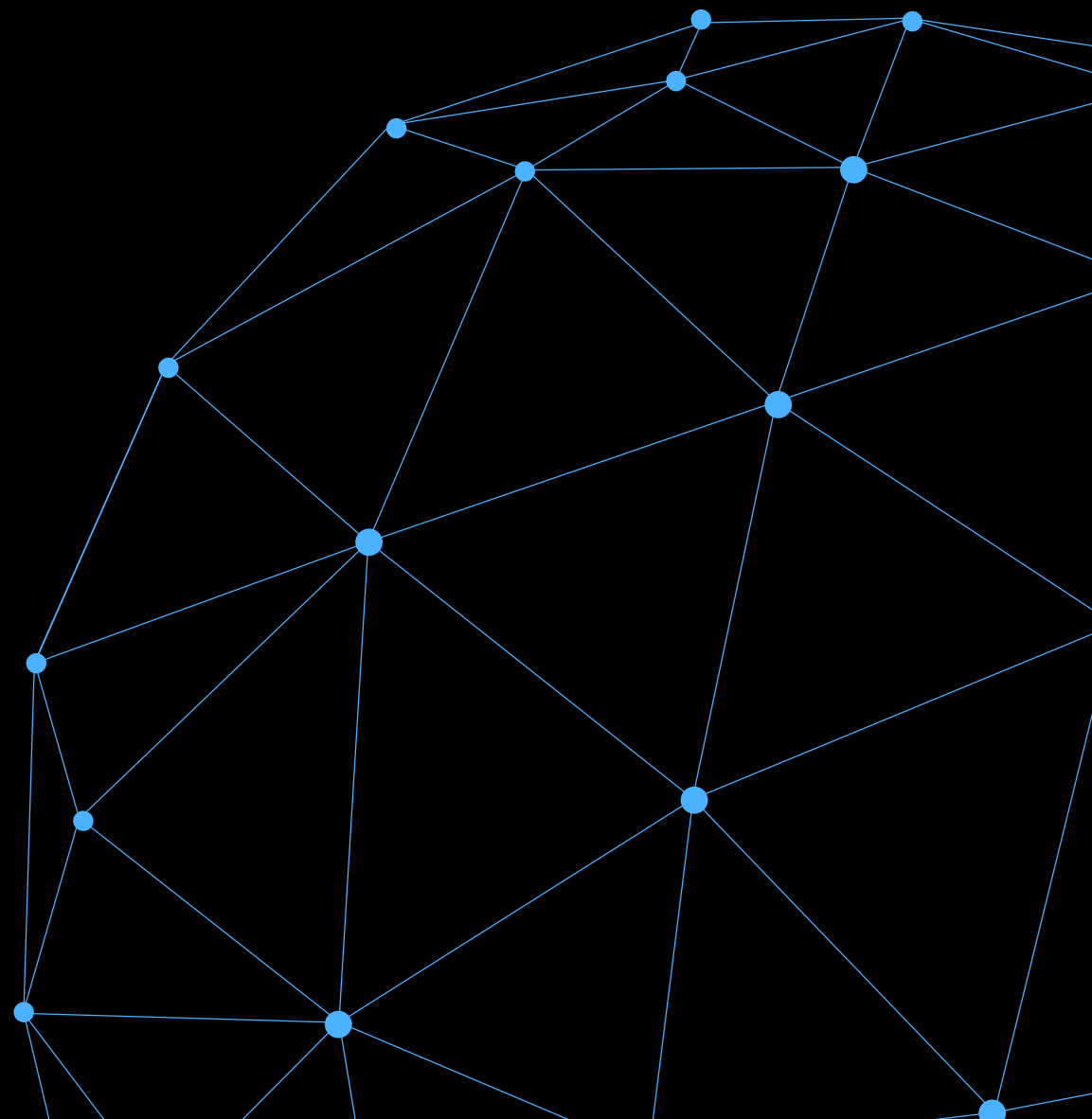
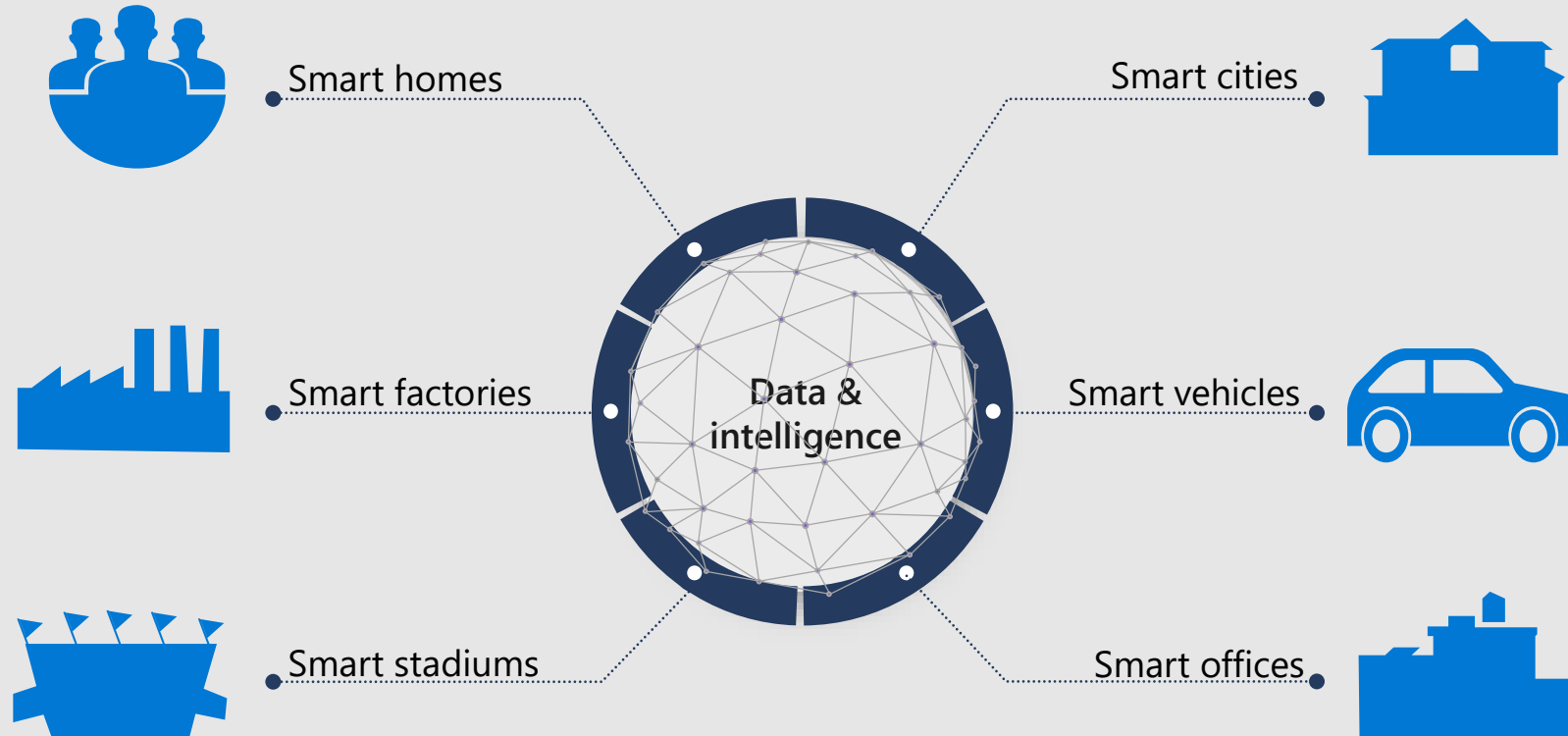


