Microsoft Cybersecurity Vision

Luís Marques, Account Technology Strategist

Portugal, Public Sector Segment

lmarques@microsoft.com

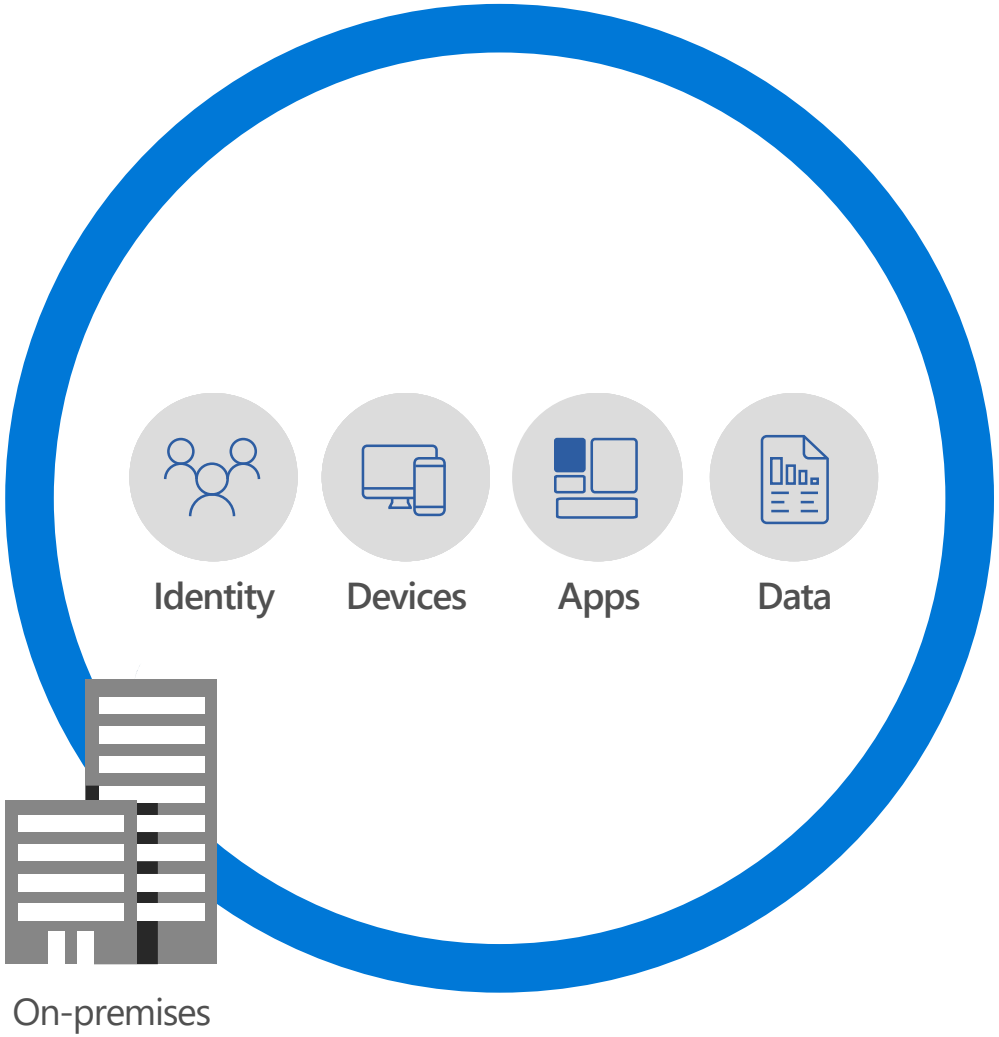
Microsoft

Let's face it, cyberspace is the new battlefield.
The world of potential war has migrated from land to sea to air and now cyberspace.

