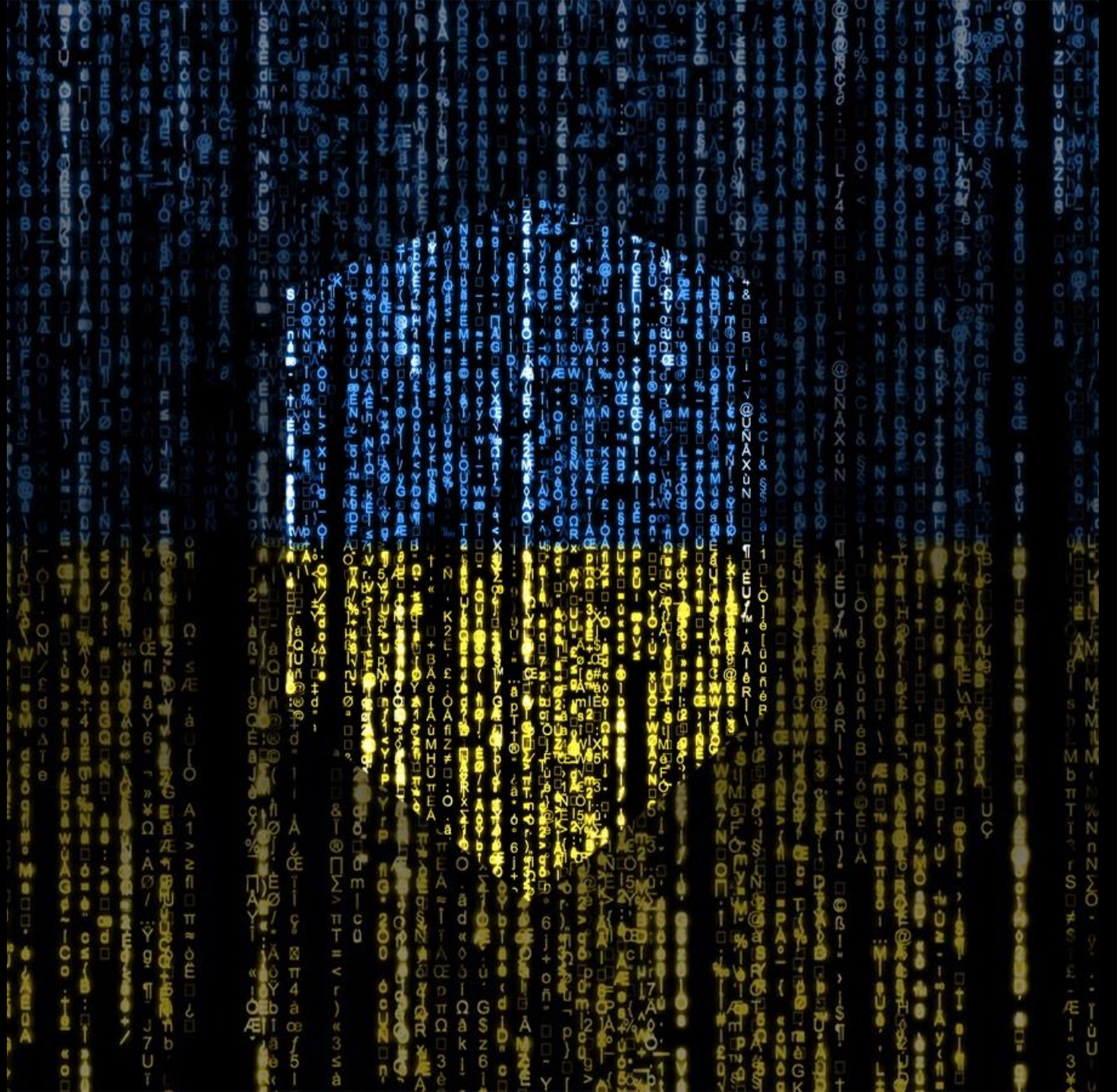
