Microsoft Security

Cybersicherheit: Welche Rolle spielt der Mensch und welche KI?

Roger Halbheer

Transformation

- Secure Collaboration
- Employee Experience
- Frontline Workers
- Modernize Services
- Accelerate Innovation
- Innovate with AI
- Developer Productivity
- Migrate Enterprise Apps
- ...

Trusted Digital Fabric

Trusted Digital Fabric

Trusted Digital Fabric

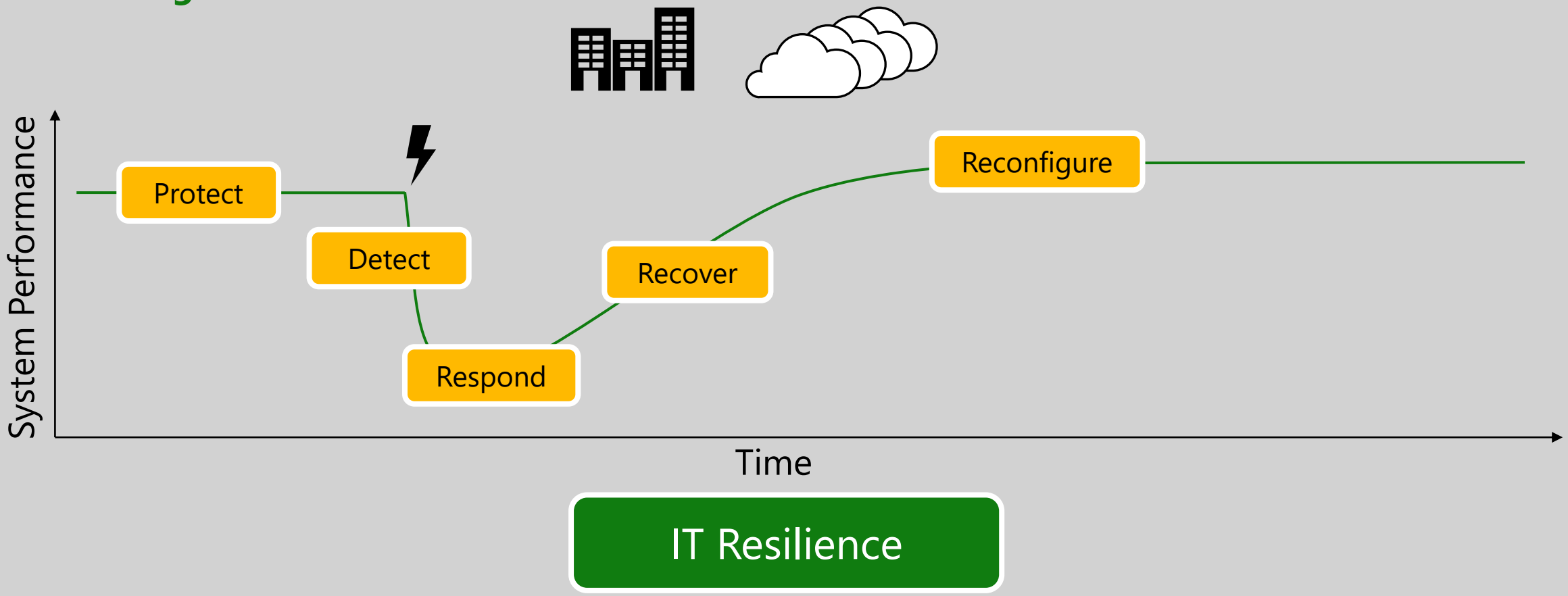
IT Resilience

The ability of an information system to continue to: (i) **operate under adverse conditions or stress**, even if in a degraded or debilitated state, while **maintaining essential operational capabilities**; and (ii) **recover to an effective operational posture** in a time frame consistent with mission needs.

Source: NIST SP 800-39 under Information System Resilience

Trusted Digital Fabric

Trusted Digital Fabric



The State of **Cybercrime**

Key developments

80-90%

of all successful ransomware compromises originate through unmanaged devices.

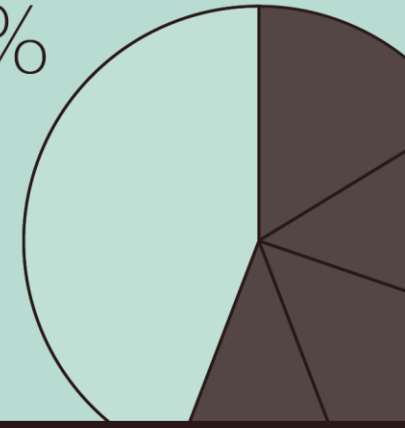
A return on mitigation (ROM) framework is helpful for prioritization and may highlight actions requiring low effort or resources but that have a high impact.

