Microsoft Azure

# Azure IoT

## Rethinking IoT Security with Azure Sphere

TAN Chee Weng
Sr IoT Solution Architect
Microsoft

# Data & device security is a top IoT customer priority

**100%** increase in IoT infections during 2020

**33%** of all infections observed in mobile and Wi-Fi networks are from IoT devices – up from 16.17 percent in 2019

IoT security breaches can have significant impact on an organization's bottom line:

## Operational & revenue impact

IoT devices can be operationally degraded, used for lateral movement, or forced offline by a security incident

## Customer impact

Incidents can degrade customer experience and influence brand reputation

## Real-world impact

Compromised security can lead to real-world effects, including potential safety & environmental incidents

## Regulation impact

Non-compliance may impact organizational ability to conform to government and industry regulations

## Cost impact

Security solutions to mitigate IoT business risks must be cost-effective in a low-margin industry with low-cost IoT devices

Source: https://threatpost.com/iot-device-takeovers-surge/160504/

“COVID-19 pandemic ratchets up threats to medical IoT”

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

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

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

“Hacking critical infrastructure via a vending machine? The IOT reality”

“Security experts warn of dangers of connected home devices”

“The IoT ransomware threat is more serious than you think”

“ Webcam firm recalls hackable devices after mighty Mirai botnet attack”

“Weaponization of IoT surges as threat actors leverage COVID-19”

“Cyberattacks have become increasingly sophisticated and dangerous.”

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

“The Lurking Danger of Medical Device Hackers”

“Hackers exploit casino’s smart thermometer to steal database info ”

# Differences between IT & OT security

## IT Security

Data confidentiality & privacy

Standard protocols & devices

High levels of connectivity

Multiple layers of controls & telemetry

## OT Security

Safety & availability

Specialized protocols, devices & legacy OS platforms

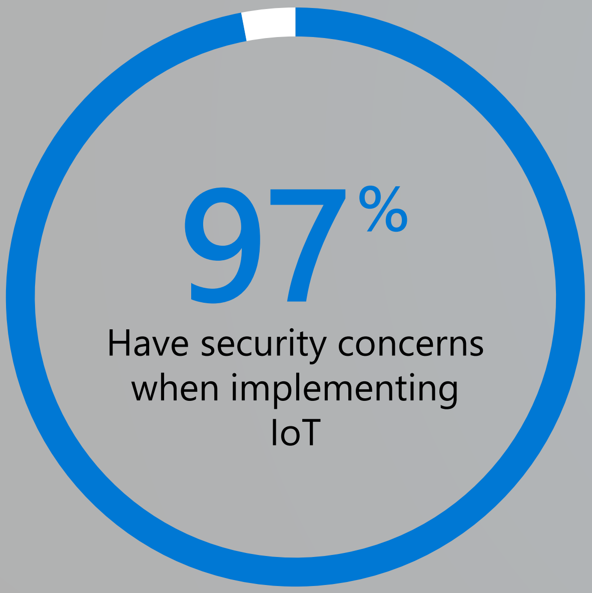
Traditionally air-gapped

Little or no visibility into IoT/OT risk

# While security is a low hinderance to IoT adoption, it is a consideration during implementation, with data privacy top of mind for about half of all organizations

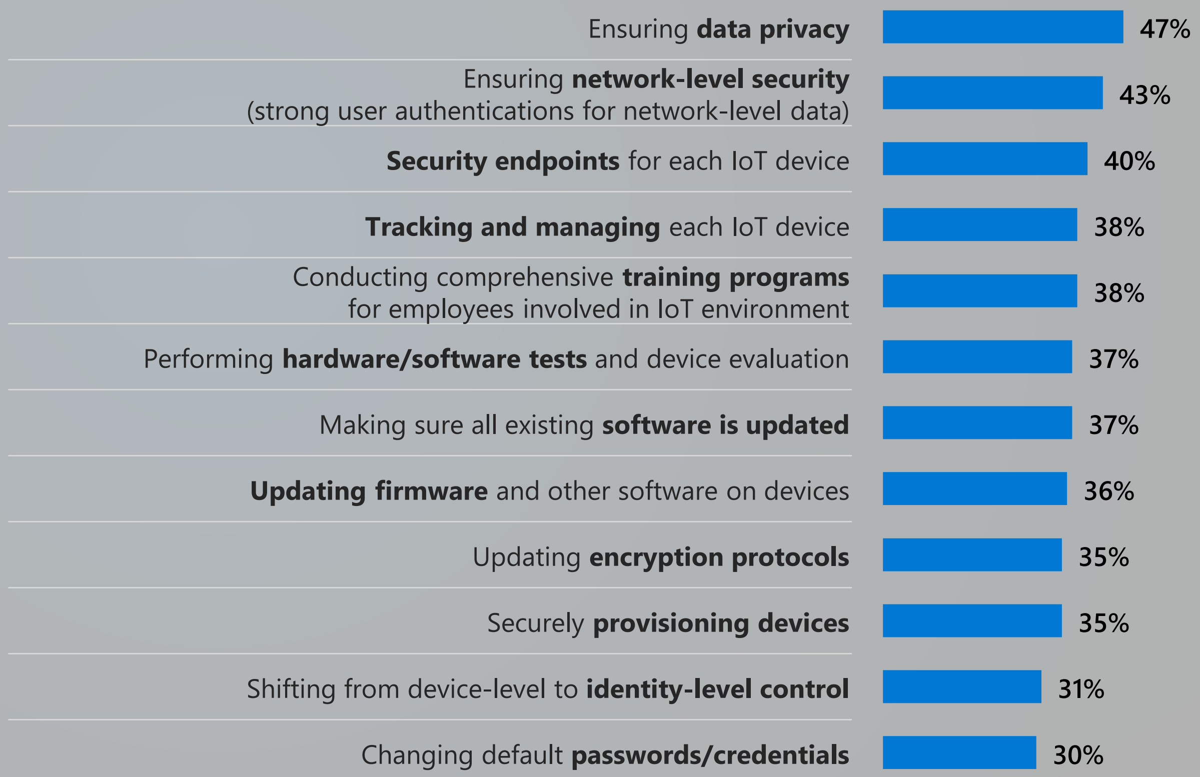
## IoT SECURITY CONSIDERATIONS

Among IoT Adopters (n=2721)

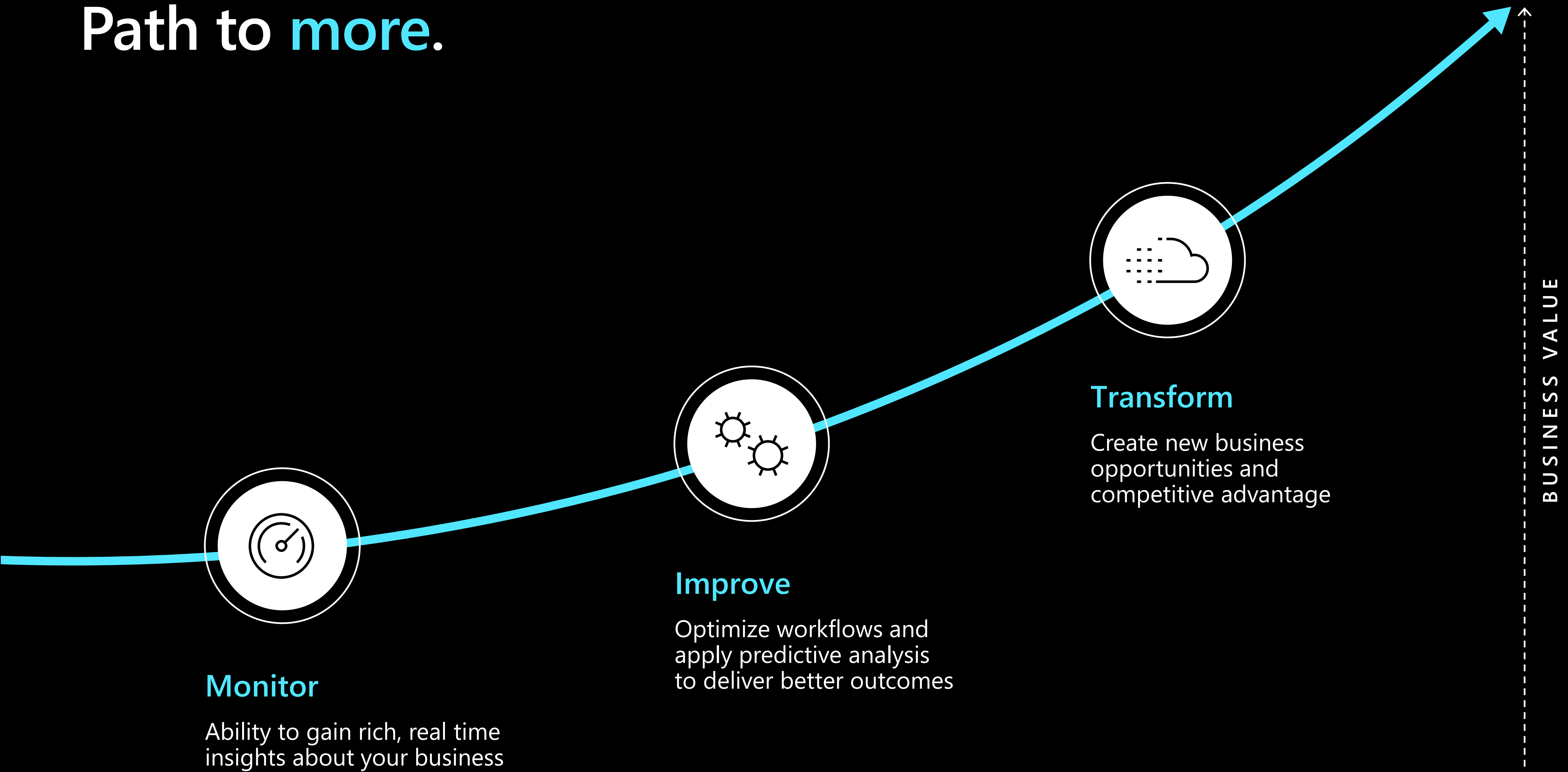


## TYPES OF IoT SECURITY CONSIDERATIONS

Among IoT Adopters (n=2721)



