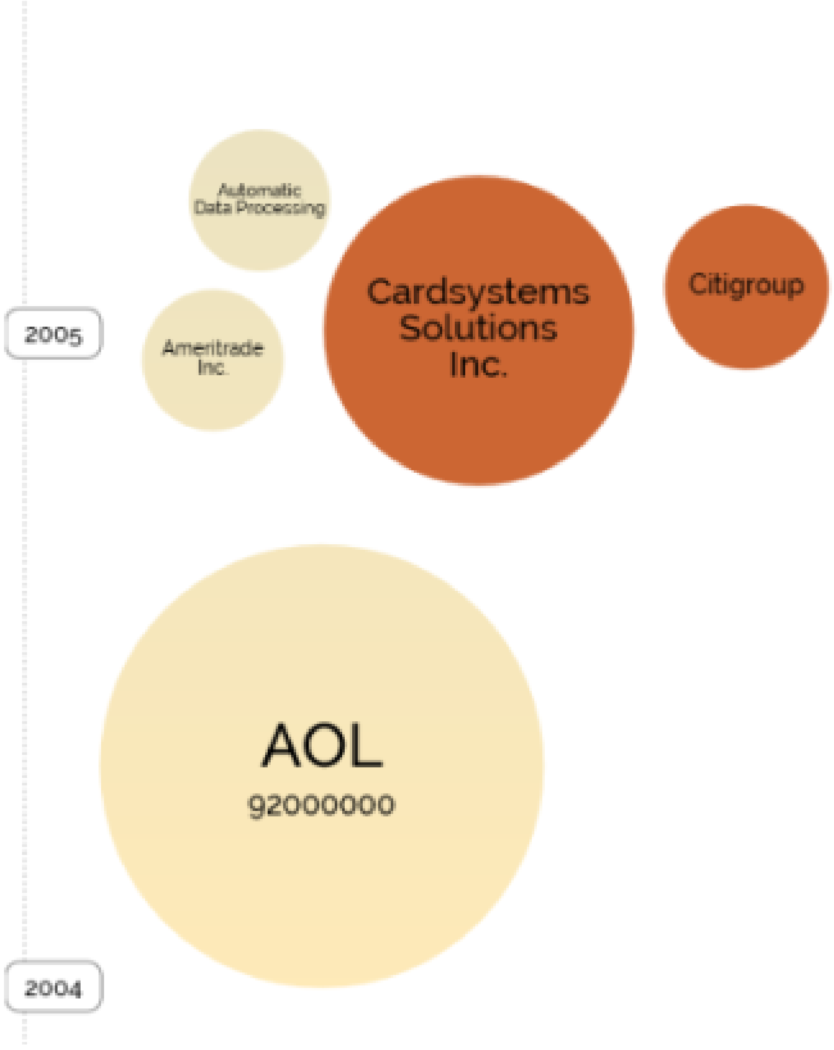
Microsoft

BRITISH COLUMBIA

Defensible Security in a Digital World

John Hewie
National Security Officer
Microsoft Canada

Brief history of breaches



TURBULENT TIMES

Industrialized Attack Industry rapidly maturing

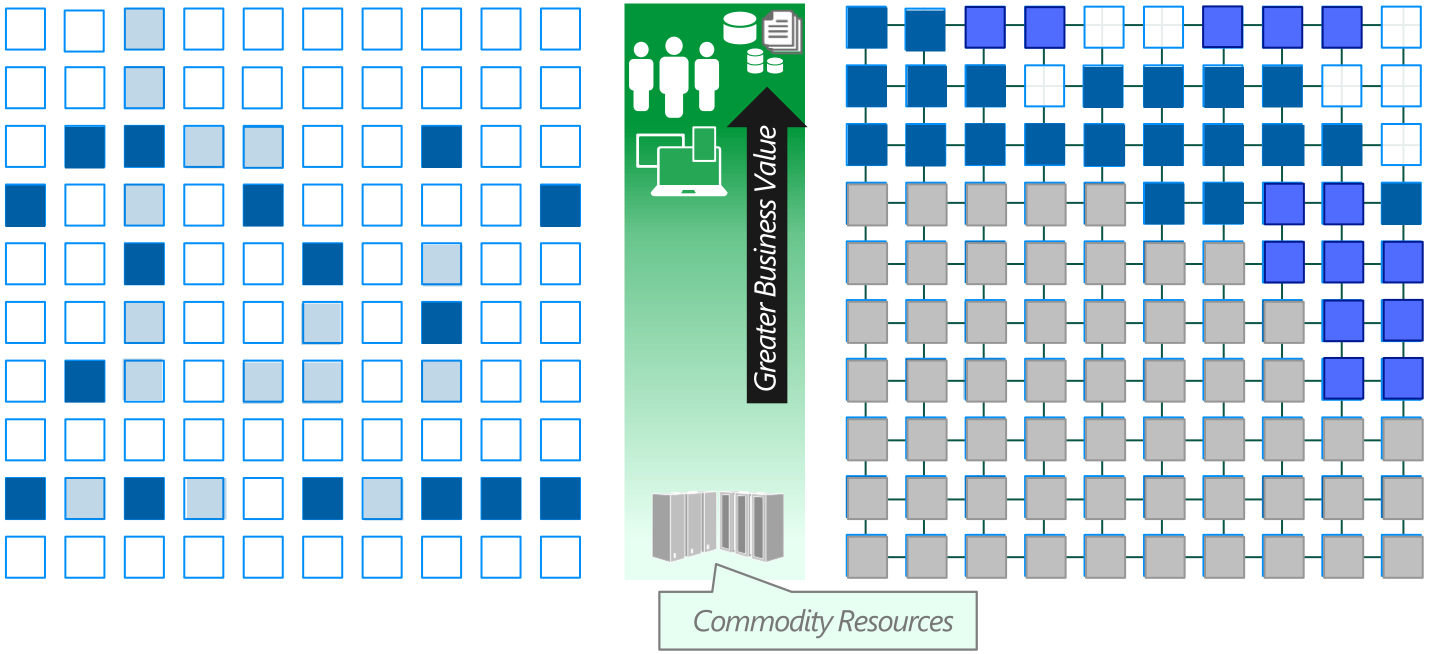
Nation States honing cyber offence capabilities