70%

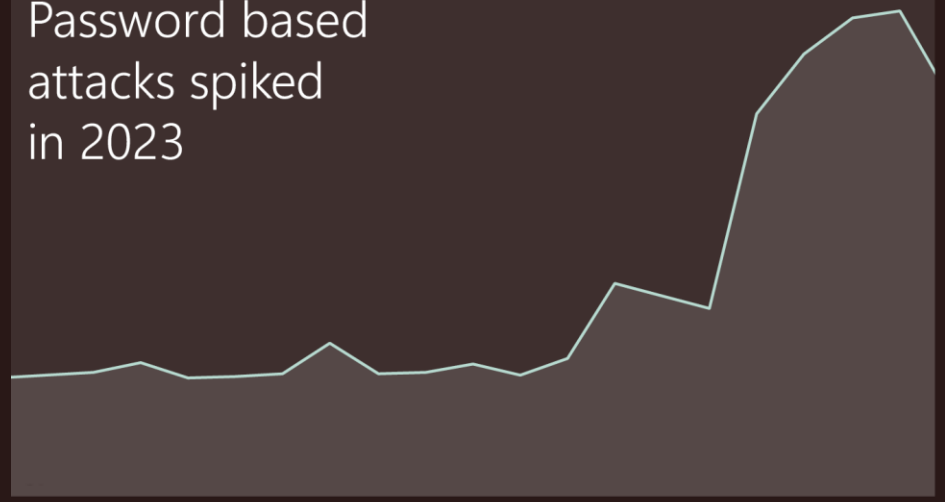
of organizations encountering human-operated ransomware had fewer than 500 employees.

Human-operated ransomware attacks are up more than

200%



Password based attacks spiked in 2023



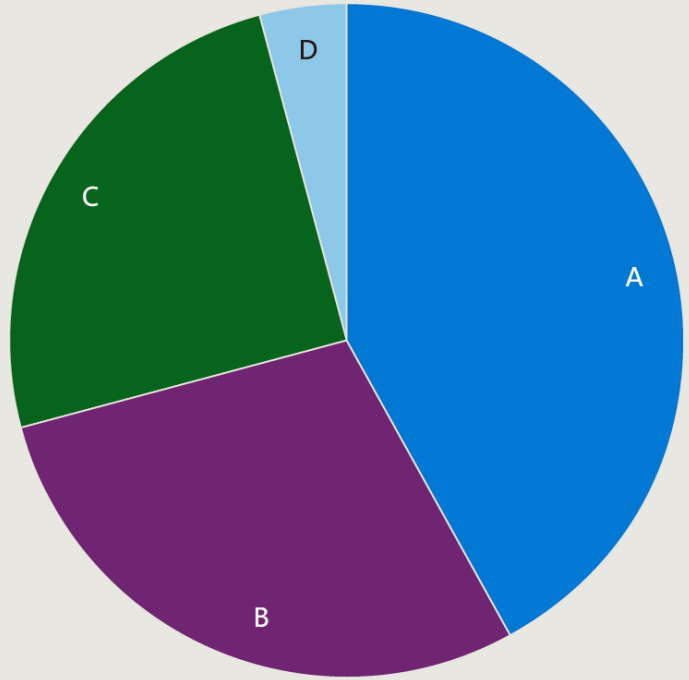
Last year marked a significant shift in cybercriminal tactics

with threat actors exploiting cloud computing resources such as virtual machines to launch DDoS attacks. When hundreds of millions of requests per second originating from tens of thousands of devices constitute an attack, the cloud is our best defense, due to the scale needed to mitigate the largest attacks.

What we're seeing in attack notifications

- Successful identity attacks
- Ransomware encounters
- Targeted phishing attempts leading to device or user compromise
- Business email compromise

Distribution of top four attack progression notifications



A 42% Successful identity attacks

C 25% Successful targeted phishing attempts

B 29% Ransomware encounters

D 4% Business email compromise (BEC)

Telemetry sources: Microsoft Defender for Endpoint, Microsoft Defender for Cloud Apps, Microsoft Defender for Identity, Microsoft Defender for Office 365, Azure AD Identity Protection, Microsoft Defender Threat Intelligence

What is the optimal ransomware resiliency state?