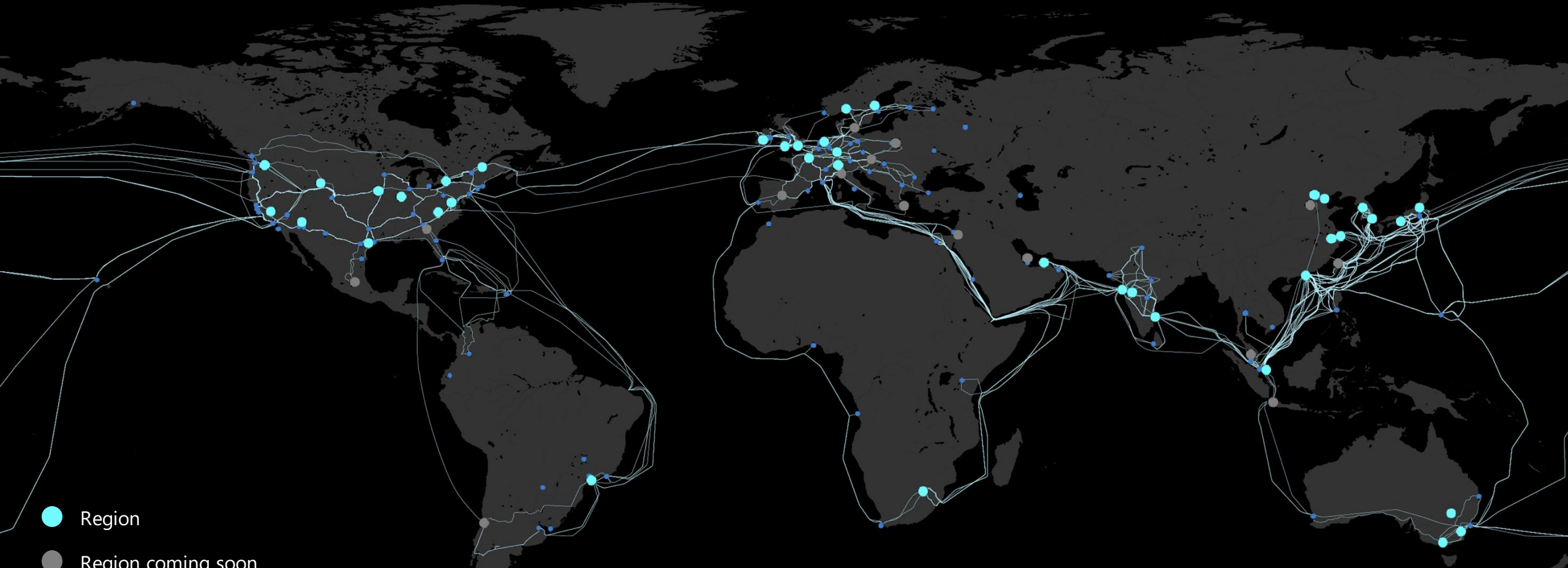


