Lockheed Martin Hardened Security for Intel® Processors

LOCKHEED MARTIN

Lockheed Martin Hardened Security for Intel® Processors

Create a Zero Trust environment using Hardened Security attribute-based controls

In the era of digital transformation, where technologically advanced companies are competing for market share, agile, secure, and efficient automating technologies that reduce time to market for products are essential to establishing market dominance. These emerging technologies are leveraging cloud to edge computing, which are dependent on innovations in 5G, software defined networking (SDN), virtualization, quality of service, and processor security technologies.

Digital transformation is necessary, but it also presents new security challenges. Organizations have traditionally used role-based access controls to protect their data. Role-based access controls grant unrestricted critical compute and data access based on a user's physical location and assigned group or department. But digital transformation has rendered role-based access controls ineffective against advanced threats. This combined with the acceleration of remote work and the increased use of digital networks to interact with customers creates the need for a new security model to counteract external bad actors and insider threats.

As a result, companies are moving to a Zero Trust security model to secure intellectual property and avoid operational compromise. Zero Trust security alters the security posture by assuming critical computing assets and data are untrusted until they are authenticated, thereby only granting access to resources that are required at the time they are used. Companies can accomplish Zero Trust by implementing attribute-based security controls.

Attribute-based access controls perform cryptographic verification and authentication of critical resources at the time required to execute. A security architect must also consider how strong the security boundary of the asset is versus other assets. This is where strong virtualization isolation technologies prevent data spills across security boundaries defined by the cryptographically verified attributes.

Lockheed Martin Hardened Security

Lockheed Martin Hardened Security* offers a hardened, full-stack security solution that utilizes attribute-based controls to isolate and protect virtual machines (VMs) at runtime and allocate compute resources for more consistent performance that creates a Zero Trust environment. This verified solution on 2nd and 3rd Generation Intel® Xeon® Scalable processors simplify deployments and help to protect your most valued data at the edge and in the data center with:

- **Power-On Boot Protections:** Boot protections and a chain of trust from power-on through the launching of your most critical applications at runtime.

**Lockheed Martin Hardened Security is part of the Intel Select Solutions portfolio - a classification Intel awards to solutions that have been benchmark-tested, verified, and optimized for real-world performance.*

• **UEFI Virtual Secure Boot:** Independent UEFI BIOS secure boot virtual machine environments supporting industry standard keys or customer generated x.509 keys for a secure chain of trust extending beyond just platform boot but also inclusive of an instance's virtual environment. Protects customers from third party global industry accepted keys imported from power-on, prohibiting the changing of the platform without customer approval.

• **Runtime Security (Isolated Resources):** User controls and security choices to isolate and protect virtualized workloads. Provides segmentation of shared resources such as cores, cache, memory, and devices.

• **Quality of Service (QoS):** More consistent and deterministic performance with isolated VMs through the segmentation and ideal allocation of compute resources.

• **Inline Memory Encryption:** On 3rd Generation Intel® Xeon® Scalable processors, hardware accelerated Multi-Tenant Key inline memory encryption protects from unauthorized data access from external threats and cross tenant domain attacks while preserving processor performance.

• **Reduce Total Cost of Ownership (TCO):** Promotes the reduction of growing ownership and security costs. Modernize infrastructure by consolidating multiple, complex, and dedicated legacy servers into a simplified and partitioned solution with advanced performance, new security protections, and QoS features. Minimize time, cost, and complexity of evaluating and integrating hardware and software.

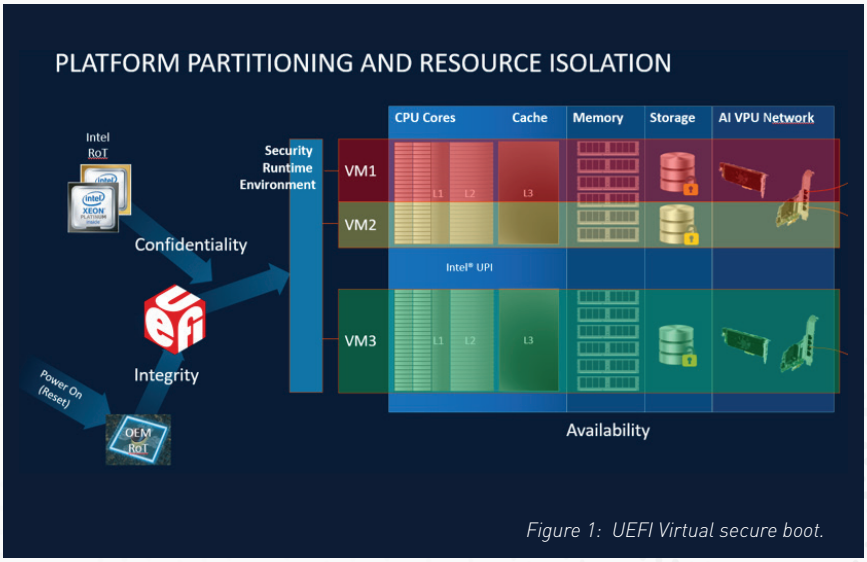

Figure 1: UEFI Virtual secure boot.