# Path to more.



**Monitor**

Ability to gain rich, real time insights about your business

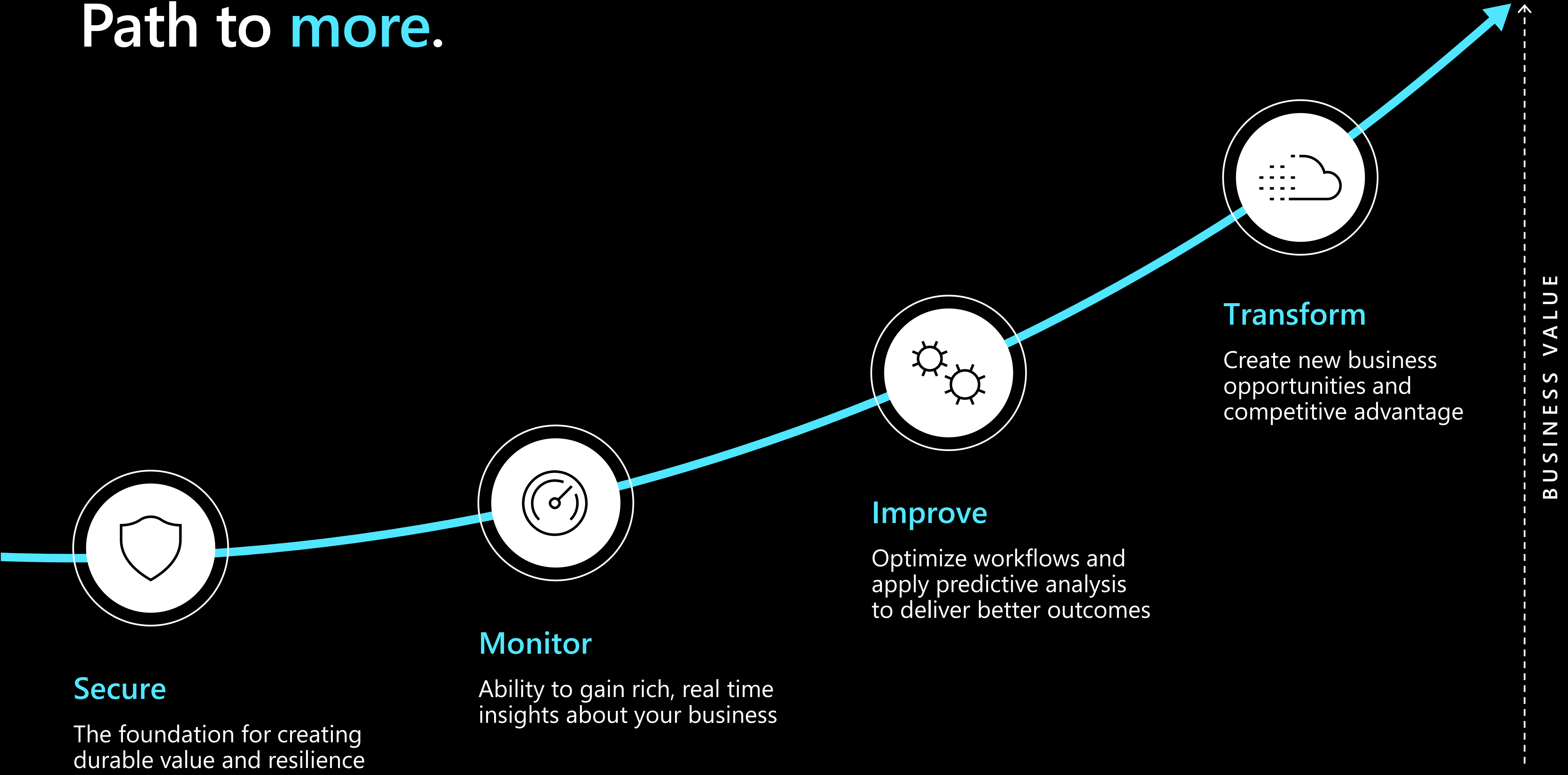
**Improve**

Optimize workflows and apply predictive analysis to deliver better outcomes

**Transform**

Create new business opportunities and competitive advantage

# Path to more.



### Secure

The foundation for creating durable value and resilience

### Monitor

Ability to gain rich, real time insights about your business

### Improve

Optimize workflows and apply predictive analysis to deliver better outcomes

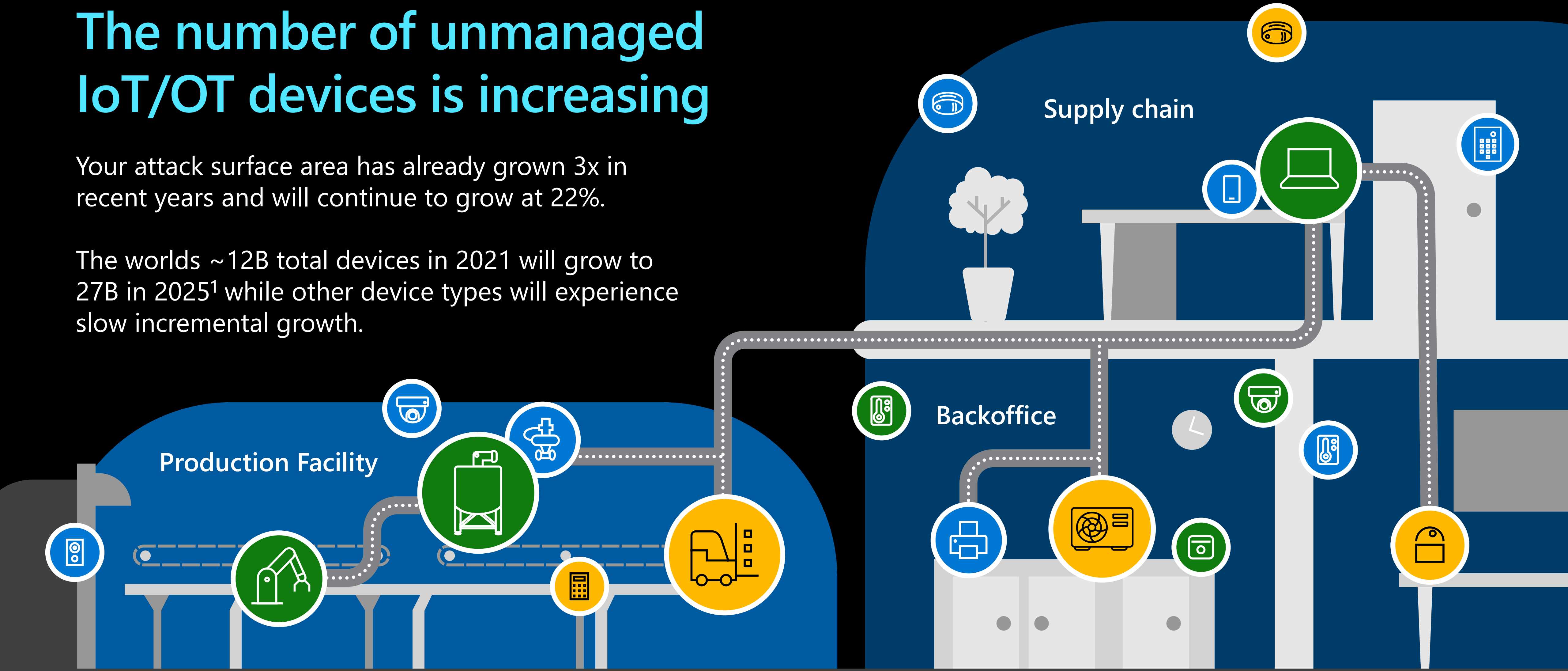
### Transform

Create new business opportunities and competitive advantage

# The number of unmanaged IoT/OT devices is increasing

Your attack surface area has already grown 3x in recent years and will continue to grow at 22%.

The worlds ~12B total devices in 2021 will grow to 27B in 2025[1] while other device types will experience slow incremental growth.



