SOLUTION BRIEF

Security

Intel® Security Essentials

Security Designed-in From the Start to Deliver Best Practice Hardware Protections

> "While it can be implemented in software, it is only through dedicated hardware that the root of trust is truly immutable. Lower cost & better ease of use will democratize adoption."
>
> - Michela Menting, Director ABI Research

Fragmented Adoption

Today, implementing hardware-based security is a widely recognized best practice compared to software-only based approaches. However, the complexities of enabling systems with discrete hardware security components from multiple vendors creates design, deployment, and operational barriers that hinder adoption of such protections. With multiple discrete hardware security components, each with different and disconnected root of trust capabilities (see Table 2) it may not be possible to fully integrate these security capabilities into a cohesive security architecture. The result is often a fragmented solution with significant barriers for upgrades post-deployment. In contrast, Intel's general purpose systems-on-a-chip (SoCs) with integrated security offer a new way forward to implement hardware-based security.

Intel Security Essentials – Built-in Foundation with Security at the Core

Intel's built-in foundation of security capabilities are called Intel® Security Essentials. These core capabilities are available[3] across Intel® processor lines. They enable security professionals to protect the platform and the data, and to 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 for ecosystem innovation (see Table 1).

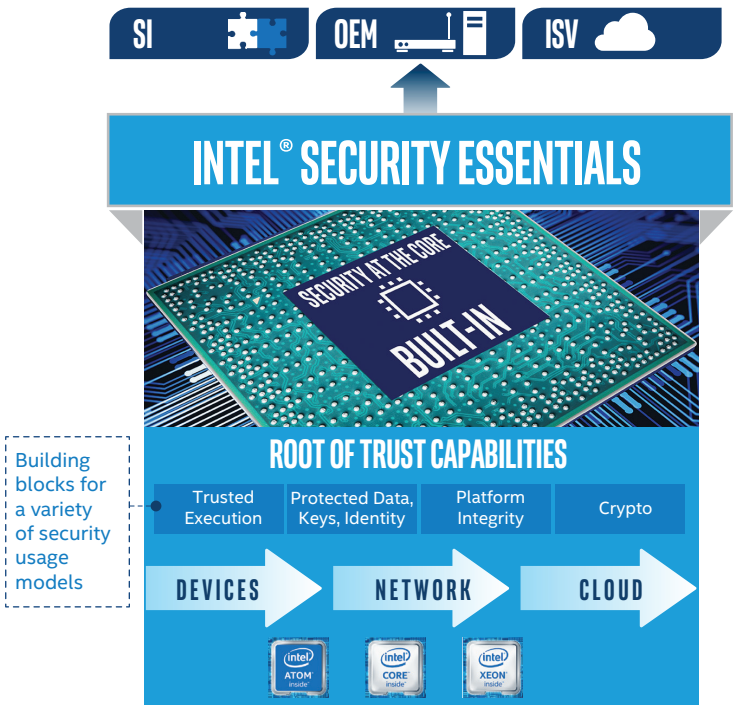

Figure 1. Intel® Security Essentials

Benefits

- **High Security Model** – Recommended suite of security capabilities (see Table 1)
- **Integrated** – Built-in to Intel processors and chipsets for lower cost and higher performance
- **Consistent Usages** – Foundational firmware and development libraries for consistent ecosystem implementations
- **Performance** – Headroom to handle future security workloads, and flexibility to upgrade firmware in the field to respond to evolving threats

Protecting Attack Surfaces with Solutions Rooted in Hardware Trust

To best harden platform attack surfaces, security technologies should be rooted in hardware (see Figure 2). Such hardening is critical as attackers are increasingly exploiting software vulnerabilities and launching sophisticated attacks on hardware. Each surface layer builds on the security of the layers below—for example, a hardened BIOS/FW surface layer provides a firmer foundation for OS/VMM though mechanisms such as protected boot.

Although hardware-based security is not a silver bullet, it does provide a "chain of trust" rooted in silicon that makes the device and extended network more trustworthy and secure (see Table 1). Intel Security Essentials equips original equipment manufacturers (OEMs), system integrators (SIs), operating system vendors (OSVs), and independent software vendors (ISVs) with the building block ingredients to implement a variety of security usage models and best practices (see Table 2).

