Cybersecurity & system resilience in the energy sector

Ole Tom Seierstad
National Security Officer, Microsoft Norway

Microsoft

Navigating a shifting world

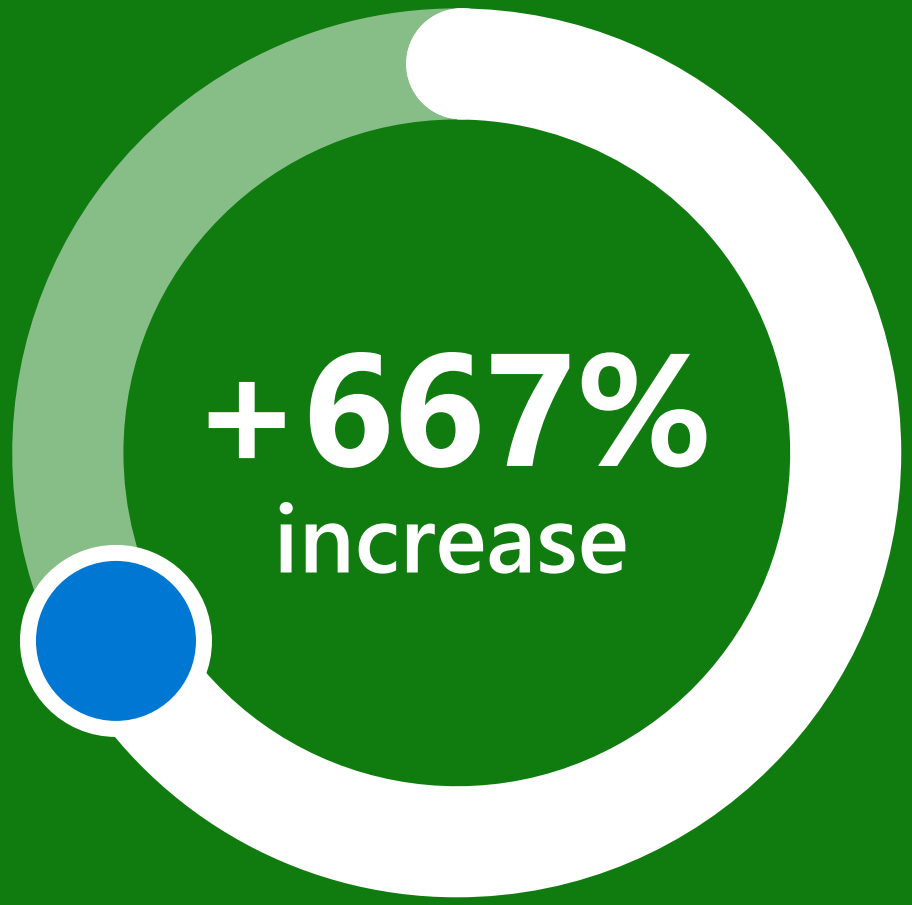
Conventional security tools
have not kept pace

Attacks growing
more sophisticated

Regulatory landscape
becoming **more complex**

100M

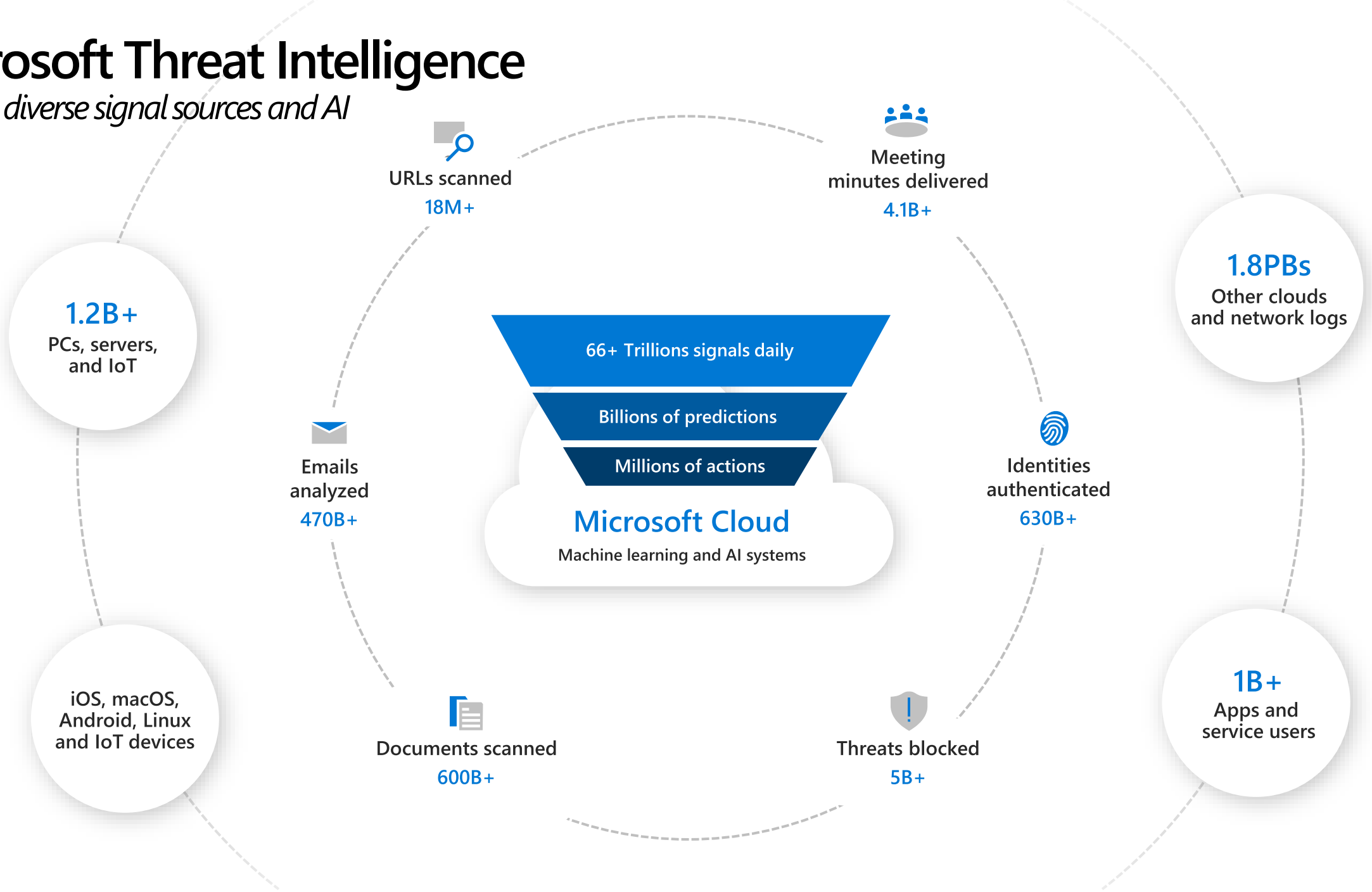
password attacks took place globally everyday



