RSAConference2018

San Francisco | April 16 – 20 | Moscone Center

MATTERS NOW

SESSION ID: SPO1-W04

CIRCLE THE WAGONS! HOW ALL OF US DEFENDERS CAN WORK TOGETHER

Johnnie Konstantas

Sr. Director, Enterprise Cybersecurity Group
Microsoft
@jkonstantas

Rob Lefferts

Director, Enterprise and Security
Microsoft

Sam George

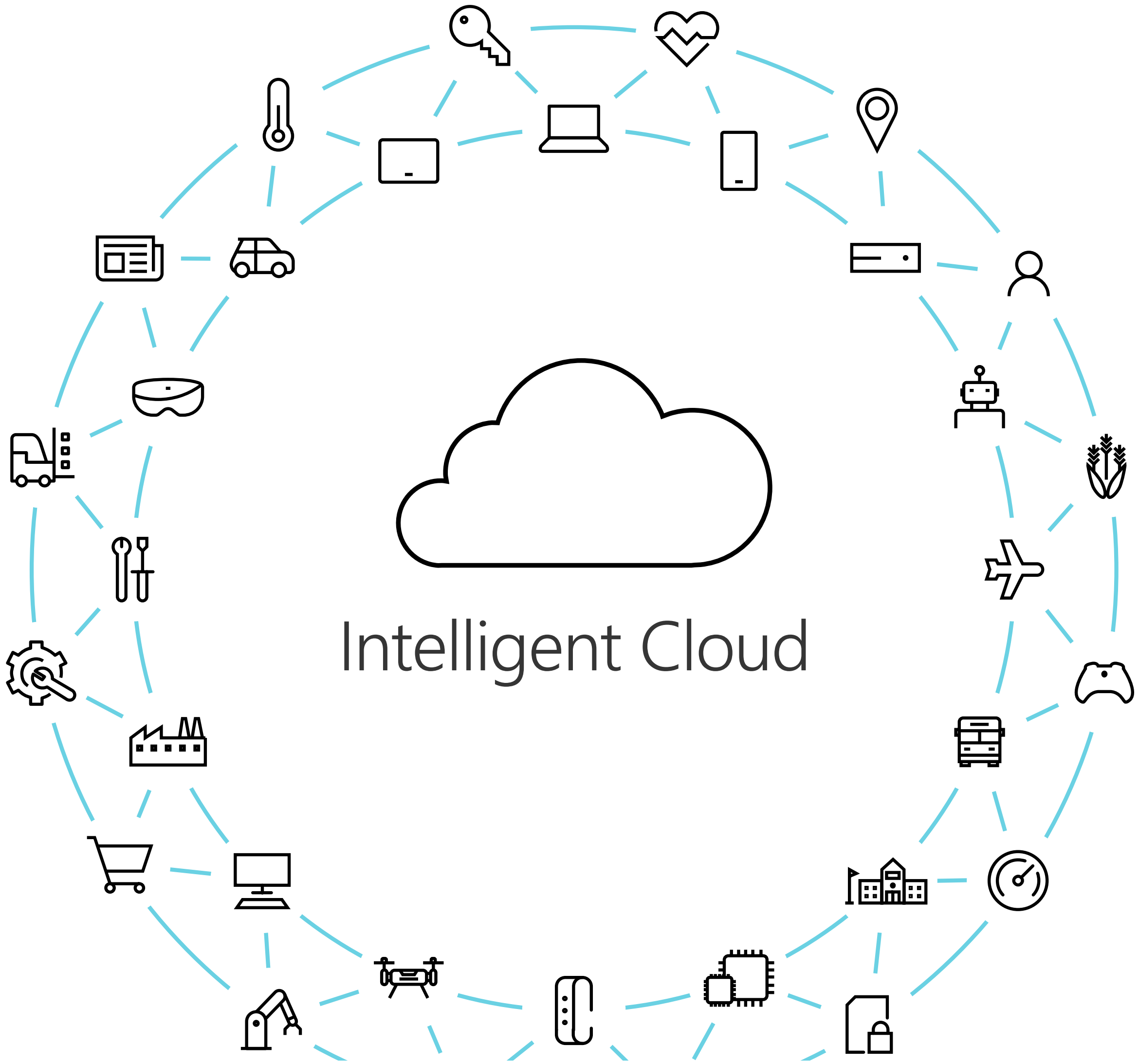
Director, Azure IoT
Microsoft
@samjgeorge

Easy marks are under attack

Adversaries still find low-hanging fruit quite tasty

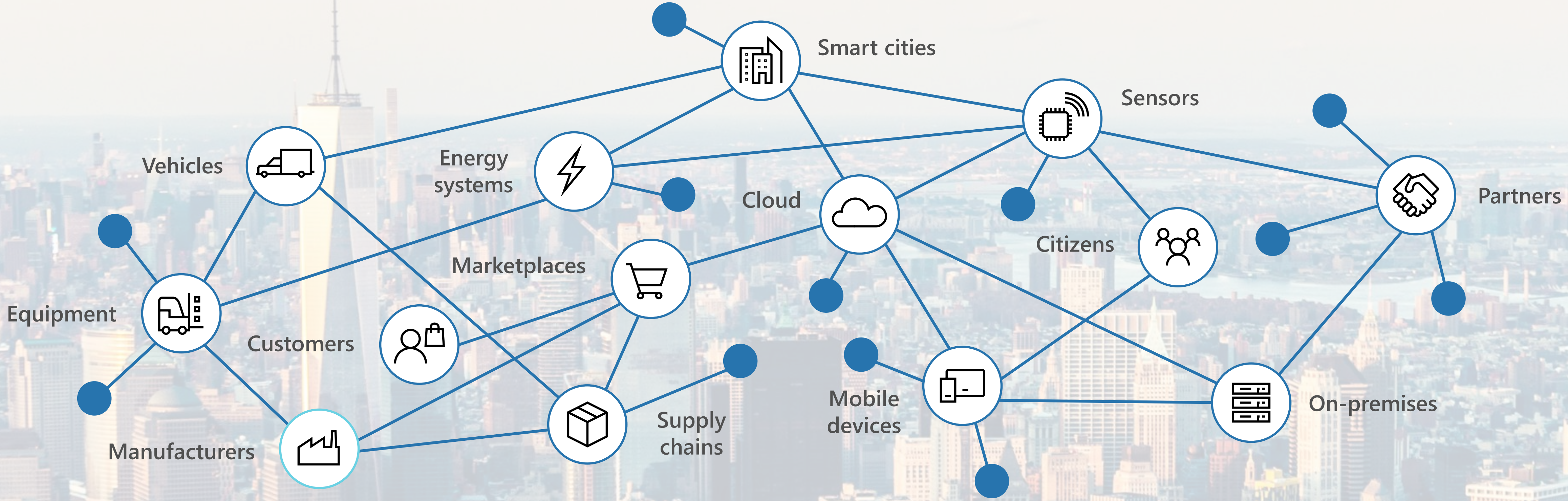
- Only 4% of SaaS apps support all HTTP headers session protection
- Gamarue: 23 million infected IPs, 1,200 C2 points, 464 distinct botnets
- 96% of malware is automated polymorphic
- Phishing volume: 200 million messages a month

https://www.microsoft.com/SIR



Intelligent Edge

The digital estate



150+ security controls
500+ vendors

The market is fragmented and confusing

Anomaly detection

Endpoint protection

Hybrid cloud security

Data & application security

Fraud prevention

Infrastructure security

Security management

Threat management

Data loss prevention

Data center security

Cloud Access Security Broker

Information rights management

Identity & access management

Compliance tools

Threat detection

IoT security

Email security

Circle the wagons!

