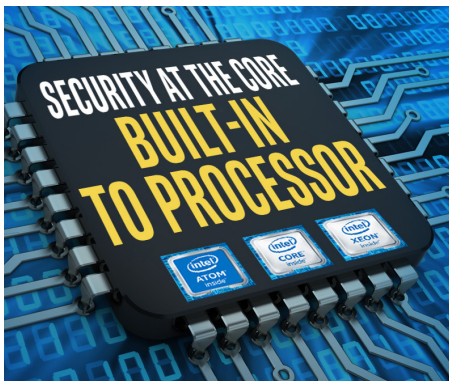
SECURITY CAPABILITY REFERENCE GUIDE

IoT Security

A Security Model to Protect Intelligent Edge Devices

Protecting connected systems from the inside out with hardware security.



While it can be implemented in software, it is only through dedicated hardware that the root of trust is truly immutable. Lower cost and better ease of use will democratize adoption in broader IoT, enabling more secure management of devices throughout their lifecycle.

- Michela Menting, Director ABI Research

INTRODUCTION

The phenomenal growth of Internet of Things (IoT) opens an enormous new attack surface for hackers and malware. To create an environment of trust in which the IoT can truly thrive, ecosystem suppliers must architect security into IoT devices from the start. A "designed-in" security foundation, rooted in the added protections of hardware security, can help drive a consistent, cohesive security model for IoT.

Intel® has a strategic commitment to remove security as the top barrier to adoption and scale for the IoT. Intel's hardware security approaches include processors and chipsets that offer a programmable security framework of core capabilities that can equip devices with baseline trust and flexibility to counter unforeseen threats. Intel's security capabilities guide for IoT provides a roadmap for implementing our portfolio of solutions to help secure high-performance, intelligent devices.

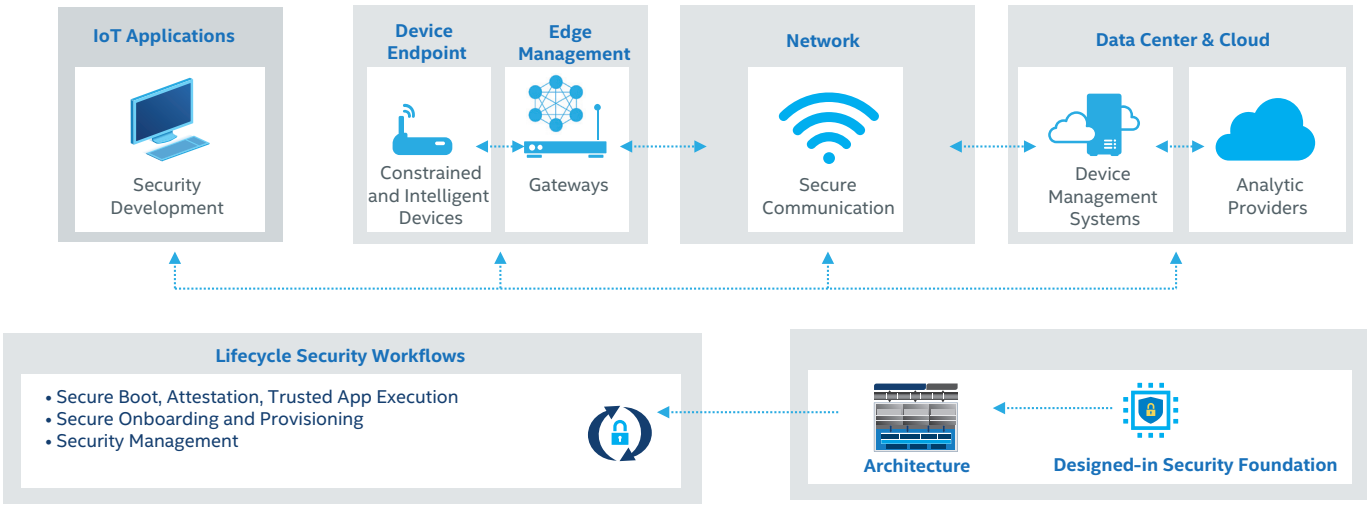


Figure 1. Scope of Intel's end-to-end IoT security architecture

Table of Contents

1.0 BACKGROUND

ABOUT THIS PAPER

This paper is designed to inform security architects and engineers/developers about the spectrum of Intel security solutions that can be applied to help better protect the IoT. It is written for the hardware and ISV ecosystem for building innovative and complete security solutions.

1.1 INTEL'S IOT PORTFOLIO

Intel has a comprehensive architecture and product portfolio to meet the vision for next-generation intelligent IoT systems. Intel has a long history of providing increasingly capable and cost-effective processors with a backward-compatible instruction set that preserves software capabilities over time. Intel silicon products provide an architecture that scales from the data center down to the device level. The Intel® x86 and Instruction Set Architectures (ISA) enable a huge ecosystem across servers, PCs, mobile devices, embedded platforms, and virtualized systems. Intel also provides application and system developers with advanced tools and pre-validated system components.

Intel has delivered remarkable advancements in hardware-based security, hardware-based manageability, hardware-based virtualization, and deterministic real-time compute/networking. More recently, Intel has increased its portfolio of hardware-based machine and deep learning, computer vision, and rich media processing technologies. These advances have demonstrated significant scale, performance, power, security and availability improvements over operating system or software-based approaches.

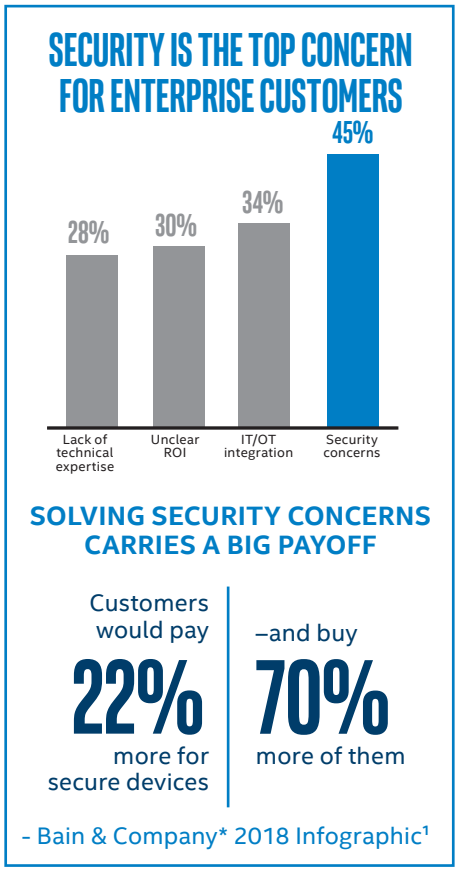
1.2 HARDWARE SECURITY CAN INCREASE SCALE AND ADOPTION OF IOT

Various analysts project that there will be 30 billion IoT devices by 2020[2] and over trillion devices by 2035. IoT devices need to work both independently and securely together to form reliable, available, safe, and secure IoT networks.

Security has become the primary barrier to adoption for IoT. The operational technology (OT) environment has traditionally been considered isolated, and therefore "secure." The connected IT environment is often a poor fit for the isolated OT environment. Furthermore, OT environments place priority on safety and reliability, and IT solutions generally do not address safety concerns, resulting in friction when converging IT and OT.

Software security, alone, has proven relatively unsatisfactory in protecting networked devices against known and freshly discovered threats (so-called "zero day" vulnerabilities). Software security is simply not good enough; it's more vulnerable, not in-depth, easier to manipulate, and there's the threat of IP theft. What is needed is software rooted in the added protections of hardware security. Intel has a charter to ensure hardware security is affordable and simple.

Embedded security is especially important today in creating a trusted supply chain. The supply chain is currently highly vulnerable, whether it is the technology supply chain post-market for delivery of software and services, or contract manufacturing pre-market. A hardware root of trust (RoT) creates a trusted anchor, from which all additional hardware, software and services can be securely linked. So whether they provide identity, access, authentication, PKI, or secure OTA, the semiconductor and hardware OEMs play an important role at the beginning of that supply chain to offer not just a secure hardware piece, but the tools to link it to the rest of the supply chain in a cost-effective, and easy-to-implement manner.



