Tomorrow's Contested Cyberspace: What It Means for Us

Mark McIntyre, CISSP, CCSP
Executive Security Advisor
marmci@microsoft.com
marmci@microsoftfederal.com

Microsoft on the Front Lines

Protecting

850K organizations in 120 countries

Analyzing

75T threat signals every day

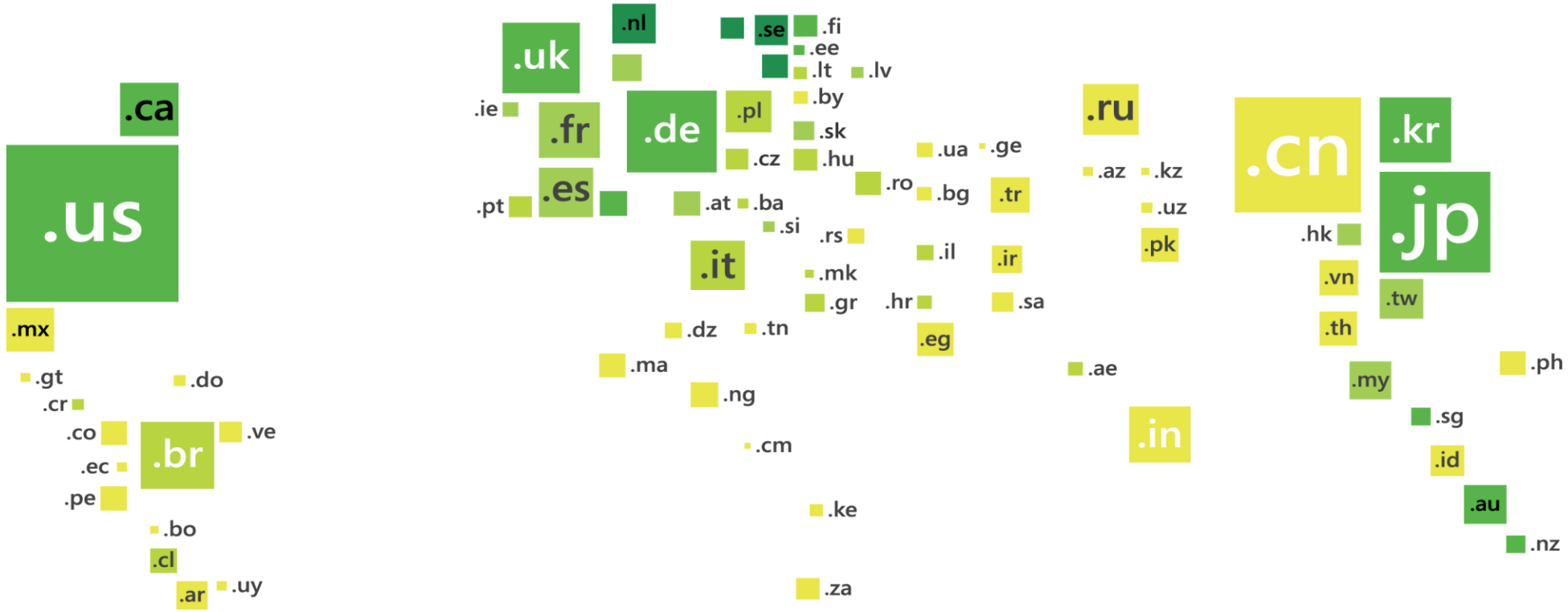
Tracking

40+ nation-state actors & 140+ threat groups

Blocked

32B email threats last year

Microsoft



2005 Internet User Map

Sizing Legend

▫ = 2M Internet Users

□ = 5M Internet Users

Percent Penetration of Internet Users

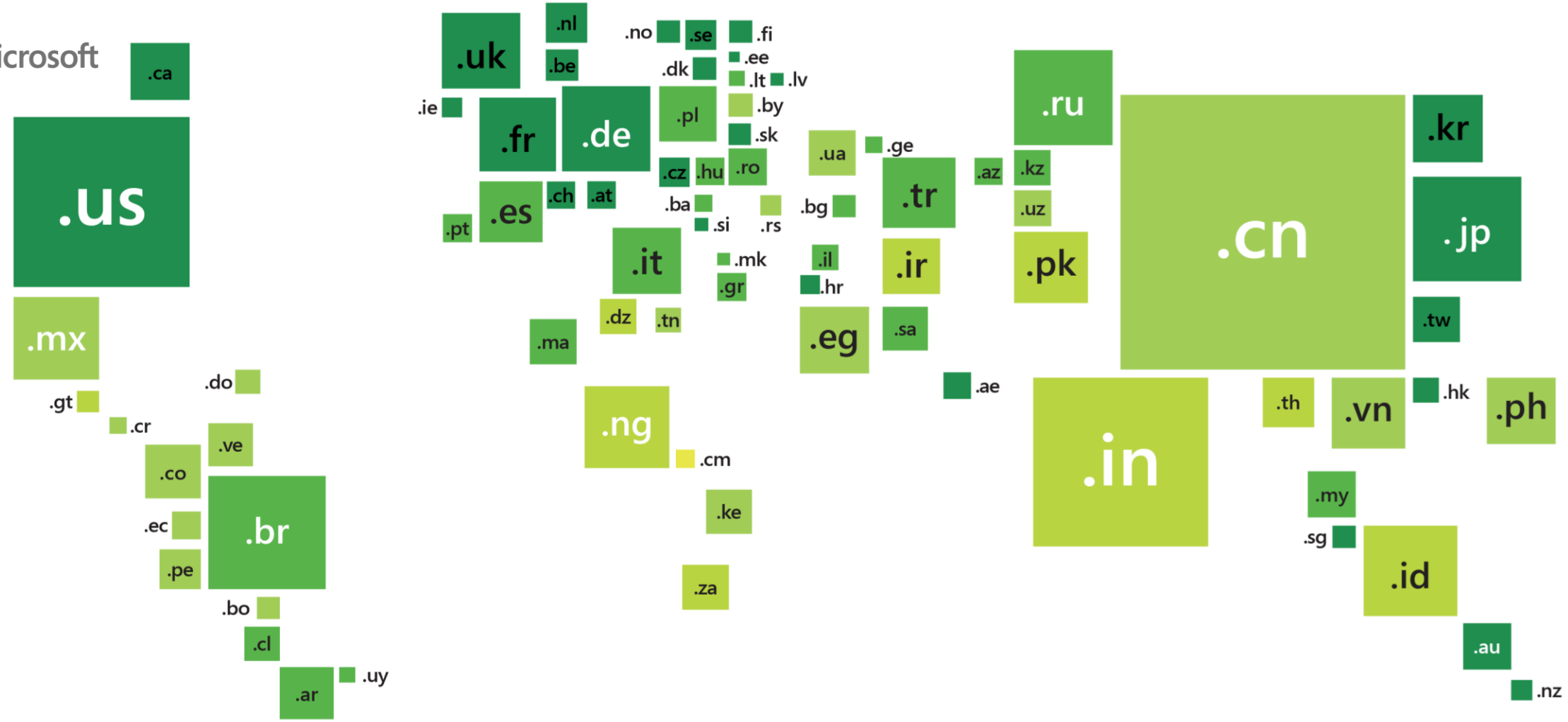
0 20 40 60 80 100

Number of Internet Users

USA	China	Japan	Germany	United Kingdom	Brazil	South Korea	India
201M	111M	86M	57M	42M	38M	35M	26M

Data visualization and design created by Column Five Media, data provided by Euromonitor Intl.; map concept derived from Geographies of the World's Knowledge, Graham, M., Hale, S.A., and Stephens, M. (Convoco! Edition, London, 2011).

