



# Developing an IoT security practice for durable innovation

**Liam Jones**

Senior Technical Account Manager

**IoT** in Action

# Why Security?

- The Mirai Botnet (aka Dyn Attack)
- Hackable Cardiac Devices
- Baby Monitor Vulnerabilities
- Vehicle Hack



"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"

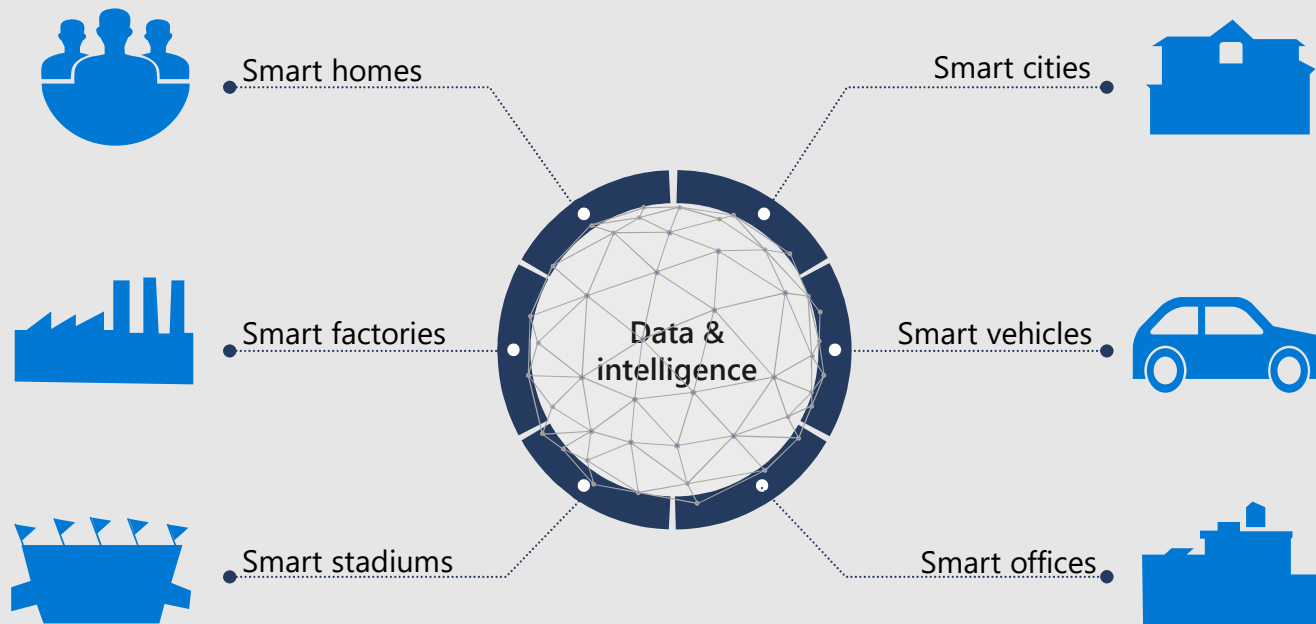
"The Lurking Danger of Medical Device Hackers"

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

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



# IoT is fueling digital transformation



20 billion connected devices by 2020

—Gartner



**80B**

Connected “things” by 2025  
generating 180ZB of data



**\$130B**

New monetization avenues  
due to IoT-related services



**80%**

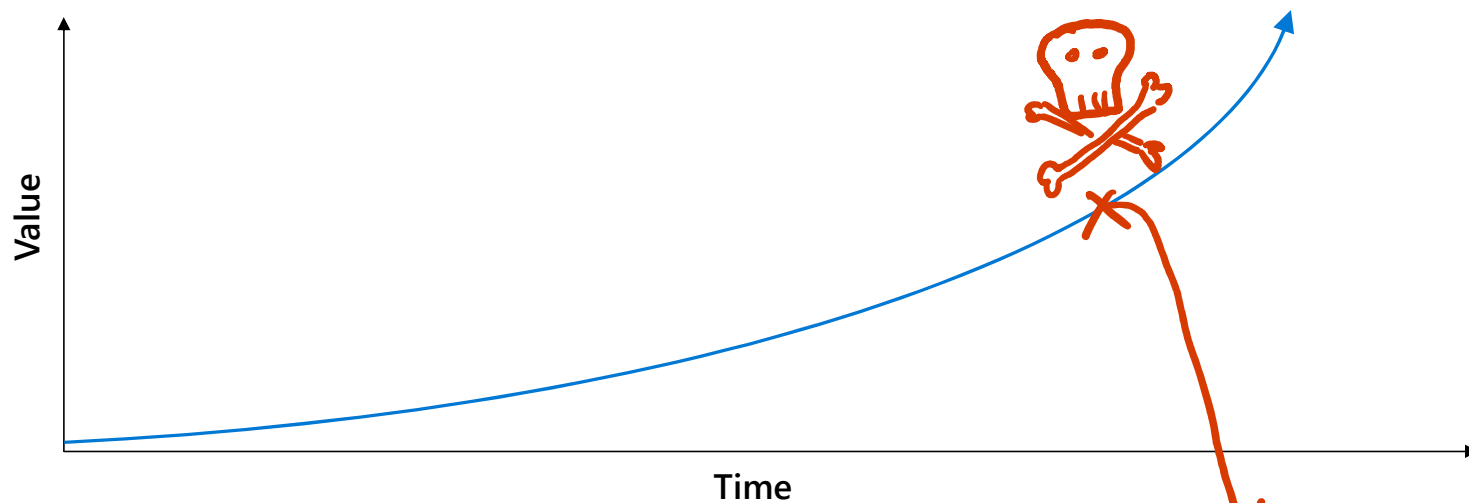
Companies that increased  
revenue as a result of IoT  
implementation



