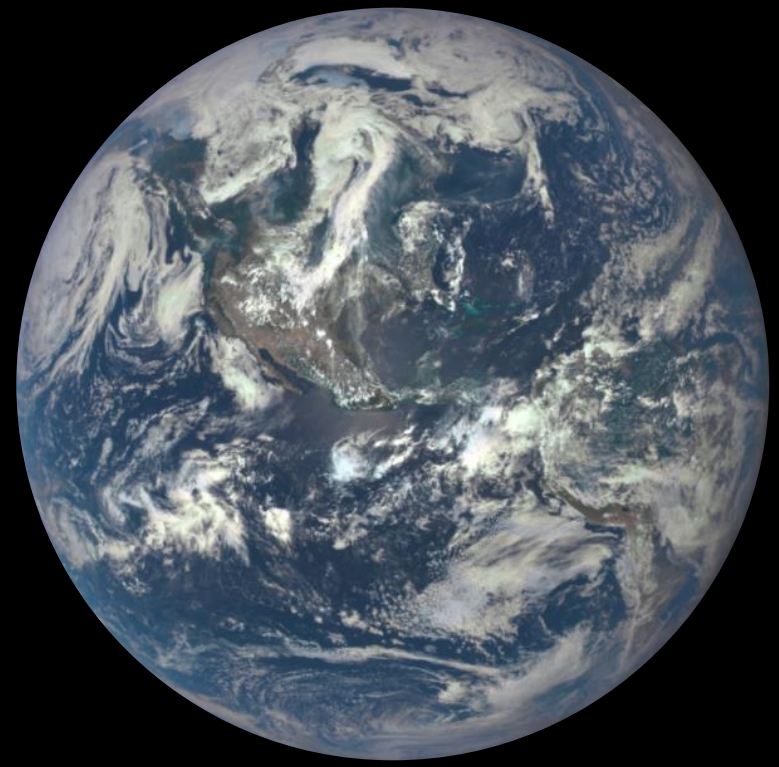
Security for your digital transformation

Aylton Souza

Microsoft

Microsoft mission

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



Microsoft

My own personal journey to empower every person and every organization on the planet to achieve more

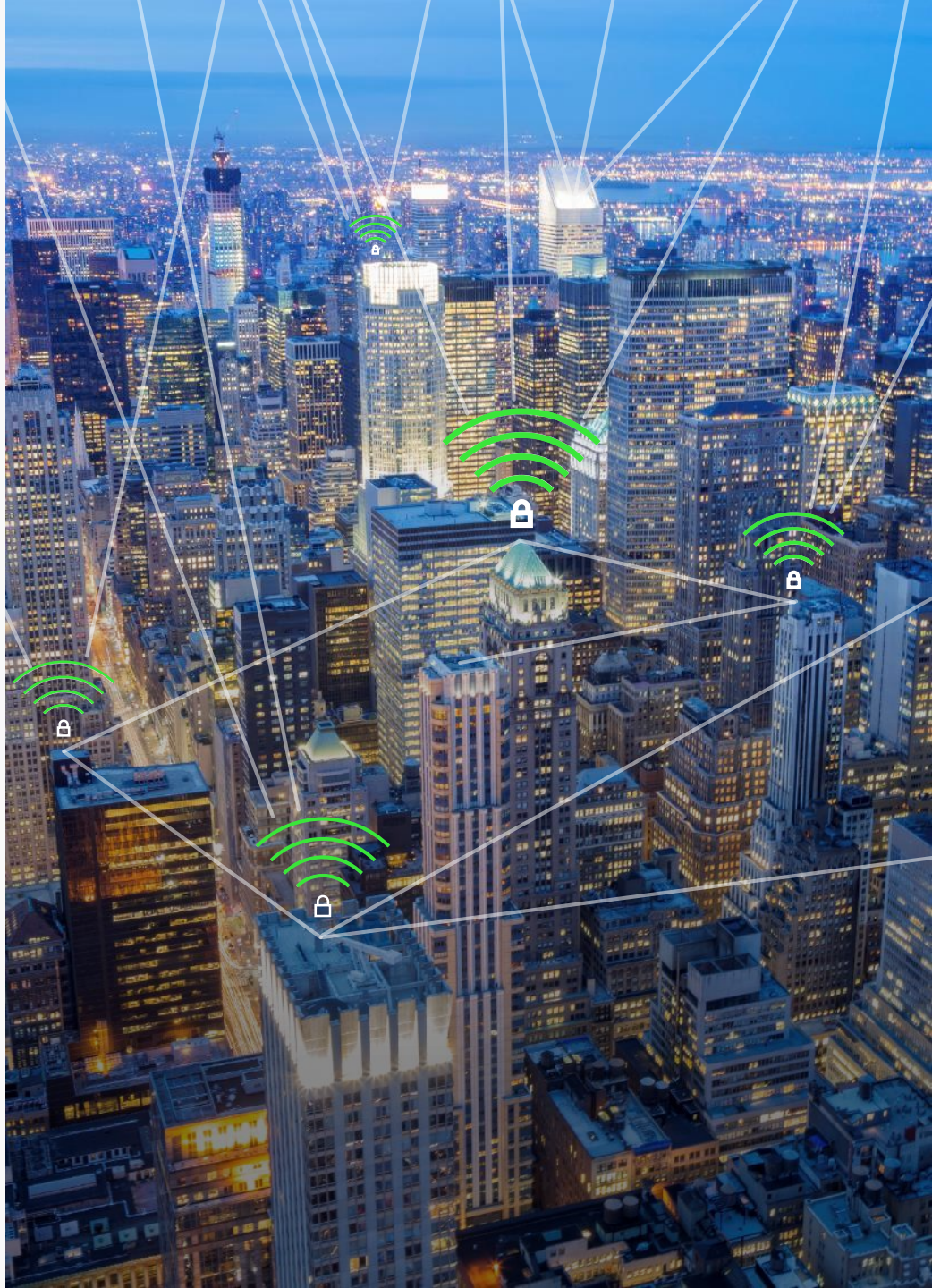
Connecting Women Businesses globally: Accelerating Growth Through Innovation & Technology

