



IoT in Action

#IoTinActionMS



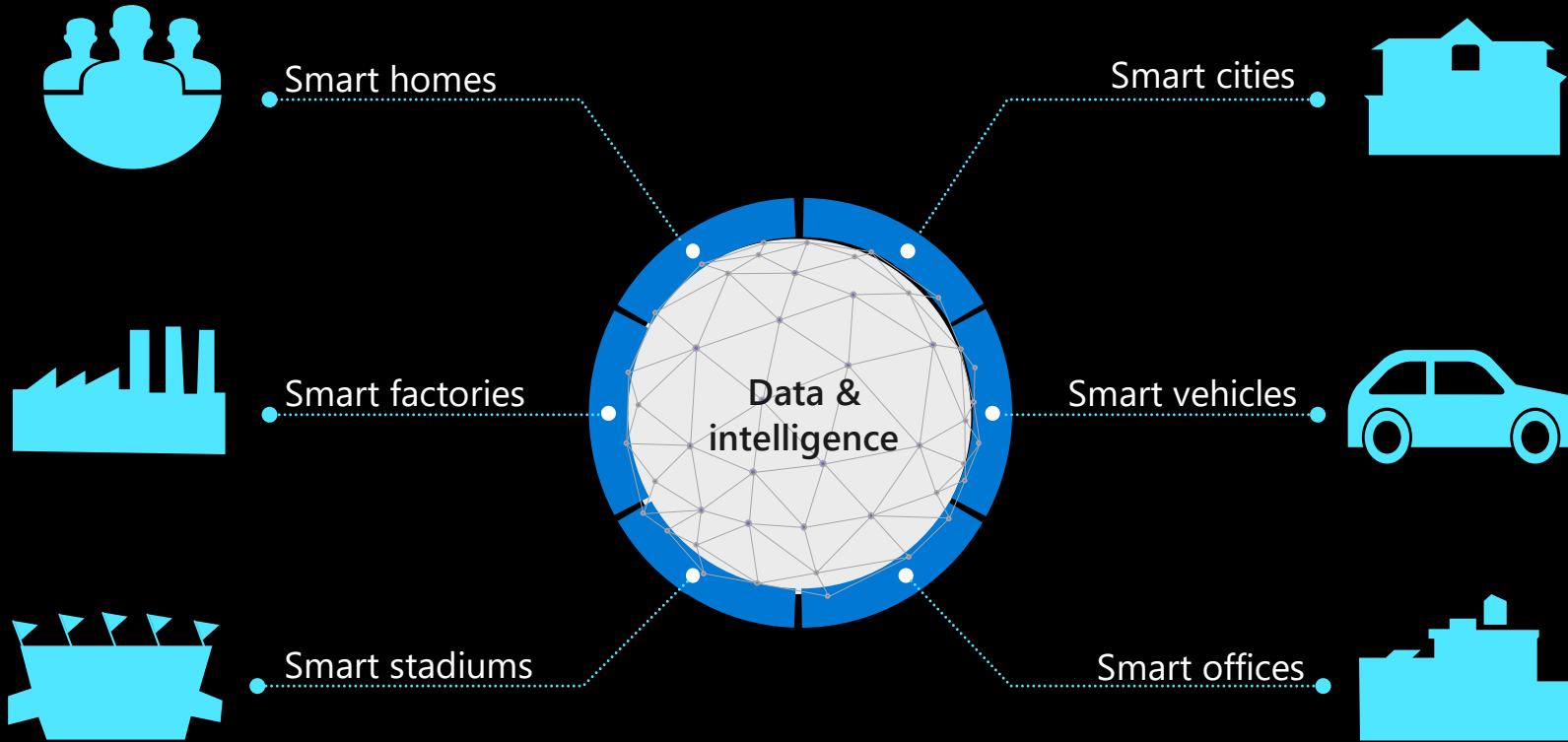
Developing an IoT security practice for durable innovation

Maarten Struys
Sr. Technical Specialist, Microsoft

IoT in Action

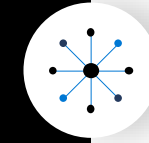


IoT is fueling digital transformation



20 billion connected devices by 2020

—Gartner



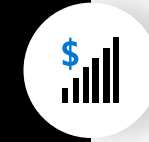
41.6B

Connected "things" by 2025
generating 180ZB of data



\$130B

New monetization avenues
due to IoT-related services



80%

Companies that increased
revenue as a result of IoT
implementation



\$100M

Average increase in
operating income (avg. 8%)
among the most digitally
transformed enterprises



