



# “Meet the growing need of cybersecurity”

Tomislav Vracic  
National Technology & Security Officer  
Microsoft Corporation  
Central and Eastern Europe  
Tomislav.Vracic@microsoft.com  
<https://www.linkedin.com/in/tomislavvracic/>

2014 CYBERSECURITY = TECHNICAL PROBLEM

2020 CYBERSECURITY = BUSINESS PRIORITY

**2022 CYBERSECURITY = ORGANIZATIONAL EXISTENCE**



# Lessons from Ukraine's Hybrid War

Destructive  
cyber attacks

Cyber  
espionage

Cyber influence  
operations



# Defending Ukraine

The advent of cyberweapon deployment in the hybrid war in Ukraine is the dawn of a new age of conflict.

January 15, 2022 • 6 min read

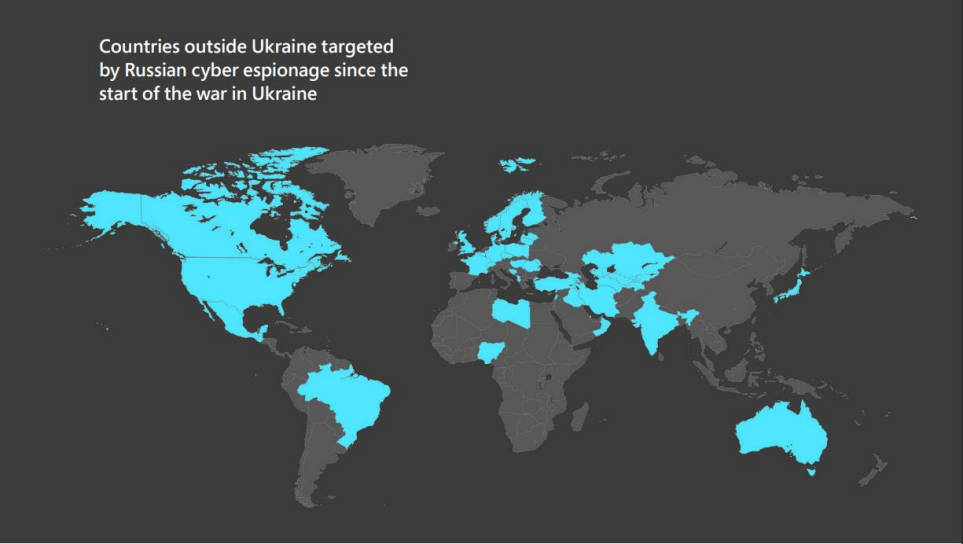
## Destructive malware targeting Ukrainian organizations

- Microsoft Threat Intelligence Center (MSTIC)
- Microsoft Digital Security Unit (DSU)
- Microsoft Defender Threat Intelligence
- Microsoft Detection and Response Team (DART)



Share

Microsoft Threat Intelligence Center (MSTIC) has identified evidence of a destructive malware operation targeting multiple organizations in Ukraine. This malware first appeared on victim systems in Ukraine on January 13, 2022. [Microsoft is aware of the ongoing geopolitical events in Ukraine](#) and surrounding region and encourages organizations to use the information in this post to proactively protect from any malicious activity.



# Understanding how Microsoft approaches security

## ➤ Comprehensive Security

- We secure devices, identities, apps, and clouds, with the full scale of our comprehensive multi-cloud, multi-platform solution.