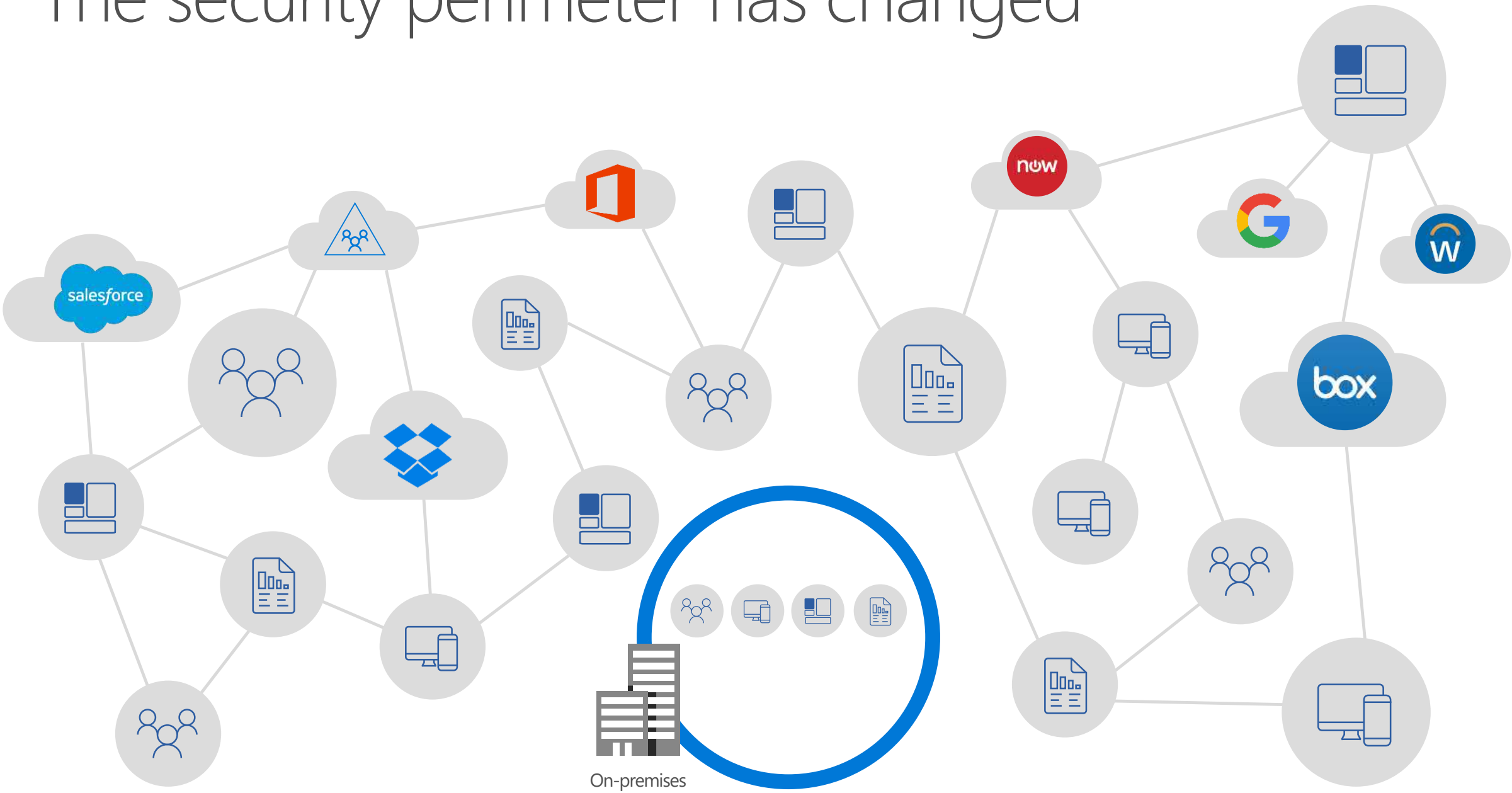


BRAD SMITH
PRESIDENT AND CHIEF LEGAL OFFICER MICROSOFT

The security perimeter has changed



The security perimeter has changed



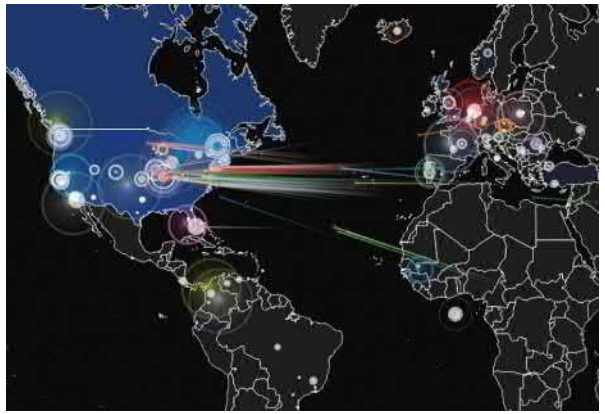
CYBER ATTACKS EVOLUTION

SAME TACTIC. NEW SOPHISTICATION.

