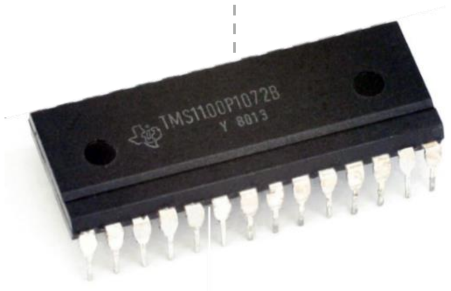
Azure Sphere Overview

Martin Grossen
Director Embedded Software and Cloud
Martin.Grossen@Avnet.com
Microsoft MVP

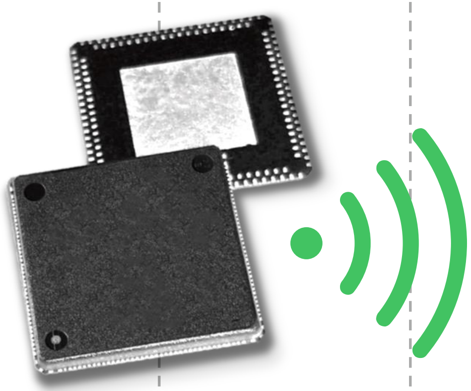
AVNET® SILICA

Prepare for the 2nd wave of Digital Transformation…



2018: 9 BILLION new MCU devices built and deployed every year. Over 85% have network connectivity.

Today: Fewer than 1% of existent MCUs designs are connected…



Wave 1:
The Microcontroller (MCU)

Wave 2:
Internet Connectivity

1970's	1980's	1990's	2000's	2010's	2020's	2030's

“Ransomware attacks will target more IoT devices in 2022”

“Huge IoT botnet may be used for Ukraine attack”

“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”

“Security experts warn of dangers of connected home devices”

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

“Hackers infect 500,000 consumer routers all over the world with malware”

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

“The Lurking Danger of Medical Device Hackers”

“Why the KRACK Wi-Fi mess will take decades to clean up

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

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

Mirai Botnet attack

October 2016

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

(The Guardian, 2016)

Context matters

April 2018

Attackers gain access to casino database through fish tank

Entry point was a connected thermometer

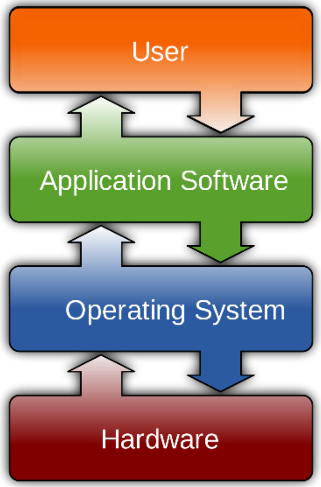
Once in, other vulnerabilities were exploited

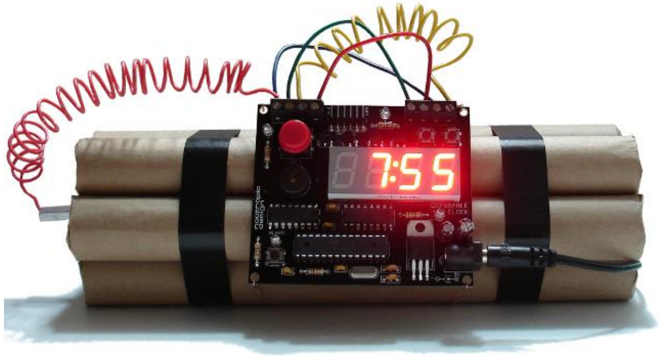
Gained access to high-roller database

(Business Insider, 2016)

Example: Gas Heating

- Number of gas heatings in Germany 2016: 7.8 Mio.
- Ireland 2016: 34% of all houses were heated by gas.





Difference between the product and a bomb is only software!
Open gas valve, wait 5 minutes, then ignite….

The internet security battle

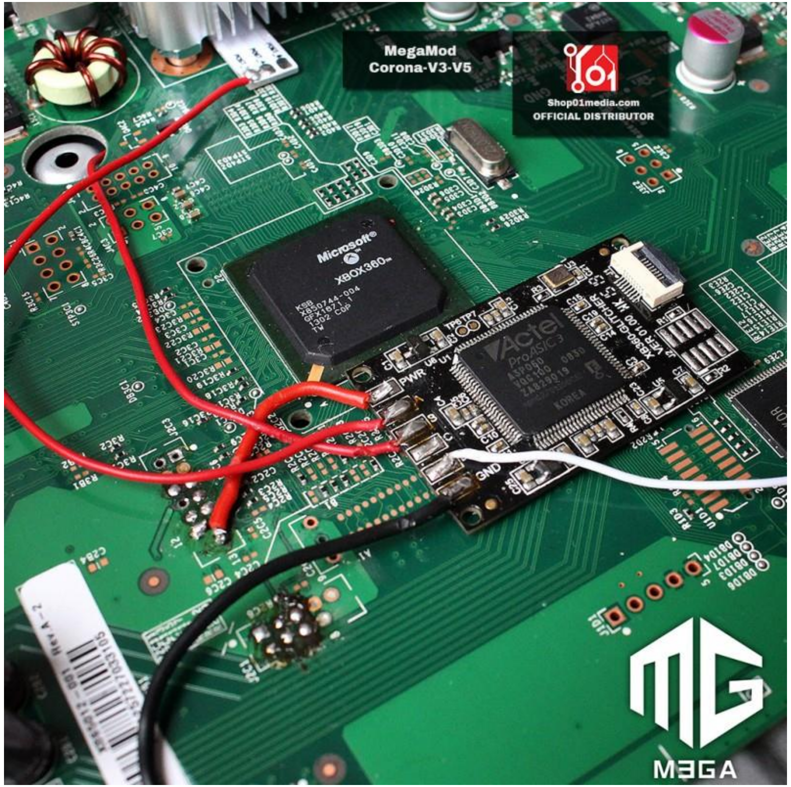
Microsoft has been fighting it for decades so they have some experience to share.
Also on hardware side!