## ➤ Unique Insights

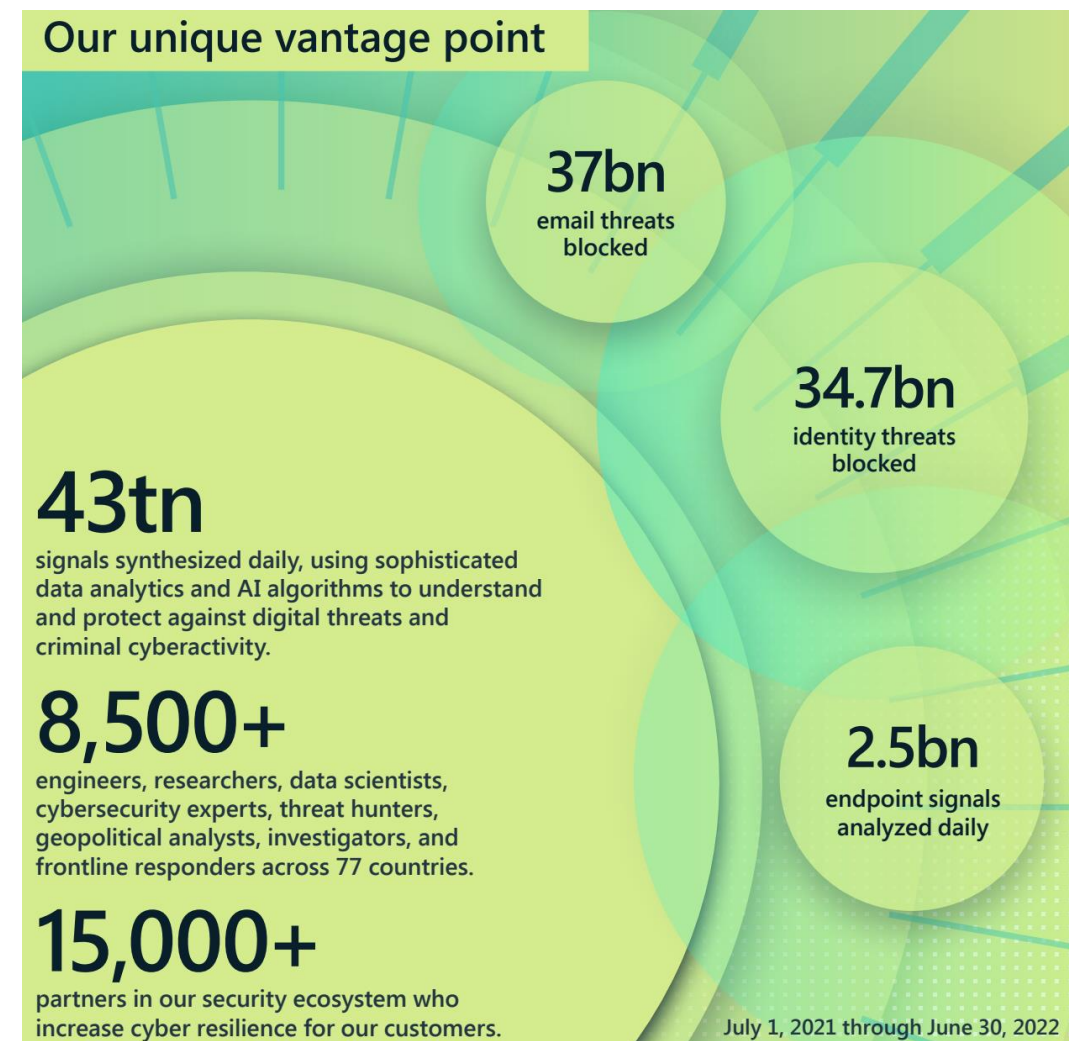
- Our unique view of the global cybersecurity landscape, informed by trillions security signals collected per day, enables us to respond quickly to emerging threats.

## ➤ Built-in Intelligence

- Our security solution is infused with world-class, responsible artificial intelligence (AI) and automation, enriched by always-on global threat intelligence.

## ➤ Our Experience

- We apply learnings and insights gained from protecting our global infrastructure and working with customers across 120+ countries.



# Dismantling cybercrime

To date, Microsoft removed more than 10,000 domains used by cybercriminals and 600 used by nation state actors.



