Microsoft

Denmarks path to AI leadership

3rd of April 2025

Rasmus Knappe, PhD.
Chief Technology Officer
Microsoft Denmark & Iceland

Agenda

1. Cyber Threat Landscape and AI’s role in Cybersecurity
2. Innovation and AI trends
3. Regulatory Compliance
4. Gefion

Agenda

1. **Cyber Threat Landscape and AI’s role in Cybersecurity**
2. Innovation and AI trends
3. Regulatory Compliance
4. Gefion

Our presence in the digital ecosystem positions us to observe key trends in cybersecurity. Microsoft's perspectives on cybersecurity are framed through **50 years of experience and insight.**

Society | Microsoft stakeholders | Microsoft Customers

Microsoft's unique vantage point

Billions of customers globally, from a broad and diverse spectrum of organizations, and consumers.

78 trillion security signals per day

1,500 unique threat groups tracked

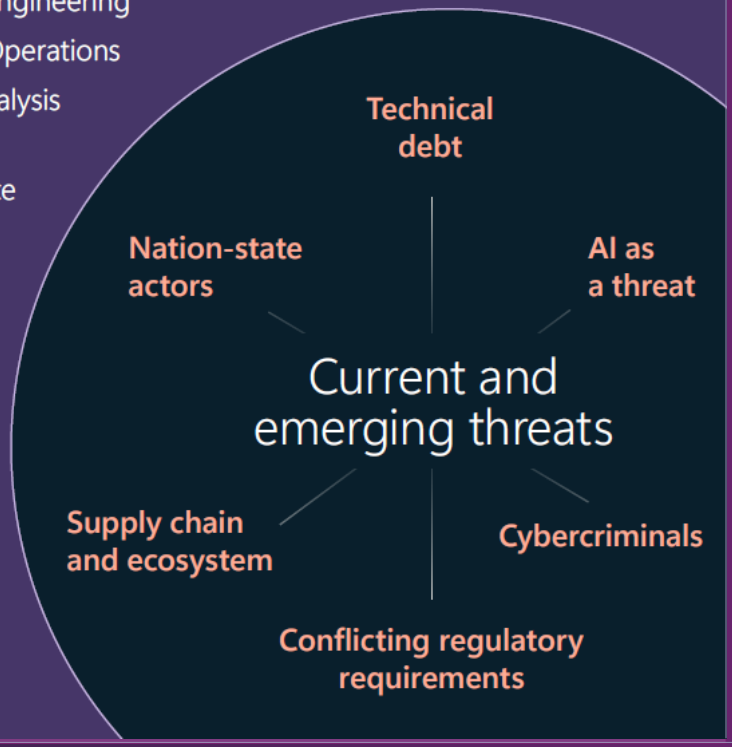
Microsoft's cybersecurity approach

Microsoft security investments

- AI Red Teams
- Defending Democracy
- Detection and Response
- Digital Crimes
- Digital Safety
- Incident Response
- National Security
- Physical Security
- Public Awareness and Education
- Responsible AI
- Security Engineering
- Security Operations
- Threat Analysis
- Threat Intelligence

34,000 dedicated security engineers

focused full-time on the largest cybersecurity engineering project in the history of digital technology.



Source: Microsoft Digital Defense Report 2024

Chapter 1

The evolving cyber threat landscape

How have trends and tactics changed?

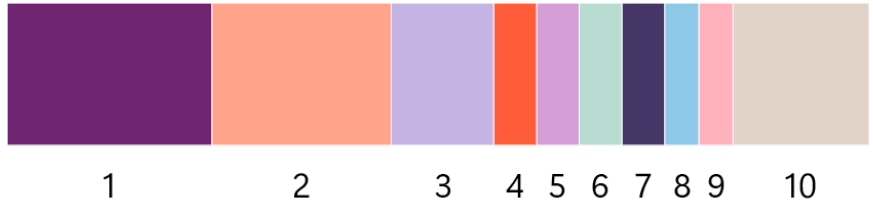
- Nation-state threats
- Ransomware
- Fraud
- Identity and social engineering
- DDoS

Nation-state threat activity by the numbers

- State-affiliated threat actors played a persistent supporting role in broader geopolitical conflicts.
- The Education and Research sector became the second most targeted by nation-state threat actors.

Threat actors from Russia, China, Iran, and North Korea pursued access to IT products and services, in part to conduct supply chain attacks against government and other sensitive organizations.

Top 10 targeted sectors worldwide

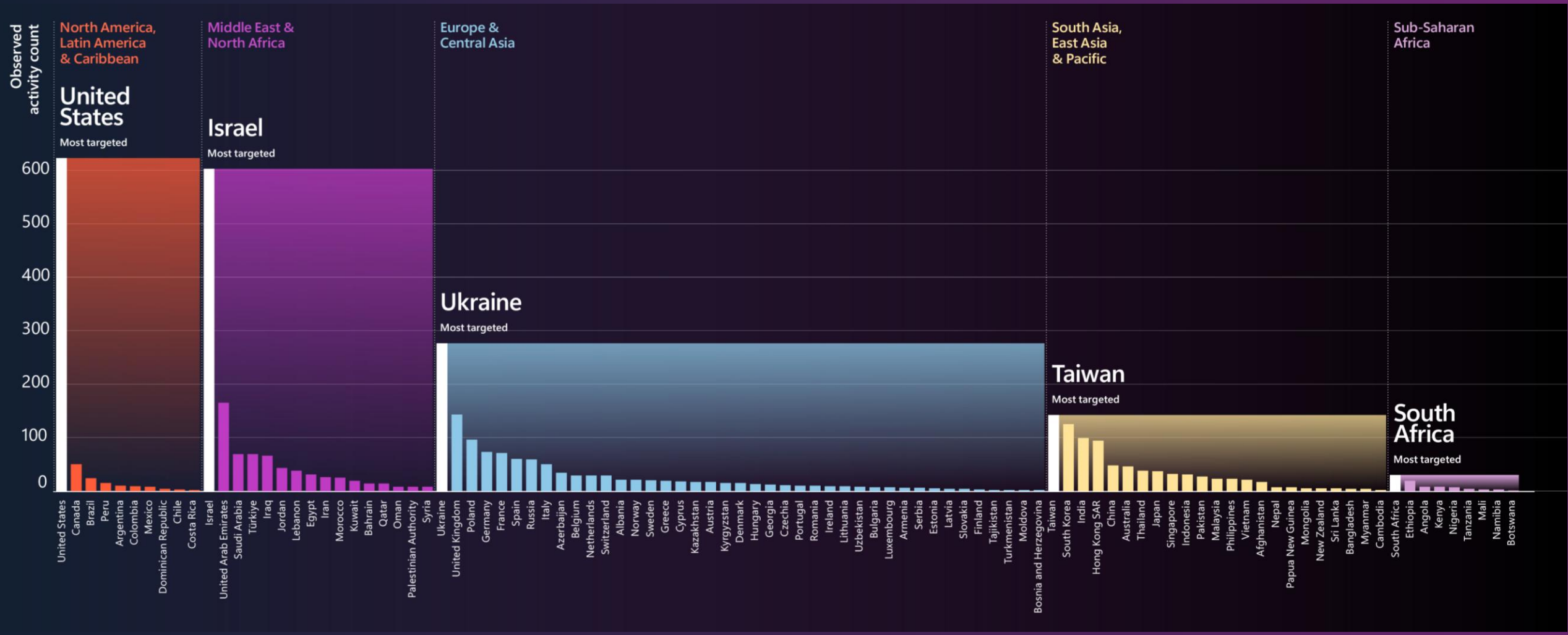


	Sector	Percentage
1	IT	24%
2	Education and Research	21%
3	Government	12%
4	Think tanks and NGOs	5%
5	Transportation	5%
6	Consumer Retail	5%
7	Finance	5%
8	Manufacturing	4%
9	Communications	4%
10	All others	16%

Source: Microsoft Threat Intelligence

Nation-state threat activity by the numbers

Regional sample of activity levels observed



Source: Microsoft Threat Intelligence data

Election interference

Defending elections against influence campaigns—as well as opportunistic cybercriminal efforts—demands a collective commitment from industry, media, and governments alike.

The convergence and parallel nature of nation-state operations throughout 2024 underscores just how persistent adversarial states are in their attempts to exert influence over US elections and outcomes. Left unchecked, this poses a critical challenge to US national security and democratic resilience.

Election-related influence operations timeline

China (December 22, 2023)

PRC-linked influence actor Taizi Flood uses AI-generated audio files to allege then Taiwanese Democratic Progressive Party presidential candidate was an informant in the 1980s.

China (January 13, 2024)

Taizi Flood promotes faked AI-generated audio recording of former presidential candidate and Foxconn founder Terry Gou endorsing then Taiwanese Nationalist Party presidential candidate Hou Yu-ih.

Russia (February 23, 2024)

Russia-affiliated actor Ruza Flood registers a series of US election-themed news websites. The websites are amplified over social media by inauthentic accounts using website redirect networks to mask the actors' infrastructure and likely use AI tools to generate content.

Russia (April 19, 2024)

Russia-affiliated influence actor Storm-1516 produces fake video that attempts to frame Ukraine for interference in the 2024 US presidential election.

China (May 2024)

Sophisticated PRC-linked sockpuppet accounts position on new social media platforms to spread divisive messaging, particularly surrounding protests on US college campuses ahead of the US presidential election.

Iran (June 15, 2024)

Iran sends spear phish to presidential campaign, likely in preparation stage for influence operations targeting the US elections. (Source: Microsoft data)

China (July 2024)

July 10: Deceptively edited short-form video from PRC-linked sockpuppet account masquerading as US conservative voter reaches 1.5 million views.