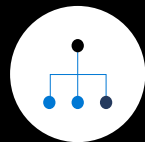
Reduce costs



Delight customers



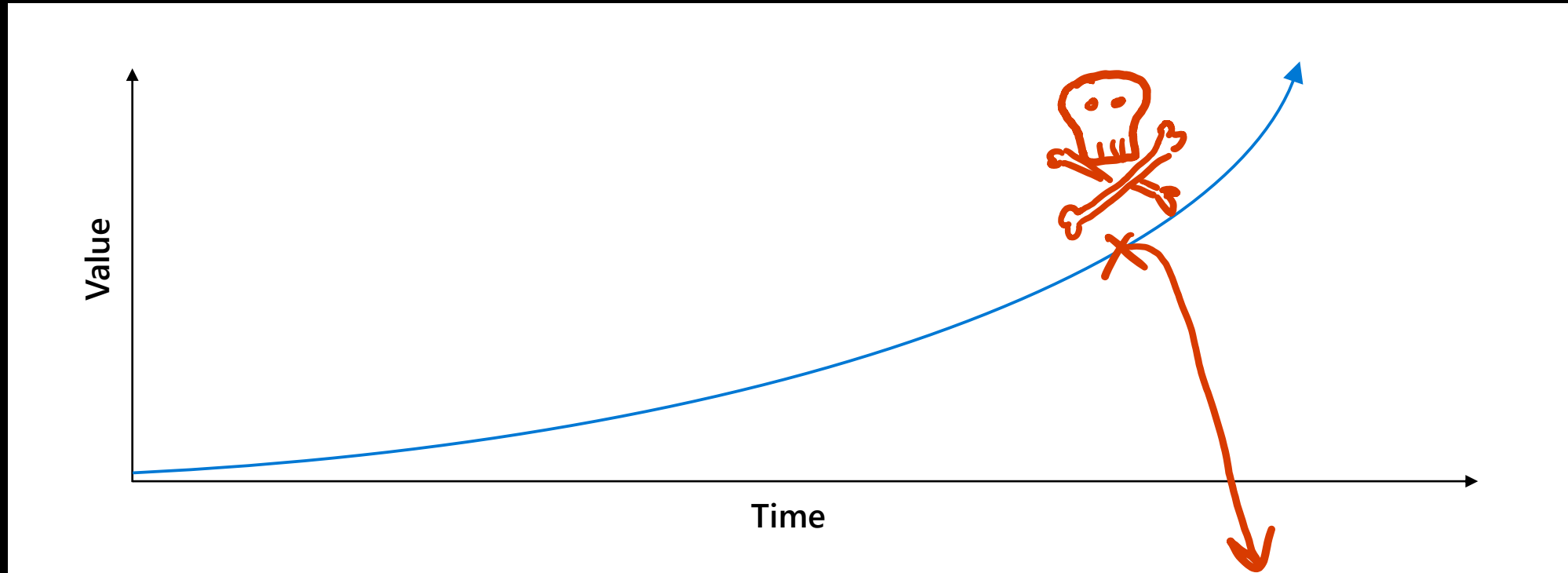
Streamline operations



Create new business models



Planning your IoT deployment



PoC stage
slow climb in value

Production deployment
delivering real business value

~~**Iteration**
accelerating value through
digital feedback loop~~

"Protecting Your Family: The Internet of Things Gives Hackers Creepy New Options"

"Security experts warn of dangers of connected home devices"

Cyberattacks On IOT Devices Surge 300% In 2019, 'Measured In Billions', Report Claims

"Industrial IoT to equip new era of corporate intruders coming in through devices"

"Industrial IoT to equip new era of corporate intruders coming in through devices"

"The IoT ransomware threat is more serious than you think"

"Industrial IoT to equip new era of corporate intruders coming in through devices"

"When smart gadgets spy on you: Your home life is less private than you think"

"Webcam firm recalls hackable devices after mighty Mirai botnet attack"

"The Lurking Danger of Medical Device Hackers"

"Hackers exploit casino's smart thermometer to steal database info"

"Hacking critical infrastructure via a vending machine? The IOT reality"





74%

of consumers would pay more for a smart device that had additional security

65%

of consumers wouldn't purchase a smart device from a brand that has experienced a security breach

93%

of consumers believe that manufacturers need to do more to secure smart devices



97%

of enterprises call out security as a concern when adopting IoT

22%

enterprise customers are willing to pay 22% more for IoT cybersecurity

70%

and they would buy 70% more devices if security concerns were mitigated



Governments taking action

USA

- State legislation passed (CA, OR, NY, IL, MD)
- Several bills introduced to Congress
- NIST mandated to define multiple baselines

Europe/UK

- Security certifications under the EU Cybersecurity Act
- UK Code of Conduct informed ETSI Standard
- UK testing different consumer labels

APAC

- Singapore aims to define security guidelines
- Japanese campaign to hack consumer devices