Microsoft



2015 Internet User Map

Sizing Legend

▫ = 2M Internet Users

□ = 5M Internet Users

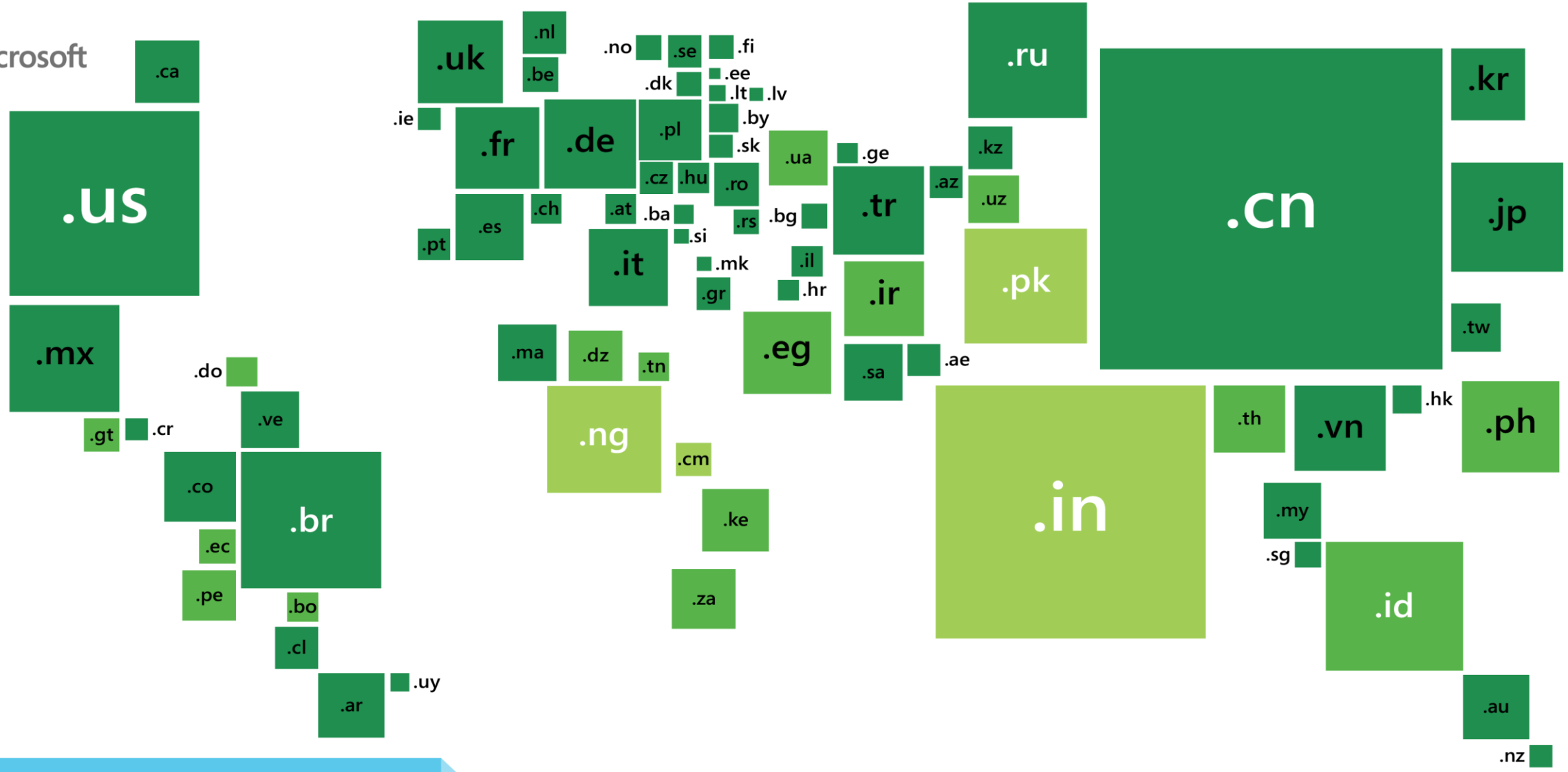
Percent Penetration of Internet Users

0 20 40 60 80 100

Number of Internet Users

China	USA	India	Brazil	Russia	Germany	Mexico	Nigeria
751M	287M	283M	127M	90M	72M	68M	66M

Microsoft



2025 Internet User Map

Sizing Legend

▫ = 2M Internet Users

□ = 5M Internet Users

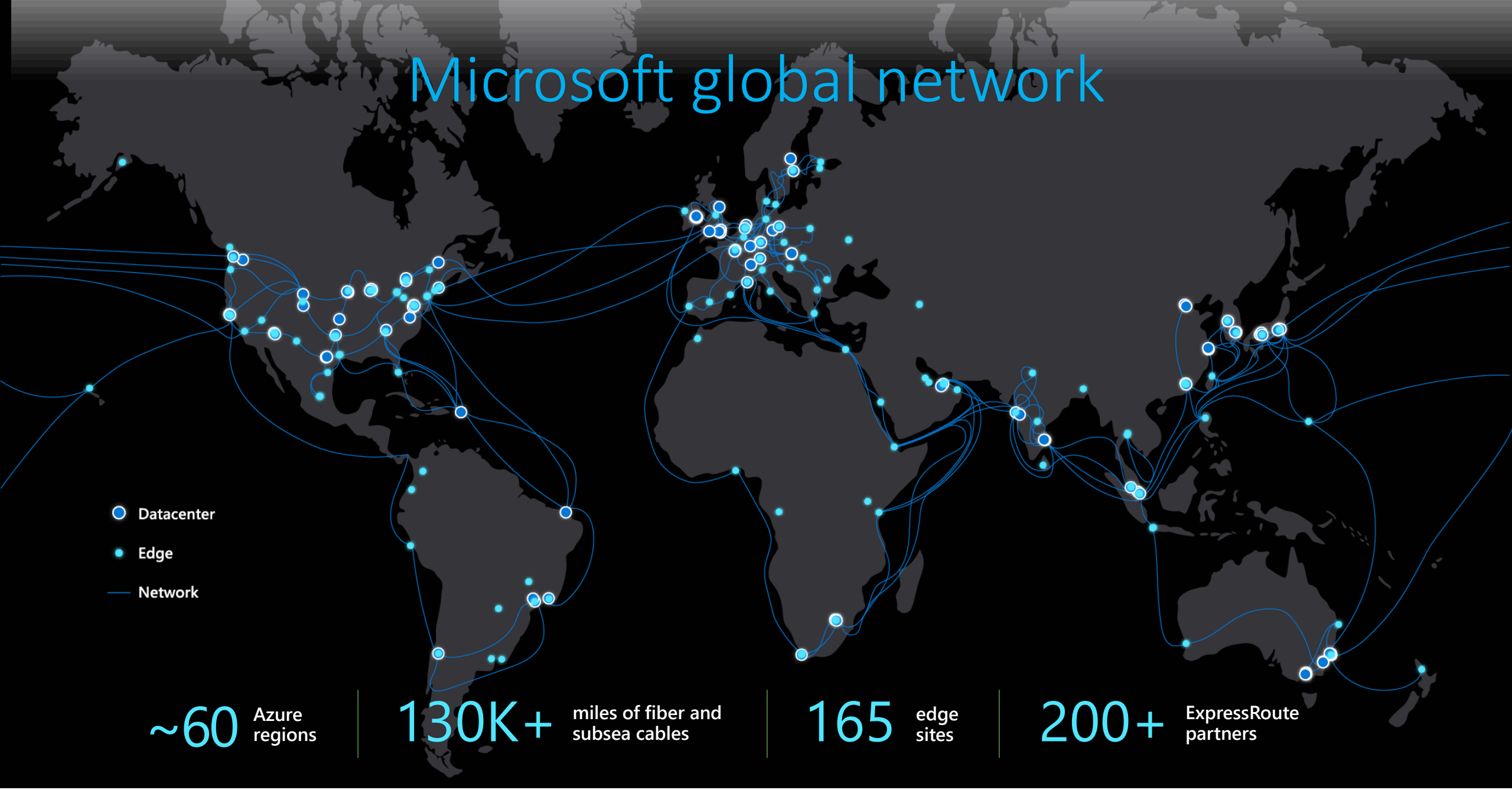
Percent Penetration of Internet Users

0 20 40 60 80 100

Number of Internet Users

China	India	USA	Indonesia	Brazil	Pakistan	Nigeria	Russia
1.1B	708M	317M	183M	173M	146M	126M	124M

Microsoft global network



~60 Azure regions

130K+ miles of fiber and subsea cables

165 edge sites

200+ ExpressRoute partners

Microsoft Intelligent Security Association

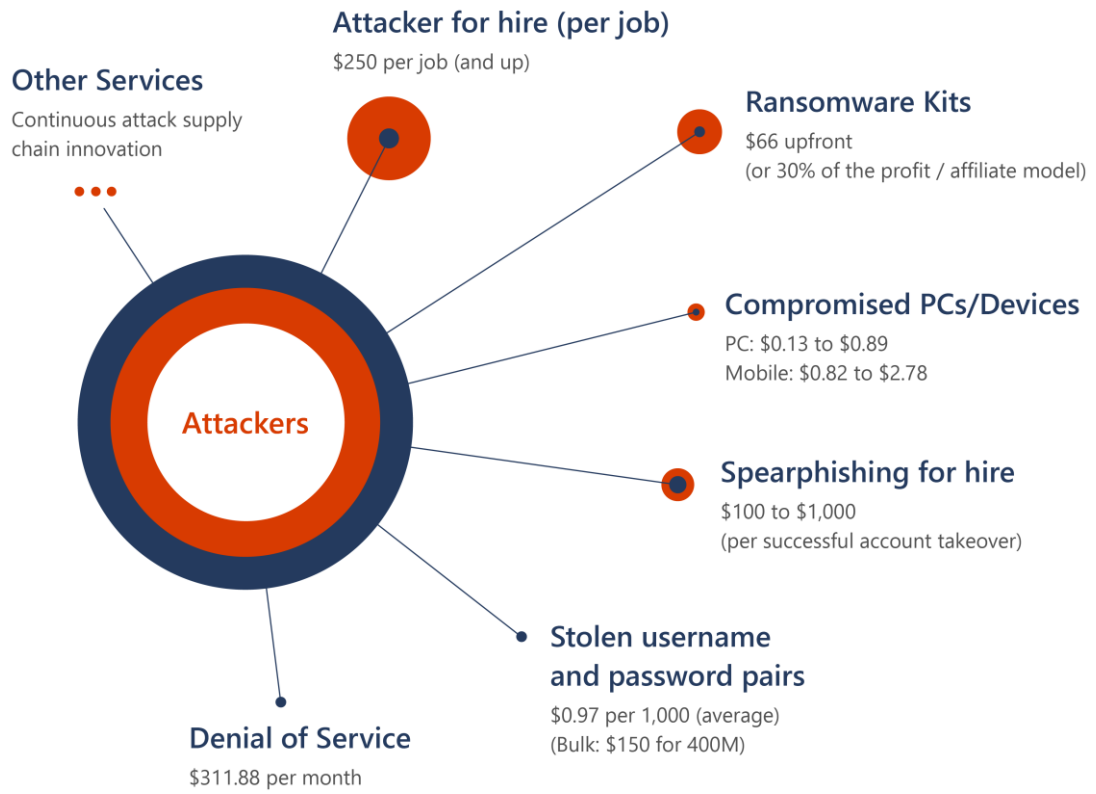
The growing threat of cybercrime

- 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

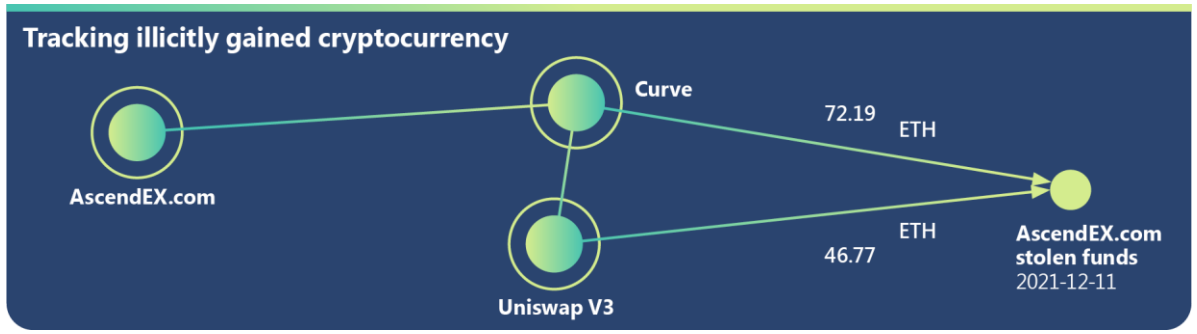


WITH NO TECHNICAL KNOWLEDGE OF HOW TO CONDUCT A CYBERCRIME ATTACK, AN AMATEUR THREAT ACTOR CAN PURCHASE A RANGE OF SERVICES TO CONDUCT THEIR ATTACKS WITH ONE CLICK.

