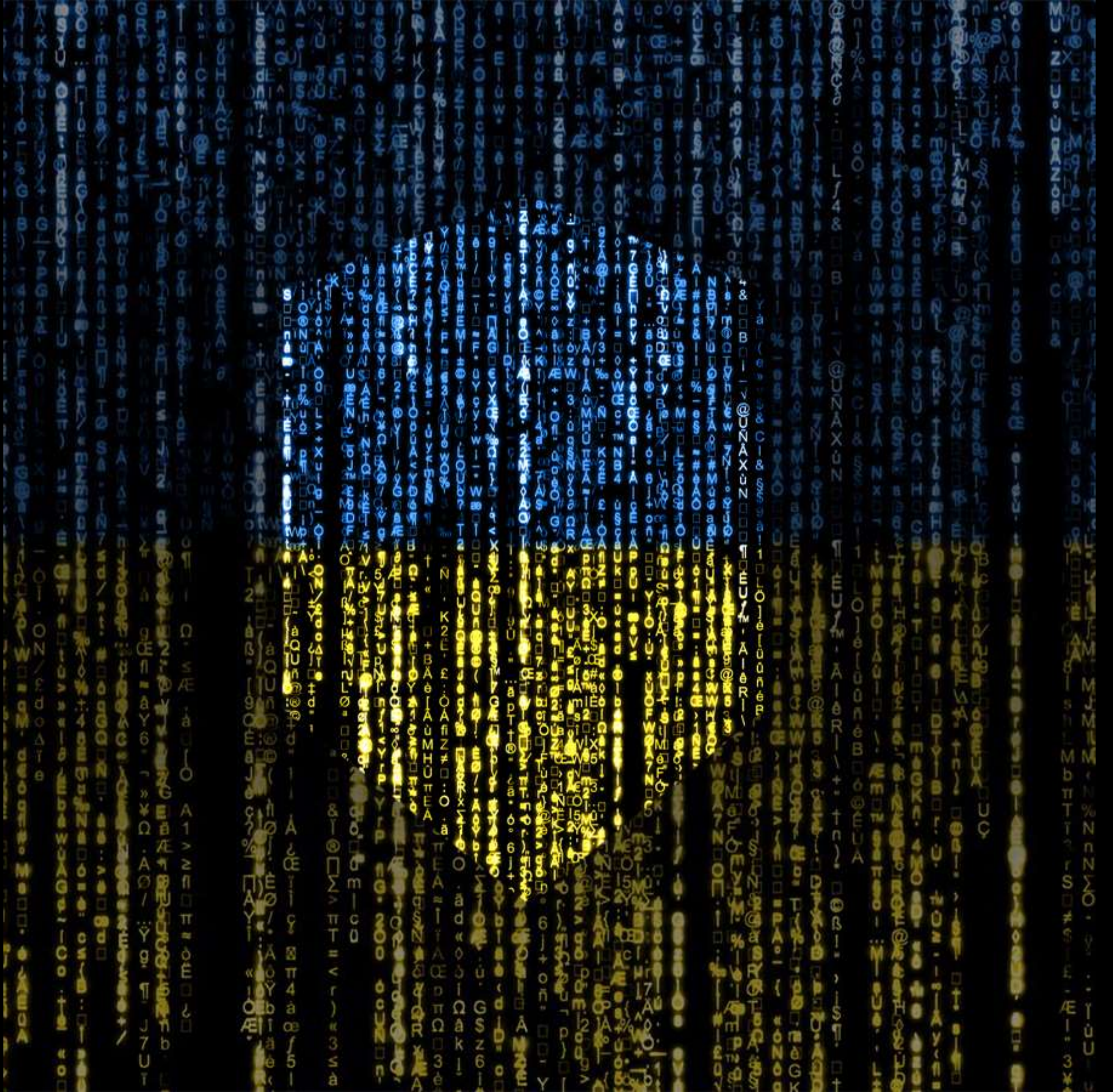
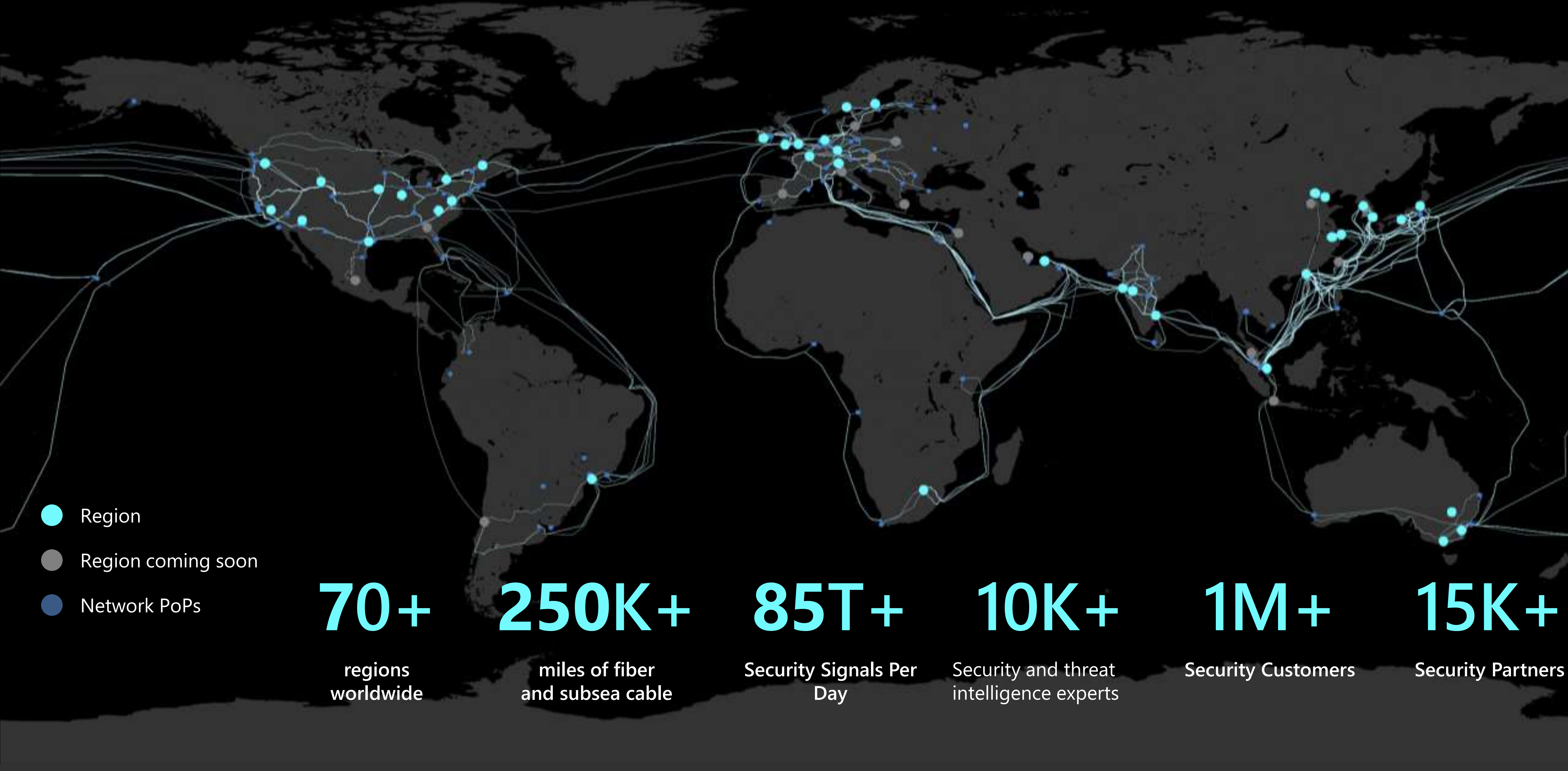
Microsoft