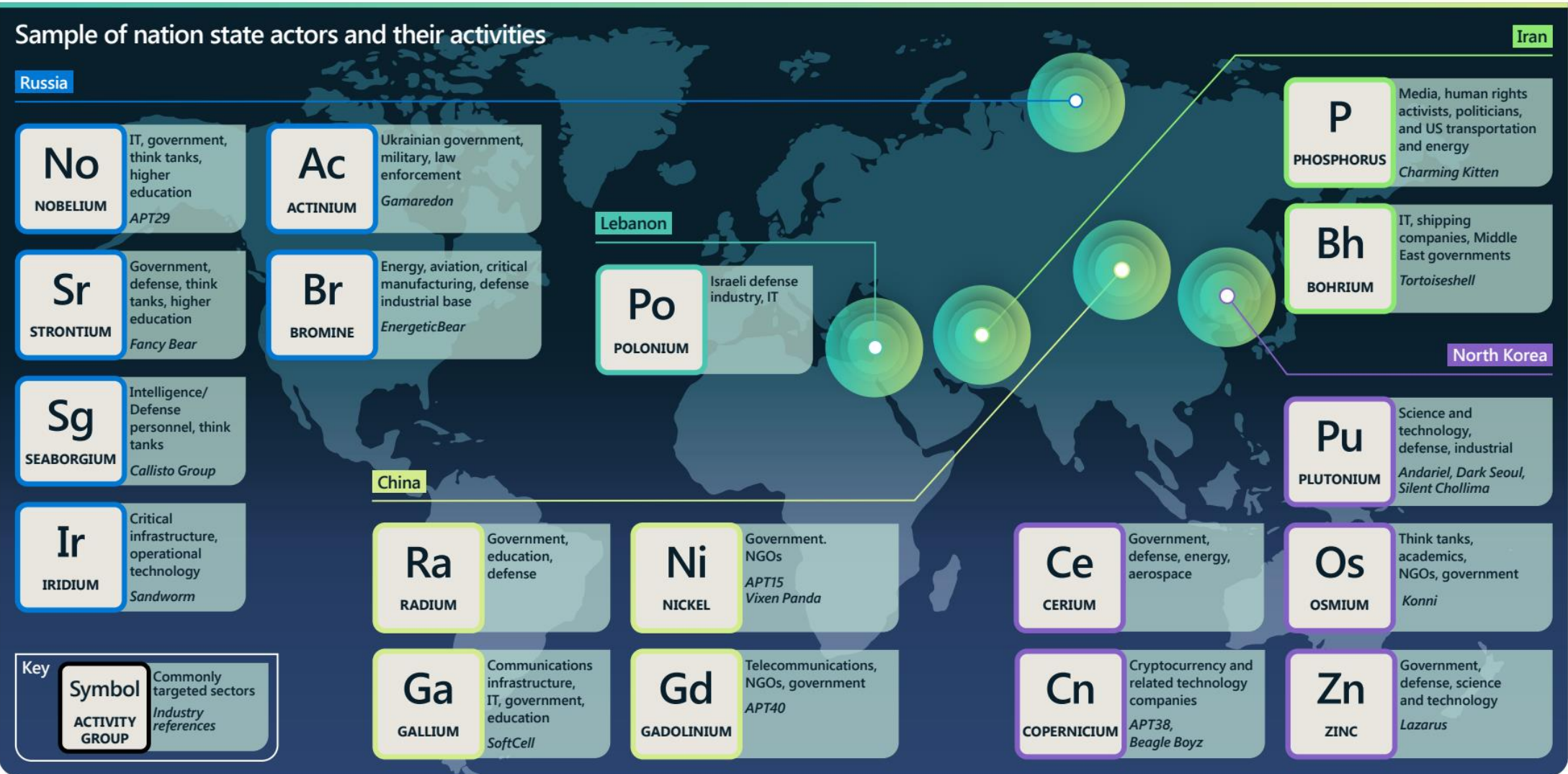
**Notorious cybercrime gang's botnet disrupted,**  
Microsoft's Digital Crimes Unit (DCU), April 2022  
<https://blogs.microsoft.com/on-the-issues/2022/04/13/zloader-botnet-disrupted-malware-ukraine/>

- **Everybody always thinks of advanced attacks or state-sponsored attacks.**
  - The reality is most of these **attacks are pretty low budget**, but yet still effective.
- **Backing up your data essential.**
- **Make sure all your systems are up to date, patched.**
  - Most successful attacks, external attacks, they're taking advantage of vulnerabilities and other types of software exploits. **It's nothing fancy.**
- **You need an internal process of further prioritizing the vulnerabilities** based on your own business context, IT context, your own threat environment to help you patch the system



# Nation State Threats

As of June 2022, we had delivered over 67,000 Nation State Notifications (NSNs) since we began in 2018.



# Cyber Influence Operations

Microsoft is building on its already mature cyber threat intelligence infrastructure to combat cyber influence operations.



- **Democracy needs trustworthy information** to flourish.
- **A key area of focus for Microsoft are the influence operations being developed and perpetuated by nation states.** These campaigns erode trust, increase polarization, and threaten democratic processes.
- **Increased coordination and information sharing** across government, the private sector, and civil society **is needed** to increase transparency and to expose and disrupt these influence campaigns.