in phishing attacks

Microsoft Threat Intelligence

Built on diverse signal sources and AI



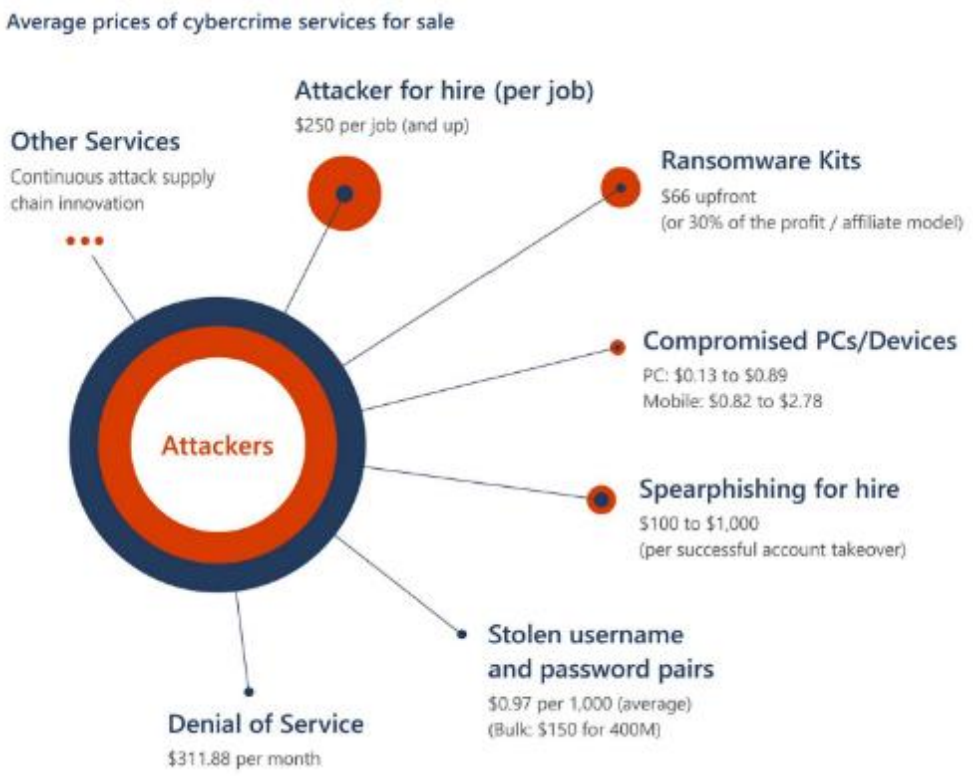
The growing threat of cybercrime

- A threat to national security
- Cybercriminals attacking all sectors
- Ransomware attacks increasingly successful
- Cybercrime supply chain continues to mature

POSITIVE TRENDS

- Transparency: governments and companies coming forward
- Priority: new laws, task forces, resources, partnerships

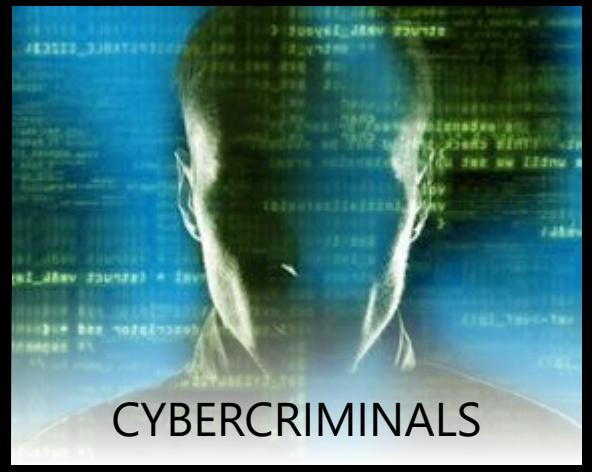
The cybercrime economy and services



WITH NO TECHNICAL KNOWLEDGE OF HOW TO CONDUCT A CYBERCRIME ATTACK, AN AMATEUR THREAT ACTOR CAN PURCHASE A RANGE OF SERVICES TO CONDUCT THEIR ATTACKS WITH ONE CLICK.

Today's top THREAT ACTORS pose unique challenges

An effective strategy must respond to a broad range of continually evolving attack types