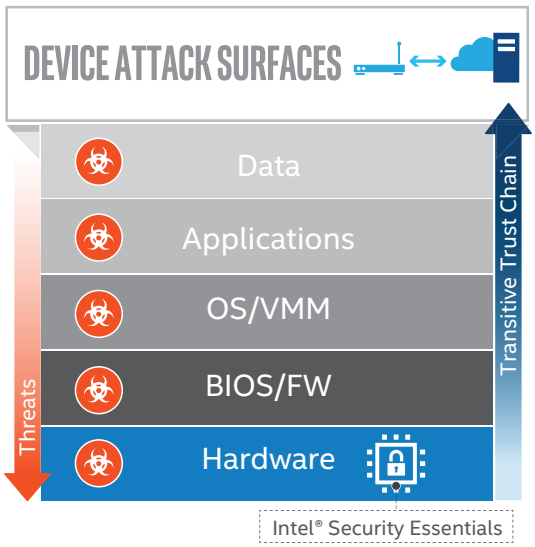

Figure 2. Transitive Chain of Trust

A Silicon-Centric Approach for Performance, Consistency and Upgradeability

Intel is delivering a wave of transformational computing models for artificial intelligence (AI), autonomous driving, 5G networks, software-defined data centers, and internet of things (IoT). These models demand higher performance[1] and lower latency from compute-intensive security operations. Leveraging security features integrated into the processor and chipset provides performance and cost-optimized security capabilities with tighter integration.

A fragmented approach to security tends to create point solutions that can be difficult to scale. Generally, each device manufacturer assembles a specific set of security components to address a particular threat model. Parts from disparate suppliers may be incompatible, thereby making it harder to update or upgrade deployed security capabilities in response to evolving threats.

Intel Security Essentials is designed to a consistent security architecture that hardens and protects against a wide range of attacks. In some cases, a silicon-centric approach with security designed–in may alleviate the need for a separate dedicated security co-processor.

Properties of Highly-Secure Trusted Computing

Intel Security Essentials delivers a foundational suite of security capabilities that deliver a chain of trust to help protect surfaces from attack.

- **Crypto** - Hardware-assisted crypto acceleration and secure key generation
- **Protected Data, Keys, and Identity** - Encryption and storage for sensitive data, keys, or credentials, at rest and in transport
- **Platform Integrity** - Protected and verified boot process with hardware attestation of the platform
- **Trusted Execution** - Isolated enclaves to help protect sensitive data, processes, and keys at runtime and create a trusted application environment

To be equipped for a high security model (see Table 1), a device should be instrumented to take advantage of all of the capabilities of Intel Security Essentials.

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	✓
Direct Anonymous Authentication	Cryptographic scheme provides anonymous attestation and authentication of device for improved privacy	✓
HW Security Acceleration	Hardware acceleration of cryptographic math calculations, key generation, and malware scanning.	✓

Table 1. Properties of Highly Secure Devices[2]

Technologies to Implement Core Capabilities

Intel processors, including Intel® Atom®, Intel® Core®, and Intel® Xeon®-based platforms, can enable the four core capabilities of Intel Security Essentials. Figure 3 shows the broad range of security usage models and layers that can be rooted in these hardware-based security capabilities. Many of the capabilities