Microsoft Säkerhet i en AI-värld

Sandra Barouta Elvin,
Nationell Säkerhetschef



Microsoft Cyberspace



- Region
- Region coming soon
- Network PoPs

70+

regions
worldwide

250K+

miles of fiber
and subsea cable

85T+

Security Signals Per
Day

10K+

Security and threat
intelligence experts

1M+

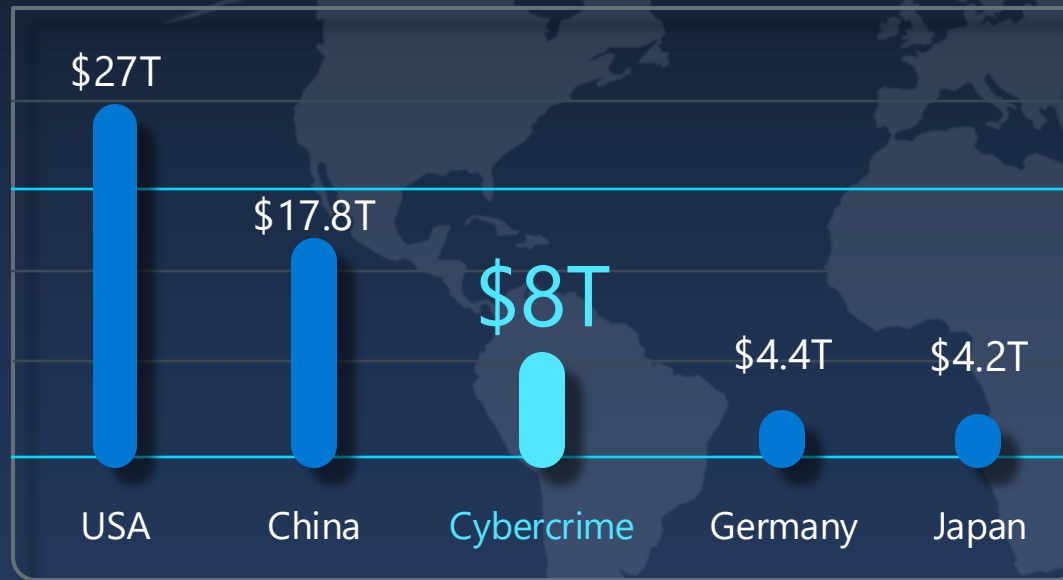
Security Customers

15K+

Security Partners

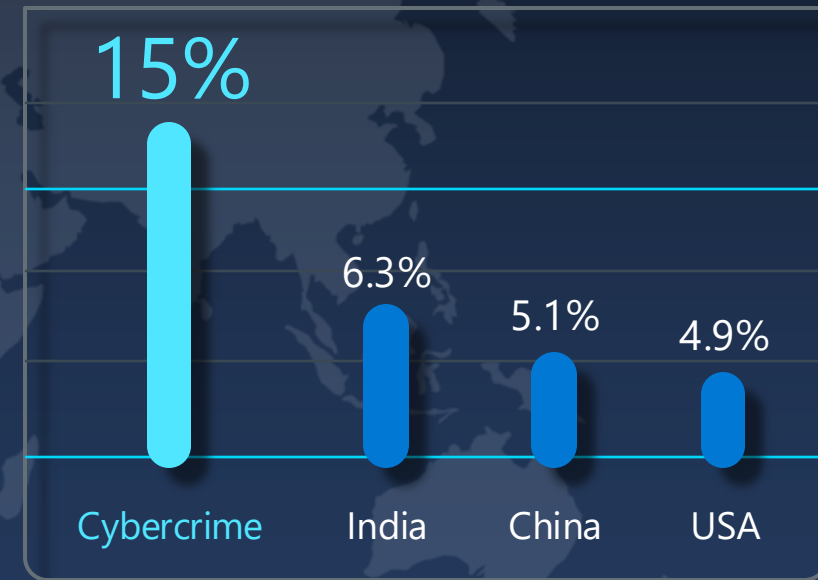
Cybercrime today equals the 3rd largest economy in the world and growing fast

Annual GDP



Source: Statista

GDP annual growth rate



Source: Statista

Security is a about managing risk

Confidentiality



- Unauthorized internal access
- Unauthorized antagonistic access

Integrity



- Intentional corruption of data
- Unintentional corruption of data

Availability



- Accidental incidents
- Antagonistic attacks
- Ransomware
- Total defense

Digitalization is not a choice



It is a necessity



More efficient
technology-enabled
operations



AI-managed smart
grids enable the
intelligent flow of
energy and data



Improved operational
predictability as well
as assist in meeting
emissions targets



More accurate
forecasting and
prediction,
harmonizing fossil fuel
and renewable energy
provision

... but the risks can be high

DYLAN FUETT	BERNARD PARKER
Prior Offense 1 attempted burglary	Prior Offense 1 resisting arrest without violence
Subsequent Offenses 3 drug possessions	Subsequent Offenses None
LOW RISK 3	HIGH RISK 10



Allegheny Family Screening Tool



Adversaries will use GenAI in creative ways

Malware generation



Customizing exploits



Phishing and social engineering



Command and control communication



Automated vulnerability discovery



Password cracking



Disguising malicious code



Deepfakes: data, email, voice



How can we protect against 99% of attacks?



Fundamentals
of cyber hygiene

99%

Basic security hygiene
still protects against
99% of attacks.

How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.¹



Enable multifactor authentication (MFA)



Apply Zero Trust principles



Use extended detection and response (XDR) and antimalware



Keep up to date



Protect data

← Outlier attacks on the bell curve make up just 1% →

Digitalization vs. electrification

1870 - Thomas Edison builds the first direct current (DC) generator



1878 - British scientist, Joseph Swan, patents the first electric lamp



1883 - Magnus Volk builds the first electric railway in Brighton



1876 - Alexander Graham Bell invents the telephone, which uses electricity to transmit speech



1881 - First public electricity supply is generated in Godalming, Surrey, using a waterwheel at a nearby mill



Digitalization complicating security operations

- IT Security

- Protecting information technology
- Focusing on technical security

- Digital security

- Protecting against digital threats
- Focusing on securing digital information and processes



