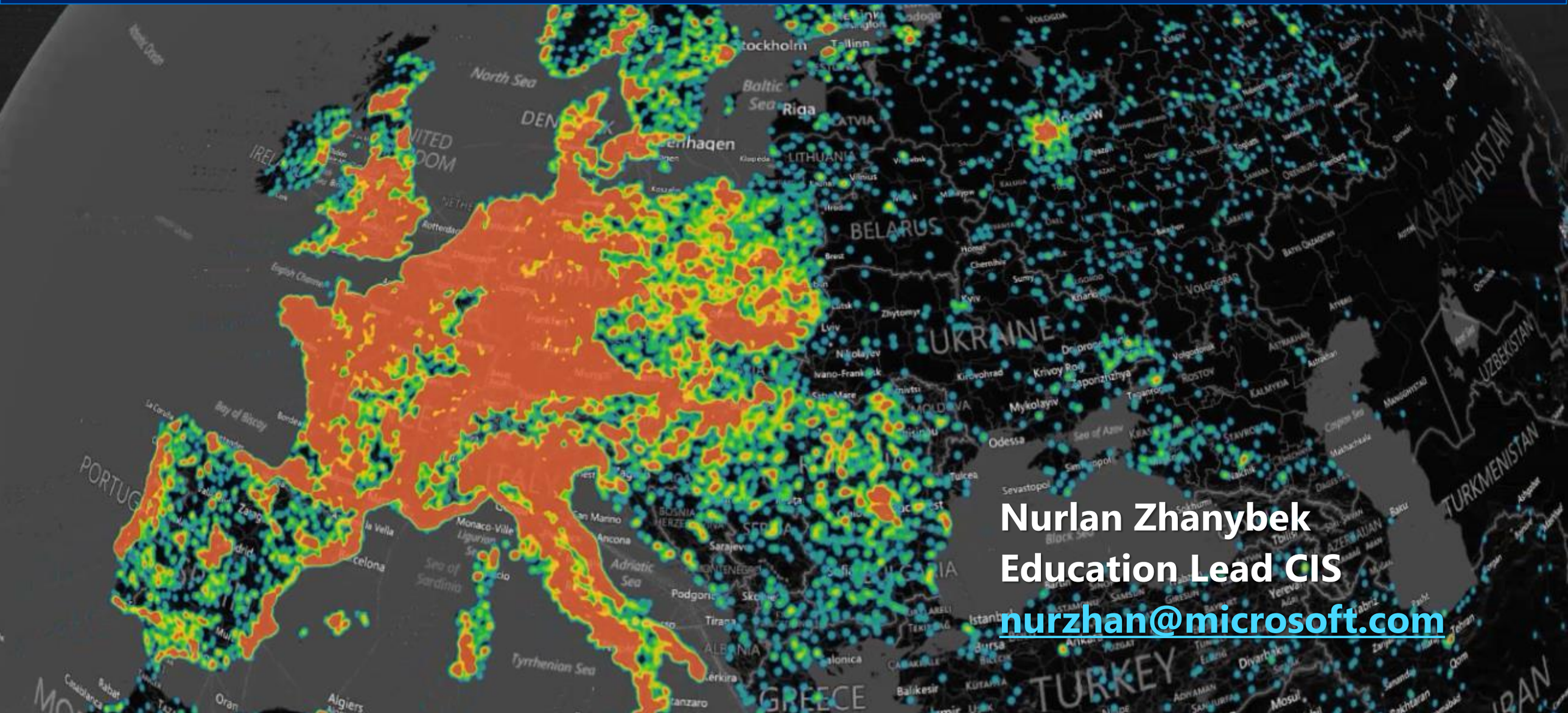
Cybersecurity landscape in 2019



Nurlan Zhanybek
Education Lead CIS
nurzhan@microsoft.com

Cyberthreats: NUMBERS

EVERY SECOND

12 PEOPLE

FALL PREY TO CYBER-CRIMINALS,

THAT IS ALMOST 400 MILLION

PEOPLE PER YEAR

Cyberthreats: NUMBERS

~85% of citizen

were exposed to

ACTIVITIES CONDUCTED BY

CYBER-CRIMINALS

Cyberthreats: NUMBERS

98.5%

OF SMBs
WERE EXPOSED TO
EXTERNAL THREATS
AT LEAST ONCE EACH YEAR

Cyberthreats: CAUSES

92%

POSSIBILITY to lose data/money

JUST BY TYPING

"DOWNLOAD WINDOWS FOR FREE"

IN THE SEARCH BOX AND CLICKING THE LINK...