We can share resources

Intelligence

Platform

Partners

Circle the wagons!

We can share resources

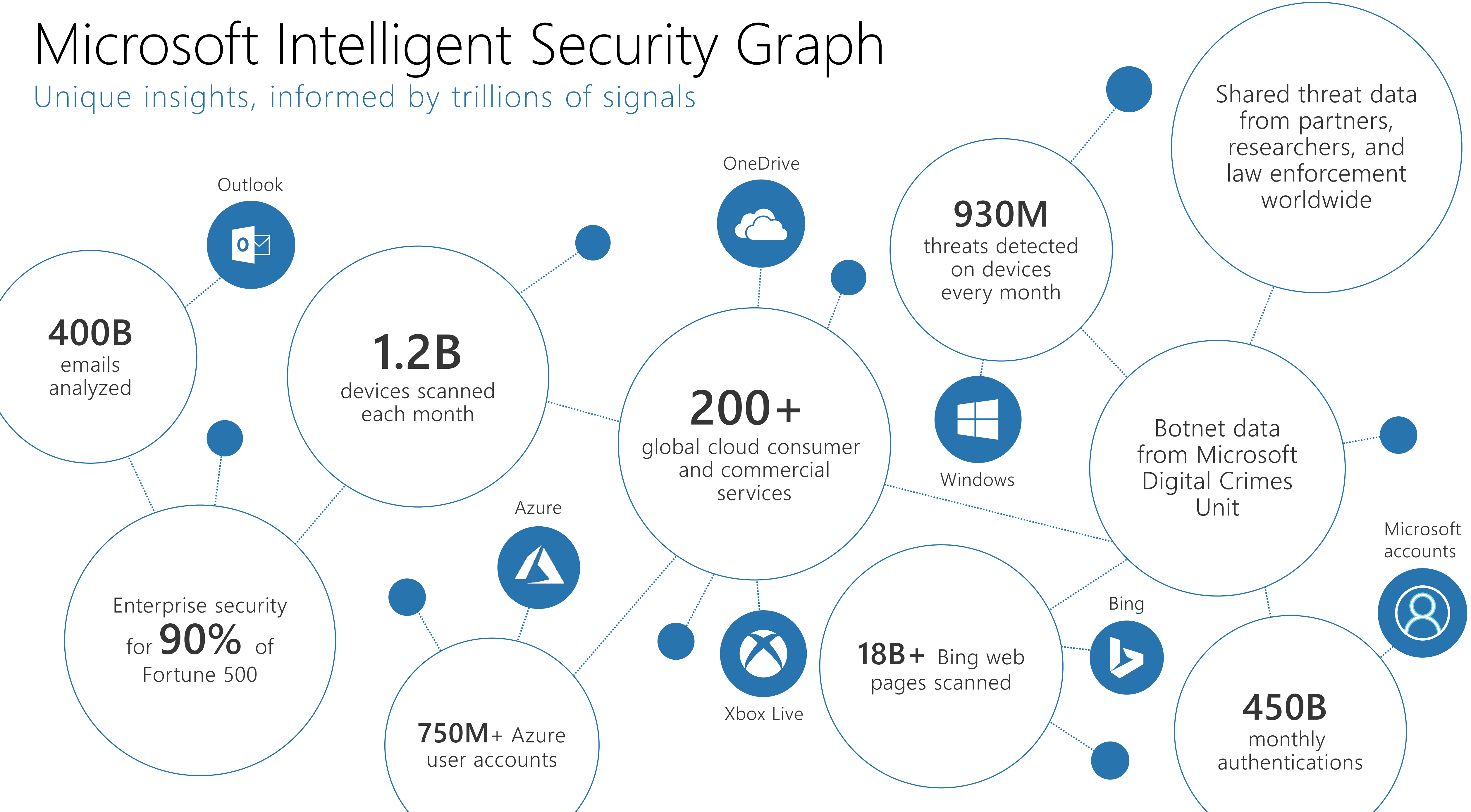
Intelligence

Platform

Partners

Microsoft Intelligent Security Graph

Unique insights, informed by trillions of signals



Outlook

400B emails analyzed

1.2B devices scanned each month

OneDrive

200+ global cloud consumer and commercial services

930M threats detected on devices every month

Shared threat data from partners, researchers, and law enforcement worldwide

Windows

Botnet data from Microsoft Digital Crimes Unit

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

Azure

750M+ Azure user accounts

Xbox Live

18B+ Bing web pages scanned

Bing

Microsoft accounts

450B monthly authentications

Human intelligence

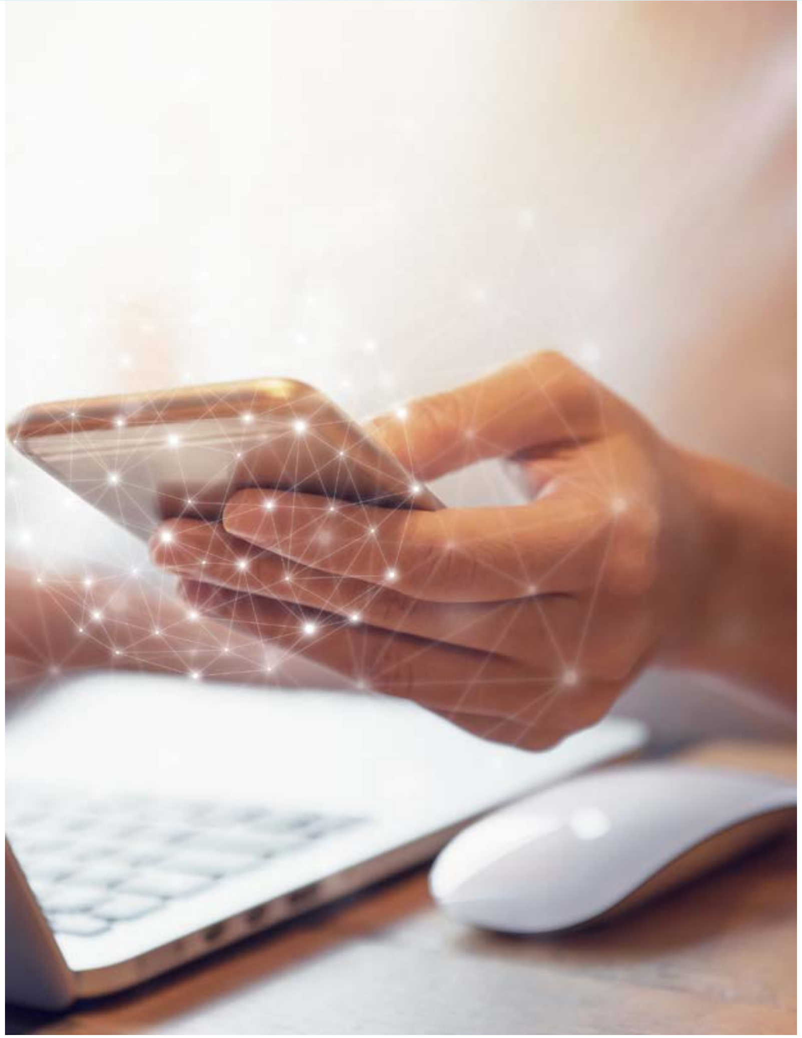
Intelligence

Platform

Partners

Partnerships to Defend Against a World of Increased Threats

By working together we can help protect our **mutual** customers



Areas of Collaboration

Identity and access management

Account authentication SSO across services and devices

Threat protection

Suspicious behavior and activity detection and response

Information protection

Business data and app classification and control

Security management

Security risk assessment, controls and intelligence

Areas of Collaboration

Identity and access management

Account authentication SSO across services and devices

Azure Active Directory

Threat protection

Suspicious behavior and activity detection and response

Microsoft Intune

Windows Defender Advanced Threat Protection

Information protection

Business data and app classification and control

Azure Information Protection

Security management

Security risk assessment, controls and intelligence

Azure Security Center

Powered by the
Intelligent Security Graph

Microsoft Intelligent Security Association

ANOMALI

Barracuda

Bitdefender

Check Point SOFTWARE TECHNOLOGIES LTD.