COMMITTED CREDENTIALS



DISTRIBUTED DENIAL OF SERVICE (DDoS)



MALWARE / RANSOMWARE





Hacking as a hobby



Hacking with financial gains



Attacks on States/Governments



Potential terrorist attacks

WHAT'S THE **THREAT LEVEL?**



$3.6M

Global average of the cost of a data breach

22.7 %

Percentage of increased cyber systems costs per year



130

Average number of security breaches, per company, each year

99 DAYS

Time that delays compromised organizations to detect threats



50 DAYS

Average time to solve an *malicious insiders* attack

23 DAYS

Average resolution time of a ransomware attack

SOURCE: ACCENTURE – THE COST OF CYBERCRIME; FireEye/Mandiant report; PONEMOM COST OF A DATA BREACH STUDY (2017)

WHAT AS **CHANGED** THE NEW WAY OF WORK?

77 % of millennials admit that a way of working more flexible makes them more productive

58 % of organization's employees have already shared sensitive information with the wrong person

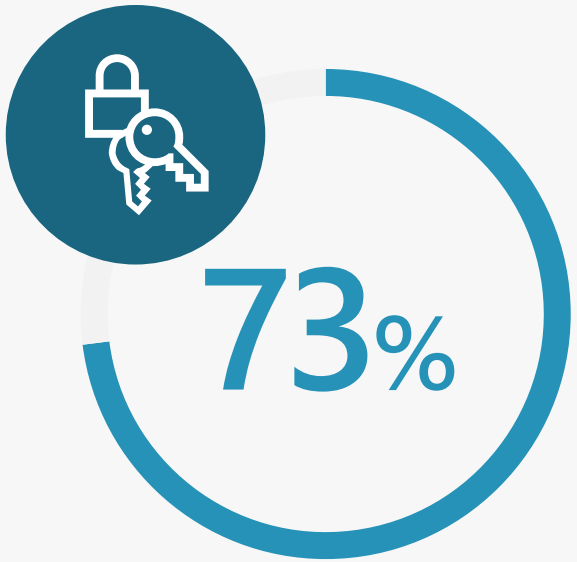


SOURCE: THALES E-SECURITY; BENTLEY UNIVERSITY

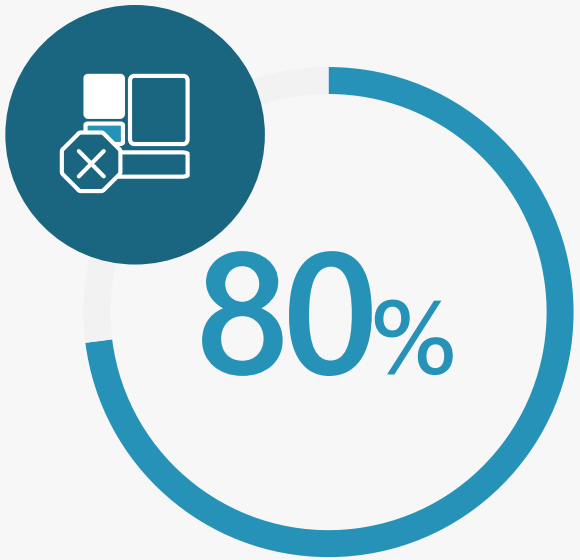
WHY IS **IDENTITY** IMPORTANT?