[1] https://iot-analytics.com/number-connected-iot-devices/

# IoT Devices – Expand the Attack Surfaces

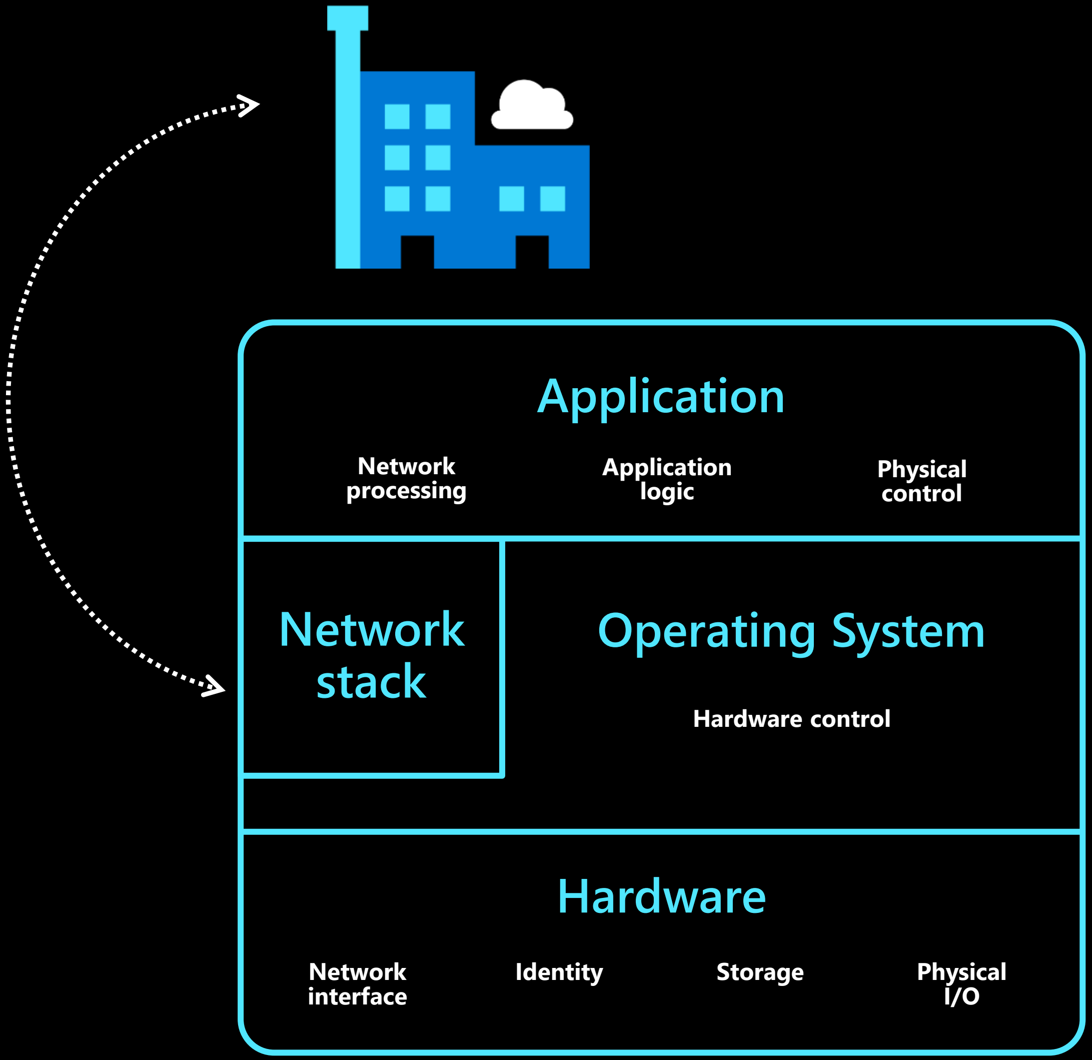
Applications

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

# Zero Trust security

A traditional network security model often doesn’t meet the security or user experience needs of modern organizations – a security posture based on the ideas of “never trust” and “verify everything” keeps your data and devices safer

By leveraging three key principles, the Zero Trust security model enables organizations to mitigate the risks of operating in an increasingly interconnected world

Verify explicitly

Use least-privileged access

Assume breach

# Why is IoT security different?

→ IoT devices are ‘user-less’ and run automated workloads

→ IoT device platforms are varied and often integrate with aging infrastructure

→ Many IoT devices have limited capability and connectivity

→ IoT devices can be high-value targets

→ IoT devices can be exposed to physical or local attacks

Effectively applying Zero Trust principles to IoT scenarios requires a specialized approach

It's important that the following core Zero Trust capabilities for IoT are enabled

**Strong identity**
To authenticate devices

**Least-privileged access**
To mitigate blast radius

**Device health**
To gate access or flag devices for remediation

**Continual updates**
To keep devices healthy

**Security monitoring & response**
To detect and respond to emerging threats

# The Seven Properties of Highly Secured Devices

Is your device highly secured or does it just have some security features?

## Hardware Root of Trust

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

## Defense in Depth

Does your device remain protected even if some security mechanism is defeated?

## Small Trusted Computing Base

Is your device's security-enforcement code protected from bugs in application code?

## Dynamic Compartments

Can your device's security improve after deployment?

## Certificate-Based Authentication

Does your device authenticate itself with certificates?

## Error Reporting

Does your device report back errors to give you in-field awareness?

## Renewable Security

Does your device software update automatically?