OUR COMMITMENT TO **YOU**

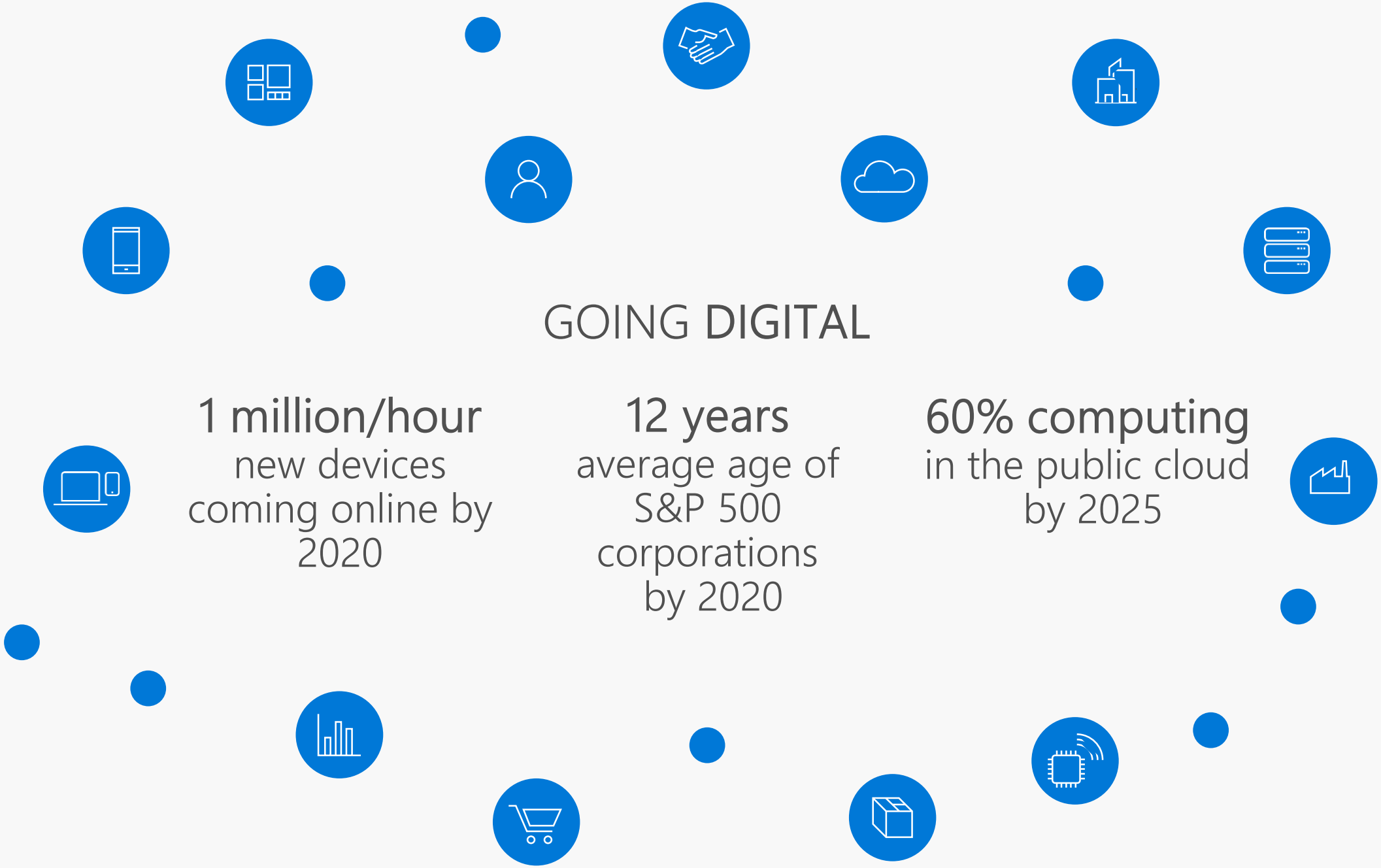
- SECURITY
- PRIVACY & CONTROL
- COMPLIANCE
- TRANSPARENCY
- RELIABILITY

Microsoft Secure

Ensuring security to enable your digital transformation through a comprehensive platform, unique intelligence, and broad partnerships



Microsoft



GOING DIGITAL

1 million/hour
new devices coming online by 2020

12 years
average age of S&P 500 corporations by 2020

60% computing
in the public cloud by 2025

Digital transformation is the next industrial revolution

Steam, water, mechanical production equipment

1784

Division of labor, electricity, mass production

1870

Electronics, IT, automated production

1969

Blurring the physical and the digital divide

2017

Industrial Revolution 4.0

Seeking balance

- With so many capabilities to drive my ideas into business, what are the challenges in cybersecurity?