The foundational five

1. Modern authentication with phish-resistant credentials
2. Least privileged access applied to the entire technology stack
3. Threat-and-risk-free environments
4. Posture management for compliance and the health of devices, services, and assets
5. Automatic cloud backup and file-syncing for user and business-critical data

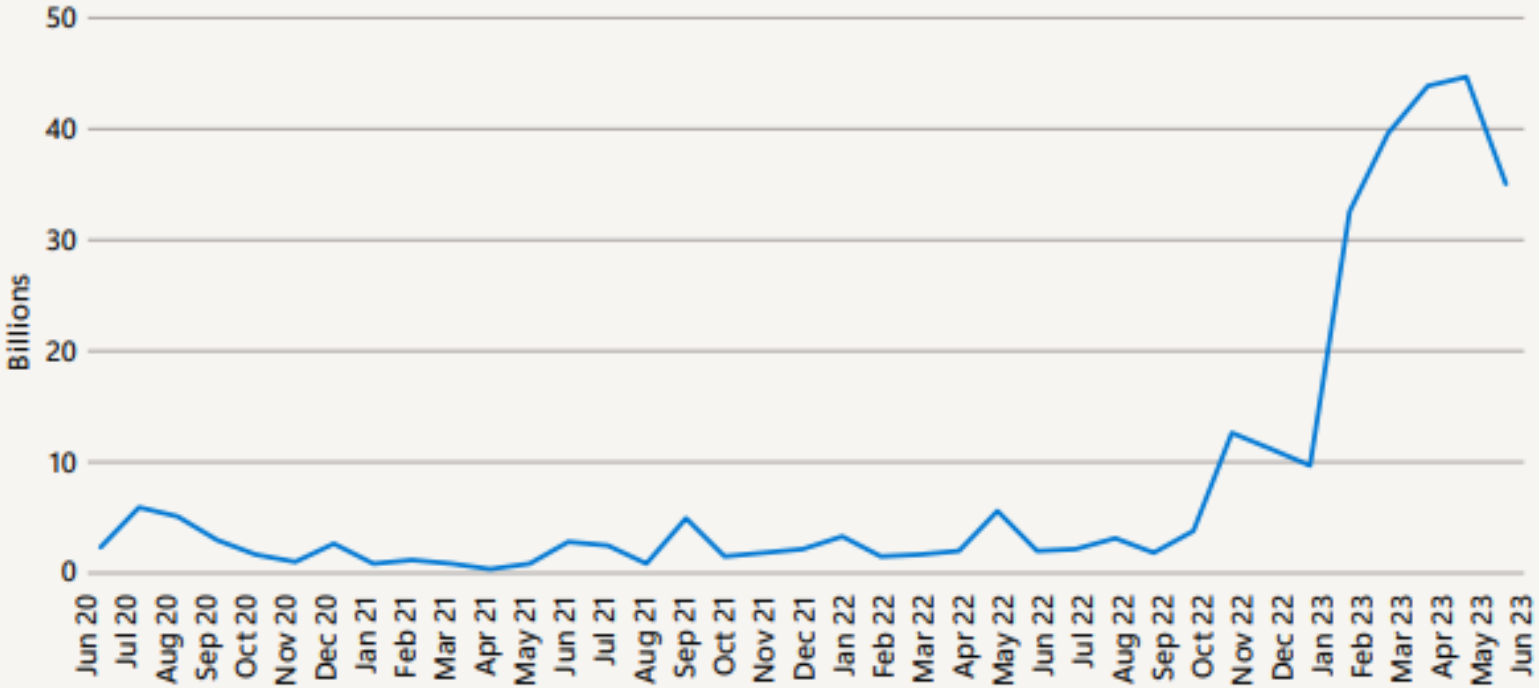
A call to action

Ransomware attackers are motivated by easy profits, so adding to their cost via security hardening is key in **disrupting the cybercriminal economy.**

Insights on **identity** attacks

- One-time password bots
- Multifactor authentication (MFA) fatigue is a threat
- Token replay remains a prevalent threat

Password based attacks spiked in 2023



Source: Microsoft Entra data

Nation-State Threats

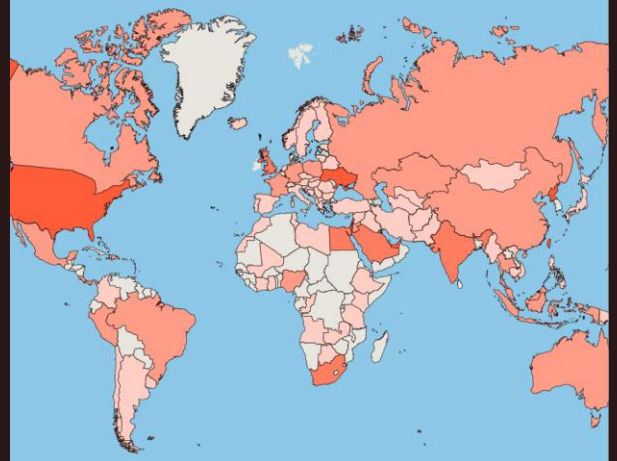
> “Nation-state actors are showing increased investment and use of cyber operations as a tool to achieve their geopolitical goals.”