Azure Sphere Overview

Pauline Hsiao, Azure Sphere Solution Specialist



IoT is fueling digital transformation



20 billion connected devices by 2020

—Gartner



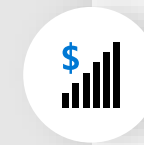
41.6B

Connected "things" by 2025
generating 79ZB 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



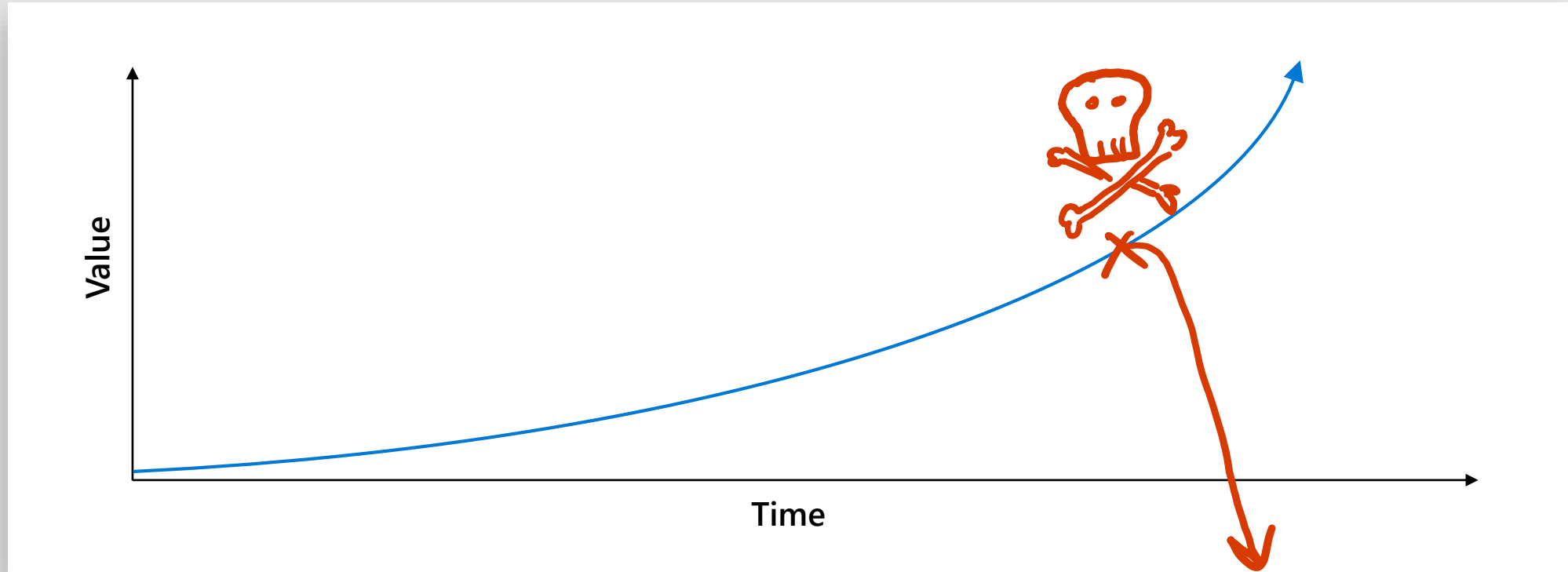
Streamline operations



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~~

Mirai Botnet attack

Everyday devices are used to launch an attack that takes down the internet for a day