<u>**Example XBox:**</u>

XBox: Hacked within weeks
-> Standard Intel x86 system

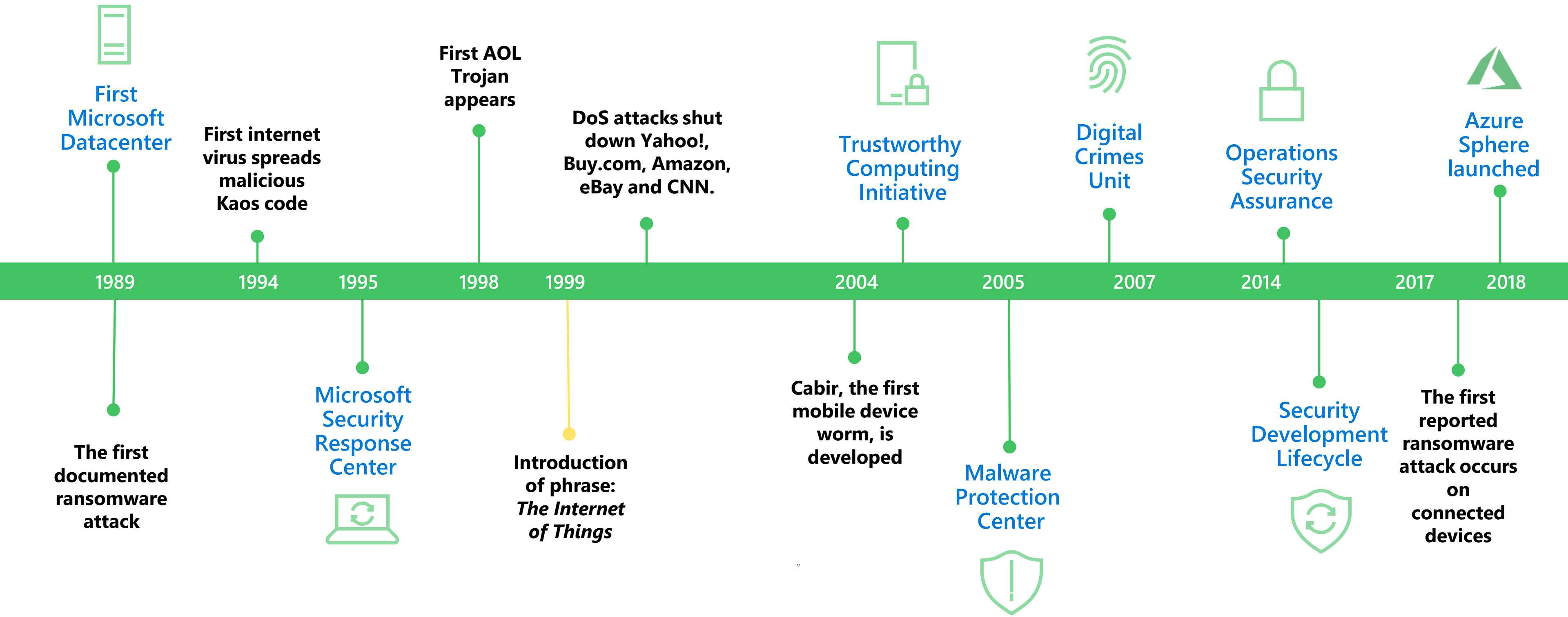
XBox 360:Hacked within 3,5 month
-> HW hack to compromise the bus:

XBox One: Not hacked until today
-> also thanks to in-chip bus firewalls



A long history of trustworthy computing

Microsoft has more than 25 years experience protecting customers and their devices



1989

First Microsoft Datacenter

The first documented ransomware attack

1994

First internet virus spreads malicious Kaos code

1995

Microsoft Security Response Center

1998

First AOL Trojan appears

1999

Introduction of phrase: *The Internet of Things*

DoS attacks shut down Yahoo!, Buy.com, Amazon, eBay and CNN.

2004

Cabir, the first mobile device worm, is developed

Trustworthy Computing Initiative

™

2005

Malware Protection Center

2007

Digital Crimes Unit

2014

Operations Security Assurance

Security Development Lifecycle

2017

The first reported ransomware attack occurs on connected devices

2018

Azure Sphere launched

Microsoft Security Response Center (MSRC)

- Microsoft Security Response Center with a team of 3´500 cybersecurity specialists is working 24/7 to protect, detect and respond to the world`s cyber attacks: MSRC - Microsoft Security Response Center

Highly-secured connected devices require 7 properties

Hardware Root of Trust

▦

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

Defense in Depth

▦ ⚙

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

Small Trusted Computing Base

▦ ⚙

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

Dynamic Compartments

▦ ⚙

Can your device's security protections improve after deployment?

Certificate-Based Authentication

▦ ⚙ ☁

Does your device use certificates instead of passwords for authentication?

Failure Reporting

▦ ⚙ ☁

Does your device report back about failures and anomalies?

Renewable Security

▦ ⚙ ☁

Does your device's software update automatically?

▦ = Silicon support required ⚙ = OS support required ☁ = Cloud Service support required

http://aka.ms/7properties

AVNET SILICA

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

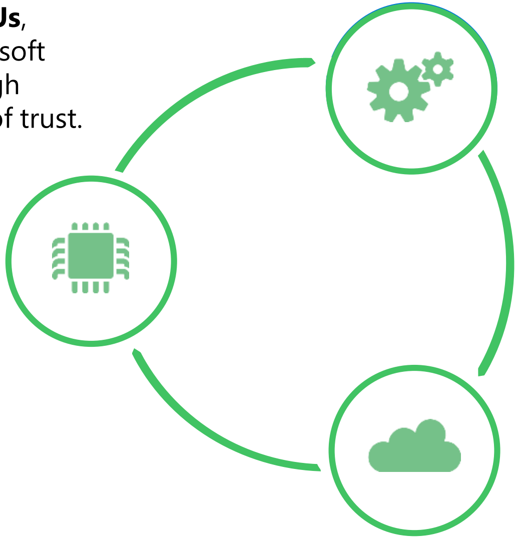
Device security renewed to overcome evolving threats

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

Azure Sphere is an end-to-end solution for creating highly-secured, connected MCU devices

Secured **MCUs**

A new class of crossover **Azure Sphere MCUs**, from our silicon partners, with built-in Microsoft security technology provide connectivity, high performance, and a secured hardware root of trust.