— John Lambert
Corporate Vice President, Distinguished Engineer,
Microsoft Security Research

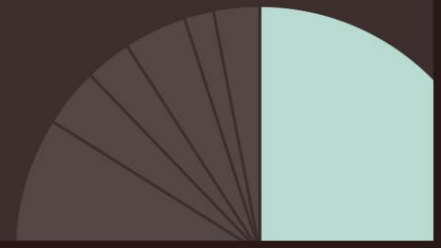
Nation-State Threats

Key developments

Nation-state and state-affiliated threat actor activities pivoted away from high volume destructive attacks in favor of espionage campaigns.



Russian state-sponsored threat actors used diverse means to access devices and networks in NATO member states.



Chinese cyber threat groups carried out sophisticated worldwide intelligence collection campaigns.

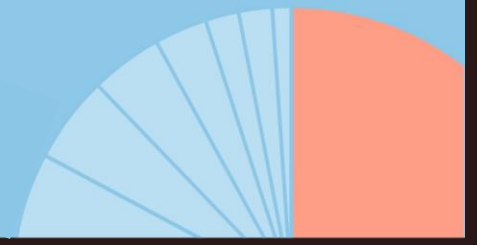
At the same time, China's cyber influence campaigns continue to operate at an unmatched scale.

The unchecked expansion of the cyber mercenary marketplace threatens to destabilize the broader online environment.

Iranian state actors are using increasingly sophisticated tradecraft

including enhancing operations in cloud environments, regularly using custom implants, and exploiting newly released vulnerabilities faster.

North Korean actors conducted a supply chain attack using an existing supply chain compromise.

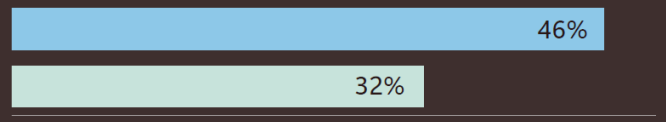


Critical cybersecurity challenges

Key developments

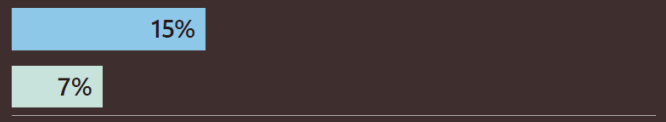
46%

Of the 78% of IoT devices with known vulnerabilities on customer networks, 46% cannot be patched.



25%

of OT devices on customer networks use unsupported systems.



15

We discovered 15 new zero-day vulnerabilities in the CODESYS runtime,

highlighting the significant risks associated with not addressing supply chain vulnerabilities to ensure the security of critical infrastructure and systems.

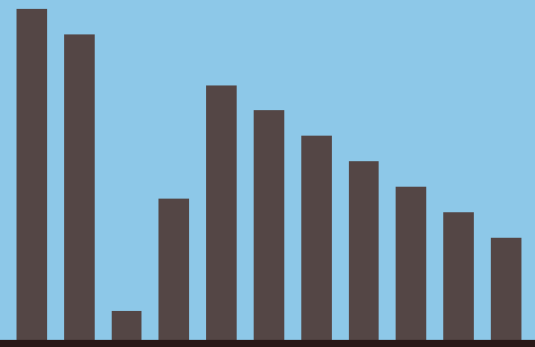
Attacks targeting open source software have grown on average