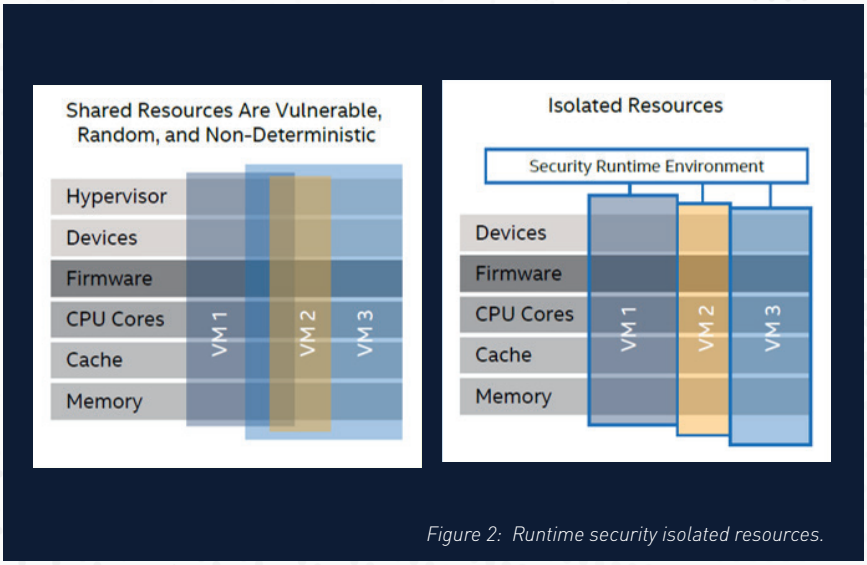

Figure 2: Runtime security isolated resources.

Hardened Security Advantages

Lockheed Martin's Hardened Security can revolutionize an organization's ability to protect its most vital information and better defend against complex threats in the age of digital transformation. These solutions run secure workloads on one of the most protected platforms in the industry, from boot through runtime, and address both security and quality of service (QoS) while delivering unique advantages over traditional security systems.

	LOCKHEED MARTIN HARDENED SECURITY	TRADITIONAL SECURITY
Minimize time, cost & complexity	Design-in security, preserved interoperability. Increased agility to deploy on the latest HW, SW, and orchestration. Reduced costs, labor, and integration demands.	More custom, less scalable, difficult to update/maintain to latest HW/SW. Expensive and labor intensive. Multiple HW/SW integration demands.
Virtualized workload isolation & protection	Customer authorized, signed, multi-tenant VM/resource isolation. Multiple attribute based security controls (NIST SP800-53-D5) per virtual environment. Hardware accelerated inline memory encryption with hardware secured independent virtual machine domain keys.	Traditional workload isolation methods (core pin/memory/devices) are not mapped to firm security policies or signed by authorized user. Security is dependent on platform admin. Lacking per instance memory encryption to protect against attacks not assigned to virtual machine instance.
Dedicated security environment secure from boot	Securely controlled/load verified OS & software versions from authorized OEMs/ISVs. Cryptographically-bound to a customer's private key.	Large attack surface, lacks integrity and relies on public/3rd party keys controlled by multiple, global companies.
Boot protections for system Integrity and virtual machine instance	Protects boot from start-up through launch using virtualized UEFI Secure Boot capability by enabling per instance independent customer provided UEFI Secure Boot Keys.	Vulnerable during system start-up and reset. System, OS, and software integrity may be compromised and vulnerable. 3rd party company signed and trusted by commercial ecosystem. Common Single UEFI Platform Secure Boot Keys applied to all virtual machine instances if enabled.
Per Part-Specific Unique Ids	Crypto-unique IDs that are on-CPU and used for key derivation. Example: CPU Socket Bounded LUKS disk encryption.	Confidentiality keys protected via external and off-CPU TPMs/devices that use un-encrypted communications for key transport.
Security policies & tenants independent of Orchestration	Hardened Security policy cannot be changed by platform's admin or cloud service provider; only by individual and authorized guests or tenants.	Traditional solutions (even NSA red/black security bare metal solutions) still need additional protections across guests for vulnerabilities. Susceptible to a platform admin or cloud service providers insider threat.
Operations real-time, noisy neighbor protection, consistent/predictable performance	Ease-of-use secure runtime domains with attribute based controls setting up deterministic control of cores, cache, memory, etc.	Poor determinism due to oversubscription and lack of controls offered by the platform owner or cloud service provider force tenants to overbuy capacity to meet workload demand.