DIGITAL GUARDIAN

f5

FORCEPOINT

IONIC

Lookout

Omada

paloalto NETWORKS

Ping Identity

SailPoint

SAVIYNT

SentinelOne

THREATCONNECT

ziften

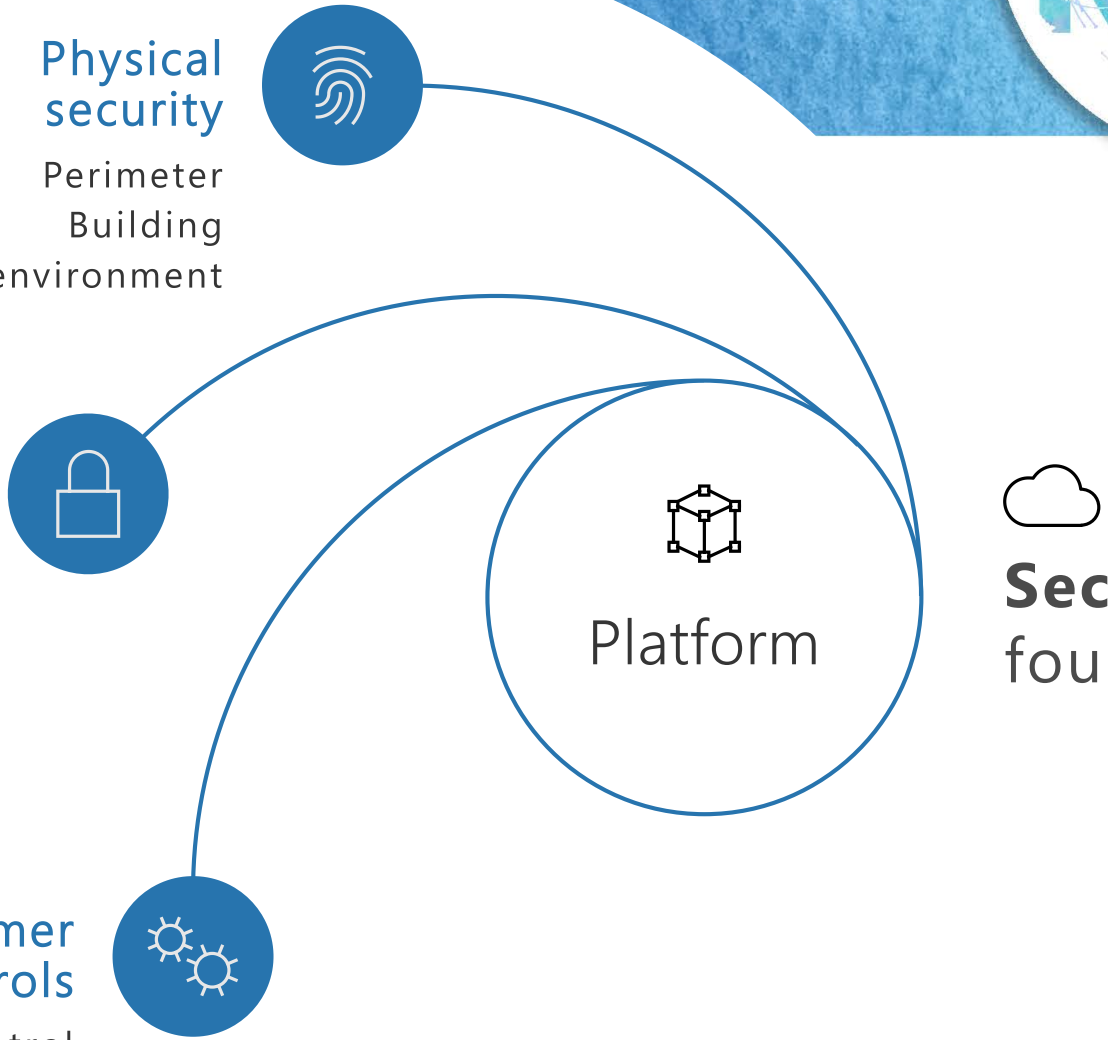
zscaler

IMPERVA

Intelligence

Platform

Partners



Physical security

Perimeter
Building
Server environment

Operational security

Continuous testing
Restricted access
Thousands of security professionals

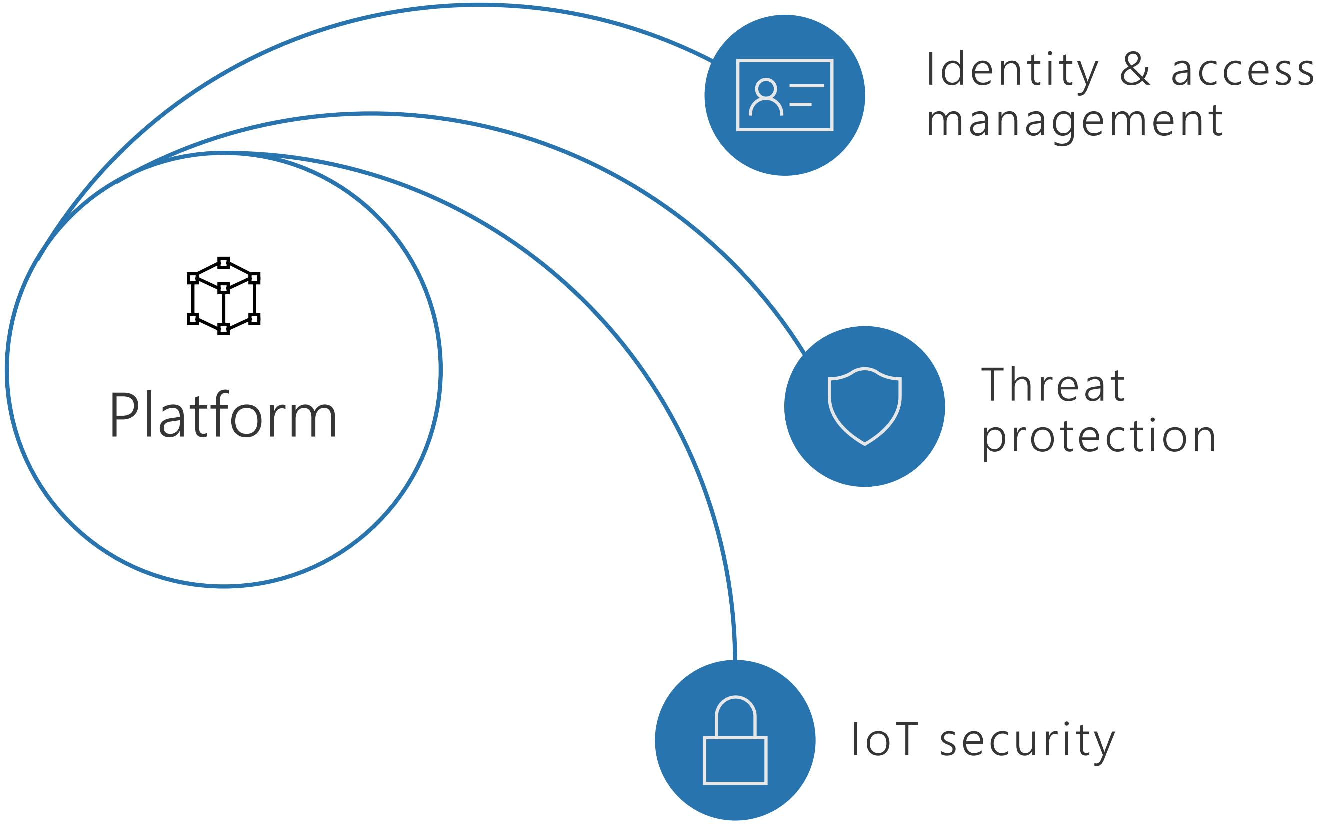
Customer controls

Access control
Encryption & key management
Network & DDoS protection

Secure foundation

Platform