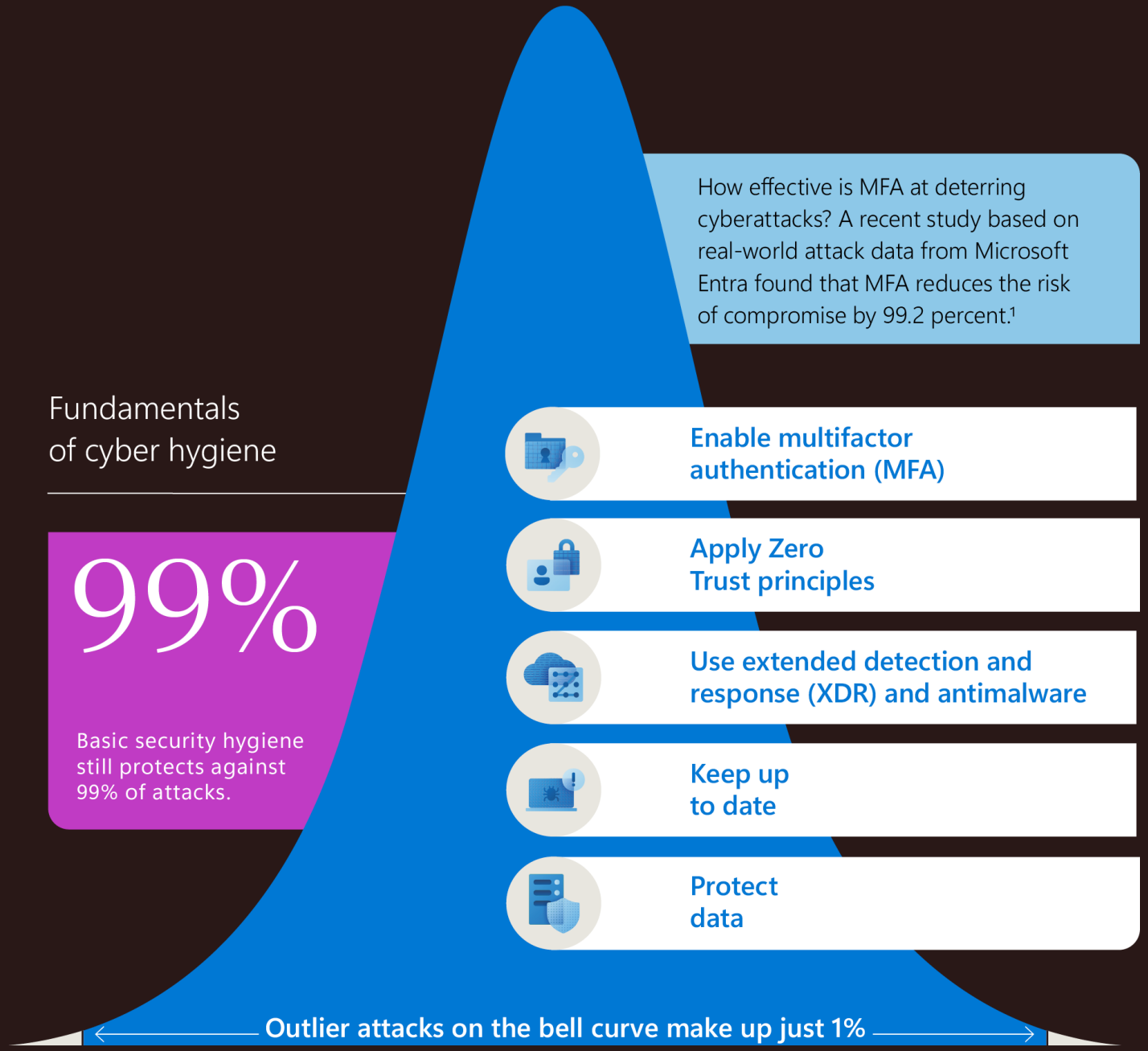
742%

since 2019.[7]

57%

of devices on legacy firmware are exploitable to a high number of CVEs (>10).

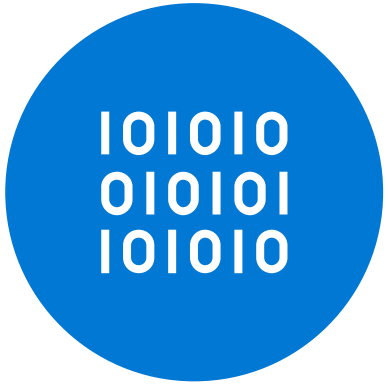



How effective is MFA at deterring cyberattacks? A recent study based on real-world attack data from Microsoft Entra found that MFA reduces the risk of compromise by 99.2 percent.[1]
Fundamentals of cyber hygiene
99%
Basic security hygiene still protects against 99% of attacks.
Enable multifactor authentication (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%