Security failures are caused by theft of credentials



Passwords are duplicated

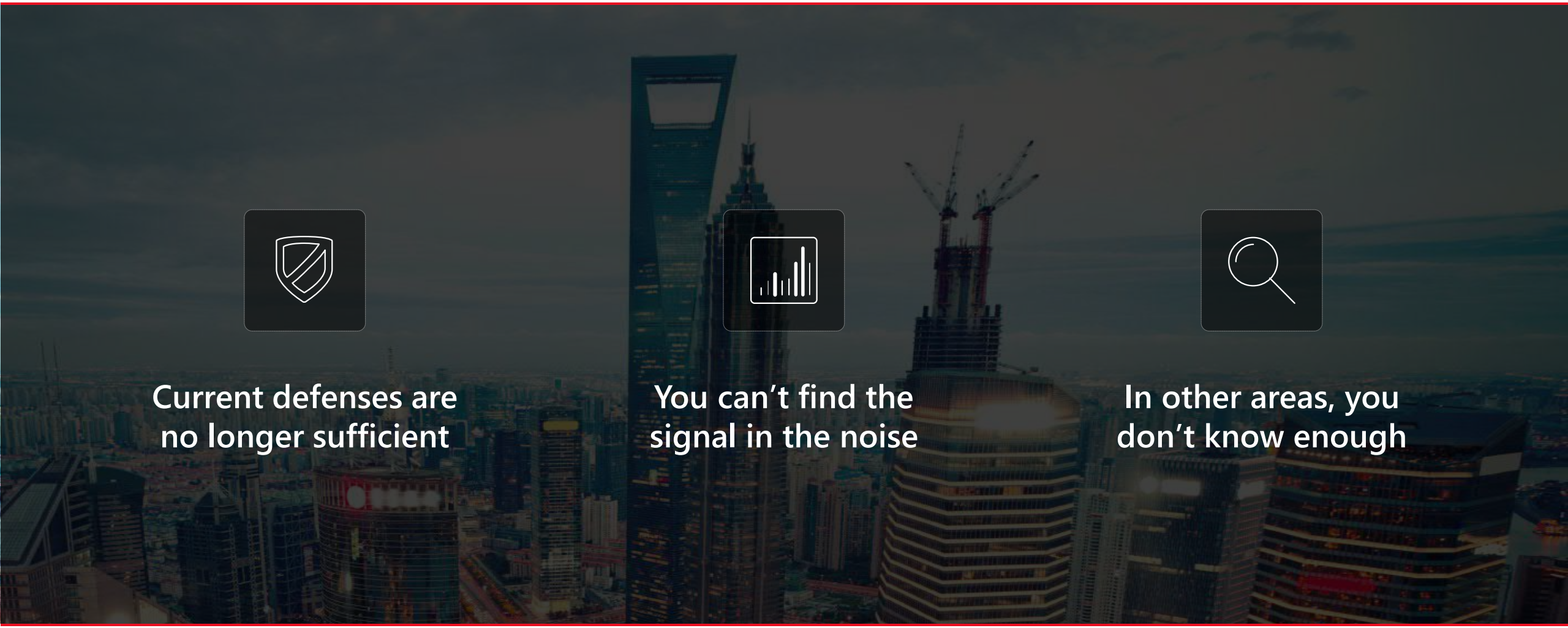


Employees use apps not approved by the organization

SOURCE – FORBES: HOW TECHNOLOGY HAS CHANGED WORKPLACE COMMUNICATION

The security landscape has changed.

We need to do more.



Current defenses are no longer sufficient

You can't find the signal in the noise

In other areas, you don't know enough


CONCERNED?
THERE'S A WAY!.

MICROSOFT'S NEW **SECURITY POSTURE**

Protect

Today's cloud-first, mobile-first world demands the highest level of identity & data security

Detect

Comprehensive monitoring tools to help you spot abnormalities and respond to attacks faster