Säkerhet i en AI-värld

Sandra Barouta Elvin,
Nationell Säkerhetschef



Microsoft Cyberspace



70+
regions worldwide

250K+
miles of fiber and subsea cable

85T+
Security Signals Per Day

10K+
Security and threat intelligence experts

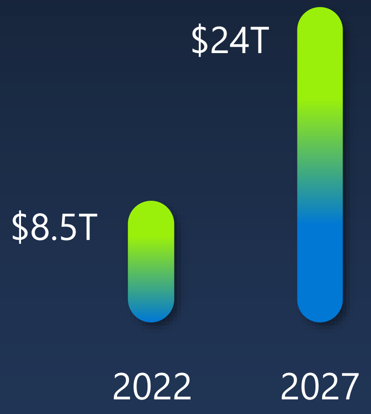
1M+
Security Customers

15K+
Security Partners

Azure global infrastructure | https://infrastructuremap.microsoft.com

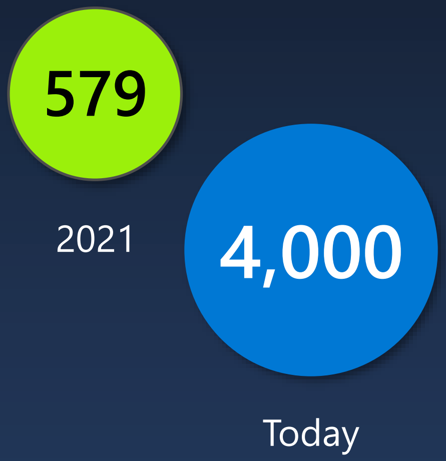
The odds are against defenders

Cost of cyberattacks (USD)



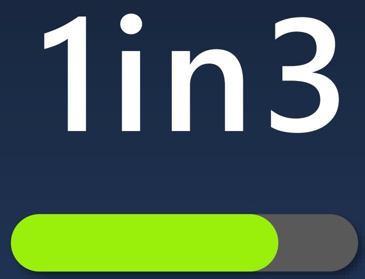
Source: Statistica

Password attacks per second



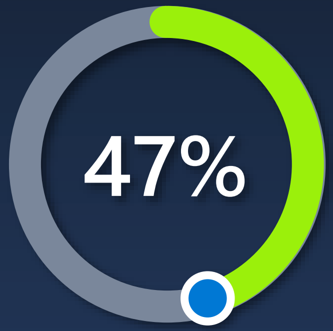
Source: Microsoft

Open cybersecurity jobs in the U.S.



Source: Cyberseek

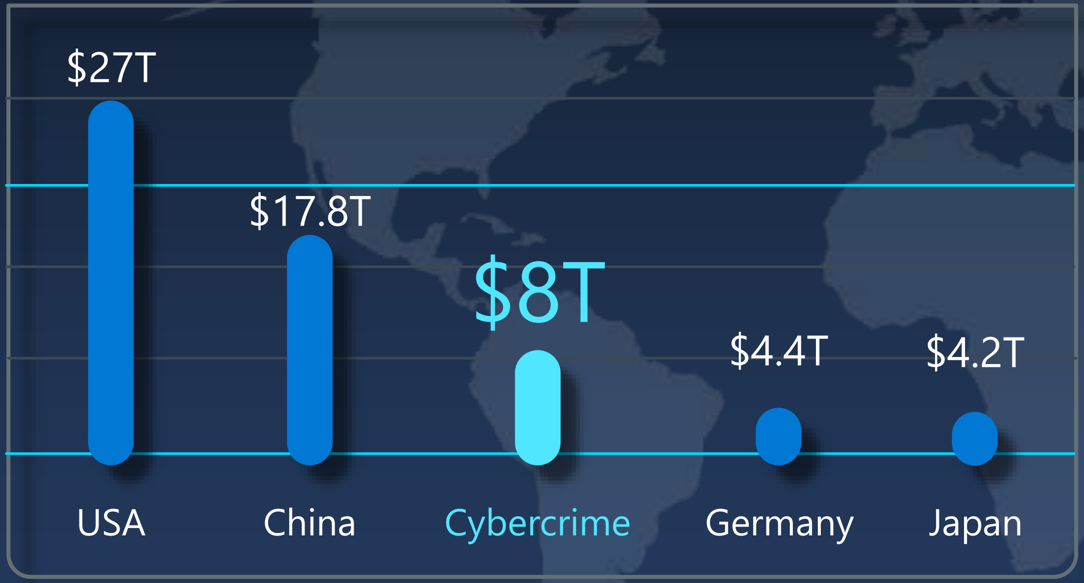
Increase in phishing attacks, driven by attack use of AI



Source: Zscaler

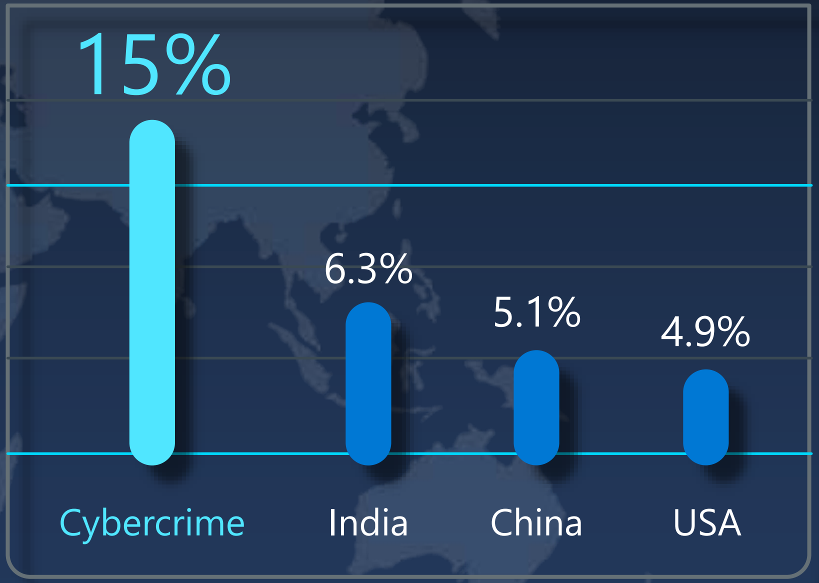
Cybercrime today equals the 3rd largest economy in the world and growing fast