**\$100M**

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

# Planning your IoT deployment



**PoC stage**  
slow climb in value

**Production deployment**  
delivering real business value

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



**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

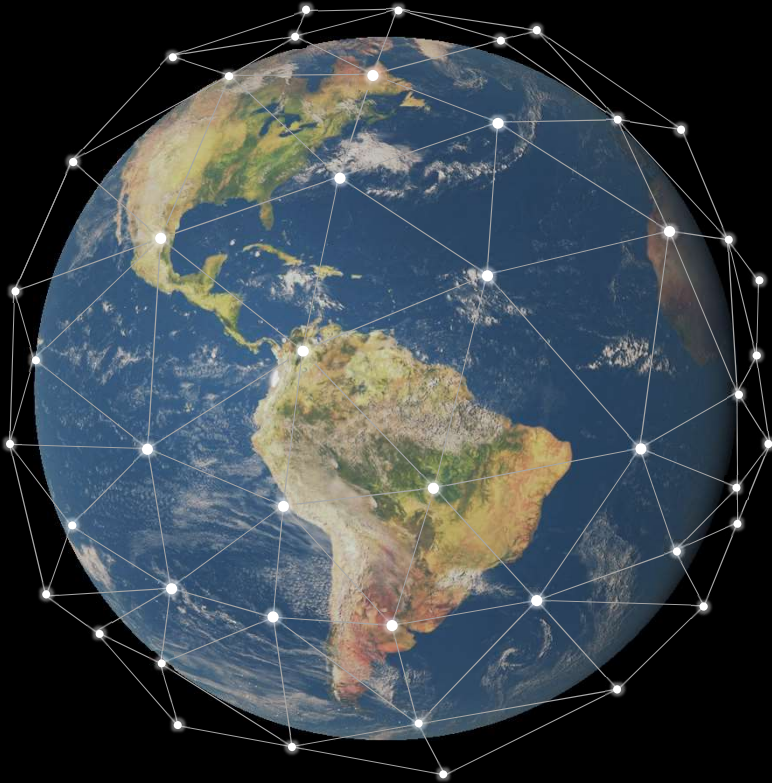
**22%**

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



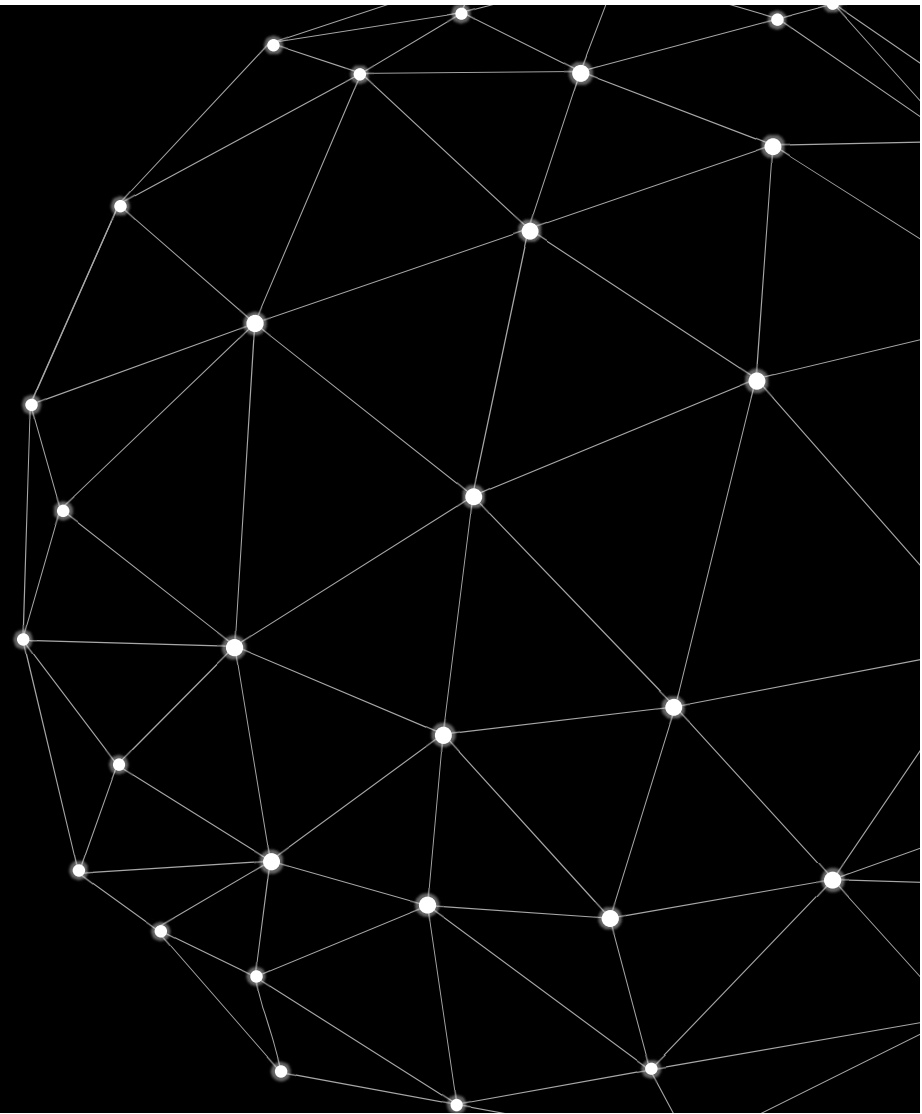
Opportunists



Hacktivists



Company insiders



# A look at device-level attack surfaces

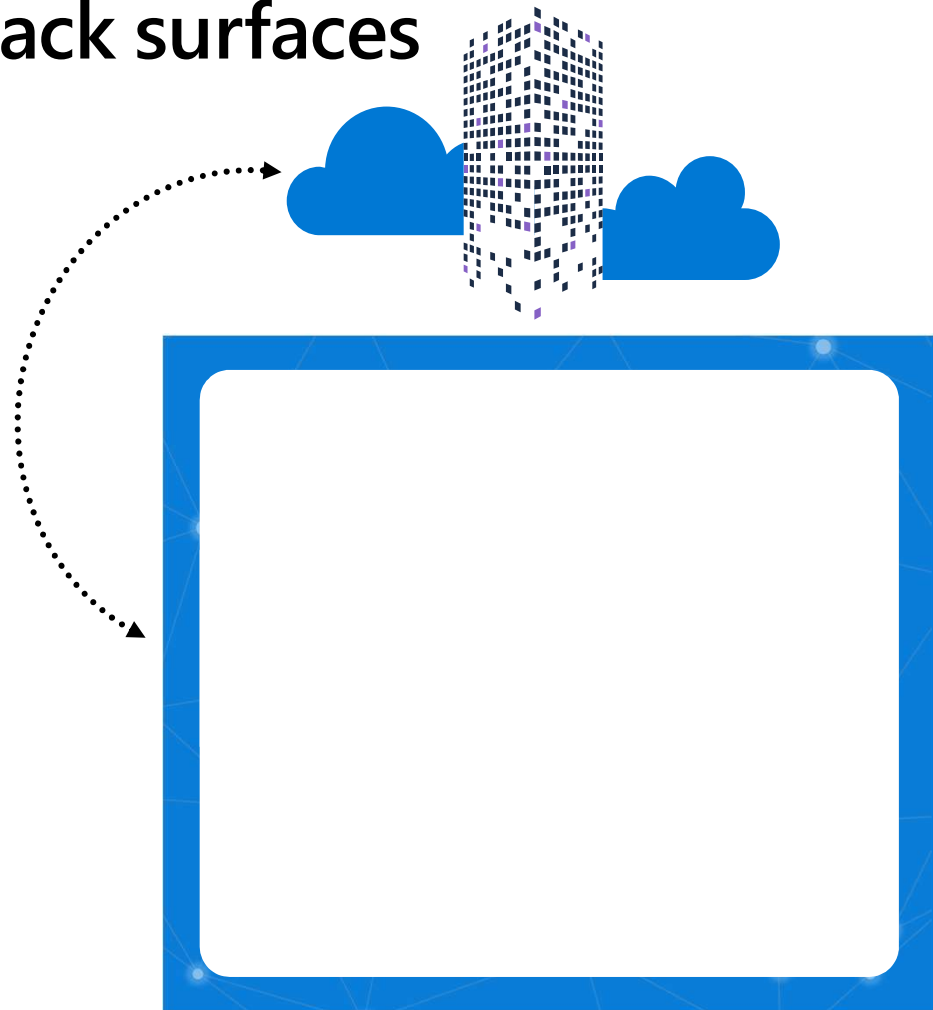
Applications

Network communications

Network stack

OS/Platform

Hardware



# IoT attacks put businesses at risk



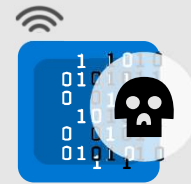
Devices bricked or held for ransom



Devices are used for malicious purposes



Data & IP theft



Data polluted & compromised



Devices used to attack networks

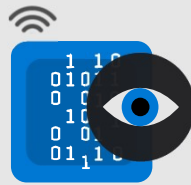