FINANCIAL
Persistent presence
Professional execution
Ransomware

ESPIONAGE
Near-unlimited resources
Sophistication
Legal autonomy

POLITICAL
Shape/influence opinions
Undermine trust

OPPORTUNISTIC
Access to IT environment
Trusted to access sensitive info

Attack Vectors


SOCIAL ENGINEERING


PHISHING


IDENTITY SPOOFING

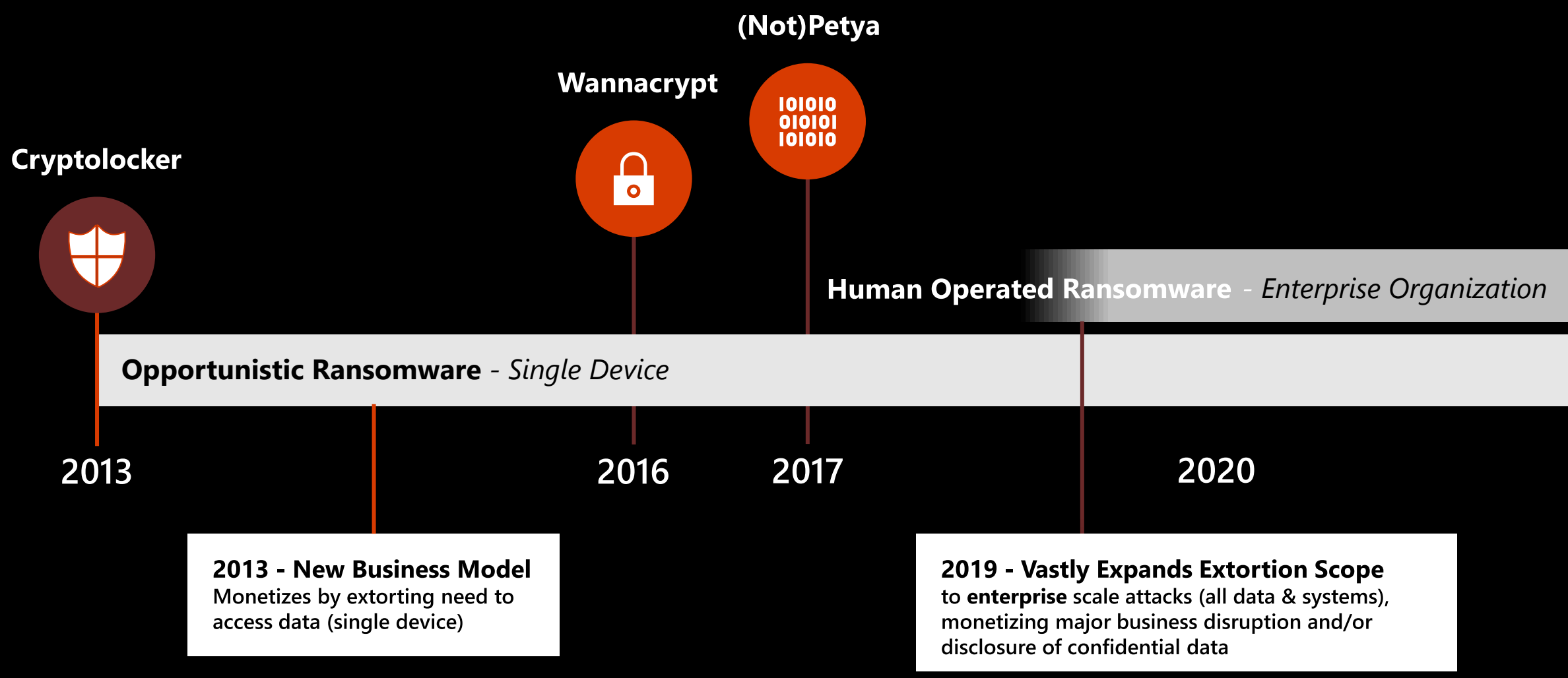

MALWARE


SUPPLY CHAIN INSERTION

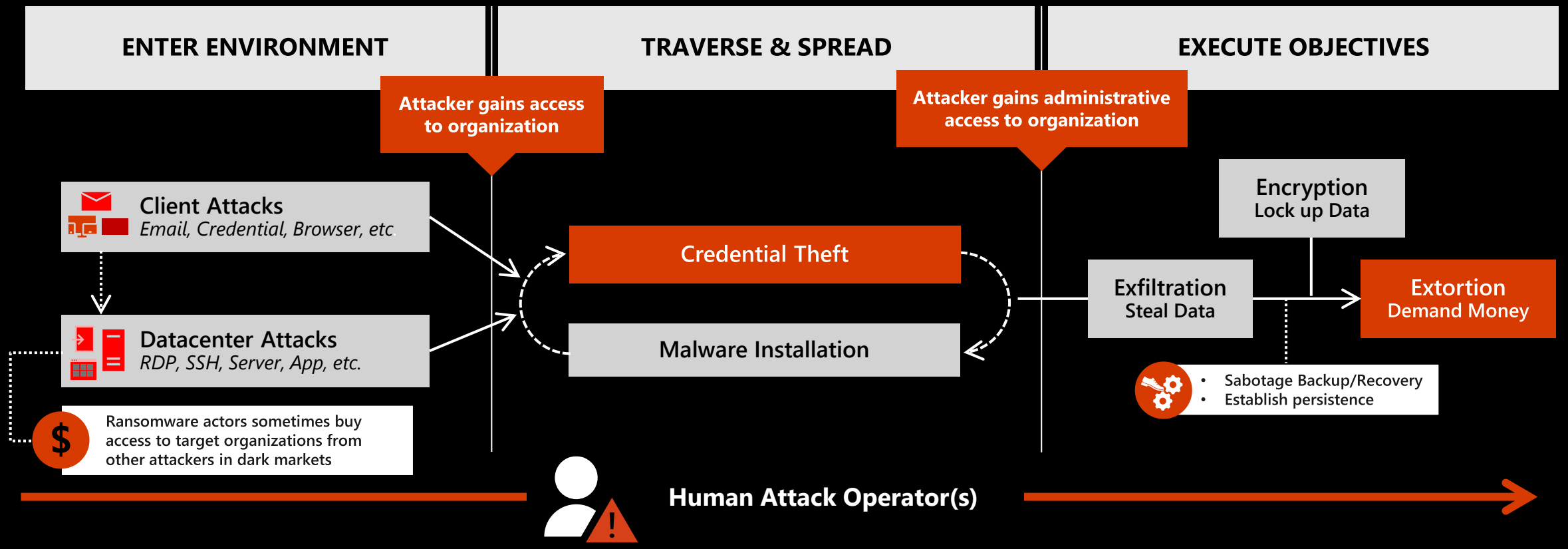

MAN-IN-THE-MIDDLE


DENIAL OF SERVICE

Evolution of ransomware models



Pattern – Human Operated Ransomware



In some instances, cybercriminals went from initial entry to ransoming the entire network in less than 45 minutes.

(Cyber)Crime Pays

Revenue opportunity for **Cybercrime** as a Service (CaaS) drives speed, scale and growth