Annual GDP



Source: Statistica

GDP annual growth rate



Source: Statistica

INFORMATION SECURITY

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

Digitalization complicating security operations

IT Security

- Protecting information technology
- Focusing on technical security

Malware

Network intrusion

Unauthorized system access

Phishing

DoS/DDoS

Digital security

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

Cybercrime/ fraud

Data breach

Identity theft

Privacy breach

Cyber espionage

Disinformation

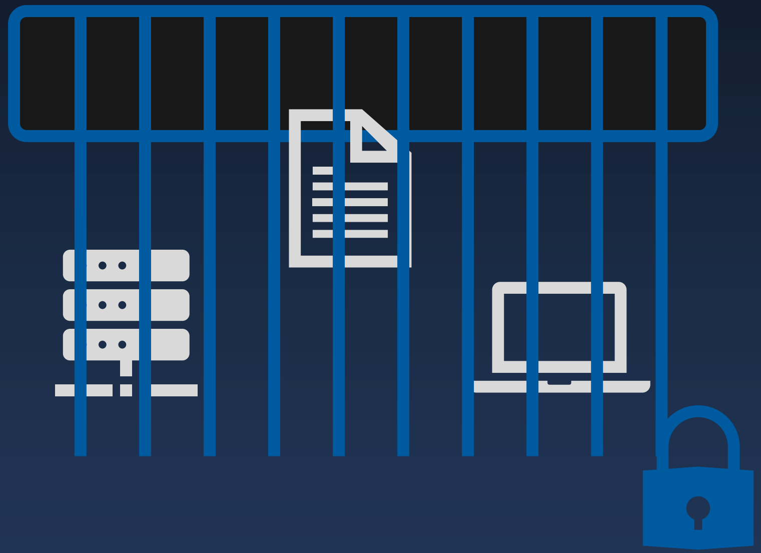
The risk management matrix

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

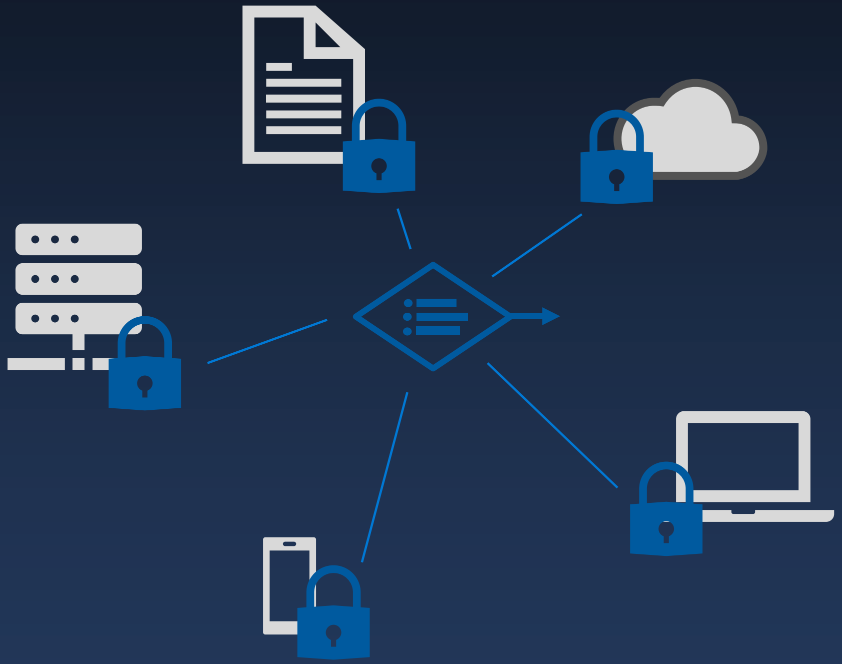
⚪ **Suppliers**

🔵 **Customers**

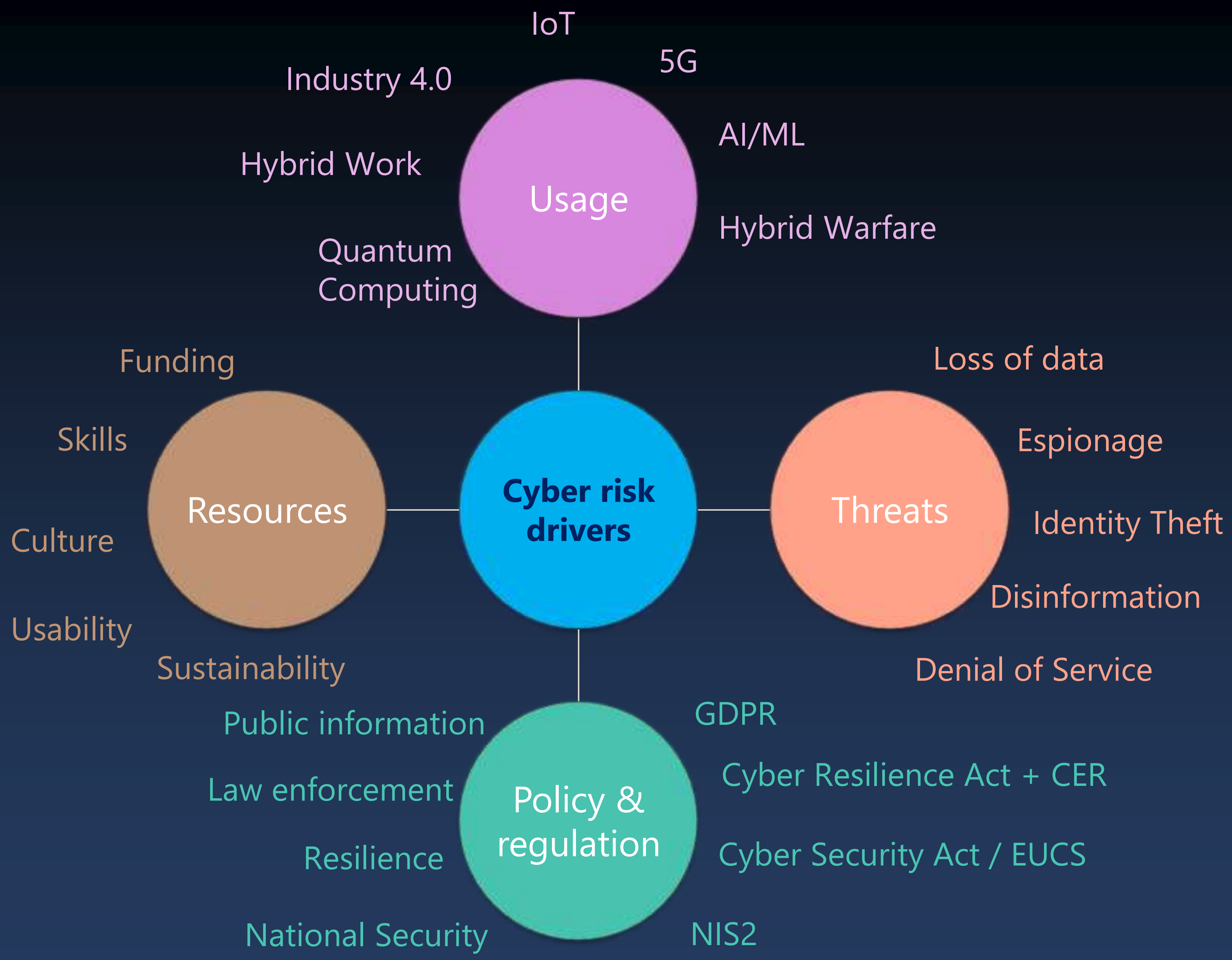
Zero Trust: security past the firewall



Classic Approach – Restrict everything to a 'secure' network