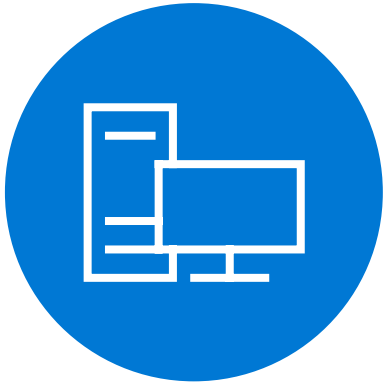
We have the means to tip the balance

But we need to re-think security

The **AI advantage** for defensive threat intelligence



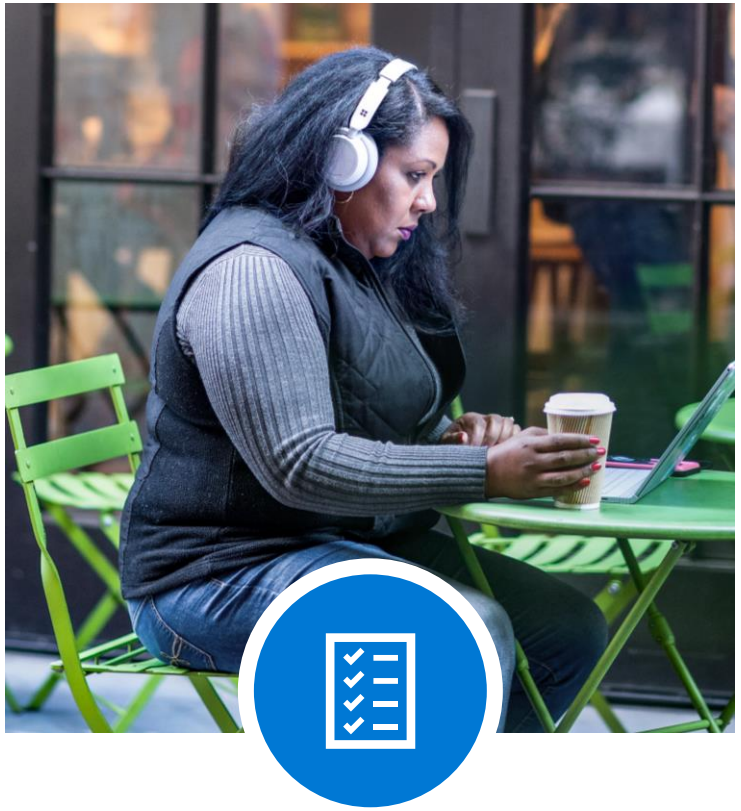
Defenders have more data



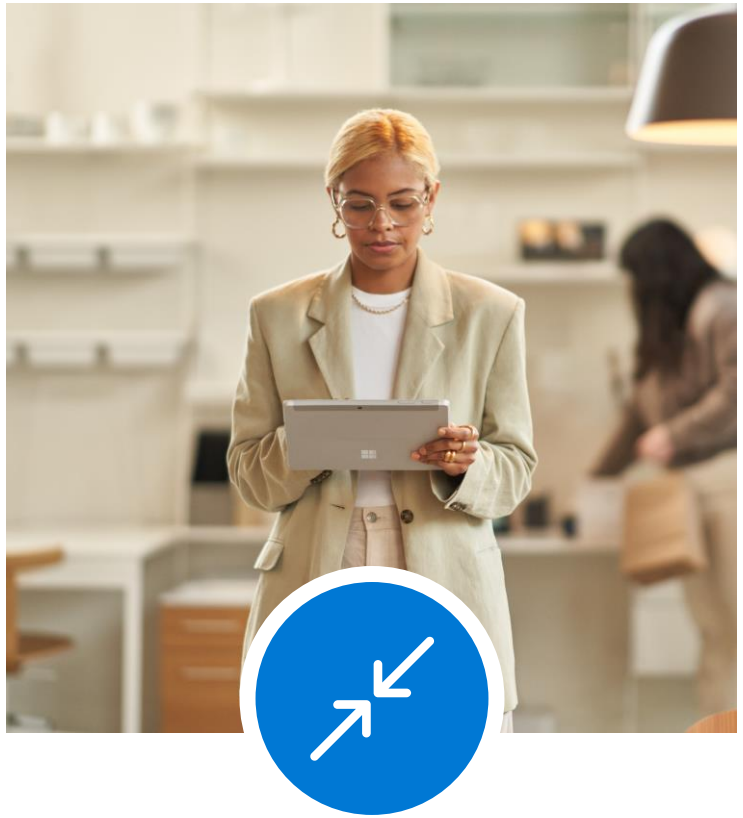
Defenders have better infrastructure

