INTEL® INDUSTRIAL IOT WORKSHOP

SECURITY FOR INDUSTRIAL PLATFORMS

Gopi K. Agrawal
Security Architect
IOTG Technical Sales & Marketing
Intel Corporation

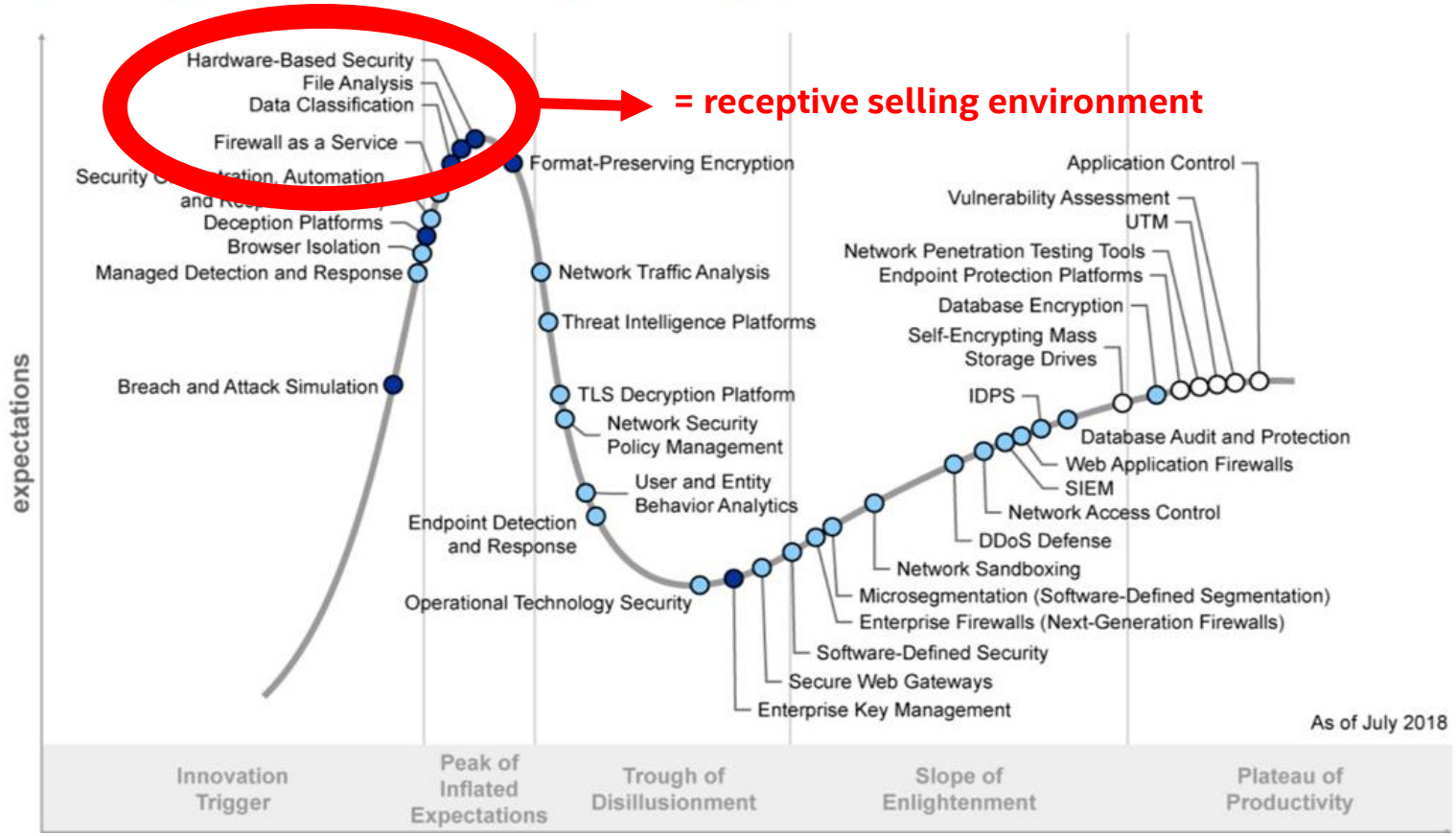
Legal

Agenda

- Learn more about the prevailing Threat environment & top market concerns, Intel Core Security Capabilities-HW Root of Trust capabilities & technologies, IoT Security Lifecycle, and use-cases.
- Overview of hardware-based solutions to address the increasing need for security and manageability as Industrial IOT is evolving into new and more demanding uses that challenge existing practices.