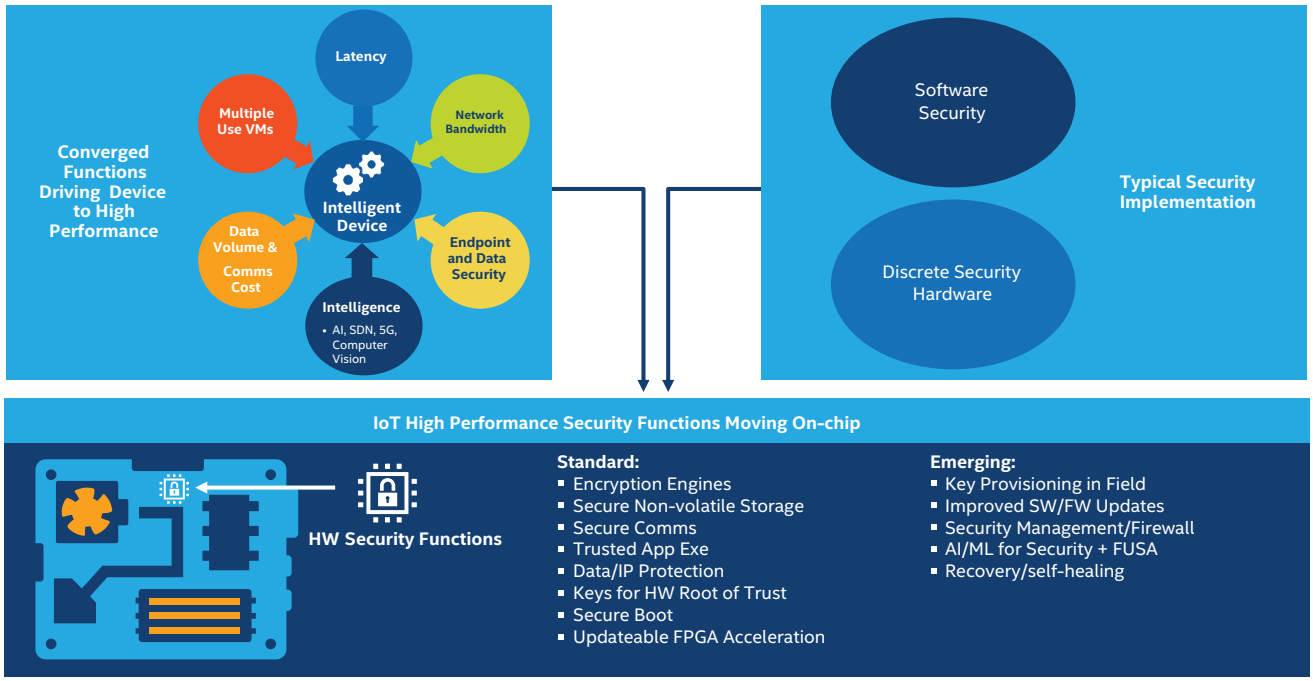


Figure 2. "Convergence concept" from Gartner Market Insight - Nov, 2017

1.3 BASE IOT PATTERN AND DEVICE SEGMENTS

A typical IoT deployment follows the pattern shown in Figure 1. On the left side is the IoT environment consisting of the devices and the applications at the edge, and engaging the management and connectivity capabilities of the edge compute layer. In the center, lies the connectivity and communications layer to enable devices to communicate with each other and with the management/monitoring systems on the back-end. On the right is the enterprise server side, sometimes referred to as the "cloud," which is either remote or on-premise. In the cloud are IT security access management systems, OT device management systems, and data forwarding to analytic providers. Security for the right side inherits traditional and mature enterprise security patterns that are used today by IT.

However, at the edge and communication layer, we have a more complex undefined model due to the heterogeneous security capabilities in devices that were designed using threat models that likely did not consider widespread connectivity. The edge is comprosed of gateway-managed sensors and actuators or embedded systems that have built-in network capabilities to communicate with on-premise or cloud platforms. These devices can be divided into two general segments: constrained or brownfield legacy devices and newer intelligent "greenfield" devices. The brownfield devices often have little or no security capabilities, limited memory, and storage on flash or RAM with minimal network protocol support. It is a significant challenge for IoT device manufacturers and software developers to design complex and comprehensive security measures within a memory footprint of 64KB to 640KB. They need to keep the design simple to avoid adding unnecessary features, and often results in a device restricted to implement a narrow band of security use cases. These limited devices can be augmented with IoT gateways for a security and communications assist.

Devices manufacturers commonly satisfy high performance security capabilities (see Figure 2 "convergence") by implementing security in software, and sometimes augmenting it with discrete add-on security components such as Trusted Platform Modules (TPMs), Hardware Security Modules (HSMs), custom ASIC components, and an emerging class of secure MCU devices. Figure 2 illustrates the trend to build hardware-accelerated security capabilities directly into the main processor. Following this trend, the hardware provides basic security capabilities, and makes them available to the OS and application layers of the CPU. One emerging design pattern is to leverage an FPGA as a hardware security container, with security capabilities similar to a stand-alone gateway device, and configure these to operate on behalf of the CPU without the applications being aware that the security exists at all.

1.4 SECURITY EVOLUTION FOR INTELLIGENT SYSTEMS

IoT devices are getting smarter to support real-time use case capabilities that sense, process, and communicate data on a massive scale. Edge compute software-defined processing paradigms are driving functional consolidation to virtualized multi-purpose devices, making the data more valuable and more exposed as an attack target. Intelligent IoT devices will need more compute power to accommodate computer vision, AI, networking analytics, and 5G communications.

By 2020, this intelligent device segment will grow at a 31% CAGR, with an estimated 90% of all IoT endpoints requiring at least 32-bit processing capability[3]. An edge management solution, such as a sensor hub, gateway or edge compute server will also be required for workload orchestration and normalization of security protocols across intelligent and constrained devices.

Intel is at the forefront of delivering intelligent functions to the high-performance segment of IoT. Intel believes a majority of customer IoT deployments desire the combination of intelligent capabilities, high performance, and a full range of embedded security capabilities. Intel also recognizes that customers will continue to deploy (non-IA) constrained devices with reduced security capabilities alongside intelligent devices.

1.5 INTEL'S DESIGNED-IN CHARTER TO SEED SECURITY

The fragmented chain of suppliers that build devices (OEM > ODM > OSV > ISV > SI > Customer) choose their own preferred implementations of security capabilities, often implementing critical RoT functions in software or expensive discrete hardware security components.

It is regularly left to the IoT environment owner/operator to determine how to implement security. However, this is far too late in the process. Baseline security constructs must be considered in advance, by the SIs and the device builders. As such, the security functionality must be enabled in the hardware in order to implement certain fundamental capabilities (e.g. RoT, boot integrity, identity storage, updateability). Intel implements such foundational security capabilities in the hardware, enabling the OEMs/ODMs to build on top of these functions, and allowing system integrators and service providers to expose them to the owner/operator of the IoT environment.

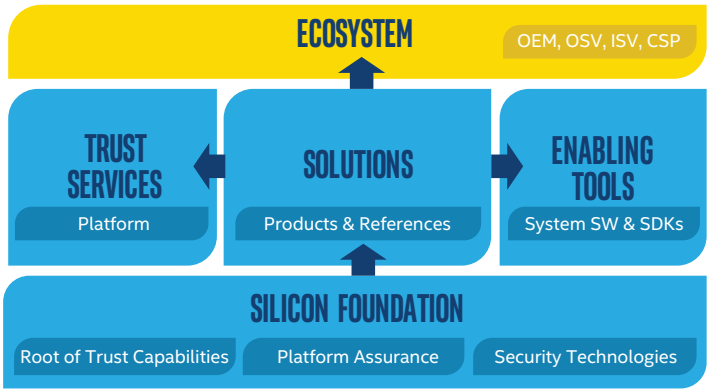


Figure 3. Intel Security Products Delivery Model

To drive consistency and a component-based approach for the ecosystem, Intel has -core charters as shown in Figure 3.

- **Silicon Foundation** – Embed an essential set of RoT capabilities in a full range of processors from Intel® Xeon®, Intel® Core®, to Intel® Atom®. Deliver on a "Security First Pledge" that provides comprehensive security assurance and security development lifecycle for our platforms.
- **Building Block Solutions for Ecosystem Innovation** – Security software and security-as-a-service to establish platform trust, and enabling tools used to build a complete software stack rooted in hardware trust.
- **Ecosystem Enabling Programs** – Security-enabling programs that assist partners in building customer-ready security solutions. For example, for our trusted execution technologies, Intel operates an Intel® Software Guard Extensions (Intel® SGX) program to help the ecosystem instrument their solutions for this technology.

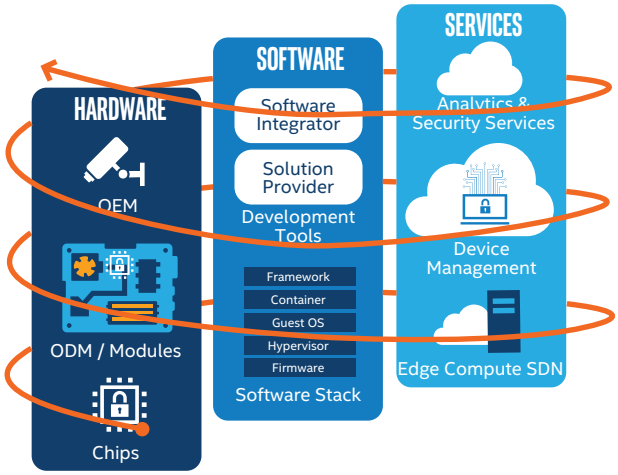


Figure 4. Seeding trust and consistent implementations from silicon security

As an integrated device manufacturer, Intel delivers a rich spectrum of enabling accelerators so the ecosystem can innovate from one binary, one architecture, and an open source-based suite of development tools.