A NEW REALITY: TURBULENT TIMES

2 Billion records compromised in the last year

99+ DAYS between infiltration and detection

$15 MILLION of cost/business impact per breach


YOUR
IT ENVIRONMENT


YOUR
IT ENVIRONMENT


YOUR
IT ENVIRONMENT
YOUR
OPPORTUNITY

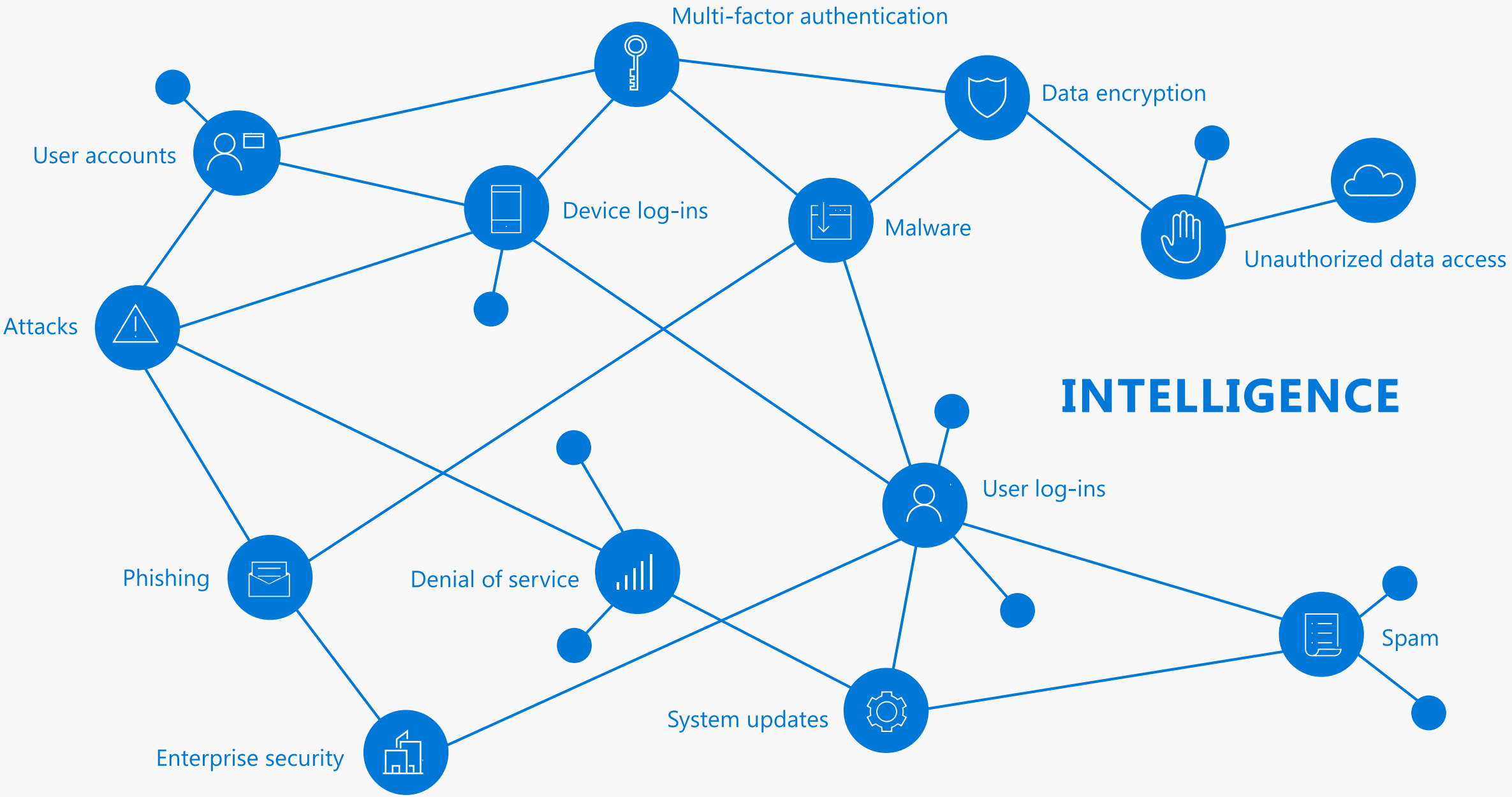

YOUR
IT ENVIRONMENT

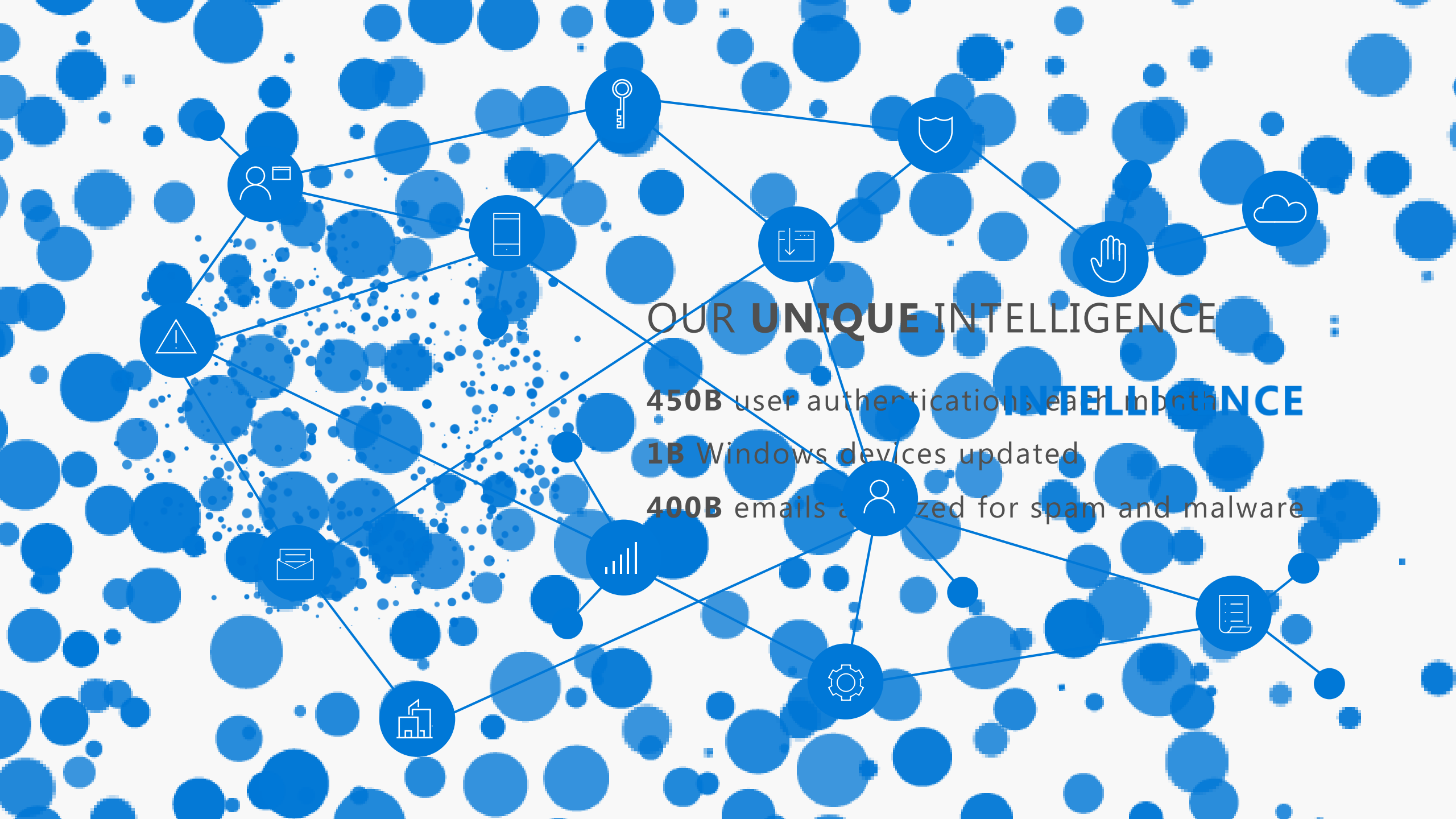
OUR **UNIQUE** APPROACH

Platform

Intelligence

Partners


Multi-factor authentication