Cybercrime is big business for bad actors



Nation-states



Organized criminal groups



Corporate competitors



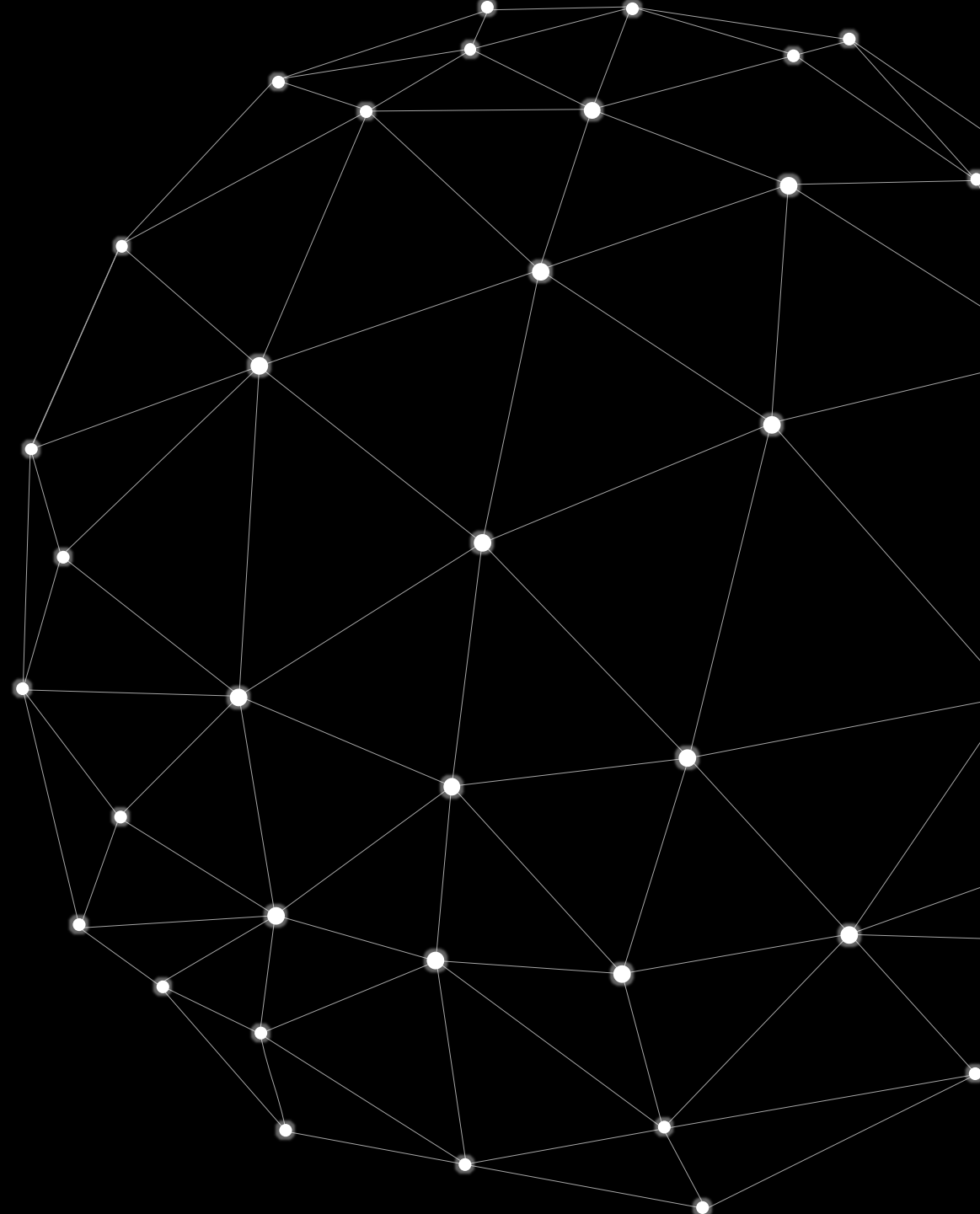
Opportunists



Hacktivists



Company insiders



A look at device-level attack surfaces

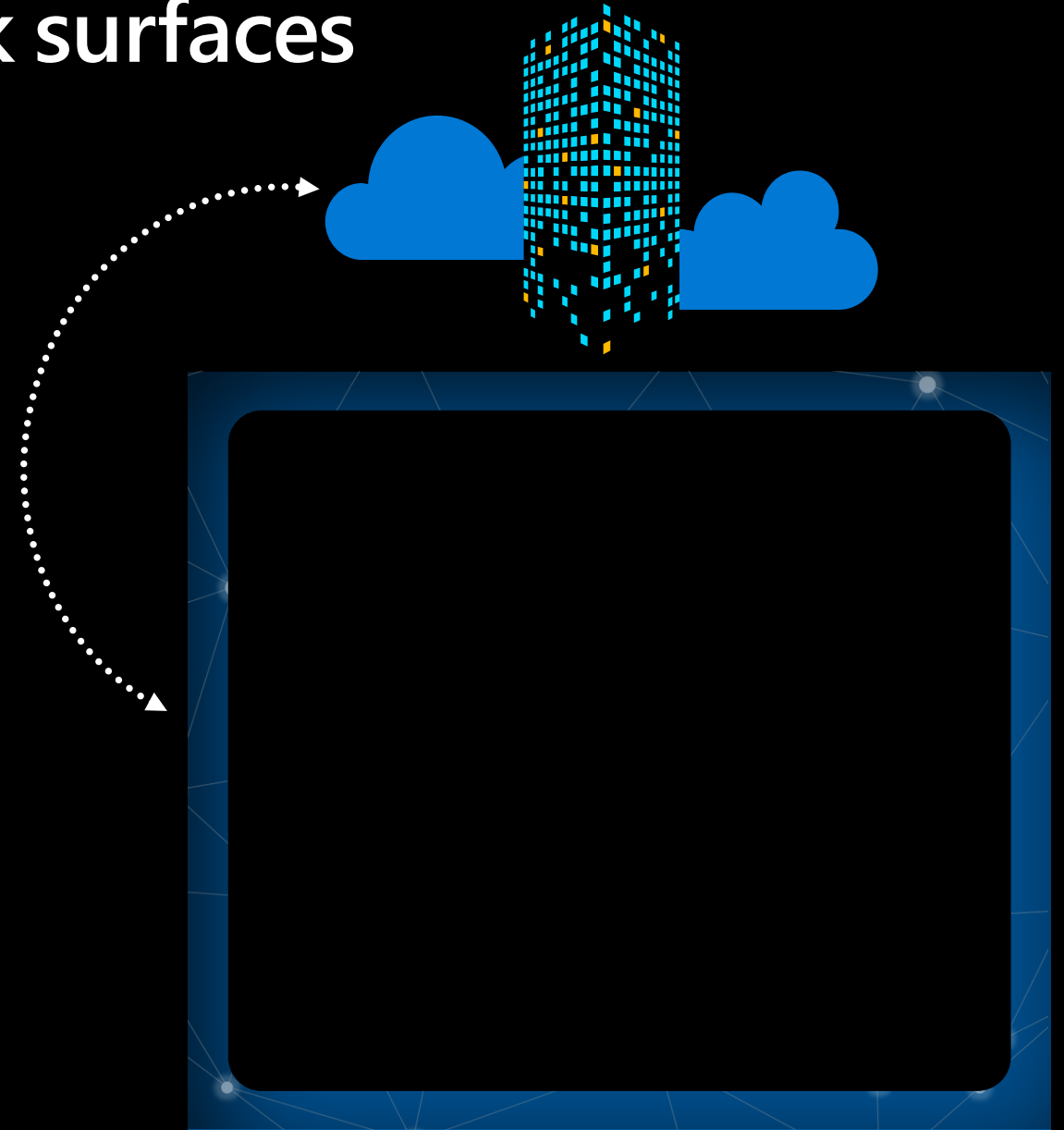
Applications

Network communications

Network stack

OS/Platform

Hardware



IoT attacks put businesses at risk



Devices bricked or
held for ransom



Devices are used for
malicious purposes



Data &
IP theft



Data polluted &
compromised



Devices used to
attack networks

IoT attacks put businesses at risk



Devices bricked or held for ransom



Devices are used for malicious purposes



Data & IP theft



Data polluted & compromised



Devices used to attack networks



The cost of IoT Attacks

Stolen IP & other highly valuable data

Compromised regulatory status or certifications

Brand impact (loss of trust)

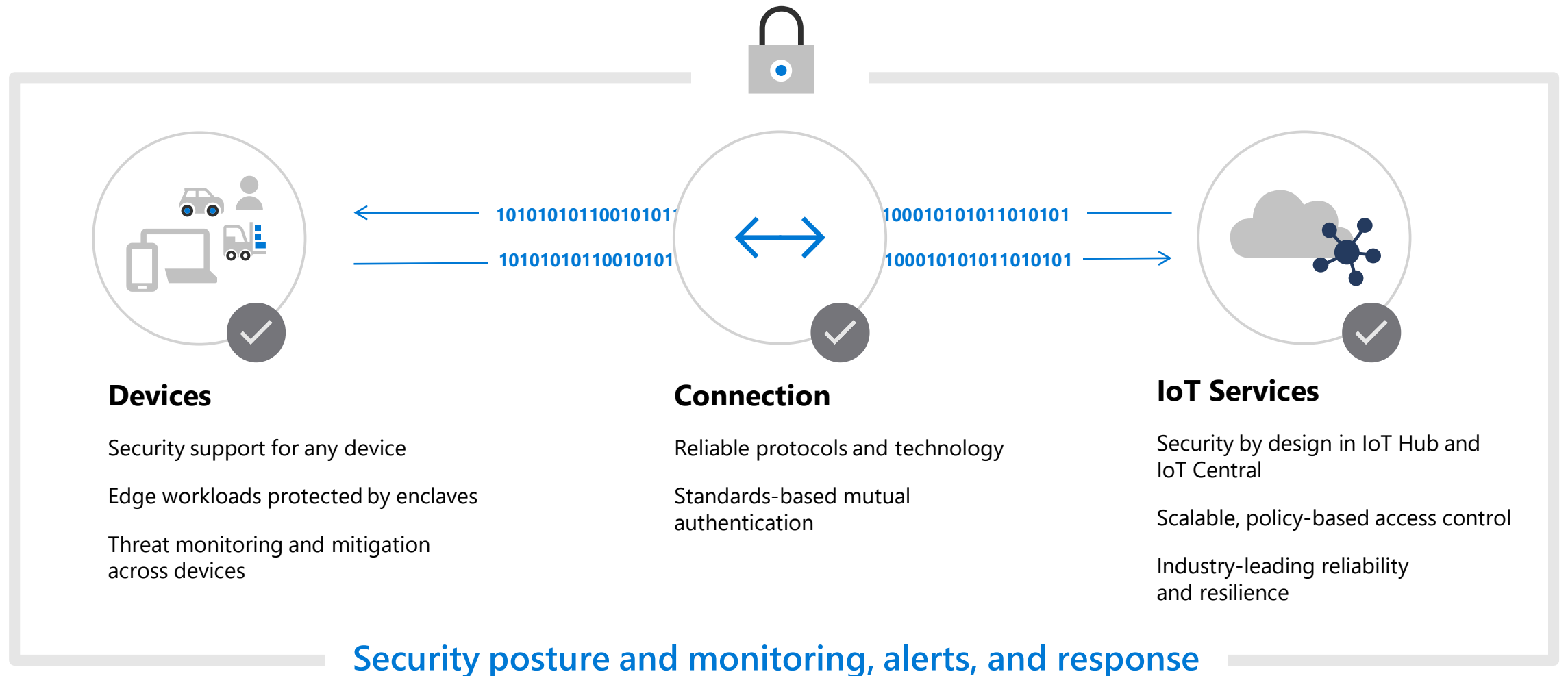
Recovery costs


Financial and legal responsibility

Downtime

Security forensics

The IoT security landscape: protect all your IoT assets





This is your security team.

The image shows a large, modern security operations center. In the foreground, several analysts are seated at long desks, each with multiple computer monitors displaying various data feeds and security software. The analysts are seen from behind, focused on their work. In the background, a large wall of screens displays complex data visualizations, including world maps, network diagrams, and charts. Two analysts are standing near the center of the background wall, looking at a large screen that shows a globe with red highlights. The room is dimly lit, with the primary light sources being the screens and overhead industrial-style lighting fixtures. The overall atmosphere is one of high-tech, professional security monitoring.



Azure Sphere overview

Giovanni Gatto
Azure Sphere Specialist, Microsoft

IoT in Action



Microsoft and partner expertise to protect the specifics of your solution



IoT security cutting edge

From the Seven Properties to the Security Maturity Model, we develop or contribute to the ideas driving IoT security



Decades of industry experience

Microsoft has protected endpoints and data for decades, and we analyze billions of threat signals today



Insight into coming standards and regulations

Our advocacy work with governments and standards bodies means you won't be surprised by new regulation



Powerful partner ecosystem

IoT partners are ready and informed with the content they need to build secure IoT for your industry

Highly-secured connected devices require 7 properties



Hardware Root of Trust



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



Small Trusted Computing Base



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



Defense in Depth



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



Dynamic Compartments



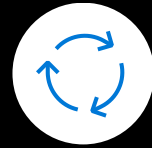
Can your device's security protections improve after deployment?