2.0 ESTABLISH TRUST IN THE DEVICE

A device must first and foremost help protect itself (including: secrets, identities, keys, data) from attacks and build a chain of trust across the multiple stack layers that each present unique attack surfaces. Compromise at one layer can propagate through the system. Hardware security does not imply a silver bullet that replaces software security in each layer. Hardware RoT capabilities provide unique isolation and seed ingredient capabilities that can be used to plug into each security layer to make the entire system or stack more secure. We call this the transitive trust chain.

2.1 BUILT-IN CAPABILITIES: INTEL® SECURITY ESSENTIALS

Intel's built-in foundational trust capabilities are called Intel Security Essentials. These capabilities are available across Intel processor lines and enable security professionals to develop tools that protect the platform and data, and build trusted applications in a consistent way. With components based on the processor, this common foundation delivers a single source of hardware-based best practice security capabilities (Table 1) for ecosystem innovation.

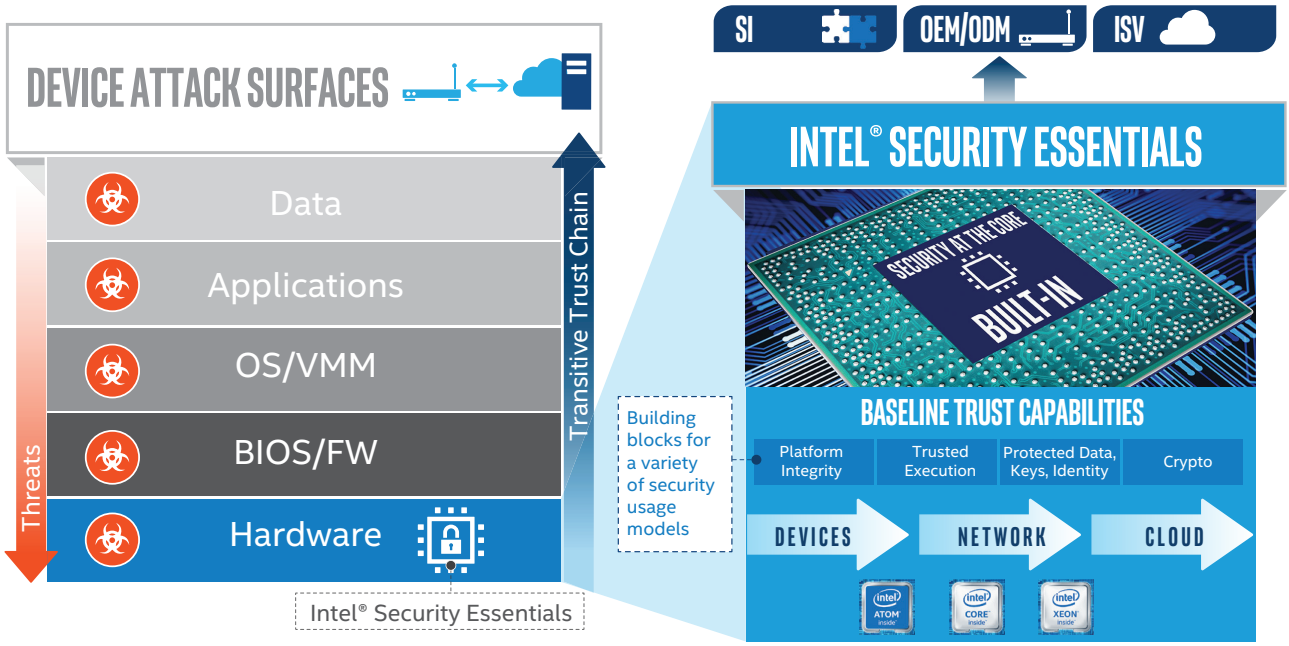


Figure 5. Intel® Security Essentials: A built-in trusted foundation

Intel Security Essentials delivers four foundational capabilities that each have distinct enabling workflows and underlying Intel security technologies, including:

- **Platform Integrity** – Protected and verifed boot process with hardware attestation of the platform
- **Trusted Execution** – Isolated enclaves and VMs that help to protect sensitive data, code, I/O processes, or keys at runtime to create a trusted application environment
- **Protected Data, Keys, and Identity** – Encrypt, generate, and store sensitive data, keys, or credentials at rest and in transport to protect from misuse or disclosure
- **Crypto** – Hardware-assisted crypto acceleration

2.2 COMPREHENSIVE SECURITY STACK

Alongside Intel Security Essentials baseline capabilities are additional Intel security solutions and technologies that the ecosystem can use to build a high-performance security implementation for the device. The following sections of the paper define the technologies and related market drivers.

Table 2 shows the individual hardware security technologies that can be used to create one of the four baseline capabilities along with a secondary reference to indicate which attack surface gains the protections. Today's intelligent devices are capable of sophisticated virtualization which enables the device to support multiple use cases, applications, and security profiles.

2.3 CORE CAPABILITY: PLATFORM INTEGRITY

2.3.1 Hardware Root of Trust for Platform Attestation

To set the anchor for Intel's RoT chain is a cryptographic key and a small trusted code in ROM or locked flash that uses the RoT key to bootstrap trusted operations.

In IoT, the most common usage of a RoT is to perform secure boot; another type is used to report health information about a platform in an attestation record; a third type, can be used to represent the identity of the platform in protocols such as TLS, or authenticated machine-to-machine (M2M) protocols like MQTT.

Intel® platforms commonly provide two RoT keys: one for secure boot and one for identity and attestation. A discrete Trusted Platform Module (TPM), or the integrated Intel® Platform Trust Technology (Intel® PTT) hardware TPM can be used to to hold the identity key used for attestation and report the platform health through measurements.

PROPERTY	DEFINITION	INTEL® SECURITY ESSENTIALS
Hardware Root of Trust	Cryptographic keys protected by hardware. ID inseparable from hardware	✓
Small Trusted Computing Base	Application leverages trusted execution environment or hardware TPM to protect keys, IDs, and data	✓
Defense in Depth	Complementary hardware and software protection	✓
Compartmentalization	Hardware-enforced barriers between software components	✓
Hardware Security Acceleration	Hardware acceleration of cryptographic math calculations, key generation, and memory scanning.	✓

Table 1. Properties of Highly Secure Devices[4]

	Core Capability – Devices	Technology Name	Intel® + "Short Name"	Surface Protected
Intel® Security Essentials	Platform Integrity	Intel® Boot Guard	Boot Guard	BIOS/FW
		Intel® OS Guard	OS Guard	OS/VMM
	Trusted Execution	Intel® Software Guard Extensions	SGX	Data and Apps
		Intel® Virtualization Technology for Directed I/O	VT/VT-d	OS/VMM
	Protected Data, Keys, Identity	Intel® Platform Trust Technology	PTT	Data
		Intel® Secure Key	Secure Key	Data
		Total Memory Encryption[4]	TME	OS/VMM
	Crypto (on chip)	Intel® Advanced Encryption Standard New Instructions	AES-NI	Data
		Secure Hash Algorithm (SHA) variant SHA-256	SHA Extensions	Data
	Additional Capabilities- Edge Compute & Device Management			
	Service – Secure Provisioning	Intel® Secure Device Onboard	SDO	Data
	Workstation – Remote Device Managability	Intel® Active Management Technology, Intel® vPro	AMT, vPro	BIOS/FW
	Gateway – Integrity	Intel® BIOS Guard	BIOS Guard	BIOS/FW
	Gateway/Server – Integrity	Intel® Trusted Execution Technology and Intel® Security Libraries for Data Center	TXT, SecL-DC	BIOS/FW
	Gateway/Server – Discrete FPGA Crypto	Intel® Stratix 10 Secure Device Manager	SDM	Data

Table 2. Security solution glossary

Market Drivers - The market is shifting to strong hardware roots of trust and recognizing this inherently trusted element provides the transitive trust chain for the entire device.

Enabling Note - Intel seeds the strong hardware RoT for the ecosystem in our SOC rather than requiring ecosystem and customers to add on discrete hardware RoT.