Cybercrime as a service (CaaS)

Trends we're seeing:

- The number and sophistication of cybercrime services is increasing.
- Homoglyph domain creation services are increasingly requiring payment in cryptocurrencies.
- Sellers of cybercrime services are increasingly offering compromised credentials for purchase.
- CaaS services and products with enhanced features for avoiding detection are emerging.
- End-to-end cybercrime services are selling subscriptions to managed services.



This diagram illustrates the laundering routes used by AcendEX hackers, uncovered by Microsoft's Digital Crimes Unit.

2,750,000

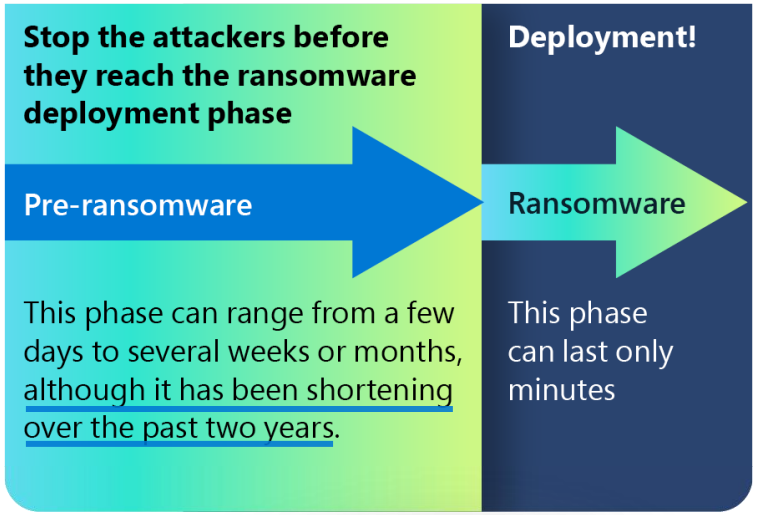
Site registrations successfully blocked by DCU this year to get ahead of criminal actors that planned to use them to engage in global cybercrime.

Ransomware and extortion: A nation-level threat

Human operated ransomware targeting and rate of success model

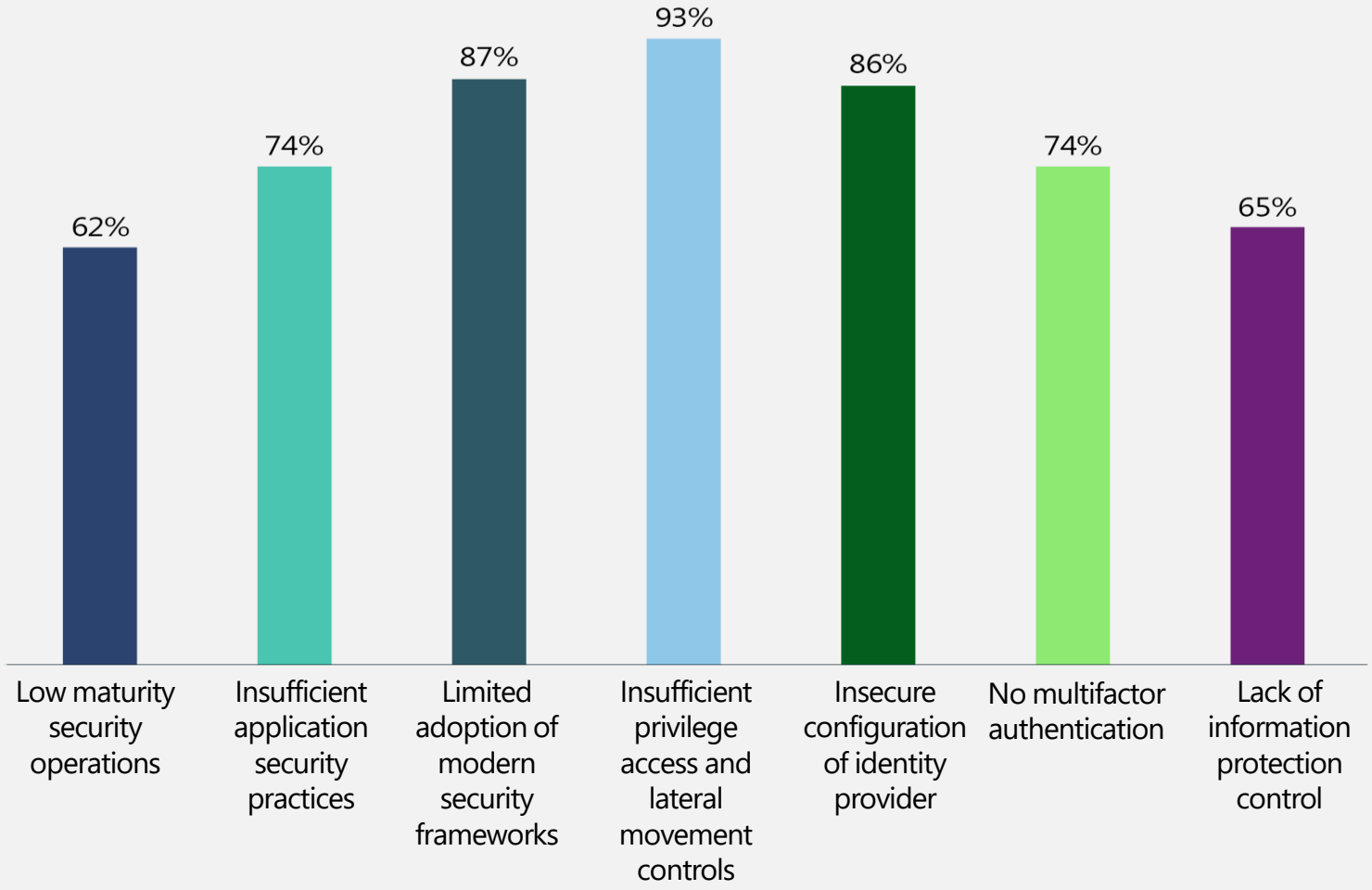
Model based on Microsoft Defender for Endpoint (EDR) data (January-June 2022).

The typical human-operated attack

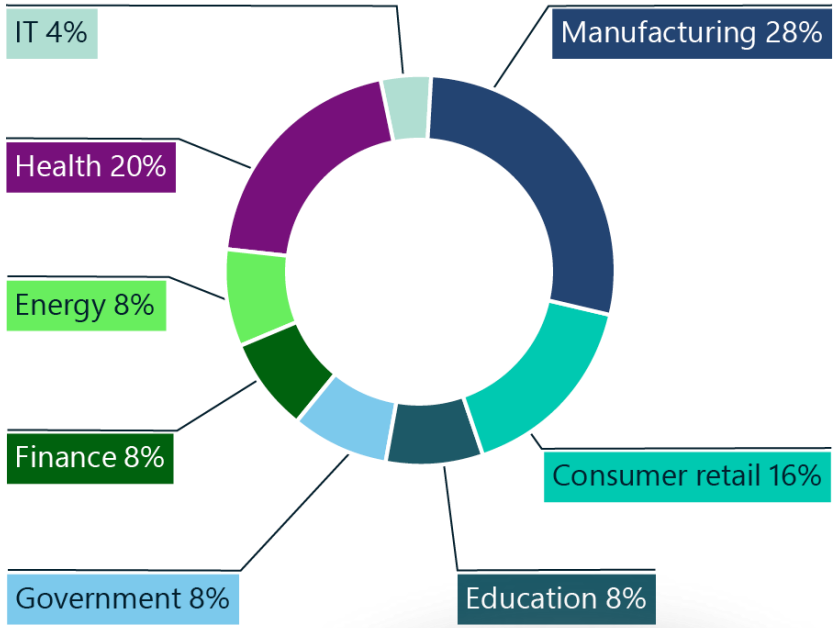


More so than malware, attackers need credentials to succeed in their operations. The successful human operated ransomware infection of an entire organization relies on access to a highly privileged account.

Ransomware insights from frontline responders



Ransomware incident and recovery engagements by industry



93%

of Microsoft ransomware recovery investigations revealed insufficient controls on privilege access and lateral movement.

The phishing threat landscape

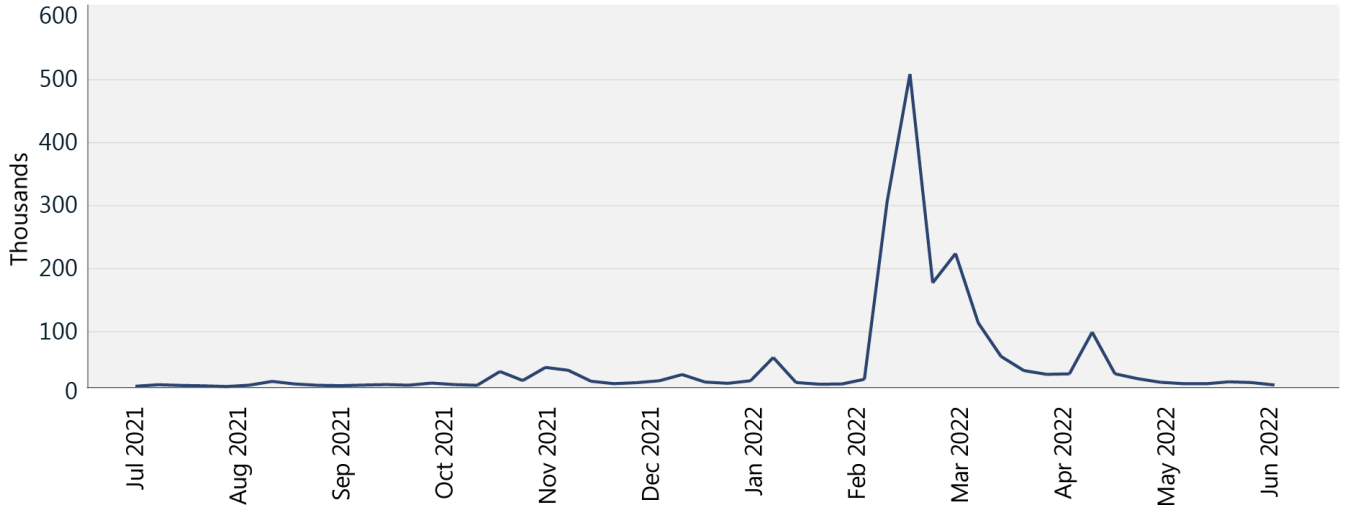
710 million
phishing emails blocked per week.