Data encryption
User accounts
Device log-ins
Malware
Unauthorized data access
Attacks
INTELLIGENCE
User log-ins
Phishing
Denial of service
Spam
System updates
Enterprise security


OUR **UNIQUE** INTELLIGENCE
450B user authentications each month
1B Windows devices updated
400B emails analyzed for spam and malware
INTELLIGENCE

OUR **INTELLIGENCE**

OUR **UNIQUE** APPROACH

Platform

Intelligence

Partners

Key takeaways

Top things you can do

Staying Sharp on Security

Takeaways from the Microsoft Security Intelligence Report

Microsoft regularly aggregates the latest worldwide security data into the Security Intelligence Report (SIR), unpacking the most pressing issues in cybersecurity.

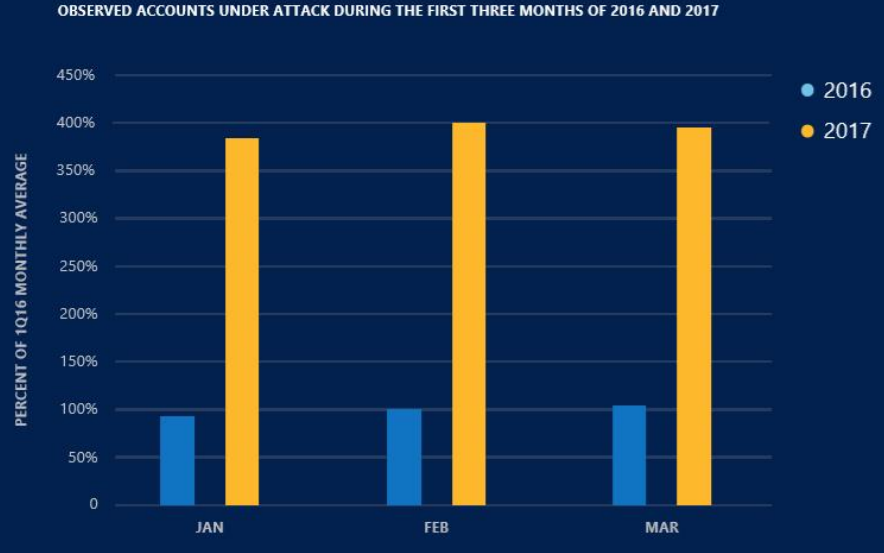
Cloud threat intelligence

The cloud has become *the* central data hub for any organization, which means it's also a growing target for attackers.