2.3.2 Protected Boot

Intel supports good, better, best technology options to achieve a protected boot for IoT devices. We ensure each stage of the boot from hardware to firmware, to the OS is signed and verified as a trustworthy system. This chain of trust is anchored to the hardware RoT in the silicon. Secure boot employs a defense-in-depth strategy that is essential for protecting platforms from attacks that modify or corrupt the system software, including the boot loader and operating system. Secure boot protects by preventing unsigned modifications from becoming operational.Intel provides reference code for a stage 1 boot loader which authenticates the stage 2 boot loader. This RoT is then extended by OSVs/ ISVs into the OS, hypervisor, kernel, and ultimately the user mode/apps framework (Figure 7).

- **UEFI Secure Boot – "good"**
  BIOS security standard that verifies the next state of the boot is authorized via signature checking the firmware.
- **Verified Boot – "better"**
  Boot process where each stage of the boot is cryptographically verified by the previous stage.
- **Measured Boot – "best"**
  Boot process where each stage of the boot is measured, by cryptographic hash, and stored for attestation in TPM. Validation can tell if something is different versus knowing what is different. Note measured boot should always be coupled with verified boot or it loses its value.

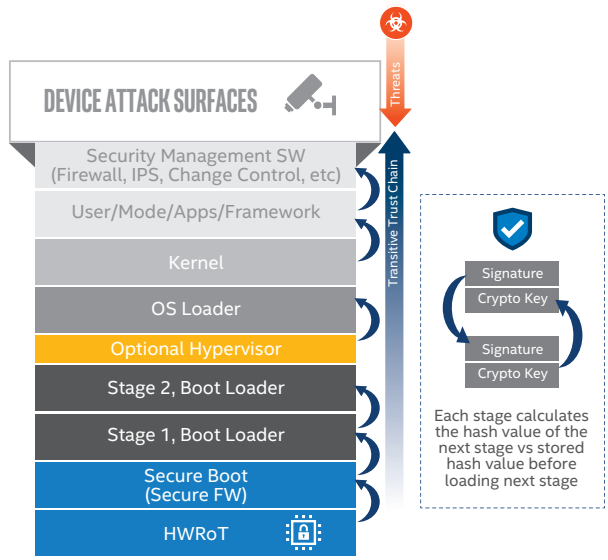


Figure 7. Protected Boot Options

2.3.3 Intel® Boot Guard

Cryptographically verifies the first portion of OEM pre-OS boot loader code executing out of reset. OEMs and ISV's use Boot Guard to add robustness to chain of trust process where a pre-OS boot loader/boot process (aka Initial Boot Block) (IBB) cryptographically verifies and/or measures each software module before executing it. It supports both TPM families TPM 1.2 and TPM 2.0 and also Intel's hardware TPM (Intel PTT) as part of measured boot.

Market Drivers – Protected boot/ pre-OS boot loader technologies apply to edge servers, intelligent gateways, and devices. This extends the platform-level attestation from bootstrap to OS startup, and assists in the prevention of unauthorized firmware or boot images that may be obtained over-the-air or over-the-network.

Enabling Notes – Boot Guard requires pre-OS boot loader enabling and OEM support in signing of the policy manifests, hashing of pre-OS boot loader boot block module, programming the hash of OEM public key and boot policies in field programmable fuses. For OEMs and ISVs, we have a UEFI Developer Kit, secure boot implementation partners and open source initiatives such as TianoCore*, which can help device manufacturers package verified and trusted boot drivers and firmware.

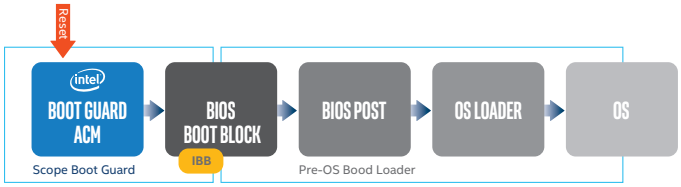


Figure 8. Intel® Boot Guard

2.3.4 OS Hardening - Intel® OS Guard

The reality of today's crimeware is that smart software is able to find vulnerabilities and invade where it's hard for virus detection tools to reach and eliminate it. Threats are inserting themselves in application memory space and executing under a privilege level assumed for the application. To outsmart this malware requires hardware-based solutions that complement – and even assist – sophisticated virus detection and security software that works below and beyond the OS, detecting and stopping threats as they try to take advantage of a vulnerability. Intel OS Guard helps to protect against such escalation of privilege attacks by preventing malicious code from executing out of application memory space, in addition to data memory.

Market Drivers – OS Guard can prevent privilege escalation such as the one used by infamous Stuxnet worm.

2.4 CORE CAPABILITY: TRUSTED EXECUTION

2.4.1 Intel SGX

To address the reality of widespread security holes and compromised systems, Intel set out to design a hardware-assisted trusted execution environment with the smallest possible attack surface – the CPU boundary. Intel SGX delivers 17 new Intel Architecture instructions that can be used by applications to set aside private regions of code and data, called enclaves, that can prevent direct attacks on executing code or data stored in memory. An enclave prevents software attacks even when the OS/drivers/BIOS/ VMM/SMM are compromised.

Market Drivers – The IoT ecosystem wants the flexibility to define their own security model to protect items like AI/ML, algorithms, licensing keys, Digital Rights Management, keys for secure communications, or other IP. They don't want to be force fit into an OS-level solution.

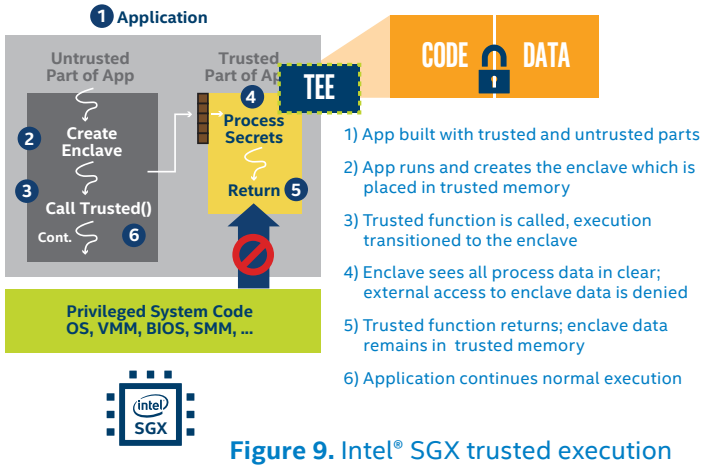


Figure 9. Intel® SGX trusted execution run-time processing

Enabling Note – (Attestation, key provisioning, sealing) Currently, device OEMs and ISVs commonly provision application software and secrets at manufacturing time or via complex field configurations that cannot cryptographically prove application integrity. Intel SGX enables local attestation between enclaves or remote attestation by a third party to ensure the application has not been compromised. The protected portion of an application is loaded into an enclave, where its code and data is measured. A report is sent to the remote application owner's server which in turn can validate that the enclave report was generated by an authentic Intel processor. Upon verification, the remote party can trust the enclave and securely provision keys, credentials, or data. The cryptographic keys generated in the enclave are never released or accessible outside of the enclave. Intel SGX includes an instruction for generating a CPU/ enclave specific "Sealing Key" that can be used to safely store and retrieve sensitive information that may need to be stored to disk.

2.4.2 Intel® Virtualization Technology (Intel® VT, VT-x, VT-d)

Intel VT provides a portfolio of technologies that increase performance for virtualization and improve security through hardware isolation. Intel® Virtualization Technology for Directed I/O (VT-d) uses hardware security to restrict device accesses to the owner of the partition managing the devices so they cannot compromise another partition or VMM.

Market Drivers – The ecosystem wants to be able to maintain a secure firewall between viruses running in the main OS and secure workloads running inside a secure VM. Software-defined edge compute models are consolidating different workloads on a device where isolation becomes an paramount.

Enabling Note – Over the last decade or so, a significant number of hypervisor vendors, solution developers, and users have been enabled with Intel VT.

2.4.3 Total Memory Encryption (TME)

As the name suggests, this technology encrypts the platform's entire memory with a single key. TME, when enabled via BIOS configuration, will help ensure that all memory accessed from the Intel CPU is encrypted, including customer credentials, encryption keys, and other IP or sensitive information on the external memory bus. The key used for memory encryption is generated using a hardened random number generator in the CPU that is never exposed to software. Data in-memory and on the external memory buses is encrypted and is only in plain text while inside the CPU, similar to typical storage encryption. This allows existing software to run unmodified while protecting memory using TME. The software running on a TME-capable system will have full visibility into all portions of memory that are configured to not be encrypted by TME, simply by reading a configuration register in the CPU.

Market Drivers – Prevents IoT hackers from stealing sensitive/confidential data out of the memory if a device is lost or stolen in the field. TME fills the security gap on DRAM/NVRAM that is outside of the SOC to cover all system memory.

Enabling Note – OSV's will use the feature to strengthen the isolation of their virtual machines. TME spec released in 2017. Contact your Intel account manager for TME platform availability[5].