531,000
Unique phishing URLs hosted outside of Microsoft taken down at the direction of our Digital Crimes Unit.

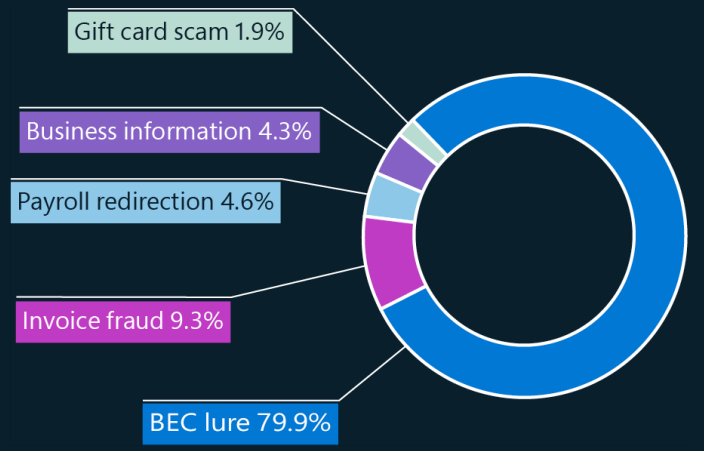
1hr 12m
The median time it takes for an attacker to access your private data if you fall victim to a phishing email.

1hr 42m
The median time for an attacker to begin moving laterally within your corporate network once a device is compromised.

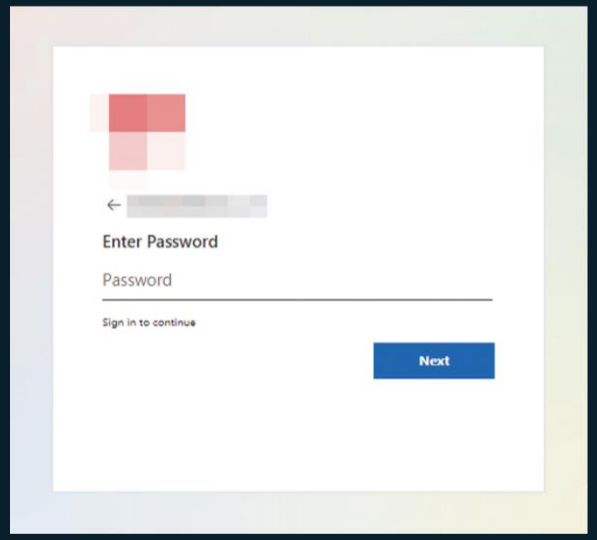
Phishing emails with Ethereum wallet addresses



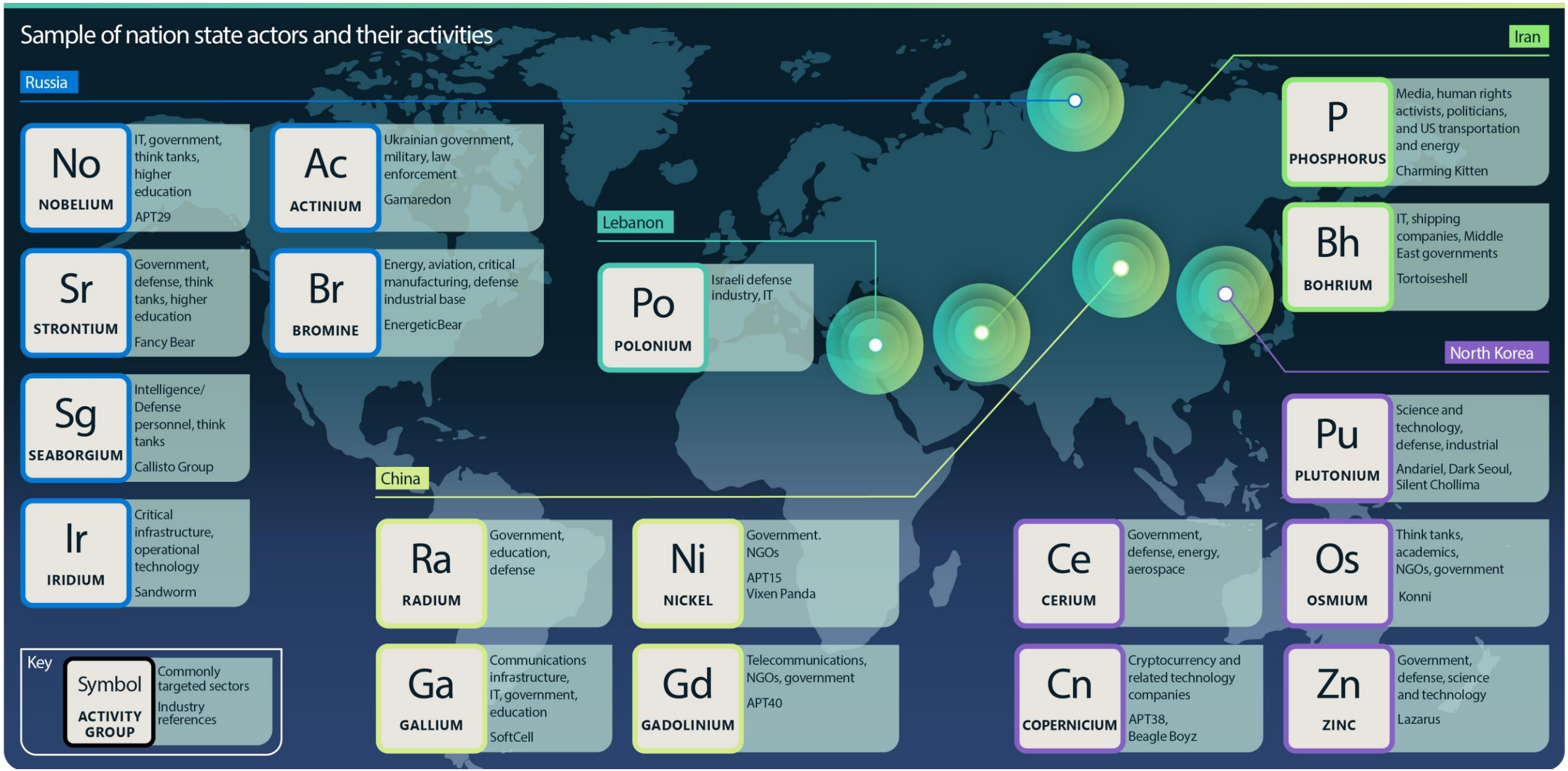
Business email compromise themes (January-June 2022)



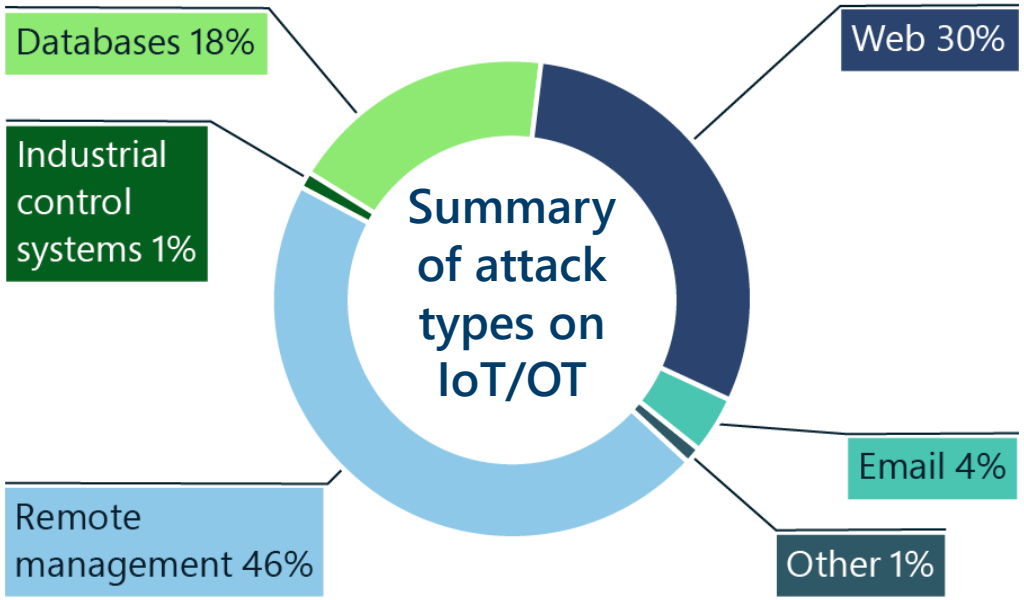
Phishing page impersonating a Microsoft login with dynamic content