Malware



Network intrusion



Cybercrime/
fraud



Data breach



Unauthorized
system access



Phishing



Identity theft



Privacy breach



DoS/DDoS











Cyber
espionage



Disinformation

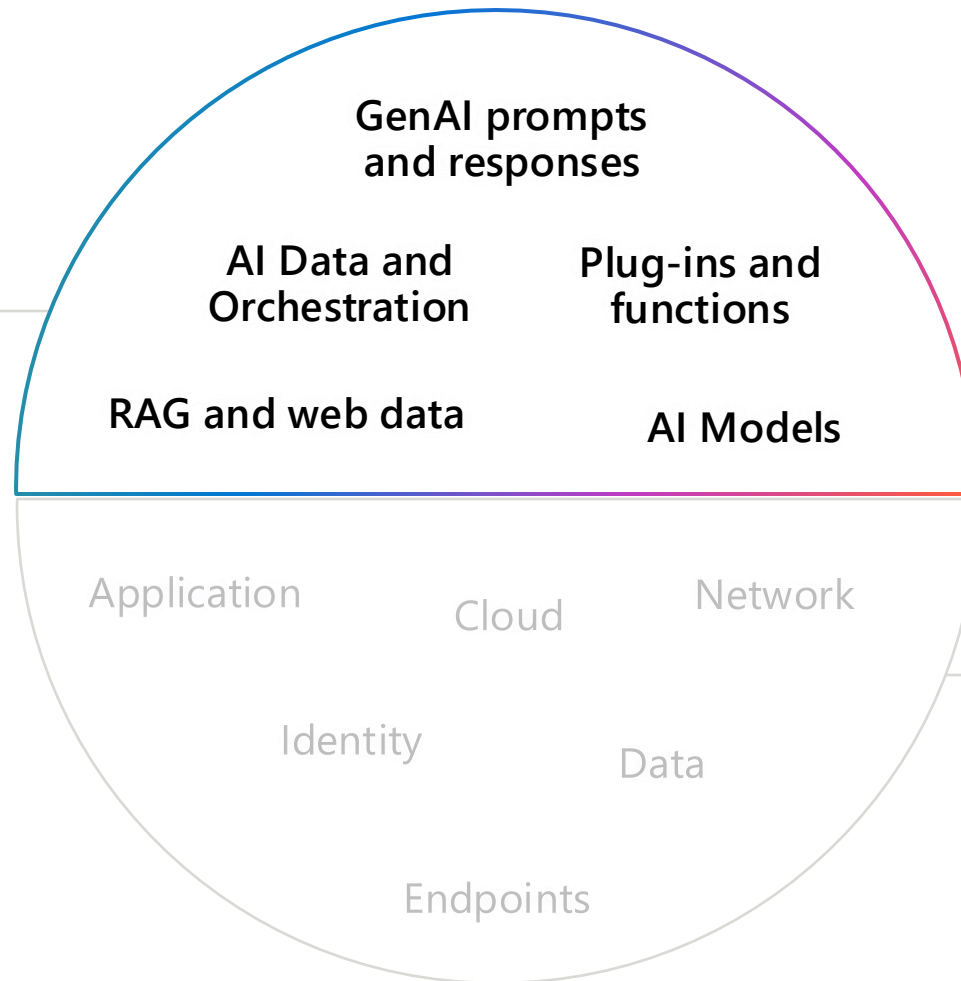
The risk management matrix, shared responsibility

	On-Prem	IaaS	PaaS	SaaS
 Users	●	●	●	●
 Data classification	●	●	●	●
 Client protection	●	●	●	●
 Identity & access protection	●	●	●	●
 Application controls	●	●	●	●
 Network protection	●	●	●	●
 Server security	●	●	●	●
 Physical security	●	●	●	●