50% OF PROGRAMS

INSTALLED ON PCs IN 2013 WERE

COUNTERFEIT

Cyberthreats: CAUSES

WINDOWS ZVERCD

THE MOST POPULAR PIRATED WINDOWS VERSION IN CIS CONTAINS

63

VULNERABILITIES

INCLUDING KEY-LOGGERS, VIRUSES AND TROJANS

Cyberthreats: CAUSES

53% OF USERS

NEGLECT TO USE

AUTOMATIC UPDATES OF

SECURITY

FUNCTIONS

Cyberthreats: CAUSES

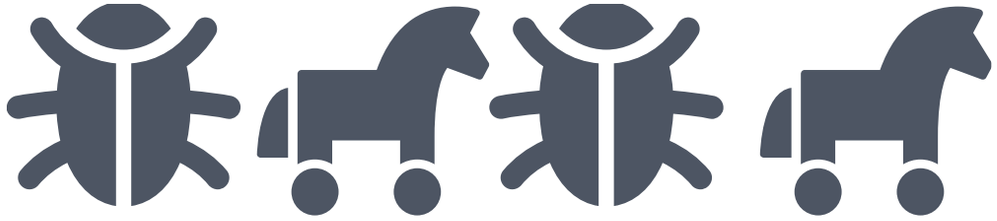
28% of companies

cyberattacks on corporate PCs, websites and IT networks

Once a month or more

in 65% of cases, corporate employees' PC's were revealed to contain

pirated software



Cyberthreats: CAUSES

27% of employees
INSTALL SOFTWARE AND APPLICATIONS
BY THEMSELVES
ON WORKPLACE PCs,
WHICH ACCOUNTS FOR

ALMOST 20%

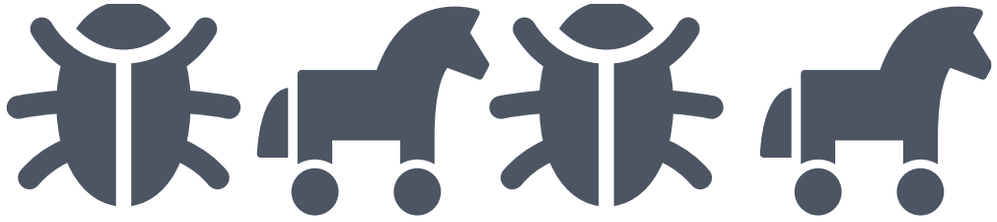
OF ALL PIRATED SOFTWARE

IN USE BY COMPANIES

SURPRISINGLY, ONLY

14% OF CIS COMPANIES

CONDUCT AN INVENTORY ANALYSIS OF THESE SOFTWARE PROGRAMS
REGULARLY



NEW REALITY

317 million

NEW MALICIOUS PROGRAMS
WERE CREATED
DURING THE LAST YEAR

THAT AMOUNTS TO
APPROXIMATELY 1 MILLION
NEW **cyberthreats**
EVERYDAY

CONSEQUENCES

THE IT INDUSTRY LOSES APPROXIMATELY **$3 billion** a year IN CIS

WHICH IS MORE THAN THE **EARNINGS** RECEIVED BY DEVELOPERS FROM THE EXPORT OF IT PRODUCTS

Pressure on financial markets and indices

- ENCRYPTORS AS A CAMOUFLAGE
- CIS AS TEST GROUNDS (RU LEADS)
- DNS, BODYLESS, SCRIPTS
- TERMINAL PROCESSING
- SOCIAL ENGINEERING (PRIVATE MAIL ATTACKS, CUSTOMIZATION)
- FSI LEADS IN PHISHING
- CRYPTO, ICO, PERSISTENCY