Certificate-Based Authentication



Does your device use certificates instead of passwords for authentication?



Renewable Security



Does your device's software update automatically?



Failure Reporting



Does your device report back about failures and anomalies?



= Silicon support required



= OS support required



= Cloud Service support required

Some properties depend only on hardware support



Hardware
Root of Trust

Hardware Root of Trust

Unforgeable cryptographic keys generated and protected by hardware

- Hardware to protect **Device Identity**
- Hardware to **Secure Boot**
- Hardware to attest **System Integrity**

Some properties depend on hardware and software



Defense in
Depth



Dynamic
Compartments



Small Trusted
Computing Base



Dynamic Compartments

Internal barriers limit the reach of any single failure

- Hardware to Create Barriers
- Software to Create Compartments

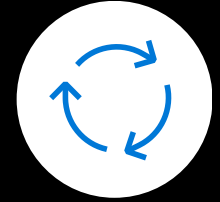
Some properties depend
on hardware, software
and cloud



Certificate-Based
Authentication



Failure
Reporting



Renewable
Security

Renewable Security

Device security renewed to overcome
evolving threats

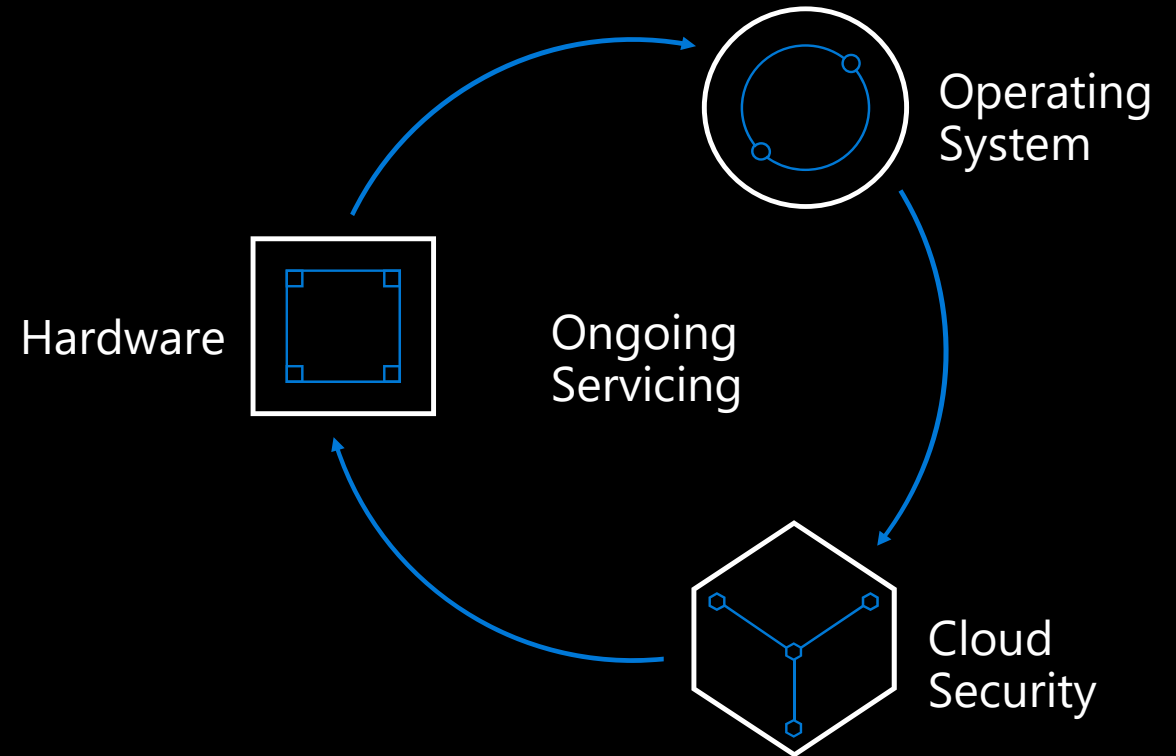
- Cloud to **Provide Updates**
- Software to **Apply Updates**
- Hardware to **Prevent Rollbacks**



Azure Sphere

An end-to-end solution for securely connecting existing equipment and to create new IoT devices with built-in security. Put the power of Microsoft's expertise to work for you everyday.

- Azure Sphere certified chips
- The Azure Sphere Operating System
- The Azure Sphere Security Service
- Azure Sphere Ongoing Servicing