https://aka.ms/7properties

# 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.

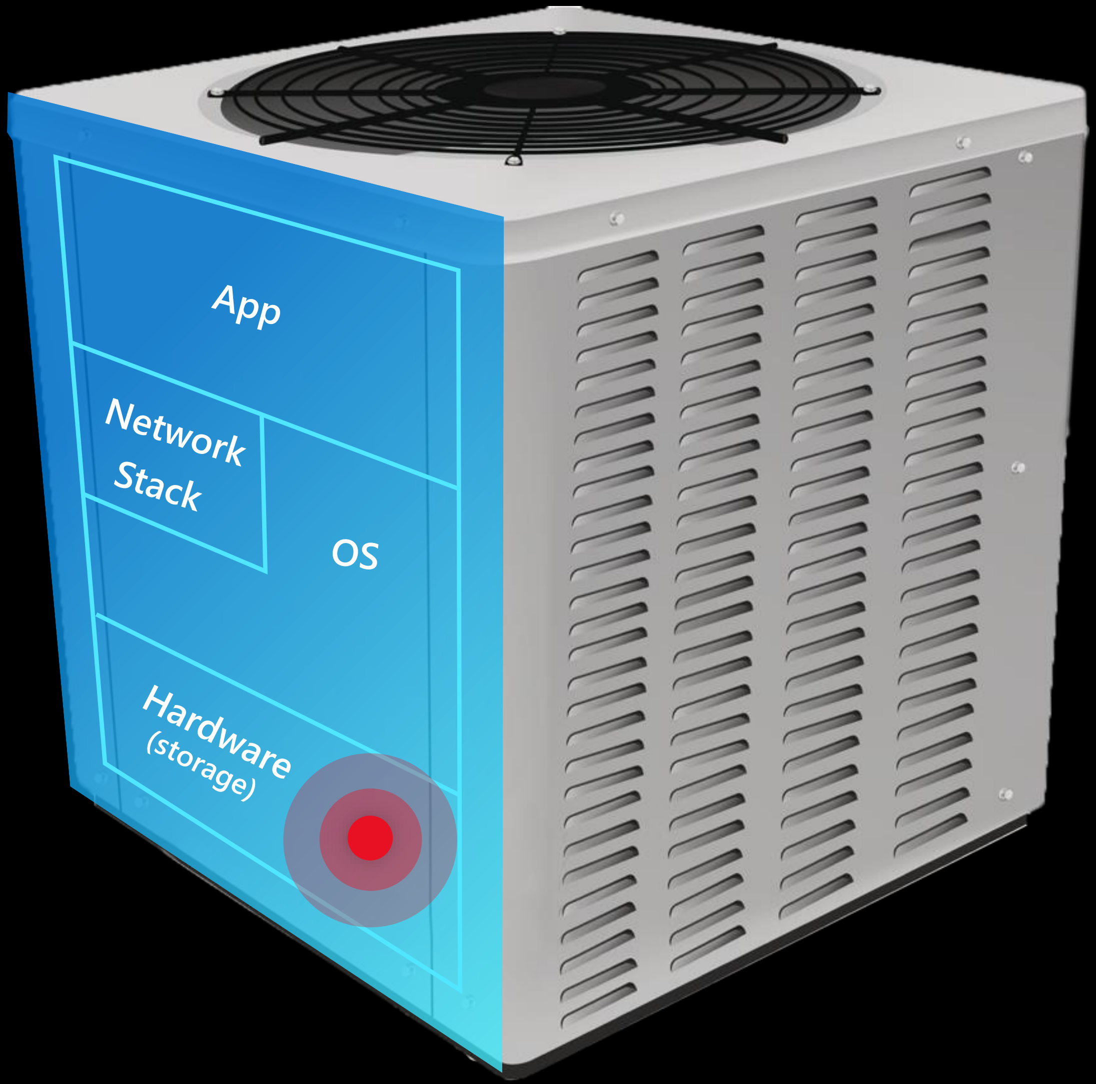
**Assessing the risk:**

- 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

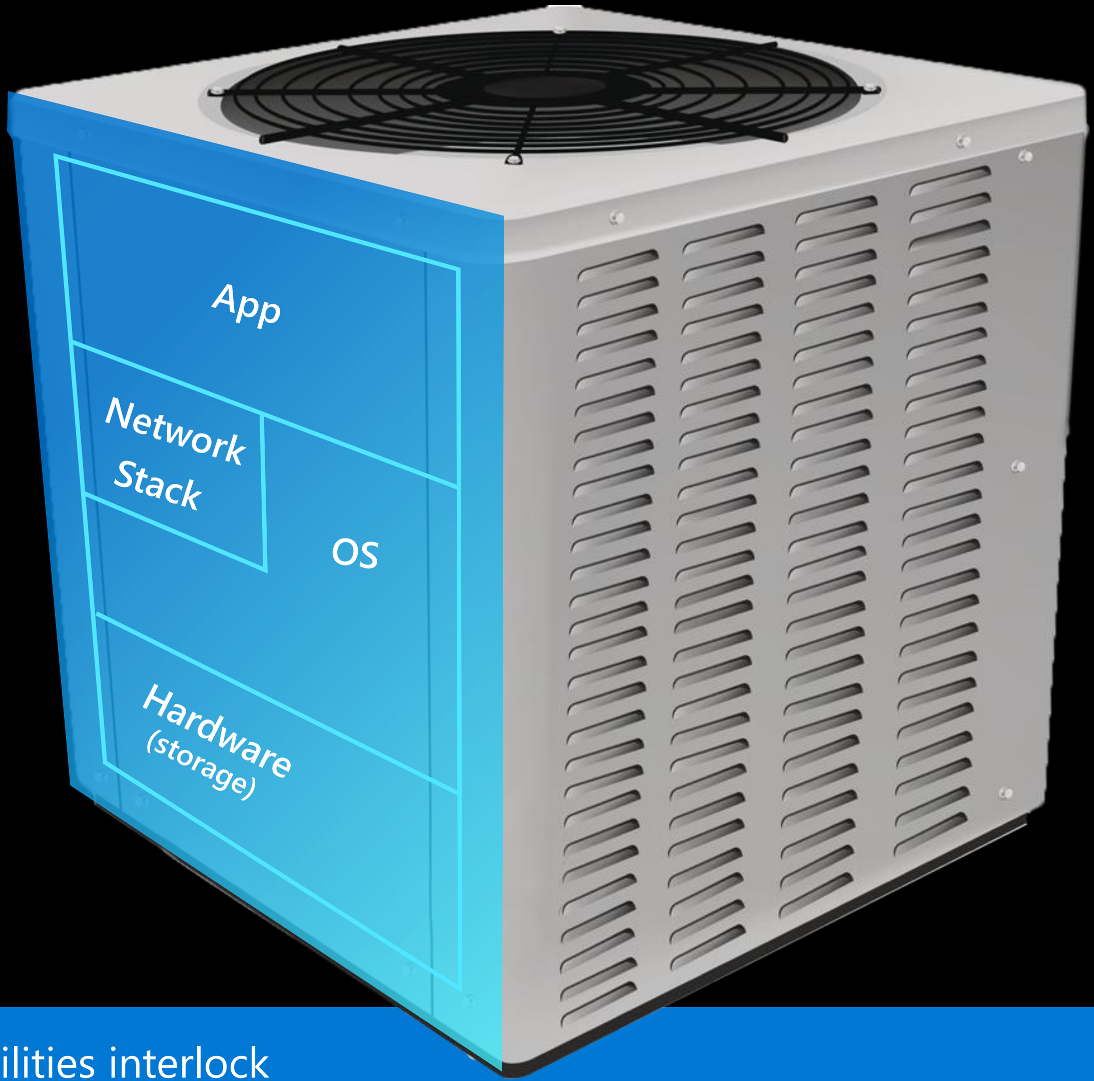
Strategies and capabilities for mitigation:

**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



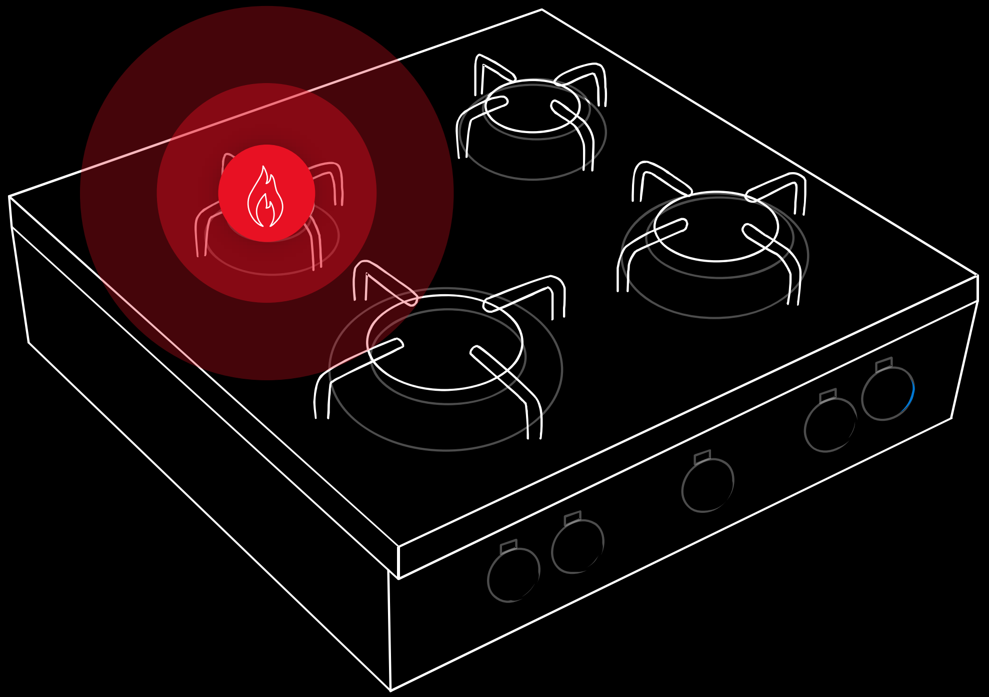
**Best practice:** Vertically integrated system where all these capabilities interlock and are comprehensively refreshed together.

# 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:**

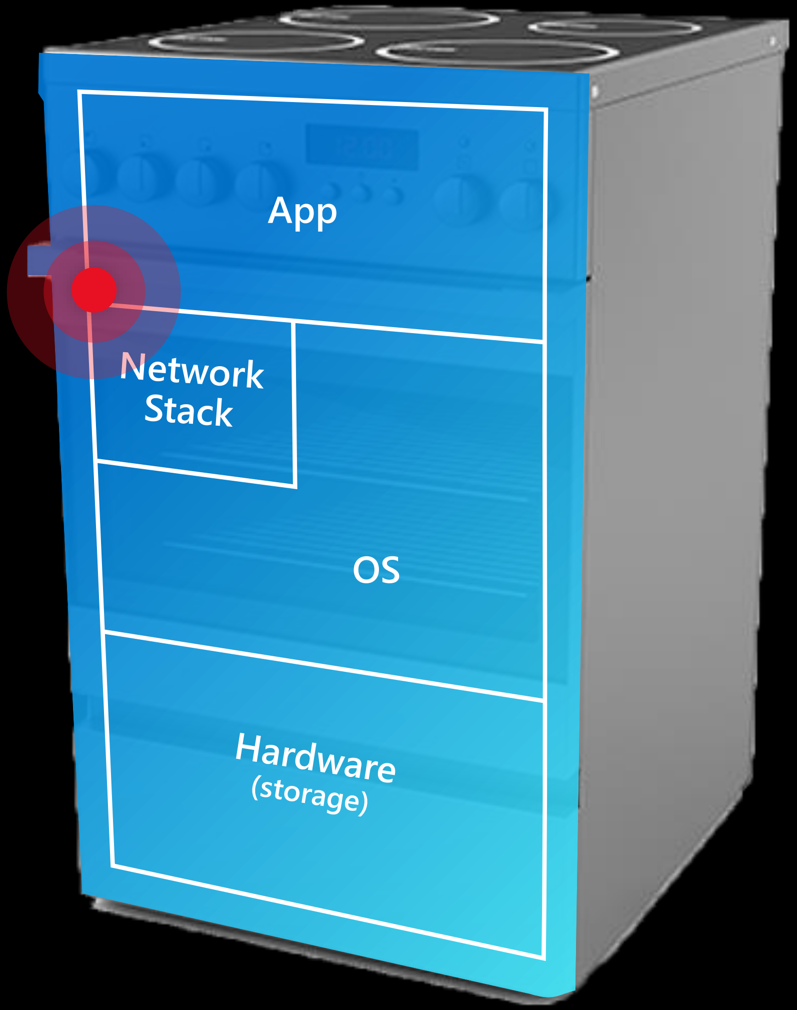
- Do your devices access heating elements, gas or water lines, or operate in a potentially dangerous context?
- Could your devices cause physical harm to the people that operate them?
- Can your devices cause a privacy breach in their environment?



