:

1. Skills and innovation
2. Approach
3. Mindset
4. Technology

The image below illustrates the differences between the national security agencies and their cyber offensive adversaries in terms of cybersecurity capabilities.

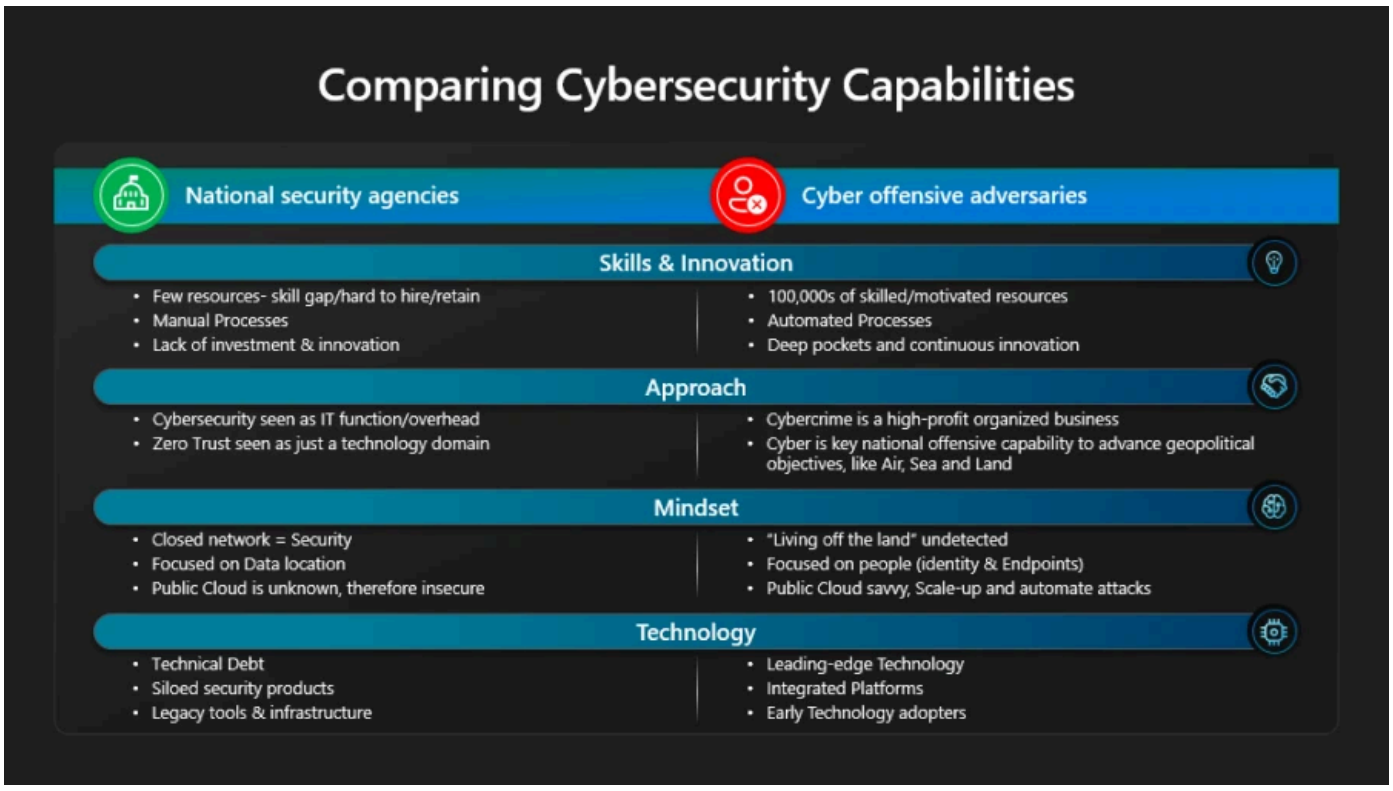


Figure 1: Comparing Cybersecurity Capabilities.

The public sector is the most vulnerable, with 53% of attacks in the last 12 months focused on critical infrastructure and government organizations. Cybercrime will cost the global economy up to $10.5 trillion by 2025.[1]

Reducing the impact on a nation's economy requires the latest in cyber technology to protect national digital assets, critical infrastructure, and the wellbeing of its residents.