Built in security



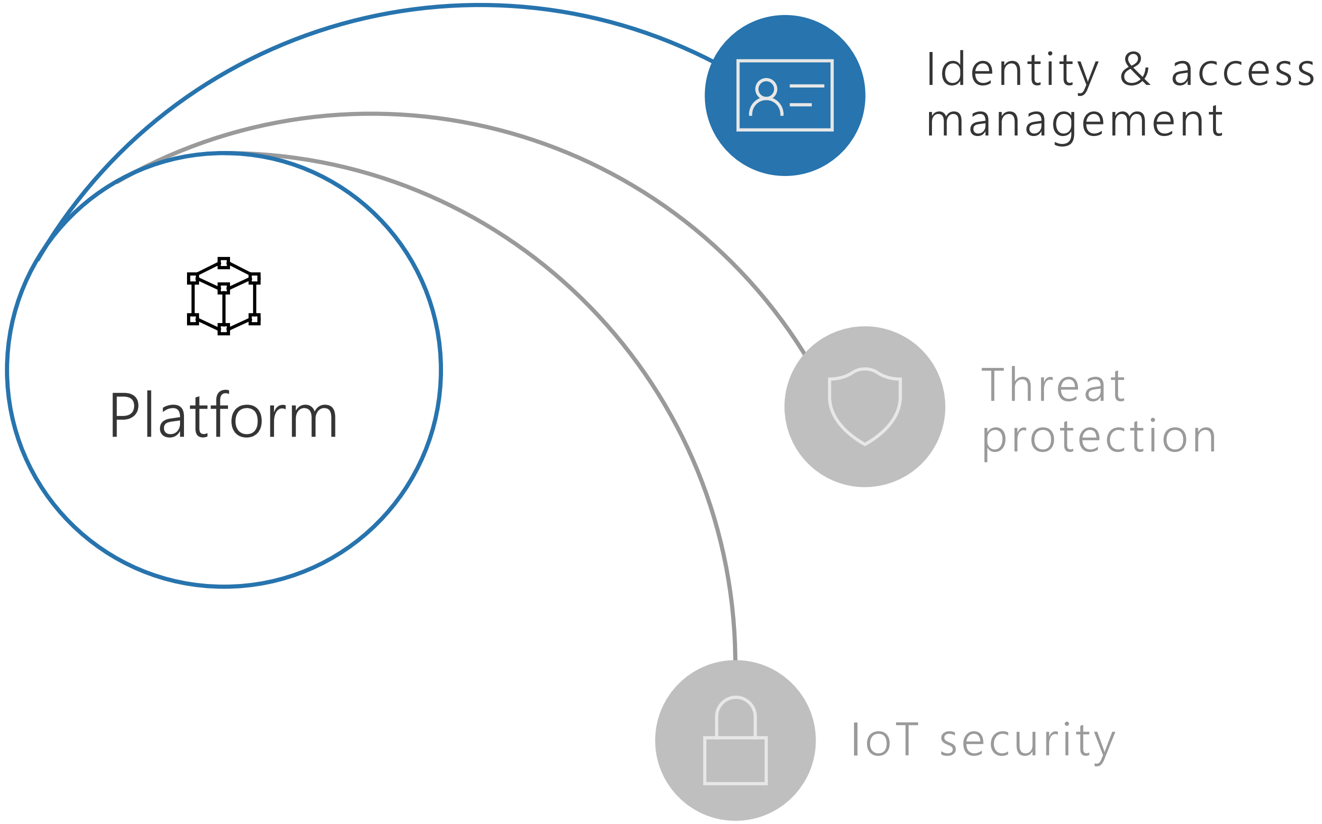
Platform

Identity & access management

Threat protection

IoT security

Built in security



Fast identity online – the FIDO Alliance

The world's largest ecosystem for standards-based, interoperable auth

Security on-premises and web

Secure mobile user credentials

Secure authentication

FIDO board members

Microsoft · Google · Nok Nok LABS · oberthur TECHNOLOGIES THE M COMPANY · Lenovo · aetna · Bank of America

PayPal · infineon · USAA · FINGERPRINTS · intel · ARM · yubico Trust the Net.