Government traditional defensive roles have been disintermediated

Risk Management approach with Cloud Computing

TRADITIONAL APPROACH

CLOUD-ENABLED SECURITY



Cloud Technology enables security to:

- ▩ Shift commodity responsibilities to provider and re-allocate your resources
- ■ Leverage cloud-based security capabilities for more effectiveness
- ⌖ Use Cloud intelligence improve detection/response/time

Security is a challenging and under-resourced function

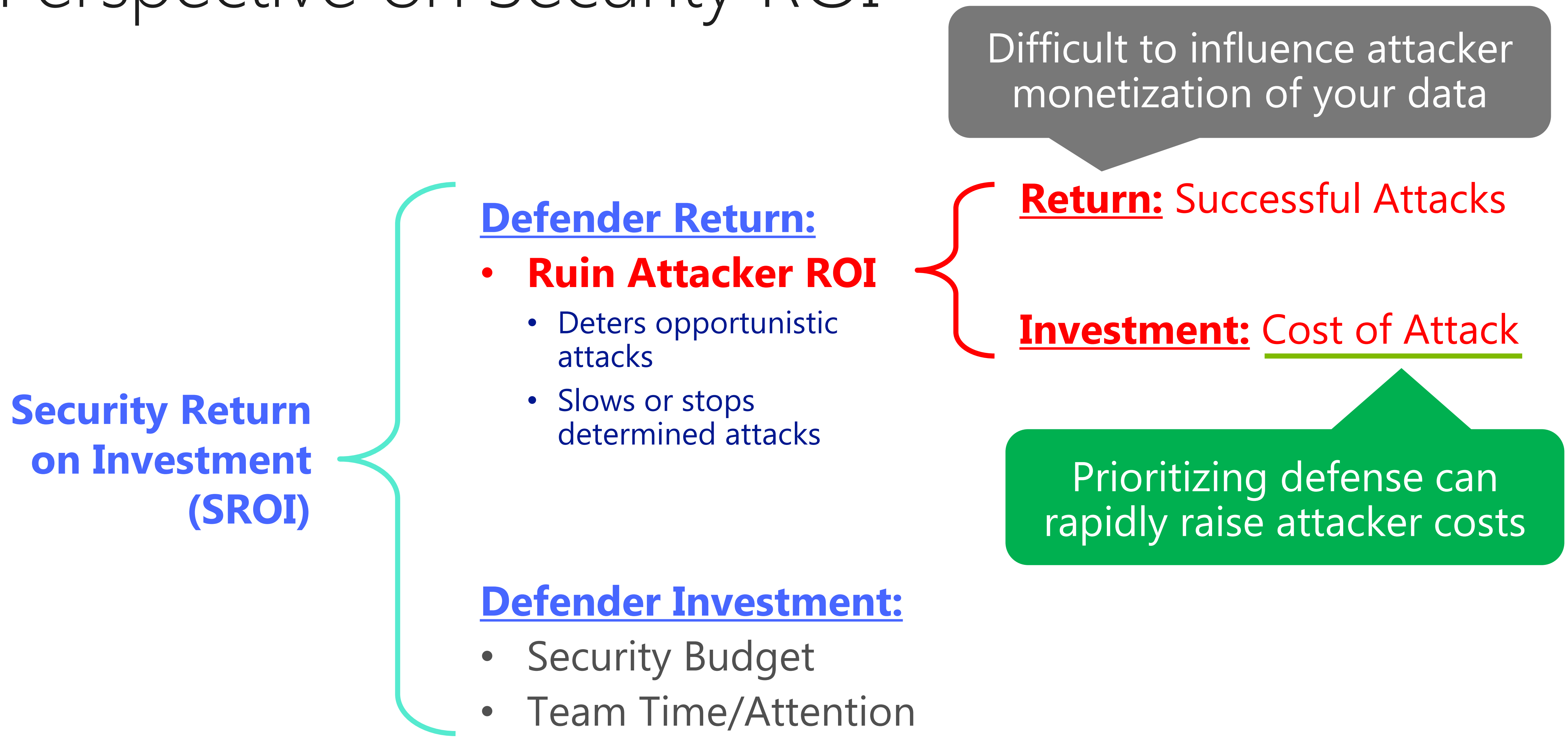
■ Satisfied responsibility

□ Unmet responsibility

▨ Partially met responsibility

▩ Cloud Provider responsibility (Trust but verify)

Perspective on Security ROI



Security Return on Investment (SROI)

Defender Return:

- **Ruin Attacker ROI**
  - Deters opportunistic attacks
  - Slows or stops determined attacks

Defender Investment:

- Security Budget
- Team Time/Attention

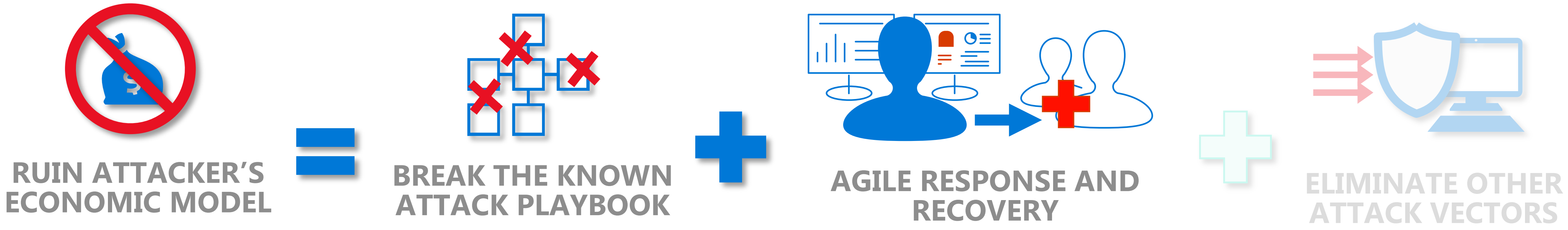
Difficult to influence attacker monetization of your data

Return: Successful Attacks

Investment: Cost of Attack

Prioritizing defense can rapidly raise attacker costs

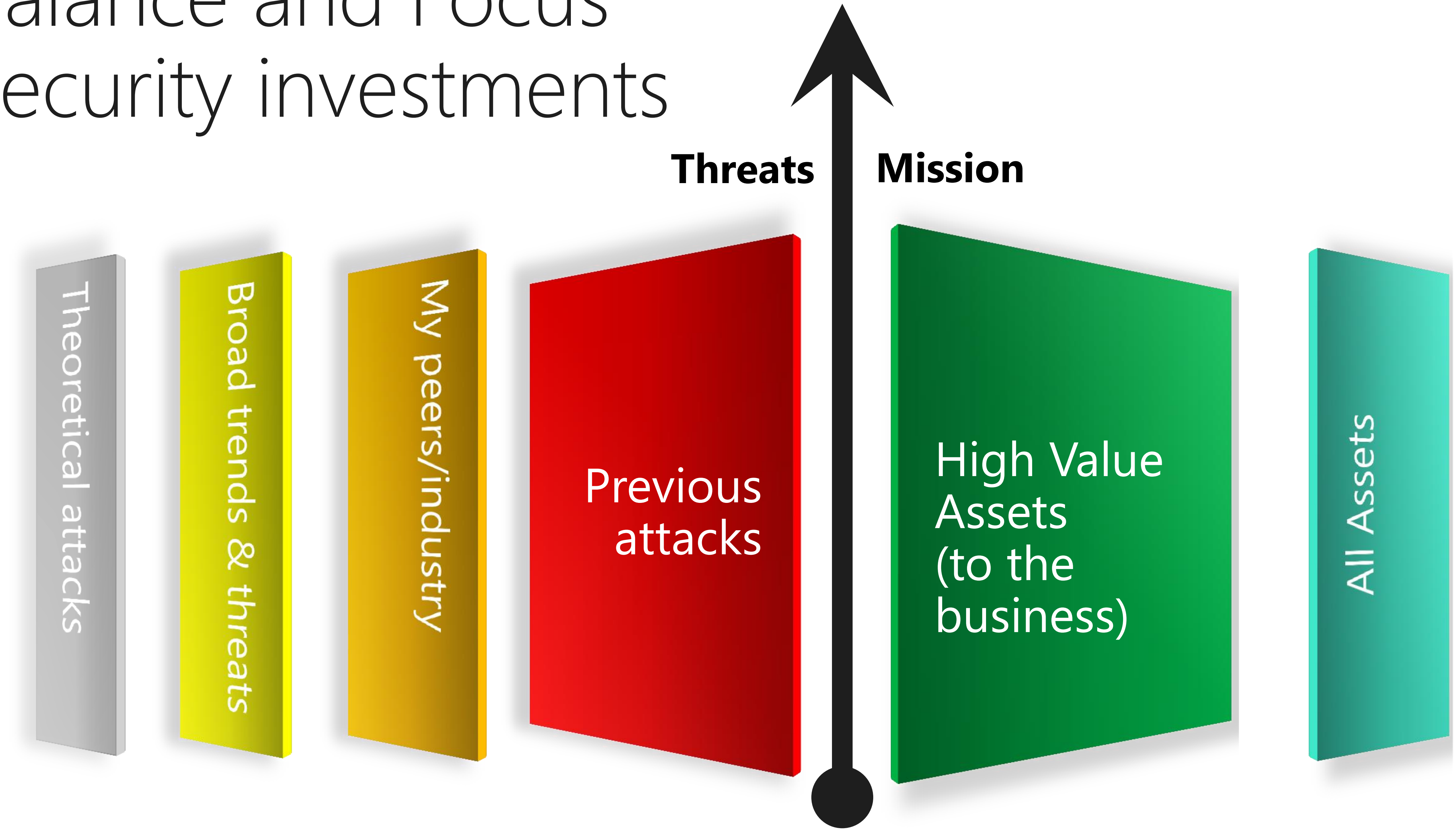
Rapidly Raising Attacker Cost



RUIN ATTACKER’S ECONOMIC MODEL = BREAK THE KNOWN ATTACK PLAYBOOK + AGILE RESPONSE AND RECOVERY + ELIMINATE OTHER ATTACK VECTORS

