Azure Sphere
Microcontrollers (MCUs)
low-cost, single chip computers

9 BILLION new MCU devices
built and deployed every year
Fewer than 1% of MCUs are connected today.
Radio
2.4GHz WiFi

MCU
192Mhz Cortex-M4
256KB SRAM
1MB NOR FLASH
GPIO, I2C, I2S, etc.
RTOS (no kernel)
Connected devices create profoundly better customer experiences.

How does a consumer know the compressor in their fridge needs to be replaced?

Option 1
Melted ice cream

Option 2
Predictive maintenance
Opportunity  |  Risk
What happens when you connect a device to the internet?
"Ransomware attacks will target more IoT devices in 2018"

"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"

"Hacking these IoT baby monitors is child’s play, researchers reveal"

"Security experts warn of dangers of connected home devices"

"The Lurking Danger of Medical Device Hackers"

"Your smart fridge may kill you: The dark side of IoT"

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

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

"Huge IoT botnet may be used for Ukraine attack"
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
No manufacturer wants to make insecure devices

From: Hackers
To: Consumer
Subject: Your Fridge

We control your fridge.
Send us $5 in bitcoin or else...

Terrorists Ignite Thousands of House Fires with Hacked Stoves
SECURITY IS FOUNDATIONAL

It must be built in from the beginning.
The 7 properties of highly secured devices

- Hardware Root of Trust
- Defense in Depth
- Small Trusted Computing Base
- Dynamic Compartments
- Certificate-Based Authentication
- Failure Reporting
- Renewable Security
Some properties depend only on hardware support

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

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

Renewable Security

Device security renewed to overcome evolving threats

- Cloud to **Provide Updates**
- Software to **Apply Updates**
- Hardware to **Prevent Rollbacks**
Azure Sphere is an end-to-end solution for securing MCU powered devices

Azure Sphere certified MCUs, from our silicon partners, with built-in Microsoft hardware root of trust.

The Azure Sphere OS with ongoing updates creates a Microsoft-secured software platform.

The Azure Sphere Security Service guards every Azure Sphere device. It brokers trust, detects emerging threats, and renews device security.
Azure Sphere certified MCUs 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 for the first time
The Azure Sphere OS is optimized for IoT, security, and agility

**Secure Application Containers**
Compartmentalize code for agility, robustness & security

**On-chip Cloud Services**
Provide update, authentication, and connectivity

**Custom Linux kernel**
Empowers agile silicon evolution and reuse of code

**Security Monitor**
Guards integrity and access to critical resources

<table>
<thead>
<tr>
<th>Azure Sphere OS Architecture</th>
</tr>
</thead>
<tbody>
<tr>
<td>OS Layer 4</td>
</tr>
<tr>
<td>OS Layer 3</td>
</tr>
<tr>
<td>OS Layer 2</td>
</tr>
<tr>
<td>OS Layer 1</td>
</tr>
<tr>
<td>Hardware</td>
</tr>
</tbody>
</table>
The 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.
Modernize MCU development with Azure Sphere and Visual Studio

Simplify development
Focus your device development effort on the value you want to create.

Streamline debugging
Experience interactive, context-aware debugging across device and cloud.

Collaborate across your team
Apply tool-assisted collaboration across your entire development organization.
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
Azure Sphere is open
SECURITY
Peace of mind

PRODUCTIVITY
Faster time to market

OPPORTUNITY
The future is now
Get started with Azure Sphere today.

**Public Preview availability**
Azure Sphere OS
Azure Sphere Security Service
Visual Studio tools for Azure Sphere

**Available Now**
Azure Sphere development kits from Seeed studios

For more information visit: [www.microsoft.com/AzureSphere](http://www.microsoft.com/AzureSphere)
Let’s secure the future.

SECURED FROM THE SILICON UP