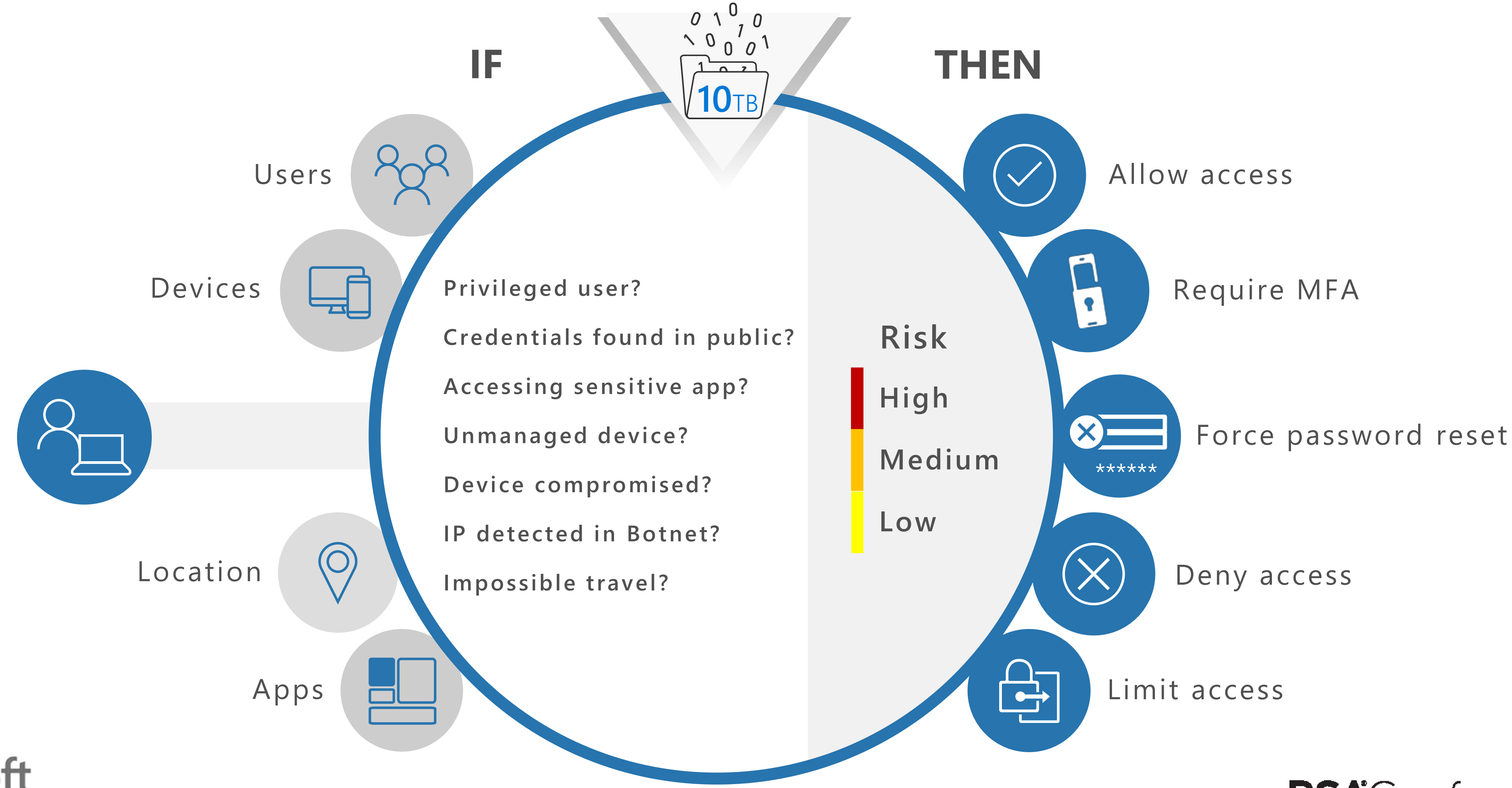
VASCO TRUST FOR THE DIGITAL WORLD · BCcard · RAON SECURE · mastercard · SAMSUNG · egis Technology · Synaptics

RSA · QUALCOMM · AMERICAN EXPRESS · gemalto security to be free · NTT docomo · NXP · ING

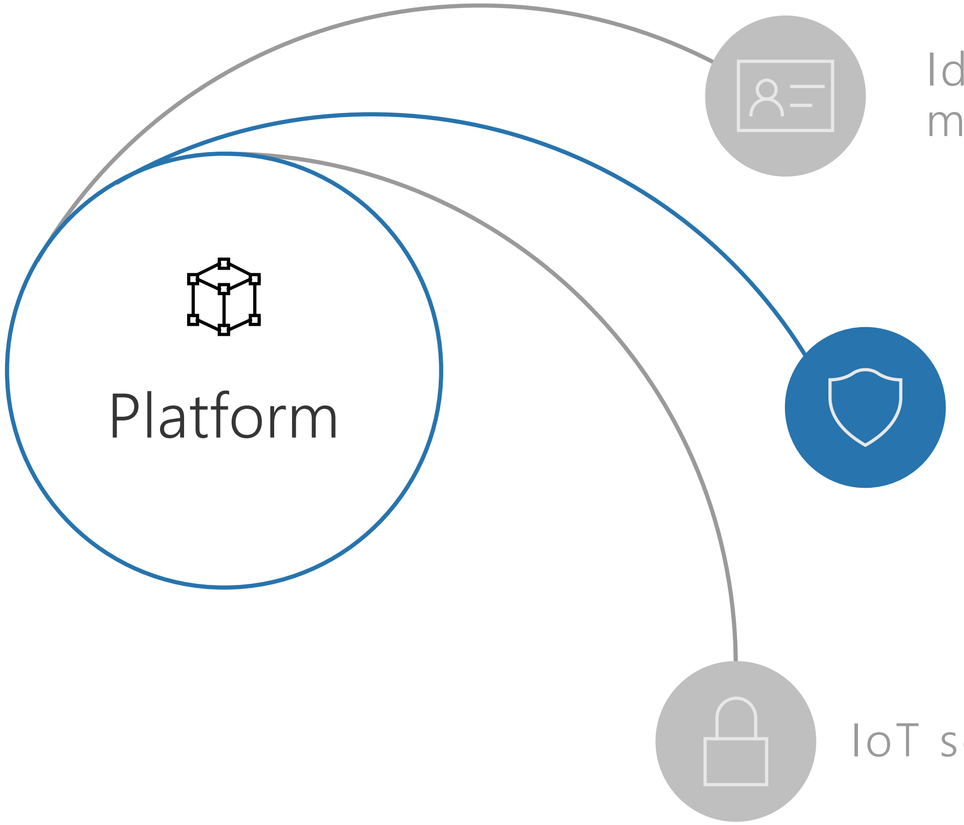
CrucialTec · VISA · Daon · FEITIAN WE BUILD SECURITY · Alibaba.com Global trade starts here. · LINE