START WITH BASICS: PERIMETER, SW INVENTORY, TRAINING, PLAN

BASIC RULES

⇒ Use only genuine software. Conduct regular inventory of installed software;

⇒ Inform your employees of basic security rules;

⇒ Install specialized security software and hardware solutions;

⇒ Do not use out-of-date and unsupported software and always install the latest security updates;

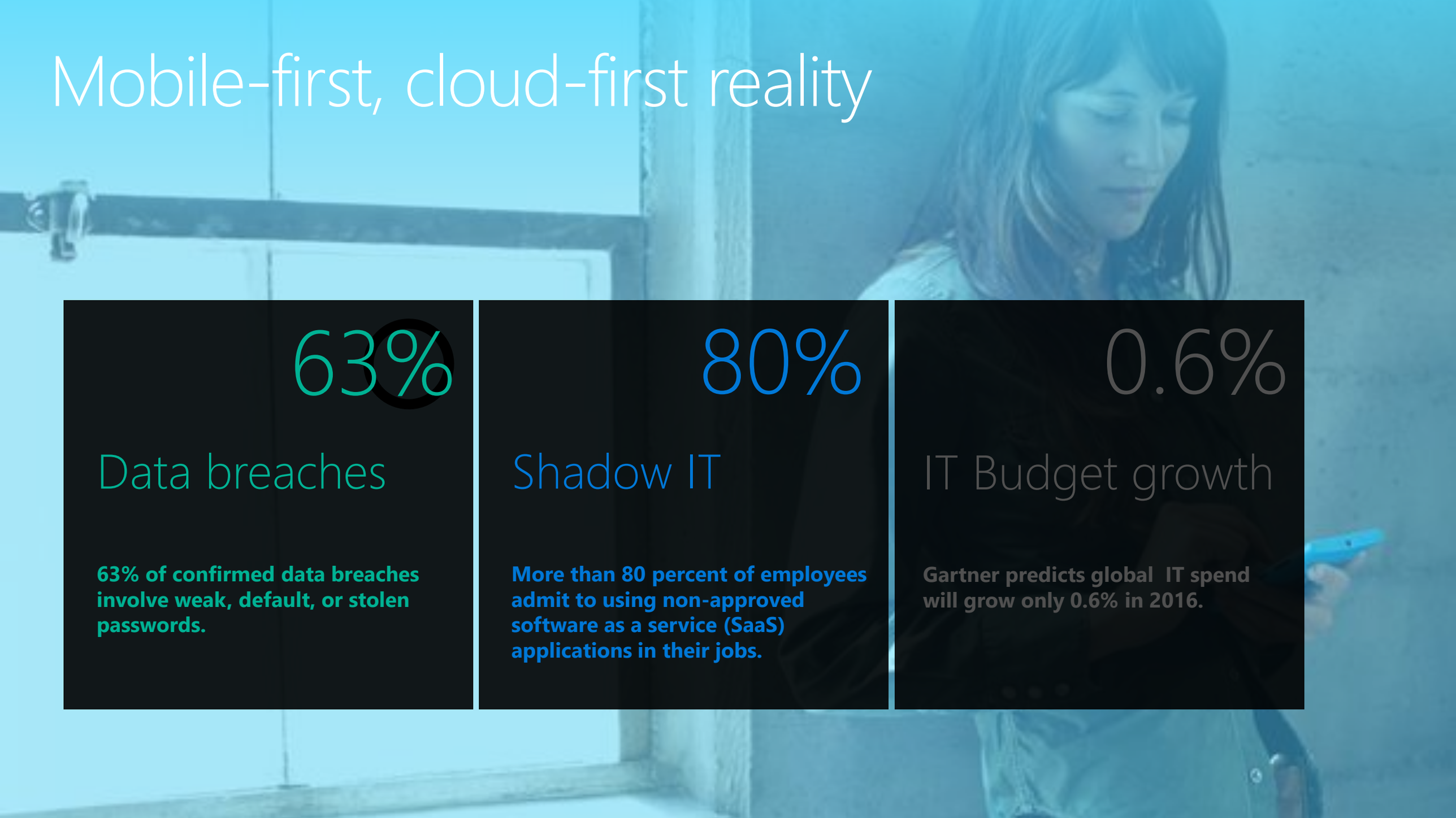
⇒Implement the SAM process.