# IoT attacks put businesses at risk



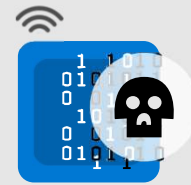
Devices bricked or held for ransom



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

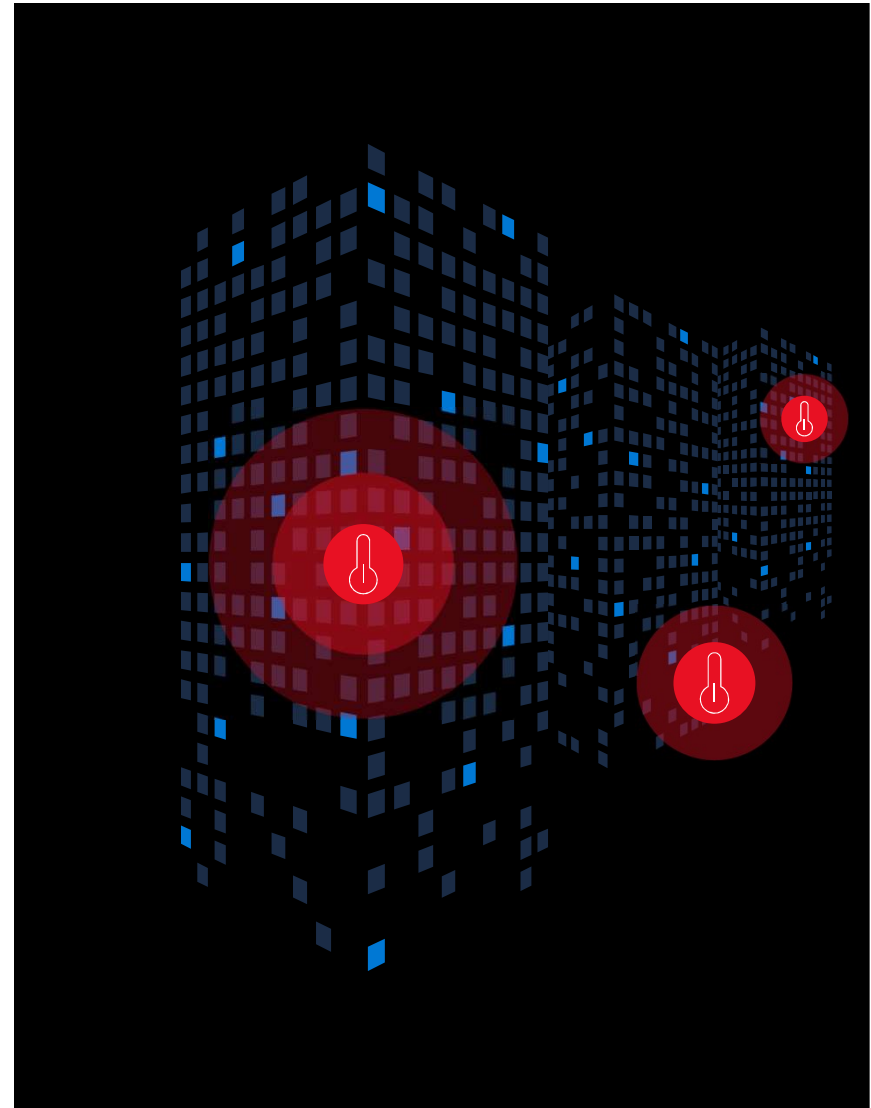


## Devices bricked or held for ransom

Your devices or mission critical equipment are rendered useless. The only possible recovery options require you to roll a truck or to pay ransom to your attacker.

### Assessing the risk:

- Would device/equipment downtime hurt revenue?
- Would there be out of pocket costs related to downtime?
- Does the device/equipment perform a critical task that people depend on for health and safety?





## Devices bricked or held for ransom

**Access to the HW and storage is typically the goal for attackers in attacks like this**

Methods of achieving this include malicious or unauthorized code execution that escalates privileges and gives them access to the deepest parts of the platform where they can modify the storage.