Change the Defender’s Dilemma to an Attacker’s Dilemma

Balance and Focus
Security investments



Security Risk Management Themes

Assume Breach mindset
Security + Productivity
Identity is the Security Perimeter

Assume Breach mindset - designing for failure

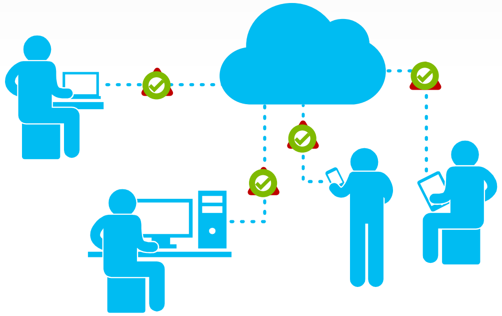
THEN

Reliability: Designed not to fail

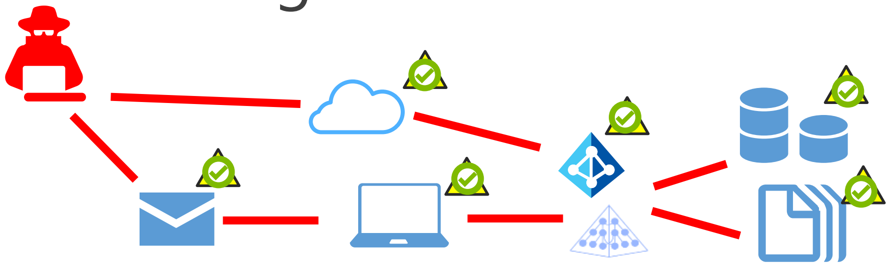
Prevent: Every possible attack

NOW

Resilience: Designed to recover quickly

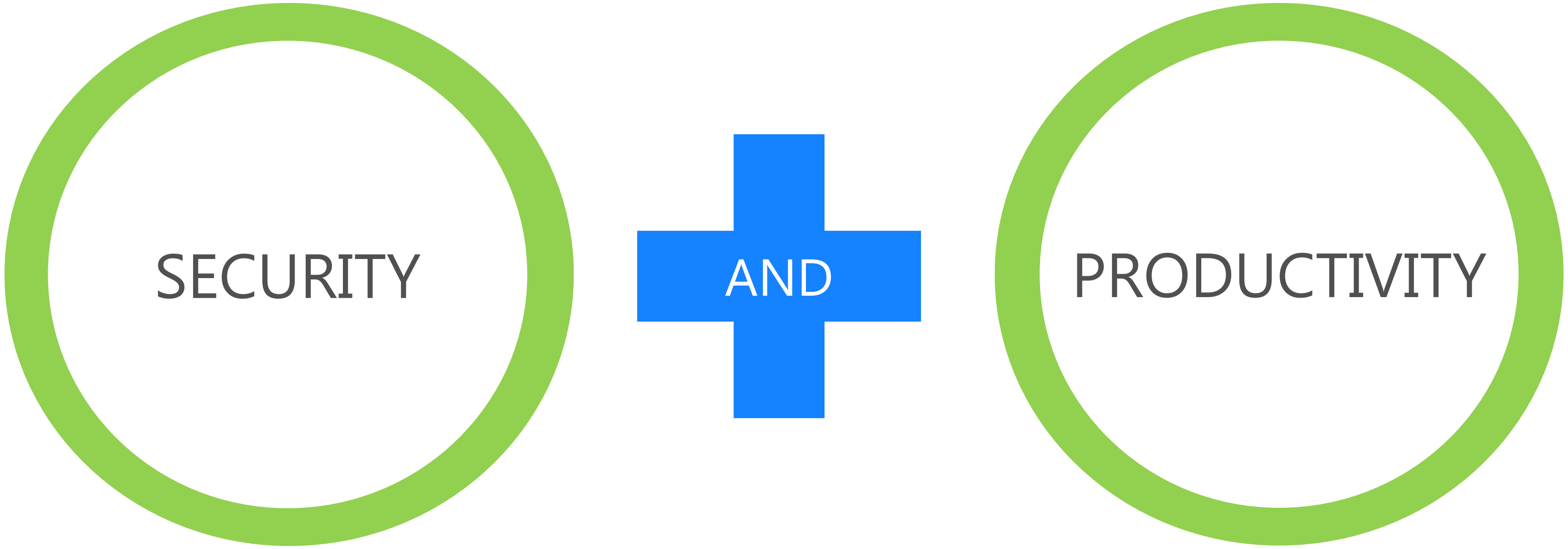


Assume Breach: Protect, Detect, & Respond along the attack chain



THE NEW IMPERATIVE:

Enable people to use devices and apps that work best for them, from anywhere, **while** protecting against current threats



SECURITY

AND

PRODUCTIVITY

COMMON INITIATIVES

- **Biometric and Virtual Smart Card Authentication**
- **Mobile Application Management**
- **Self Service Password Reset**
- **Conditional Access to Resources**
- **…and More**

BIOMETRICS = SECURITY ***AND*** PRODUCTIVITY

- Impossible to forget
- Ease of use
- Fingerprint and facial recognition
- Hardware assurances (VBS)