Zero Trust – Protect assets anywhere with central policy



Cyber risk drivers

Usage

IoT

5G

Industry 4.0

AI/ML

Hybrid Work

Hybrid Warfare

Quantum Computing

Resources

Funding

Skills

Culture

Usability

Sustainability

Threats

Loss of data

Espionage

Identity Theft

Disinformation

Denial of Service

Policy & regulation

Public information

GDPR

Law enforcement

Cyber Resilience Act + CER

Resilience

Cyber Security Act / EUCS

National Security

NIS2

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

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.

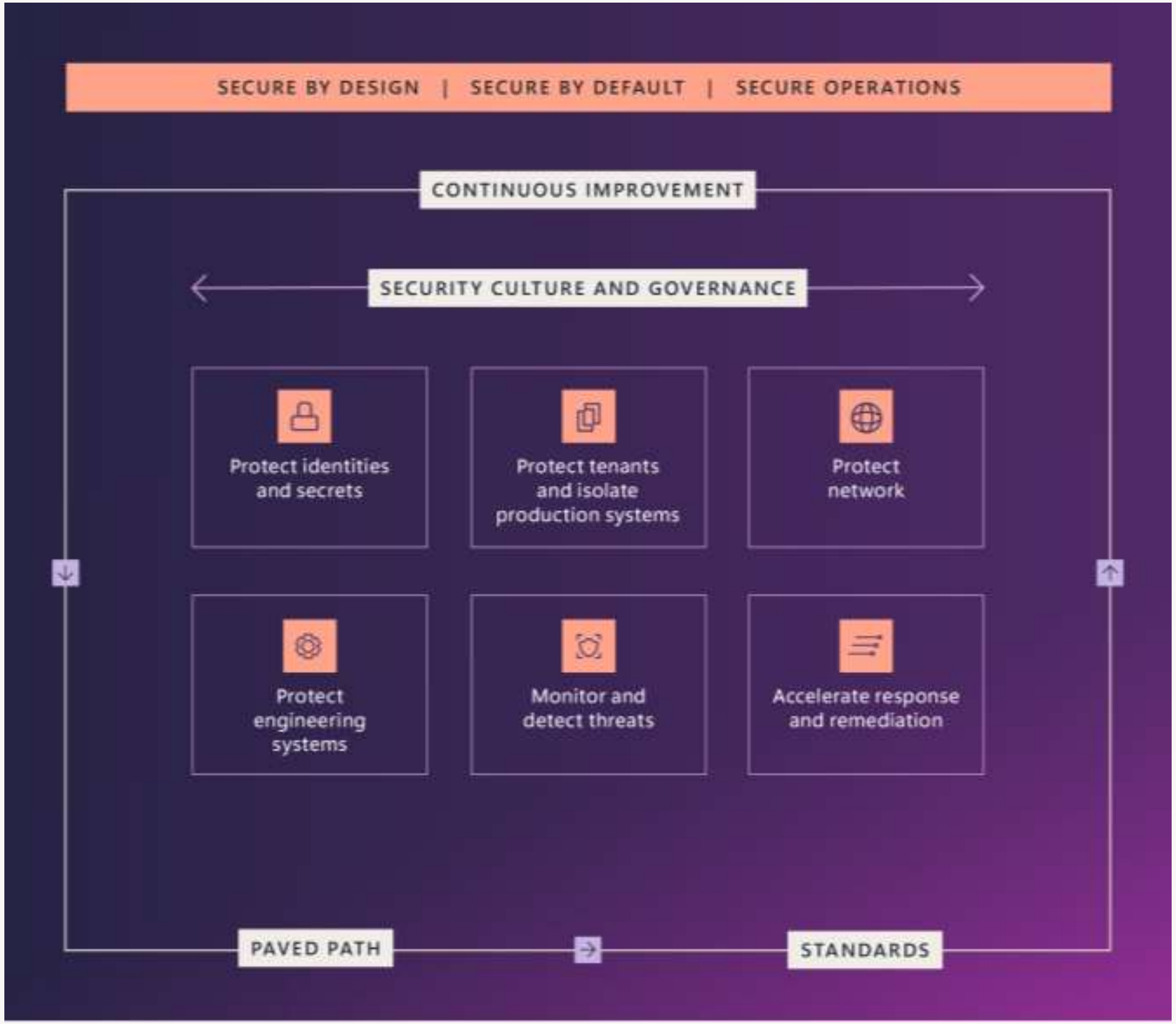
It's our long-term commitment to protect both the company and our customers in the ever-evolving threat landscape.

730k

SFI non-compliant apps eliminated

5.75 million

Inactive tenants eliminated, drastically reducing the potential cyberattack surface