July 13: PRC state media foment speculation of "deep state involvement" in Trump attempted assassination.

Presidential elections
Taiwan
Jan 2024

Presidential elections
US
Nov 2024

On the right are key elections the influence actors were likely seeking to influence.
The flags represent the nation-state affiliation of observed influence actors.

Source: Microsoft Threat Analysis Center

Ransomware trends and insights

2.75x

Increase year over year in human-operated ransom-linked encounters

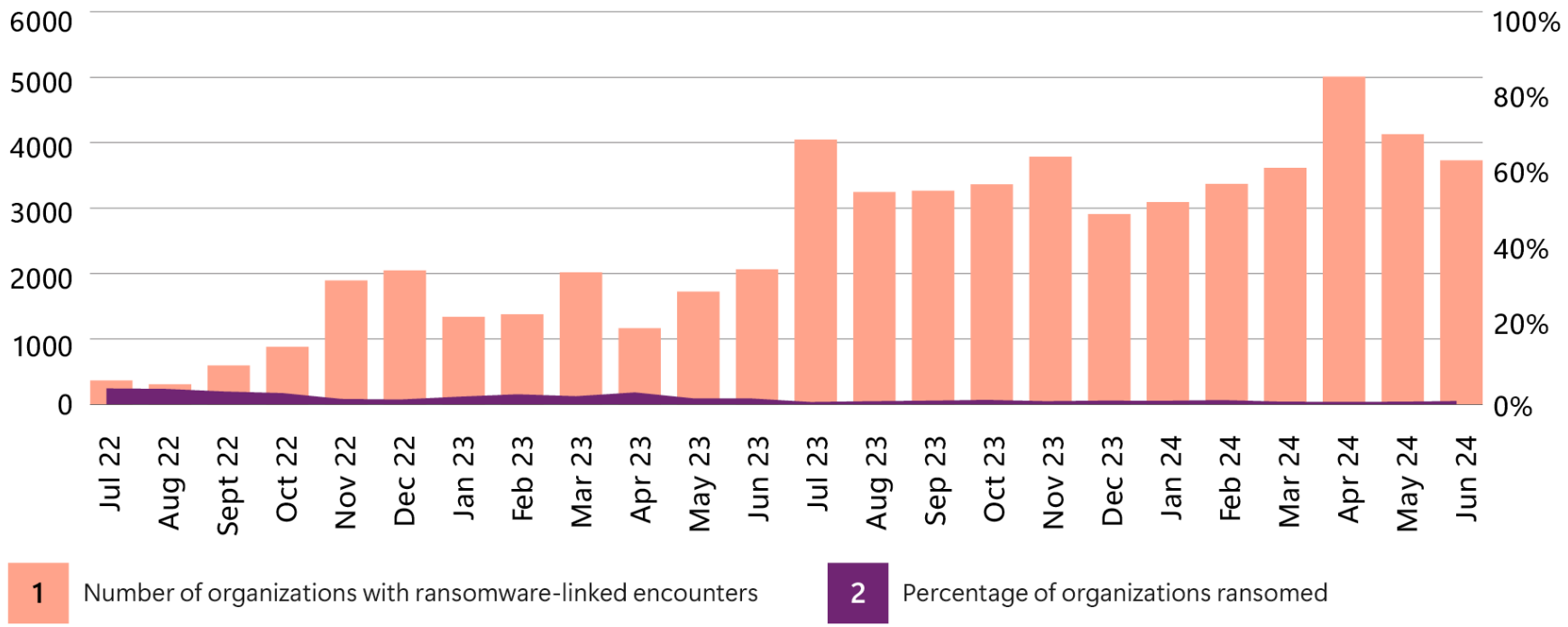
92%

Of successful ransom attacks leveraged an unmanaged device in the network

3x

Threefold decrease in ransom Attacks reaching encryption stage over the past two years

Organizations with ransom-linked encounters continues to increase while the percentage of those ransomed is decreasing (July 2022-June 2024)



Although organizations with ransom-linked encounters continues to increase, the percentage that are ultimately ransomed (reaching encryption stage) decreased more than threefold over the same time period.

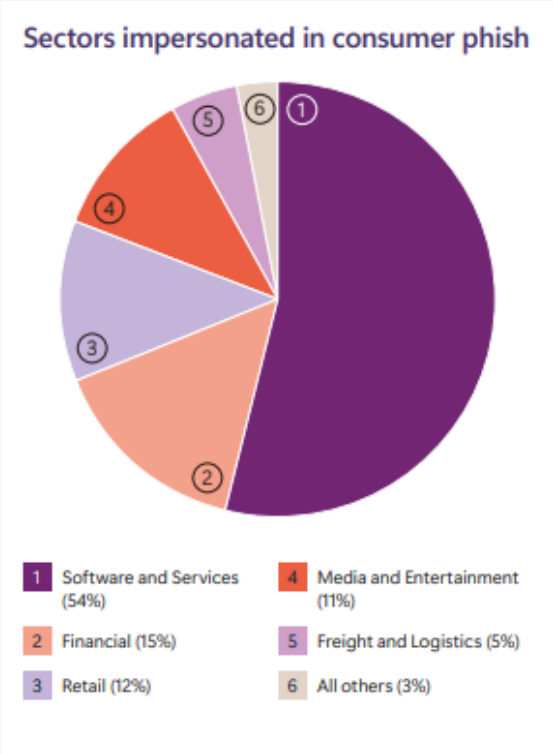
Source: Microsoft Defender for Endpoint

Fraud landscape and trends: Impersonation

Deepfakes

As deepfakes become more common in the business environment, organizations will have to implement countermeasures, such as requiring additional verification for transactions.

Corporate impersonation

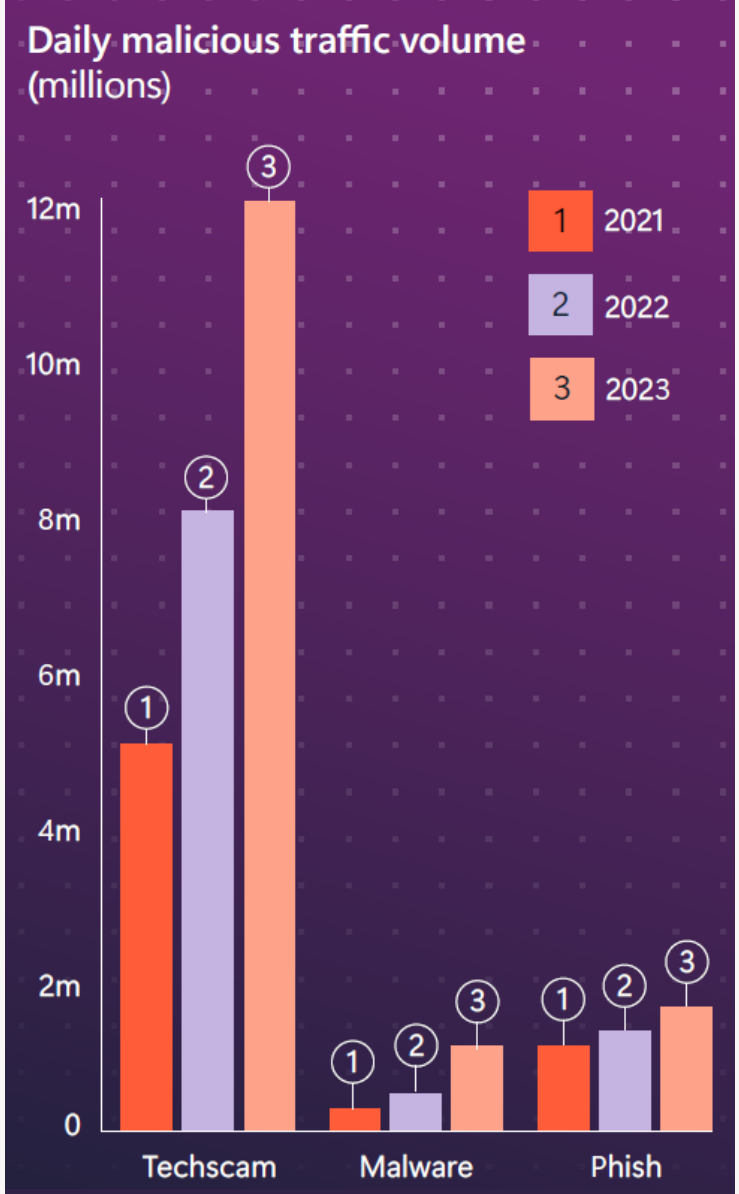


Account takeovers

Most ATOs still happen through simple methods like password spraying, phishing, keylogging, and using passwords from previous attacks found on the web.