# Devices are used for malicious purposes

Attackers trick your devices into doing something they weren’t intending:

Methods of achieving this include attacks 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:

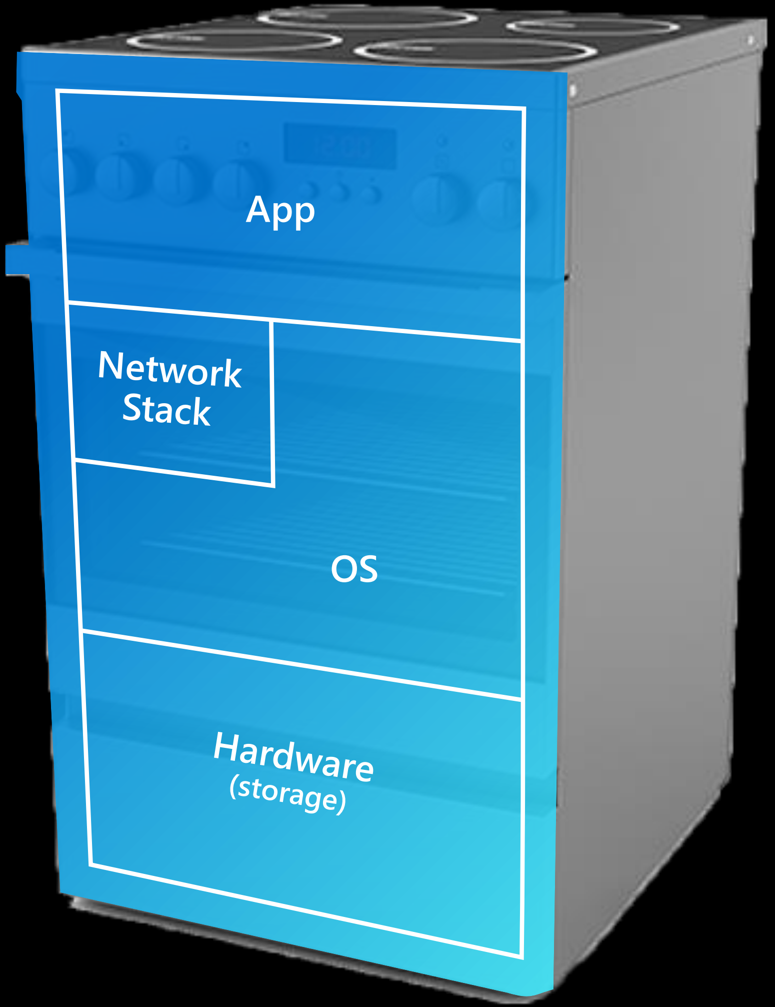
**Private/public key pairings** with trusted crypto and protocols; to ensure trusted communication

**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 renew security on devices limiting the opportunity for success

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



# Data pollution & compromised business insights

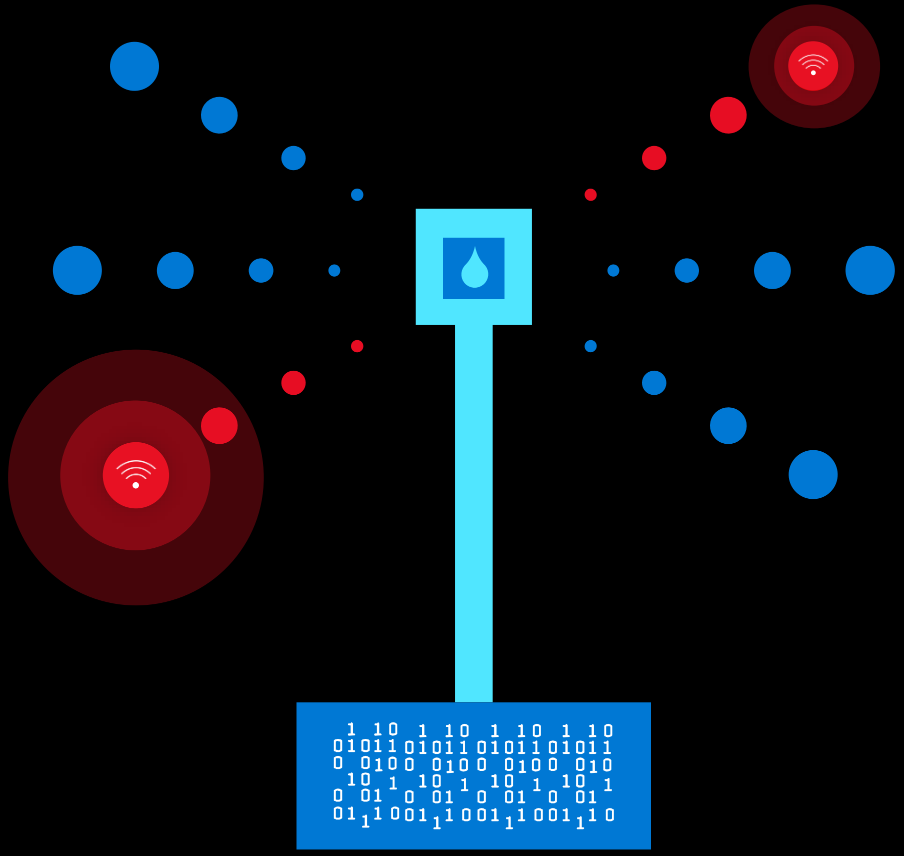
The data and insights coming from your devices can’t be trusted. You may have no way of identifying the issue until something severe goes wrong.

**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.

# Incorporating the seven properties is difficult and costly

## Design and build a holistic solution

**You’re only as secure as your weakest link.**

You must stitch disparate security components into an gap-free, end-to-end solution.

TECHNOLOGY

## Recognize and mitigate emerging threats

**Threats evolve over time.**

You must have the ongoing security expertise to identify and create the updates needed to mitigate new threats as they emerge.

TALENT

## Distribute and apply updates on a global scale

**Update efficiency is critical.**

You must have the infrastructure, logistics, and operational excellence to deliver and deploy updates globally to your entire fleet of devices in hours.

TACTICS

Microsoft

# Securely Connect the Disconnected with Azure Sphere

# Azure Sphere in a Nutshell…

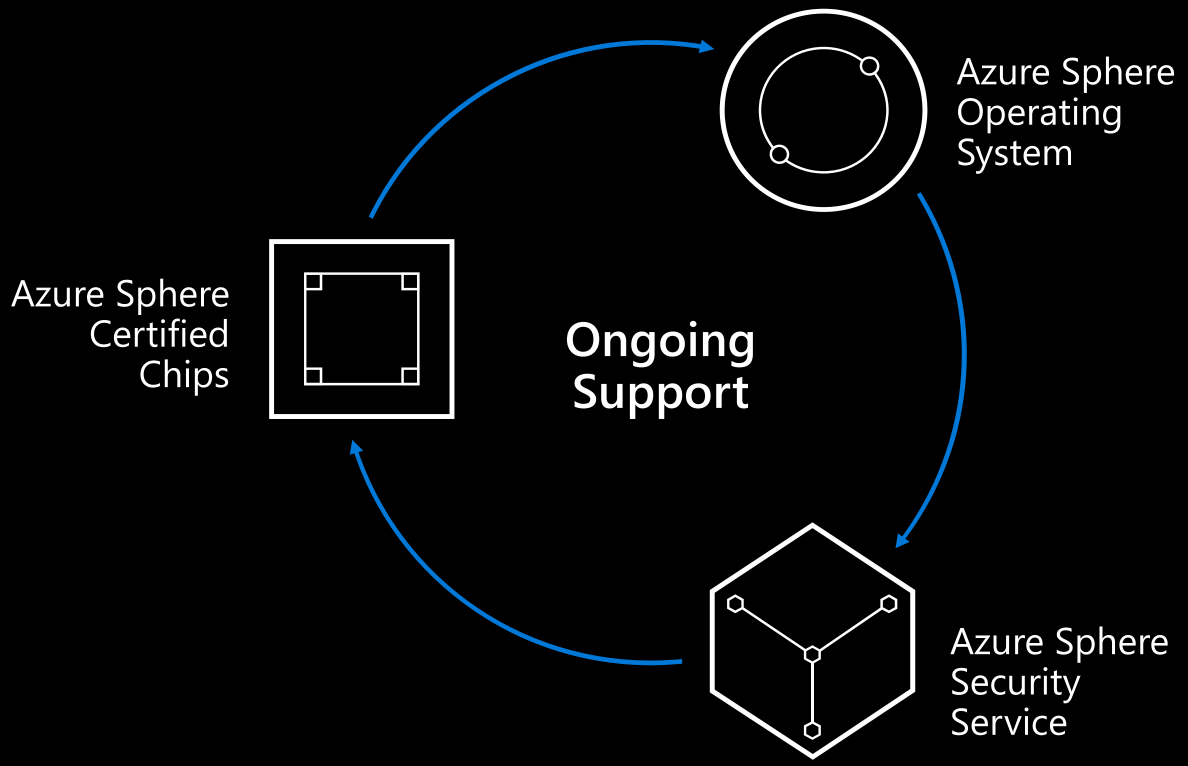
An end-to-end solution for securely connecting existing equipment and to create new IoT devices with built-in security. Put the power of Microsoft's expertise to work for you everyday.