100k devices

Exploited a well known weakness

No early detection, no remote update



Hackers attack casino

Attackers gain access to casino database through fish tank

Entry point was a connected thermometer

Once in, other vulnerabilities were exploited

Gained access to high-roller database



"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"



The infographic features three white circular callouts arranged horizontally against a background of a modern shopping mall with a high, vaulted ceiling and a glass grid pattern. A network of white lines with circular nodes is overlaid on the image. The first callout on the left contains the text '74% of consumers would pay more for a smart device that had additional security'. The middle callout contains '65% of consumers wouldn't purchase a smart device from a brand that has experienced a security breach'. The third callout on the right contains '93% of consumers believe that manufacturers need to do more to secure smart devices'.

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

Source: IoT signals 2019

22%

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

Source: Bain & Co. 2018

70%

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

Source: Bain & Co. 2018



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

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 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

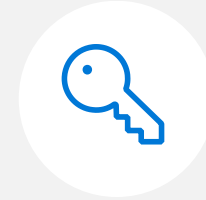
Does your device software update automatically?

<https://aka.ms/7properties>

Some properties depend only on hardware support



© Microsoft Corporation



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**



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

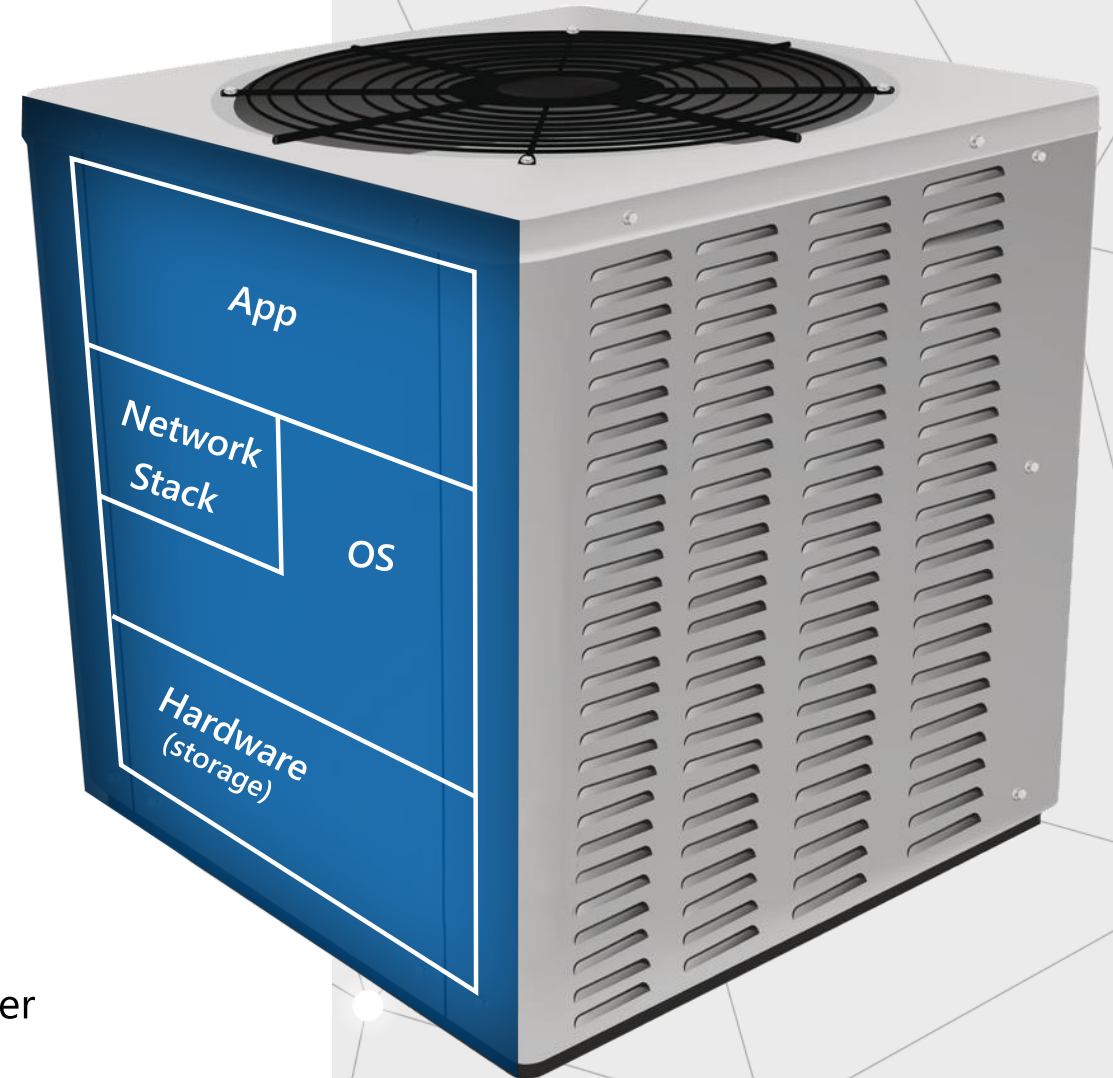
Defense in depth; multiple layers of defense that control access to storage