Techscam

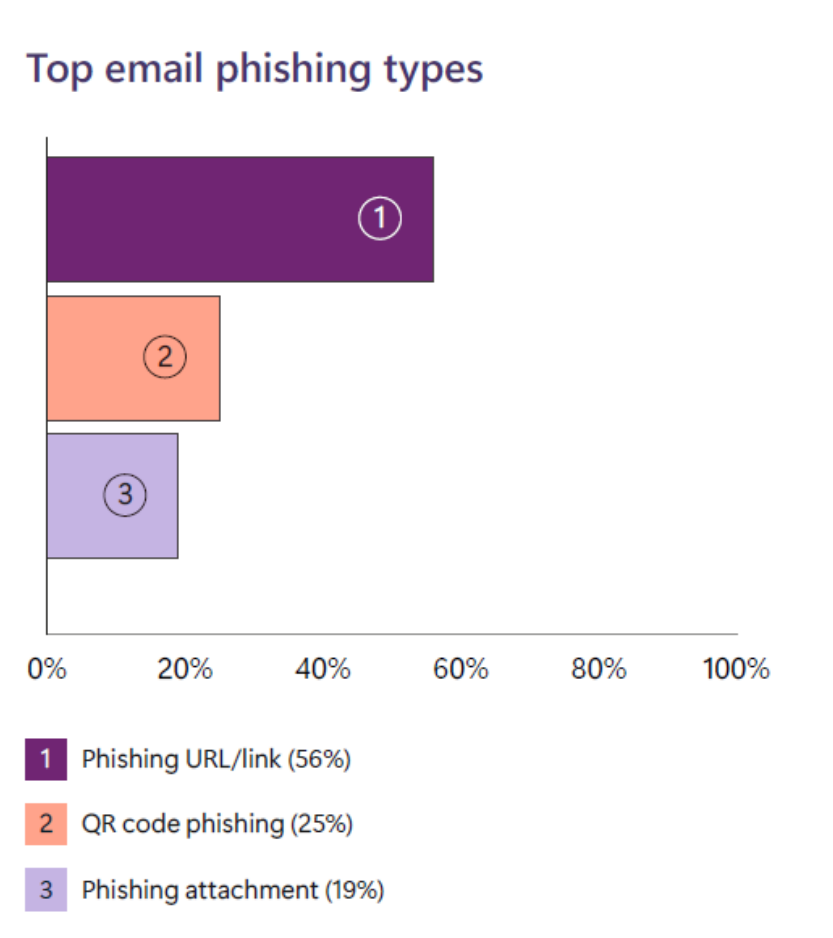
>70% of these malicious entities are active for less than two hours, meaning they may be gone before they're even detected.



The daily volume of techscam traffic has escalated dramatically, skyrocketing since 2021, a stark contrast compared to malware and phishing over the same period.

Source: SmartScreen log data

Fraud landscape and trends: phishing

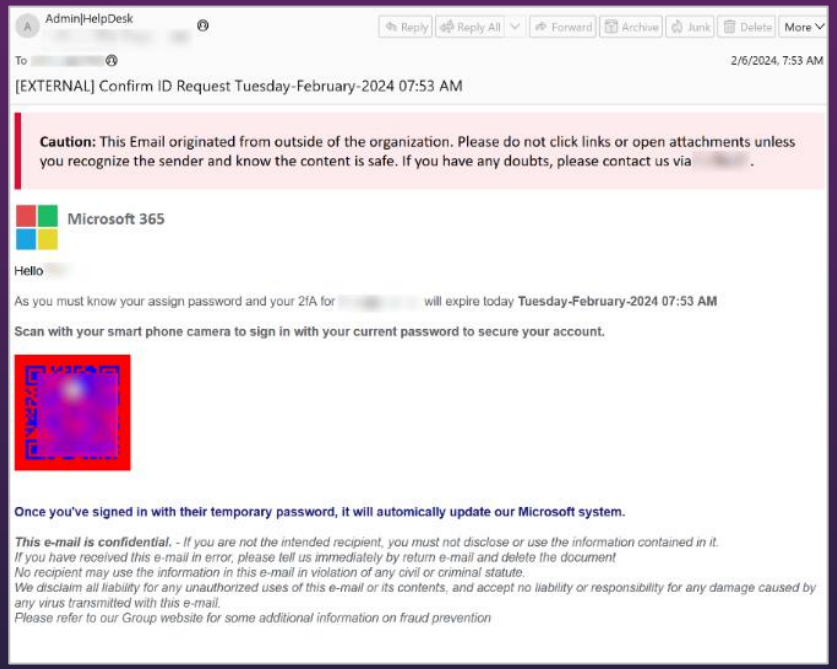


775 million

email messages contained malware

QR code phishing

By their nature, QR codes obscure the destination from the user, which creates a challenge for security



Identity attacks in perspective

Password-based attacks continue to dominate, but can be thwarted by using strong authentication methods.

<1%

of attacks

MFA attacks

SIM swapping
MFA fatigue
AitM

Post-authentication attacks

Token theft
Consent phishing

Infrastructure compromise

Source: Microsoft Threat Intelligence

7,000

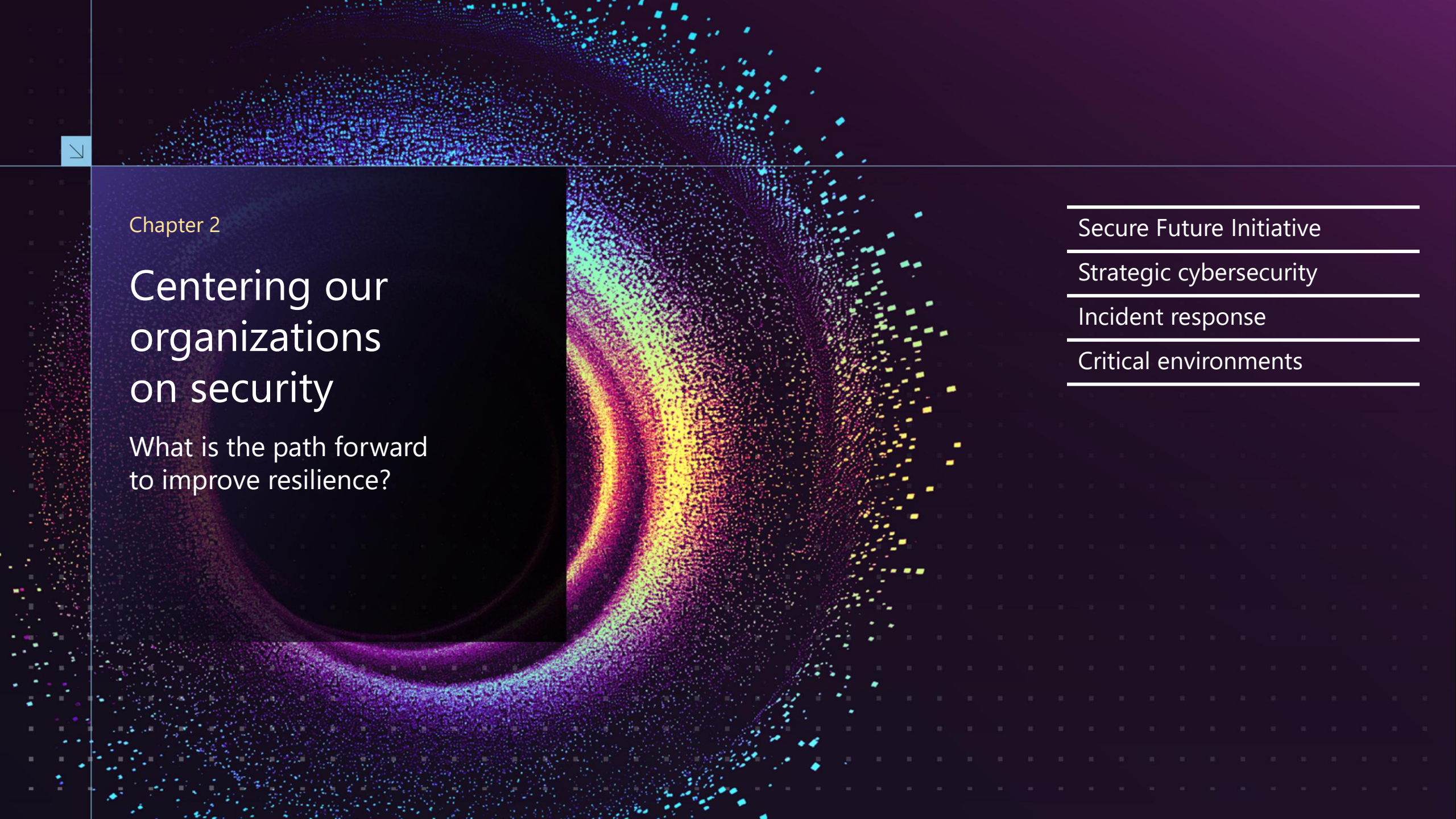
Password attacks per second

39,000

Token theft incidents per day

146%

Rise in AiTM phishing attacks



Chapter 2

Centering our organizations on security

What is the path forward to improve resilience?

Tackling technical debt and shadow IT for a secure future

Putting security above all else

The Microsoft Secure Future Initiative (SFI) is a multiyear initiative to evolve the way we design, build, test, and operate our products and services, to achieve the highest possible standards for security.