**Azure Sphere certified chips**

**Azure Sphere Operating System**

**Azure Sphere Security Service**

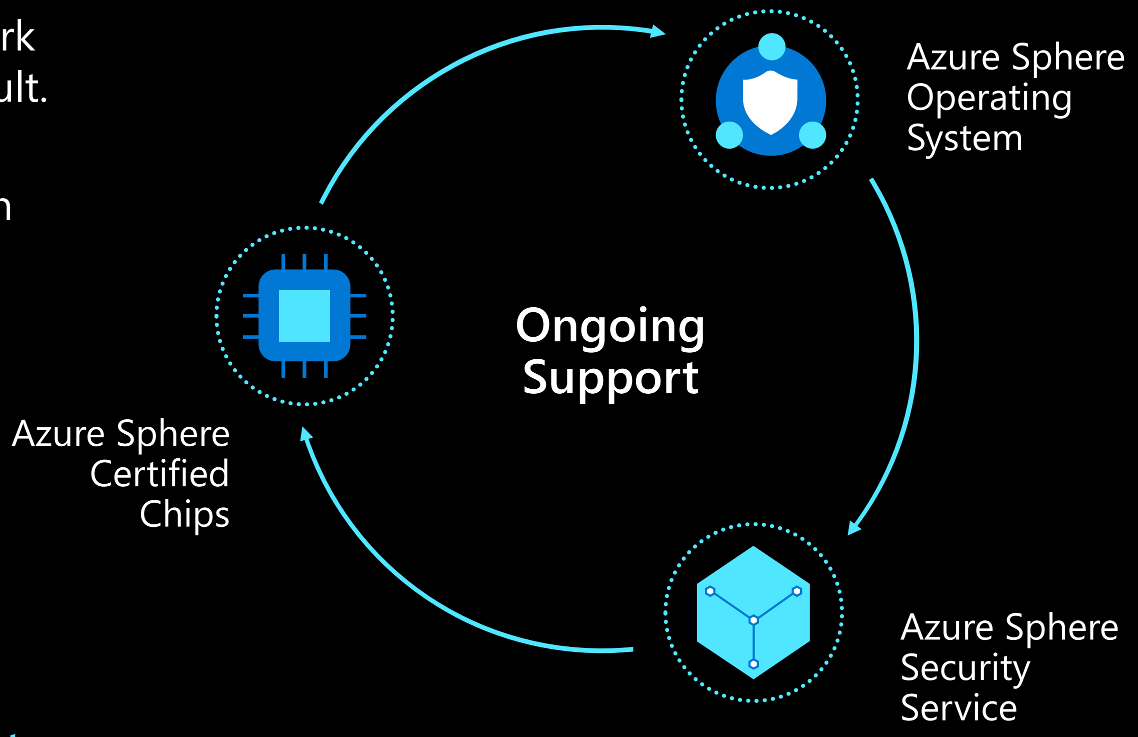
**Ongoing OS and Security Updates**


Azure Sphere Operating System
Azure Sphere Certified Chips
Ongoing Support
Azure Sphere Security Service

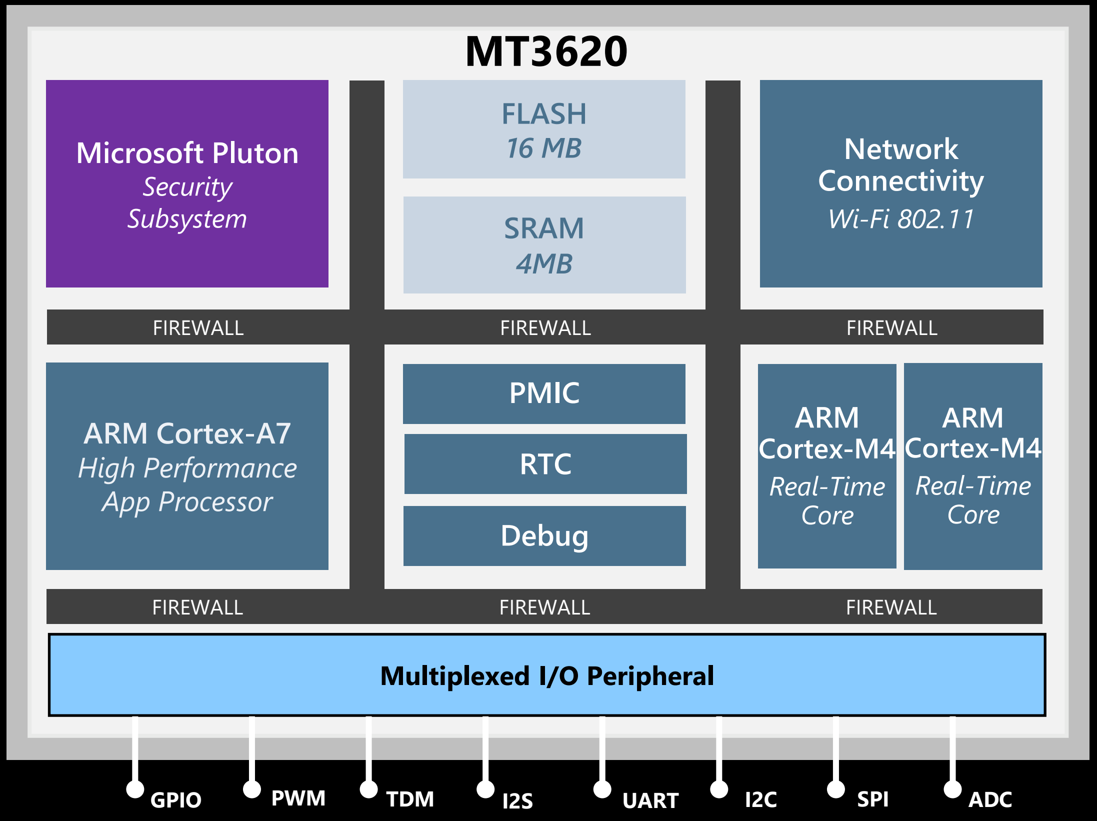
**Over 10 years of security and OS updates delivered directly to each device by Microsoft**

# Protect your data, physical safety, and infrastructure with Azure Sphere.

- ✓ **Integrated hardware, software, and cloud services** work seamlessly together and deliver active security by default.
- ✓ **Defense in depth** provides multiple layers of protection to help guard devices against and respond to threats.
- ✓ **Ongoing security and OS updates** from Microsoft keep your devices secured over time.
- ✓ **Implementation options** allow you to secure existing equipment and build security into new IoT devices.
- ✓ **Simplified OEM business model with one-time upfront price** includes hardware, security service, and full OS update servicing for over a decade.


Azure Sphere Operating System
Ongoing Support
Azure Sphere Certified Chips
Azure Sphere Security Service

# Azure Sphere certified SOCs create a secured root of trust for connected, intelligence edge devices



**Connected**
with built-in networking

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

**Crossover**
Cortex-A processing power brought to MCUs and crossover SOCs for the first time

# Azure Sphere Security Service connects and protects every Azure Sphere device

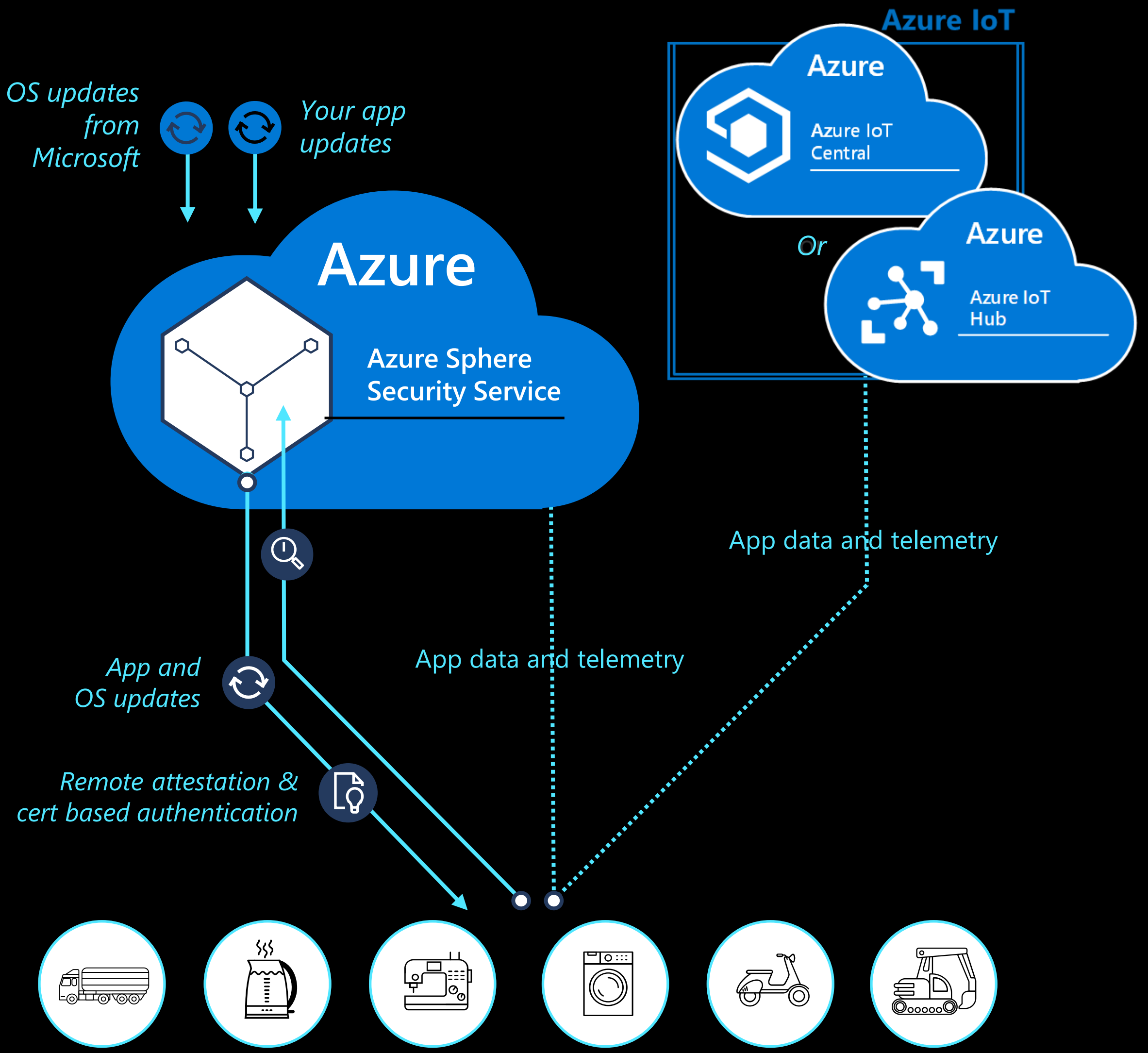
**Protects** your devices and your customers with certificate-based authentication of all communication