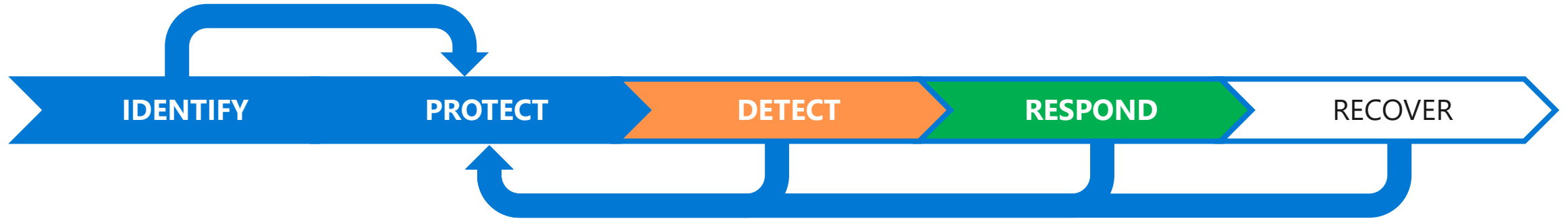


# We focus on raising Cost of Attack

Drive up attacker cost using real world context

## 1. Asset and Vulnerability Identification

(including "audit mode" of policy enforcements)



## 2. Learnings from real world incidents

# Designing for Success and Failure

Then



## **RELIABILITY**

Designed not to fail



## **PREVENT**

Every possible attack

Now



## **RESILIENCE**

Designed to recover quickly



## **ASSUME COMPROMISE**

Protect, Detect & Respond  
along attack  
phases

Security

Resilience

# 4 Dimensions of Threat Timeline



## Geostrategic

T-12

Positioning the **strategic control** within the target.

Usually not activated, in sleeper's mode, being ready to be activated. Potential threat by perceived existence. Strategic value for the adversary, multiple shapes and forms.

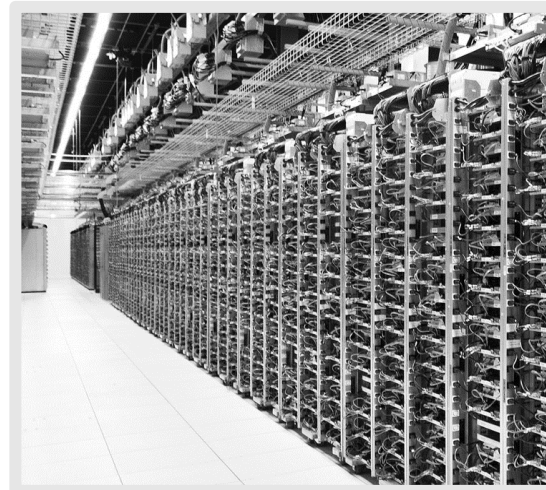


## Operational

T-6

Probing the **operational control** over the target infrastructure.

Activating and learning mode about targeted critical infrastructure and learning about response from targeted objects.



## Cyber

T-1

Activating the **command-and-control** capabilities of infrastructure.

Early indicators of the potential hybrid engagement defined by massive cyber activities activating the sleepers (internal) and deploying the attack vectors (external).



## Crisis

T

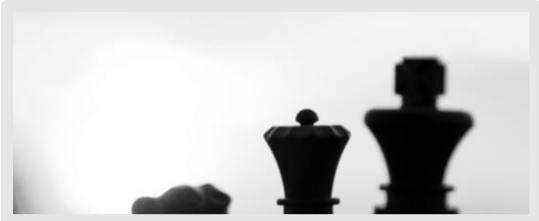
Manifesting the **damaging activities** on targeted objects.

Hybrid crisis manifestation with physical attributes of destruction (war, flood, fire, earthquake, pandemics etc.) with potential cyber activities depending on strategic capabilities.





# Addressing through 4 Dimensions of Resilience



## Geostrategic

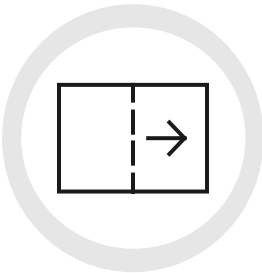


### Partnerships and Coalitions on Digital Signals

Partnerships with other organizations that scale the capabilities and manage early signals. Common interest in protection and security.

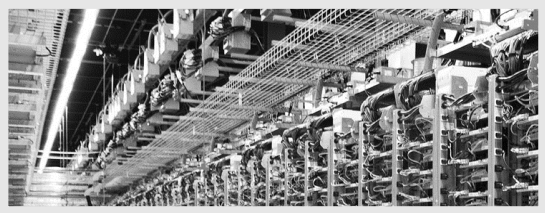


## Operational



### Digital Twins Management Systems with Zero Trust Approach

Building a digital control over the (industrial) environment with clear responsibilities on national (organizational) **critical infrastructure**.