2.5 CORE CAPABILITY PROTECTED DATA, KEYS, IDENTITY

2.5.1 Intel® Secure Key

A secure, protected encryption capability to protect data at rest starts with a random number seed, typically provided by a pseudo-random number generator within the client. Intel Secure Key provides a high-entropy source of random numbers through generation in hardware, out of sight of malware.

Market Drivers - A Digital Random Number Generator (DRNG) is valuable in encryption algorithms and virtualized environments due to their high non-deterministic in nature as opposed to software-based pseudorandom number generator (PRNG).

Enabling Notes - Intel® DRNG supports NIST SP 800-90 A, B, and C compliant functionality and is FIPS 140-2 Level 2 certifiable[4]

2.5.2 Intel® Platform Trust Technology (Intel® PTT)

Intel PTT (Figure 10), an integrated on-chip hardware TPM, provides the secure storage of keys/credentials, platform configuration registry values, and boot block measurements. Intel PTT is essential to provide attestation locally for runtime integrity protections or remotely to third party providers that need to ensure the device software stack is verified to a known value. The attestation reports communicate unauthorized modifications to device management systems.

Market Drivers – Intel PTT saves on costs for OEMs so they do not need to add additional BOM costs to use a discrete TPM provider. Intel PTT also saves the board real estate and platform power.

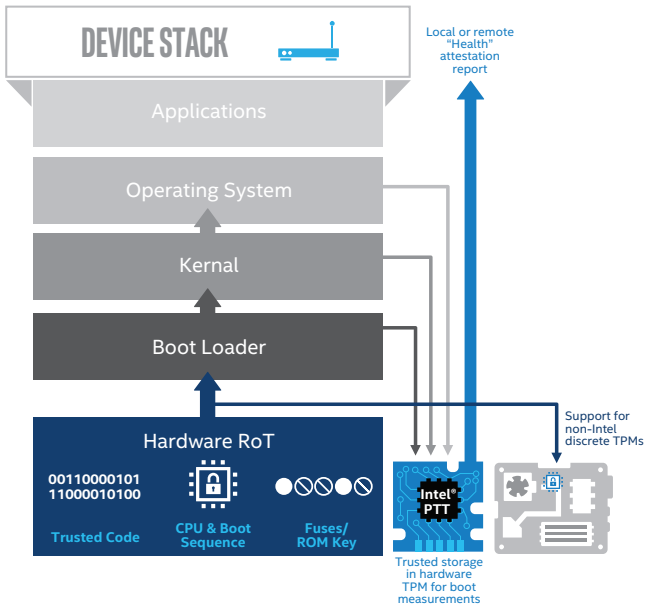


Figure 10. Measured boot using Intel PTT

Enabling Notes – Supports all Microsoft 8/10 requirements for firmware Trusted Platform Module (TPM) 2.0 and BitLocker* for hard drive encryption.

2.6 CORE CAPABILITY: CRYPTO

Intel CPUs come standard with a suite of cryptographic operations that can be performed on the main CPU. Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) and SHA-Extensions greatly reduces the overhead associated with encryption processing and enables near-ubiquitous encryption of stored data.

When it comes to real-time, time sensitive IoT deployments, an FPGA security co-processor provides many advantages especially in the areas of performance. Intel standalone FPGA + SOCs can be used to offload intensive security processing from the main processor. Additionally, accelerated cryptography or edge-to-cloud gateway assisted firewall processing are common use cases. FPGAs deliver the future-proof flexibility to update security algorithms in the field, which extends the IoT device product lifespan, especially in light of the need to eventually update with post-quantum cryptography.

IoT use cases for items such as functional safety where security and safety and critical systems must be compartmentalized, Intel® Stratix 10 Secure Device Manager provides a fully configurable boot, and key storage process that can be used to create an isolated co-processor environment.

Intel has an extensive roadmap of FPGA-related security assist use cases that will be brought to market in the areas of security management and certifiable functional safety IP.

Market Drivers – Comprehensive endpoint security requires proper use and hardware acceleration of cryptography across transport protocols, storage, and applications.

Enabling Note – Microsoft* enables Intel crypto by default on Windows*. Intel has ecosystem FPGA partners such as Barco* Silex*, Helion*, and SecureRF* that design a range of crypto and key management capabilities that can be integrated into our FPGA technologies.

2.6.1 Device Security Pattern Summary

In Figure 11, we summarize the four Intel Security Essential capabilities in a multi-function virtualized device architecture that is becoming more common with workload consolidation trends. We see a high-trust domain set of applications that can leverage Intel's trusted execution environments for run-time protections and secure I/0 across VMs for trusted external communications. Low-trust applications running on a host OS may have direct Internet connections and a more open security policy, allowing download of "app store" updates or to engage in other vulnerable actions. Functional safety-related applications may have additional real time manageability or security audit and compliance requirements to run in compartmentalized VMs.

3.0 SECURITY FOR THE EDGE

3.1 NORMALIZING EDGE SECURITY WITH IOT GATEWAYS

The edge, though difficult to consistently define, may contain a heterogeneous assortment of devices with various levels of compute, communication, and security capabilities. The IoT gateway implements consistent capabilities by acting as a more capable proxy on behalf of the various IoT devices, sensors, equipment, and local edge compute or cloud-based systems on the network, as shown in Figure 12. From the network perspective, all of the things behind the gateway have a minimal level of compute, communication, and security capability. Even though the things themselves may not natively have this capability, the IoT gateway augments their features to bring them up to the minimum level.

IoT gateways provide a number of capabilities to augment the functionality of the things behind it, including local processing and storage, and the ability to autonomously control field devices based on data input by sensors. Furthermore, the gateway is a high-performance, intelligent computing device with a reliable and fast network connection. The gateway can adapt to challenging network

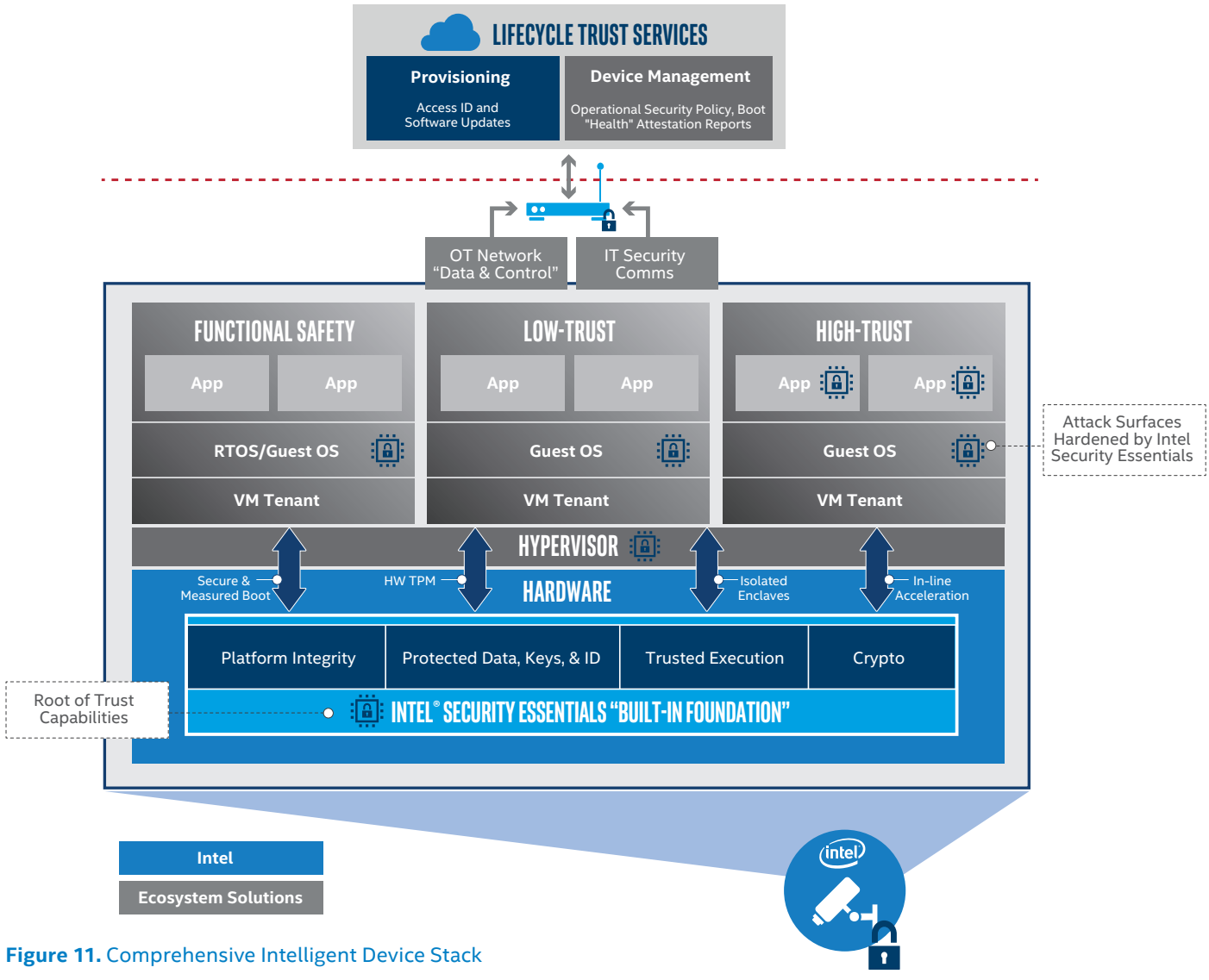


Figure 11. Comprehensive Intelligent Device Stack

environments including those that require periodic/intermittent connectivity, addressing congestion, handling large number of concurrent connections, ensuring quality of service, and providing increased security requirements.