Defenders innovating

The guiding principles of Zero Trust



Verify explicitly

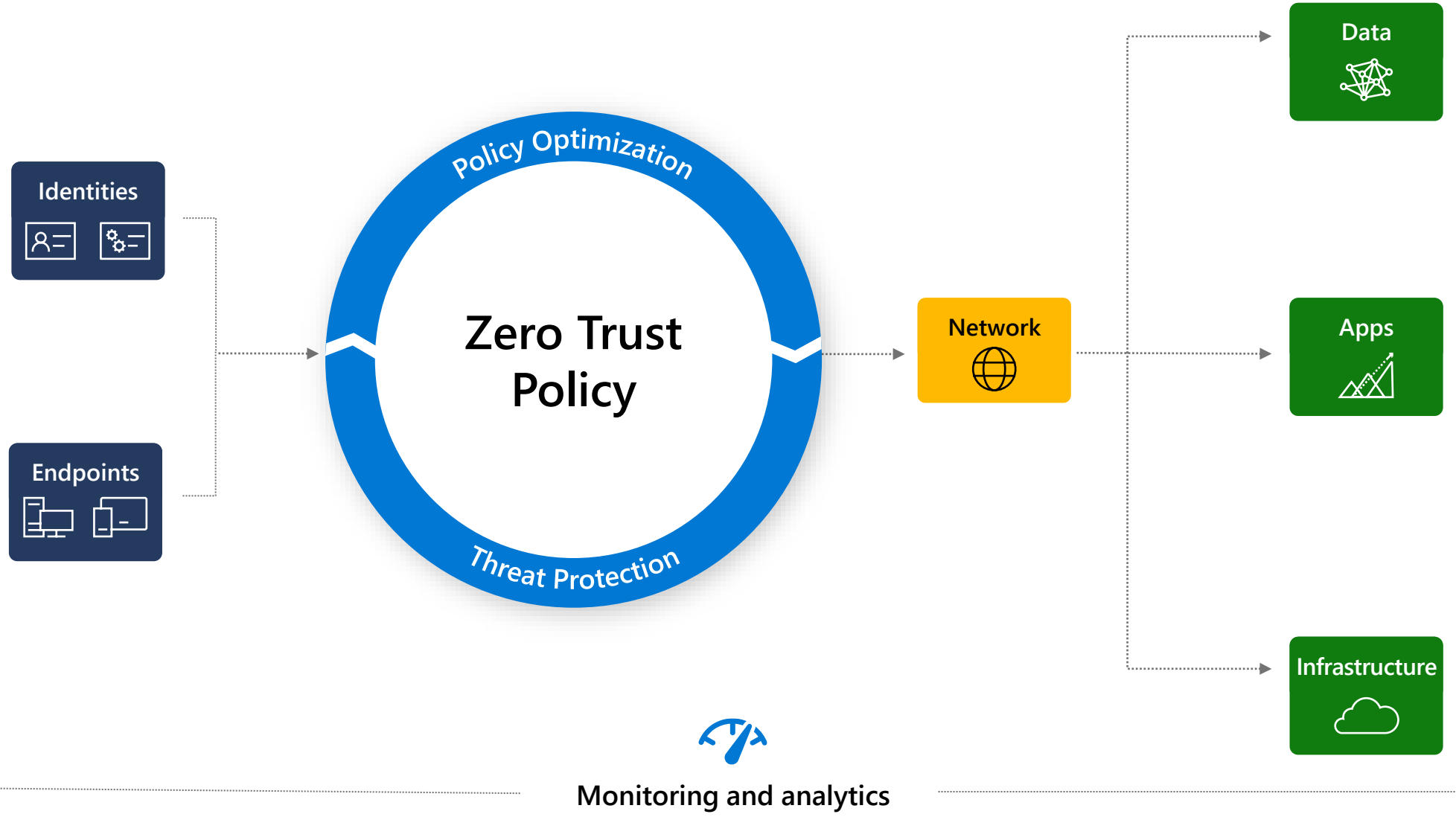


Use least privilege

Assume breach

Microsoft Security

Zero Trust architecture



AI for Security

Security for AI

Applications with AI
(e.g. Chat GPT, M365 Copilot)

AI as PaaS
(e.g. GPT on Azure)