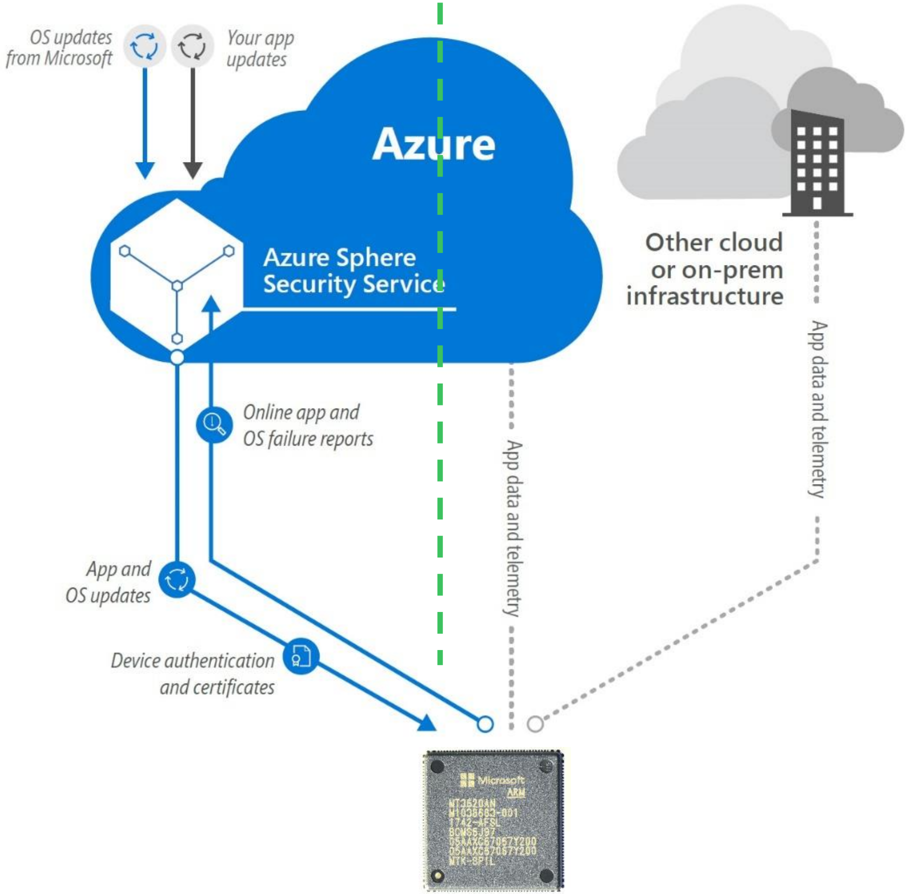
Secured **Operating System**

The highly-secured **Azure Sphere IoT OS** combines the best of Microsoft and OSS technologies to create **a trustworthy platform** for new IoT experiences

Secured by our **Cloud Service**

The **Azure Sphere Security Service** guards every Azure Sphere device; it **protects** your devices and customers, **detects** emerging threats, and proactively **responds**.

Azure Sphere Cloud Security Service


OS updates from Microsoft
Your app updates
Azure
Azure Sphere Security Service
Other cloud or on-prem infrastructure
App data and telemetry
App data and telemetry
Online app and OS failure reports
App and OS updates
Device authentication and certificates
Microsoft
ARM
MT3620AN

The Azure Sphere Security Service guards every Azure Sphere device. It renews security, identifies emerging threats, and brokers trust between device, cloud, and other endpoints.

- Protecting devices with certificate-based authentication
- Guaranteeing device authenticity and running only your genuine software
- Getting insight into device and application
- failure and visibility into emerging threats
- Deploys app updates to your Azure Sphere powered devices

Azure Sphere Silicon Partners to implement the Pluton Security Core

Microsoft is working with other suppliers to implement the Azure Sphere Pluton Security Core into their HW:

MediaTek

ARM

STMicroelectronics

NXP

Silicon Labs

Nordic

Nuvoton

Hilscher

Toshiba

VeriSilicon

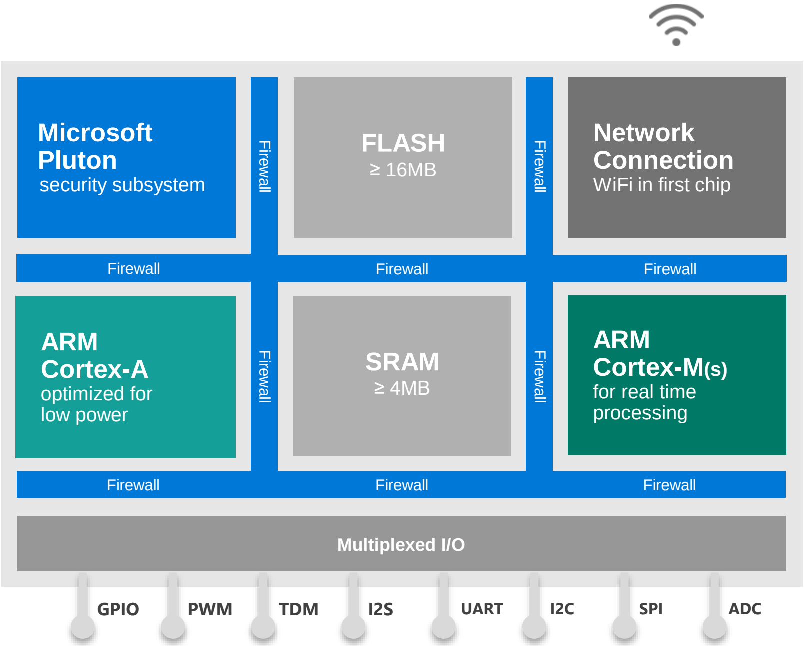
Qualcomm

Azure Spheres MCU’s - Create a secured foundation for intelligent edge devices

- Secured
  - With built-in Microsoft security technology
  - i.e. I/O bus firewalls
  - including the Pluton Security Subsystem