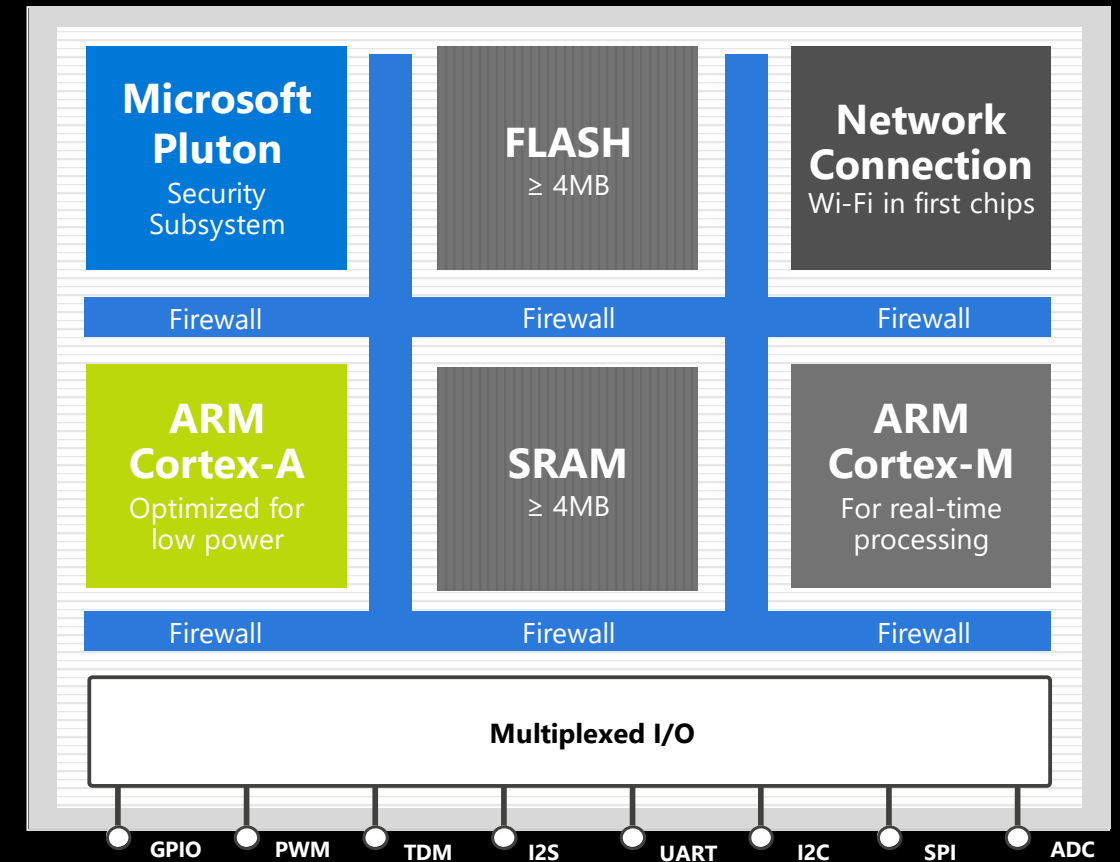
Over 10 years of security and OS updates delivered directly to each device by Microsoft

Azure Sphere certified MCUs create a secured root of trust for connected, intelligent edge devices

Connected with built-in networking

Secured with built-in Microsoft silicon security technology including the Pluton Security Subsystem

Crossover real-time and application processing power brought to MCUs for the first time