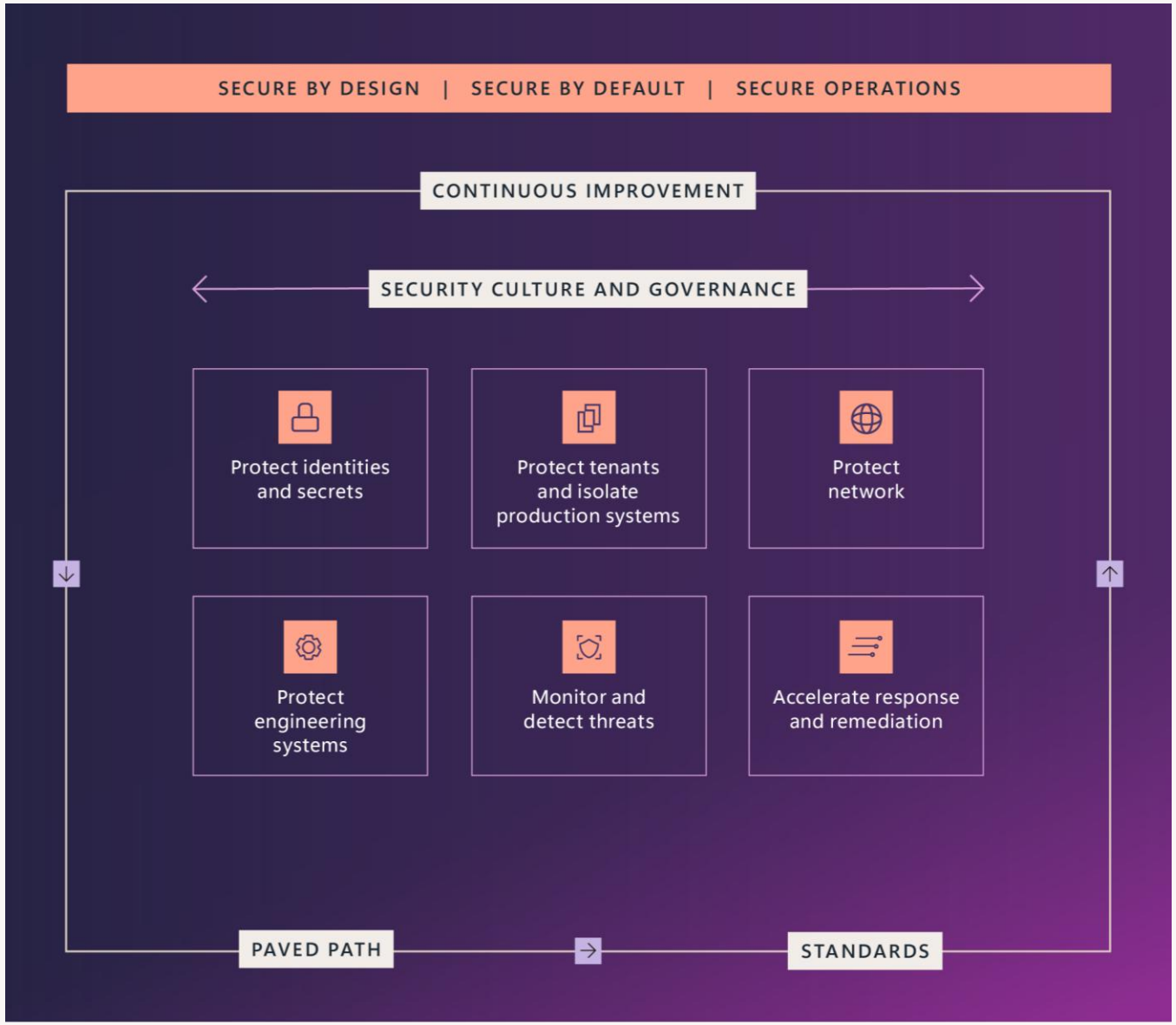
It's our long-term commitment to protect both the company and our customers in the ever-evolving threat landscape.

730k

SFI non-compliant apps eliminated

5.75 million

Inactive tenants eliminated, drastically reducing the potential cyberattack surface



Hierarchy of cybersecurity needs

Drawing inspiration from Maslow's hierarchy of needs, this graphic illustrates a prioritization of cybersecurity, starting with the most basic need: protecting identities. AI has a role at each tier, underscoring its potential to enhance security measures.

Cultivating a robust security culture within the organization, helps ensure the technological defenses and human practices evolve in concert to mitigate threats effectively.

AUTOMATE SECURITY OPERATIONS
Automating security operations is the holistic approach to building on perspectives and insights across all layers in the pyramid.

IMPACT...
Automating processes at scale creates new opportunities for insights as well as relief for stressed defenders.

DETECT AND REMEDIATE THREATS
Monitoring your ecosystem to identify anomalous activity and contain threats.

IMPACT...
The ability to identify and respond quickly can limit lateral movement, contain damage to assets and deny persistence.

SECURE DIGITAL ASSETS
Digital assets, whether code, traditional data stores, and now generative AI models are all key components of modern workloads.

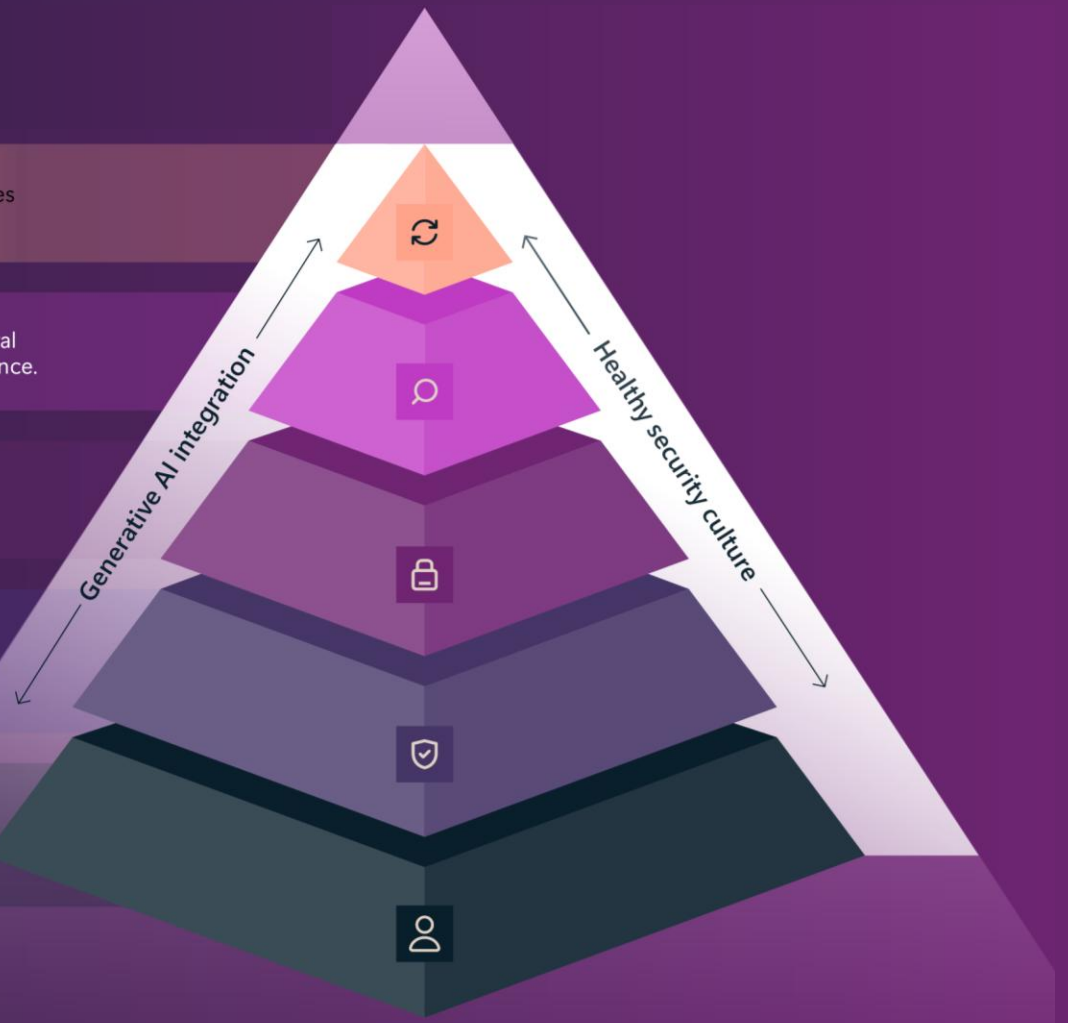
IMPACT...
Modern workloads deliver the value-add to end users who increasingly rely on their integrity and availability.

PROTECT ENDPOINTS
Protected endpoints include the multiple dimensions of devices in use today – from PCs and mobile devices, to network and operational technology (OT), and servers in datacenters.

IMPACT...
Effective endpoint protection can limit the repercussions of unauthorized access.

PROTECT IDENTITIES
"Attackers don't break in, they log in." Credentials for both individuals and machines are the perimeter of the modern attack surface.

IMPACT...
Strong identity security can greatly reduce risk exposure—particularly for ransomware attacks.



Chapter 3

Early insights: Ai's impact on cybersecurity

What do we know about new AI challenges and solutions today?