# Devices bricked or held for ransom

## Strategies and capabilities for mitigation

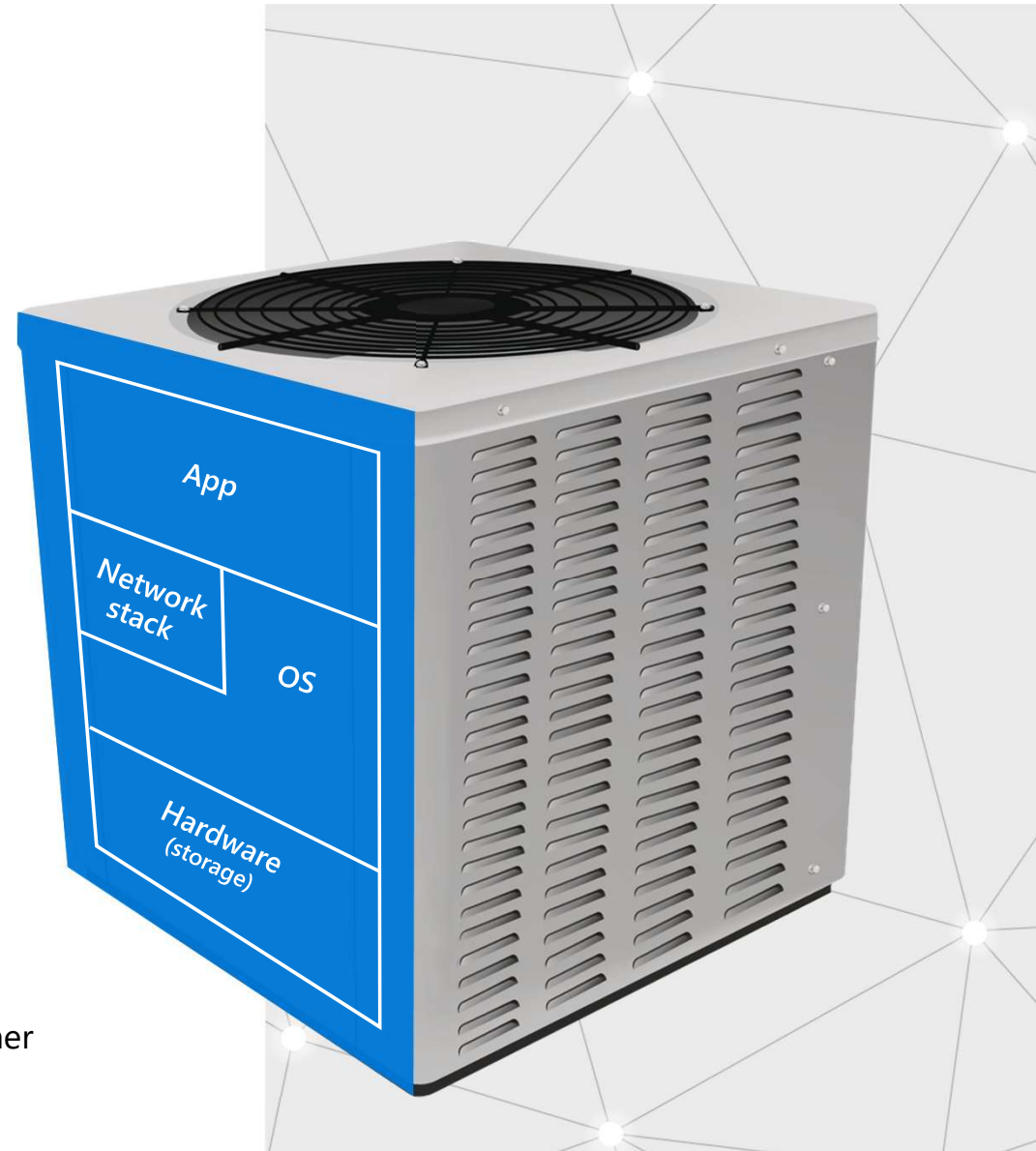
**Defense in depth;** multiple layers of defense that control access to storage

**Compartmentalization;** to limit access to various aspects of the OS

**Hardware barriers;** such as MMU to manage the flow of communication on the chip

**Over-the-air (OTA) updates;** to renew security on devices limiting the opportunity for success

**Best practice:** Vertically integrated system where all these capabilities interlock and comprehensively refreshed together





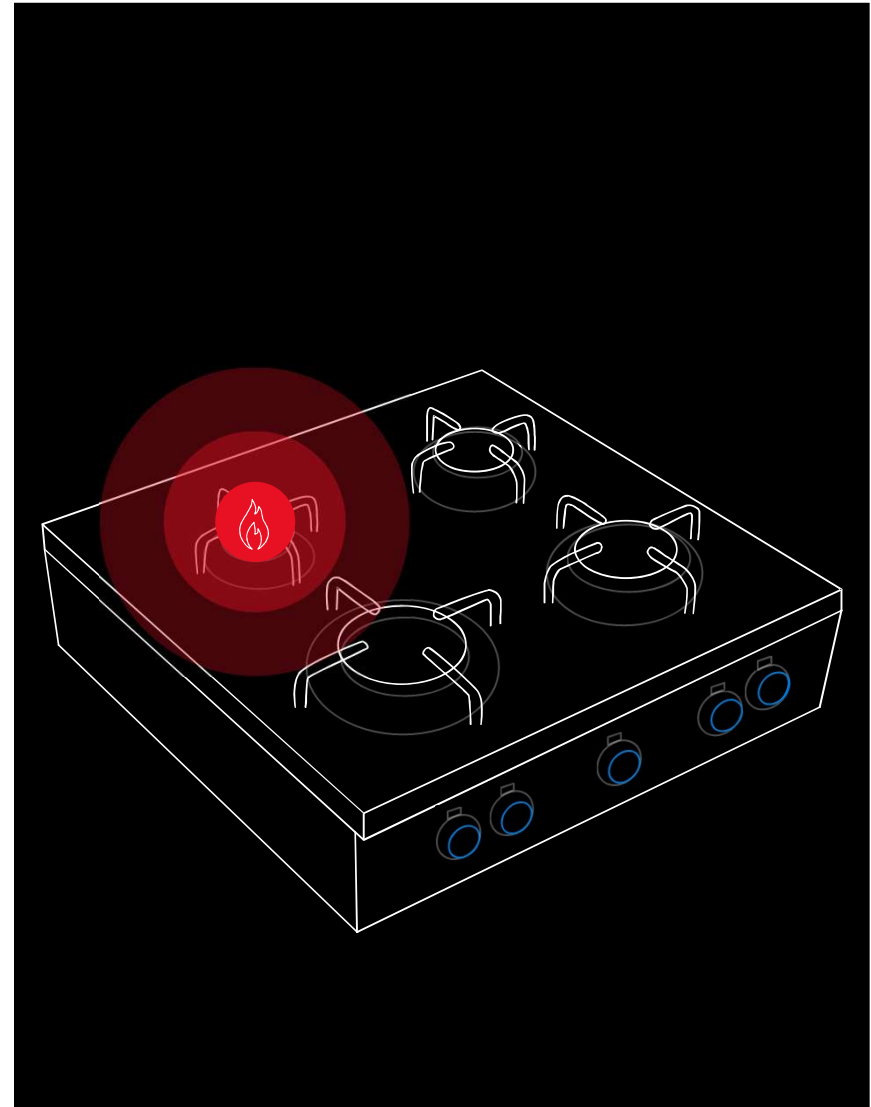


## Devices are used for malicious purposes

Your devices are used to do harm in the environments they operate in. This could lead to privacy breaches, physical damage and injury, brand degradation and legal liability

### Assessing the risk:

- Do your devices access heating elements, gas or water lines, or operate in a potentially dangerous context?
- Could your devices cause physical harm to the people that operate them?
- Can your devices cause a privacy breach in their environment?