Respond

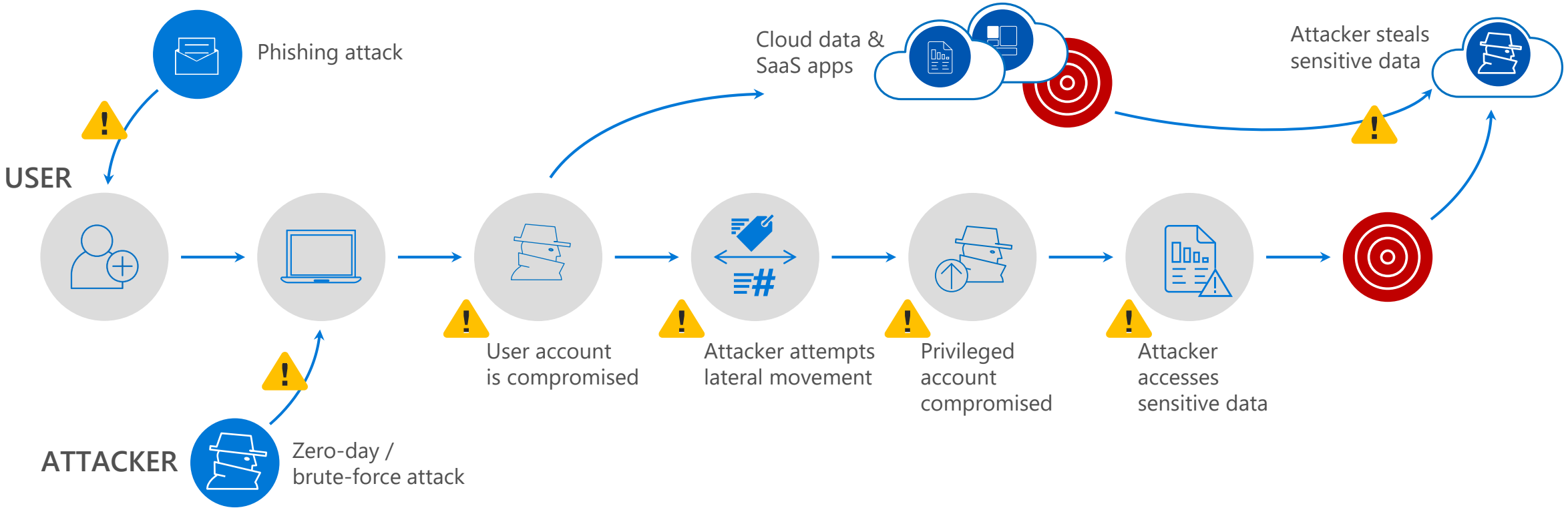
Leading response and recovery technologies plus deep consulting expertise

OBJECTIVE

Make it more difficult

Increase Hackers Costs and Efforts to successfully attack organizations

I want to shorten the attack timeline



Anonymous user behavior

Unfamiliar sign-in location

Anonymous user behavior

Lateral movement attacks

Escalation of privileges

Account impersonation

Data exfiltration

How to Address Security

Identity and Access Management



Investments in securing the perimeter are no longer enough. Identity is the new security perimeter.

Threat Protection



Increasing use of machine learning at scale to provide threat intelligence to inform decisions and detections.

Information Protection



In an era of “Assume Compromise”, end-to-end security is increasingly important to deter and defeat attackers.

Security Management



Adoption of point “best of breed” products creates extremely complex management challenges. Security automation and orchestration are key to future success.