Countering the rise of AI-enabled attacks

Microsoft collaborated with OpenAI to produce a cyber threat intelligence research study focusing on AI-based cyber activity and threat actors.

EMPOWERING RESPONSIBLE AI PRACTICES

Learn more ↗

The focus of the collaboration is to ensure the safe and responsible use of AI technologies, upholding the highest standards of ethical application, and to protect the community from potential misuse. Additionally, in line with Microsoft's leadership across AI and cybersecurity we also announced principles mitigating the risks associated with the use of AI tools and application programming interfaces (APIs) by nation-state advanced persistent threats (APTs), and advanced persistent manipulators (APMs), and cybercriminal syndicates. As the research illustrates, Microsoft and OpenAI took action to disrupt assets and accounts associated with threat actors, improve the protection of large language models technology and users, and shape the guardrails and safety mechanisms around the models.

Microsoft is further committed to using generative AI to disrupt threat actors and leverage the power of new tools, such as Microsoft Copilot for Security, to elevate defenders everywhere, including across the defense and national security ecosystem.

Using an AI-centric approach to shift the advantage to the cyber defenders

Defense and national security organizations need to modernize their approach and rapidly adopt new technologies to counter the significant advantage of their agile cyber adversaries. Implementing a National AI-cyber shield system, which is powered by Microsoft Copilot for Security, will help to shift the advantage to the cyber defenders.

A National AI Cyber Shield System aggregates key security information and event management (SIEM) and extended detection and response system (XDR) hosted on a hyperscale platform, achieving efficiencies of scale and centralized reporting. Government organizations have multiple generations of technology, spanning clouds, devices, and operating systems. The National AI Cyber Shield System monitors those systems, whether on premises, in a public cloud, or elsewhere. The National AI Cyber Shield System provides cyber threat intelligence, behavior analytics, security orchestration, and response, to deliver a unified, comprehensive view of a customer's security posture.