About our nation state data

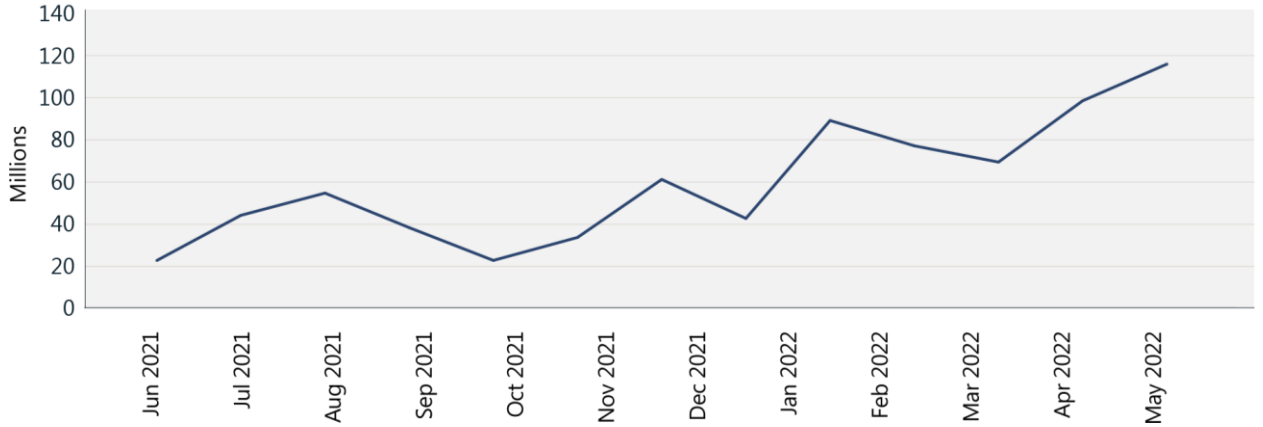


IoT and OT exposed: Trends and attacks

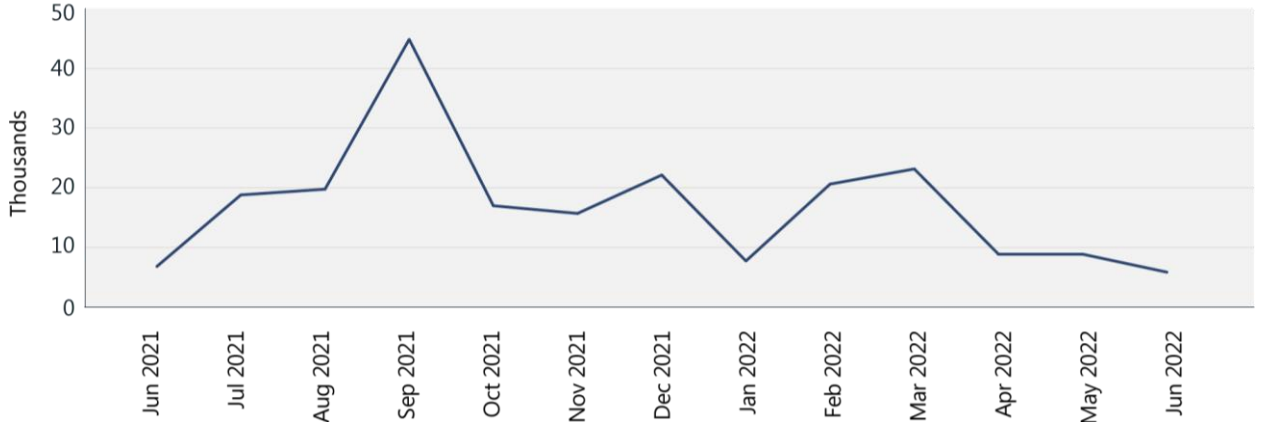


IoT devices pose unique security risks as entry and pivot points in the network. Millions of IoT devices are unpatched or exposed.

Attacks against remote management devices



Web attacks against IoT and OT



Spotlight on firmware vulnerabilities

27%

Contained accounts with passwords encoded using weak algorithms.

32%

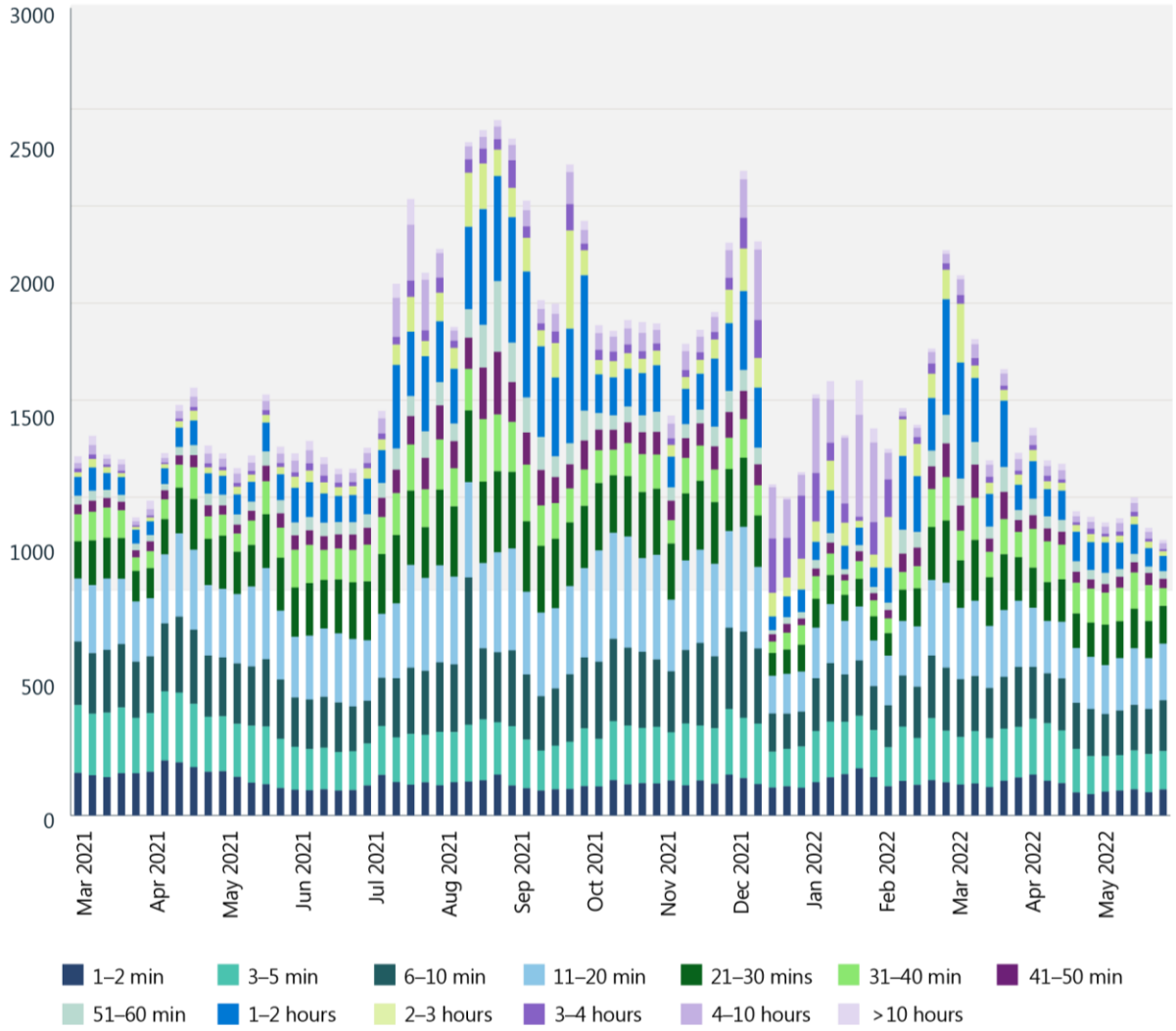
of firmware images analyzed contained at least 10 known critical vulnerabilities.

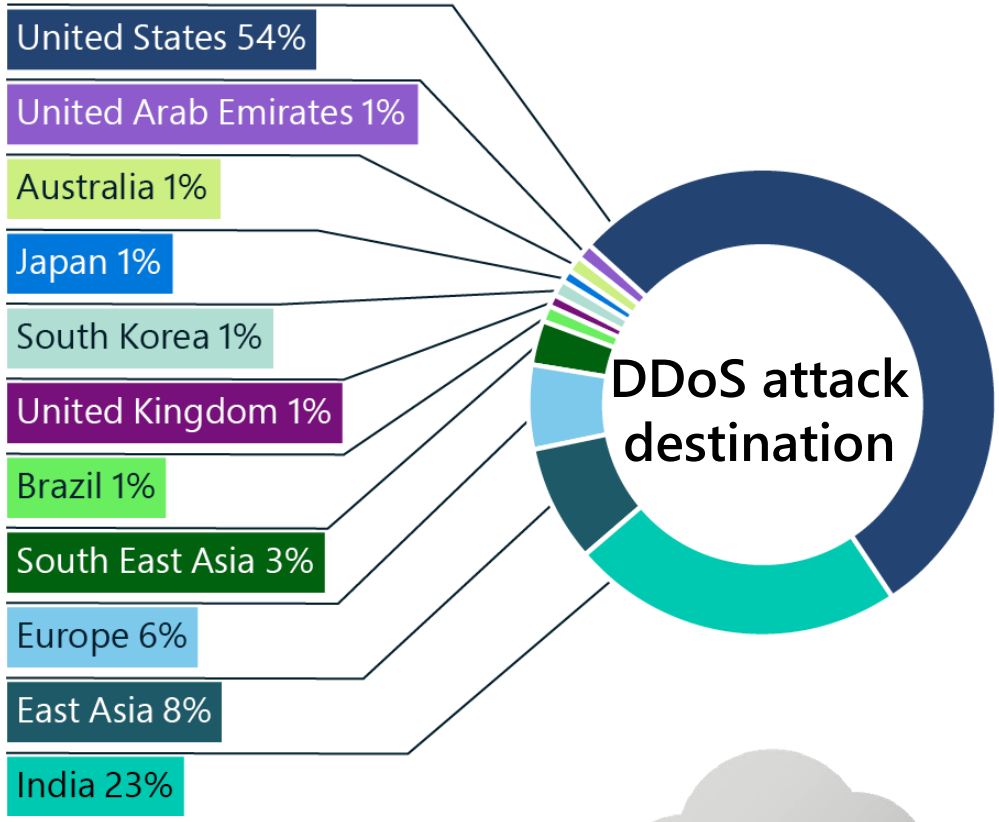
Microsoft is partnering with government and industry on firmware analysis technology for deeper visibility and full lifecycle device security.