**Detects** emerging security threats through automated processing of on-device failures

**Responds** to threats with fully automated on-device updates of OS

**Allows** for easy deployment of software updates to Azure Sphere powered devices

**Cloud** choice for app data and telemetry



# A secured environment for RTOS applications

## Real-time cores secured from remote attacks

Cortex-M – safety critical apps physically isolated from network

Cortex-A – OS separates networking from high-level processing

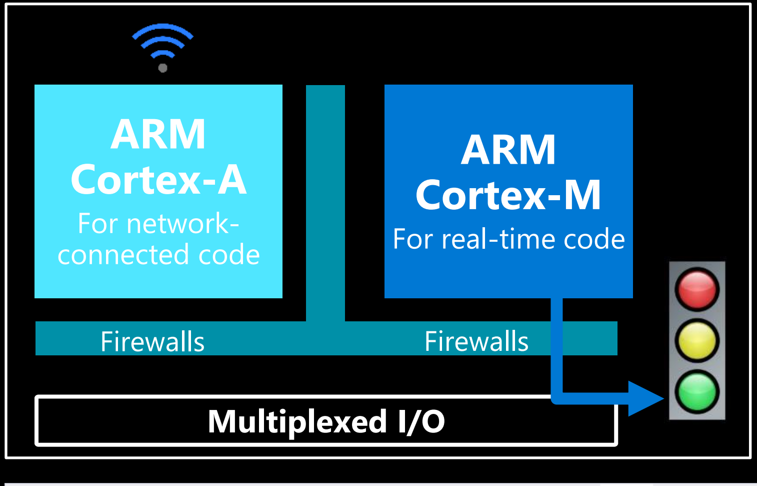
## Portability

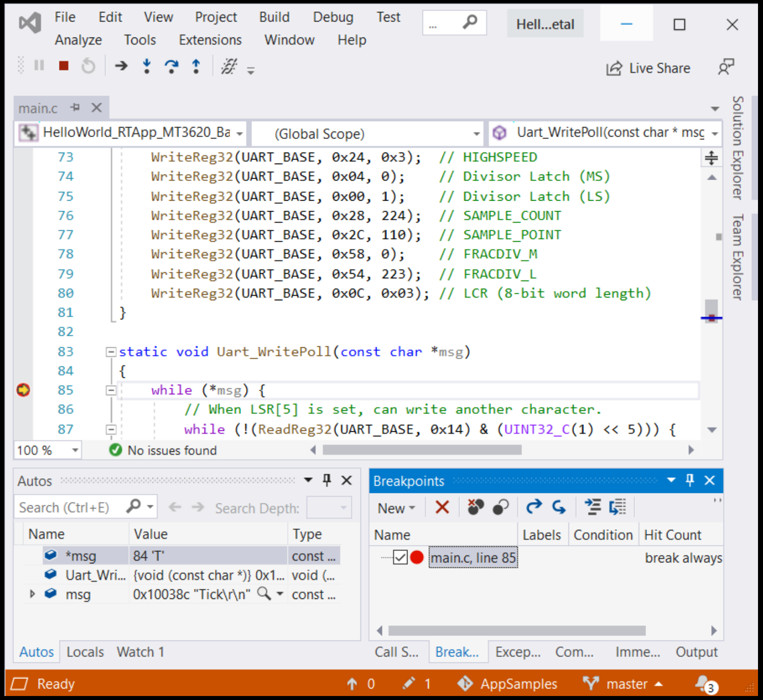
Customers can easily port their real-time apps

Azure Sphere supports any RTOS library, including Azure RTOS ThreadX

## Best in-class Developer Experience

Fully integrated Visual Studio support for development, deployment, and debugging of RT apps





```
73        WriteReg32(UART_BASE, 0x24, 0x3);  // HIGHSPEED
74        WriteReg32(UART_BASE, 0x04, 0);    // Divisor Latch (MS)
75        WriteReg32(UART_BASE, 0x00, 1);    // Divisor Latch (LS)
76        WriteReg32(UART_BASE, 0x28, 224);  // SAMPLE_COUNT
77        WriteReg32(UART_BASE, 0x2C, 110);  // SAMPLE_POINT
78        WriteReg32(UART_BASE, 0x58, 0);    // FRACDIV_M
79        WriteReg32(UART_BASE, 0x54, 223);  // FRACDIV_L
80        WriteReg32(UART_BASE, 0x0C, 0x03); // LCR (8-bit word length)
81    }
82
83    static void Uart_WritePoll(const char *msg)
84    {
85        while (*msg) {
86            // When LSR[5] is set, can write another character.
87            while (!(ReadReg32(UART_BASE, 0x14) & (UINT32_C(1) << 5))) {
```

✓ No issues found

| Name | Value | Type |
|---|---|---|
| *msg | 84 'T' | const ... |
| Uart_Wri... | {void (const char *)} 0x1... | void (... |
| msg | 0x10038c "Tick\r\n" | const ... |

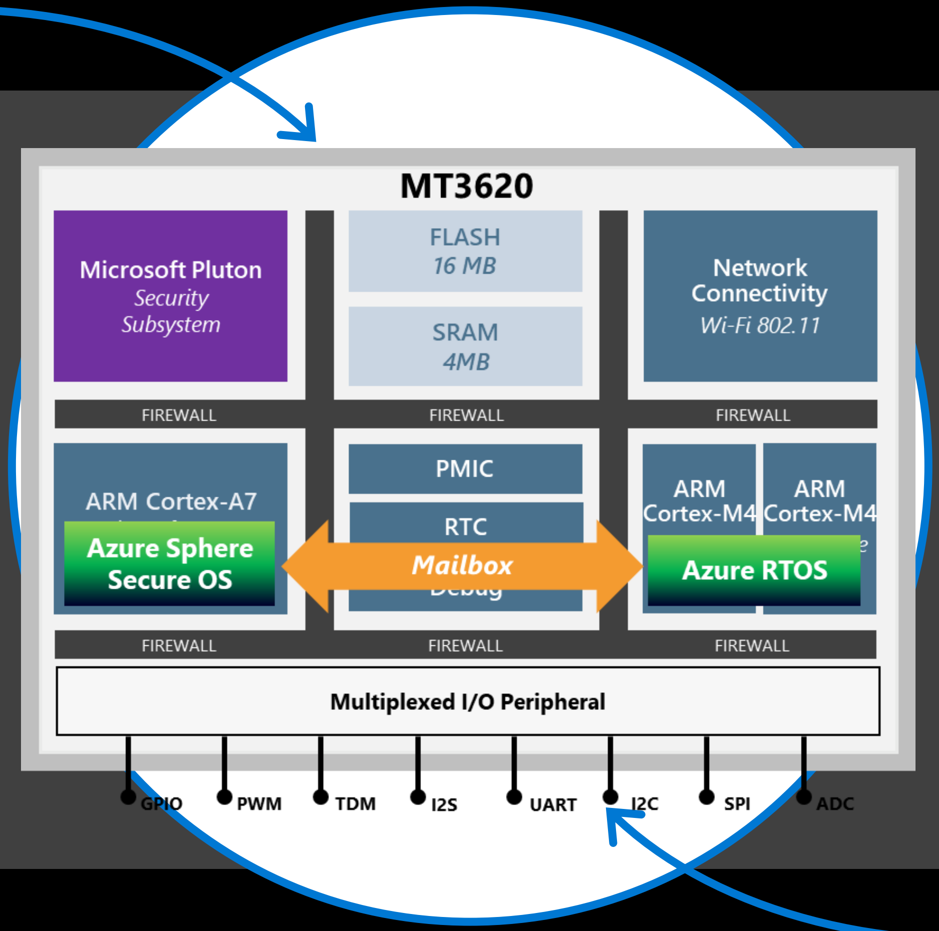
| Name | Labels | Condition | Hit Count |
|---|---|---|---|
| ☑ ● main.c, line 85 | | | break always |