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

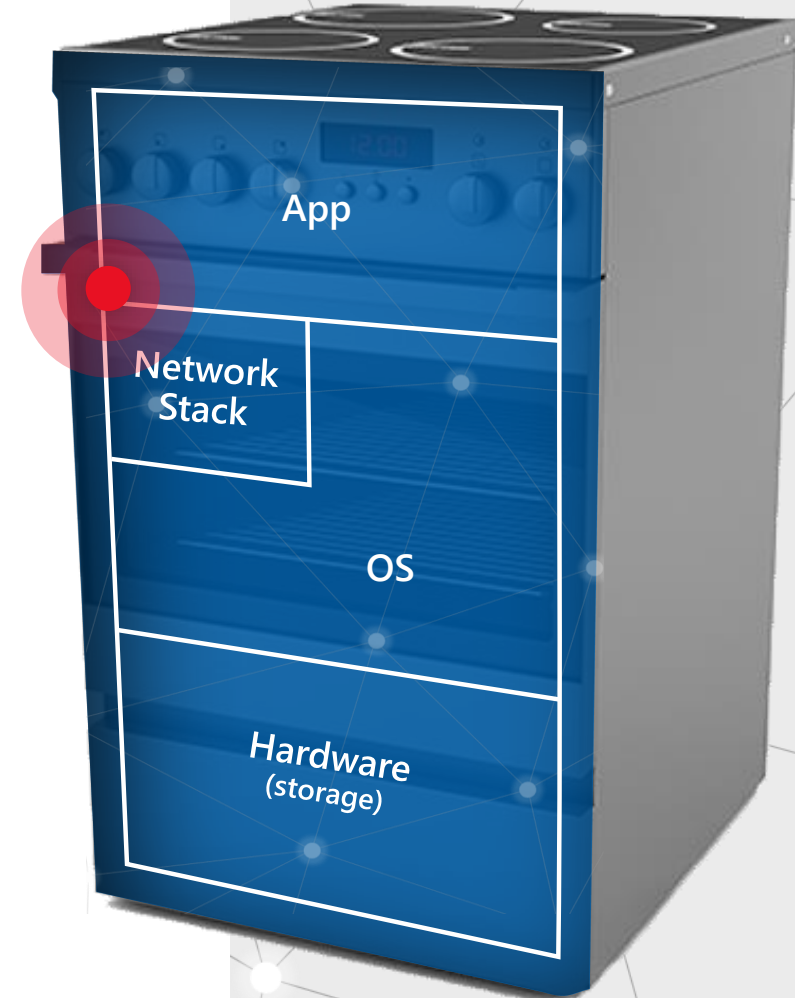




Devices are used for malicious purposes

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

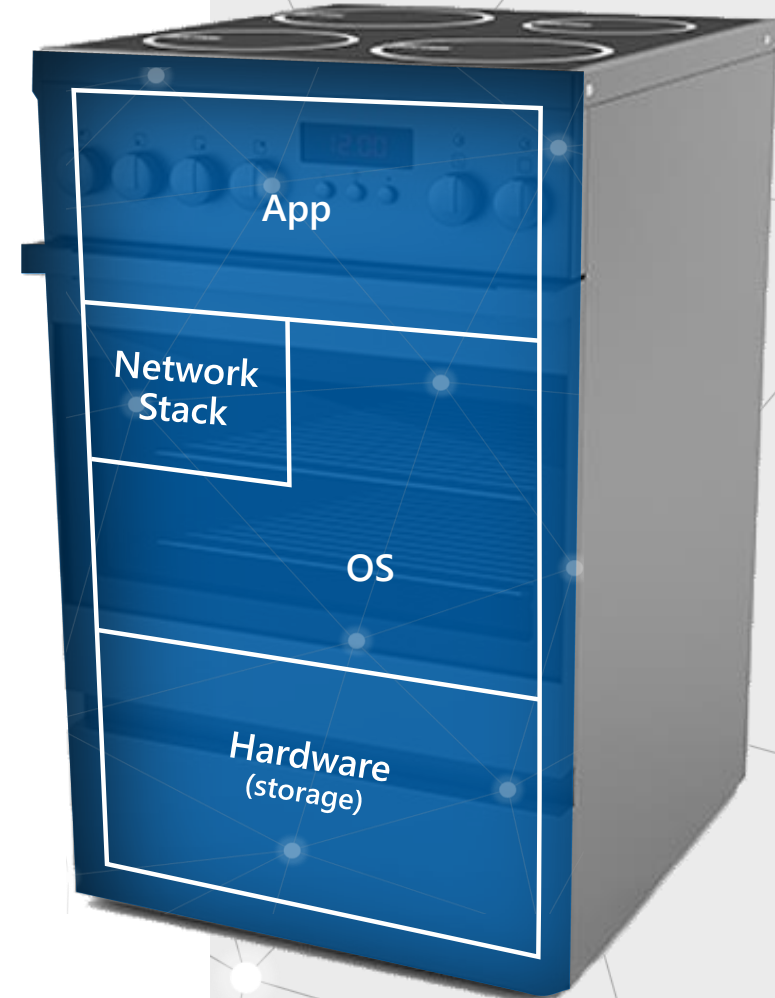
Private/public key pairings with trusted crypto and protocols; to ensure trusted communication