Nation-state threat actors using AI for influence operations

Adversarial use of AI in influence operations

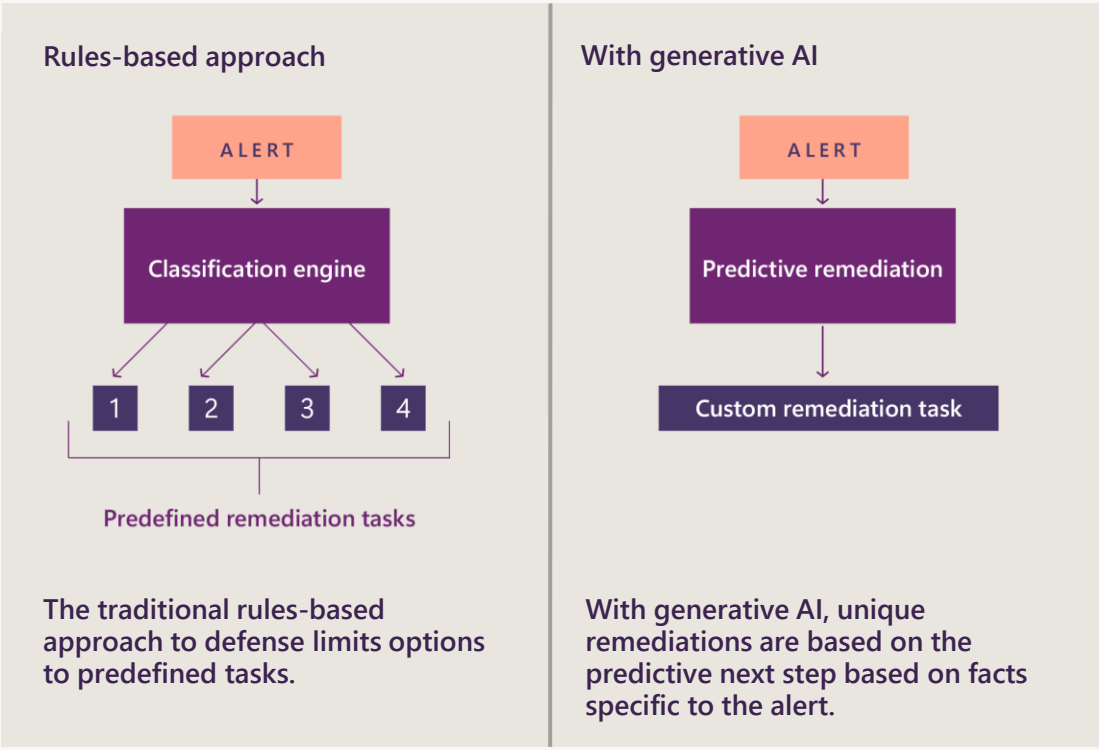
Capability	China	Russia	Iran & proxies
Text	MEDIUM / LOW	MEDIUM / LOW	LOW
Image	HIGH	HIGH	MEDIUM / LOW
Audio/video	HIGH	HIGH	LOW
Example	May 2024: Bespoke Taizi Flood AI-generated cartoon 	June 2024: AI-generated audio of Elon Musk narrating fabricated documentary 	April 2024: Likely AI-generated video leading up to Iranian military operation 

Nation-state threat actor groups, such as those backed by Russia, Iran, and China, are increasingly incorporating AI-generated or enhanced content into their influence operations in search of greater productivity, efficiency, and audience engagement.

AI for defense

Microsoft's significant investment in AI innovation is aimed at providing cybersecurity defenders with an asymmetric advantage over attackers.

Using generative AI to understand cyberattacks and create tailored mitigations



Harnessing AI to detect and disrupt cyberattacks

Detecting hidden attacks with AI

Hands-on-keyboard attacks, where cybercriminals directly interact with compromised systems, are hard to detect.

- LLMs fine-tuned to identify suspicious activities
- Can learn from the context and semantics and flag potential threats

Disrupting attacks by combining endpoint detection and response with AI

AI model alerts when it detects hands-on-keyboard attack.

MDE automatically:

- isolates affected device
- temporarily disables compromised user accounts

Extending AI across cybersecurity

AI models can analyze and find malicious activities using large and complex data sources such as network logs, email communications, web traffic, and social media.

Seven areas of security operations efficiencies

AI can enhance threat detection, response, analysis, and prediction. It can process large volumes of unstructured data to gain insights, answer questions and make informed decisions. Microsoft is leveraging AI in seven key areas in order to support our security operations:

1 **Triaging.** Teams in a security organization receive large volumes of requests and tickets. Depending on the complexity of the logic that determines how these items are dispositioned, AI can help triage some of the items and increase the efficiency and effectiveness of responding teams. Saving at least 20 hours per person, per week.

2 **Prioritizing work items.** Assess the priority of a given item based on how similar items were prioritized in the past.

AI can ensure that the prioritization criteria are up to date with the ever-evolving compliance requirements.

3 **Knowledge gathering from diverse external sources.** Augmenting proprietary in-house datasets with online content. AI can scrape online content and extract security-related information at scale.

One of our internal teams identifies and processes 50 articles per week.

Before: 2 hours per article

With AI: Reports within minutes

4 **Knowledge retrieval.** Integrate information about security policies, best practices, and the remediation actions necessary for compliance. LLMs can generate tailored answers to questions and follow-ups.

5 **Risk assessment.** Assimilate information from diverse sources, to conduct informed risk assessment.

Leverage unstructured organizational knowledge and historical precedents to enrich the set of factors determining risk.

6 **Learning from the past.** Security operations generate large volumes of diverse artifacts (tickets, reports, playbooks). LLMs can ingest data about previous incidents, violations, and remediations to uncover valuable learnings.

7 **Reporting.** Distill artifacts such as documents and slides into reports tailored to the audience and report goal.

Governments and industries advancing global AI security

- There is a consensus on the importance of safety and security in the development, deployment, and use of AI.
- Governments have pursued different approaches in implementing security requirements.

Policy approaches vary in scope and scale

Differences among governments' policy initiatives reflect:

- Core values of the governments' leadership
- Countries' legal and constitutional frameworks
- The state of the technology industry and its potential for future growth.

International standards

International standards can help mitigate the fragmentation of AI security regulation.

- There are two ISO standards (42001 and 27090) that relevant to AI security
- The US government's National Institute of Standards and Technology has a risk management framework and crosswalk that address AI and security intersections

Collaborative policy initiatives for AI security

Organizations around the world are collaborating to advance government policy initiatives on enhanced AI security.

July 2023

- Microsoft, Anthropic, Google and OpenAI launched Frontier Model Forum, an industry body focused on ensuring safe and responsible development of frontier AI models.[63]

August 2023

- The White House announces the AI Cyber Challenge, for cybersecurity researchers to spur the use of AI to identify and fix software vulnerabilities.[64] Microsoft committed to host competition on Microsoft Azure.

November 2023

- The UK launched the world's first safety institute to spur collaboration on AI's safety with leading AI companies and nations.[65]
- The US Department of Commerce, through National Institute of Standards and Technology (NIST) announced the US Artificial Intelligence Safety Institute (USAISI) to lead the US Government's efforts on AI safety and trust, including working with partners in academia, industry, government, and civil society to advance AI safety.[66]
- The Bletchley Agreement for collaboration resulted from an AI Safety Summit convened by the UK and including the US, EU, and China, likeminded AI companies, and 28 country delegations.[67]
- Microsoft contributed to the development of secure AI system guidelines alongside the UK National Cyber Security Centre (NCSC), and the US Cybersecurity and Infrastructure Security Agency (CISA),[68] among others. It was co-sealed by 23 domestic and international cybersecurity organizations. This publication marked a significant step in addressing the intersection of AI, cybersecurity, and critical infrastructure.

January 2024

- CISA's cross-sector analysis of sector-specific AI risk assessments completed by sector risk management agencies. Microsoft provided recommendations through the IT Sector Coordinating Council - a public private partnership for collaboration between IT sector and the Department of Homeland Security (DHS).

February 2024

- The Japanese government launched a new AI Safety Institute within the Information-technology Promotion Agency (IPA) in collaboration with relevant ministries and agencies.[69] The Institute aims to examine evaluation methods and standards related to AI. Japan plans to collaborate with the UK and the US.

March 2024

- The US Department of Treasury released a report on the current state of AI-related cybersecurity and fraud risks in financial services, including an overview of current AI use cases, trends of threats and risks, best-practice recommendations, and challenges and opportunities.[70]

April 2024

- In April 2024, building on the NCSC secure AI development guidelines release in 2023, the US National Security Agency's Artificial Intelligence Security Center published the joint Cybersecurity Information Sheet Deploying AI Systems Securely[71] in collaboration with CISA, the US Federal Bureau of Investigation, the Australian Signals Directorate's Australian Cyber Security Centre, the Canadian Centre for Cyber Security, the New Zealand National Cyber Security Centre, and the United Kingdom's National Cyber Security Centre.
- The US Department of Homeland Security (DHS) released Safety and Security Guidelines for Critical Infrastructure Owners and Operators.[72] Microsoft contributed to the cross-sector risk assessments that informed the DHS guidance.
- Microsoft joined the DHS AI Safety and Security Board (AISSB).[73] The AISSB advises the DHS Secretary, the critical infrastructure community, other private sector stakeholders, and the broader public on the safe, secure, and responsible development and deployment of AI technology in our nation's critical infrastructure.

May 2024

- The second global AI summit secured safety commitments from companies. It is a new agreement[74] between 10 countries and the EU to establish an international network similar to the UK's AI Safety Institute,[75] the world's first publicly backed organization to accelerate the advancement of AI safety science. The network will promote a common understanding of AI safety and align its work with research, standards, and testing. Australia, Canada, the EU, France, Germany, Italy, Japan, Singapore, South Korea, the UK, and the US have signed the agreement.[76]
- Microsoft released a blueprint for mutual prosperity through AI governance in Korea.[77]

June 2024

- Microsoft funded the Securing Critical Infrastructure in the Age of AI workshop led by Georgetown University's Center for Security and Emerging Tech (CSET). CSET will publish a report based on findings from the workshop offering policy recommendations for AI security in critical infrastructure. Expected publication date: September 2024.
- Microsoft hosted and participated in the first federal AI security tabletop exercise led by CISA JCDC.AI,[78] convening more than 50 AI experts from US and international agencies and industry partners focused on effective and coordinated responses to AI security incidents.