$6T
Annually today

$10T
By 2025

... and it's accelerating

1k
Attacks/Second

2x
Ransomware demands

74%
Increase YoY
Password attacks

Time is not on our side

Cyberattacks move fast, victims are slow

1 hr
to access data

<2 hr
to move laterally

14 days
after vulnerability is published
before exploit is broadly available

The more you wait, the more they take

78% of devices still used an unpatched version even

9 months after a patch is released

Microsoft

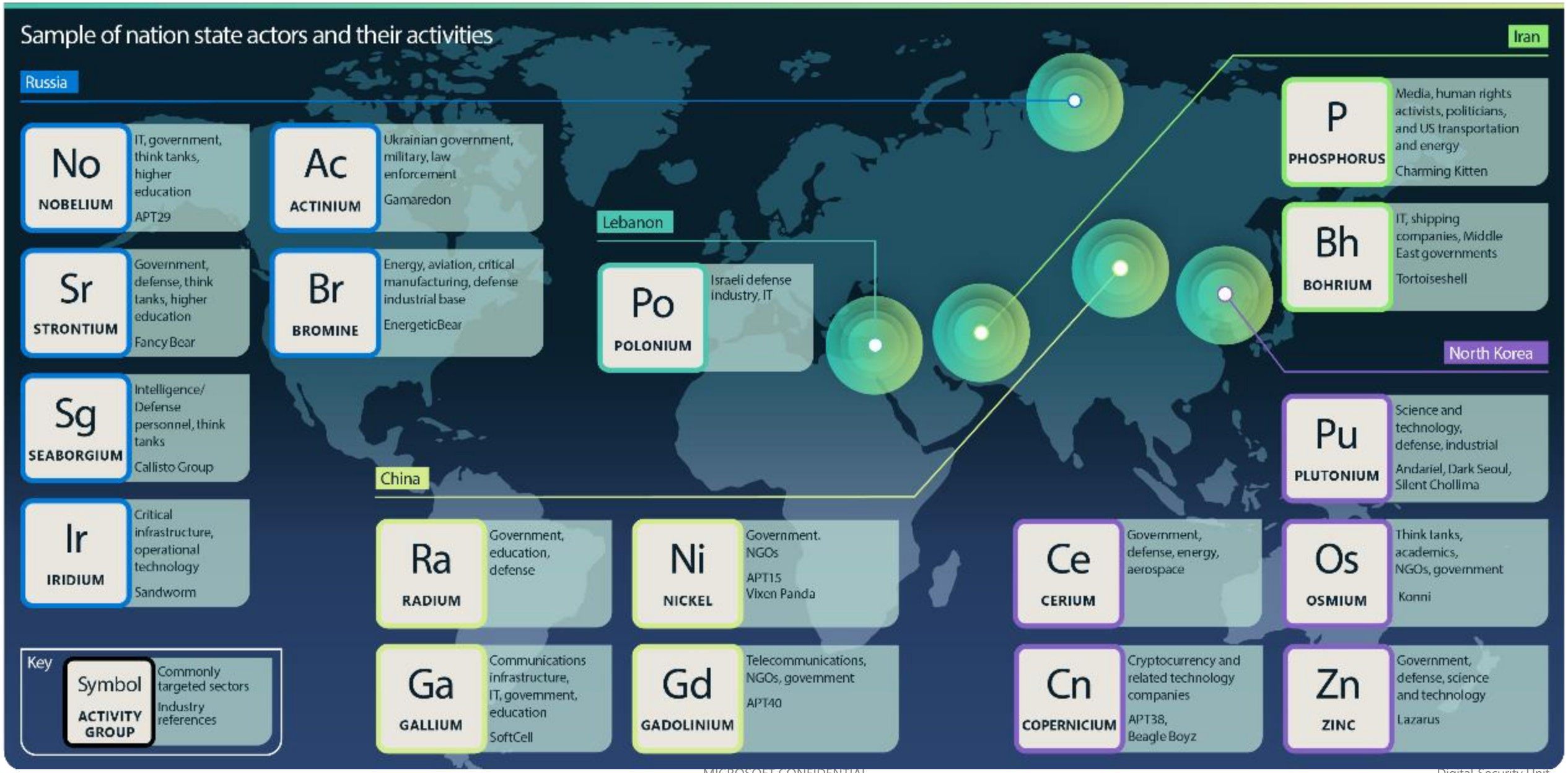
Hackers don’t break in - they log in

Assume Breach, Explicit Verification, Least Privilege

Nation State Threats

Nation state actors are launching increasingly sophisticated cyberattacks to evade detection and further their strategic priorities.

About our nation state data



Russian government's cyber influence operations

Presidential Administration

- Media initiatives & branding
- State media control
- Funding

MFA

- Diplomatic accounts
- Interaffairs
- Rossotrudnichestvo

- Agenda setting
- Global outreach

GRU

- InfoRos
- Donbass Tragedy
- Anonymous social media

- Leveraging cyber
- Flooding the zone

SVR

- Strategic Culture
- Odna Rodyna
- New Eastern Outlook
- Oriental Review

- Historical revisionism
- Think tanks & academia

FSB

- NewsFront
- SouthFront
- PolitNavigator
- Antifascist

- Near-abroad focus
- Establishing new media environment

MOD

- Zvezvda
- War correspondents

- Frontline communications
- Providing access for preferred media

Highlights*

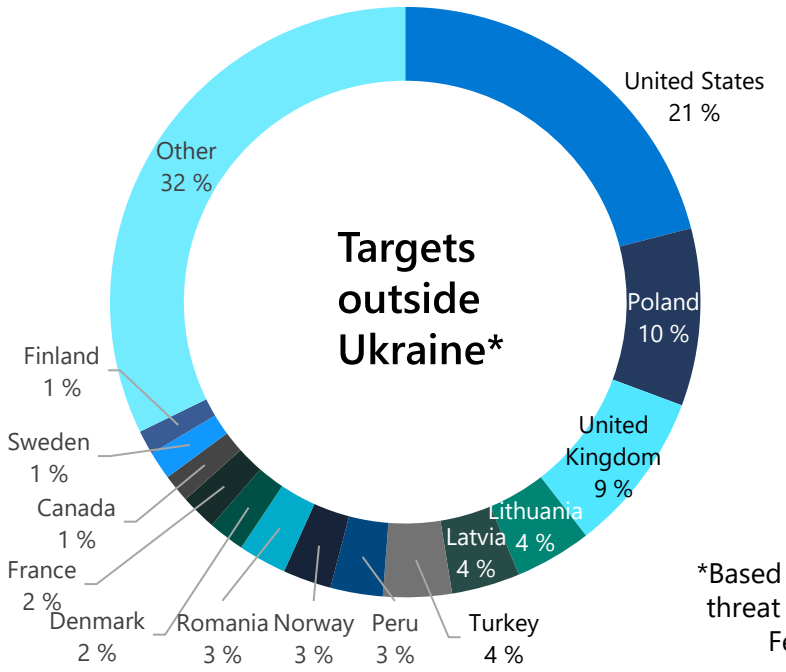
Russian threat actors challenged but undeterred by robust Ukrainian cyber defense

Targeting supply lines and sources of support to Ukraine for espionage and destruction

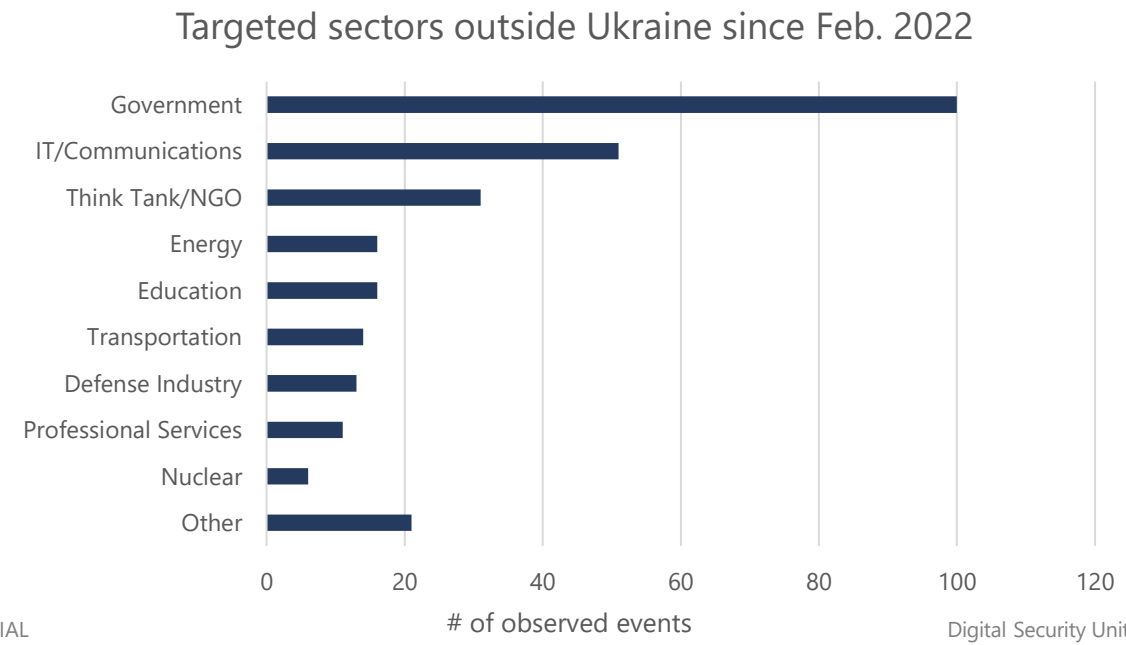
- IRIDIUM destructive attacks on Ukrainian and Polish transportation sectors
- ACTINIUM, SEABORGIUM, and STRONTIUM targeting humanitarian aid organizations, weapons manufacturers, and defense-related entities, respectively. Most likely for intelligence collection based on past patterns of behavior.
- Cyberespionage and influence operations against Ukraine's allies.