Since gateways are deployed in front of legacy equipment, they are often used to normalize communication through protocol translation. They provide comprehensive security capabilities across both constrained and intelligent devices to make deployment of consistent security policy possible. For separation of concerns, it is best to leverage an isolated security channel to send/route security communications from the security policy management system operated by IT. IT typically operates firewall, security information event management (SIEM), global threat intelligence networks, and security event monitoring publish/subscribe protocols such as Open Data Exchange Layer (DXL) that can ingest and pro-actively act on edge collected security meta data. Emerging trends that will impact gateway security include the industry's movement toward virtualization and Edge X Foundry*, where data on devices and gateways are managed with plug-and-play components in a container-based approach.

Intel offers IoT gateway providers a rich stack. Intel provides hardware security and software that can be used to enable their SKUs for a sophisticated gateway managed edge security pattern. As mentioned earlier, the Intel Security Essentials foundation provides the same baseline device security foundation for the ecosystem to enable the gateway to protect itself, with secure boot, accelerated cryptography, and encrypted memory protections for data at rest and in motion.

For system integrators that build custom "vertical and analytics" applications to run on the gateway, Intel SGX trusted execution environment delivers flexible partitioning of sensitive code/data/keys that can be protected at runtime in 1-n secure enclaves. The hardware TPM (Intel PTT) delivers on-chip secure key storage and remote attestation capabilities that can be instrumented with IT's security management directories and Authentication, Authorization, and Accounting (AAA) systems of record.

3.2 SECURE EDGE ORCHESTRATION - EDGE COMPUTE SECURITY PATTERNS

Edge computing is a new paradigm that extends the Cloud platform model by providing localized virtual computing resources on the edges of a network to support geographically distributed, latency sensitive, and Quality-of-Service (QoS)-aware IoT applications. OpenFog, Industry 4.0, and other vertical initiatives are pioneering how to tie network assets to each other and the cloud. Any device, such as switches, routers, servers and even intelligent devices (e.g. cameras) can become a virtualized edge compute node that have computing, storage, and network connectivity.

Security management through intelligent gateways, as previously described, are still part of the edge compute model but are joined by real-time, deterministic workload orchestration servers. In the edge compute model, applications operate as virtualized containers with telco operator supplied Multi-access Edge (MEC) servers that provide connectivity and a management framework for onboarding of third party apps and network communication services.

3.2.1 Edge Compute Security Challenges

Edge computing represents an attractive target for cyber-criminals due to high volumes of data throughput and the likelihood of being able to acquire sensitive data from both Cloud and IoT devices. Some of the unique challenges include:

- **Shared Technology/Virtualization** – Insecure hypervisor = single point failure, VM tenant segregation, and privilege escalation attacks.
- **Denial-of-Service** – Due to a lack of centralized authority, a DoS attack can prevent legitimate service use as the network becomes saturated.
- **Trust** – Edge nodes that offer services to IoT devices should be able to validate whether the devices requesting services are genuine and operating an attestable stack.
- **Provisioning** – A device needs to be provisioned with network access credentials, node management agents, and analytics software to participate in a closed loop edge compute model.

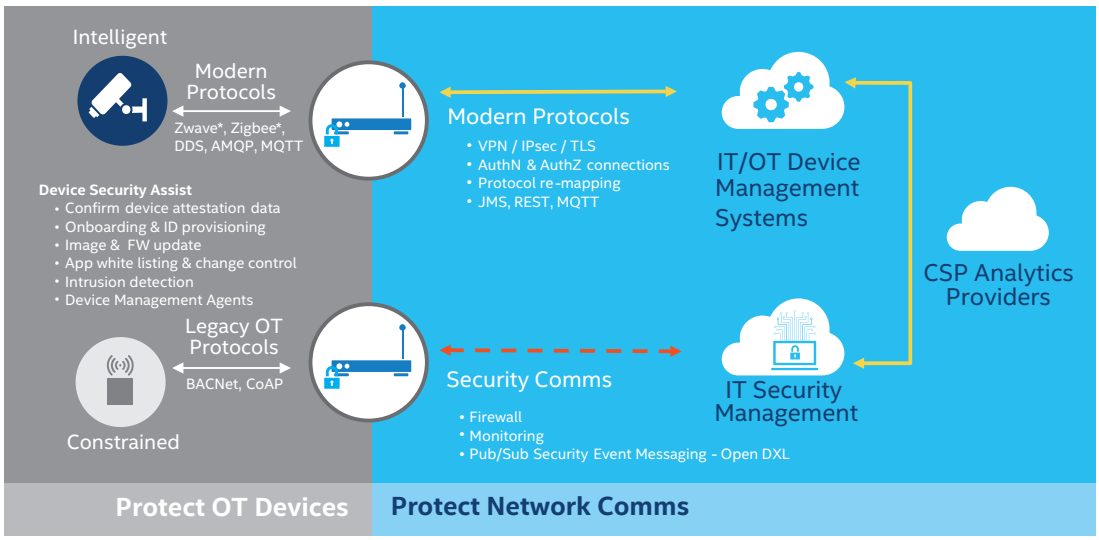


Figure 12. Normalizing edge security

- **Privacy** - Privacy preservation is more challenging since local edge nodes may collect GDPR sensitive or location-related data that must be anonymized prior to edge or cloud processing. Privacy concerns also apply to cloud environments, especially when all data is aggregated for analytics purposes. CSPs have recently launched confidential computing services based on Intel SGX that delivers runtime isolations.

3.3 INTEL SOLUTIONS EDGE COMPUTE SOLUTIONS

As shown in Figure 13, the same pattern of Intel Security Essentials capabilities are applicable to establish baseline trust across each of the three tiers of edge architecture. Many of Intel's data center security capabilities from our Intel Xeon platform are applicable to the more distributed resource compute model of the edge where "micro data centers" may be deployed locally running SDN/NFV (software defined networking and network function virtualization) workload orchestration servers.

3.3.1 Intelligent Devices

Intelligent and constrained devices deployed for edge compute operate with various degrees of native capability. They can request additional storage, network, or compute processing from edge nodes in a master/slave relationship. Intel's protected and measured boot technologies provide essential device health status information that can be attested to edge nodes that may be tasked with security management trust brokering responsibilities (as described in the gateway security section). Intel® Secure Device Onboard (Intel® SDO) services (see coming section 4.0) can speed device provisioning of access credentials and edge compute software to devices and nodes.

3.3.2 Edge Nodes and Server Platforms

Edge nodes collaborate among themselves in a peer-to-peer network when they need to manage network resources or to manage communications to network servers (e.g. platform orchestration or MECs). Edge IoT devices interact with edge nodes only when they need to offload a processing or storage request. Secure communications to protect data in transit can be configured by setting up trusted transaction spaces for edge subnets with encrypted SSL/TLS protocol encapsulation and mutual authentication. Security policy and enforcement for trusted transaction spaces with firewalls, and intrusion prevention is traditionally configured in threat protection ISV systems. However, application to software-defined orchestration models, such as edge computing, presents a host of virtualized network security functions that are difficult to configure in east/west traffic across local virtualized nodes. Intel's New Device Group works with firewall providers to automate the deployment of virtualized network security functions at the edge.

Multi-function device compute nodes and platform orchestration servers are key workload aggregation points that need to apply platform integrity and trusted execution protections.

3.3.2.1 Intel® BIOS Guard

For edge compute workstations and gateways, Intel BIOS Guard protects against pre-OS boot loader recovery attacks. It moves flash update authentication and write protection out of SMM and into the CPU authenticated code.

3.3.2.2 Intel® Trusted Execution Technology (Intel® TXT)

Intel TXT works by creating a Measured Launch Environment (MLE) that enables an accurate comparison of all the critical elements of the launch environment against a known good source with enforcement mechanisms to block launch of code. It is critical to provide controls to help verify only a trustable hypervisor is run on a platform server prior to virtualization software booting. Additionally, the threat of compromised VM migration can be restricted so that edge workloads only run on trusted platforms. Intel® Security Libraries for Data Center (Intel® SecL-DC) provide the policy management API to manage Intel TXT across edge compute server nodes. The Wind River* Titanium Control server provides an example of how to apply Intel hardware-based protections as it is optimized for accelerated AES-NI crypto processing, implements Intel TXT for measured launch, isolates VMs with VT-x and VT-d, and leverages Intel PTT for protected hardware TPM key storage.