- Performance
  - With built-in Cortex-A processors
  - Delivers significantly greater performance vs. similar traditional MCU

- Connected
  - With built-in networking



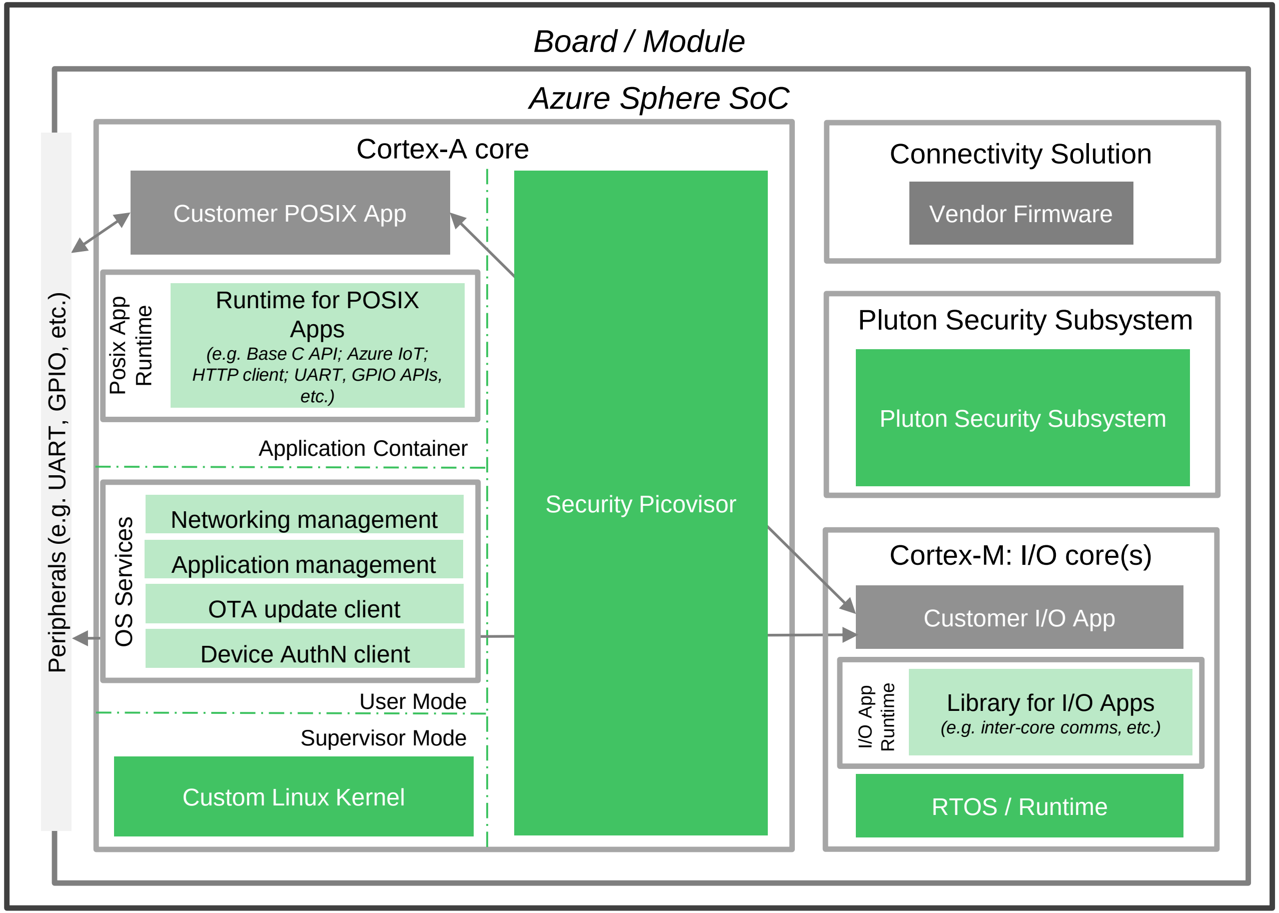
Azure Sphere OS: Basic Architecture

Developer Experience
(on PC)

- Visual Studio Integration
- Azure Sphere SDK
- Azure Sphere Device Communication Service

Architectural Layers

- Customer Applications
- OS Services
- Custom Linux Kernel
- Picovisor & Firmware



Board / Module

Azure Sphere SoC

Peripherals (e.g. UART, GPIO, etc.)

Cortex-A core

Customer POSIX App

Posix App Runtime

Runtime for POSIX Apps
(e.g. Base C API; Azure IoT; HTTP client; UART, GPIO APIs, etc.)