HW Security is a Key Element to Scale IoT Deployments

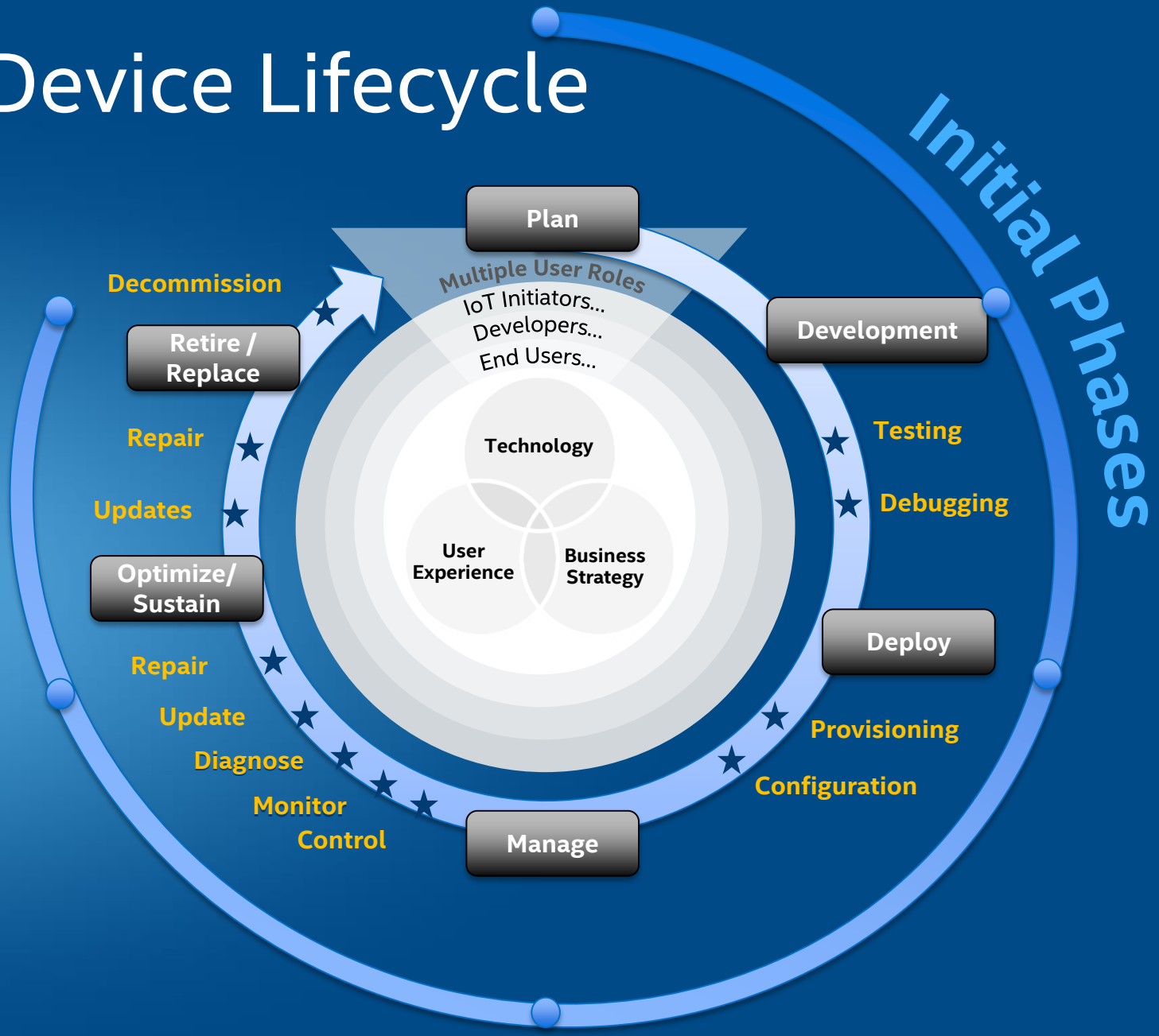
Figure 1. Hype Cycle for Threat-Facing Technologies, 2018