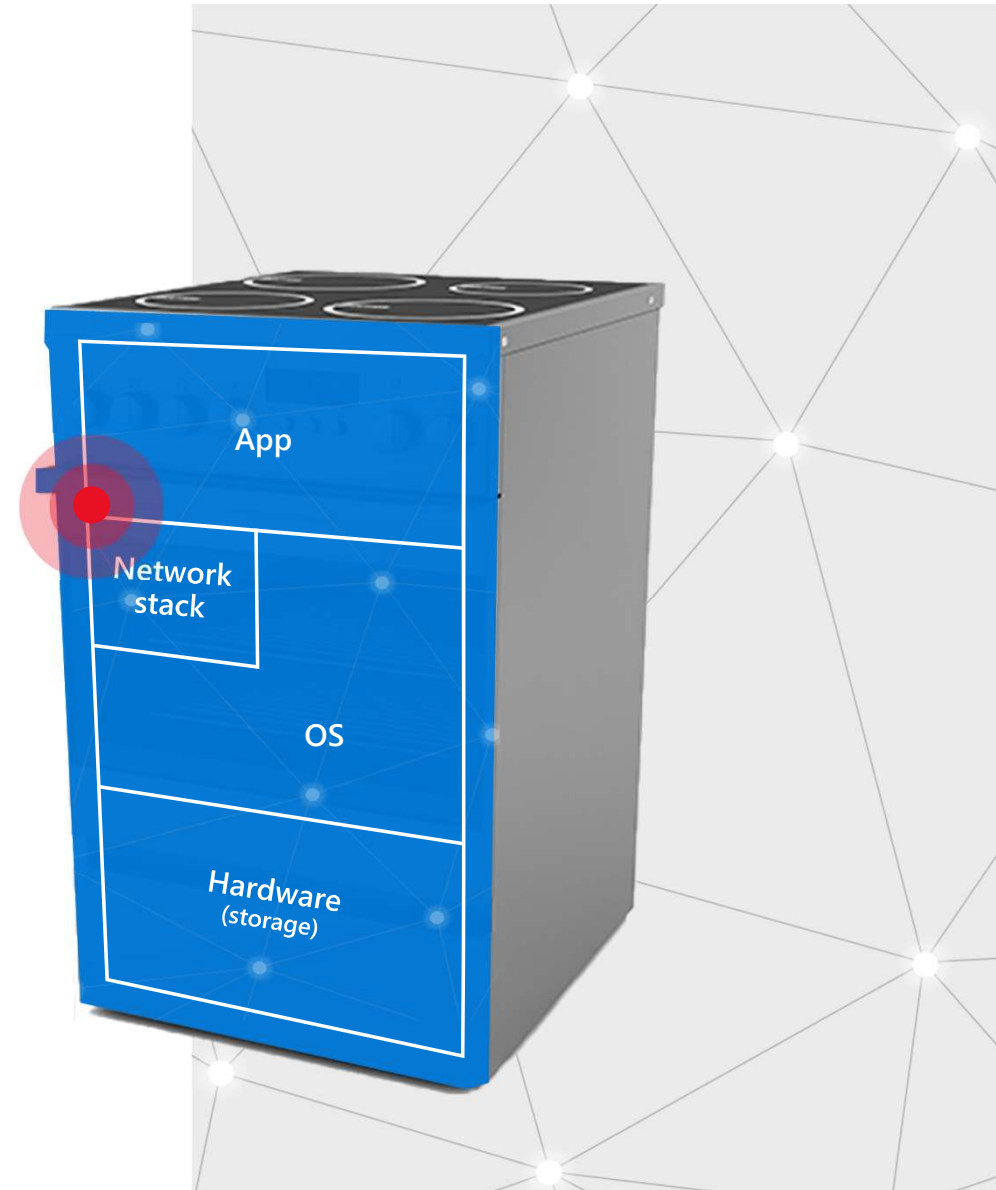




## Devices are used for malicious purposes

**Attackers trick your devices into doing something they weren't intended for**

Methods of achieving this include attack that imitate your command and control through network tampering. Attackers may also trick a device into running malicious code, giving them access to a device's physical controls.





# Devices are used for malicious purposes

## Strategies and capabilities for mitigation

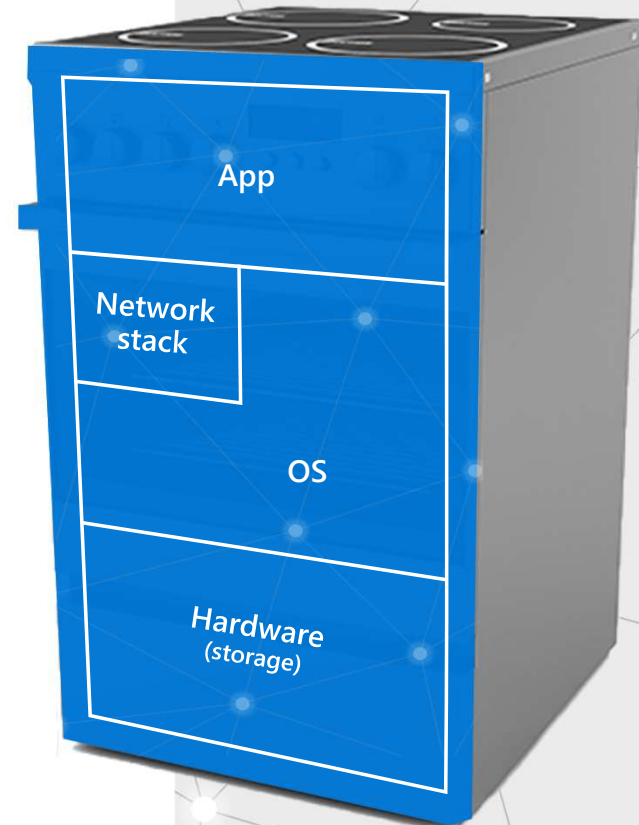
**Private/public key pairings** with trusted crypto and protocols; to ensure trusted communication