Application Container

OS Services

- Networking management
- Application management
- OTA update client
- Device AuthN client

User Mode

Supervisor Mode

Custom Linux Kernel

Security Picovisor

Connectivity Solution

Vendor Firmware

Pluton Security Subsystem

Pluton Security Subsystem

Cortex-M: I/O core(s)

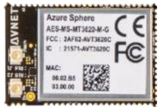
Customer I/O App

I/O App Runtime

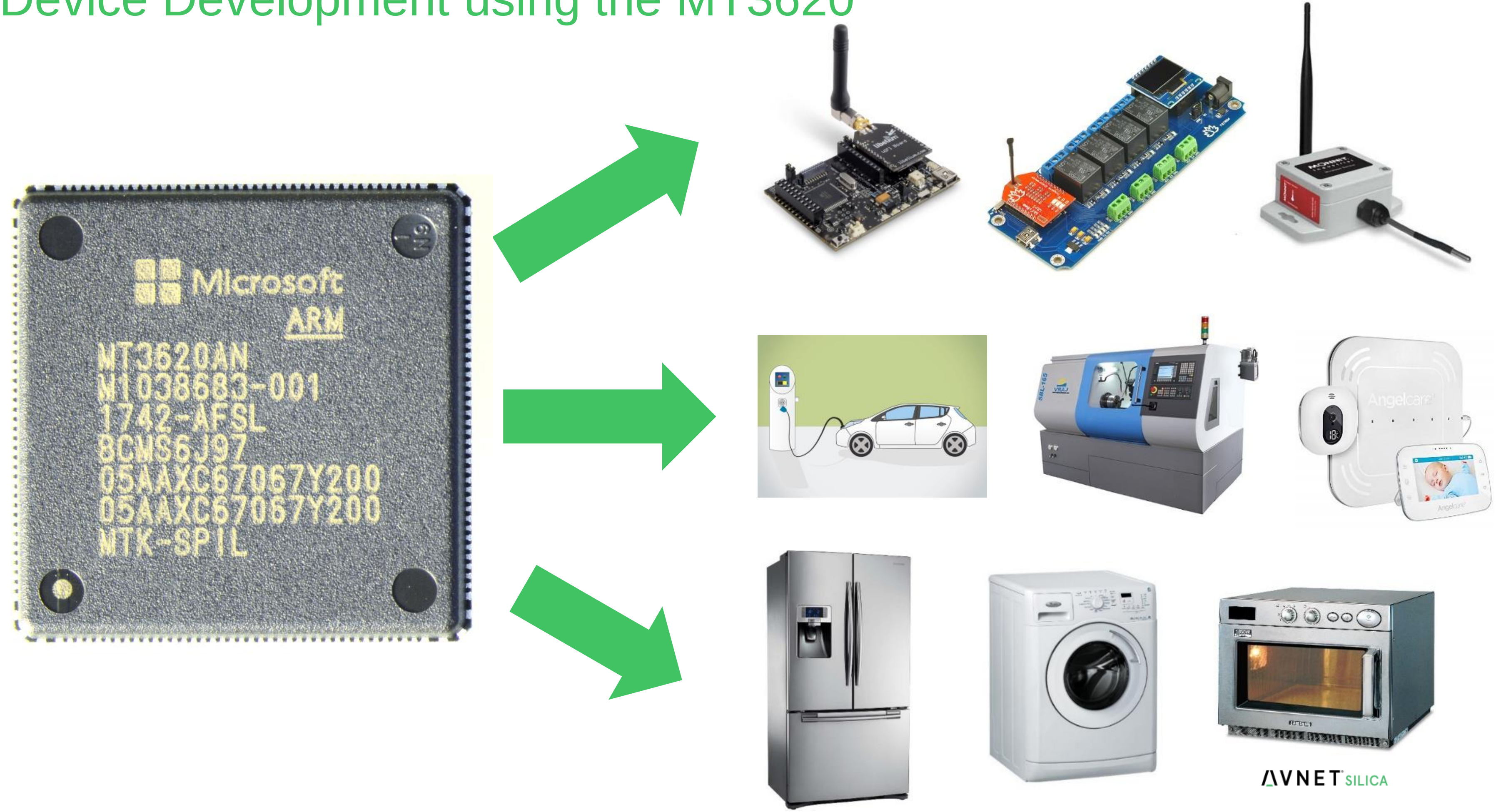
Library for I/O Apps
(e.g. inter-core comms, etc.)

RTOS / Runtime

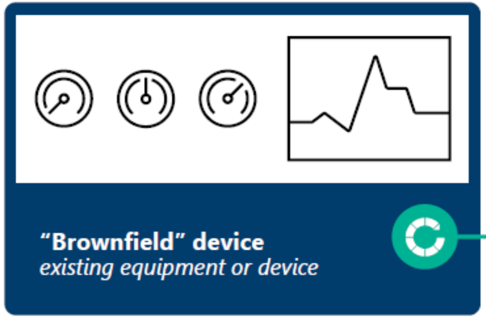
Avnet’s Sphere Product Roadmap

Chip	Module	Starter Kit	Guardian	
Targeting higher volume (>50K) applications	Certified and production ready for quick time to market	Eases prototyping and PoC development with expansion and add-ons	Production ready, Sphere-based system with enclosure for quick deployment. Off-the-shelf or customizable to meet exact application needs.	Target Applications
Available Now **MT3620 Sphere MCU** - Arm Cortex A7 MPU with 4MB SRAM - Dual M4F MCUs with 64KB SRAM each - Dual band b/g/n WiFi - Up to 5 ISU interfaces configurable as UART, I2C, or SPI ports - Up to 72 GPIOs - PWM, I2S, ADC, RTC	Available Now **Chip Antenna Module** - Based on the MT3620 - Dual band b/g/n Wi-Fi - Chip antenna - Three ISU interfaces - 33 x 22 x 3 mm	Available Now **MT3620 Starter Kit** - Based on the MT3620 Chip Antenna Module - Two MikroE Click Board expansion slots - Five on-board sensors - Optional OLED port - I2C Grove connector - User push buttons - User LEDs - USB powered	 Available Now **Guardian 100** - WiFi Uplink - Ethernet Up or Downstream - USB-UART Downstream	- Machine monitoring/control - Asset monitoring - IoT Appliances - Predictive Maintenance - HVAC and Refrigeration - Food Services
			   Available Now **Cellular Guardian (from Qiio)**	- Smart Retail - Smart City - Smart Agriculture - Factory Automation - Building Automation - ….
Coming H1 ‘22 Under Development **NXP Sphere MCU** - i.MX8ULP based	Available Now  **External U.FL Antenna** - Based on the MT3620 - Dual band b/g/n Wi-Fi - TX/RX Ant. Diversity - U.FL connectors - Three ISU interfaces - 33 x 22 x 3 mm		Under Development Coming 2021 **Other partner Guardian solutions will follow**	- M.2 Socket - BT LE - Lora / Sigfox - ….