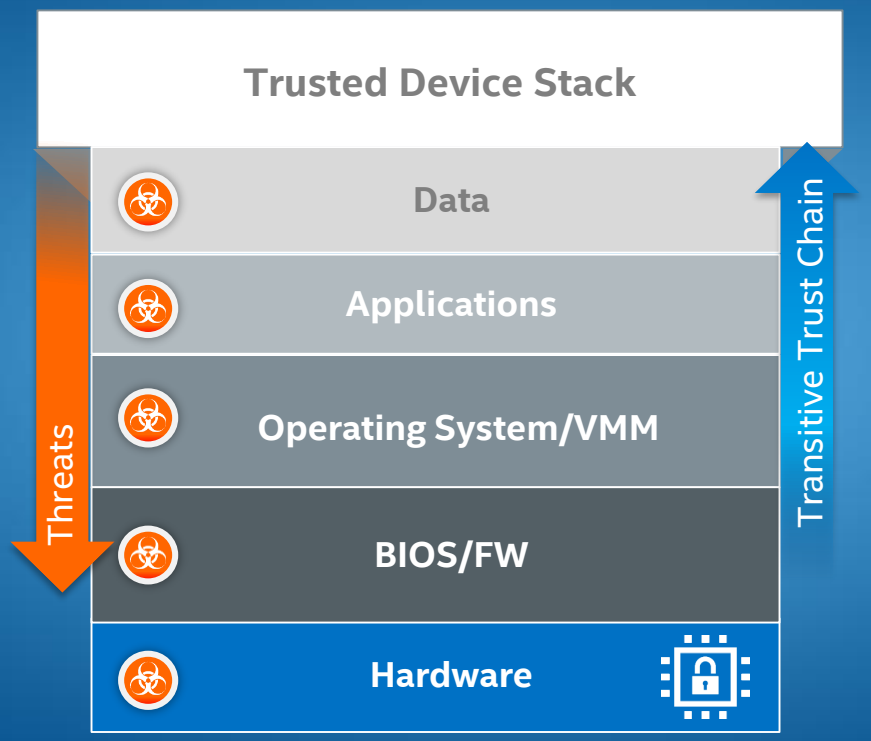
Source - Gartner

Uniqueness of IoT Device Lifecycle

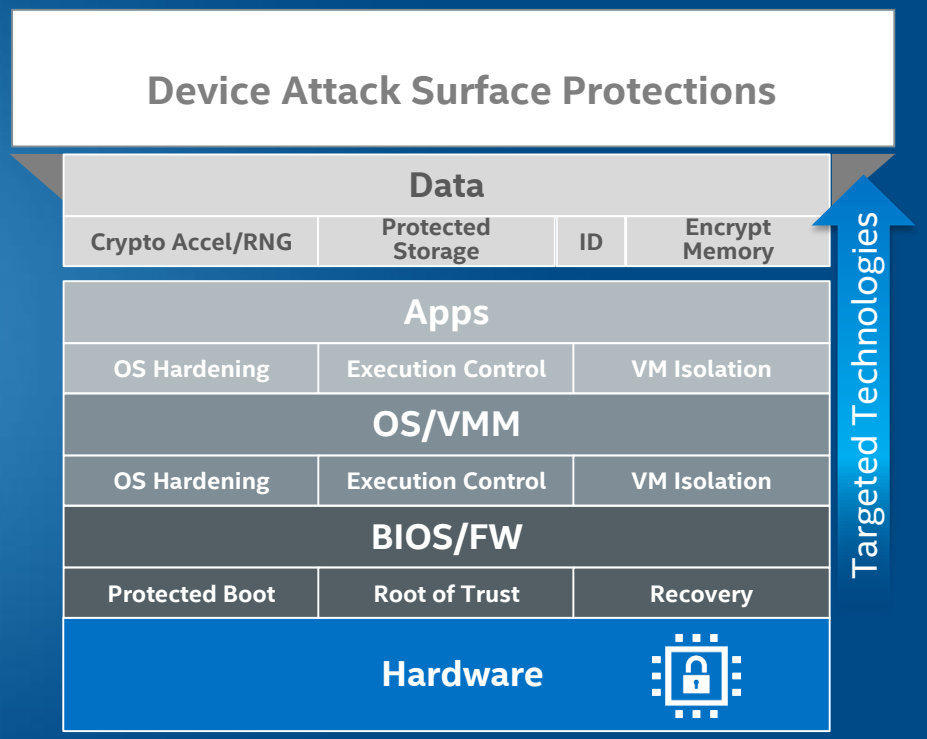
- IoT Device usage mode implies 10+ years life time, longer than Client & Server traditional products
- Security is intrinsic to each stage of device lifecycle
- Intel has assets to help protect customer's assets in all phases



HW Instruments Software with Added Protections



Hardware Security Makes Entire System More Secure



Hardware Technologies Designed to Harden Specific Attack Surfaces

Consistent Security Foundation

What is it?

- Set of foundational security capabilities that **must** be supported at **platform level**.
- Recommended set of technologies for each capability.

Why?