SECURE BY DESIGN | SECURE BY DEFAULT | SECURE OPERATIONS

CONTINUOUS IMPROVEMENT

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

PAVED PATH

STANDARDS

The benefits of AI are real

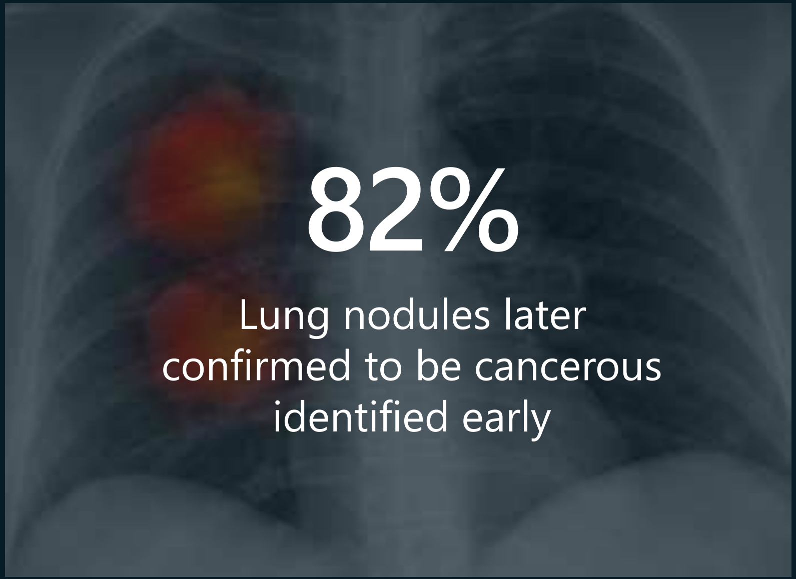
1 in 10

Cars expected to be self-driving by 2030

PROGRESSIVE

$10M

Annual saving with AI chatbots



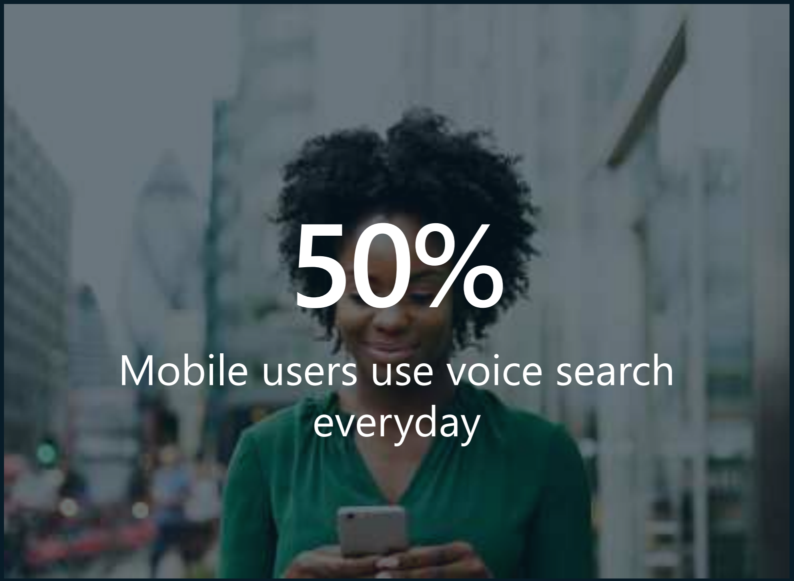
82%

Lung nodules later confirmed to be cancerous identified early

STRABAG

80%

accuracy in identifying projects at risk



50%

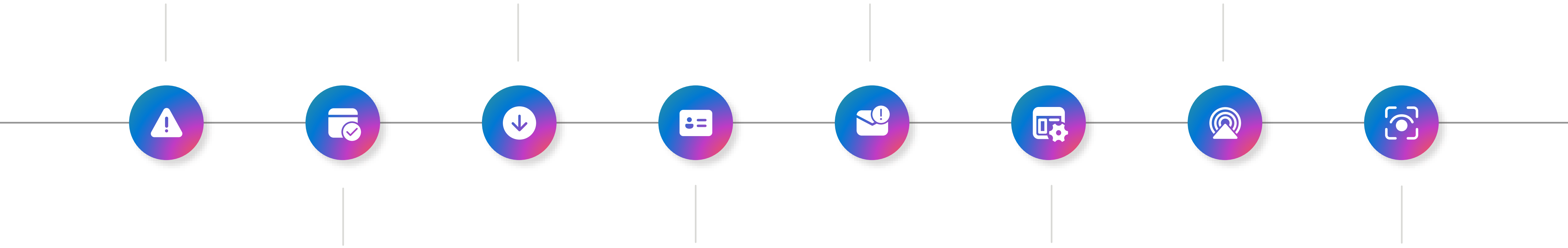