**Secure boot;** to ensure that devices only run authentic and current software

**App containers and privilege restrictions;** to limit access to physical controls

**Stack canaries** to defend against ROP attacks and some forms of overflows

**OS-based app manifest;** that defines what is appropriate and governs app behavior



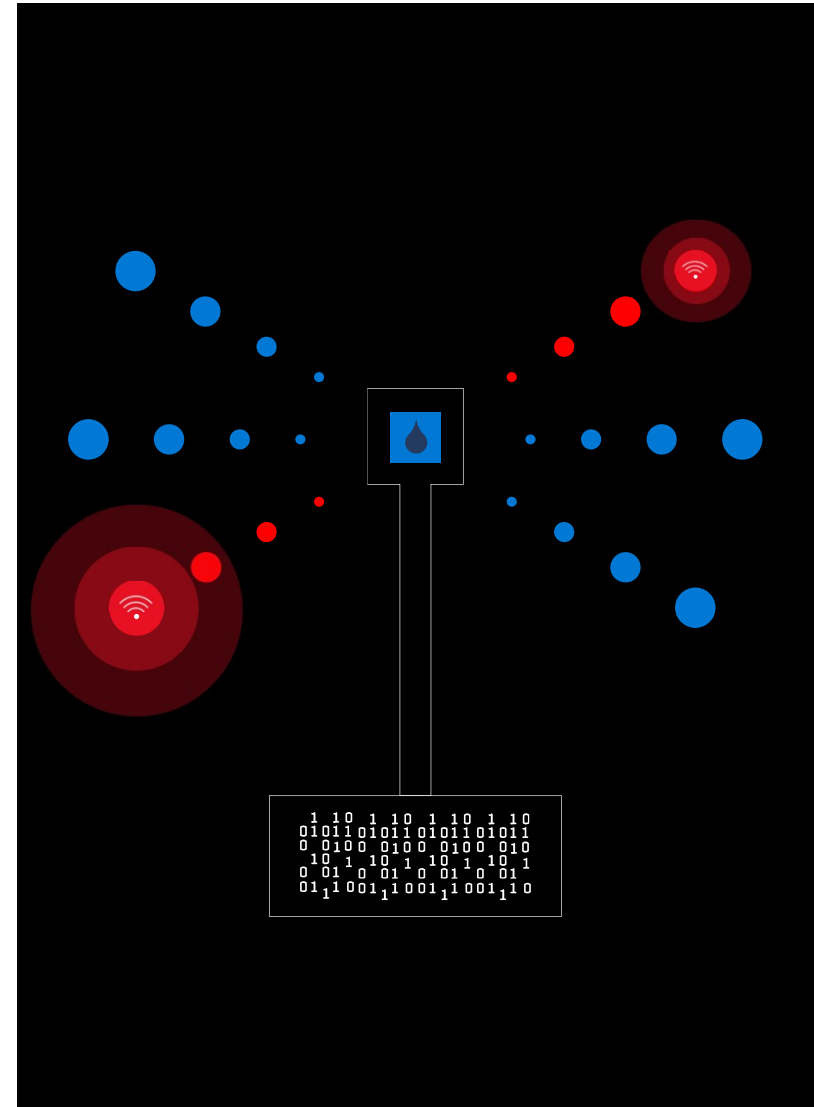


# Data pollution & compromised business insights

The data and insights coming from your devices can't be trusted. You may have no way of identifying the issue until something severe goes wrong.

## Assessing the risk:

- Are you using the data to make critical decisions about your business?
- Does the data from your devices inform machine learning (ML) or artificial intelligence (AI) models?
- Are you generating revenue or billing customers based on the data coming from your devices?





## Data pollution and compromised business insights

**Attackers manipulate data or impersonate your devices with a counterfeit/stolen identity**

Methods of achieving this include man-in-the-middle type attacks where outbound data/packets are manipulated. Devices may also be impersonated by exploiting identity weakness including shared passwords and keys and certificates that are not protected properly.





# Data pollution and compromised business insights

## Strategies and capabilities for mitigation

**A unique unforgeable identity** in the silicon

**Mutual authentication;** ensures the server and client are authenticated.

**Attestation;** to ensure only authentic devices, running trusted software, connect to your service

**Signed, encrypted communications;** to ensure data and packets in motion are not compromised

**Best Practice:** private keys generated by device in a secured environment and stored in a key vault that is only accessible by the HW root of trust.





This is your security team.

The image shows a large, dimly lit room filled with people working at computer terminals. In the background, three large screens display various data visualizations, including a world map and a network diagram. The text "This is your security team." is overlaid in the center of the image.



# 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

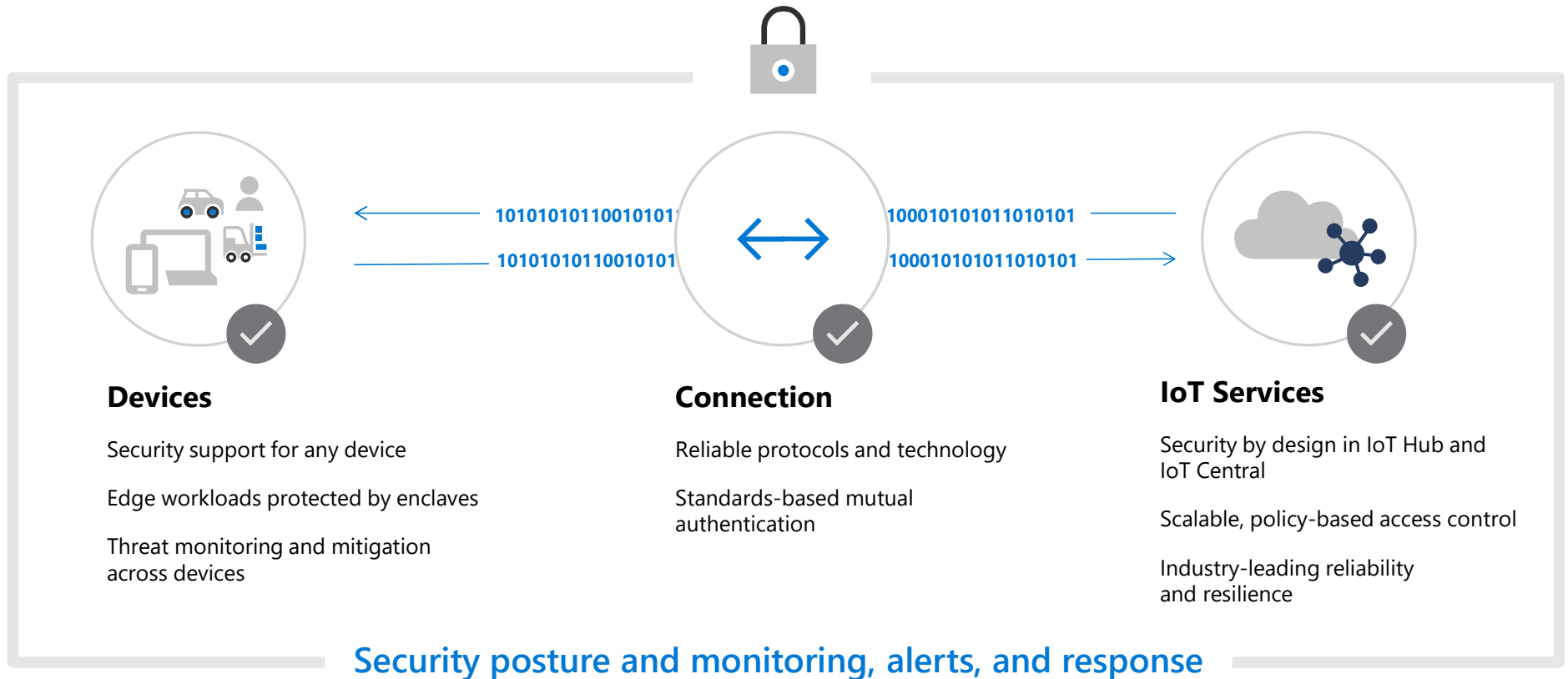
Our advocacy work with governments and standards bodies means you won't be surprised by new regulation