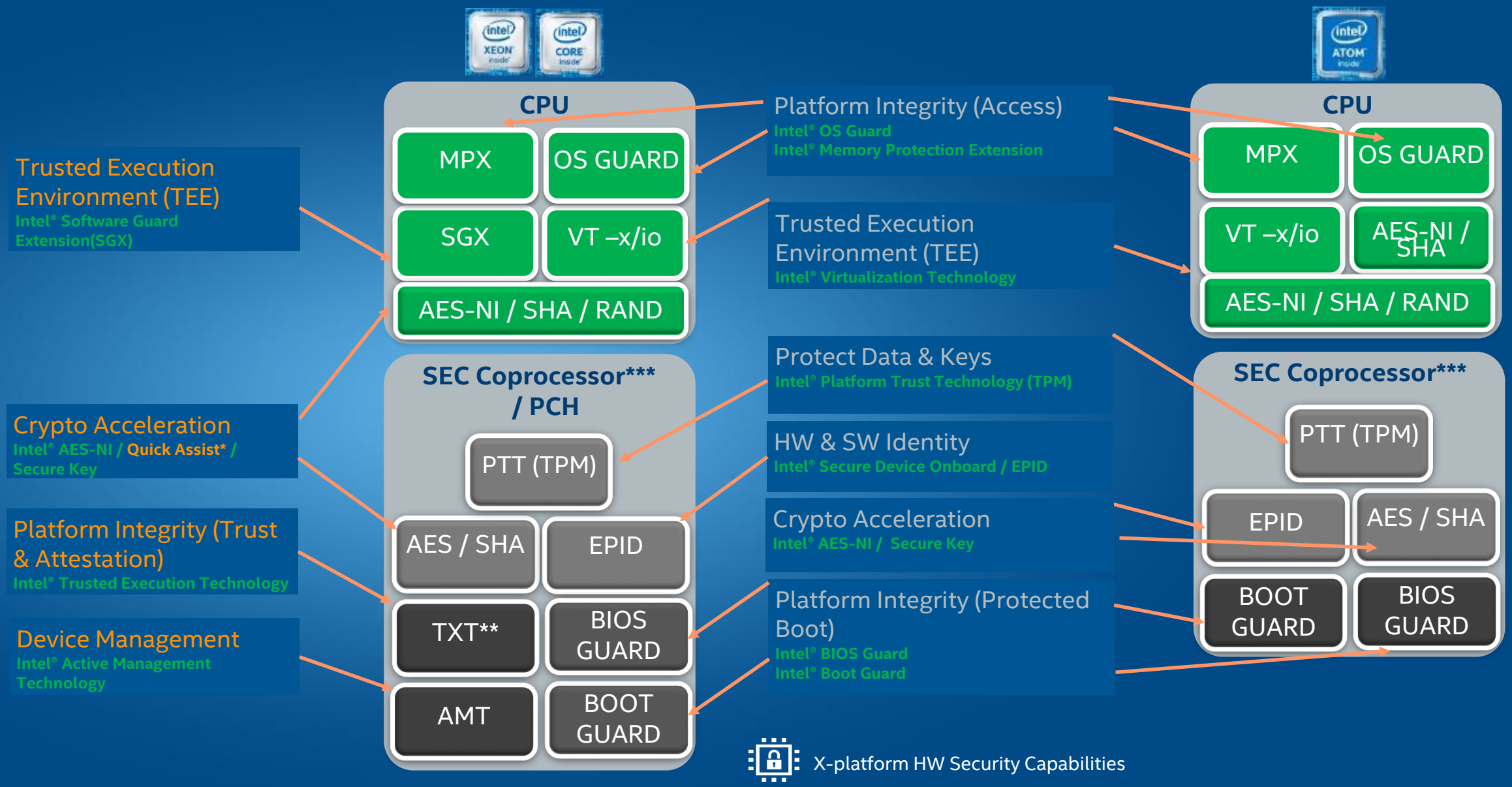
- Enable common security posture on all platforms.
- Promote reuse and consistency in Intel security solutions.

Enables for the evolving IoT markets

Portfolio Definitions

	Core Capability	Value Prop Achieved	Industry Technologies	Map to Intel Technologies
	Crypto Acceleration	Hardware-assisted crypto acceleration and secure key generation	Encryption /Decryption Random Keys	AES-NI, Quick Assist Secure Key
Baseline	Platform Integrity	Protected and verified boot process with hardware attestation of the platform	OS/VMM Hardening	OS Guard, VT-d/x
			Device Identification	PTT (TPM, measured boot, RSA/EDCSA Key Support)
			Software Identification	
			Protected Boot	Boot Guard, OS Guard)
	Protected Data & Keys, & Identity	Encryption and storage for sensitive data, keys, or credentials, at rest and in transport	Protected Storage	PTT, TME (future)
	Trusted Execution	Isolated enclaves to help protect sensitive data, processes, and keys at runtime and create a trusted application environment	Trusted Execution Environment (TEE)	SGX, DAL, VT -x

Security & Management Technologies[1] - Hardware



[1] Subset of intel security technologies Specific to Industrial & Energy

* Intel® Quick Assist Xeon only

**Intel® TXT vPro and Xeon only

***Intel® CSME / TXE / CSE/ SPS

Securing Devices & Communication

Threats

Sensitive Data Protection
Unauthorized access of app data due to week OS security