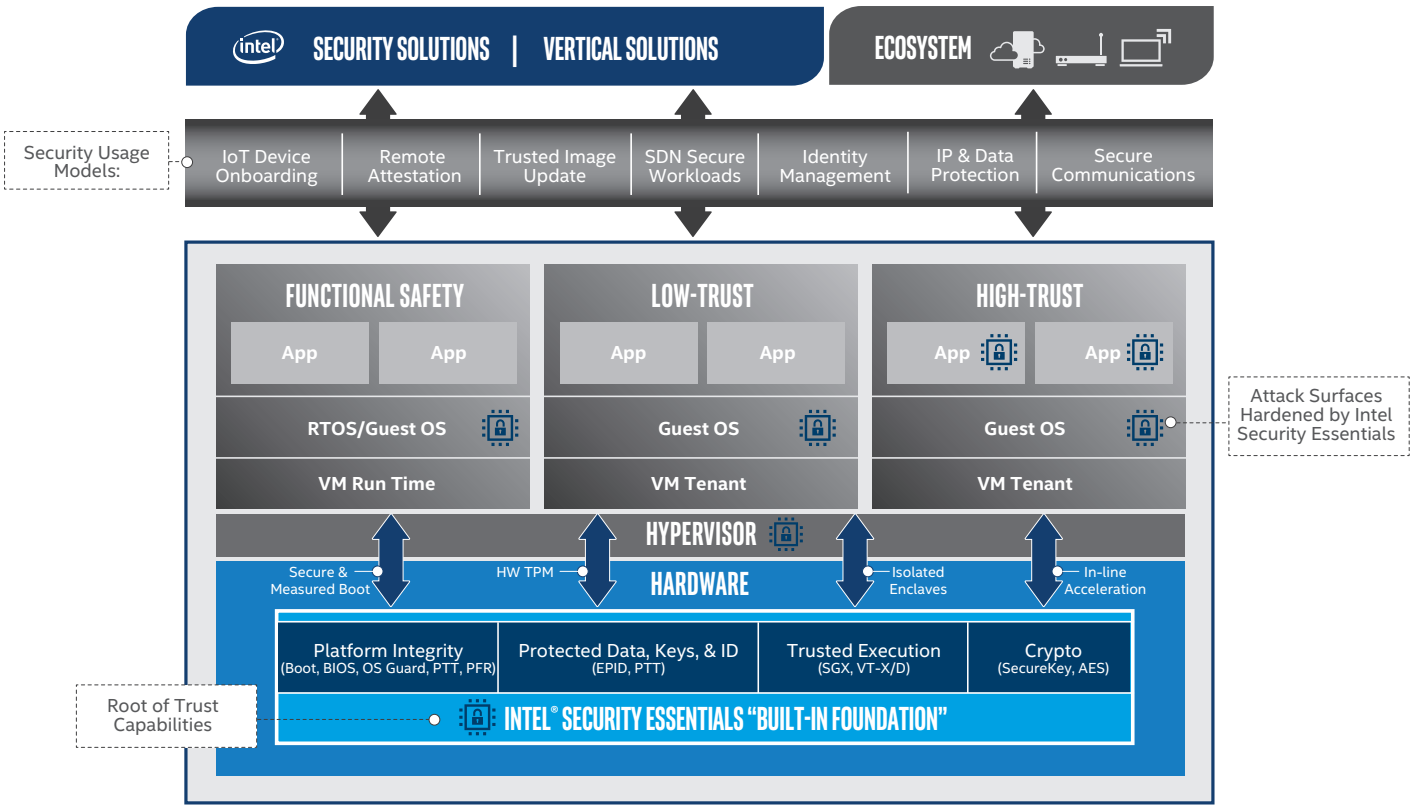

Figure 3. Sample Device and Solution Stack Rooted in Hardware-based Trust

can be used to help the device protect itself (see Figure 2) or to extend trust remotely to cloud services and solutions.

Table 2 (next page) gives a sample view of each Intel Security Essentials technology available to the ecosystem, and the corresponding attack surface protected. The optimal mix of technologies to implement varies depending on the market segment use case, threat, risk, and performance profile of the device workload. Sample usages:

IoT - A constrained IoT device might leverage Intel® Enhanced Privacy ID (Intel® EPID) identity technology with a device management service to help ensure privacy during on-boarding. After on-boarding, the service could provision image updates to store additional identities using Intel Security Essentials protected data and key capabilities.

Cloud - Software-defined data centers in the cloud and fog-based IoT edge environments are consolidating workloads to run in virtualized compute pools. Each distinct workload may require different levels of trusted execution. In a low-trust example, Intel® Virtualization Technology (Intel® VT) in Intel Security Essentials could be used to restrict VMM access as VMs migrate across servers to avoid compromise. Conversely, a high-trust model could leverage Intel SGX technology to wrap application containers with a more granular set of runtime protections.

Ecosystem Enabling and Roles

Intel Security Essentials provides a consistent approach that packages integrated firmware, development libraries, validation on a wide range of operating systems, and support. Because of its hardware strengths, Intel is uniquely positioned to influence and promote a consistent hardware security model across a broad ecosystem.

Although end-customer security requirements may not be known at the time of device manufacture, enabling for Intel Security Essentials can help future-proof the device against evolving threats by seeding security best practice capabilities (see Table 1).