YOU **(WE)** HAVE A PROBLEM

INTELLIGENCE

should be **part of the security framework**, not just a referenced artefact

DETECTION

Detectors should be **automated, correlated and interlinked** in their findings



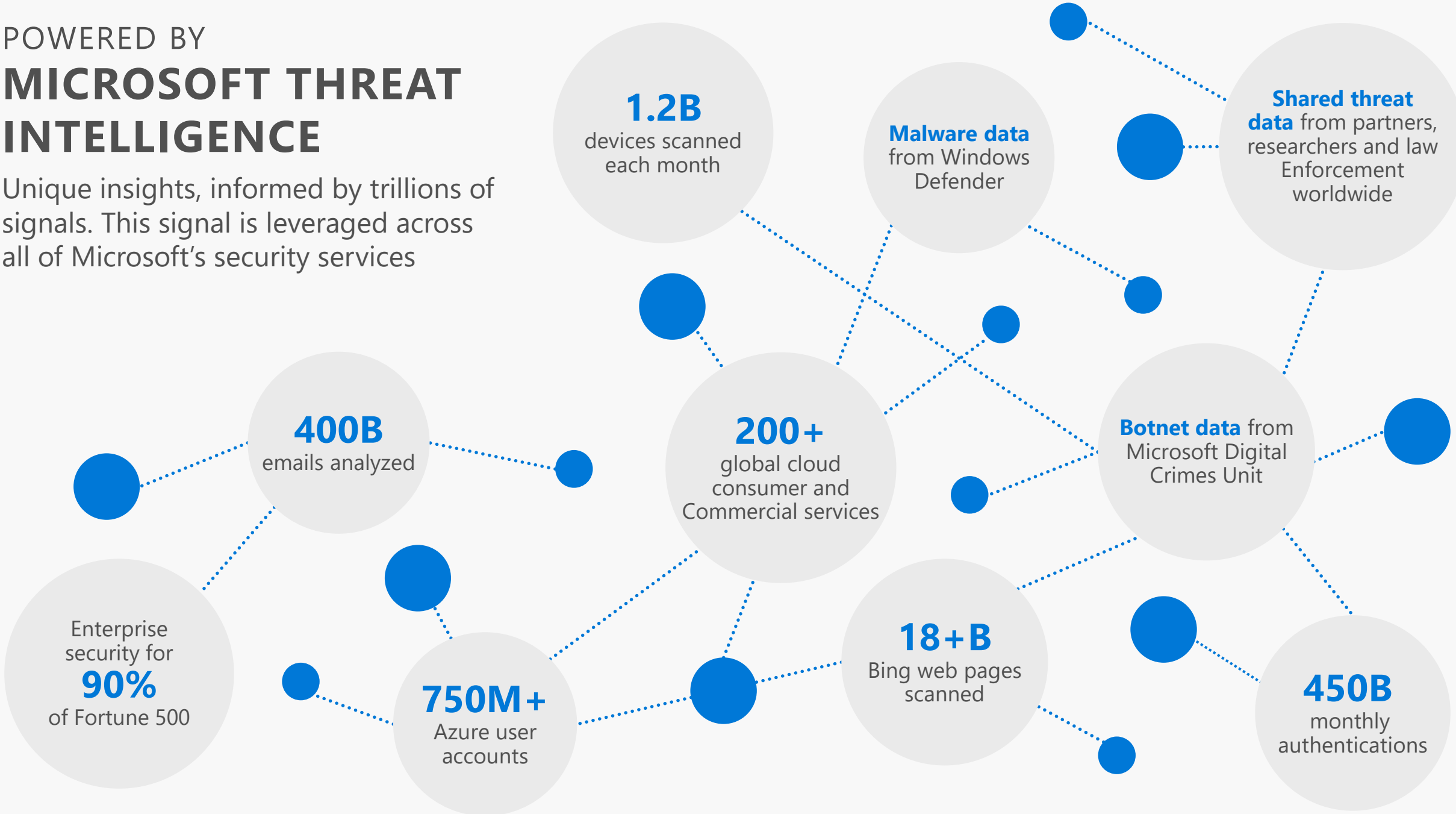
SIEMS

Must **reduce busy work** of incident roll-up, response, and management

POWERED BY

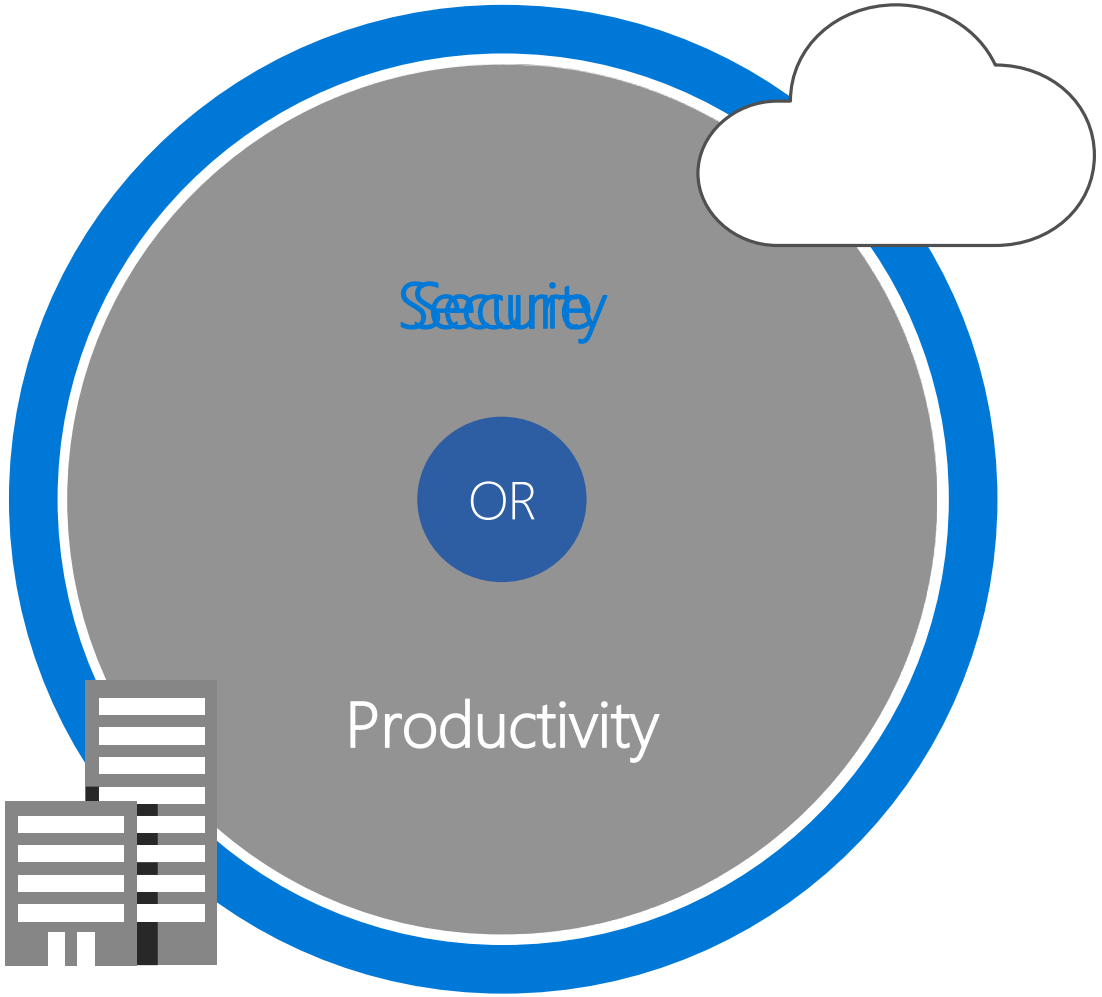
MICROSOFT THREAT INTELLIGENCE

Unique insights, informed by trillions of signals. This signal is leveraged across all of Microsoft's security services




Microsoft Accounts
Xbox Live
Azure Active Directory
Skype
Azure
Bing
Office365
Enterprise Mobility + Security
OneDrive
Microsoft Digital Crimes Unit
Microsoft Cyber Defense Operations Center
Microsoft Intelligent Security Graph

How do we enable productivity without compromising security?



It's a delicate balance
between productivity & security

The security you need integrated with the productivity tools you want

Microsoft Enterprise Mobility + Security

Holistic and innovative solutions for protection across users, devices, apps and data