Credential / Provisioning
Attacker can gain unauthorized access to the device with little effort

Escalation of Privilege / Ransom Ware
Using device vulnerable known software exploit

Insecure Key Storage
cryptographic keys used to protect platform a owner secrets easily recovered by hacker

Insecure Data-in-Transit
Sending data in clear increases eavesdropping risks

Unsigned Firmware / Rootkit
Modification Of Firmware By Malware

Unauthorized BIOS Write
Unprotected BIOS leaves device vulnerable to known exploit

Hardware limitations
Limited security options availability

Applications

Other Drivers

Operating System (Window & Linux)

Boot Drivers

BIOS

Hardware

Solutions

Intel® Software Guard Extension(SGX)*
Trusted Execution Environment (TEE) for Embe Applications, app run time protection

Intel® Secure Device Onboard / EPID
Provides service that uses HW key to secure the rendezvous of device to its owner

Intel® OS GUARD / MPX / VT-x
Prevent escalation of privilege, boundary protection, utilize VT / containers

Intel® Platform Trust Technology (TPM)
Enable secure PKI keys storage

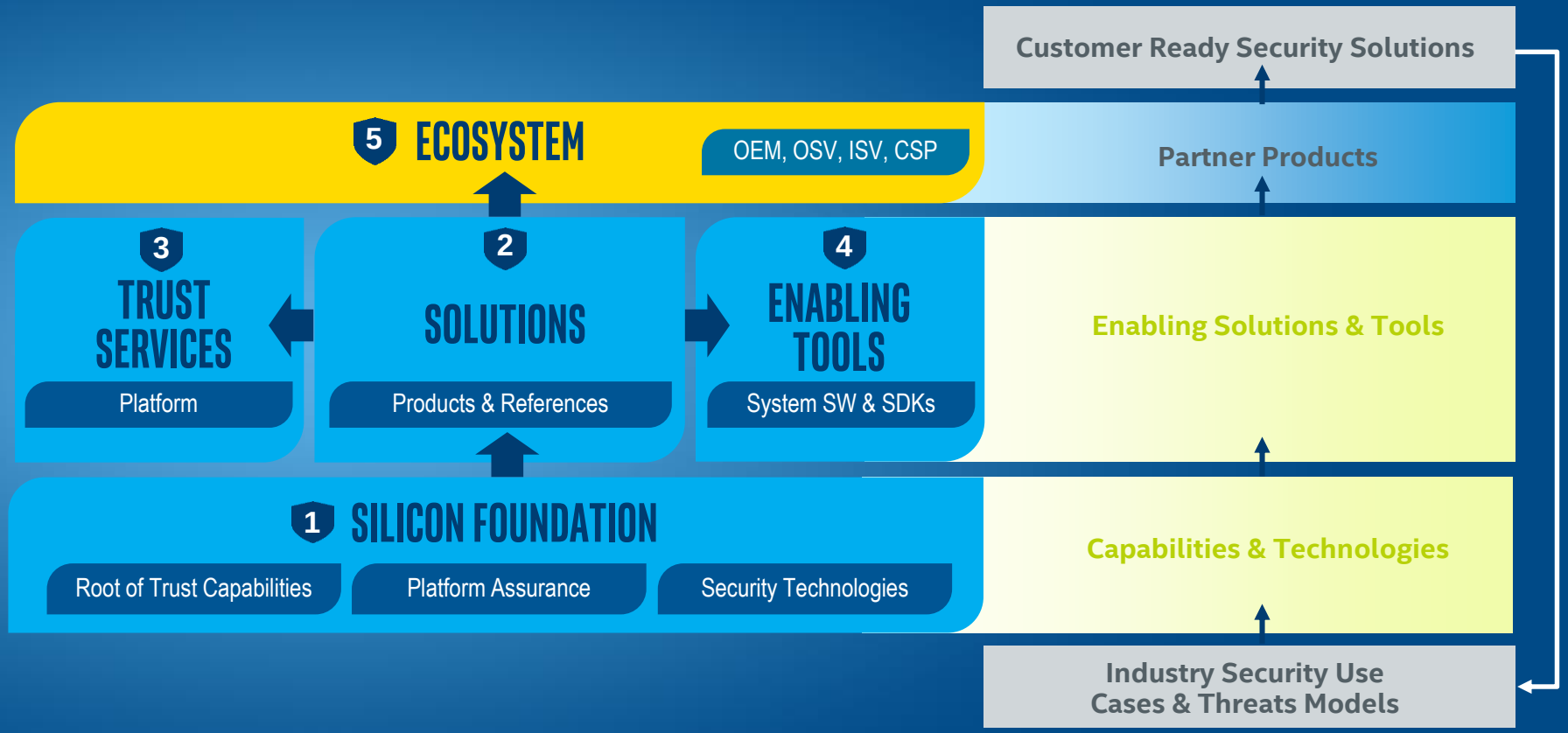
Intel® AES-NI/Quick Assist / Secure Key
Enable TLS/SSL ops without compromising performance