## Powerful partner ecosystem

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

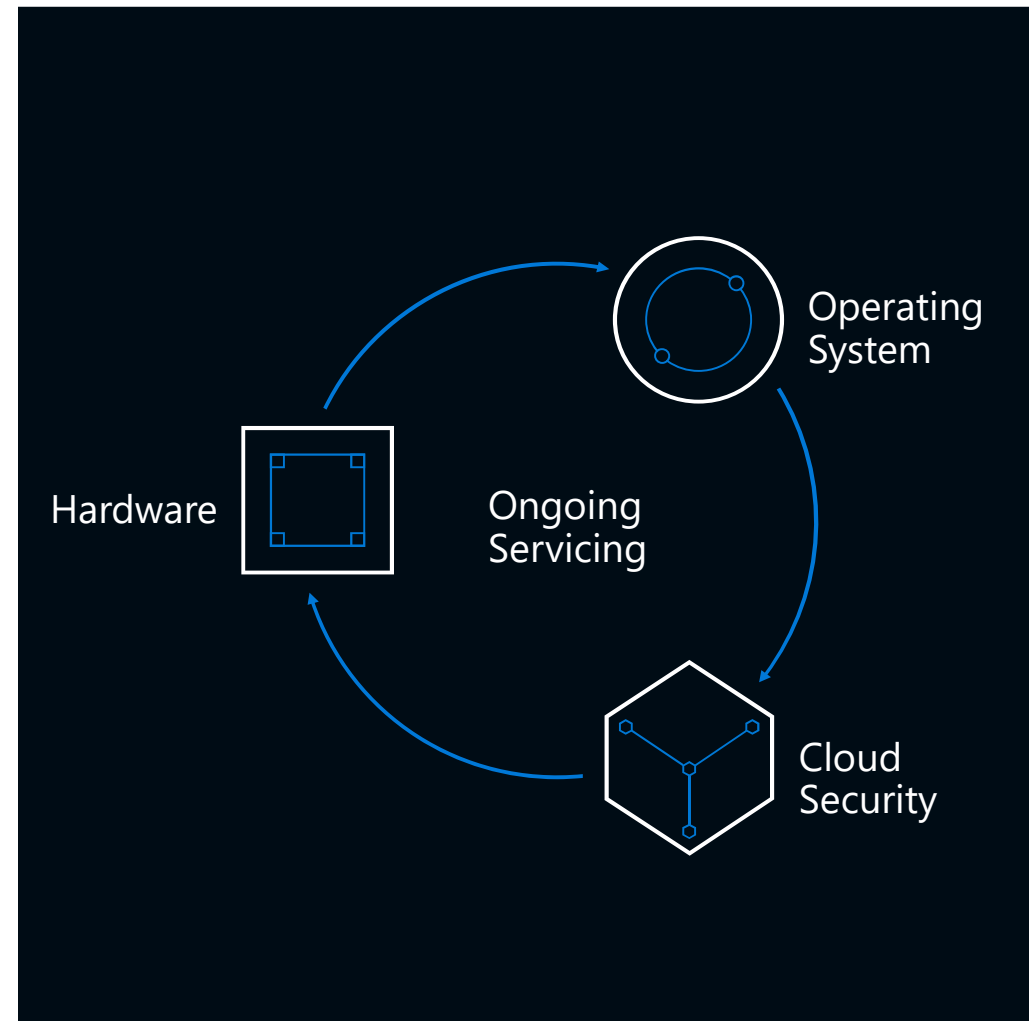
# The IoT security landscape: protect all your IoT assets