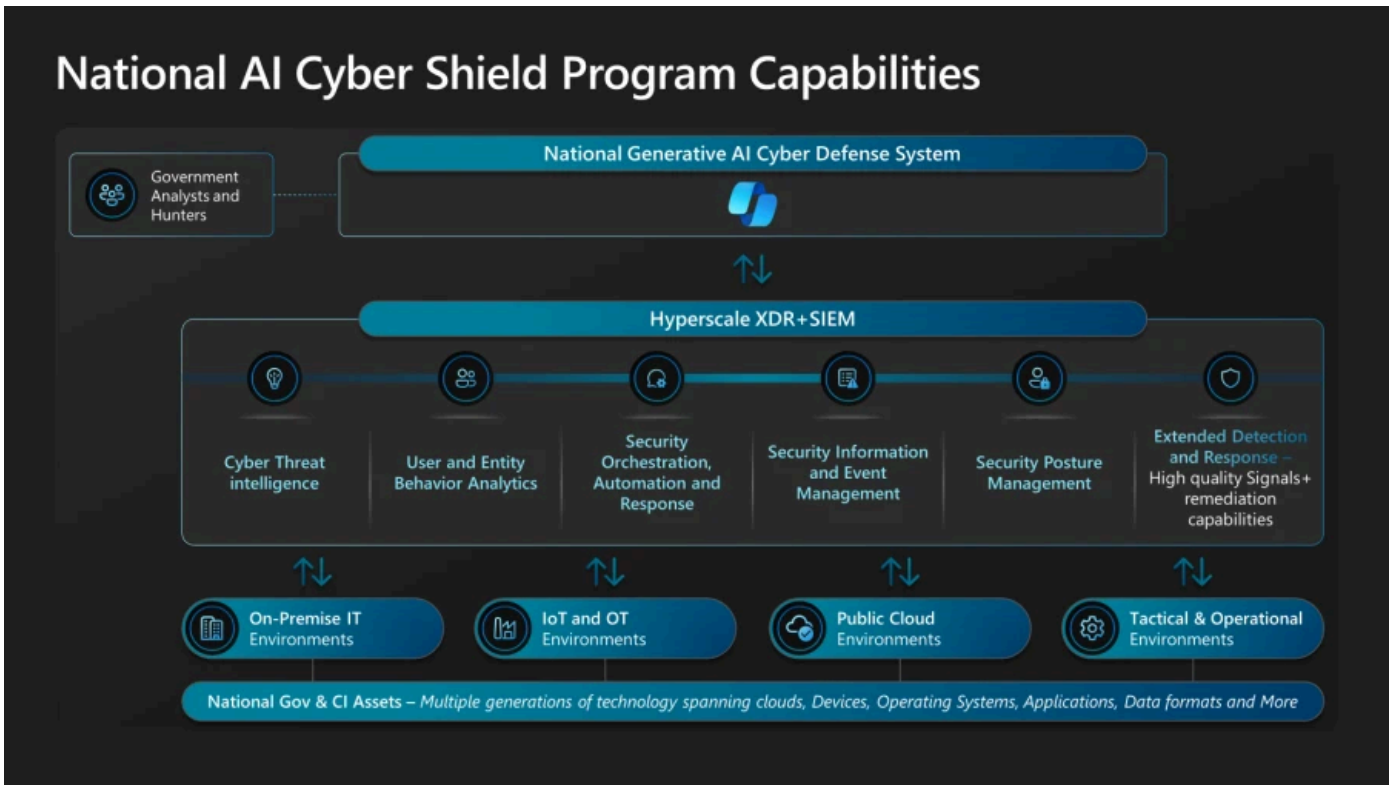


Figure 2: Modern Generative AI-cyber shield system.

The national AI-cyber system needs a Hyperscale XDR and SIEM platform to provide rich high quality security signals and security posture across the digital estate. This is delivered by Microsoft Defender XDR, Microsoft Sentinel, and the Hyperscale native SIEM providing a solution that can correlate events from disparate data sources and aggregate the results.

Cyber professionals can then use natural language prompts in Copilot for Security to dramatically increase the speed of hunting for threats as well as the necessary focus to hone in on high-risk events. This AI-centric approach resulted in an improvement of **up to 40% in speed** when completing tasks like investigation and response, threat hunting, and threat intelligence assessments.

Your strategy and application of AI tools is your cybersecurity shield against ever increasing threats from cyber offensive adversaries.

Shift the advantage and seize the power of cloud and AI to thwart cyber offensive adversaries. Modern cloud-based AI-cyber defense systems deliver speed, scale, and sophistication to stay ahead of cyber offensive adversaries, and attain mission outcomes.

Get started on your AI cyber defense journey

A private and public partnership must be forged between Microsoft and defense and national security organizations to shift the advantage towards defense organizations, and counter the volume, innovation, and sophistication of threat actors and cyber criminals.

> *"Artificial Intelligence will be a critical component of successful defense. In the coming years, innovation in AI-powered cyber defense will help reverse the current rising tide of cyberattacks."*
>
> *—Tom Burt, Corporate Vice President, Customer Security and Trust, Microsoft*

Start your AI-centric cyber defense modernization journey now. Follow these steps:

1. Prepare your AI-cyber defense transformation by implementing key foundational elements in the Hyperscale XDR and SIEM platform that would interact and feed your national AI-cyber defense system.
2. Get familiar with the generative AI cyber defense system: Copilot for Security.
3. Ensure your cyber defense and security operations teams understand how the generative AI cyber defense system works and start skilling them on how to implement and operate Copilot for Security.

Visit the Microsoft Defense and Intelligence to learn more about how we're helping defense and national security organizations protect national interests and ensure security.

Next steps

To learn more: Listen and apply insights from defense, government, and industry leaders on how AI-cyber capabilities are shifting the competitive advantage:

- Malta Gov National Cyber security Center Podcast

- Canadian Cybersecurity Centre Podcast
- Military Lessons on Cyberdefense
- Podcast with Tom Burt
- Read the Microsoft Digital Defense Report, 2023

---

[1] Cybercrime To Cost The World $10.5 Trillion Annually By 2025, Cybercrime 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 10 5 min read read