Intel® Boot Guard / Intel® TXT*
Allows only trusted & untampered firmware to execute

Intel® BIOS Guard
Signed OEM Secure bios update

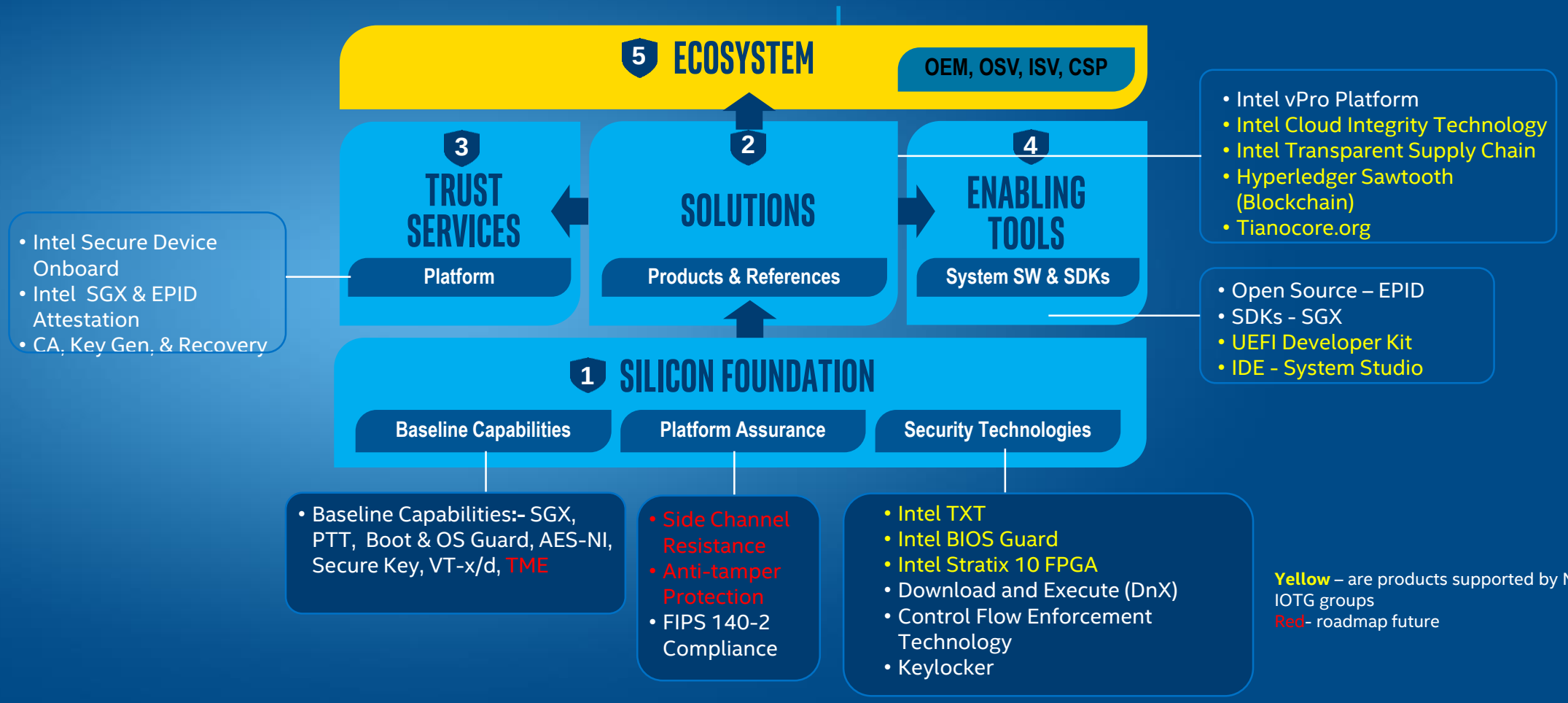
*SGX & TXT supported only on Xeon & Core

Security Products Delivery Model



Intel provides comprehensive edge to cloud security solutions rooted in HW security that the ecosystem turns into customer ready solutions