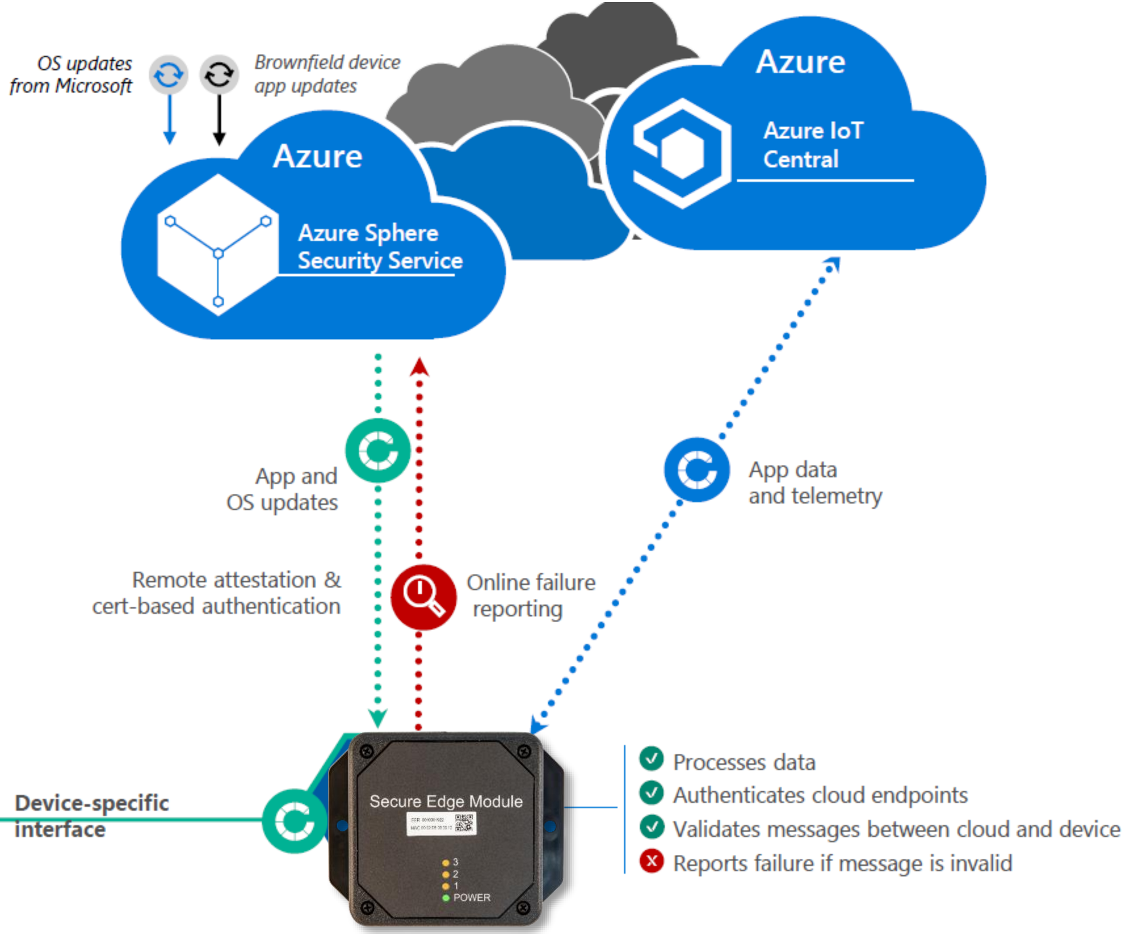
Device Development using the MT3620



Securing Brownfield Devices with Azure Sphere



“Brownfield” device
existing equipment or device



OS updates from Microsoft

Brownfield device app updates

Azure

Azure Sphere Security Service

Azure

Azure IoT Central

App and OS updates

Remote attestation & cert-based authentication

Online failure reporting

App data and telemetry

Device-specific interface

Secure Edge Module

- ✓ Processes data
- ✓ Authenticates cloud endpoints
- ✓ Validates messages between cloud and device
- ✗ Reports failure if message is invalid

Example: StartUp Partnership Qiio / Avnet / Microsoft

Qiio: https://qiio.com

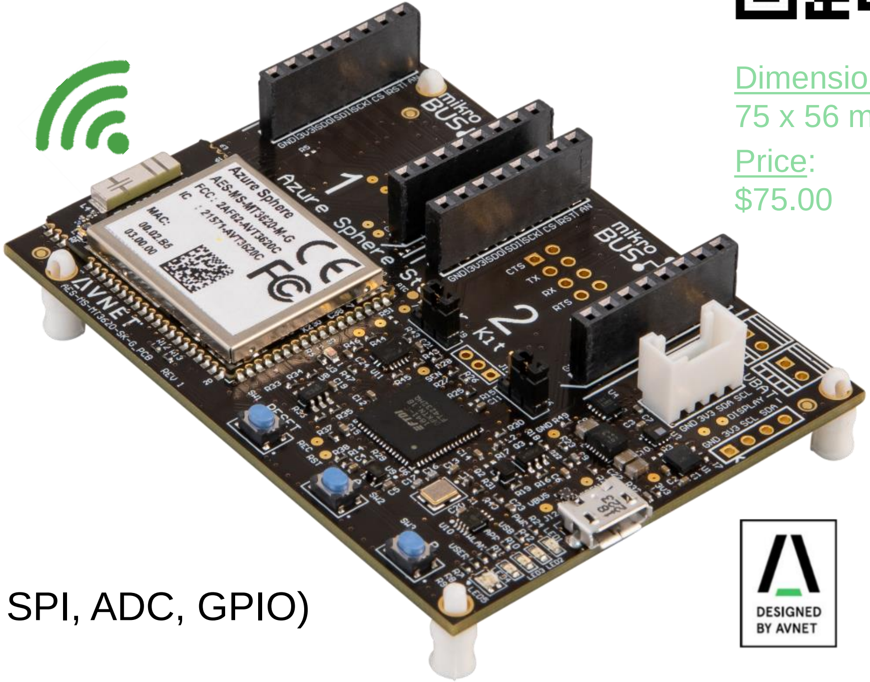
partner ••

We work with partners to create solutions that work for your business.