Maximize machine learning and data management in Azure Data Manager for Energy >

Apr 10 4 min read read

Beyond HIMSS24: Microsoft partners redefine healthcare with AI solutions >

Apr 9 5 min read read

Industrial transformation: Scaling AI across the manufacturing value chain >

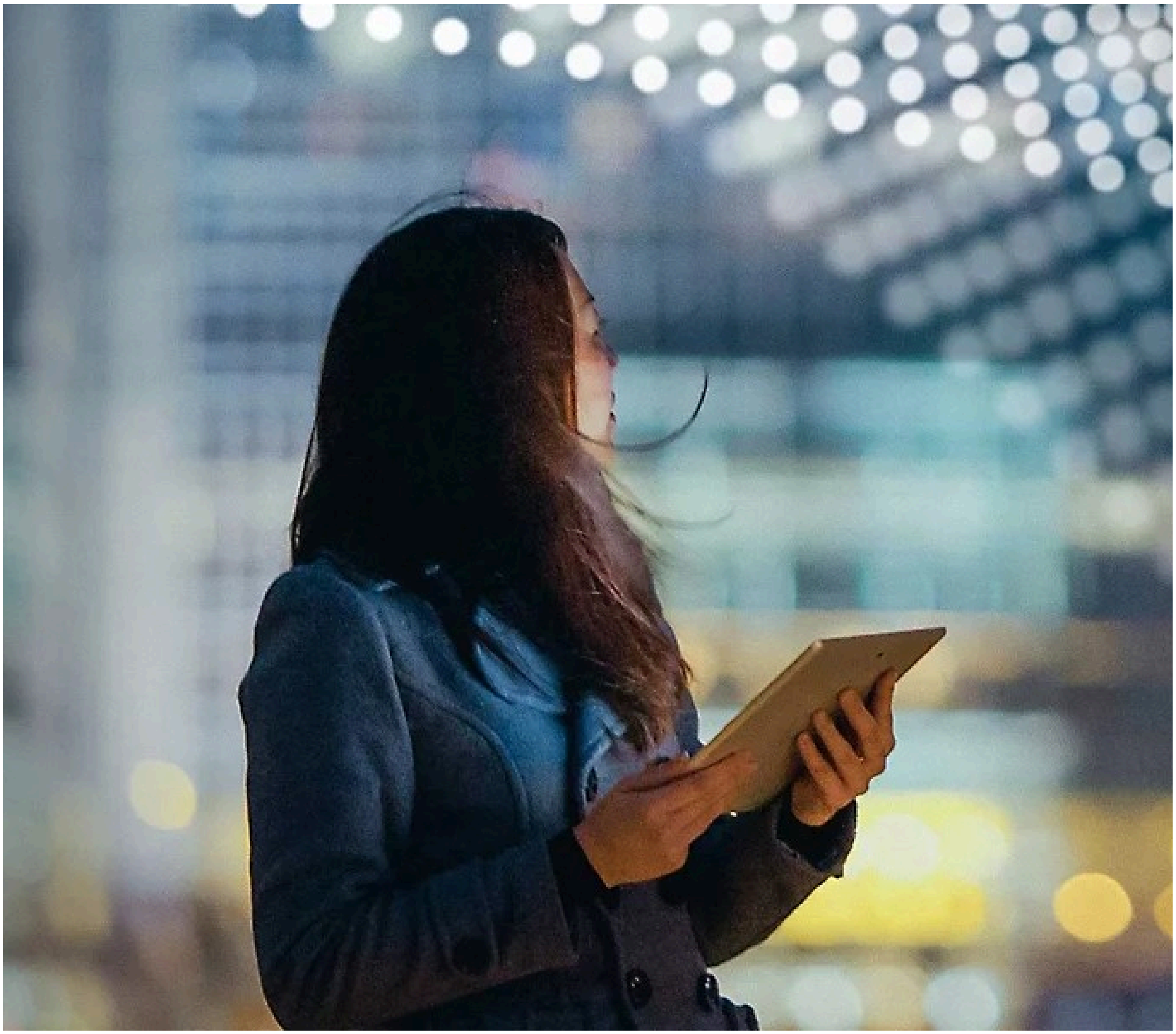
Apr 9 5 min read read

AI for social impact: 3 ways financial services can influence global challenges >

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.

Explore now



Follow us:

© Microsoft 2024