Committed to security

“As the world continues to change and business requirements evolve, some things are consistent: a customer’s demand for security and privacy. We firmly believe that every customer deserves a trustworthy cloud experience and we are committed to delivering that experience in the cloud.”

– Satya Nadella, CEO

Mobile-first, cloud-first reality



63%

Data breaches

63% of confirmed data breaches involve weak, default, or stolen passwords.

80%

Shadow IT

More than 80 percent of employees admit to using non-approved software as a service (SaaS) applications in their jobs.

0.6%

IT Budget growth

Gartner predicts global IT spend will grow only 0.6% in 2016.

"THERE ARE TWO KINDS OF BIG COMPANIES, THOSE WHO'VE BEEN HACKED, AND THOSE WHO DON'T KNOW THEY'VE BEEN HACKED."

JAMES COMEY, EX-DIRECTOR FBI

146

Median number of days attackers are present on a victim's network before detection

24-48HRS

It takes to attacker to get complete control of the network

$4BILLION

Cyber-attacks cost organizations in 2015

$3.8MILLION

Average cost of a data breach (7.6% YoY increase)

Attacks are more sophisticated

Attacker

Think different

Well funded

Have time

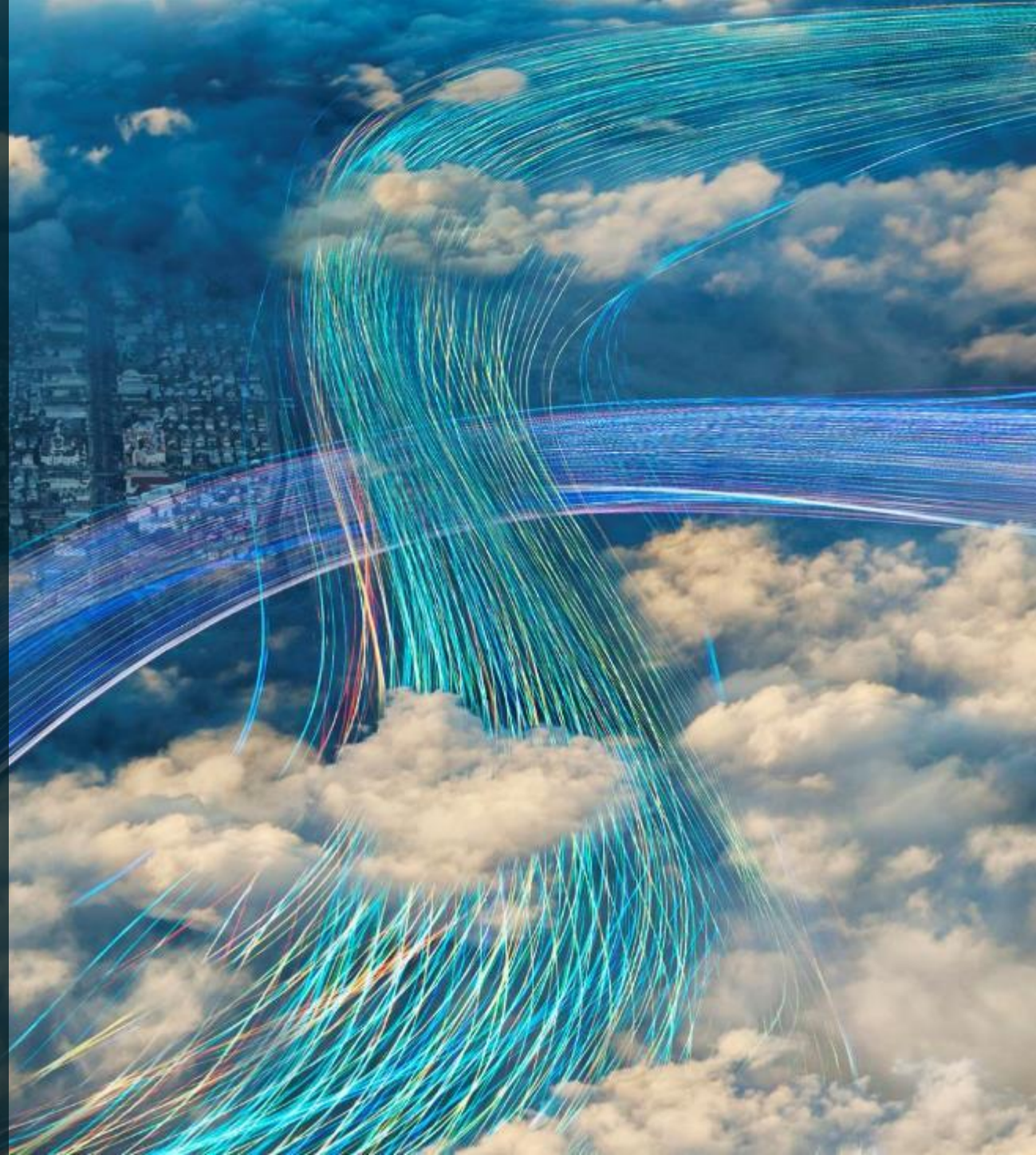
Security team

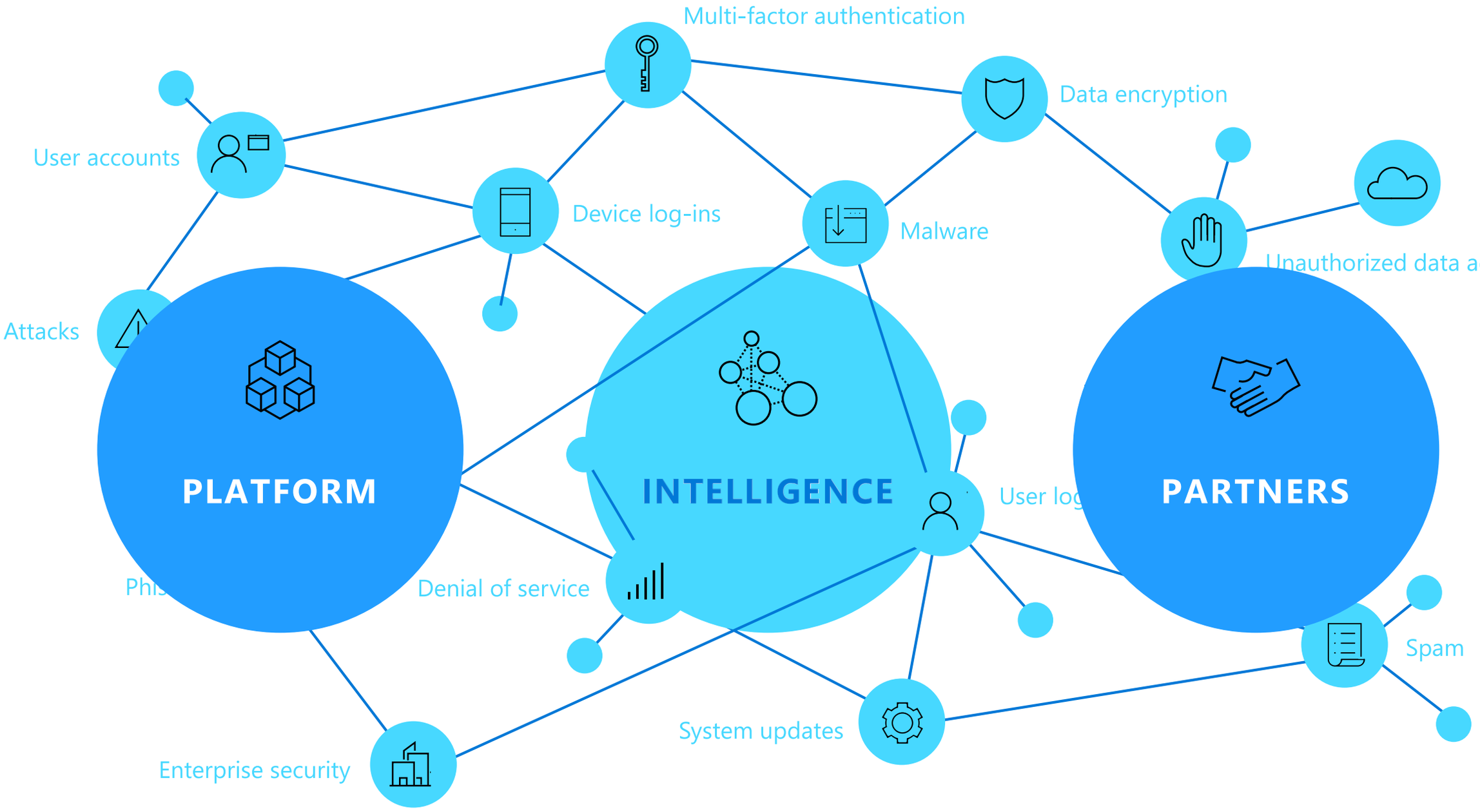
Short of expertise

Lack of resource

Limited response time

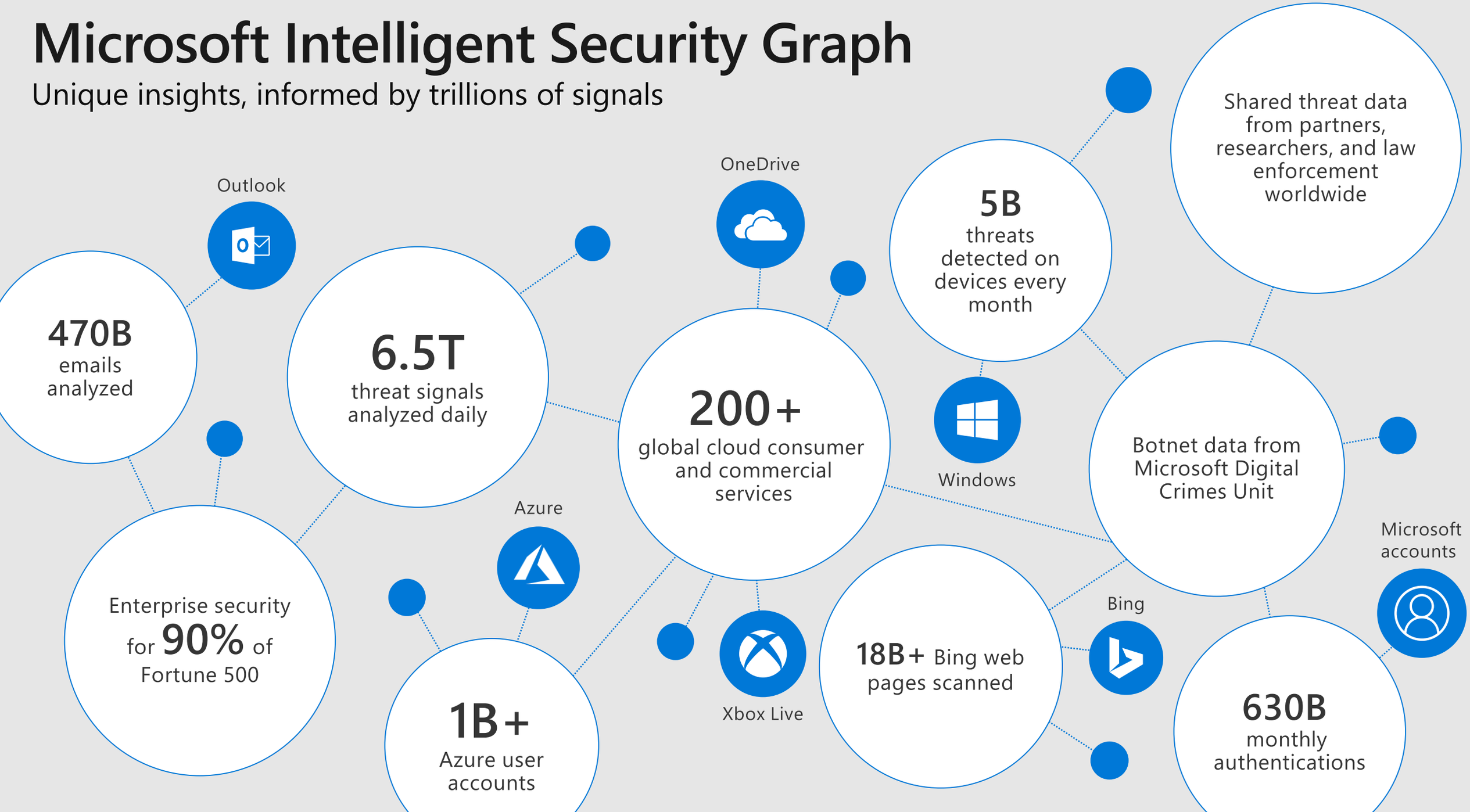
Microsoft spends $1B+ on security R&D every year