Microsoft

Conditional Access



Built in security



Threat protection
Cloud-driven and automated

#RSAC

Reduce attack surface

Detect attacks faster and block them

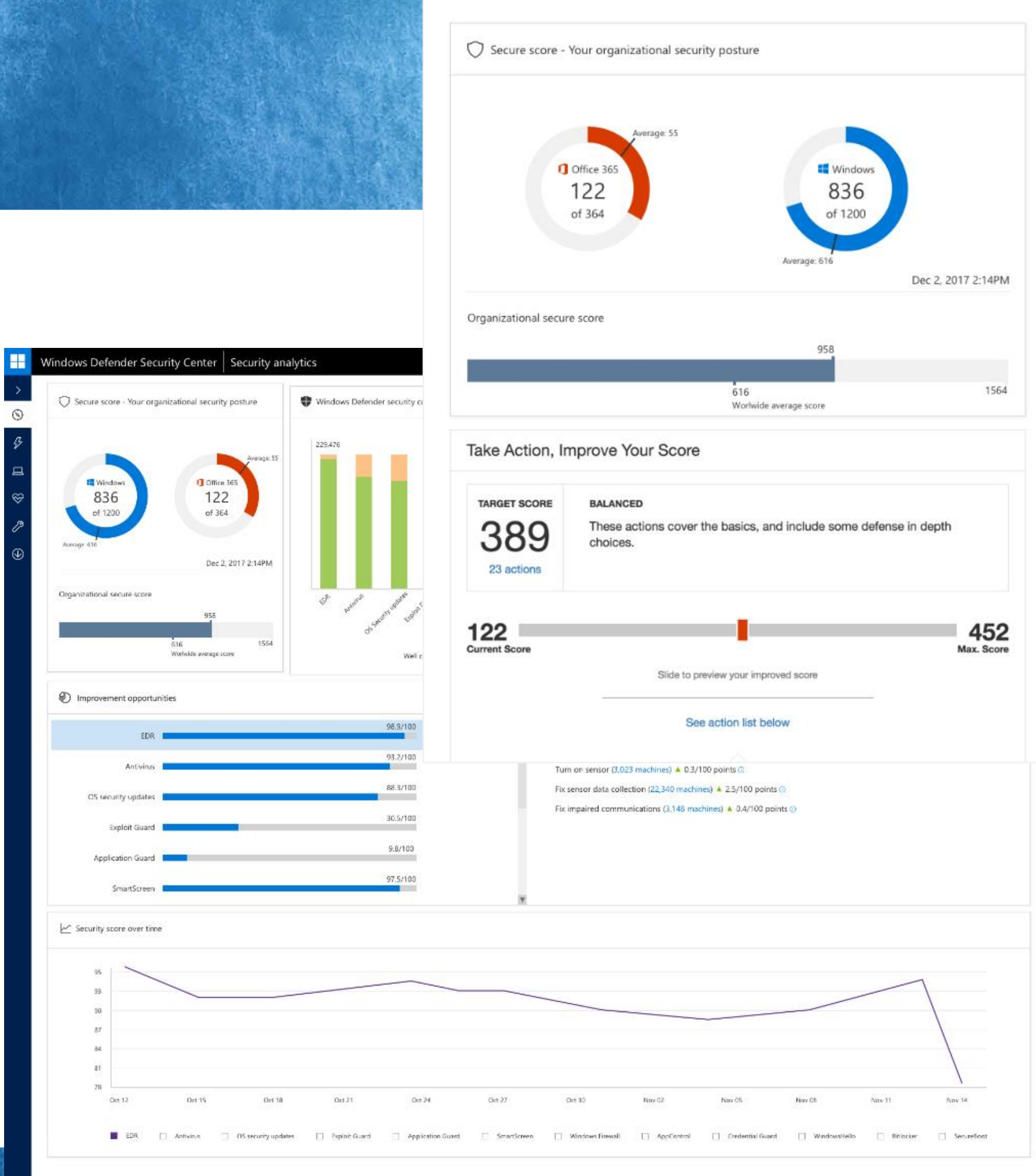
Respond automatically to breaches where appropriate

Reduce attack surface

Assess your security state **continuously**

Enable security controls, and receive recommendation for further improvements

Remediate vulnerabilities and **drive** compliance



Windows Defender Security Center | Security analytics

Secure score - Your organizational security posture

Improvement opportunities

EDR	98.9/100
Antivirus	93.2/100
OS security updates	88.3/100
Exploit Guard	30.5/100
Application Guard	9.8/100
SmartScreen	97.5/100

Security score over time

Secure score - Your organizational security posture

Take Action, Improve Your Score

TARGET SCORE
389
23 actions

BALANCED
These actions cover the basics, and include some defense in depth choices.

Slide to preview your improved score

See action list below

Turn on sensor (3,023 machines) ▲ 0.3/100 points

Fix sensor data collection (22,340 machines) ▲ 2.5/100 points

Fix impaired communications (3,148 machines) ▲ 0.4/100 points

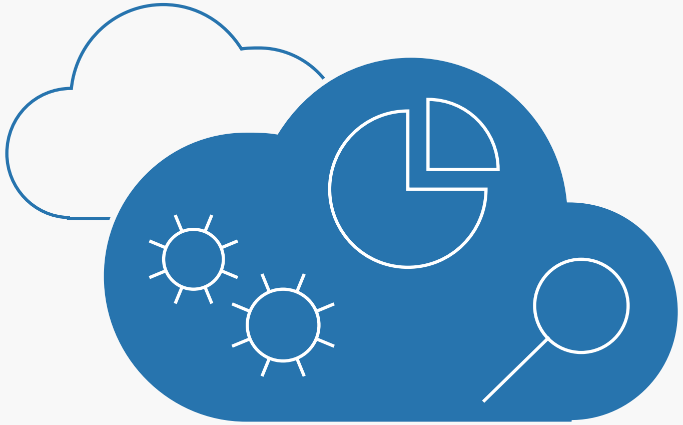
Detect and block attacks

Gain **visibility** and **reduce** blind spots

Detect attacks and **zero-day** exploits

Investigate your cloud ecosystem, the device, and your identities

Cloud-driven advanced behavioral analytics and machine learning



POWERED BY
THE INTELLIGENT
SECURITY GRAPH

Respond automatically to breaches

Investigate and remediate threats

We do the investigation and remediation faster than anyone, and we do it at scale.