Security Products Delivery Model

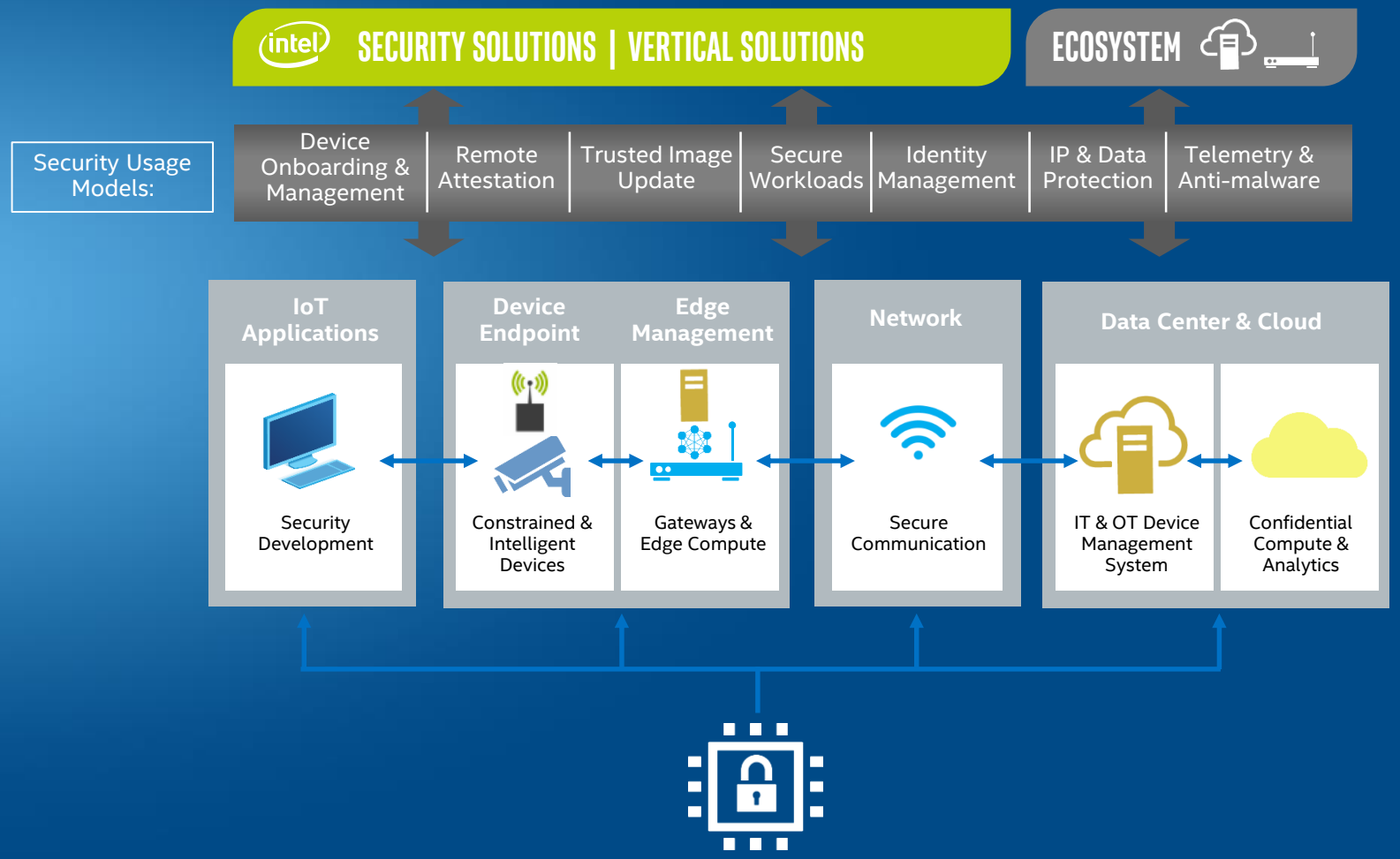


Yellow – are products supported by Non IOTG groups
Red- roadmap future

IoT Security Spans Edge to Cloud

Intel has cross-BU security portfolio to protect complete e-to-e workflow

- Intel IoTG Group - IoT workstations, intelligent devices at endpoint, edge gateways, device onboarding
- Intel Server Group - Edge compute servers & confidential compute in cloud (support via server group)



Sample: Industrial Cloud/Edge Compute

Yellow* – are products supported by non- IOTG Intel division

IoT Cloud & Device Management Platforms

PREDIX
EcoStruxure Innovation At Every Level
MindSphere
LUMADA

- **Intel® CIT & TxT**
- **Intel® SGX enabled Blockchain**
- **Intel® Secure Device Onboard**

Workstation & Connectivity Control

Industrial Control Point

Apps – MEC (Multi-Access Edge Compute)

- **Baseline Capabilities**
  - **Intel® AES-NI/ Quick Assist /Secure Key-TLS/SSL**
- **Intel® Active Management Technology (AMT)***