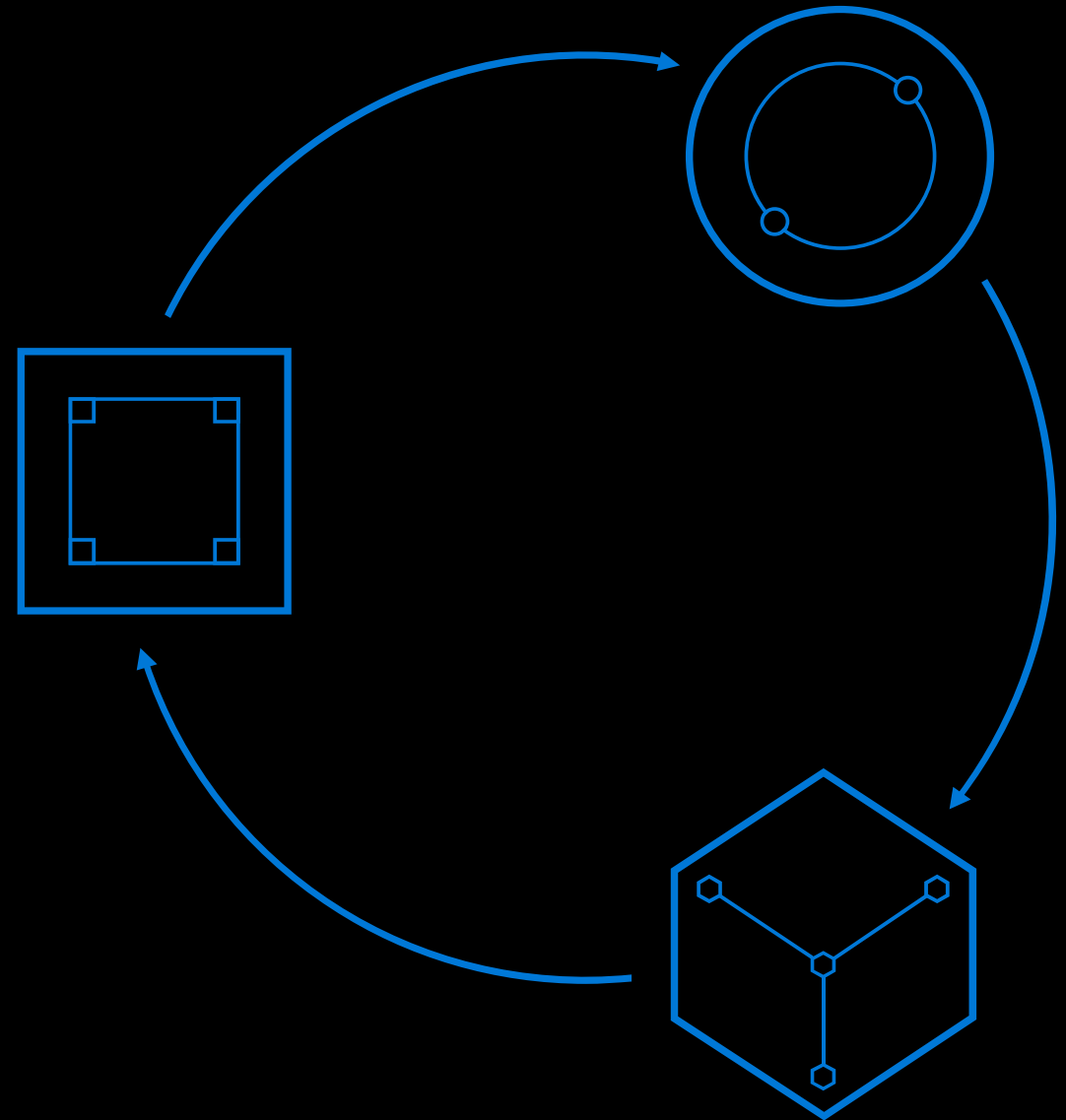


**Three components.
One low price.
No subscription fees.**

An Azure Sphere certified MCU

The Azure Sphere OS
with ongoing on-device OS updates

The Azure Sphere Security Service
with ongoing on-device security updates





Security at the Edge

Nicolas Vasseur
Technical Specialist, Microsoft

IoT in Action



Windows for IoT

Windows for IoT has the features and manageability you expect from Windows 10

Built-in Windows 10 security that's always up-to-date and supported for 10 years with security patches

Protects your IoT solutions from device to cloud with the latest security advances in Windows 10

A team of security and privacy experts focused on the platform

Windows 10 IoT Core & Services

For small-footprint, smart devices
Enabling lower cost devices

Windows 10 IoT Enterprise

For fixed-function, smart devices
Locked down, full edition of Windows 10

Windows Server IoT 2019

For the most demanding edge
computing workloads

Built on the foundation of 900M active Windows 10 devices

Security offerings

- *Proven security technology across a wide range platforms from Server, Desktop, Gaming to IoT.*
- *IoT security benefits from analytics and mitigations of threats across millions of devices.*

	Device Platform	Service offerings
Windows 10 IoT Core	<p>Security is built-in to Windows</p> <ul style="list-style-type: none">• Secure applications through UWP• Health attention and provisioning• Data protection at rest volume encryption and HW supported key storage (BitLocker, TPM)	<p>Windows 10 IoT Core Services</p> <ul style="list-style-type: none">• 10y LTSC support• Device Health Attention• Manage updates via DUC (Device Updated center)• Azure Security Center
Windows 10 IoT Enterprise	<ul style="list-style-type: none">• Secure execution: Device Guard, Secure Boot• Threat mitigation Device update and management• Turn-key security and manufacturing tools	<p>Windows 10 Enterprise license</p> <ul style="list-style-type: none">• 10y LTSC support• Servicing via Windows Update• Advanced Thread Protection (ATP)

How Windows 10 IoT addresses the 7 properties of security for devices



Hardware Root of Trust



Supports strong device identities through HSM like TPM



Small Trusted Computing Base



Utilize TrustZone for critical processing such as fTPM (enclave??)



Defense in Depth



Various levels of defense in depth including: Device Guard, UWP Appx, containerization, etc.?



Dynamic Compartments



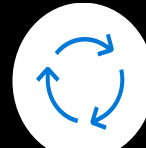
UWP apps run in their own contexts; Windows is built in a compartmentalized way



Certificate-Based Authentication



Certificate or key protected code execution through Device Guard.
Certificate or key cloud authentication leveraging hardware HSM



Renewable Security



Proven and scalable update infrastructure through Windows updated and Device Update Center.



Failure Reporting



Different level of failure reporting for HW, OS and apps are available via Watson through OEM portals