Mitigating the most advanced risks in the age of AI

Russia

Forest Blizzard: Research into satellite communications protocols

North Korea

Emerald Sleet: Identify experts focused on Asia-Pacific defense issues

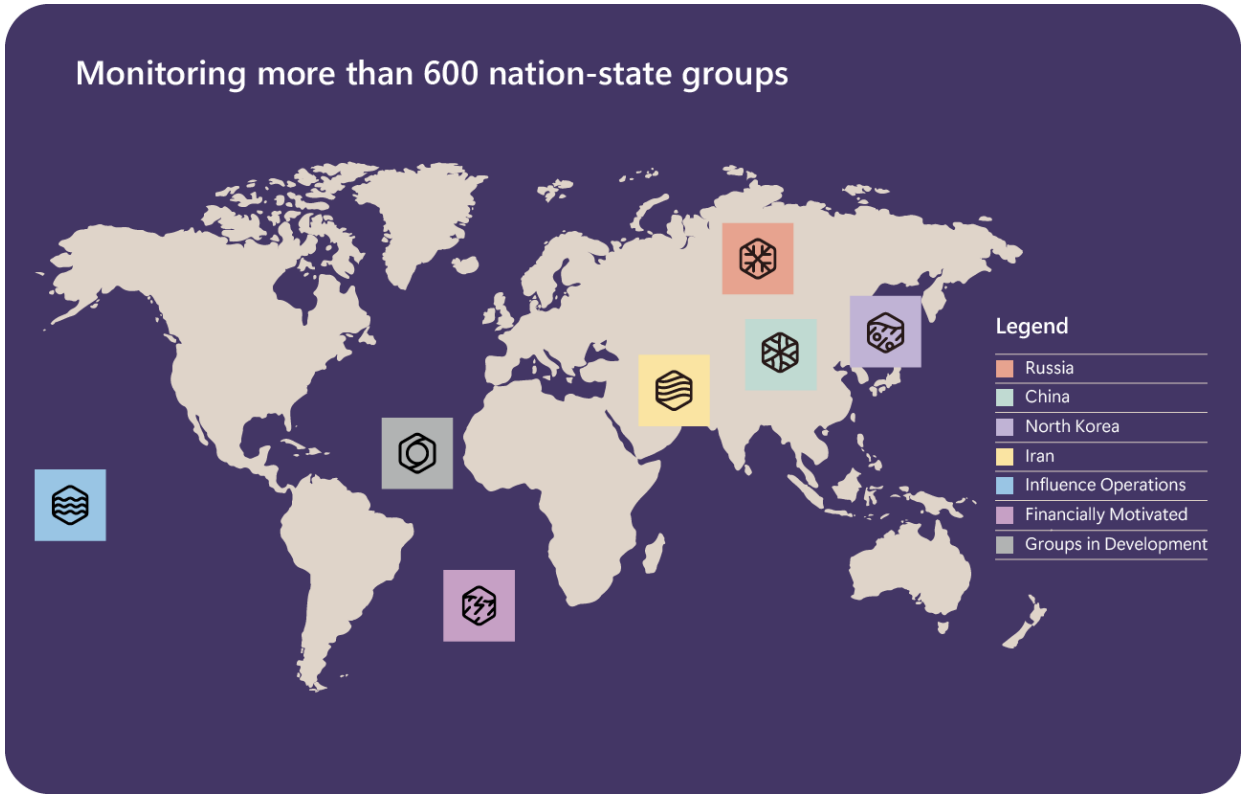
Iran

Crimson Sandstrom: Research ways malware can evade detection

China

Charcoal Typhoon: Create content likely for use in phishing

Salmon Typhoon: Translate technical papers and assist with coding



Microsoft policy to stay ahead of threat actors:

- **Identification and action:** We will disrupt their activities if we detect use of our AI APIs, services or systems by threat actors
- **Notification to other providers:** We will notify other providers if we detect threat actor use of their AI, AI APIs, services, and/or systems
- **Collaboration with other stakeholders:** We collaborate with others to regularly exchange information about detected threat actors' use of AI.
- **Transparency:** We will inform the public and stakeholders about actions taken under these principles, including details on the use of AI within our systems and measures taken against them.

Source: Staying ahead of threat actors in the age of AI (in collaboration with OpenAI). Microsoft Security Blog | February 2024

SECURE FUTURE INITIATIVE ABOVE ALL ELSE

Why Now?

Source: Secure Future Initiative | Microsoft

SECURE FUTURE INITIATIVE

Secure by design | Secure by default | Secure operations

Security culture and governance

Protect identities and secrets

Protect tenants and isolate production systems

Protect network

Protect engineering systems

Monitor and detect threats

Accelerate response and remediation

Continuous improvement

Paved path → Standards

Source: Secure Future Initiative | Microsoft

Agenda

1. Cyber Threat Landscape and AI’s role in Cybersecurity
2. **Innovation and AI trends**
3. Regulatory Compliance
4. Gefion

AI is shifting business today

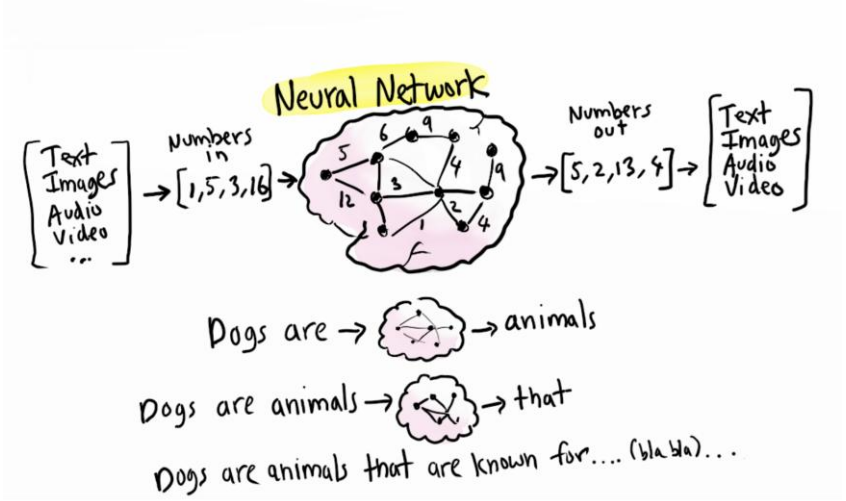
Every
individual

Every
team

Every
industry

Generative AI is a potential paradigm shift

- We are now able to ask a business question in the business language we speak and can expect to get a meaningful response
- Generative AI can be instructed to take on different multimodal tasks, and does not have to be built for specific purposes, greatly reducing time to market and value
- We need to consider adoptability and adaptability, across people, process and technology as a key success criteria because innovation is moving very fast
- **Generative AI and agents offer great flexibility for- and empowerment of employees and opportunities for Danish companies**



Few small examples before we continue …

Video anomalies

Enhancements

Vision
Azure AI Services

I'm observing a series of images that display a concerning situation. A fire is visible, gradually consuming the vegetation in a confined area. The smoke is becoming denser and spreading outwards. The surrounding environment includes some structures and trees, which could potentially be at risk if the fire continues to spread.

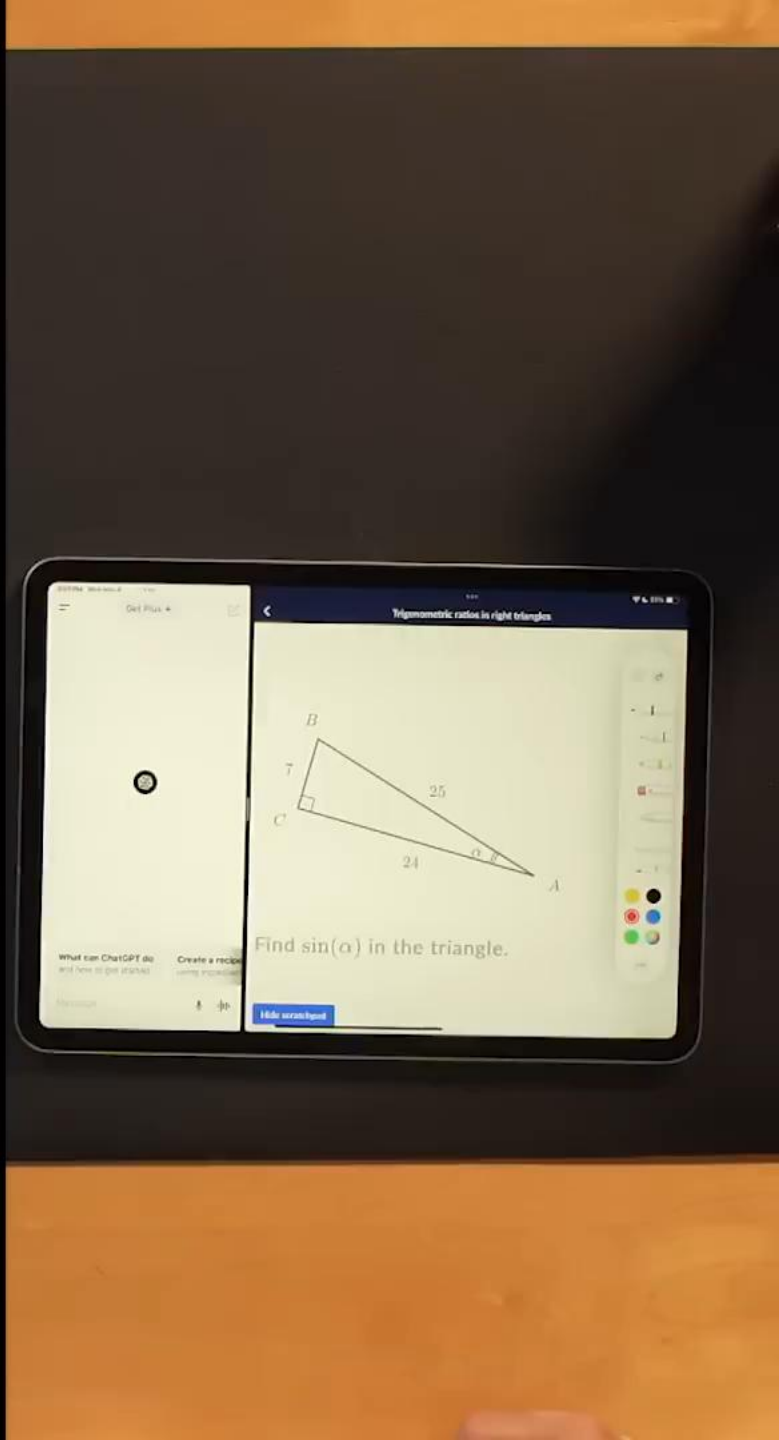
There is no visible intervention or efforts to control the fire at this point. The assessment of the situation should be escalated to ensure that necessary measures are taken to mitigate the risk and secure the area. The origin and cause of the fire are not clear from the images, requiring a thorough investigation.