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

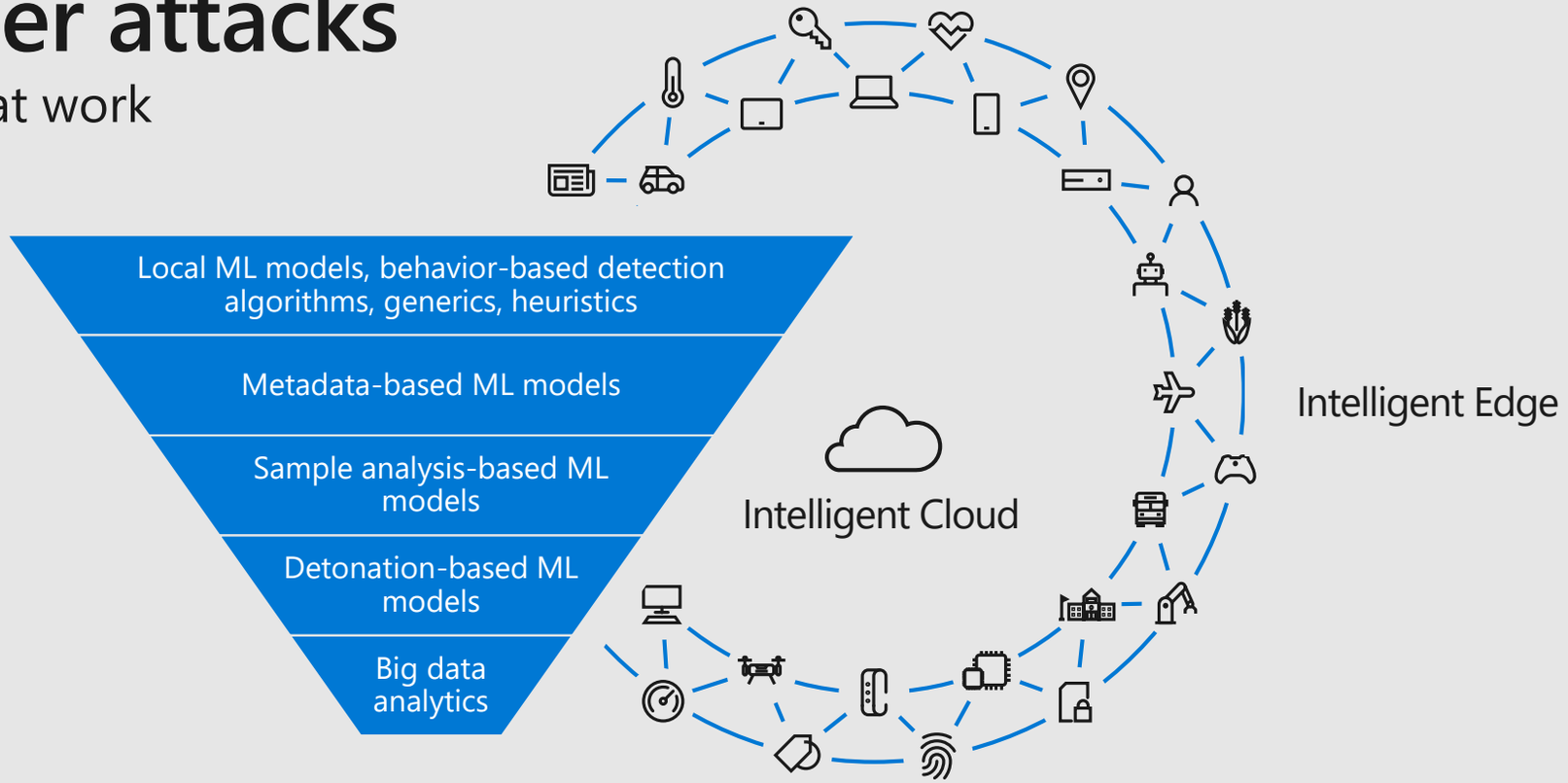
Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