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

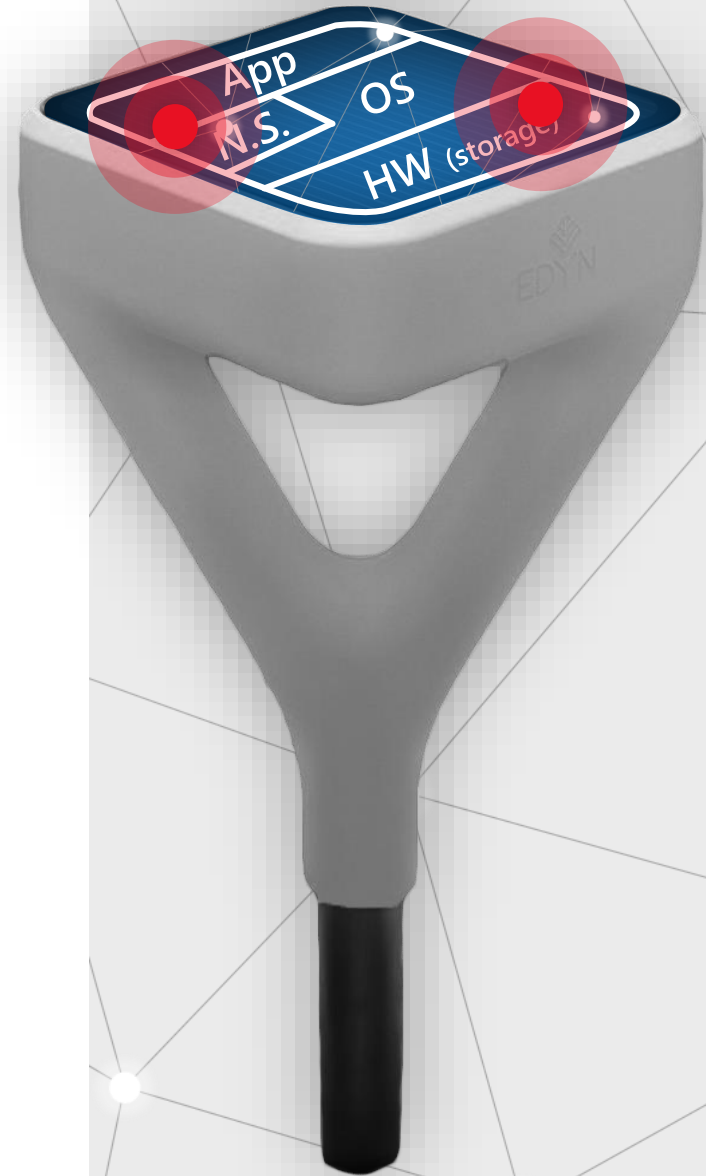




Data pollution and compromised business insights

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

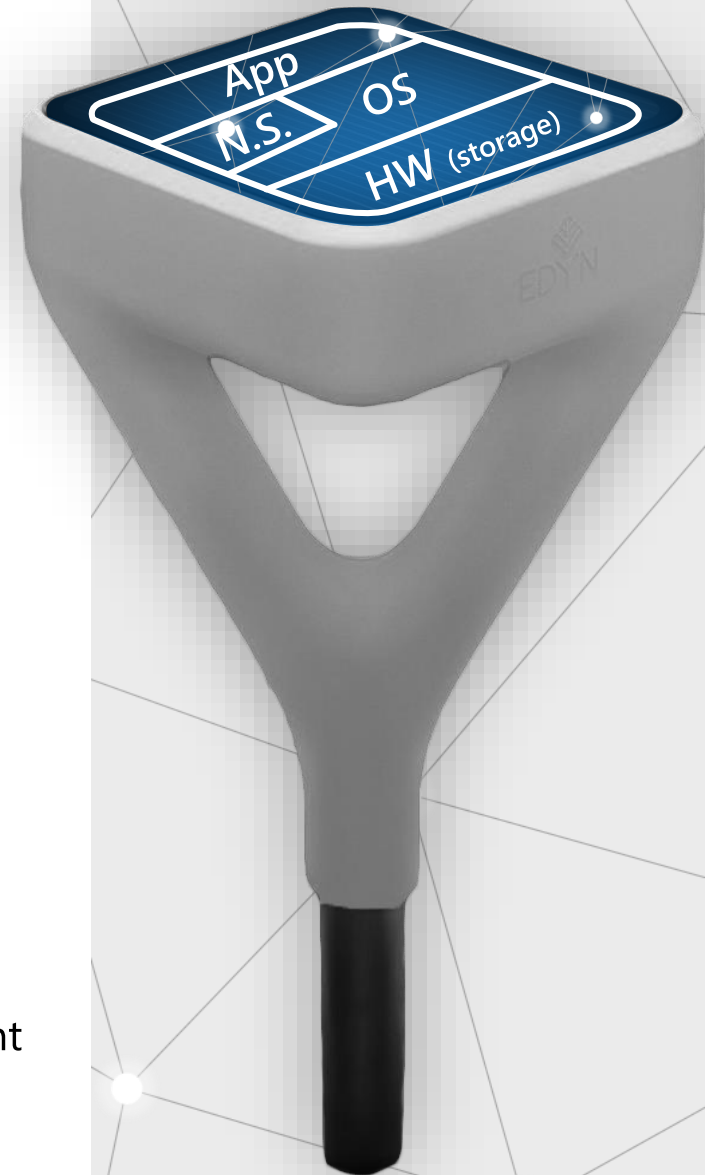
A unique unforgeable identity in the silicon

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.




The internet security battle.