Compromised accounts

DEFINITION:
Attackers break into the cloud-based account simply by using the stolen sign-in credentials of a user

ANALYSIS:
A large majority of these compromises are the result of weak, guessable passwords and poor password management, followed by targeted phishing attacks and breaches of third-party services.



Cloud-based user account attacks have increased 300% from last year, showing that attackers have found a new favorite target.

Tip #1:

Protect your accounts and identities all times!

Every company or home has at least one user that will click on anything

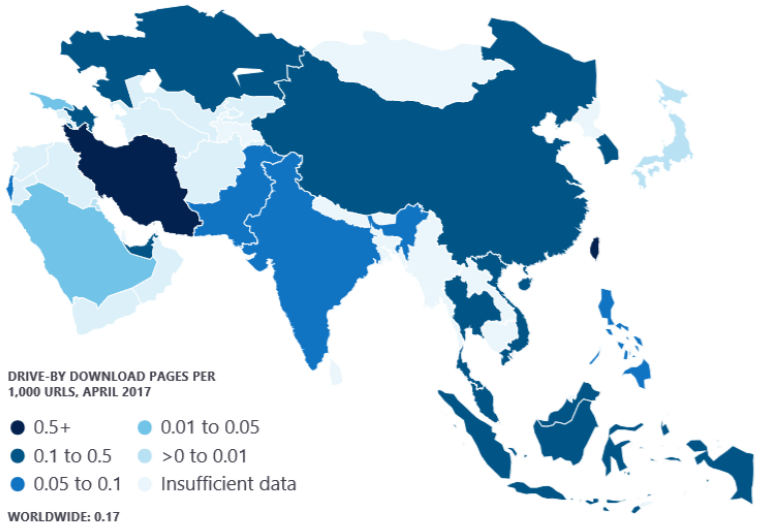
Tip #2: Watch for malicious websites or legitimate websites running malicious code

Drive-by download sites

DEFINITION:
A website that hosts malware in its code and can infect a vulnerable computer simply by a web visit

ANALYSIS:
Attackers sneak malicious code into legitimate but poorly secured websites. Machines with vulnerable browsers can become infected by malware simply by visiting the site. Bing search constantly monitors sites for malicious elements or behavior, and displays prominent warnings before redirecting to any suspicious site.

Taiwan and Iran have the **highest** concentration of **drive-by download** pages.