Microsoft AVNET Reach Further® /IOTCONNECT® Partner Program swisscom ERICSSON

Avnet Sphere Starter Kit

- Avnet MT3620 Azure Sphere Module
  - Dual-band 2.4GHz/5GHz chip antenna
  - 32kHz XTAL for RTC and LP operation
- 4-Port USB-to-Serial Bridge (FT4232HQ)
  - Service-, Debug- and Recovery UARTs
  - SWD interface, Recovery and Reset
- Multiple Onboard Sensors
  - Accelerometer, Gyro, Temperature
  - Barometric Pressure (Elevation)
  - Ambient light sensor
- Multiple Expansion Ports
  - 2x mikroBUS Click sockets (UART, I2C, SPI, ADC, GPIO)
  - 1x Grove connector (I2C)
  - 1x OLED 128x64 display (I2C) *-not fitted*
  - 1x Pmod connector (UART, GPIO) *-not fitted*



Dimensions:
75 x 56 mm

Price:
$75.00

DESIGNED BY AVNET

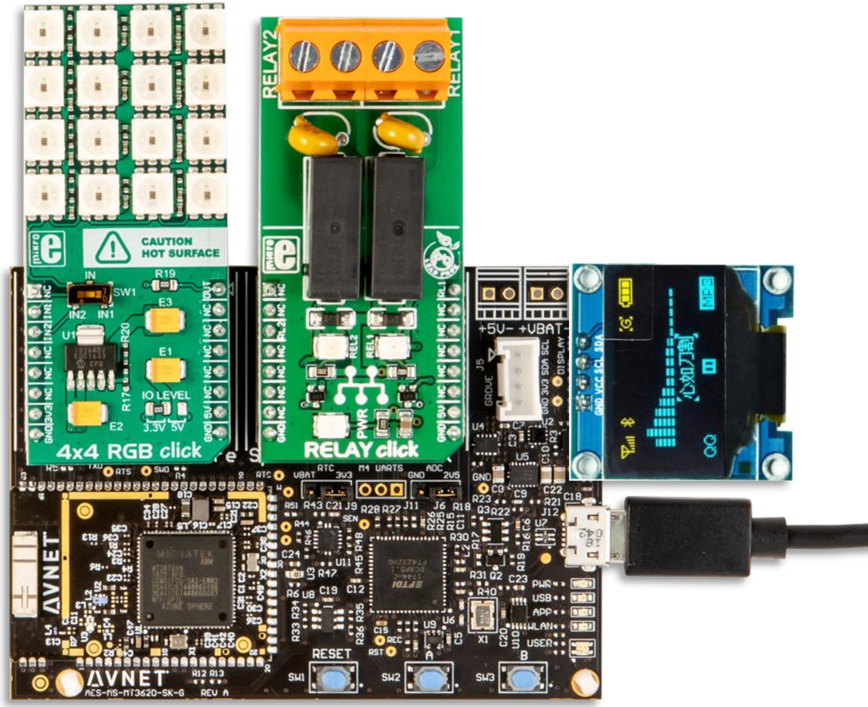
http://avnet.me/mt3620-kit

Starter Kit Expandability

- **MikroE Click boards** - www.mikroe.com/click
  - Starter Kit has two Click board sockets
  - 750+ different Click boards now available!

- **Grove Connector**
  - Now hundreds of Grove boards - link
  - Cable interface adds flexibility
  - 4-pin connector with I2C interface

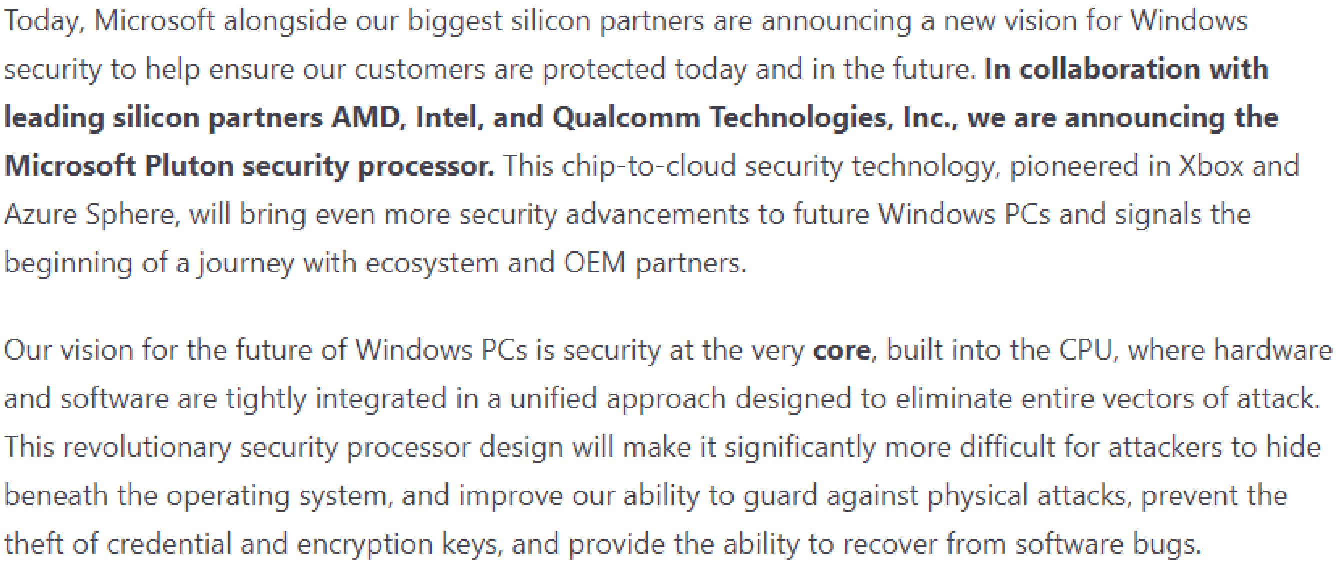
- **OLED Display Interface**
  - Easy addition of <u>optional</u> graphic display
  - Many sub-$10 OLED 128x64 graphic display options available - link