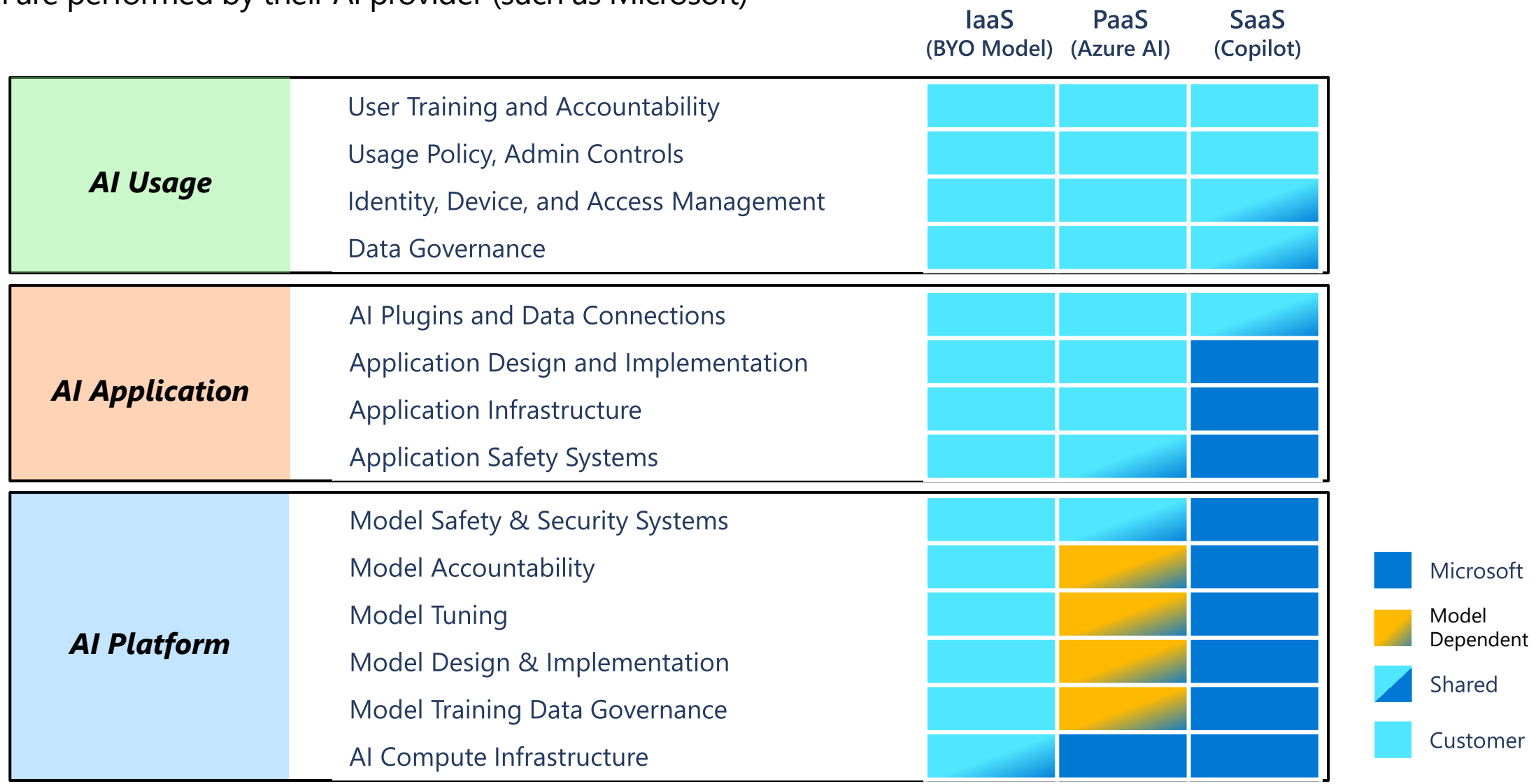
Finetuning

Own Models

AI for Security

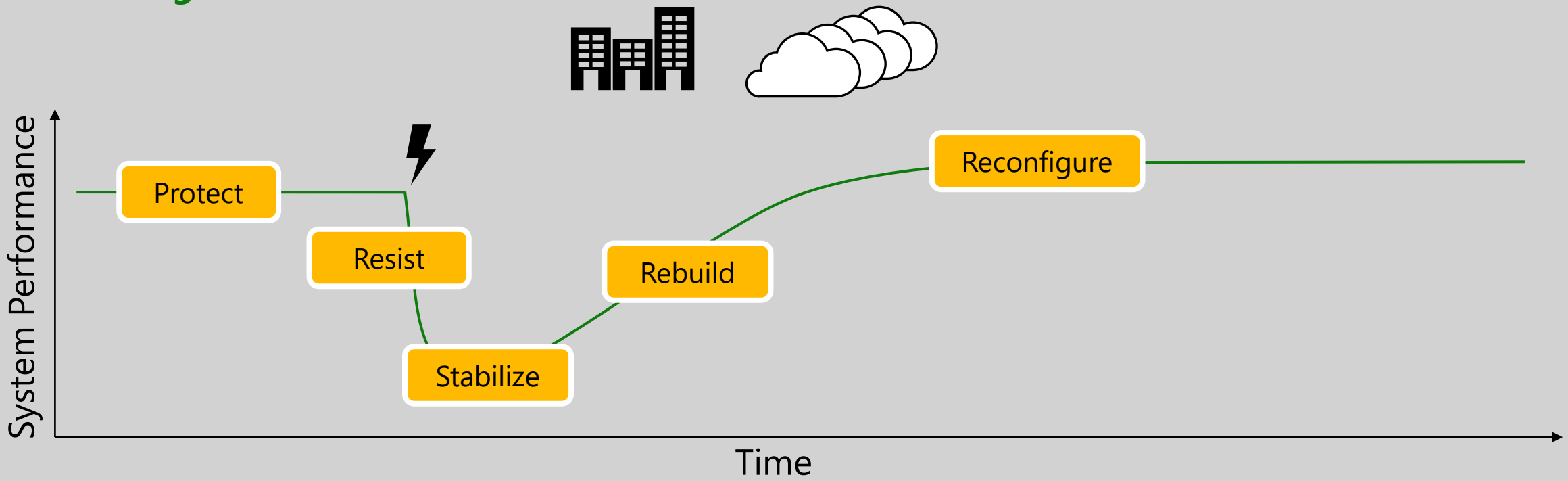
AI Shared Responsibility Model

Illustrates which responsibilities are typically performed by an organization and which are performed by their AI provider (such as Microsoft)



Trusted Digital Fabric

Trusted Digital Fabric



IT Resilience

Thank you

Roger Halbheer
roger.halbheer@microsoft.com

+41 78 844 65 55