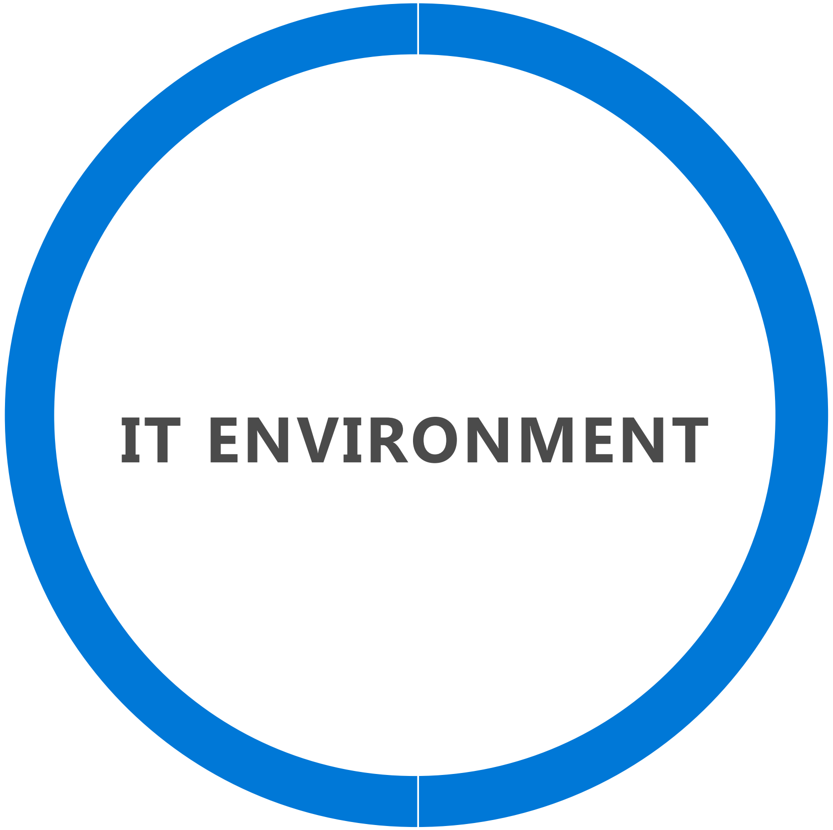
Hello Erwin McDaniel

2:30

Tuesday, July 7

Project sync with Marc
Fourth Coffee
3:30 PM—4:30 PM

SECURITY PERIMETER



YOUR

IT ENVIRONMENT

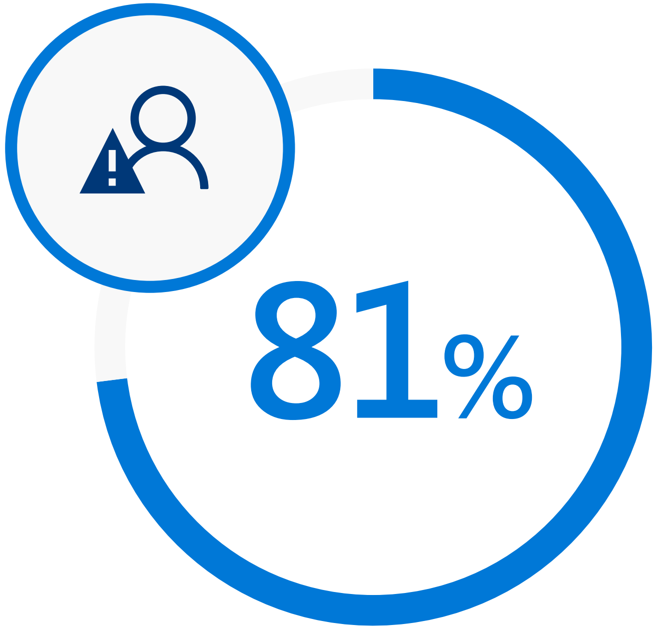
YOUR IT ENVIRONMENT

YOUR OPPORTUNITY

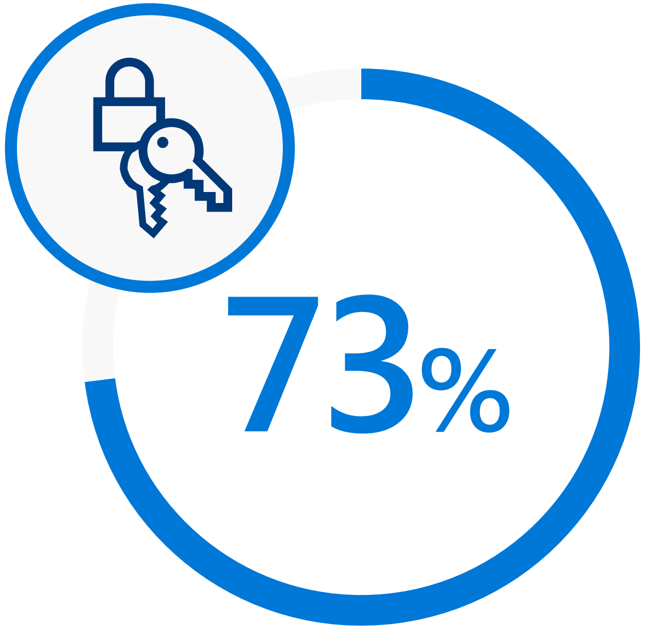
YOUR

IT ENVIRONMENT

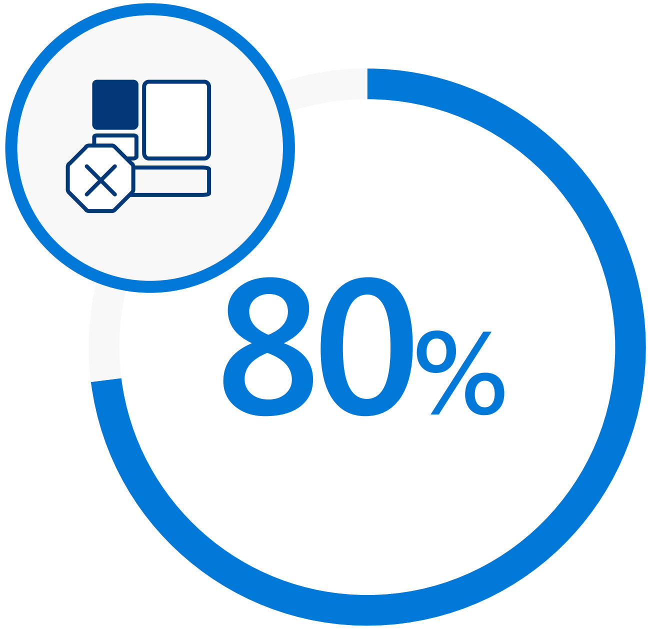
WHY **IDENTITY** IS IMPORTANT



of breaches are caused by credential theft

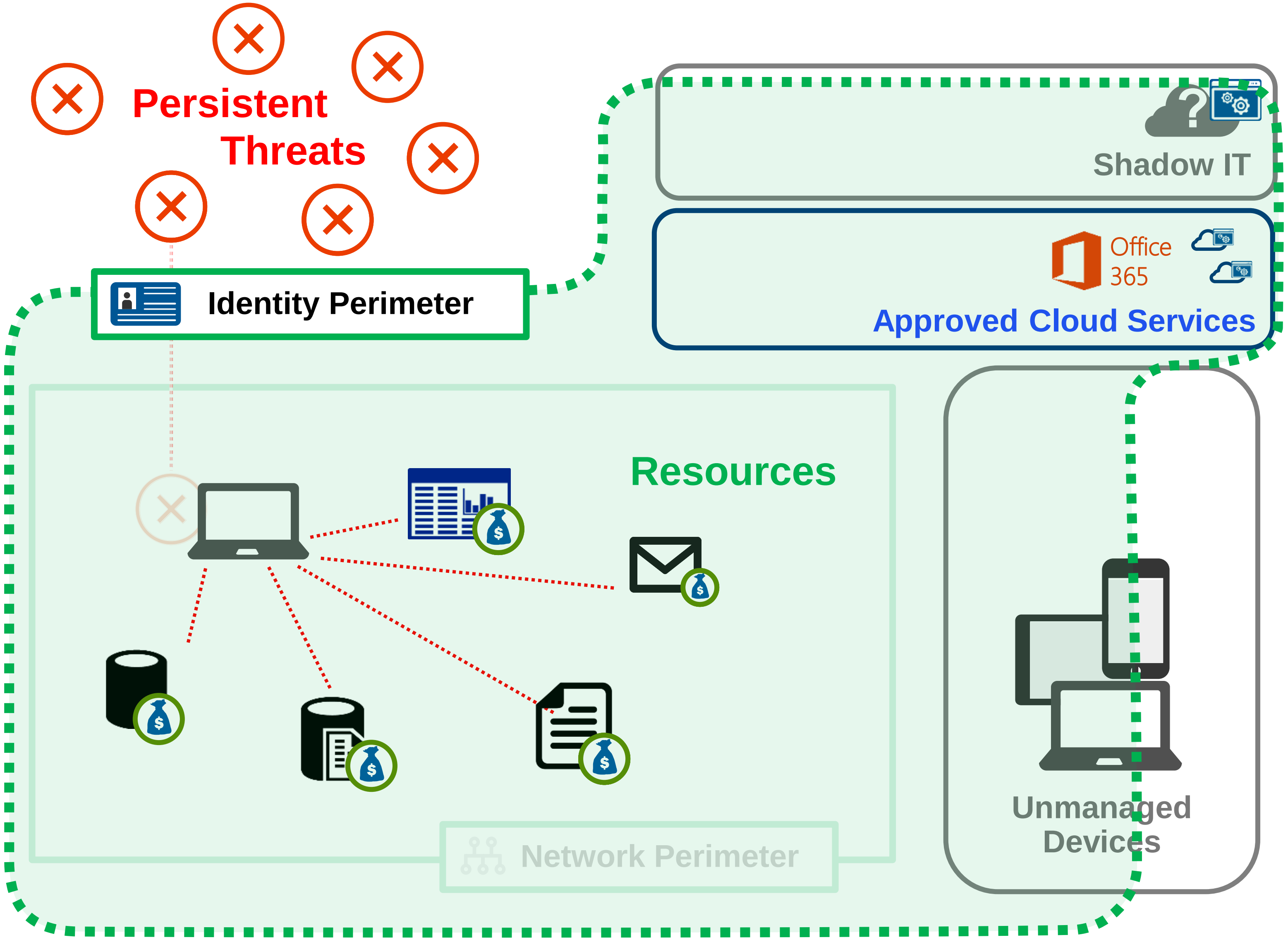


of passwords are duplicates



of employees use non-approved apps for work

Modernizing the Security Perimeter



Network protects against classic attacks…

…but bypassed reliably with
- Phishing
- Credential theft

+ Data moving out of the network

= Critical to build an **Identity security perimeter**

- ***Identity*** - Strong Authentication
- ***Access Management*** – Monitor and enforce access policies
- **Threat intelligence** integration into protections and detections

Who is accessing? What is their role?
Is the account compromised?

Where is the user based? From where is the user signing in? Is the IP anonymous?

Which app is being accessed?
What is the business impact?