Stopping cyber attacks

Real-world intelligence at work



October 2017 – Cloud-based detonation ML models identified Bad Rabbit, protecting users 14 minutes after the first encounter.

February 3 – Client machine learning algorithms automatically stopped the malware attack Emotet in real time.

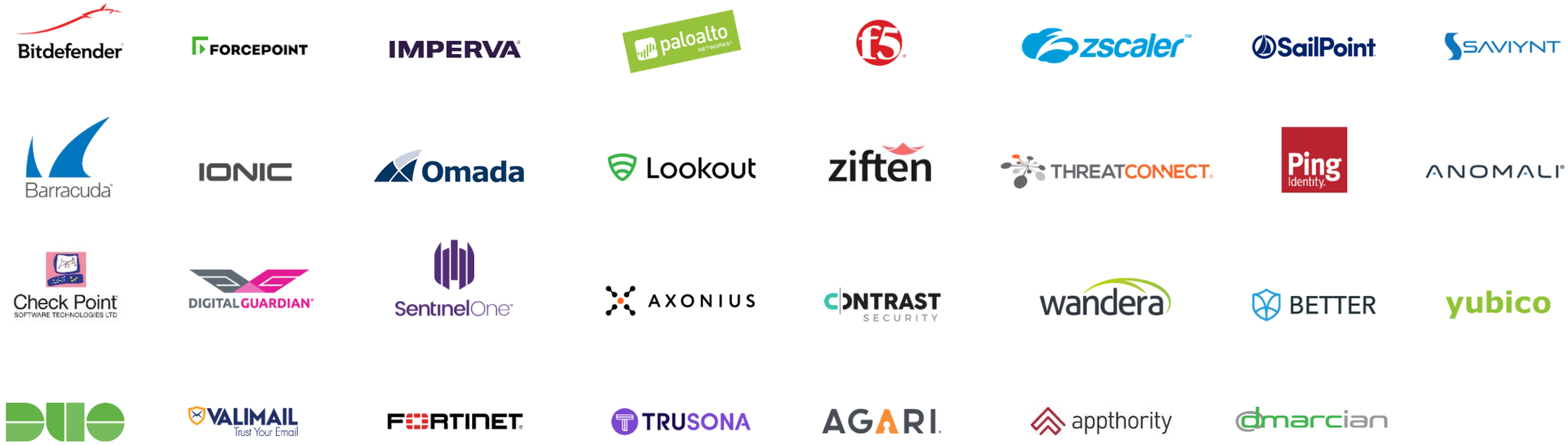
March 6 – Behavior-based detection algorithms blocked more than 400,000 instances of the Dofoil trojan.

August 2018 – Cloud machine learning algorithms blocked a highly targeted campaign to deliver Ursnif malware to under 200 targets

2017 — 2018

Microsoft Intelligent Security Association

Collaboration strengthens protection



Teaming up with our security partners to build an ecosystem of intelligent security solutions that better defend against a world of increased threats

Thank you!

Nurlan Zhanybek
Education Lead, CIS
Nurlan.Zhanybek@microsoft.com
+77019727318