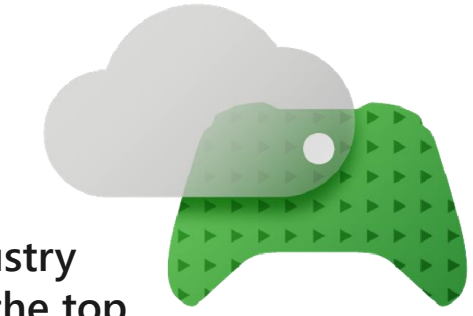
Security weaknesses in firmware images analyzed

What we're seeing in DDoS attacks

DDoS attack duration distribution
(March 20–21May 2022)

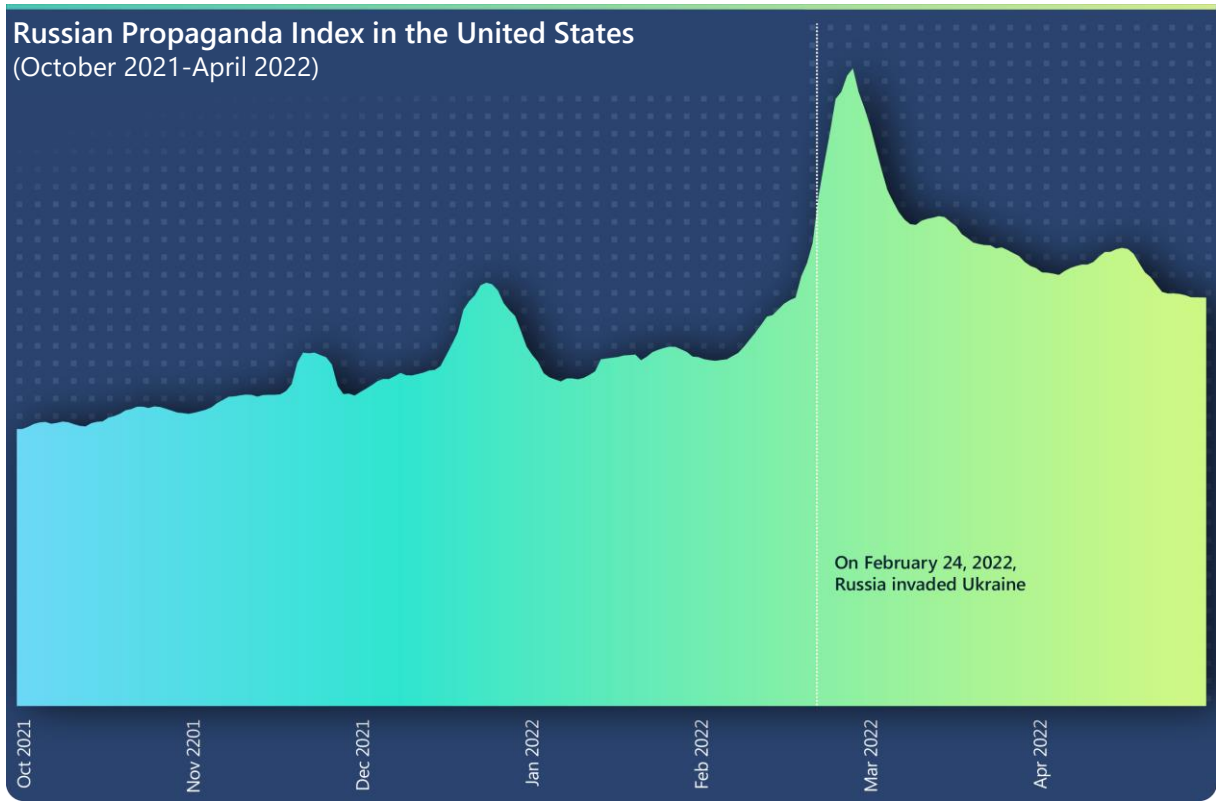






The gaming industry continues to be the top target of DDoS attacks.

Tracking the Russian Propaganda Index



Microsoft is building on its already mature cyber threat intelligence infrastructure to develop a broader, more inclusive view of cyber influence operations.

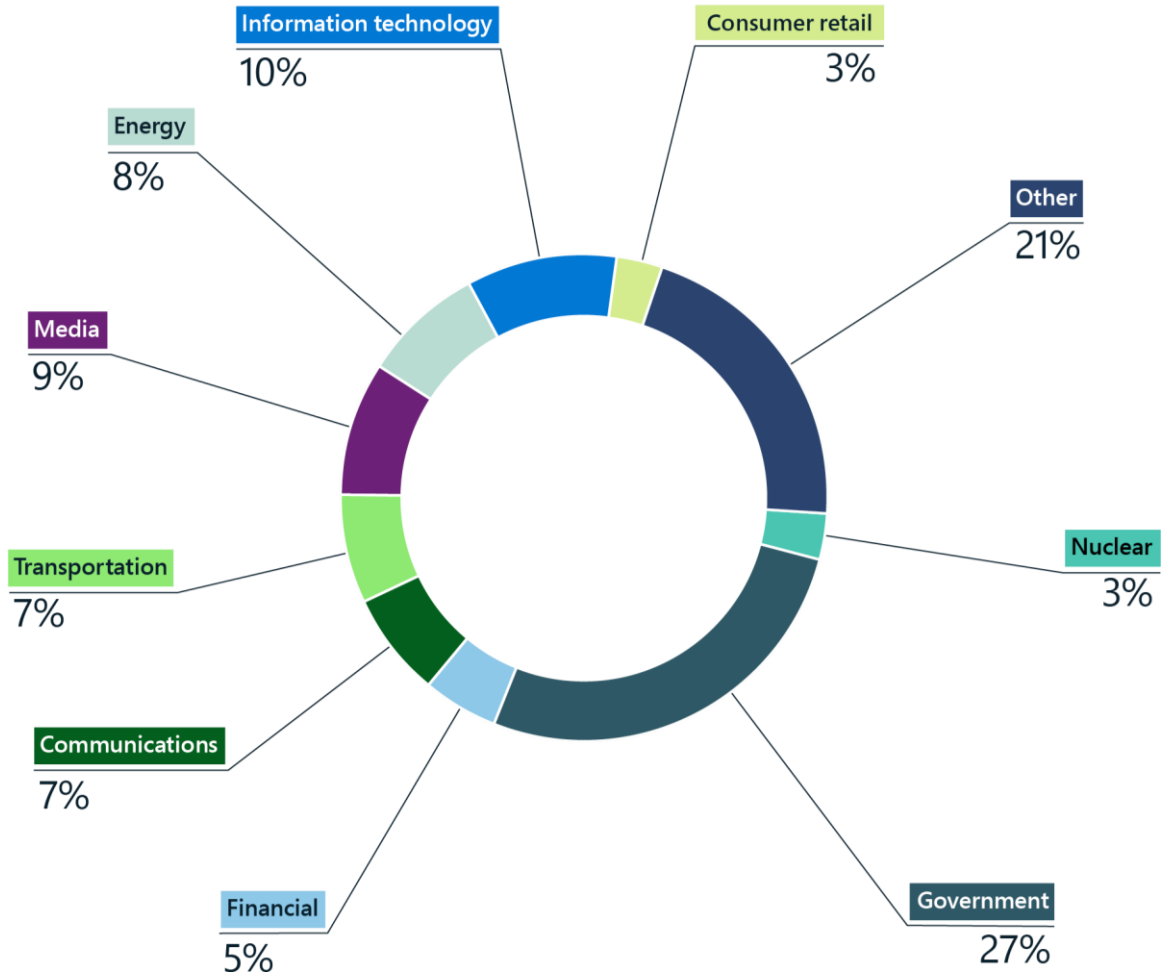
Russian false narrative around purported bioweapons and biolabs in Ukraine

Nov 29, 2021
Narrative uploaded to YouTube

Feb 24, 2022
Narrative "sent into battle" just as Russian tanks crossed the Ukraine border.

Russian state actors' wartime cyber tactics threaten Ukraine and beyond

Most targeted industry sectors in Ukraine since the invasion

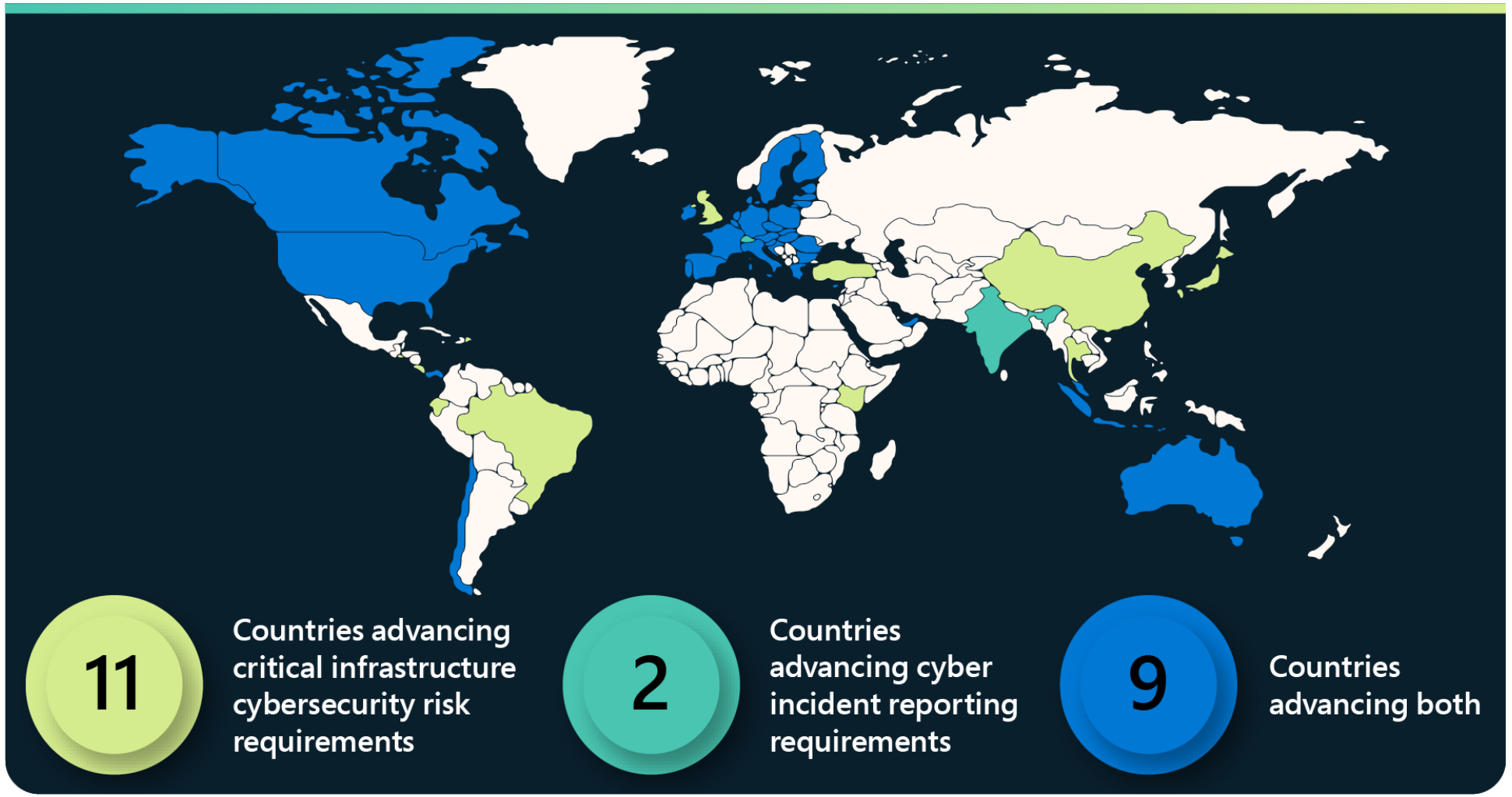


Cyber Resilience

Understanding the risks and rewards of modernization becomes crucial to a holistic approach to resilience.