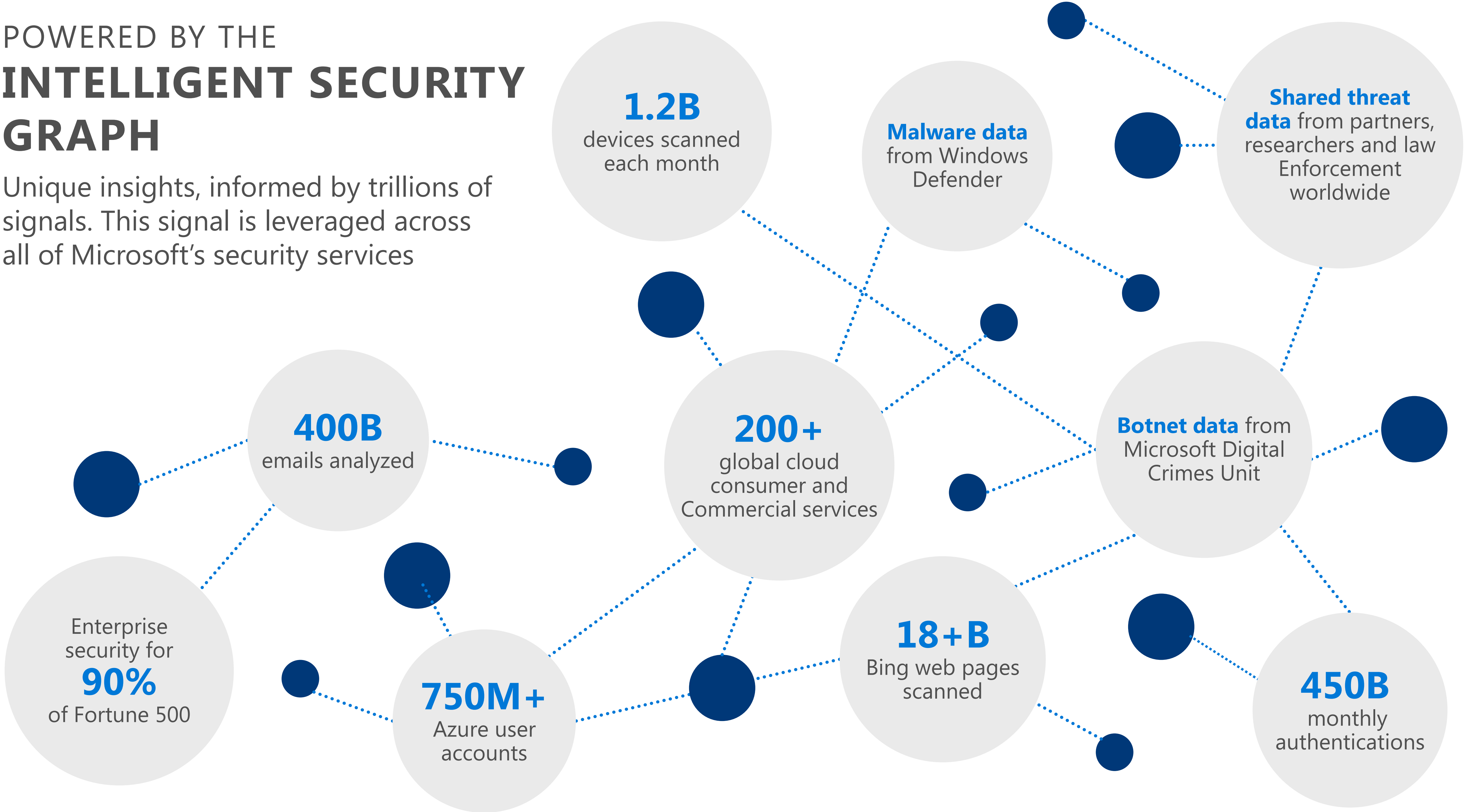
Is the device healthy? Is it managed?
Has it been in a botnet?

What data is being accessed?
Is it classified? Is it allowed off premises?

POWERED BY THE

INTELLIGENT SECURITY GRAPH

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



1.2B devices scanned each month

Malware data from Windows Defender

Shared threat data from partners, researchers and law Enforcement worldwide

400B emails analyzed

200+ global cloud consumer and Commercial services

Botnet data from Microsoft Digital Crimes Unit

Enterprise security for **90%** of Fortune 500

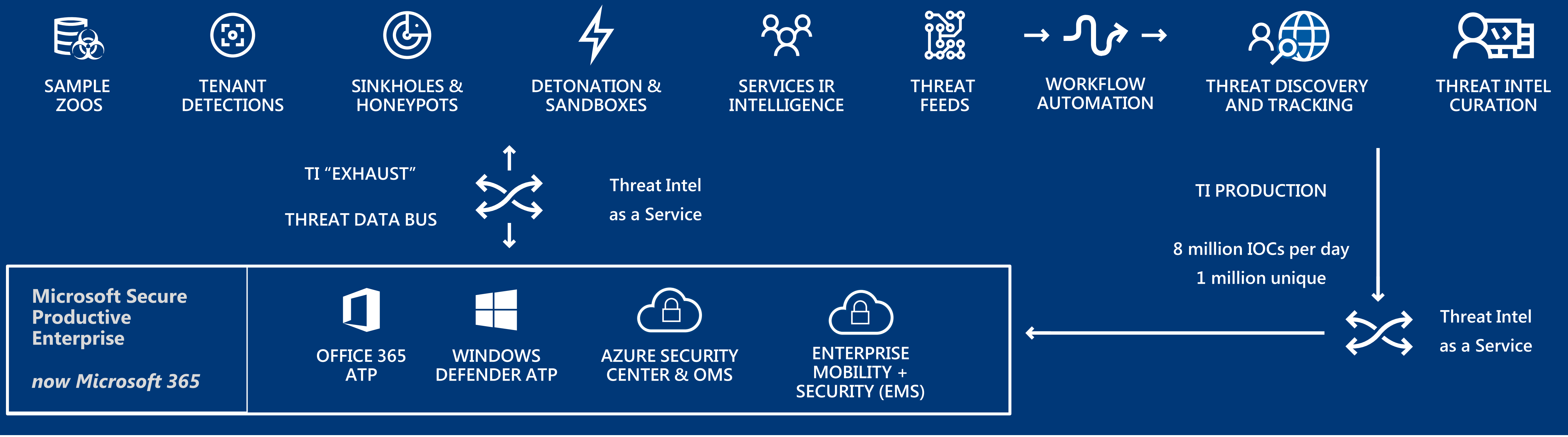
750M+ Azure user accounts

18+B Bing web pages scanned

450B monthly authentications

Microsoft Threat Intelligence System

THREAT DATA SOURCES AND ANALYSIS TOOLS



SAMPLE ZOOS

TENANT DETECTIONS

SINKHOLES & HONEYPOTS

DETONATION & SANDBOXES

SERVICES IR INTELLIGENCE

THREAT FEEDS

WORKFLOW AUTOMATION

THREAT DISCOVERY AND TRACKING

THREAT INTEL CURATION

TI "EXHAUST"