Driven by artificial intelligence

Applies industry best practices and intelligent decision-making algorithms to determine whether a threat is real and what action to take.

Cyber analyst logic at scale

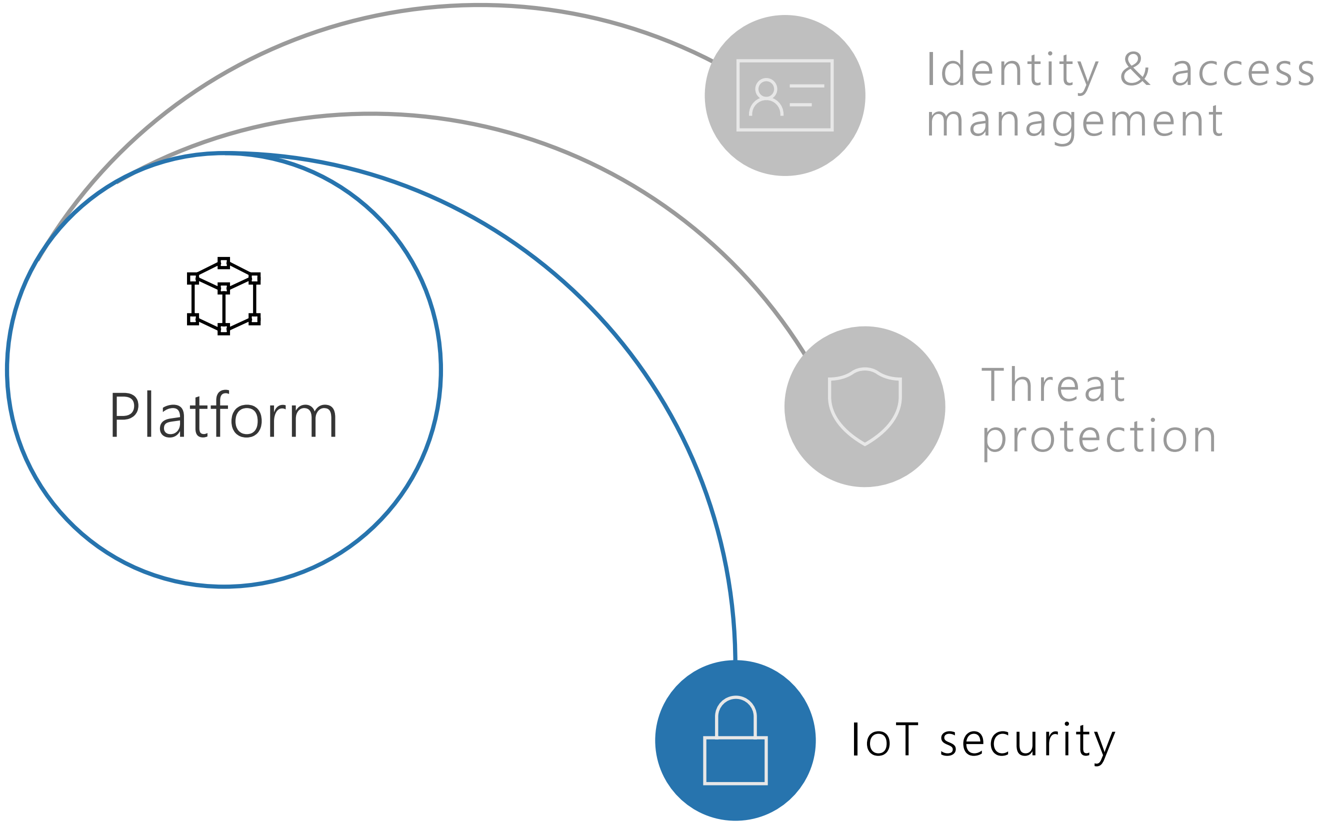
Automatically investigates alerts to determine the appropriate course of action. Multiple parallel investigations to resolve the full extent of a breach.

Choose how to close the loop

Remediates threats automatically without human intervention to stop further damage or infection. Your choice: fully automated or semi-automated.

Going from alert to remediation in minutes at scale

Built in security



How do you know that the compressor in your fridge needs to be replaced?

How do you know that the compressor in your fridge needs to be replaced?

TODAY

Melted ice cream and spoiled milk

TOMORROW

Message that a technician with replacement compressor will arrive tonight

How do you know that the compressor in your fridge needs to be replaced?

TODAY

Melted ice cream and spoiled milk

TOMORROW

Message that a technician with replacement compressor will arrive tonight

THE DIFFERENCE IS CLOUD CONNECTIVITY

Highly secured connected devices require 7 properties

Hardware Root of Trust

▣

Is your device's identity and software integrity secured by hardware?

Defense in Depth

▣ ⚙

Does your device remain protected if a security mechanism is defeated?

Small Trusted Computing Base

▣ ⚙

Is your device's TCB protected from bugs in other code?

Dynamic Compartments

▣ ⚙

Can your device's security protections improve after deployment?

Certificate-Based Authentication

▣ ⚙ ☁

Does your device use certificates instead of passwords for authentication?

Failure Reporting

▣ ⚙ ☁

Does your device report back about failures and anomalies?

Renewable Security

▣ ⚙ ☁

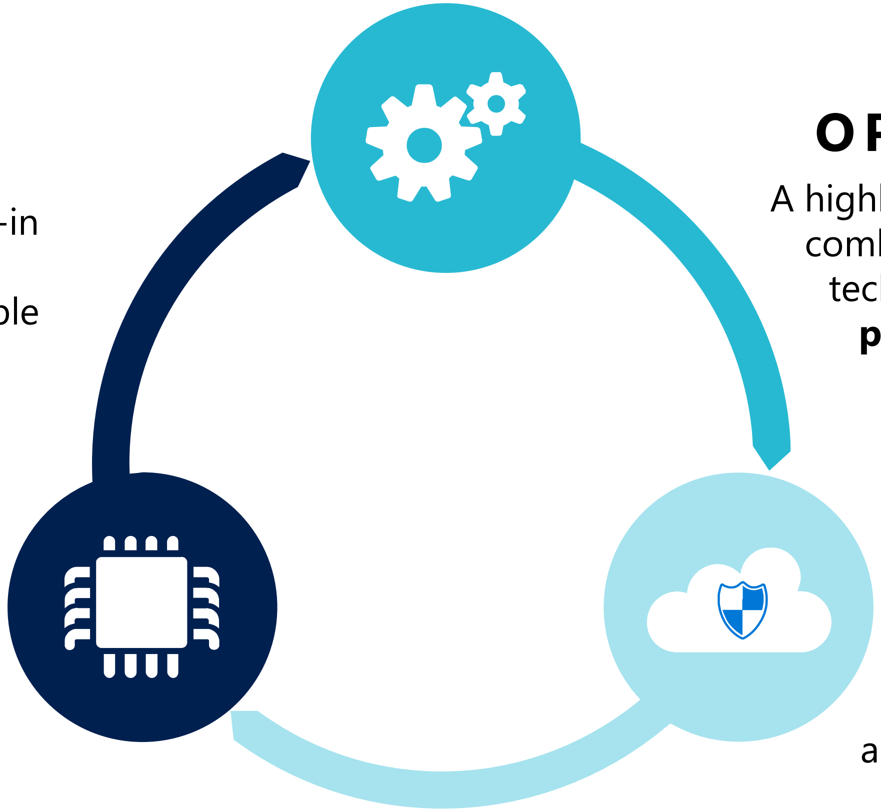
Does your device's software update automatically?