Trends since start of invasion of Ukraine likely to persist:

- Ransomware as deniable destructive weapon
- Diverse means for initial access
- Using hacktivists for power projection
- On the malign influence side, pro-Kremlin operators:
  - Weaponize fact-checking; release leaks targeting Ukrainian political figures; conduct multi-faceted operations in countries neighboring Ukraine to discredit leadership and promote pro-Russian networks.



*Based on observed threat activity since February 2022



Devices and Infrastructure

With the acceleration of digital transformation, the security of digital infrastructure is more important than ever.

IoT attacks put businesses at risk

Devices bricked or held for ransom

Devices are used for malicious purposes

Data & IP theft

Data polluted & compromised

Devices used to attack networks

The cost of IoT Attacks

Stolen IP & other highly valuable data

Compromised regulatory status or certifications

Brand impact (loss of trust)

Recovery costs

Financial and legal responsibility

Downtime

Security forensics

CyberX Risk Report

Data from 1,800 Industrial Control System Networks

71%

Sites have old versions of Windows without regular patching

64%

Have unencrypted passwords facilitating compromise

66%

Sites that are not automatically updating with latest AV definitions

54%

Have devices able to be remotely accessed enabling attackers to pivot undetected

27%

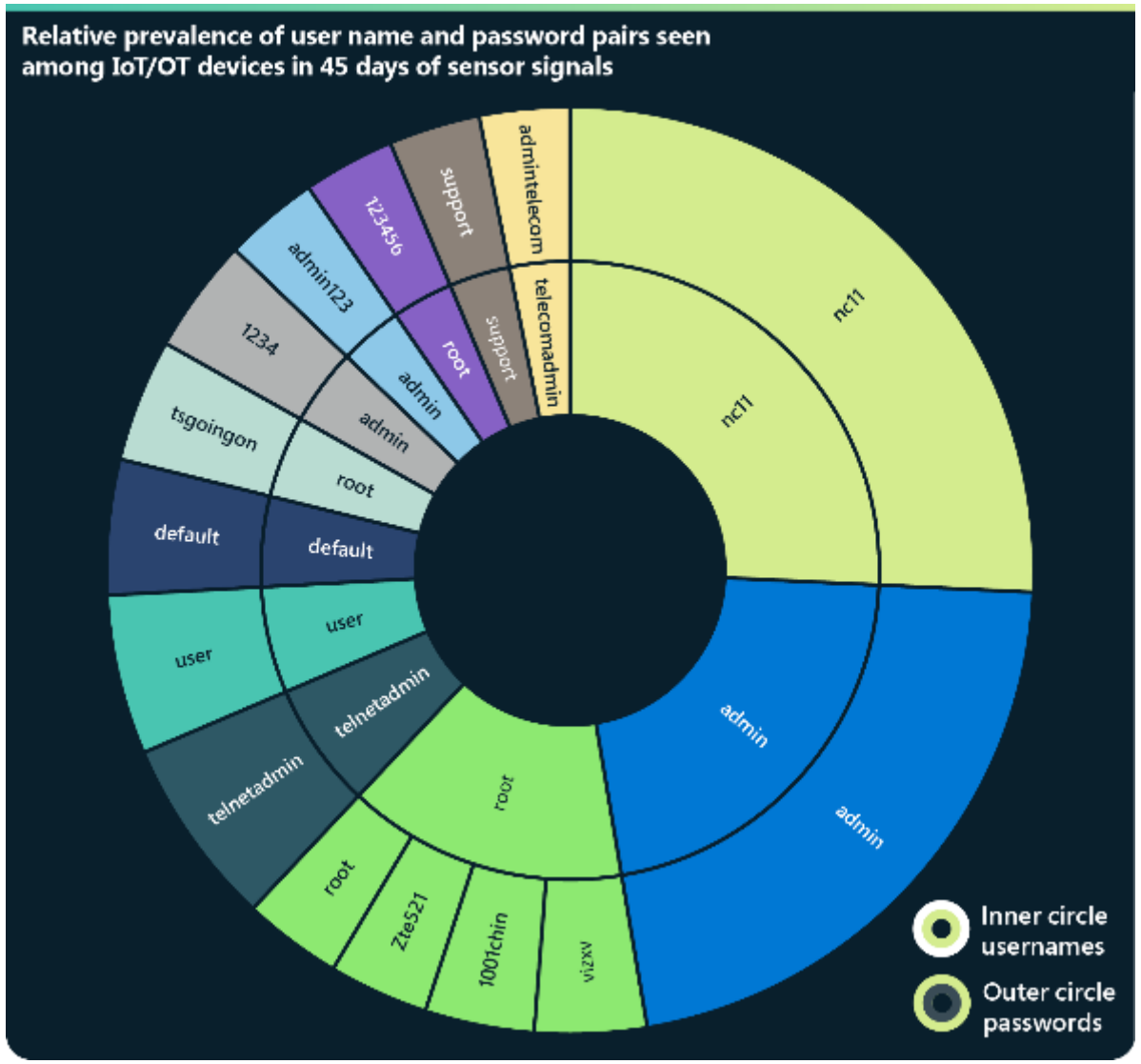
ICS devices that have direct connections to the internet

CyberX: recently acquired by Microsoft

IoT and OT Devices

Actionable insights

1. Ensure devices are robust by applying patches, changing default passwords, and default SSH ports.
2. Reduce the attack surface by eliminating unnecessary internet connections and open ports, restricting remote access by blocking ports, denying remote access, and using VPN services.
3. Use an IoT/OT-aware network detection and response (NDR) solution and a security information and event management (SIEM)/security orchestration and response (SOAR) solution to monitor devices for anomalous or unauthorized behaviors, such as communication with unfamiliar hosts.
4. Segment networks to limit an attacker's ability to move laterally and compromise assets after initial intrusion. IoT devices and OT networks should be isolated from corporate IT networks through firewalls.
5. Ensure ICS protocols are not exposed directly to the internet.