Ready ↑ 0 1 AppSamples master 3

# Azure RTOS + Azure Sphere: Better together

## Azure Sphere

Everything an embedded developer needs to build a highly secured device



## Azure RTOS

Enables embedded developers to quickly build real-time software

# Azure Sphere
# Key Benefits & Differentiator

### ENTERPRISE GRADE SECURITY FOR IOT DEVICES

SECURING E2E

SOC ↔ DEVICE ↔ OS ↔ CLOUD

### TURNKEY SECURITY SOLUTION

↗ IOT SECURITY POSTURE

↘ TTM

↘ TCO (DEVELOPMENT, OPERATIONAL, MAINTENANCE)

◎ FOCUS ON BUILDING E2E SOLUTION & VALUE CREATION

### OVER 10 YEARS SUPPORT FROM MICROSOFT

SECURITY AND OS UPDATE FROM MICROSOFT

USAGE OF AS3 CLOUD SECURITY

DEVICE MANAGEMENT SERVICES

### MICROSOFT PLUTON SECURITY

BUILT INTO THE SOC

GOES BEYOND A HSM

↘ EBOM COST ON EXTERNAL TPM / HSM

### AUTOMATED CERTIFICATE MANAGEMENT

CERT BASED AUTHENTICATION

AUTO ROLLING & EXPIRATION

### EASE OF DEPLOYMENT & INSTALLATION

ZERO-TOUCH DEVICE PROVISIONING

DEVICE LIFECYCLE MANAGEMENT

### SECURE OTA UPDATE

OS + APP DEPLOYMENT AND MANAGEMENT SECURELY VIA OTA

HW ANTI-ROLLBACK

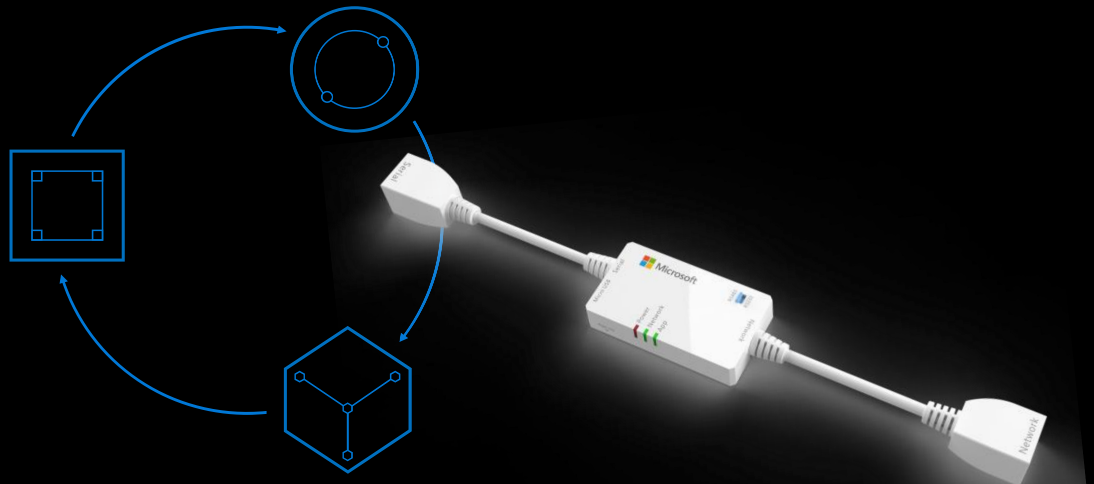
AUTO RECOVERY

Microsoft Azure

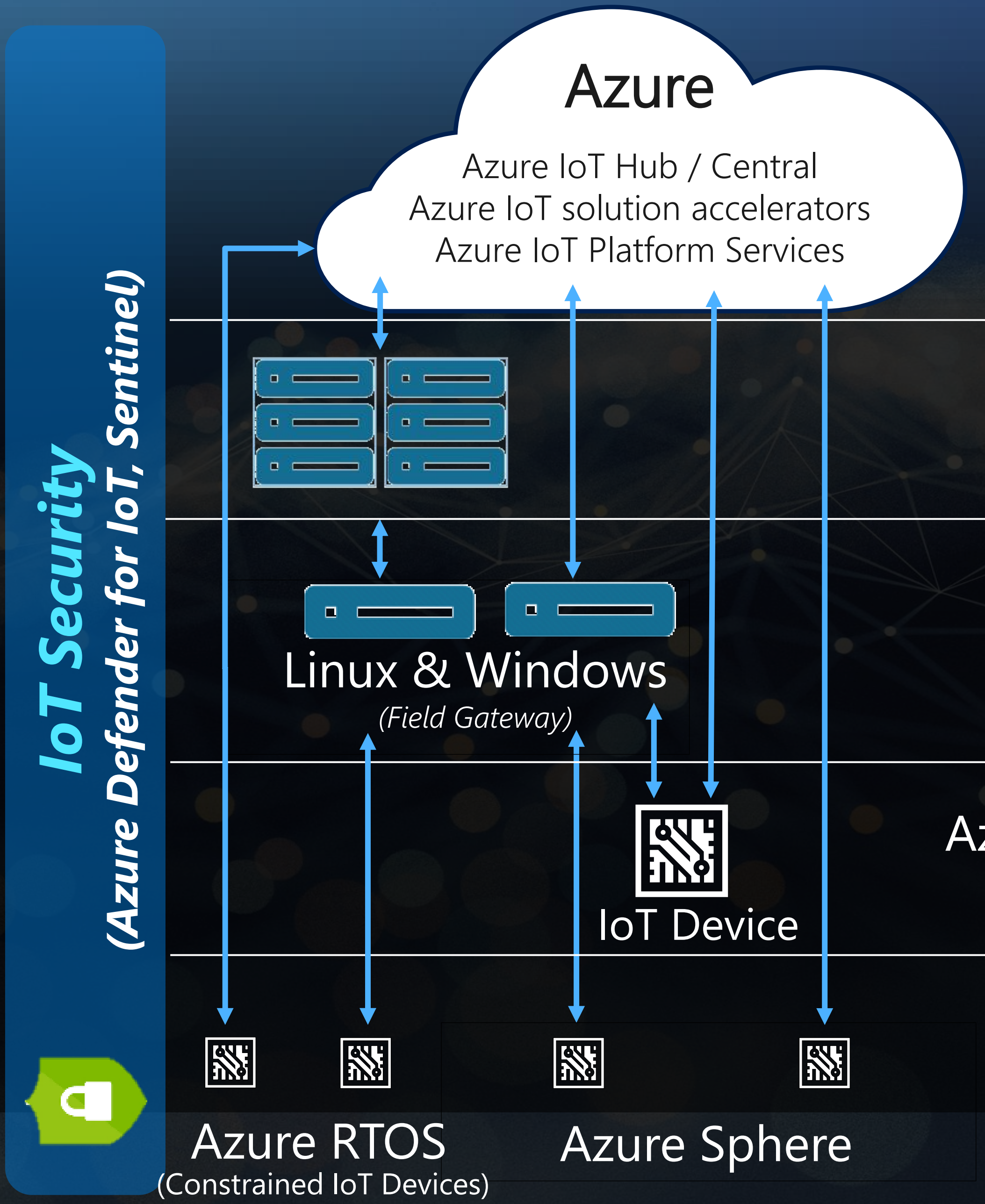
# Microsoft Data Centers

## Securing critical infrastructure with Azure Sphere

Securely connecting vital mechanical systems, electrical systems, air handling units, power distribution units and more



# Microsoft Intelligent IoT Devices Portfolio


Azure
Azure IoT Hub / Central
Azure IoT solution accelerators
Azure IoT Platform Services
Linux & Windows
(Field Gateway)
IoT Device
Azure RTOS
(Constrained IoT Devices)
Azure Sphere
IoT Security
(Azure Defender for IoT, Sentinel)

| | |
|---|---|
| Azure | • Available in Azure Regions<br>• Full functionality |
| Azure Stack | • Azure Services & Management on-prem<br>• Azure IoT Hub |
| Azure IoT Edge | • Deploy and manage cloud services<br>• Managed by Azure or Azure Stack |
| Windows IoT, Linux | • Azure IoT Edge runs on Windows and Linux |
| Azure IoT Device SDK<br>Azure IoT PnP | • Multi-device, multi-language, multi-OS<br>• Linux, iOS, Android, Windows, RTOS |
| Azure Sphere<br>Azure Sphere OS | • Peerless security for MCU devices<br>• Connect directly to Azure or via Azure IoT Edge<br>• Linux Kernel that modernizes MCU devices |
| Azure RTOS | • Comprehensive suite featuring high performance small, fast and reliable RTOS, middleware and tools |

Microsoft

# Let’s secure the future.

SECURED FROM THE SILICON UP

Microsoft Azure

# Thank you.