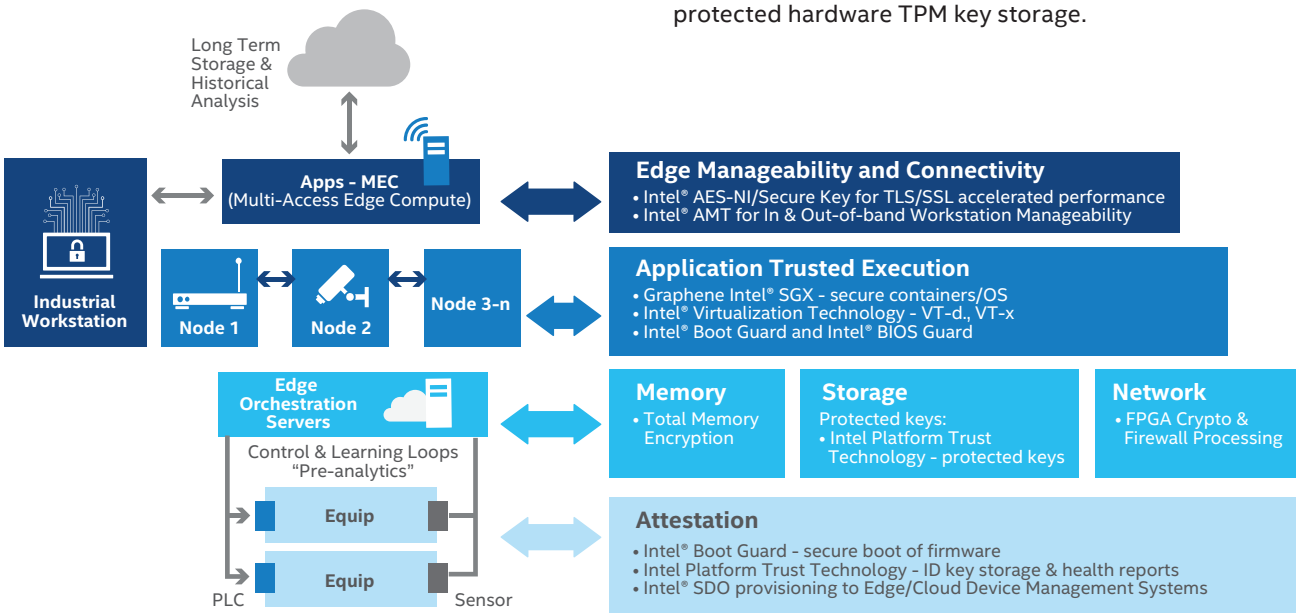


Figure 13. Edge Compute Security Stack

Edge computing presents new challenges to apply Intel SGX's runtime protections to wrap the entire application and OS since each edge node can be a virtual server, gateway, or controller. Intel's Graphene - Intel SGX project on Github* (https://github.com/oscarlab/graphene) demonstrates how Linux containers can be seamlessly wrapped using off the shelf ISV tools.

4.0 DEVICE MANAGEMENT SERVICES (DMS)

4.1 SECURE ONBOARDING/PROVISIONING

Intel SDO is a service that enables a device to be drop-shipped and powered on to dynamically provision to a customer's IoT platform of choice in seconds. This zero-touch model simplifies the installer's role and scales the number of devices that can be automatically deployed in production. Intel SDO eliminates poor security practices, such as shipping default passwords. Intel SDO delivers a groundbreaking late binding model where the cloud device management selection and configuration of credentials and software can happen post supply chain delivery at power on/install.

Market Drivers – Provisioning today takes an average of 20 minutes per device and is insecure[3]. Intel SDO brings this down to seconds thereby delivering an essential scaling element to drive production volumes. Intel SDO delivers a hardware attested device and clean baseline to management platforms that can overlay additional operational security controls. Suppliers can reduce custom SKU counts and deliver a standard image device that gets customized at install for customer.

Enabling Note -

At Device Manufacture

- The processor (Intel or Arm) contains a unique hardware root of trust key (either ECDSA or Intel® EPID)
- The ODM uses the SDO Manufacturing Toolkit to insert credentials into the device.
- The ODM installs the SDO Client software on the device.
- The SDO Manufacturing Toolkit creates a digital 'Ownership Voucher' that is sent to the new device owner i.e. VAR, SI or end customer.

Before Installation

Step 1: The Ownership Voucher is passed to target IoT platform e.g. Arm Pelion*.

Step 2: The new device is registered in the SDO 'Rendezvous' Service together with the URL for the target IoT platform.

At Installation

Step 3: Device powers on and contacts the SDO 'Rendezvous' Service which authenticates the device and then points it to its target platform using the URL from Step 2.

Step 4: The platform and device mutually identify each other using the root of trust and Ownership Voucher. An authenticated tunnel is established between the device & platform.

Step 5: The provisioning payload for the target platform is transferred to device. This can be credentials such as passwords or can be a complete platform agent.

Now the platform takes control of device and SDO shuts down. SDO remains dormant for the remainder of the life of the device unless a specific decision is made e.g. to re-sell the device and onboard it to a new platform.

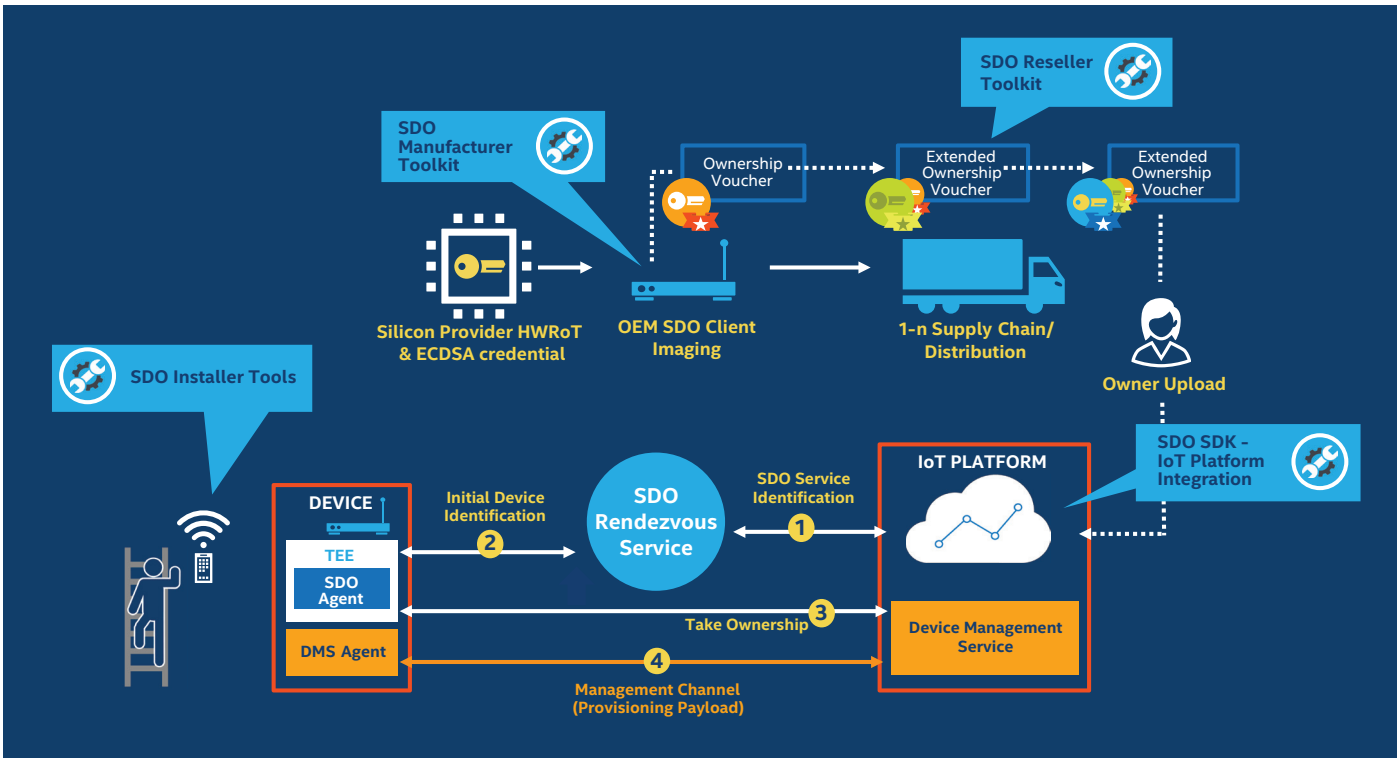


Figure 14. Intel Secure Device Onboarding flow/tools

4.2 DEVICE MANAGEABILITY AND MANAGEMENT SERVICES

Device Management Services
Failure to provide manageability and adequate update mechanisms in IoT devices makes them much more vulnerable. Regular updates can keep the device safer and offers remediation in case of attack. Manageability offers the last line of defense in case of proactive or unintentional issues. An IoT endpoint management solution requires a modular, remotely updatable, standards-based approach due to the number of different customer environments. Intel integrates our Intel SDO service with various device management service (DMS) vendors including major CSPs and device management ISVs such as Mocana*, Arm*, Hitachi JP1*, and Infosim*. Key lifecycle functions include: deploying, monitoring, servicing, updating, and decommissioning IoT devices.