A close watch on the development of this situation is essential, and immediate action is needed to prevent any potential damage to property or threat to safety. The relevant authorities should be alerted to address this anomaly promptly.

Video insurance

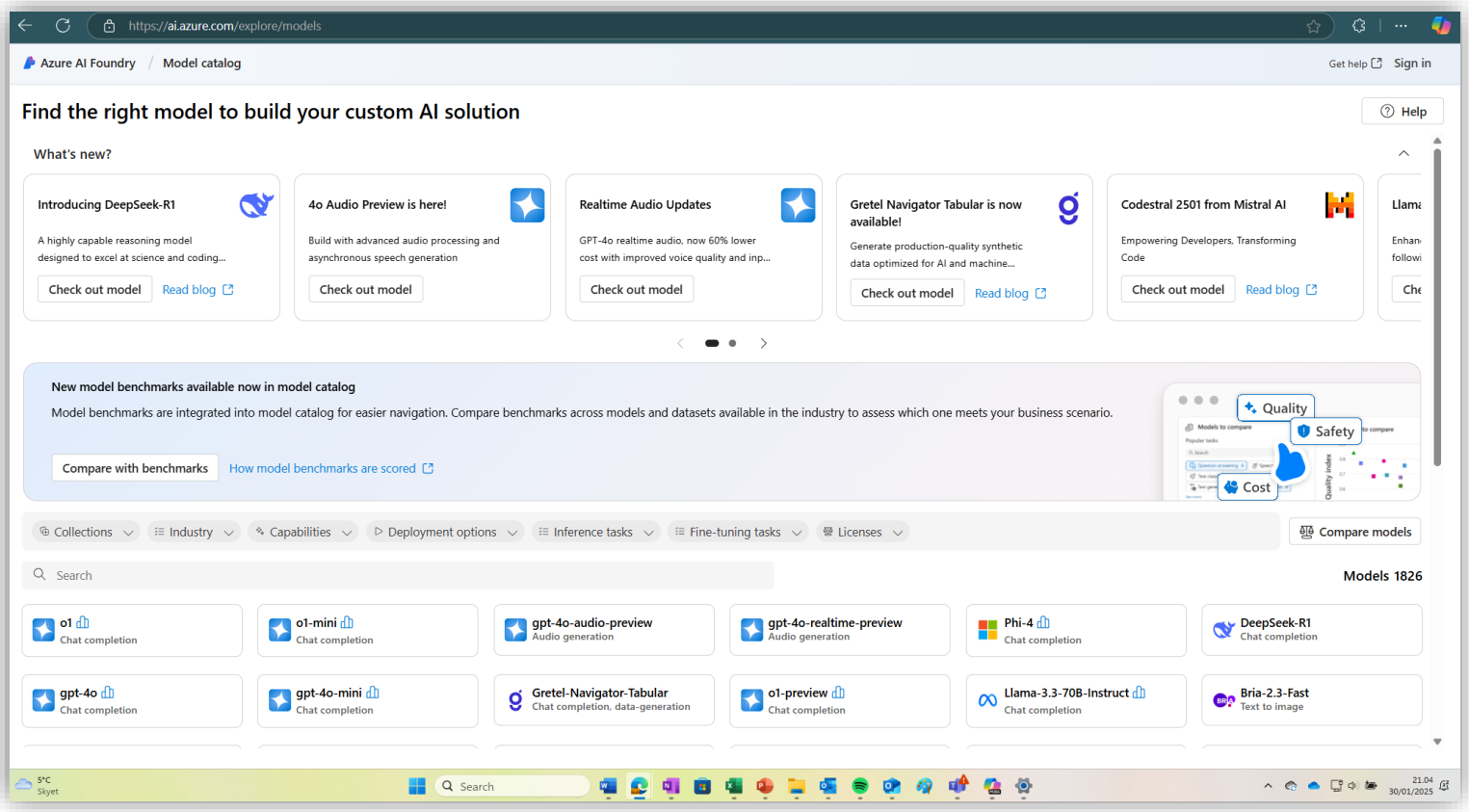
Enhancements

Vision
Azure AI Services


Trigonometric ratios in right triangles
B
7
25
C
24
A
Find sin(α) in the triangle.
Hide scratchpad

Azure AI Foundry

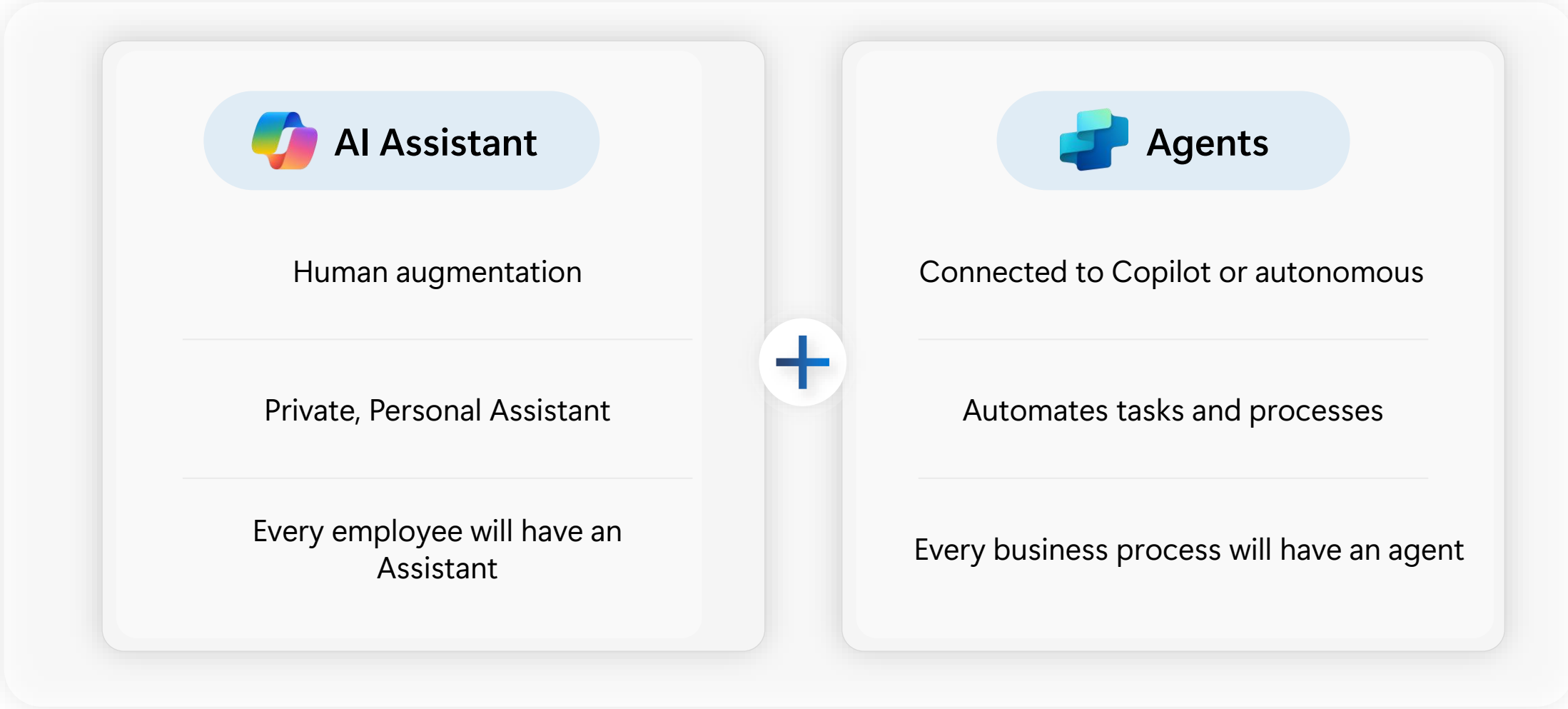
Find the right model to build your custom AI solution



Develop and deploy custom AI apps and APIs responsibly with a comprehensive platform

[Model catalog - Azure AI Foundry]

Generative AI and agents – Not products, but concepts and terminology



AI Assistant

1. Consistent UI for AI
2. Integrated in the tools millions use every day
3. Platform for agents and extensibility
4. Enterprise-grade security, privacy, and compliance
5. Flexible purchasing and deployment options
6. Measure AI impact and business value

There are also concerns – Top security and governance concerns about generative AI

Data oversharing and data leaks

80%

of leaders cited leakage of sensitive data as their main concern[1]

Identification of risky AI use

41%

of security leaders cited that the identification of risky users based on queries into AI was one of the top AI controls they want to implement[2]