● Customers ● Suppliers

We should also expect adversaries to target GenAI

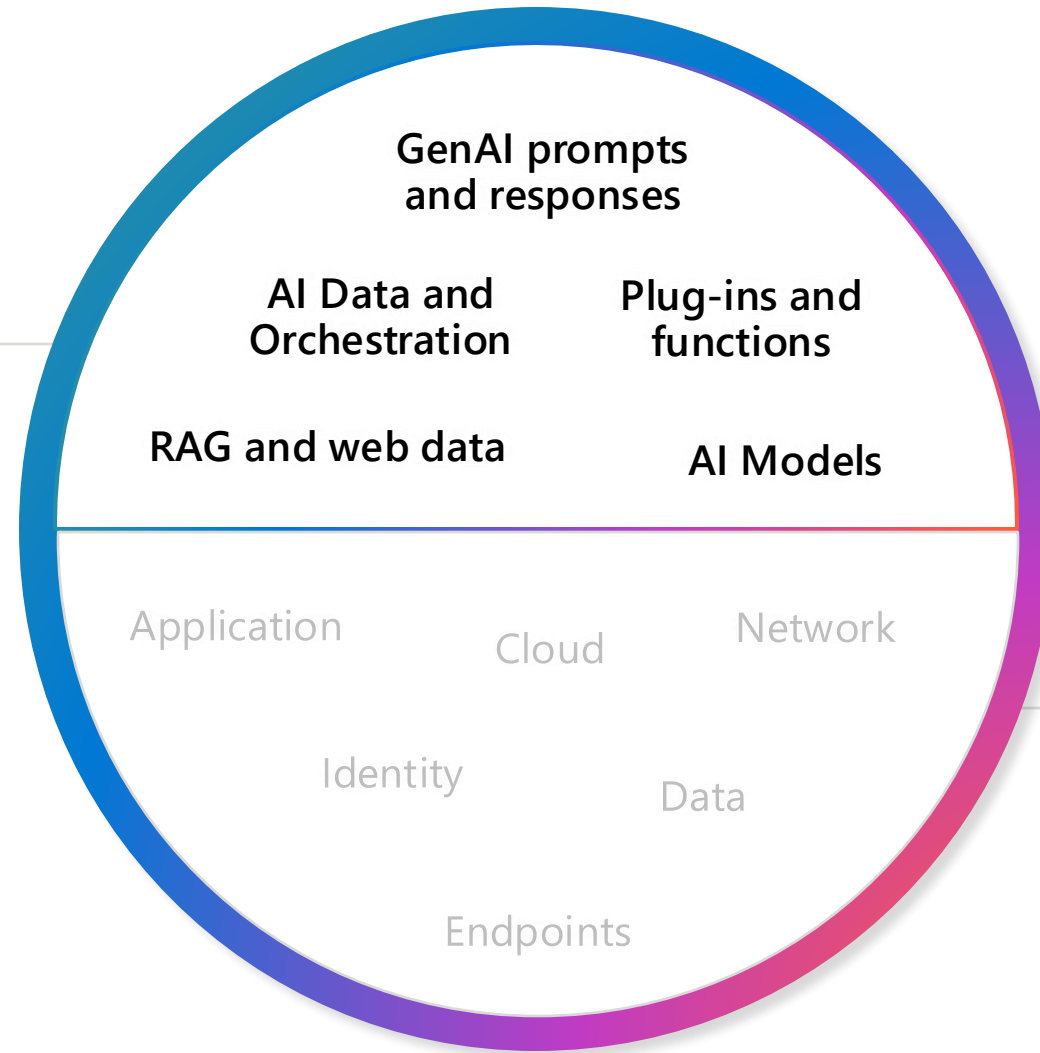
**New GenAI
attack surfaces**



**Traditional
threat vectors**

We have to protect it all comprehensively

New GenAI
attack surfaces



Traditional
threat vectors

Security for AI shared responsibility model

IaaS (BYO model)

PaaS (Azure Open AI)

SaaS (Copilot)



AI usage

User training, identity & access, data security & governance



AI application

Plugins, design, infrastructure, safety systems



AI platform

Model safety, accountability, tuning, design, training data governance

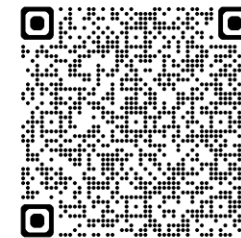


Organization



Microsoft

Microsoft Responsible AI Standard, v2



Secure by Design

Secure by Default

Secure Operations

Security culture and governance



Accountability

- Impact assessment
- Oversight of significant adverse impacts
- Fit for purpose
- Data governance and management
- Human oversight and control



Transparency

- System intelligibility for decision making
- Communication to stakeholders
- Disclosure of AI interaction



Fairness

- Quality of service
- Allocation of resources and opportunities
- Minimization of stereotyping, demeaning, and erasing outputs



Reliability & Safety

- Reliability and safety guidance
- Failures and remediations
- Ongoing monitoring, feedback, and evaluation



Privacy & Security

- Privacy Standard compliance
- Security Policy compliance



Inclusiveness

- Accessibility Standards compliance

Continuous improvement

Paved path

Standards

Thank you!



sandra.elvin@microsoft.com



[@sandrabarouta](https://twitter.com/sandrabarouta)



[linkedin.com/in/sandrabaroutaelvin/](https://www.linkedin.com/in/sandrabaroutaelvin/)