Mobile users use voice search everyday

CARMAX

11 years

worth of work done in days

Adversaries will use GenAI in creative ways



Malware generation

Automated vulnerability discovery

Customizing exploits

Password cracking

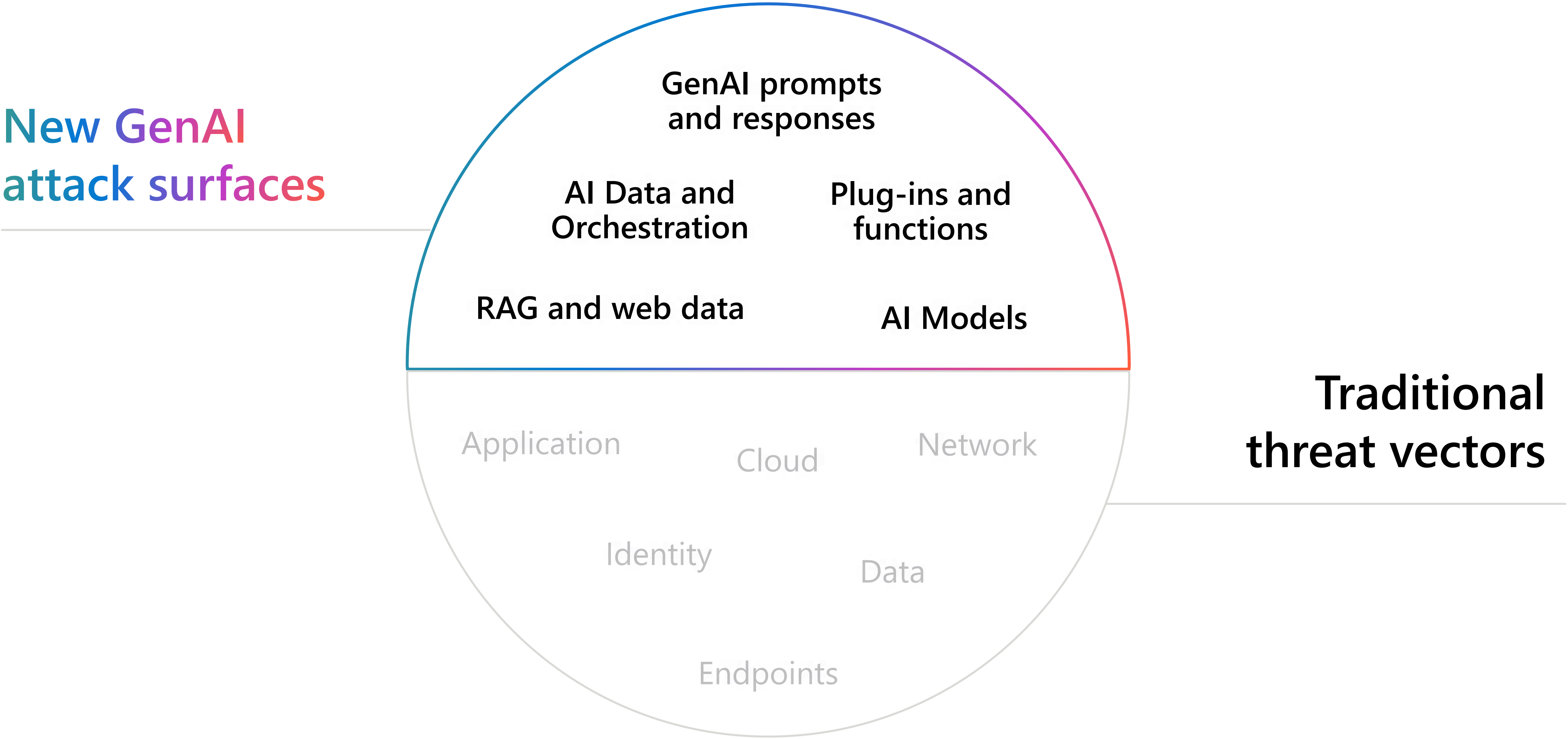
Phishing and social engineering

Disguising malicious code

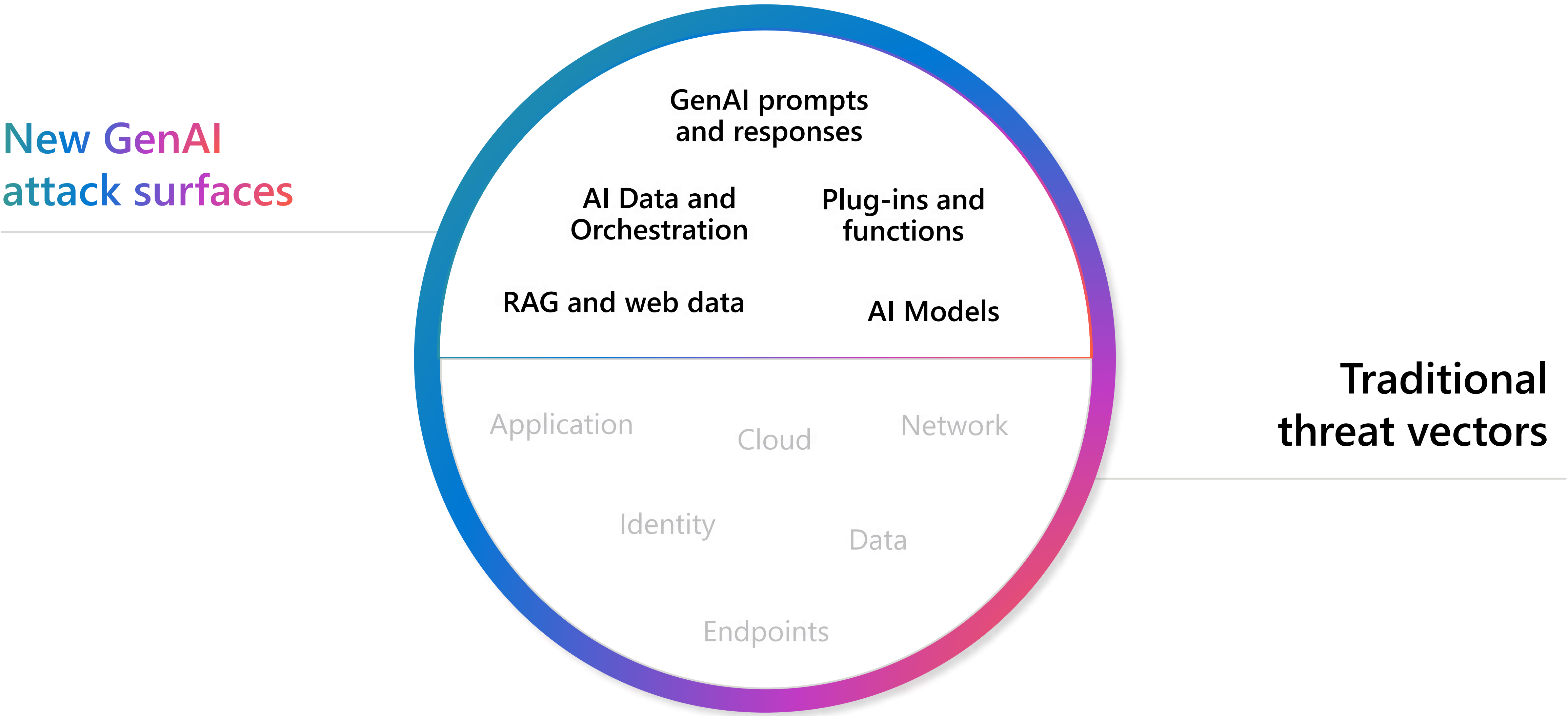
Command and control communication

Deepfakes: data, email, voice

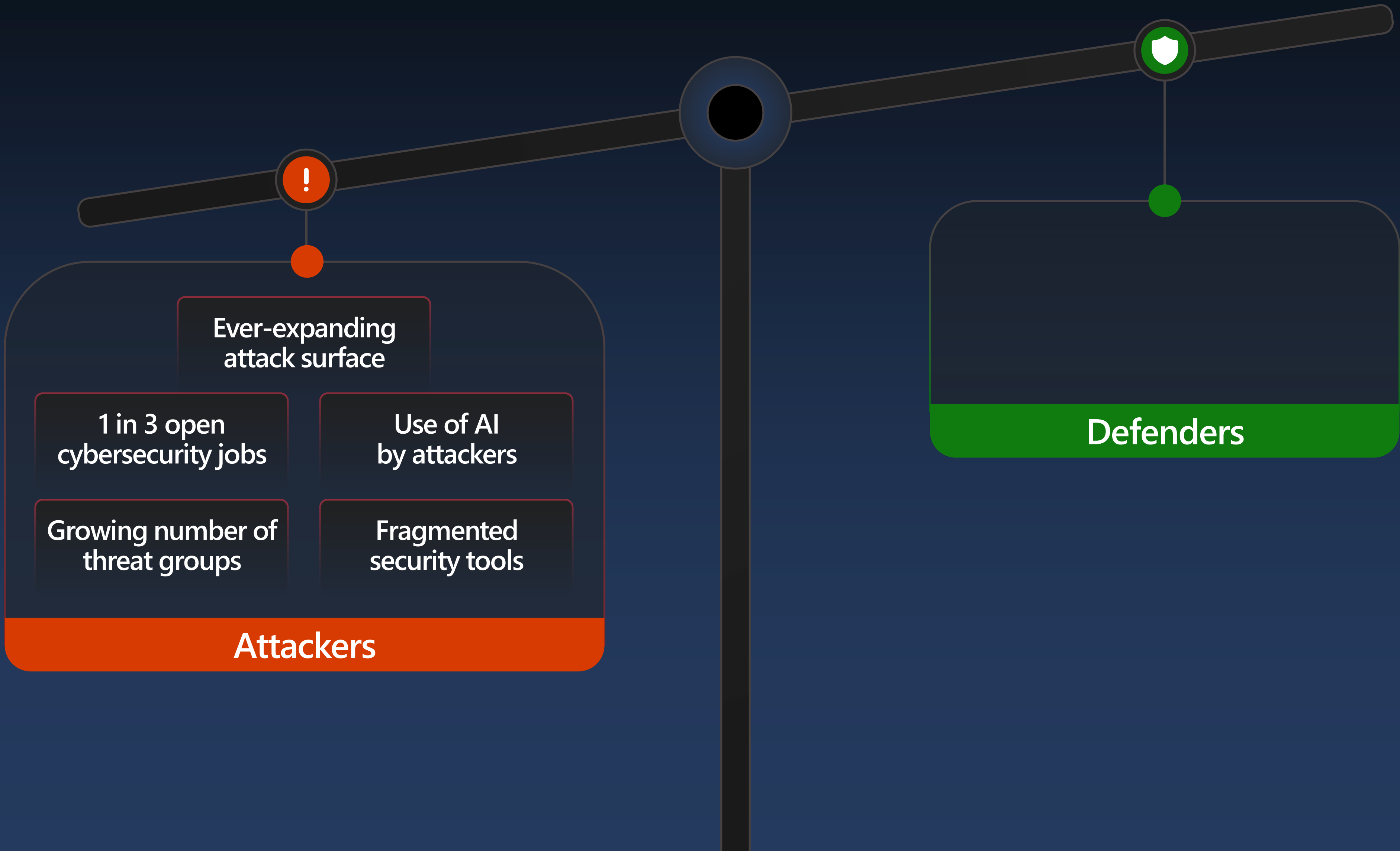
We should also expect adversaries to target GenAI