▣ = Silicon support required ⚙ = OS support required ☁ = Cloud Service support required

http://aka.ms/7properties

Azure Sphere

an end-to-end solution for creating highly-secured, connected MCU devices



SECURED **MCUs**

A new **4x4-class of MCUs** with built-in Microsoft security technology provide connectivity and a dependable hardware root of trust.

SECURED **OPERATING SYSTEM**

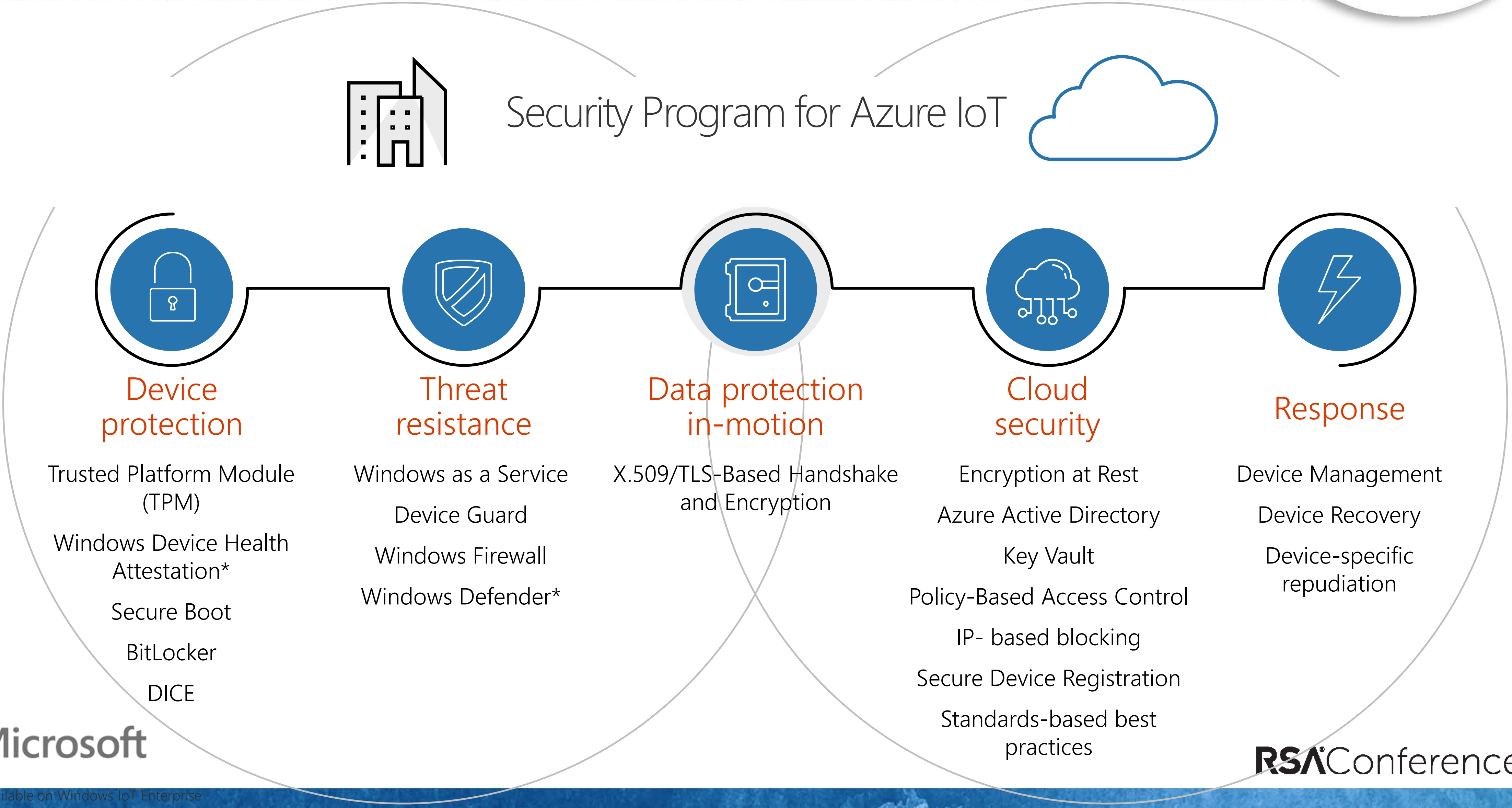
A highly-secured **4x4 IoT OS** from Microsoft combines the best of Microsoft and OSS technologies to create **a trustworthy platform** for new IoT experiences

CLOUD SERVICE SECURING EACH DEVICE

The **4x4 Security Service** guards every 4x4 device; it **brokers trust** for device-to-device and device-to-cloud communication, **detecting emerging threats**, and **renewing security**.

Device to Cloud Security

#RSAC



Security Program for Azure IoT

Device protection

Trusted Platform Module (TPM)

Windows Device Health Attestation*

Secure Boot

BitLocker

DICE

Threat resistance

Windows as a Service

Device Guard

Windows Firewall

Windows Defender*

Data protection in-motion

X.509/TLS-Based Handshake and Encryption

Cloud security

Encryption at Rest

Azure Active Directory

Key Vault

Policy-Based Access Control

IP- based blocking

Secure Device Registration

Standards-based best practices

Response

Device Management

Device Recovery

Device-specific repudiation

*Only available on Windows IoT Enterprise

Security Program for Azure IoT

Trusted security auditors trained on Azure IoT

Discover issues, get recommended remediations

Keep your IoT Solution secure

{X}

AppSec Application security Labs

AUJAS Managing Information Risk

casaba

Crowe Horwath.

CyberX

Microsoft

OccamSec Advanced infosec operations

PRAETORIAN

SecureGUARD

Tech Mahindra

UNISYS

Not all partners may be listed; check internetofyourthings.com for latest status

Apply what you have learned today

- Next week:
  - Understand what low hanging fruit your organization is offering to adversaries
- In the next three months:
  - Find three ways you can increase security through cloud adoption
- In the next six months:
  - Assess your IoT supply chain against the 7 principles

THANK YOU!