## Cyber

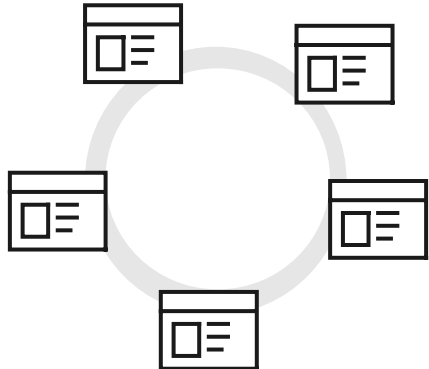


### Security Operation Center w/ Intelligence Graph integration

Strong SOC capabilities integrated with external intelligence networks. Deployed latest integrated tools for **threat intelligence**, but also platform technologies like confidential computing, encryption etc.



## Crisis



### Emergency Management & Response Systems

Software driven capabilities on Public Safety and National Security (+others) that support **availability, confidentiality and integrity** of the data, apps and processes.

# Expand your Trust

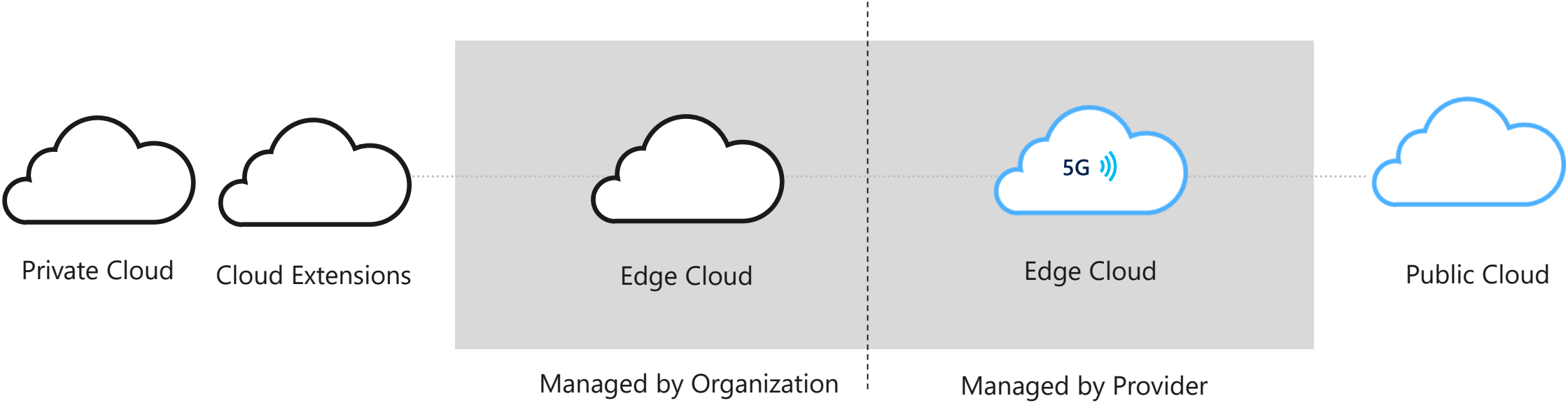
TRUST **CLOUD**

TRUST **BUT VERIFY**



VERIFY **THEN TRUST**

# Cloud Security and Resilience Continuum

← New orchestrated platform services that provide application and services virtualization →



← Consistent security, identity, management, and AI →

Datacenters & Private Cloud		Edge Cloud	Hyperscale Cloud
 Internal approach to protect the classified data, usually disconnected Scenarios with limited resilience scenarios.	 Connected approach that utilizes cloud services but fulfills specific national obligations on data and services governance.	 Connected approach that utilizes cloud services but fulfills specific national obligations on data and services governance.	 External approach for application and data resilience with integrated security intelligence.



# Lessons Learned

Start with: You are compromised. > **CyberSecurity**

Integrity of your data is compromised.

Your cover of adversary's identities.

Your devices are not protected.

Restart with the Zero Trust Security.

Lead with: You will rebound. > **CyberResilience**

Every component of the system will need recovery.

You will recover to different infrastructure.

You will rebuild everything from the scratch.

Restart with Full Scale Resilience.

# The cyber resilience bell curve

**98%**  
Basic security hygiene  
still protects against  
98% of attacks



Key

- Enable multifactor authentication
- Apply Zero Trust principles
- Use modern anti-malware
- Keep up to date
- Protect data

# Microsoft Mission

Empower every person and every organization on the planet to achieve more.

Illuminating the threat landscape and empowering a digital defense.

- Learn more: <https://microsoft.com/mddr>
- Dive deeper: <https://blogs.microsoft.com/on-the-issues/>
- 🐦 Stay connected: @msftissues and @msftsecurity