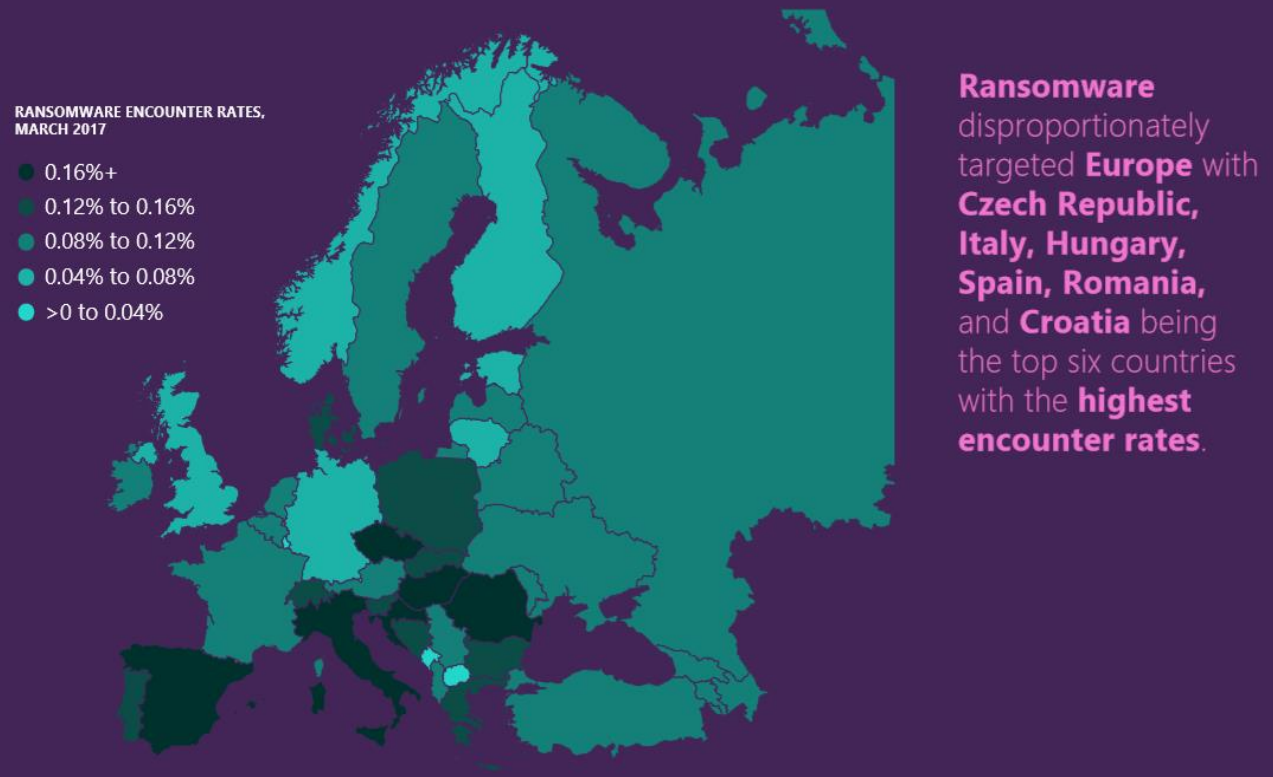
Ransomware

DEFINITION:

Malware that disables a computer or its files until an amount of money is paid to the attackers

ANALYSIS:

Ransomware attacks have been on the rise, disrupting major organizations and grabbing global headlines. Attacks like WannaCry and Petya disabled thousands of machines worldwide in the first half of 2017. Windows 10 includes mitigations that prevent common exploitation techniques by these and other ransomware threats.



Ransomware disproportionately targeted **Europe** with **Czech Republic, Italy, Hungary, Spain, Romania,** and **Croatia** being the top six countries with the **highest encounter rates**.

Tip #3: Backup, backup (and ability to restore…)

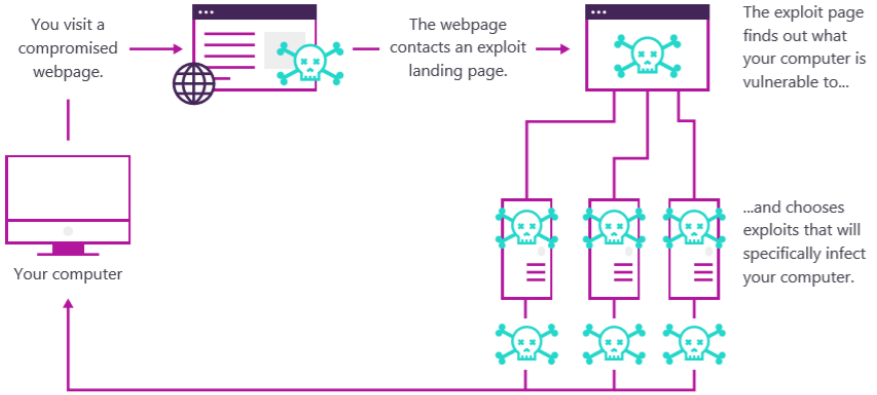
Tip #4: Keep your systems updated

Exploit kits

DEFINITION:
A bundle of malicious software that discovers and abuses a computer's vulnerabilities

ANALYSIS:
Once installed on a compromised web server, exploit kits can easily reach any computer lacking proper security updates that visits the site.

Many of the more **dangerous exploits are used in targeted attacks** before appearing in the wild in larger volumes.



Takeaways and checklist

The threats and risks of cyberattacks are constantly changing and growing. However, there are some practical steps you can take to minimize your exposure:

Reduce risk of credential compromise by educating users on why they should avoid simple passwords, enforcing multi-factor authentication and applying alternative authentication methods (e.g., gesture or PIN).

Enforce security policies that control access to sensitive data and limit corporate network access to appropriate users, locations, devices, and operating systems (OS).

Do not work in public Wi-Fi hotspots where attackers could eavesdrop on your communications, capture logins and passwords, and access your personal data.

Regularly update your OS and other software to ensure the latest patches are installed.

Some practical takeaways from today's session

See also: https://qnamaker.ai/

Aylton Souza
aysouza@microsoft.com

aysouza@microsoft.com

Stay on top of all the latest information in cybersecurity, gleaned from Microsoft's worldwide intelligence.

Read more and download the full Security Intelligence Report at microsoft.com/sir

Microsoft