Governments act to improve critical infrastructure security and resilience

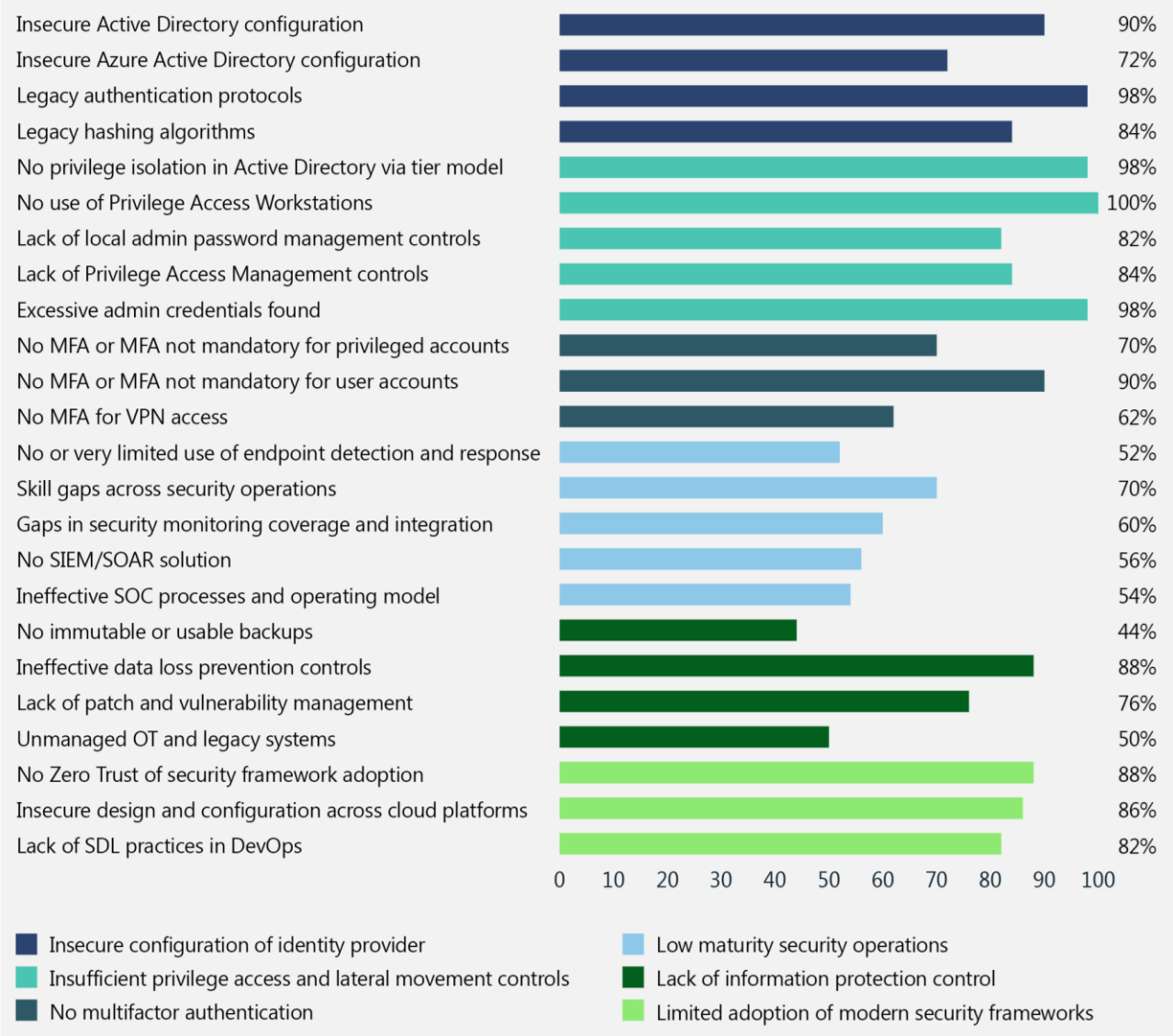
Governments worldwide are developing and evolving policies to manage critical infrastructure cybersecurity risk.



July 2021-June 2022

The importance of modernizing systems and architecture

Key issues impacting cyber resiliency



Over 80 percent of security incidents can be traced to a few missing elements that could be addressed through modern security approaches.

This chart shows the percentage of impacted customers missing basic security controls which are critical to increasing organizational cyber resilience. Findings are based on Microsoft engagements over the past year.

As we develop new capabilities for a hyperconnected world, we must manage the threats posed by legacy systems and software.

Recommendations

Understand strategic priorities of Russia, China, Iran, and North Korea to identify high-value data targets and at-risk technologies, information, and business operations.

Assess the threat landscape of critical infrastructure and high-value organizations to determine risk exposure and the likelihood of being targeted for intellectual property theft or third-party partnerships.

Implement a proactive cybersecurity strategy and legal framework that defines and addresses changing roles and responsibilities for all parties involved in any security incident.

Conduct due diligence on third-party contractors.

Implement latest patches for internet-facing servers, systems, databases, and applications.

Enable multi-factor authentication for corporate network access wherever possible.

The cybersecurity bell curve:

Basic security hygiene still protects against 98% of attacks

Enable multifactor authentication

Make it harder for bad actors to utilize stolen or phished credentials by enabling multifactor authentication. Always authenticate and authorize based on all available data points, including user identity, location, device health, service or workload, data classification, and anomalies.

Apply least privilege access

Prevent attackers from spreading across the network by applying least privilege access principles, which limits user access with just-in-time and just-enough-access (JIT/JEA), risk-based adaptive polices, and data protection to help secure both data and productivity.

Keep up to date

Mitigate the risk of software vulnerabilities by ensuring your organization's devices, infrastructure, and applications are kept up to date and correctly configured. Endpoint management solutions allow policies to be pushed to machines for correct configuration and ensure systems are running the latest versions.

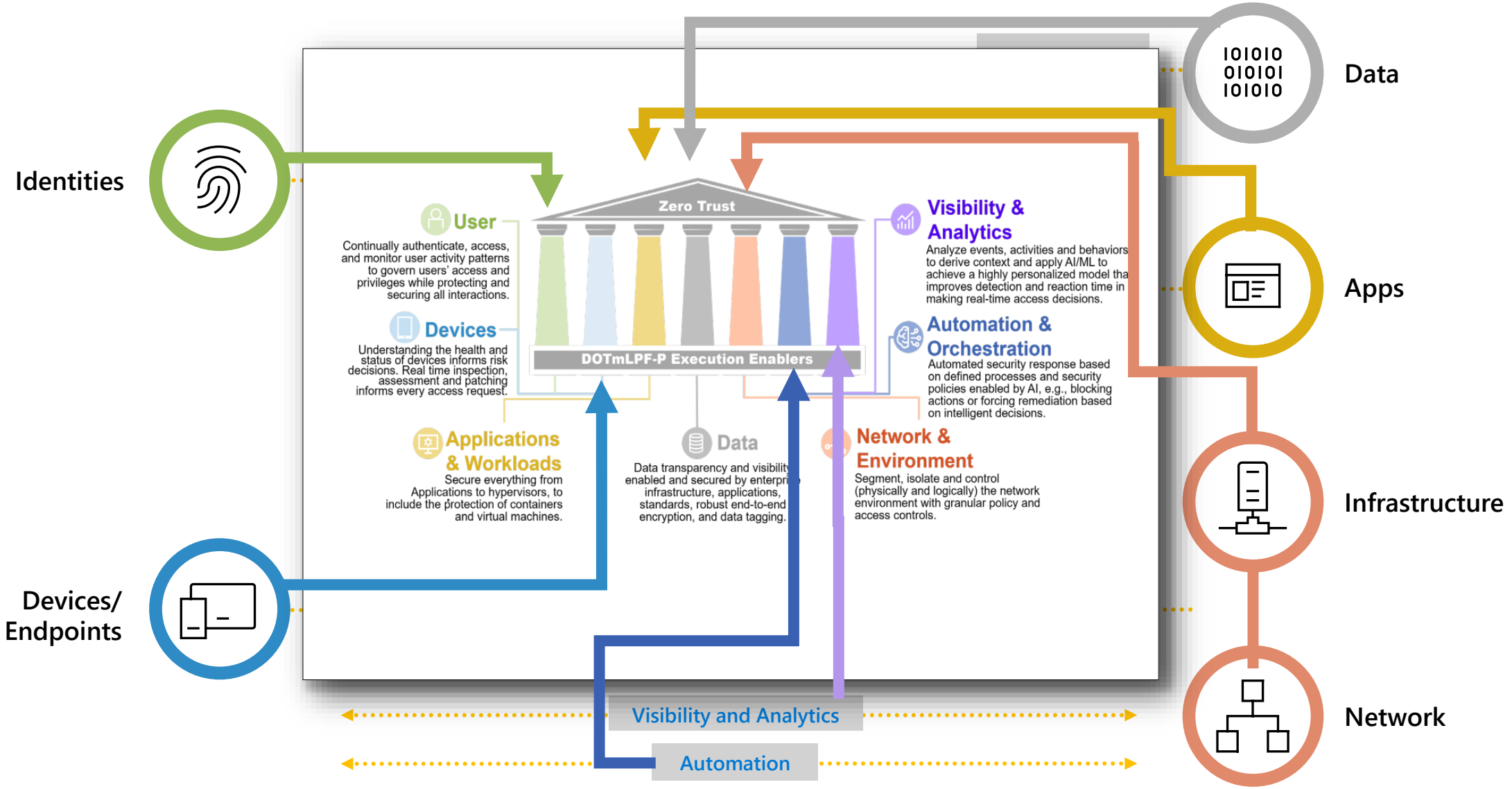
Utilize antimalware

Stop malware attacks from executing by installing and enabling antimalware solutions on endpoints and devices. Utilize cloud-connected antimalware services for the most current and accurate detection capabilities.