New GenAI attack surfaces
GenAI prompts and responses
AI Data and Orchestration
Plug-ins and functions
RAG and web data
AI Models
Traditional threat vectors
Application
Cloud
Network
Identity
Data
Endpoints

We have to protect it all comprehensively


New GenAI attack surfaces
GenAI prompts and responses
AI Data and Orchestration
Plug-ins and functions
RAG and web data
AI Models
Application
Cloud
Network
Identity
Data
Endpoints
Traditional threat vectors

Enterprise Security Paradigm



Ever-expanding attack surface

1 in 3 open cybersecurity jobs

Use of AI by attackers

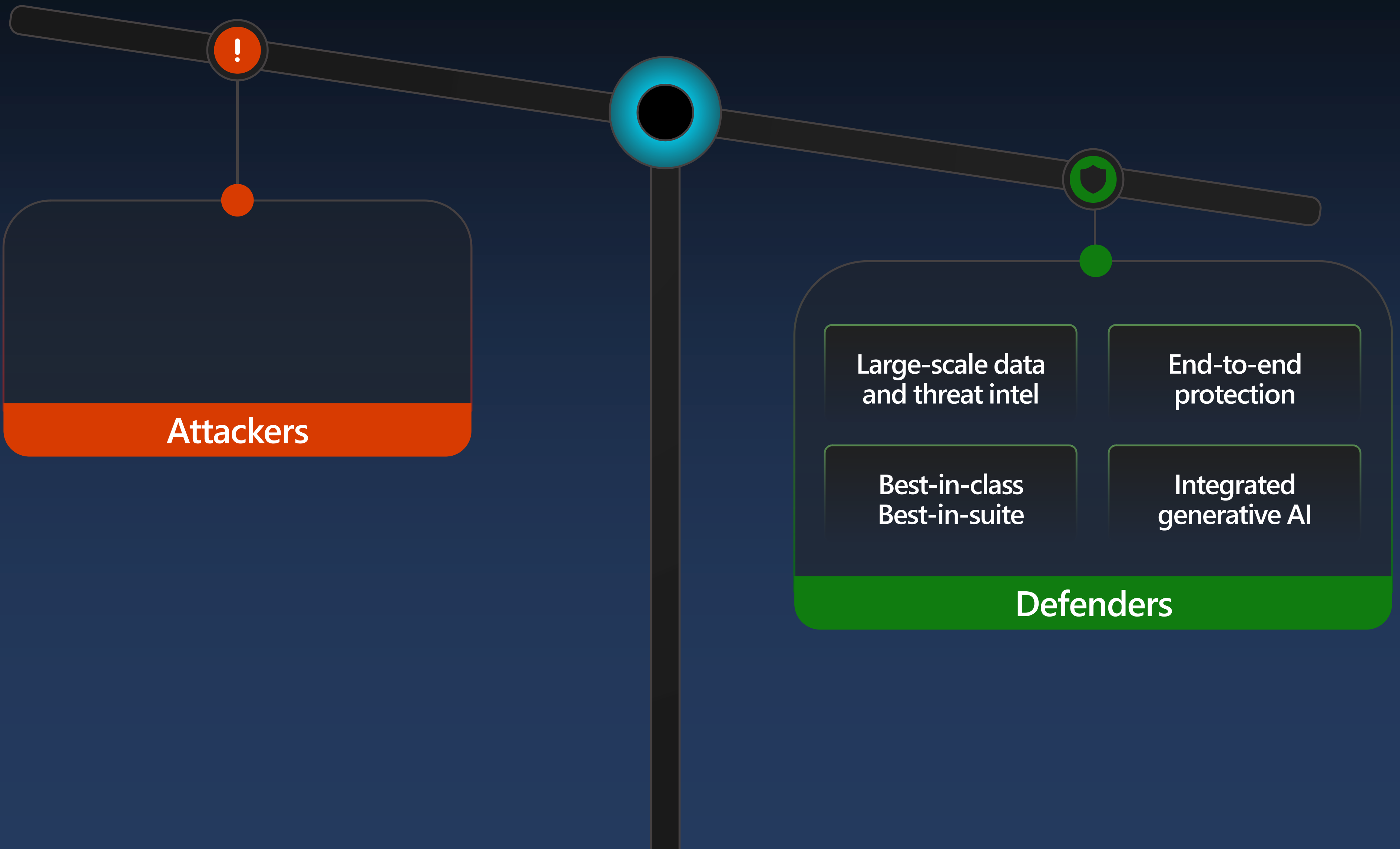
Growing number of threat groups

Fragmented security tools

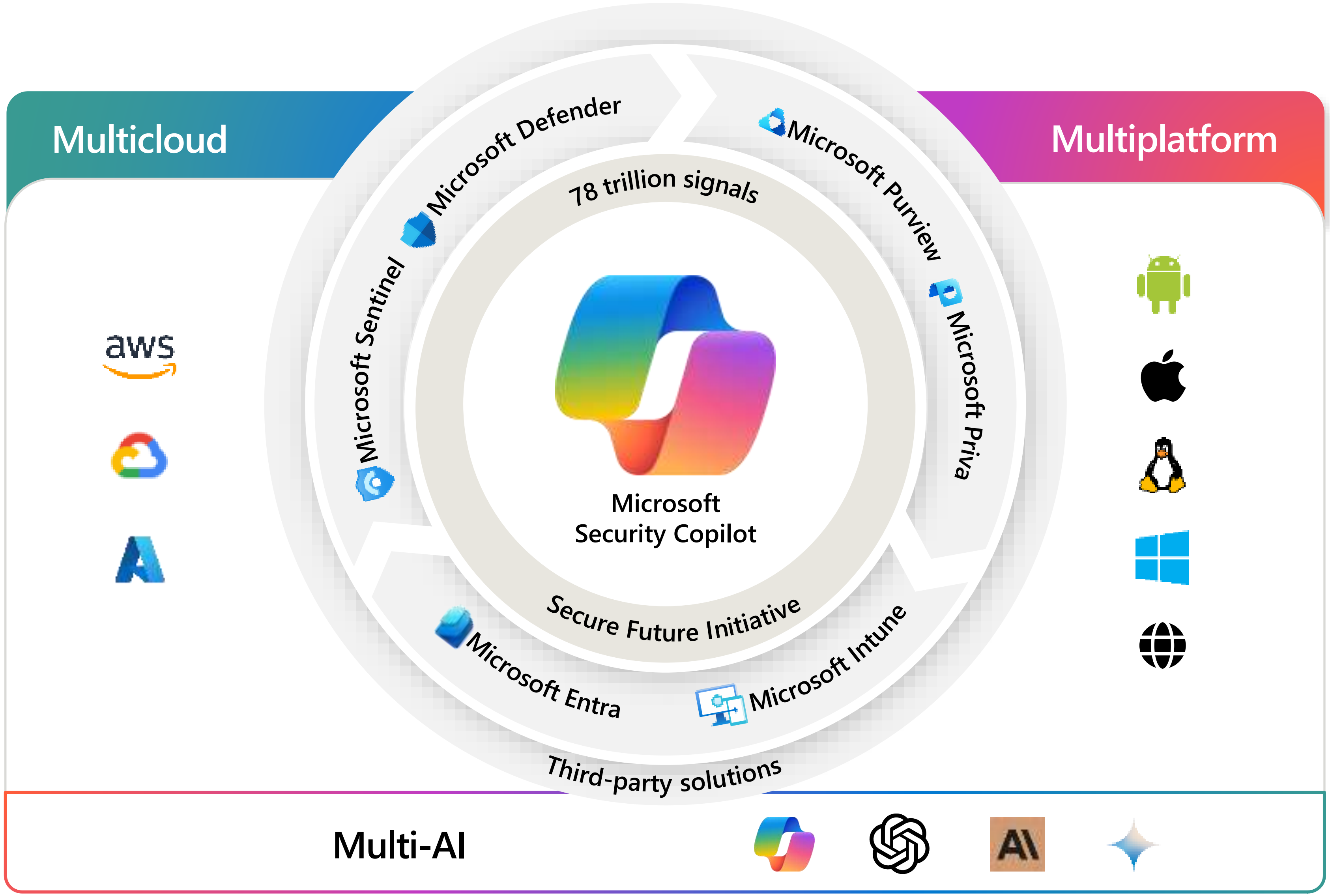
Attackers

Defenders

Enterprise Security Paradigm



AI-first end-to-end security for the age of AI



How can AI help secure organizations?

Strengthen your security posture management

Discover whether your organization is susceptible to known vulnerabilities and exploits. Prioritize risks and address vulnerabilities with guided recommendations.

Drive faster incident response