Meeting the seven properties is difficult and costly

Design and build a holistic solution



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

You must to 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.**

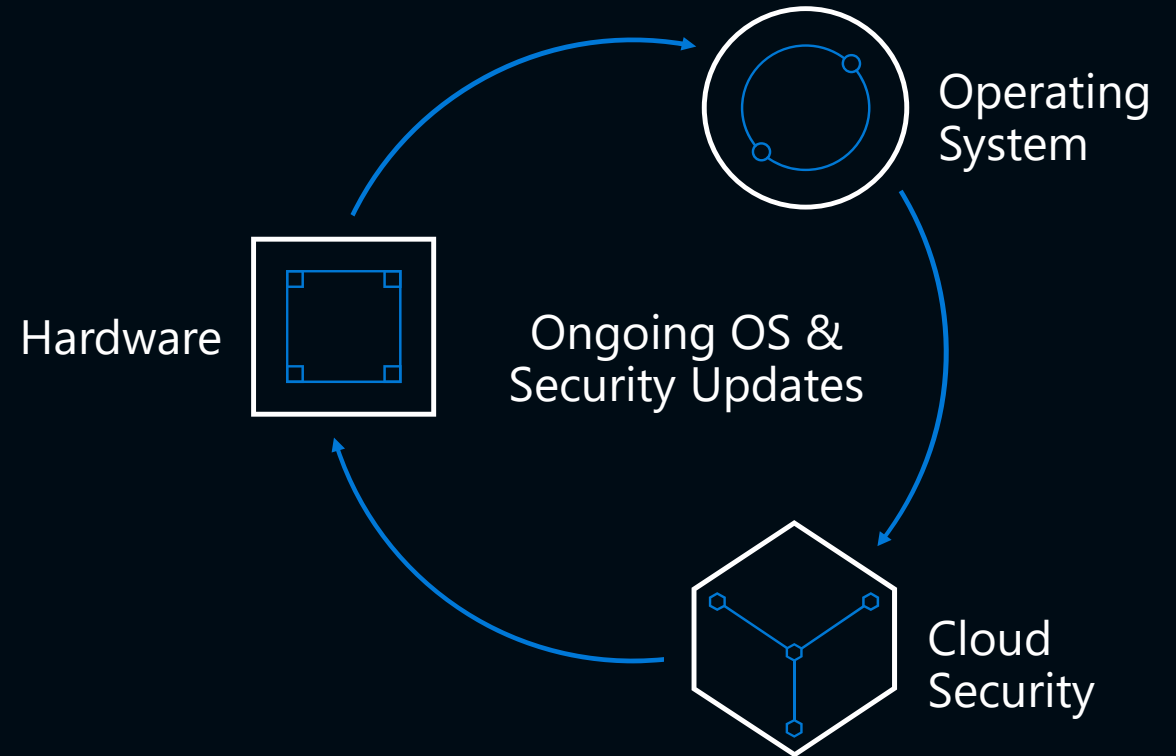
You must have the infrastructure, logistics and operational excellence to deliver and deploy updates globally to your entire fleet of devices in hours.

Tactics

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
- Ongoing OS and Security Updates