# 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

# 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

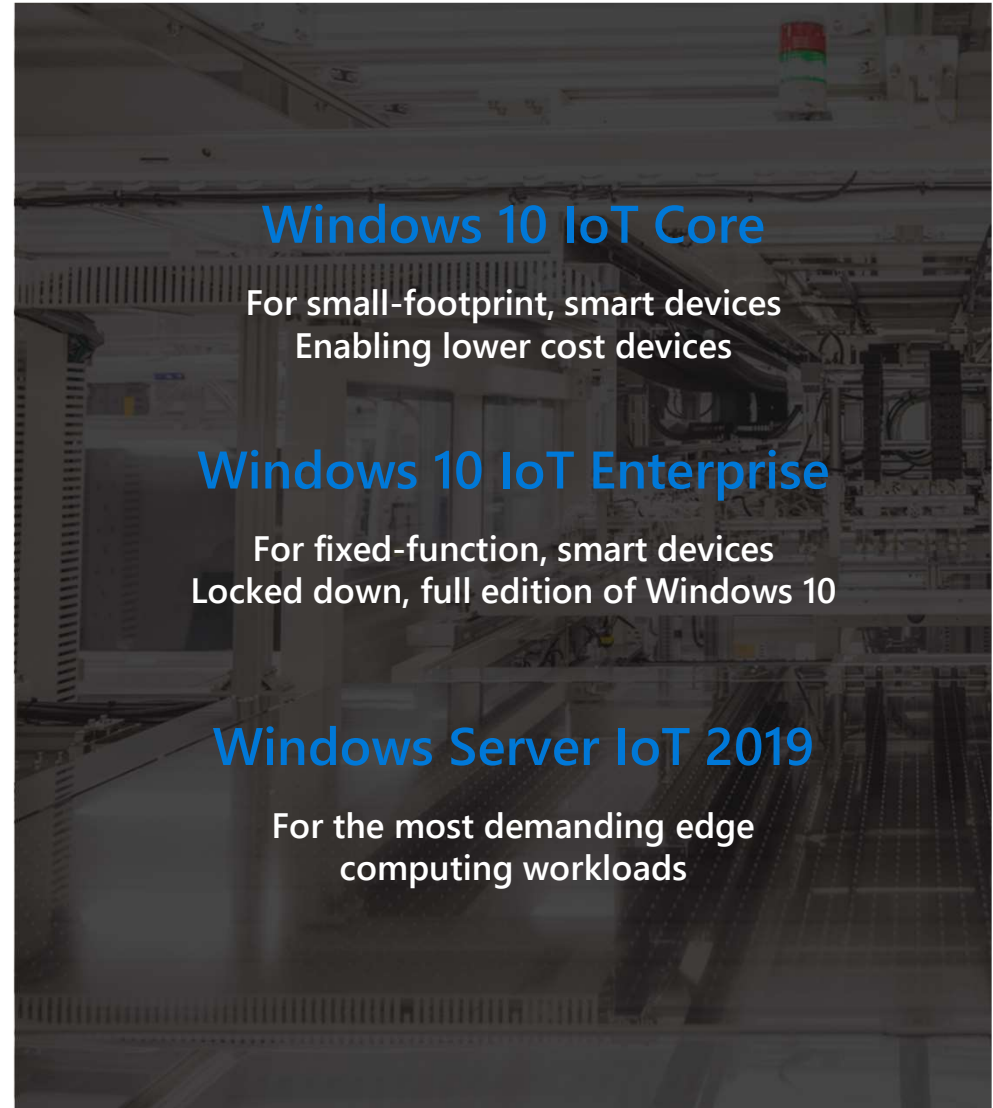
For small-footprint, smart devices  
Enabling lower cost devices

## Windows 10 IoT Enterprise

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

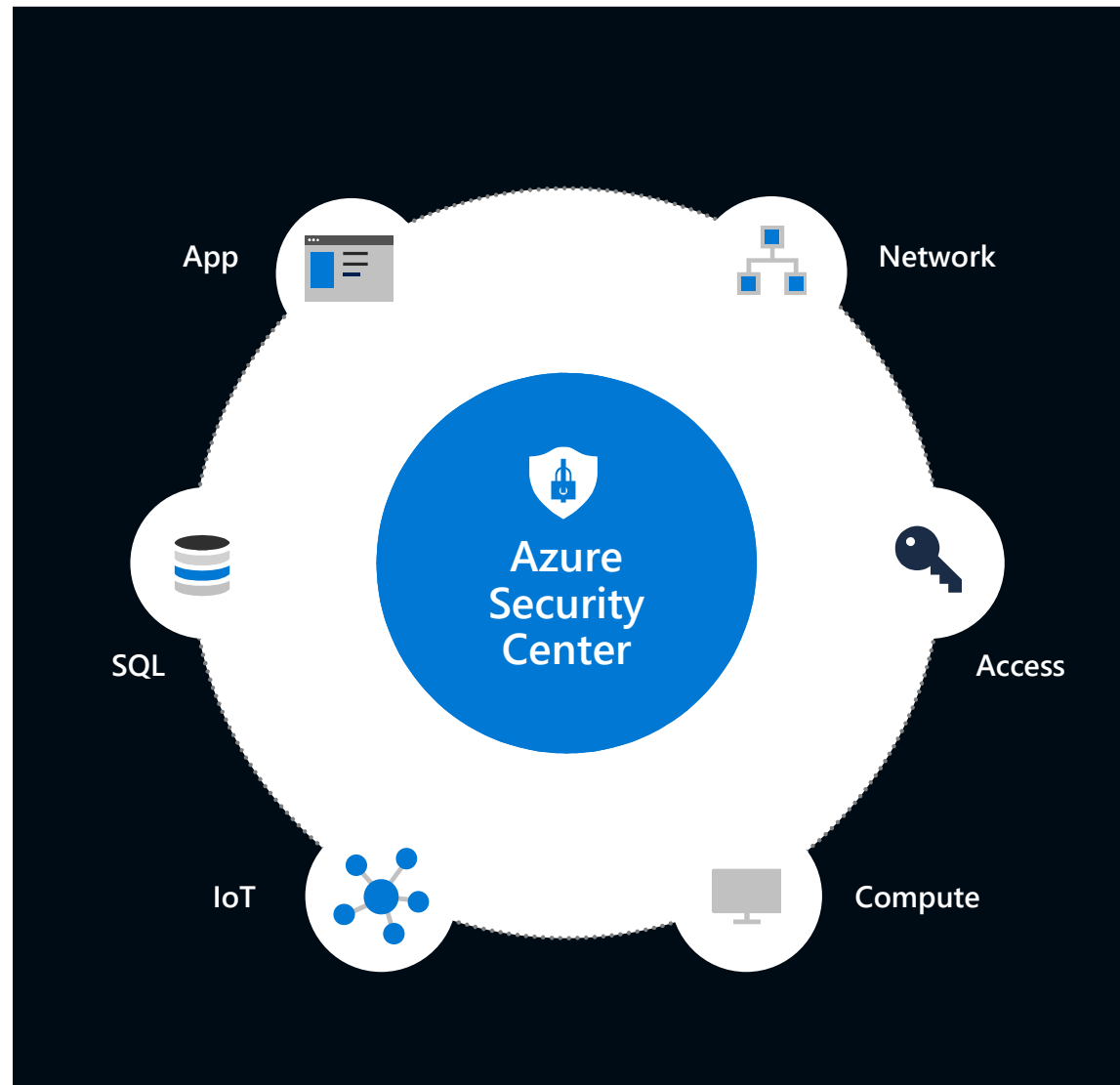
## Windows Server IoT 2019

For the most demanding edge  
computing workloads



# 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.



The time is now





# Call to action



## Partner

---

Sign up as a Microsoft Partner

Reach out to a Solution Aggregator

Promote your solution on Marketplace

Reach out to Cloud Enablement Desk  
to start your journey with Microsoft



## Customer

---

Visit Marketplace to get exposure  
to Azure based IoT cloud solutions

Leverage your Microsoft account  
managers for prioritized solutions



IoT Continuum  
IoT Community  
IoT Chasm

---

Survey  
Solution Showcase & Reception

---

Thank you



Thank you!