Surface an ongoing incident, assess its scale, and get instructions to begin remediation based on proven tactics from real-world security incidents

Enhance your security reporting

Summarize any event, incident, or threat in seconds and prepare the information in a ready-to-share, customizable report for your desired audience

300+ product innovations in the past 12 months and counting

Transforming threat protection and cloud security

Secure, connected endpoint management and identity

Data security for today’s world

The AI-powered future of Security

Microsoft Defender Threat Intelligence in Microsoft 365 Defender

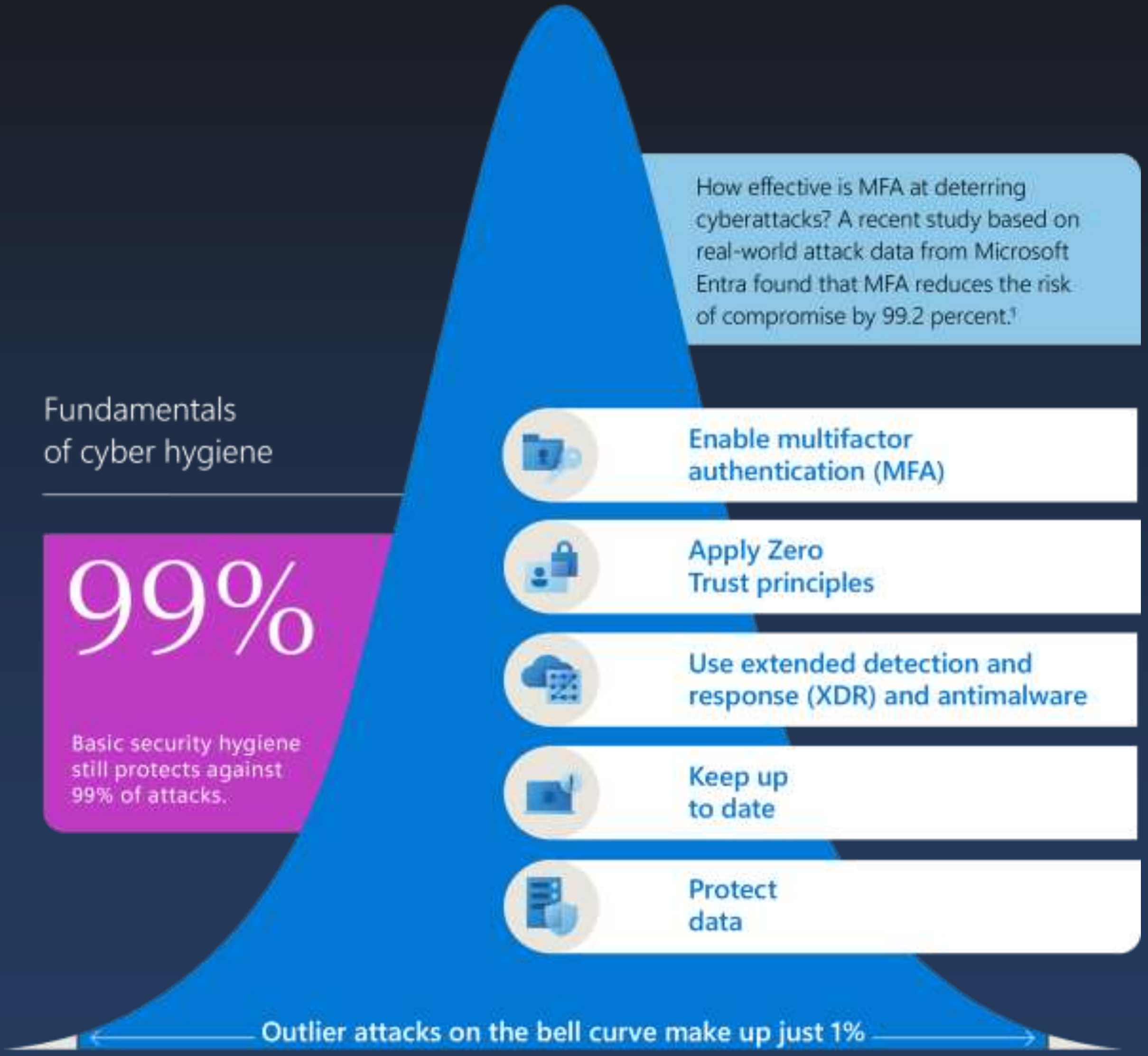
Microsoft Intune Suite

Microsoft Entra governance controls

Adaptive protection in Microsoft Purview

Microsoft Security Copilot

How can we protect 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]

Fundamentals of cyber hygiene

99%

Basic security hygiene still protects against 99% of attacks.

- 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%

Take Aways

- Security = Risk management
- A journey, not a destination
- Fight AI with AI

Microsoft

Thank you!

sandra.elvin@microsoft.com

@sandrabarouta

linkedin.com/in/sandrabaroutaelvin/