Call to action

- Ensure you understand and are prepared

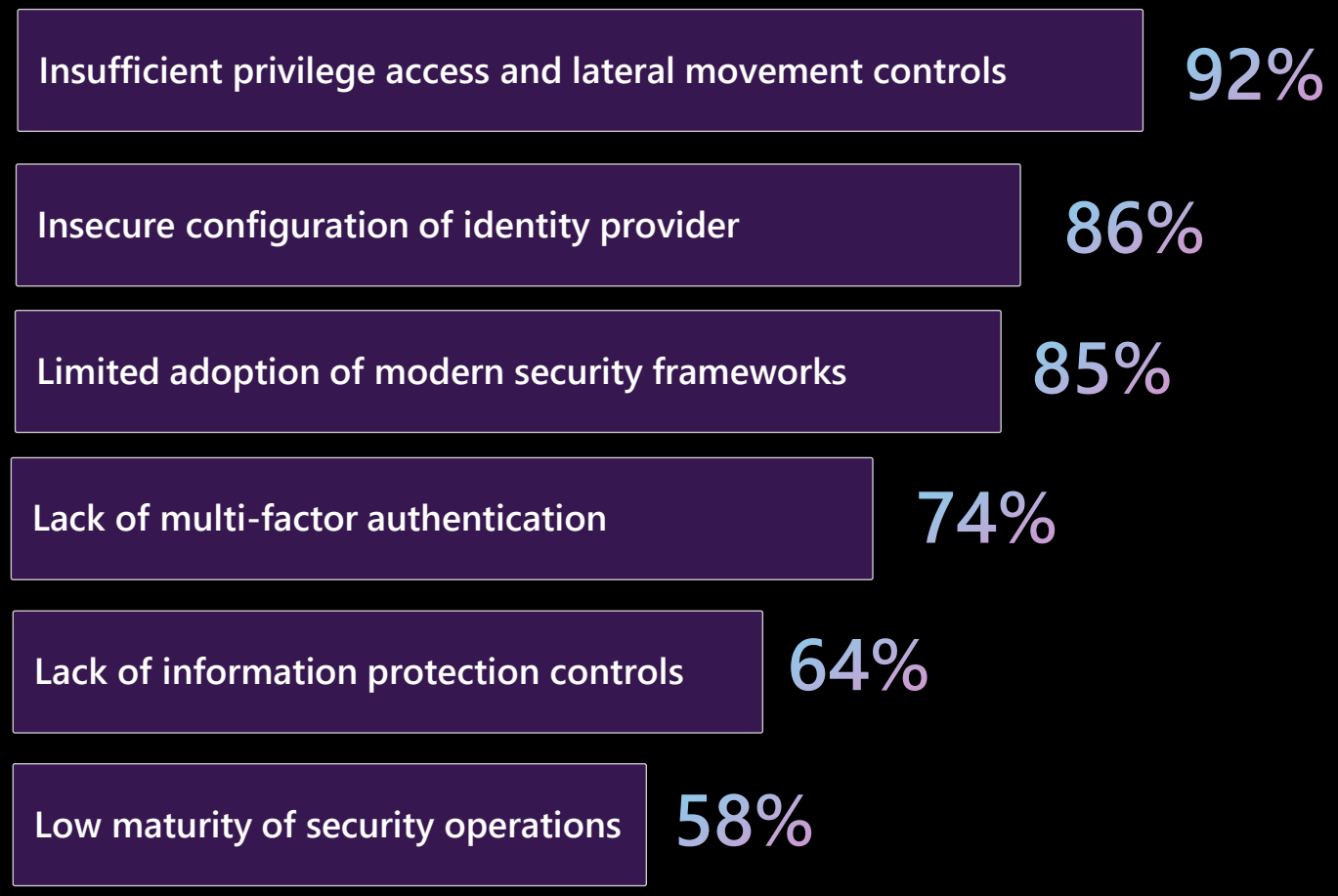
How resilient is my organization?

80%

of security incidents can be traced to a few missing elements that could be addressed through modern security approaches