= Silicon support required



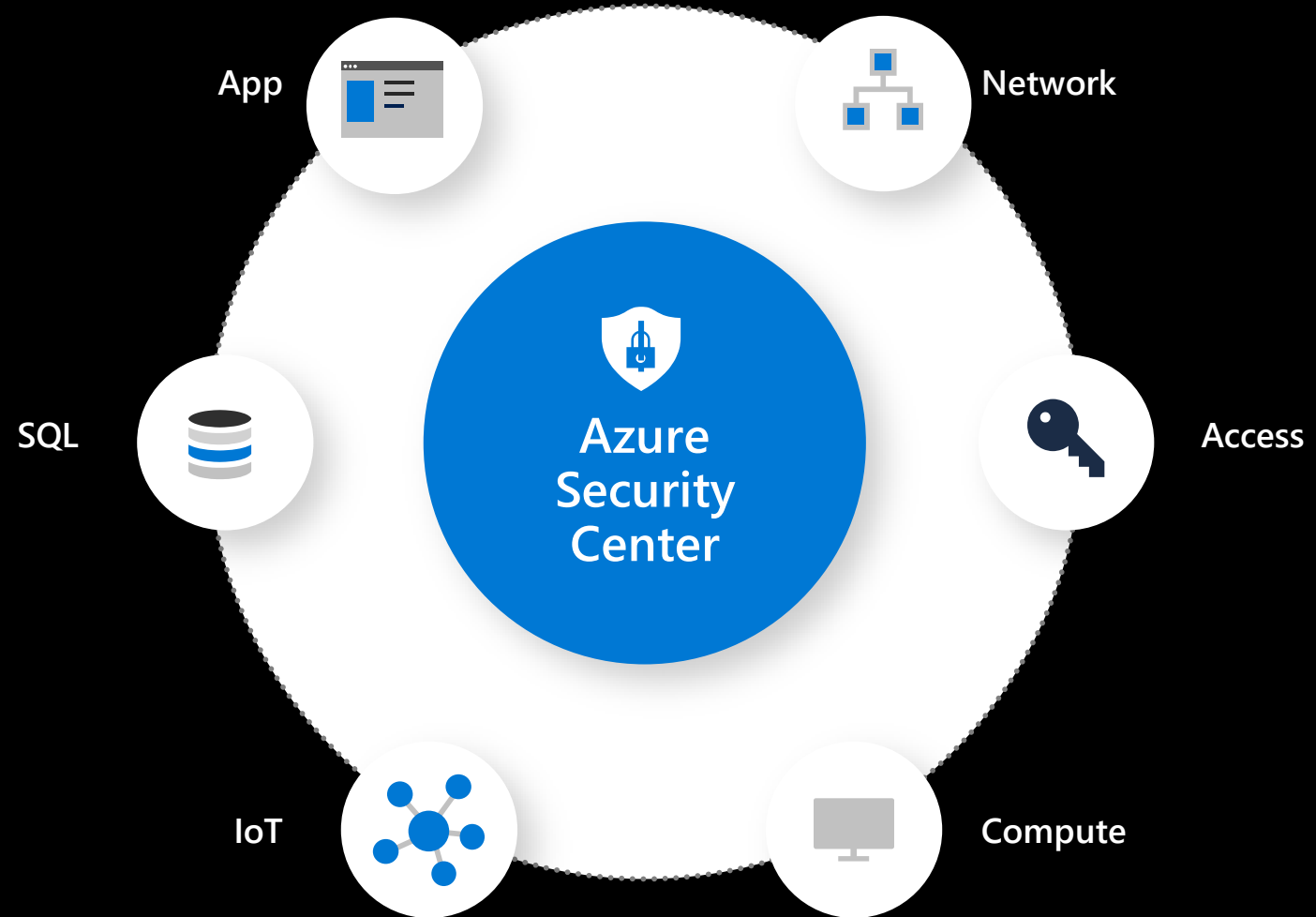
= OS support required



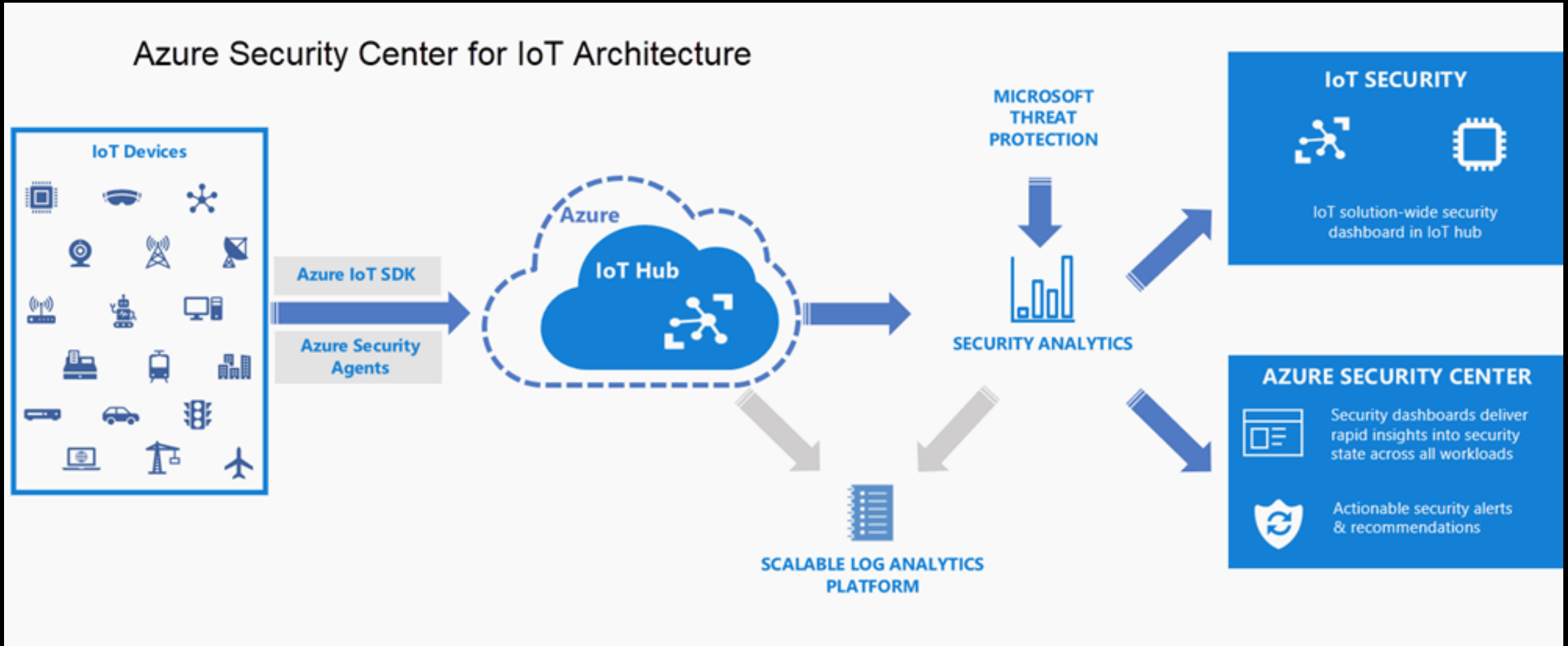
= Cloud Service support required

Azure Security Center

Azure Security Center provides threat protection and security posture management capabilities for your cross-cloud and IoT resources, including Microsoft and 3rd party devices. Azure Security Center is the first end-to-end IoT security service from a major cloud provider that enables organizations to prevent, detect, and help remediate potential attacks on all the different components that make up an IoT deployment.



Azure Security Center - Demo



The time is now

Talk to your Microsoft
representative **today**