DMS Functions –

- **Secure Signed Update** – Over The Air (OTA) and Firmware OTA (FOTA) integrity checked software or kernel update over encrypted channel. Update manifest including list of signed, hashed components and a package signature for component integrity. Reconfigure anything to respond to vulnerabilities.
- **Security Monitoring** – Alerts and secure logs.
- **Hardened Management Server** – Distributed Denial of Service (DDOS), anti-spoofing, script and forgery protection
- **Mutual Authentication** – Client and server authenticate each other
- **Secure Comms Channel** – DTLS or equivalent and can independently define the security. Some channels require higher levels of security, while other channels require lower levels of security.
- **Lifecycle** – Suspend, decommission, rollback image in case of corruption or vulnerability

Market Drivers – Customers want to supplement CSP/ ISV device management offerings (such as Azure*, Google* Cloud Platform, and Amazon* Web Services) with a more powerful, scalable device management broker that forwards data into IoT platforms for analytics.

Enabling Notes – Intel SDO can onboard to a DMS and provision the DMS agent to the device. The Intel SDO DMS SDK is used to integrate into the DMS enrollment capabilities.

4.3 WORKSTATION MANAGEABILITY

For IoT workstation class devices such as retail point-of-sale/ digital signage, medical devices, and industrial displays, Intel provides hardware endpoint manageability solutions. Intel® Active Management Technology (Intel® AMT) delivers standard recovery capabilities to remotely control the power, securely wipe drives, and access the BIOS. Intel® vPro enables a superset of security and manageability for both in-band and out-of band models.

Market Driver – Customers desire automation to scale remote workstation manageability and patch updates for critical vulnerabilities.

Enabling Notes – IT departments that use security policy management systems can instrument for Intel AMT and Intel vPro remote workstation management and recovery functions.

5.0 ECOSYSTEM ENABLING ROLES

IoT devices (see Figure 15) have an unusually long, complex lifecycle with infrequent updates post deployment. This means devices need to be equipped with a baseline set of security capabilities throughout their production lifecycle or the industry will be living with hard to fix security holes for years to come.

In the Design/Manufacture Stage, the risk model for the class of device is assessed to design for an appropriate threat model. Considerations such as privacy, functional safety, and severity of attacks are early concerns. While the end security

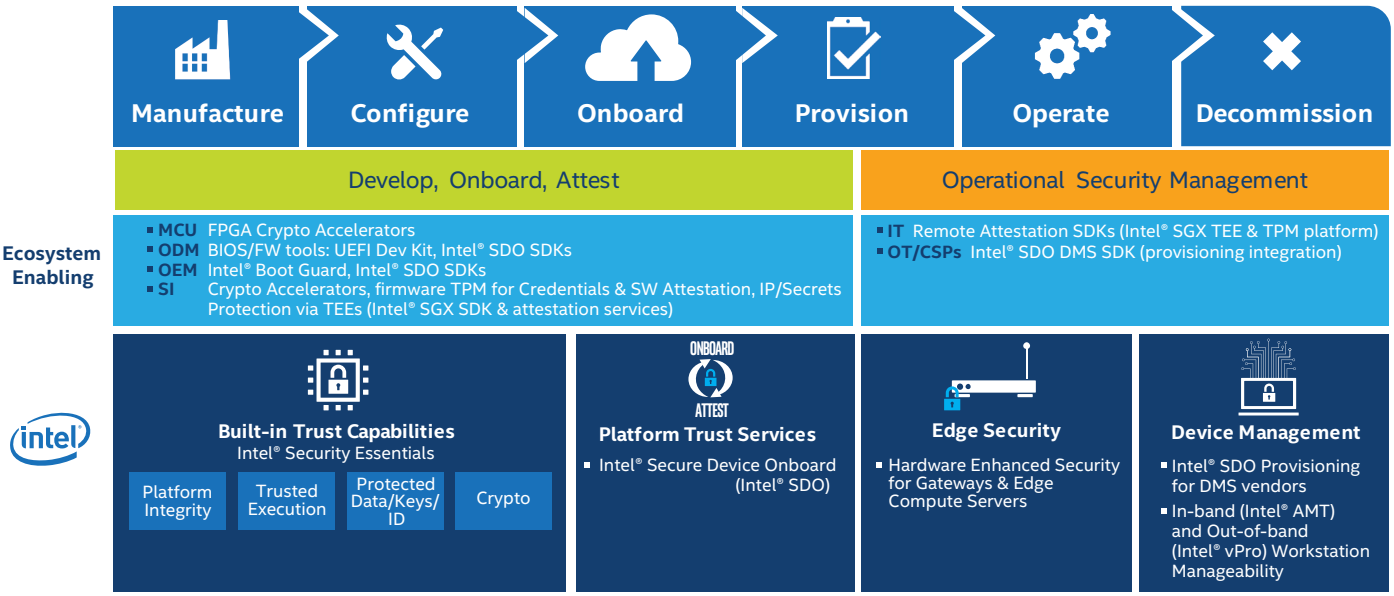


Figure 15. Security involved in every lifecycle phase of an IoT device.

requirements may not be known, ODM/OEM adoption of Intel Security Essential's capabilities provides a minimum baseline to help future proof the device for a broad range of security usages. Enabling:

- ODM use of Intel's BIOS/FW tools.
- OEM decisions to incorporate Intel® Boot Guard, Intel PTT as a hardware TPM for measured boot, and Intel SDO client SDKs to seed the device for secure onboarding.

The Configuration/Build Phase is generally implemented by System Integrators or security ISVs that begin to activate capabilities in software using Intel's API/SDKs to meet the customers end security requirements. Enabling:

- Intel SGX as a trusted execution environment can provide the application runtime memory protection.
- Device Management System instrumentation to leverage Intel PTT's measured boot attestation reports that validate firmware/BIOS/boot loader/OS integrity.

The Deployment/Operational/Decommission phases involves IT and OT departments in the enterprise that onboard the device on to the corporate network and set up the command, control, and monitoring infrastructure.

- OT's device installers can leverage Intel SDO for password free zero-touch onboarding to IT and OT systems.
- Device Management Systems and Intel SDO can be used to push a secure image update that may contain credentials, firewall configurations, or security patches.
- Provisioning of additional application secrets into an Intel SGX application enclave.
- Device inventory management is improved with Intel PTT's attestation, as you know which devices run where along with security health status.
- Retirement and decommissioning through device management systems can safely remove assets/secrets from multiple vendors that may reside in the device. Intel SDO enables a graceful resale capability to transfer ownership of a device to another party for re-provisioning.

6.0 CONCLUSION

The rapid adoption of IoT, OT, and cyber-physical systems has opened new attack surfaces that threaten critical infrastructure and individual privacy. The industry has a narrow window of opportunity to put in place designed-in security protections that can help protect devices throughout their long lifecycles. Intel can equip the coming wave of intelligent edge devices with a high performance security model based on Intel Security Essentials foundation of trust capabilities. Intel's unique ability to enable the entire ecosystem with best practice protection tools will accelerate consistent implementations and advance IoT security.

Learn More

- **Device Onboarding**- www.intel.com/securedeviceonboard
- **Hardware Security** - www.intel.com/content/www/us/en/security/hardware/hardware-security-overview.html

[1] Used with permission from Bain & Company*. Source: www.bain.com/IOT-cybersecurity . "Cybersecurity Is the Key to Unlocking Demand in the Internet of Things"-Oct 11, 2018

[2] Worldwide IoT Forecast, 2015-2025, IDC#25639

[3] Processors to Meet IoT Endpoint Analytics and Security Demands - Gartner Market Insight - Nov, 2017.

[4] DRNG FIPS certification-https://software.intel.com/en-us/articles/intel-digital-random-number-generator-drng-software-implementation-guide

[5] Contact your Intel account manager for TME platform availability. Spec announcement https://software.intel.com/en-us/blogs/2017/12/22/intel-releases-new-technology-specification-for-memory-encryption.