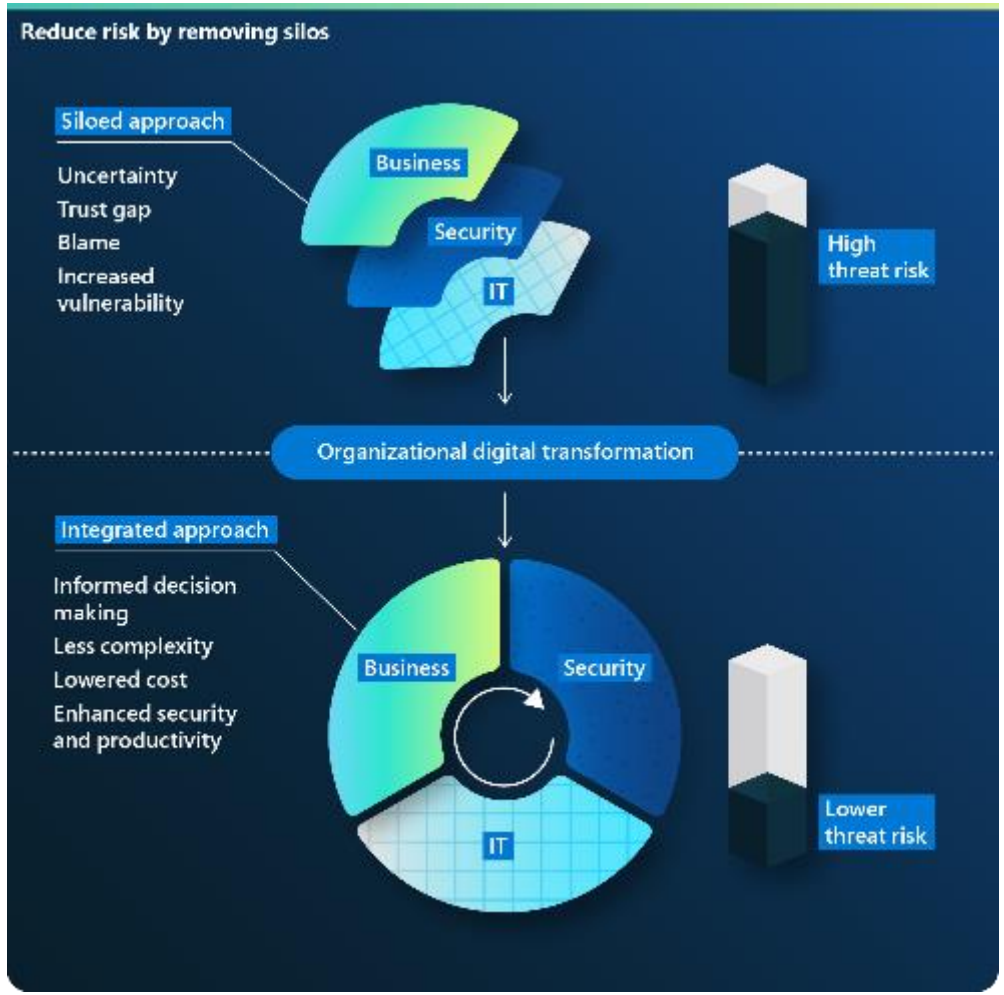
Key areas affecting Cyber Resilience

Microsoft studied victims of cyberattacks and found these factors to be the top 6 contributors to their vulnerability

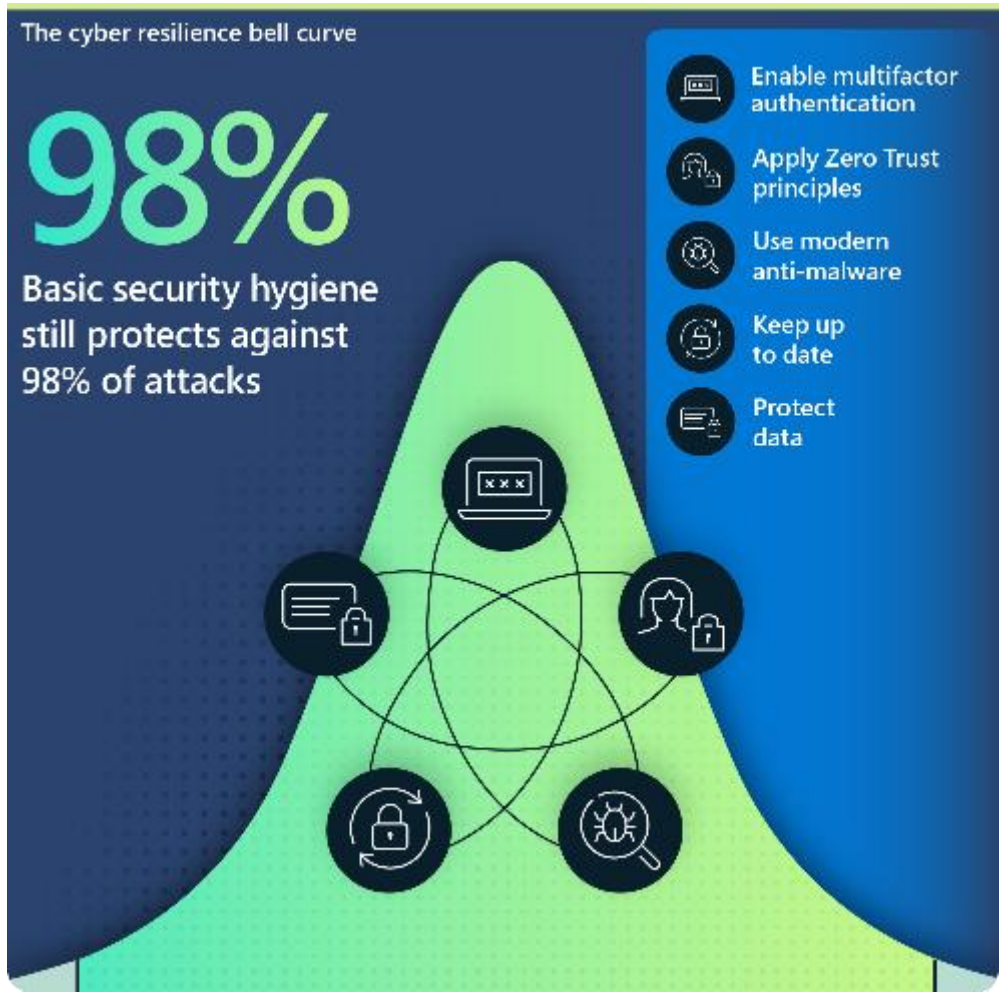


Calls to action for cyber resilience

Integrate business, security, and IT for greater resilience



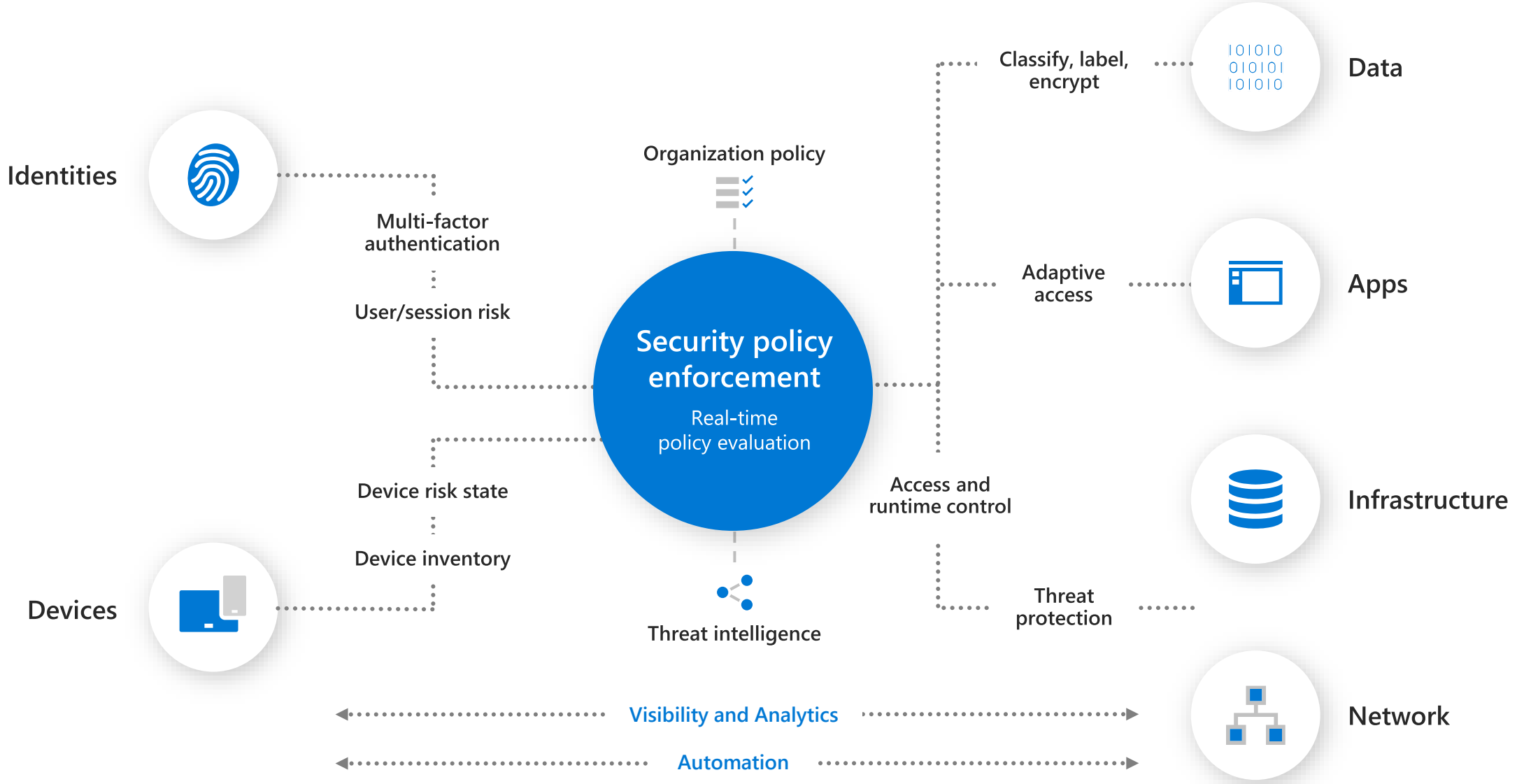
Resilience success factors every organization should adopt