THREAT DATA BUS

Threat Intel as a Service

TI PRODUCTION

8 million IOCs per day

1 million unique

Threat Intel as a Service

Microsoft Secure Productive Enterprise

now Microsoft 365

OFFICE 365 ATP

WINDOWS DEFENDER ATP

AZURE SECURITY CENTER & OMS

ENTERPRISE MOBILITY + SECURITY (EMS)

Next-gen analytics built from security awareness and endpoint data

+

Enhanced correlation driven by big data + machine learning

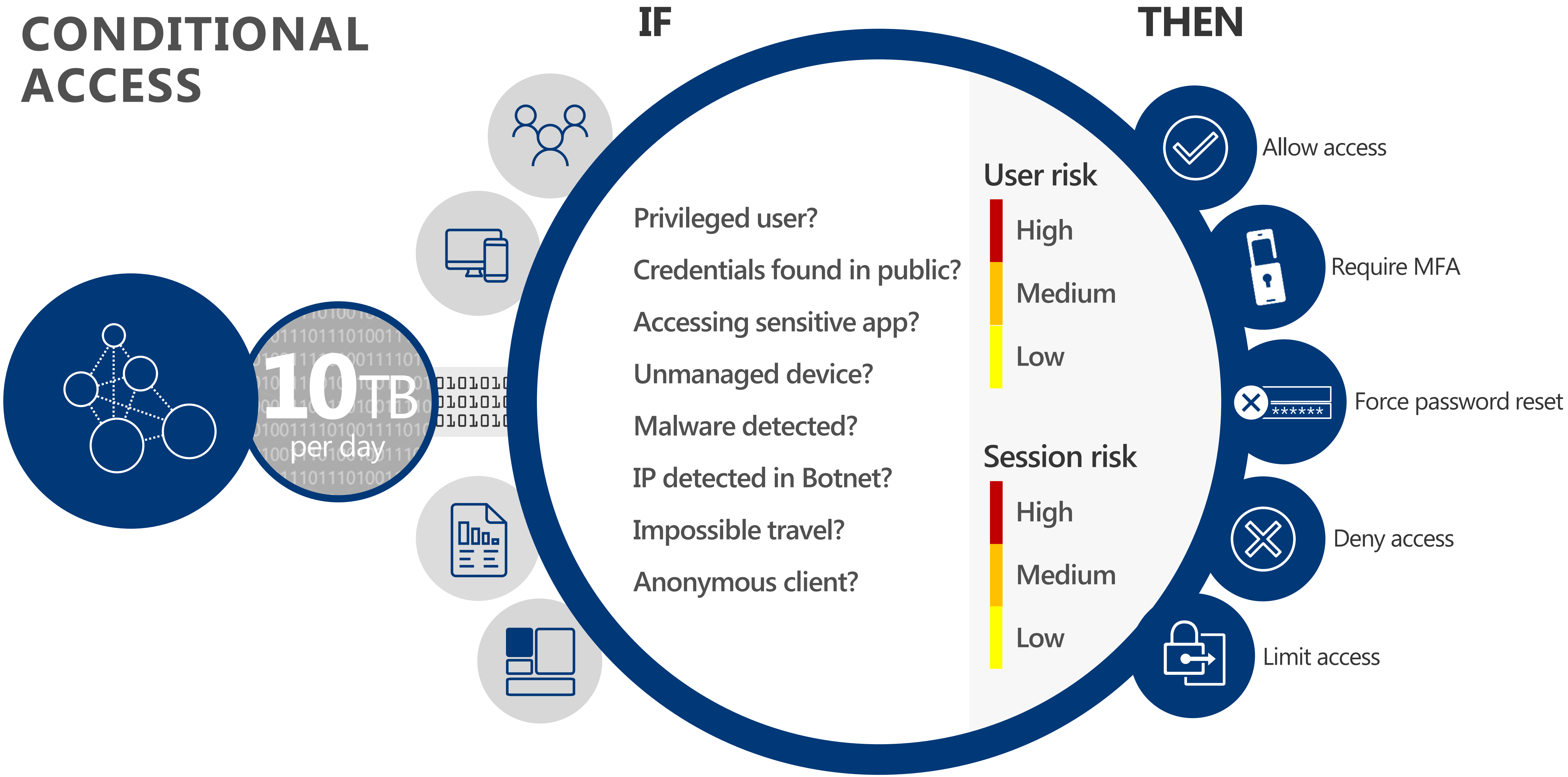
=

Enables **customer-focused** threat intelligence

Relevant, Accurate and Actionable intelligence – enriching the ***Intelligent Security Graph***

Microsoft Threat Intelligence Center

AZURE AD
CONDITIONAL ACCESS



10TB per day

IF

Privileged user?

Credentials found in public?

Accessing sensitive app?

Unmanaged device?

Malware detected?

IP detected in Botnet?

Impossible travel?

Anonymous client?

User risk

- High
- Medium
- Low

Session risk

- High
- Medium
- Low

THEN

- Allow access
- Require MFA
- Force password reset
- Deny access
- Limit access

Summary

- This is a cyber arms race
  - You need a Cloud Service Provider partner
- Focus on raising attacker cost
- Assume breach mindset
  - Protect / Detect / Respond across the attack chain
- Security + Productivity
- Identity is the Security Perimeter

This presentation was delivered on a Surface Pro 4

Microsoft