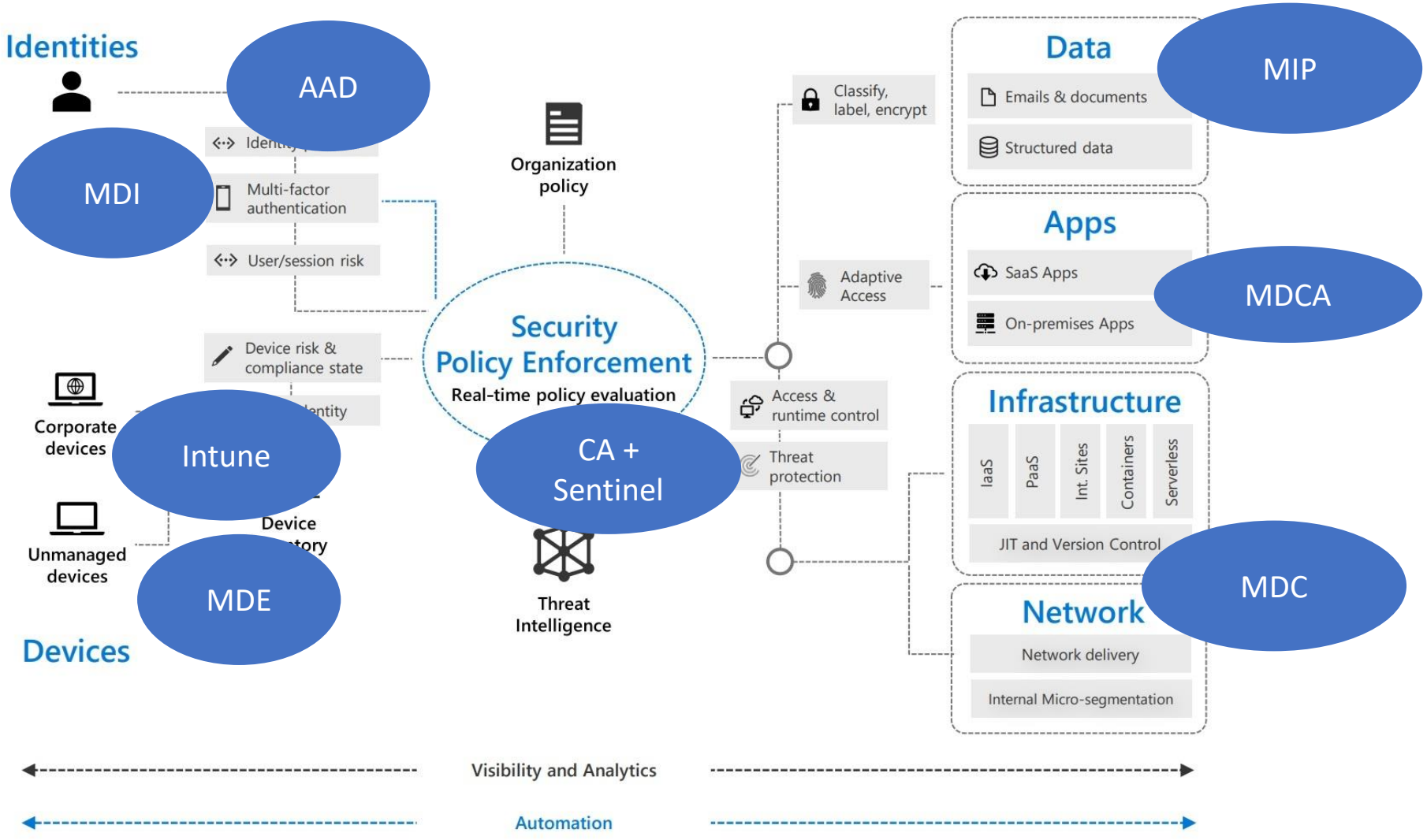
Protect data

Know where your sensitive data is stored and who has access. Implement information protection best practices such as applying sensitivity labels and data loss prevention policies. If a breach does occur, it's critical that security teams know where the most sensitive data is stored and accessed.

Microsoft-DOD Zero Trust Alignment



Zero Trust with M365+Azure



MSSA | Microsoft Software & Systems Academy

MSSA is offered virtually and accessible worldwide to all active-duty service members and veterans provided they can accommodate the instructional time zone.

MSSA international offerings include the Asia Pacific and European regions to help facilitate instruction in a more favorable time zone for US service members and allies, the Australian Defense Force (ADF) and Ministry of Defense (MoD), respectively, within those regions.

MSSA is fully funded by Microsoft.

MSSA **offers specialization** in:

- Cloud Application Development (CAD)
- Server & Cloud Administration (SCA)
- CyberSecurity & Operations (CSO)

Microsoft

Digital Dexterity Impact on Security

“People are the heart of digital business transformations, but few organizations have a comprehensive strategy to ensure that talent and digital business strategies are aligned.”

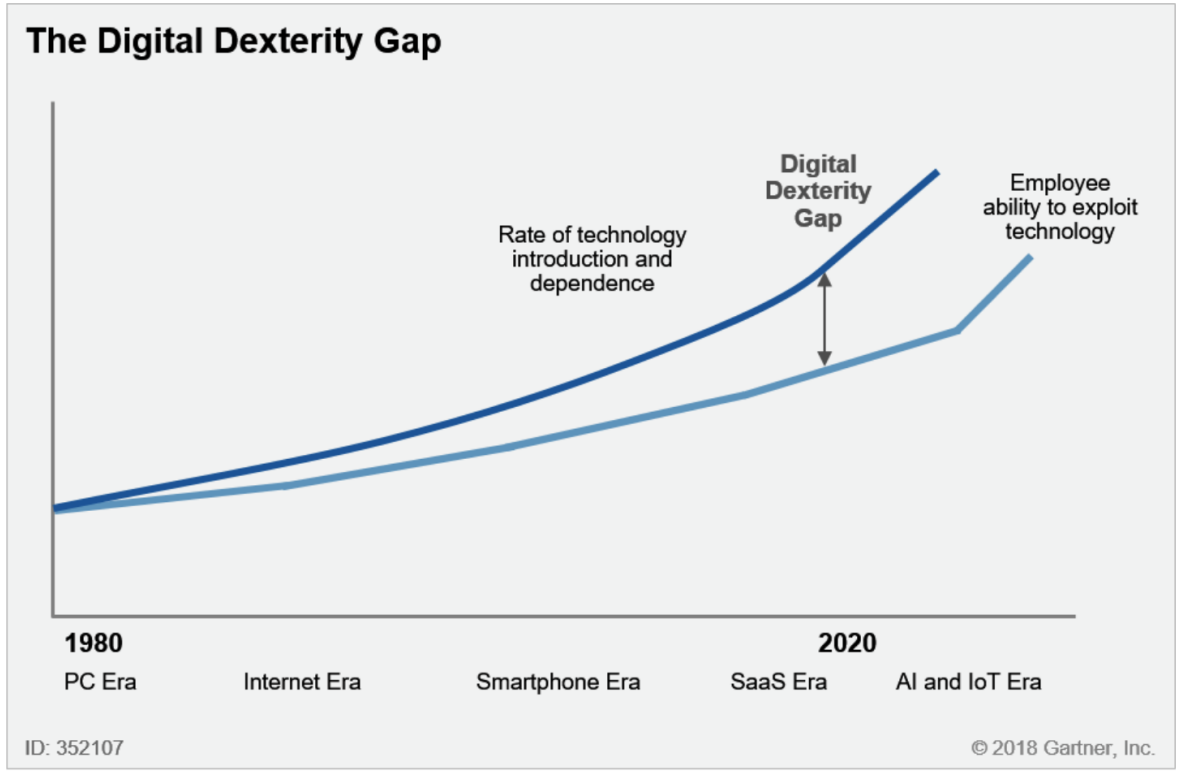
- **Gartner**; Closing the Digital Dexterity Gap in Digital Business Strategies, July 2018

CHALLENGES

Digital business initiatives introduce organizations to new security risks

Customer security teams operate within silos resulting in security awareness gaps within the organization

Customer IT and HR groups rarely promote new digital literacies as part of an engagement initiative



Source: Gartner (June 2018)

MSSA | By the numbers

January 2023, Program All Up

Graduates
3,526

Graduation Rate
95%

Employed or Continuing Education
97%
(includes 12% who chose to pursue a degree - DoD/IMCOM consider continuing education as a result of this program a measure of employment)

Employed in Tech
92%

Unique Companies That Have Hired MSSA Graduates
nearly 1000

Hiring Partners Who Have Hired
3+ graduates = 113 companies
10+ graduates = 29 companies

MSSA | Graduate Profile

- ~8 years active duty
- >90% have active security clearances
- High in learning agility
- Disciplined
- Grace under pressure
- Effectively deals with ambiguity
- Excellent teaming skills
- Highly collaborative
- Experienced in leadership & managing teams

Roles | MSSA grads have been hired as

- Software Engineers
- Service Engineers
- IT/Network Support
- Operations
- Project Managers
- Program Managers
- Help Desk
- (IT) Consultant
- Support Engineer
- (IT) Sales
- Customer Engineer (*previously called PFE*)
- Customer Success Account Manager (*previously called Technical Account Manager*)
- Supply Chain Management
- And many more

Microsoft