Sample ecosystem roles for enabling Intel Security Essentials include:

- **OEMs** - Use the BIOS/firmware security tools
- **OEMs** - Incorporate protected boot and activate the hardware TPM
- **OEMs & SIs** - Instrument measured boot and publish known-good platform attestation reports, allowing the ecosystem to validate firmware/BIOS/boot loader/OS integrity on protected platforms
- **OSVs** - Incorporate the security foundation provided by the platform to enhance the security of the operating system and/or hypervisor
- **SIs & ISVs** - Incorporate a trusted execution environment inside the application to deliver runtime memory and

replay protections, and to enable remote provisioning of secrets to the hardware platform

- **IoT Device Management, Cloud and Fog Platforms** - Leverage devices with Intel EPID for anonymous remote attestation to ensure privacy and to comply with the Global Data Protection Regulation (GDPR)
- **Intel® Solutions** – Intel Security Essentials root of trust capabilities are integrated into vertical solutions: from autonomous driving, 5G networks, and software-defined data centers, to laptop and modem hardware. Intel also offers turn-key security solutions that leverage Intel Security Essentials to solve a specific security use case. Examples include Intel® Secure Device Onboard (IoT provisioning) and cloud data protection (Intel SGX for blockchain)

IoT ISV Ecosystem Example:

Wind River® Titanium Control is an on-premise cloud infrastructure platform that delivers the level of performance needed for workload consolidation of industrial applications and control services. Titanium Control is optimized with hardware root-of-trust security. Specific optimizations with Intel Security Essentials include:

- **Trusted Execution** - Isolation for VMM workloads leveraging Intel VT
- **Platform Integrity** - Secure and measured boot with hardware TPM delivers cryptographically-signed images for host environment protection
- **Protected Data, Keys, and Identity** - Administrative credentials and private keys used for Transport Layer Security (TLS), secure communications stored in the hardware TPM
- **Crypto** - Platform acceleration for Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI) ensures near-real time system-wide performance

CORE CAPABILITY	TECHNOLOGY	PROTECTION FOR	DESCRIPTION
Platform Integrity	Intel® Platform Protection Technology with Boot Guard	BIOS/FW	Verifies OEM pre-OS boot loader code executing out of reset
	Intel® Platform Protection Technology with BIOS Guard	BIOS/FW	Enables a HW based static Root of Trust for measurement and verification for boot integrity
	Intel® Runtime BIOS Resilience	OS/VMM	Helps protect SSM from malicious code injection
	Intel® Platform Protection Technology with OS Guard	OS/VMM	Helps prevent malicious code from executing out of application memory space
	Intel® Platform Firmware Resiliance	BIOS/FW	Helps protect firmware from corruption; assists with system restoration in case of malware
Trusted Execution	Intel® Software Guard Extensions	Apps	Enables creation and use of isolated app enclaves to protect against attacks on executing code or data stored in memory
	Intel® Virtualization Technology	OS/VMM	Creates firewall between main OS and secure workloads running inside a secure VM
Protected Data, Keys, Identity	Intel® Platform Trust Technology	Data	Integrated HW TPM enables secure storage of keys/credentials, registry values, & boot block measurements for remote attestation
	Intel® Enhanced Privacy ID	Data	Cryptographic scheme provides direct anonymous attestation of hardware for privacy
Crypto Accelerators	Intel® Data Protection Technology with Secure Key	Data	High entropy source of random numbers to generate keys
	Intel® Advanced Encryption Standard New Instructions	Data	Accelerates math calculations for AES-NI encryption

Table 2. Intel Security Essentials Implementation Technologies[3]

Learn More

Solution overview and collateral:
https://intel.com/content/www/us/en/security/
https://hardware/hardware-security-overview.html

References

(1) "Design-In High-Performance Processors to Meet IoT Endpoint Analytics and Security Demands"- Gartner Market Insight- November, 2017

(2) Galen Hunt, George Letey, and Edmund B. Nightingale, "The Seven Properties of Highly Secure Devices," Microsoft Research NExT Operating Systems Technologies Group, 2018.

(3) Represents a sample of Intel technologies that can be used to implement the capability. Many security technologies are designed for vertical specific use cases and may not be relevant for all market sectors. Intel is not announcing specific availability of technologies by platform, for more information on relevance or availability by platform, contact your Intel account manager. The Intel® Security Essentials announcement does not deliver new technologies. With Intel Security Essentials, Intel has defined and validated the specific technologies that can be used to deliver each of the core capabilities.