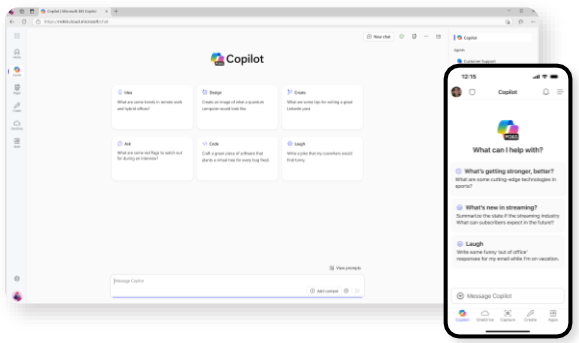
AI governance and risk visibility

84%

Want to feel more confident about managing and discovering data input into AI apps and tools[2]

1. First Annual Generative AI study: Business Rewards vs. Security Risks, Q3 2023, ISMG, N=400
2. Microsoft data security index 2024 report

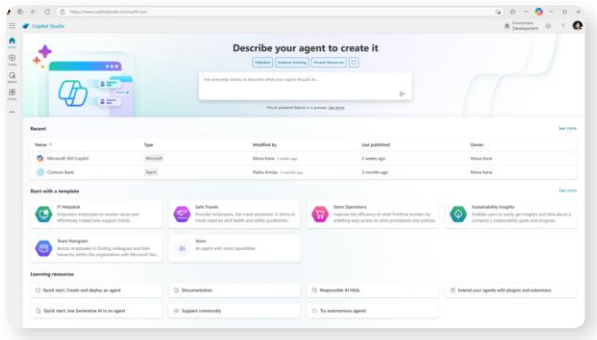
Agent enabled AI Assistants



AI Assistant

Private, Personal Assistant,
Human augmentation

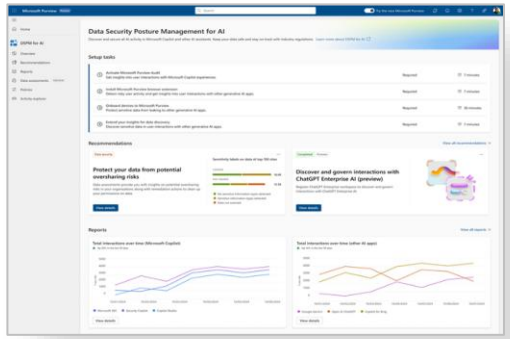
+



Agents

Integrated into the experience

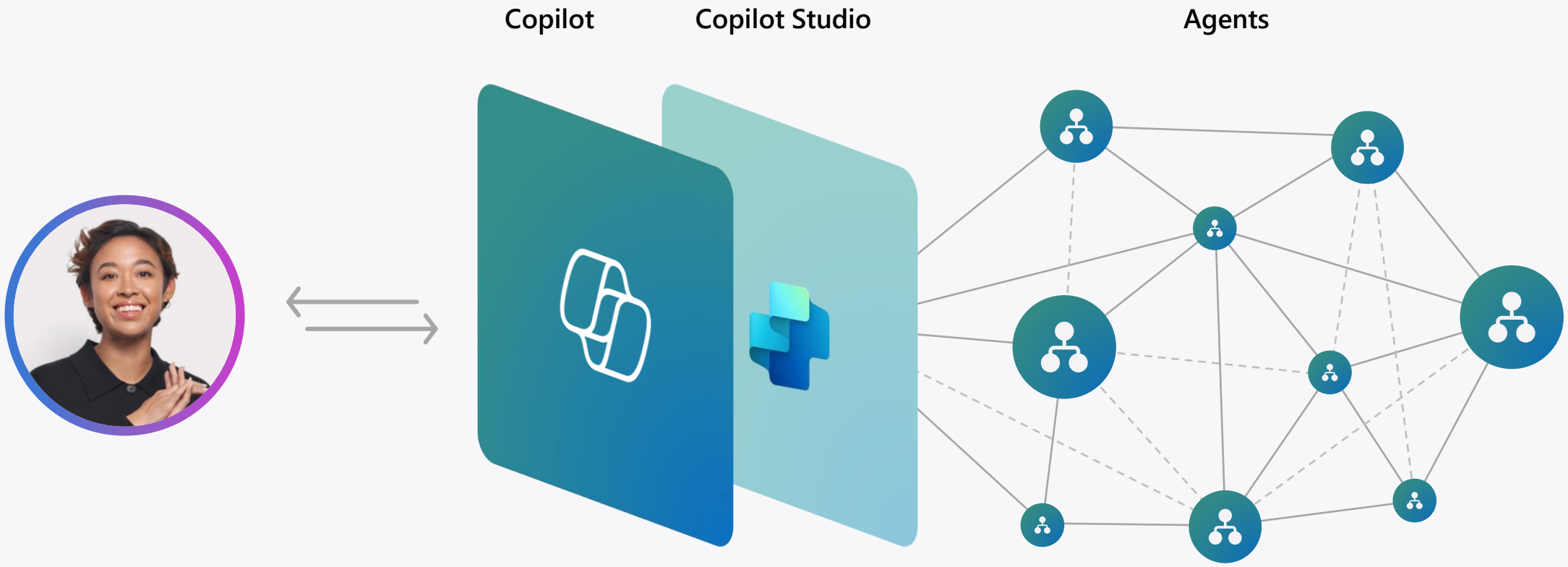
+



IT Controls

Enabling Enterprise Data Protection
and agent management

A UI for AI


Copilot
Copilot Studio
Agents
Data access, governance, Agent management and outcome measurement

Example Agents

Agents in SharePoint

Generally available

Employee Self-Service Agent

Private preview

Facilitator

Public preview

Interpreter

Public preview early 2025

Project Manager

Public preview

Generative AI and Agent focus areas

- **Explosion in available Agents**
- Larger groups of models, both large and small
- Model modality capabilities
- **AutoGen – Agents to solve interdisciplinary, complex challenges**
- O1 models for complex reasoning
  - Reinforcement learning and chain-of-thought
  - Domain specific models
- Industries
- **Agent Tooling and platforms**
- Studios and AI Foundry platform
- Simplified architectures to drive adoption of AI
- Copilot and Agent architecture enhancements

- Further out
- **AI generated Agents**
- Quantum computers training models

Agenda

1. Cyber Threat Landscape and AI’s role in Cybersecurity
2. Innovation and AI trends
3. **Regulatory Compliance**
4. Gefion

AI models

1. Your data is your data
2. Your data is not used to train or enrich foundation AI models
3. Your data and AI models are protected at every step
4. Our Customer Copyright Commitment

EU AI Act - Staggered Enforcement Timeline

Effective
February 2, 2025
Prohibited practices,
AI Literacy

Effective
August 2, 2025
GPAI models, including
those with systemic risk

Effective
August 2, 2026
High-risk AI systems,
Transparency obligations

Regulated actors

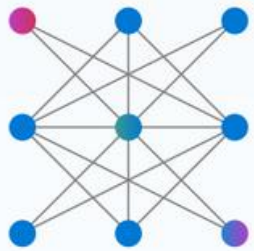
Provider
Developer of high-risk AI systems and GPAI models

Deployer
Operator of high-risk system built by provider

Distributor
Sellers of high-risk system built by a third-party provider

Importer
Sellers of high-risk system from a third-countr y

Regulated technologies



AI systems
Machine-based systems operating with varying autonomy levels that generate predictions, content, or decisions that can impact physical or virtual environments

General Purpose AI (GPAI) models
General Purpose AI (GPAI) models are capable to competently perform a wide range of distinct tasks

Our approach to the EU AI Act

60+ related regulatory efforts

Establish cross-functional working groups

Innovation & compliance

Policy engagement

Microsoft is collaborating with the EU AI Office and Member State authorities, sharing insights, addressing open questions, and advocating for practical solutions.

Internal preparation

AI governance, engineering, legal, and policy experts collaborate to update internal standards and practices, and ensure technology readiness.

Customer support

Microsoft is committed to sharing our compliance journey and helping customers continue to innovate and meet EU AI Act obligations.

How customers can prepare

Evaluate your AI use cases to understand how the AI Act applies and seek legal guidance.

1

Understand your AI footprint

Review the EU AI Act to understand its impact on your role, models, and systems.

2

Review your AI governance

Prepare your framework to meet the AI Act's requirements for responsible AI development and deployment, if applicable.

3

Engage in regulatory process

Engage with policymakers and industry groups to track evolving requirements as new regulations and guidelines are introduced.

Responsible AI Transparency Report

How we build generative AI applications responsibly

How we make decisions about releasing generative AI applications

How we support our customers as they build generative AI applications

How we learn, evolve and grow

Agenda

1. Cyber Threat Landscape and AI’s role in Cybersecurity
2. Innovation and AI trends
3. Regulatory Compliance
4. **Gefion**

Denmark’s first AI supercomputer is now operational

- Gefion is an NVIDIA DGX SuperPOD AI supercomputer, powered by 1,528 NVIDIA H100 Tensor Core GPUs and interconnected using NVIDIA Quantum-2 InfiniBand networking
- Gefion is the result of a public-private partnership between the Novo Nordisk Foundation and the Export and Investment Fund of Denmark (EIFO)
- Fist projects are:
  - “Large-scale distributed simulation of quantum algorithms for quantifying molecular recognition processes.”, University of Copenhagen
  - “Unravelling CO2 reduction in Non-Metal Formate Dehydrogenase (FDH) using Machine-Learned Force Fields.”, Technical University of Denmark
  - “Multimodal genomic foundation model”, University of Copenhagen
  - “Multi-Modal Document Understanding: Transforming Data Entry with Multi-Modal Precision.”, Go Autonomous
  - “Building an AI Care Companion with Large Video Pretraining.”, Teton and the University of Copenhagen
  - “SAPIEN – Skilful Atmospheric Prediction with Intelligent Environmental Networks.”, Danish Meteorological Institute

Thank you!