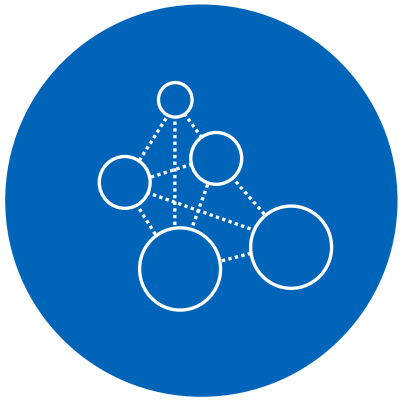
Secure your organization with Zero Trust

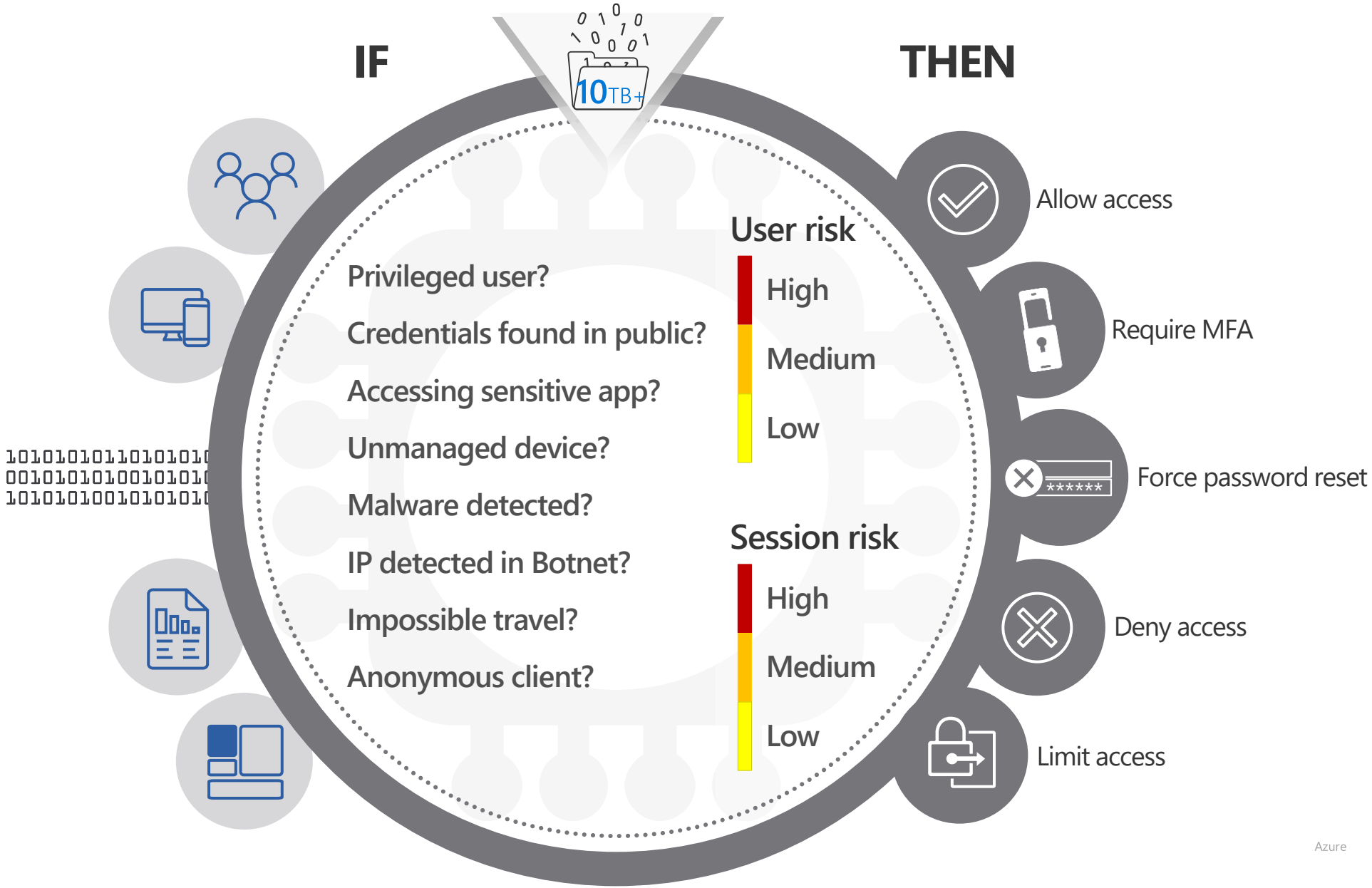
Verify **explicitly** | Use **least-privileged access** | Assume **breach**

Microsoft Zero Trust architecture



CLOUD-POWERED CONDITIONAL ACCESS





Why are Organizations Unprepared?

Lack of Skills & innovation

- Talent Gap/Retention
- Manual Processes
- Requires investment & constant innovation

Legacy Systems

- Technical debt
- Siloed standalone security products
- Legacy tools & infrastructure

Legacy Approach

- Security seen as IT function/overhead
- Security Governance is an afterthought
- Zero Trust seen as a technical issue

Legacy Mindset

- Security through obscurity
- Data location as Security
- Cloud security FUD

Thank You