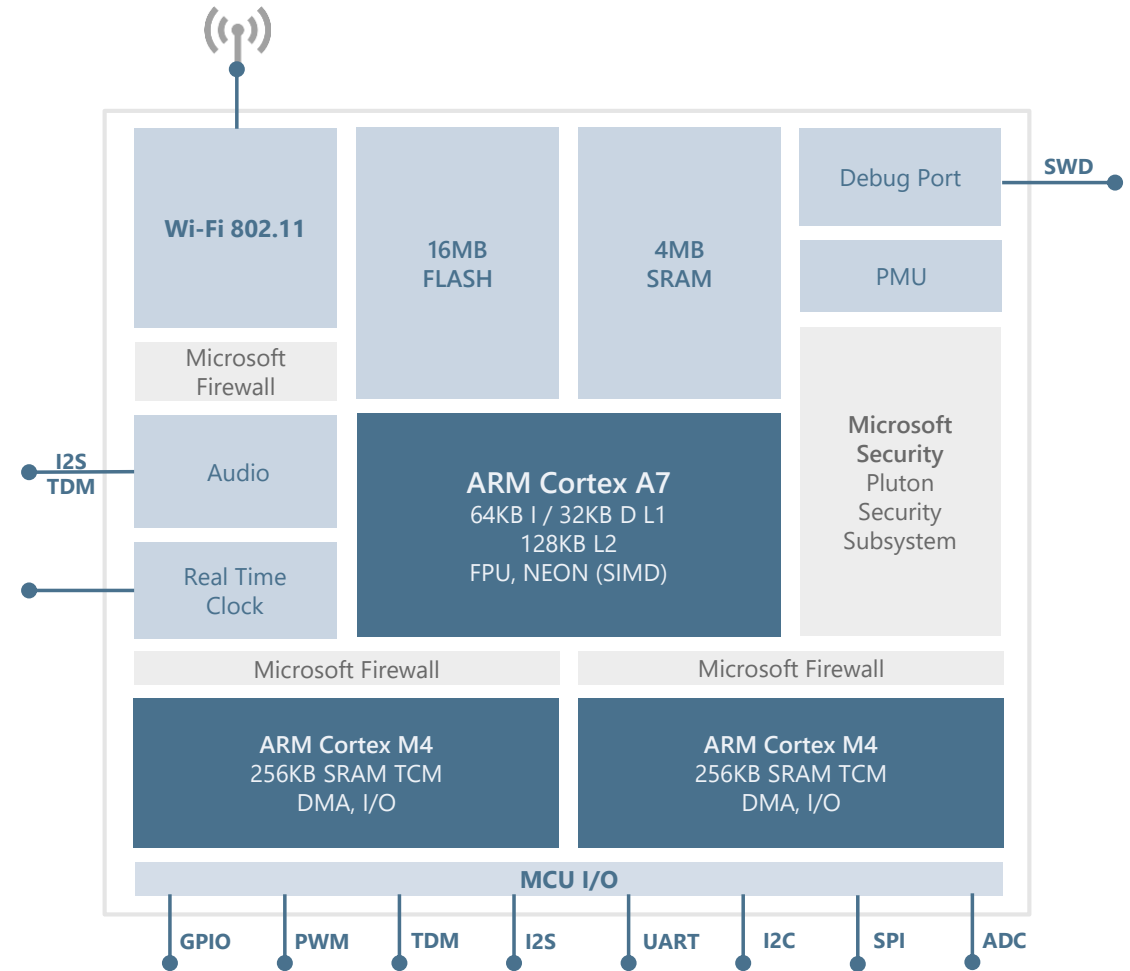


Over 10 years of security and OS updates delivered directly to each device by Microsoft

MT3620: volume production Azure Sphere MCU

Price competitive multicore MCU for device control and connectivity

CPUs	ARM Cortex A7 (500MHz) + 2 x Cortex M4 (192MHz)	
RAM	4MB	
Flash	16MB (8MB Runtime Firmware + 8MB Backup Firmware)	
Connectivity	WiFi 802.11 b/g/n, dual band: 2.4GHz, 5GHz	
Microsoft Security	Firewalls, Crypto Accelerator: AES-256, SHA-2, ECC, RSA2K, e-Fused private and public keys, attestation, ...	
I/O	GPIO	24, 4 configurable as PWM
	SPI	6 configurable
	I2C	
	UART	
	ADC	
I2S/TDM	I2S (2 interfaces) or TDM (4 channels)	
Package	DR-QFN 164	
Target Price	MCU + OS + 13 Year Azure Sphere Services < \$10	



Our silicon ecosystem



MEDIATEK

AVAILABLE NOW

MT3620

MCU form factor
Wi-Fi-enabled



NXP

COMING SOON

Part of the i.MX8 family

Optimized for performance
and power:

- Richer experiences
- Artificial Intelligence (AI)
- Graphics
- Video



QUALCOMM®

COMING SOON

Chip details to be disclosed

Built for anytime, anywhere
connectivity:

- Cellular enabled
- Support for ultra-low power scenarios

A growing network of hardware ecosystem partners (ODMs & IDHs)

- **Development kits:** Help organizations prototype quickly
- **Modules:** Speed up time to market for device makers
- **Guardian Modules:** Enable secure brownfield IoT

Azure Sphere is open

Open to any MCU manufacturer
We are licensing our Pluton security subsystem royalty **free for use** in any chip*

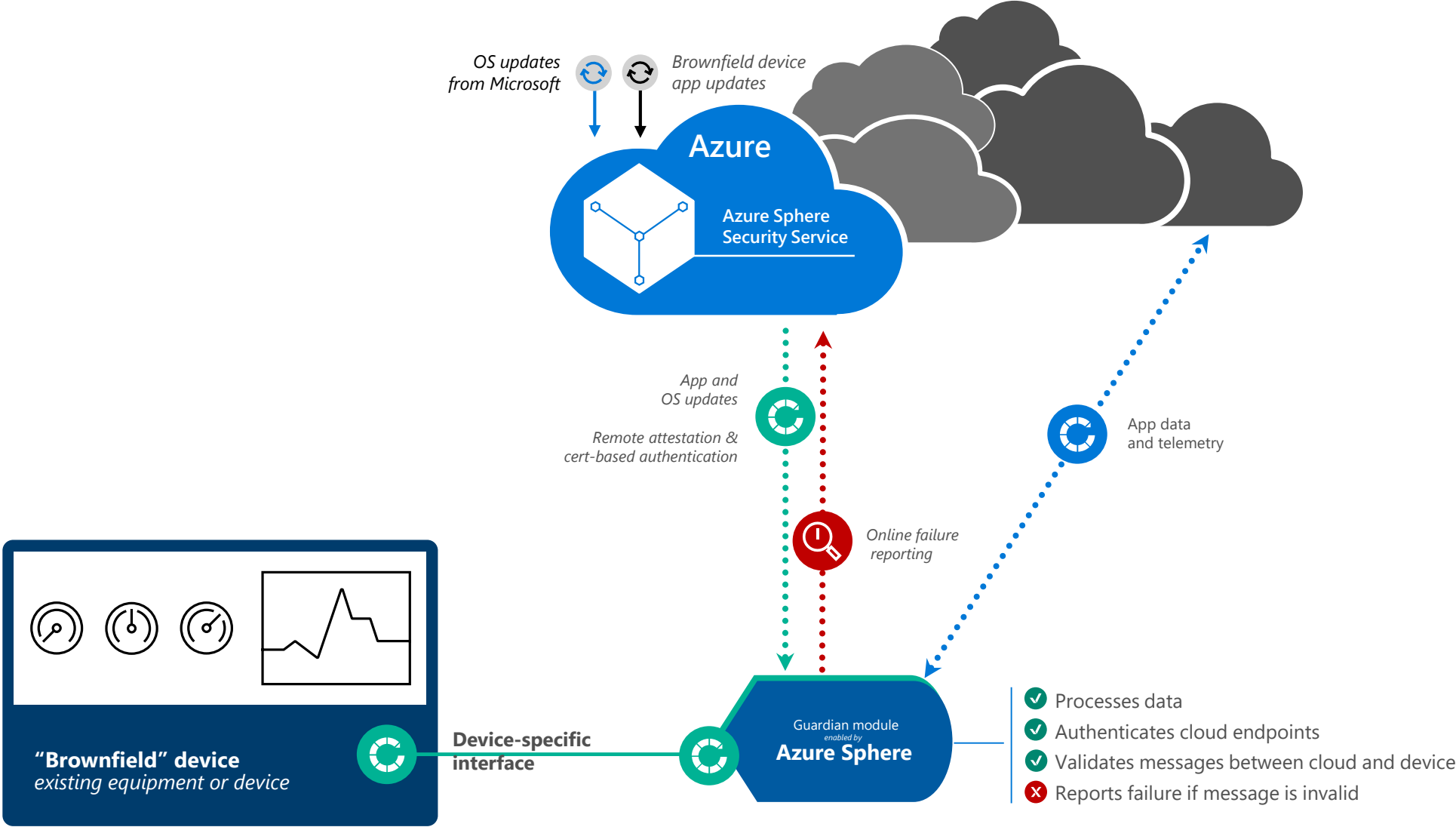
Open to any cloud
Azure Sphere devices are free to connect to Azure or any other cloud, proprietary or public for application data