Identity and access management

Mobile device & app management

Information protection

Threat detection



Protect at the front door

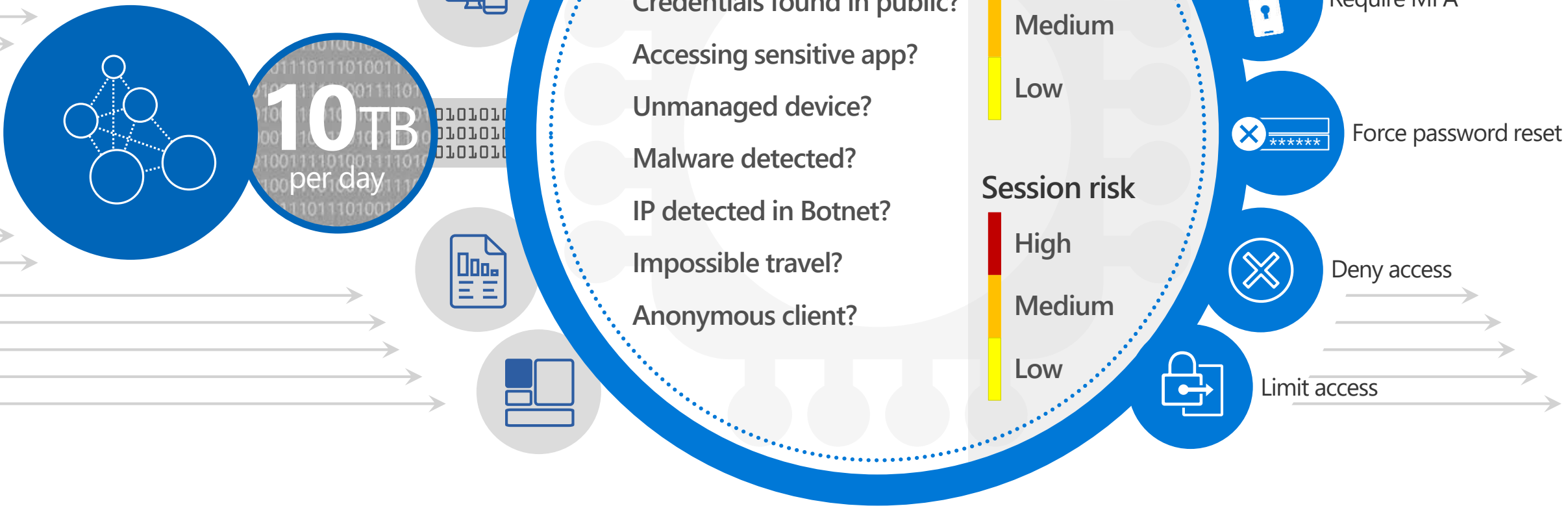


Protect your data anywhere



Detect & remediate attacks

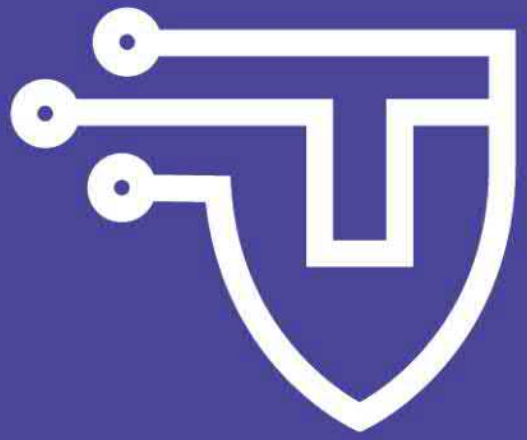
CONDITIONAL ACCESS



It’s like going to the gym every morning. Every hour of the day you need to be prepared. And so that means **you have to exercise this operational security posture on a continuous basis.**

SATYA NADELLA
MICROSOFT CEO





CYBERSECURITY

TECH ACCORD

PROTECTING USERS & CUSTOMERS EVERYWHERE

www.cybertechaccord.com

SIGNATORIES



ABB
arm
avast
Bitdefender
BT
Carbon Black.
ca technologies
cisco
CLOUDFLARE
DATASTAX
DELL
DocuSign
facebook
fastly
FireEye
F-Secure
GitHub
guardtime
hp
Hewlett Packard Enterprise
intuit
JUNIPER NETWORKS
LinkedIn
Microsoft
nielsen
NOKIA
ORACLE
RSA
SAP
stripe
Symantec
Telefónica
tenable
TREND MICRO
vmware

CYBERSECURITY TECH ACCORD PRINCIPLES

1. WE WILL PROTECT ALL OF OUR USERS AND CUSTOMERS EVERYWHERE.

2. WE WILL OPPOSE EFFORTS TO ATTACK INNOCENT CITIZENS AND ENTERPRISES FROM ANYWHERE.

3. WE WILL HELP EMPOWER USERS, CUSTOMERS AND DEVELOPERS TO STRENGTHEN CYBERSECURITY PROTECTION.

4. WE WILL PARTNER WITH EACH OTHER AND WITH LIKEMINDED GROUPS TO ENHANCE CYBERSECURITY.

– *Time* –

"Today, more than 3 billion people use the Internet
That's 7X as many people as in 2000."

– *Statista* –

"2.46 billion people utilize social networks."

– *Cisco* –

"By 2021, 73% of Internet traffic
will be on mobile devices."


Microsoft