Edge Appliances

VM: Condition Monitoring

VM: Predictive Maintenance

Servers

Gateways

Multi-function Controllers & Apps

- **Intel® CIT & TxT**
- **Baseline Capabilities**
  - **Intel® OS GUARD / VT-x**
  - **Intel® Software Guard Extension (SGX)***

Devices

- **Baseline Capabilities**
  - **Intel® Boot Guard**
  - **Intel® Platform Trust Technology**

*Non- IOTG division may be limited to long life support

Security in Lifecycle Terms

Manufacture → Configure → Onboard → Provision → Operate → Decommission

Develop, Onboard, Attest

Operational Security Management

Ecosystem Enabling

- **MCU** - FPGA Crypto Accelerators
- **ODM** - BIOS/FW tools, Intel SDO SDKs
- **OEM** - Boot Guard, SDO SDKs
- **SI** - Crypto Accelerators, HWTPM for Credentials & SW Attestation, SGX SDK & attestation services

- **IT**- Remote Attestation SDKs (SGX TEE & TPM platform)
- **OT/CSPs** - Intel SDO DMS SDK (provisioning integration)

intel

Baseline Trust Capabilities

Crypto | Protected Data/Keys /ID | Trusted Execution | Platform Integrity

ONBOARD

ATTEST

Platform Trust Services

- Intel® Secure Device Onboard (Intel® SDO)

Edge Security

- HW Enhanced Security for Gateways & Edge Compute Servers

Device Management

- Intel SDO Provisioning for DMS vendors
- In-band (Intel® AMT) and Out of band (Intel® vPro) Workstation Manageability

Secure Lifecycle Management

Lifecycle Stage	OT/IT Tasks	Challenges / Pain Points
Deployment	• Provisioning • Onboarding	• Manual effort • Lacks privacy
Operation	• System monitoring & control • Software updates • Security patching • Inventory • Troubleshoot & remediation	• Lack of visibility • Security risk caused by patch failure • Downtime caused by delayed detection of device problems and delayed resolution due to distance
Retirement	• De-commission • Dispose	• Inaccurate inventory

Intel Secure Device Onboard (SDO)

- Zero-touch onboarding service
- Takes seconds at power on
- Unique privacy preserving hardware security model
- One-to-many enablement

- Lower deployment cost
- Protect privacy

Out Of Band Manageability enabled by Intel Active Management Technology (AMT)

- Remote power control
- Remote BIOS access
- Hardware KVM
- Hardware alarm clock and alerting
- Third party data store

- Minimize system downtime
- Lower OT/IT cost

Case Studies

INTEL
BASELINE CAPABILITIES

On-premise Edge Compute platform for workload orchestration

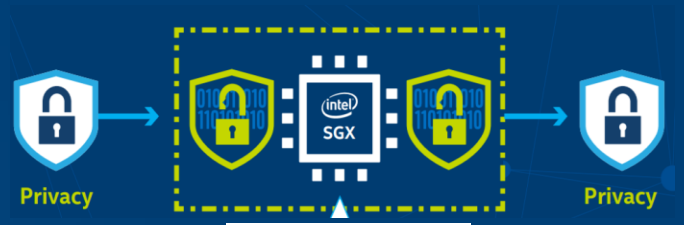
- Instrumented server for core capabilities: Intel VT-x-VM isolation, Intel PTT- measured boot & cred storage, Intel AES-NI- crypto acceleration

INTEL SECURE DEVICE ONBOARD
SMART BUILDING PROVISIONING

Intel Corp Services SR4 Smart Building Implementation

- Advantech gateway onboarding via Intel SDO service for scale and to pass IT security audit

INTEL SOFTWARE GUARD EXTENSIONS
VIRTUALIZED NETWORK EDGE COMPUTE



gemalto
security to be free

Application protection for Edge Computing

- Ensures virtual functions and applications residing in edge compute network slices are protected and isolated using Intel SGX enclaves

Summary

- Intel Architecture (IA) has rich security features spanning CPU and Security Engine
- The feature set will be enhanced in future atom CPU / SoCs
- Defense in depth must be organic and is required across the whole stack

We love to get your feedback and follow up!

- Tell us about your security objectives and use-cases
- We are ready to engage in Architect-2-Architect to help designing secure IOT platform

Thank you!

Notices and Disclaimers

Intel provides these materials as-is, with no express or implied warranties
All products, dates, and figures specified are preliminary based on current expectations, and are subject to change without notice.

Intel, processors, chipsets, and desktop boards may contain design defects or errors known as errata, which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at http://intel.com.

Some results have been estimated or simulated using internal Intel analysis or architecture simulation or modeling, and provided to you for informational purposes. Any differences in your system hardware, software or configuration may affect your actual performance.

experience
what's inside™