Open to any innovation
MCU manufacturers are free to innovate with our GPL'd OSS Linux kernel code base

Two types of implementations

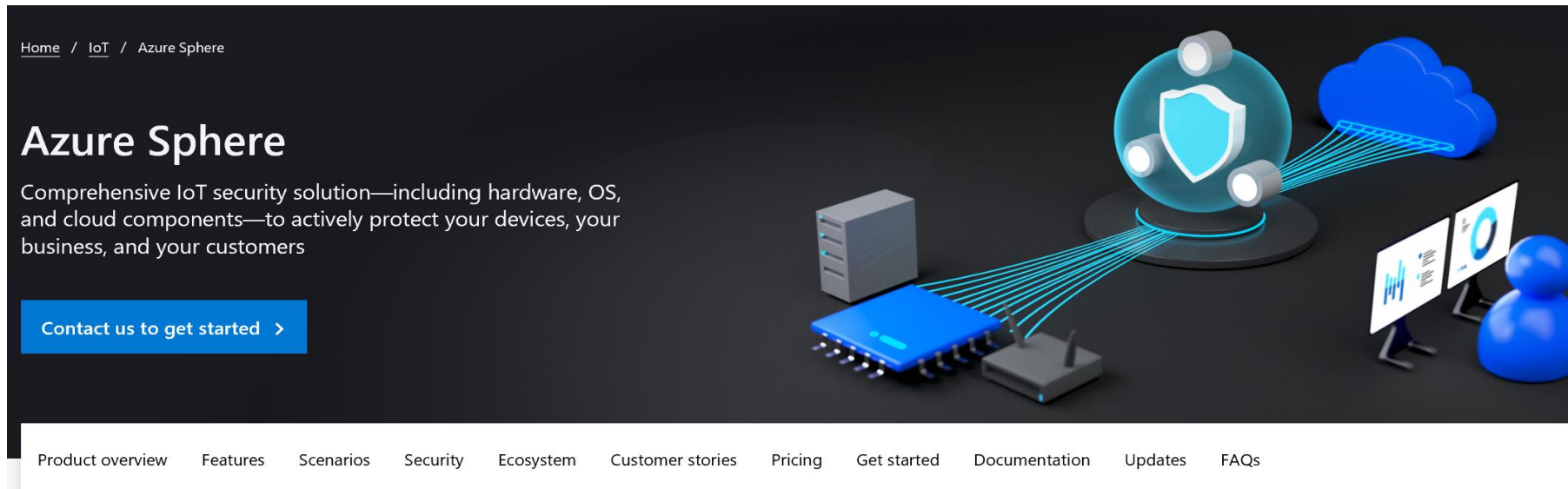


Guardian modules enabled by Azure Sphere



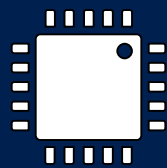
Azure Sphere Online Resources

- Azure Sphere Developer Learning Path. <https://aka.ms/azure-sphere-developer-learning-path>
- Azure Sphere Website: <https://azure.microsoft.com/en-us/services/azure-sphere/>
- Getting Started: <https://azure.microsoft.com/en-us/services/azure-sphere/get-started/>
- Documentation: <https://docs.microsoft.com/en-us/azure-sphere/>
- Hardware design reference : <https://github.com/Azure/azure-sphere-hardware-designs>



The screenshot shows the Azure Sphere website landing page. At the top left, there is a breadcrumb trail: [Home](#) / [IoT](#) / [Azure Sphere](#). The main heading is "Azure Sphere" in a large, bold font. Below it, a subheading reads: "Comprehensive IoT security solution—including hardware, OS, and cloud components—to actively protect your devices, your business, and your customers". A blue button with white text says "Contact us to get started >". To the right of the text is a 3D illustration of the Azure Sphere ecosystem, featuring a central glowing blue sphere with a shield icon, connected by lines to various hardware components like a server, a microcontroller, and a wireless module, as well as a cloud icon and a person icon. At the bottom, a navigation menu lists: [Product overview](#), [Features](#), [Scenarios](#), [Security](#), [Ecosystem](#), [Customer stories](#), [Pricing](#), [Get started](#), [Documentation](#), [Updates](#), and [FAQs](#).

Let's secure the future.



SECURED FROM THE SILICON UP