http://avnet.me/mt3620-kit

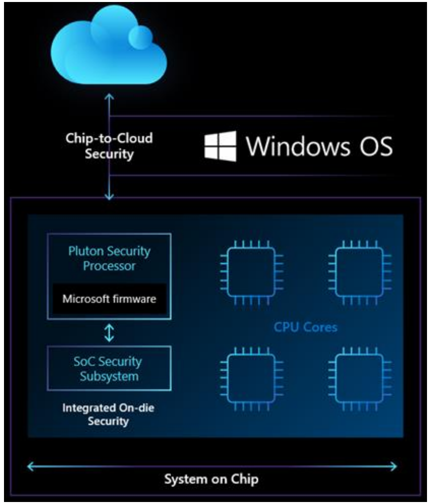
Other Silicon Partners to implement Pluton Security Core

Announcement 17th of November 2020:

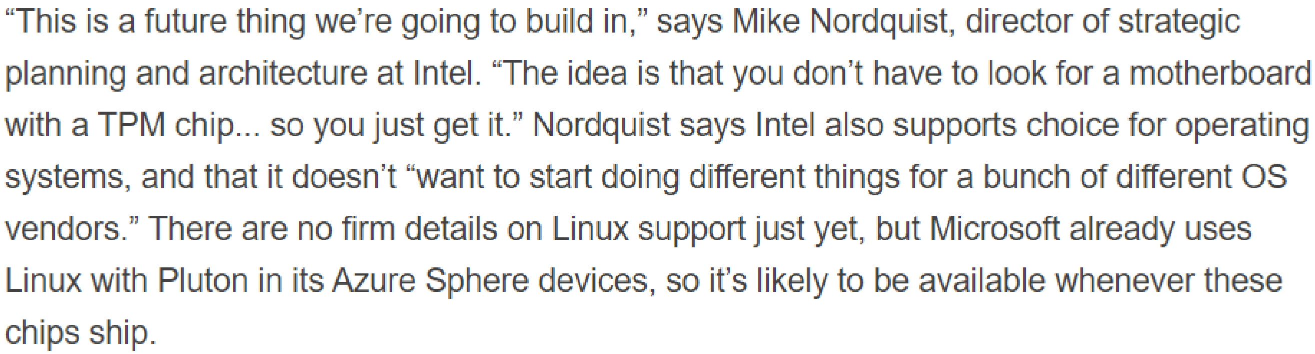


Today, Microsoft alongside our biggest silicon partners are announcing a new vision for Windows security to help ensure our customers are protected today and in the future. **In collaboration with leading silicon partners AMD, Intel, and Qualcomm Technologies, Inc., we are announcing the Microsoft Pluton security processor.** This chip-to-cloud security technology, pioneered in Xbox and Azure Sphere, will bring even more security advancements to future Windows PCs and signals the beginning of a journey with ecosystem and OEM partners.

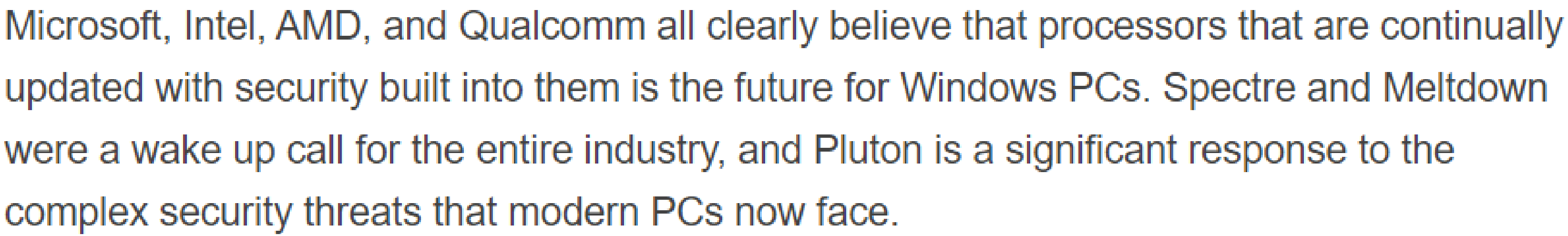
Our vision for the future of Windows PCs is security at the very **core**, built into the CPU, where hardware and software are tightly integrated in a unified approach designed to eliminate entire vectors of attack. This revolutionary security processor design will make it significantly more difficult for attackers to hide beneath the operating system, and improve our ability to guard against physical attacks, prevent the theft of credential and encryption keys, and provide the ability to recover from software bugs.



Other Silicon Partners to implement Pluton Security Core



“This is a future thing we’re going to build in,” says Mike Nordquist, director of strategic planning and architecture at Intel. “The idea is that you don’t have to look for a motherboard with a TPM chip... so you just get it.” Nordquist says Intel also supports choice for operating systems, and that it doesn’t “want to start doing different things for a bunch of different OS vendors.” There are no firm details on Linux support just yet, but Microsoft already uses Linux with Pluton in its Azure Sphere devices, so it’s likely to be available whenever these chips ship.



Microsoft, Intel, AMD, and Qualcomm all clearly believe that processors that are continually updated with security built into them is the future for Windows PCs. Spectre and Meltdown were a wake up call for the entire industry, and Pluton is a significant response to the complex security threats that modern PCs now face.

Thank you!!!

Martin Grossen
Director Embedded Software and Cloud
Martin.Grossen@Avnet.com
Microsoft MVP

AVNET® SILICA