Verified to Simplify Deployments and Reduce Cost of Ownership

Infrastructure modernization has not been easily addressable in conventional VM environments due to security, performance, determinism, complexity, and cost requirements. Lockheed Martin Hardened Security is tested and verified to optimize price and performance and reduce infrastructure TCO and evaluation time. Modernization permits:

- Fewer systems to manage
- Simplified deployments, integrations, and evaluations
- Reduced power and cooling costs
- Less rack space taken up by servers
- Potentially lower software licensing costs
- Potentially faster and easier deployment than setting up and validating systems piecemeal
- Potentially lower operating costs, like system management

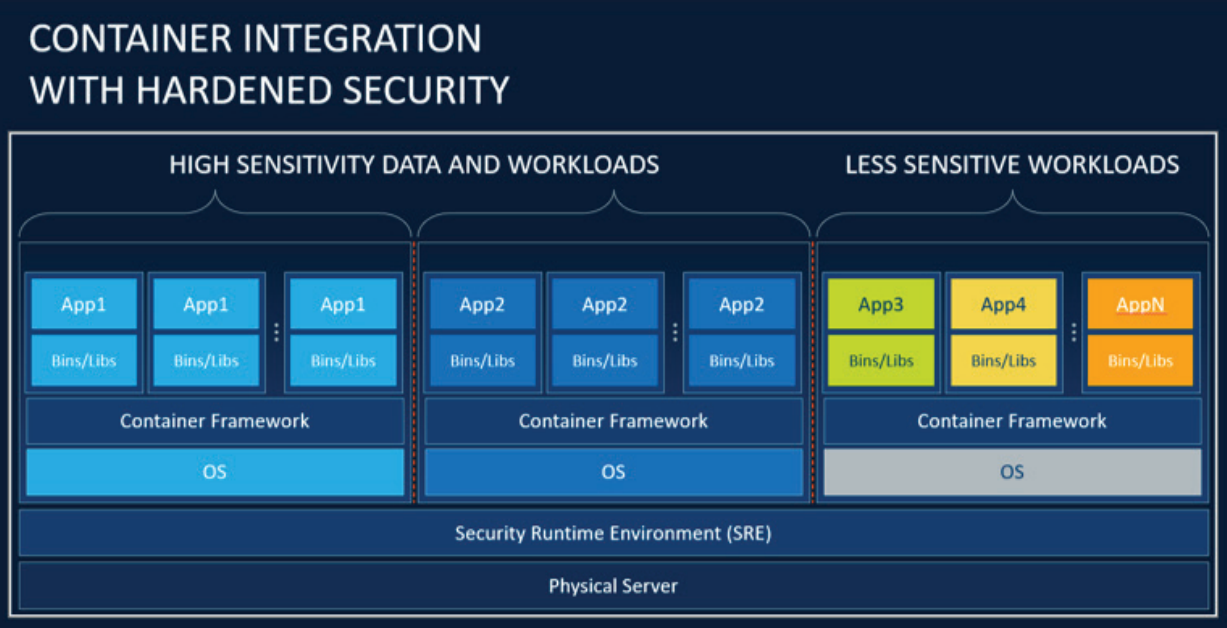

Figure 3: Orchestrated deployment of hardened security.

Hardened Security Controls

Lockheed Martin Hardened Security offers the following attribute-based security controls to prevent breaches and secure critical information:

- IC1.1 SPI flash/PCH configuration controls protected via FD0V
- IC1.2 Intel® Core™ processor mandatory verified boot (BtG)
- IC1.3 UEFI secure boot
- IC1.4 Hardware entropy seeding and generation
- IC1.5 Hardware-based revocation and version control
- IC2.1 Domain boot integrity verification (standard and above)
- IC2.2 Generated cryptographic key (standard and above)
- IC2.3 Core isolation: cores are dedicated to VMs (standard and above)
- IC2.4 Socket isolation: VMs make no cleartext UPI communications (standard and above)
- IC2.5 Memory isolation: dedicate pages per VM (standard and above)
- IC2.6 Cache isolation (enhanced and above)
- IC2.7 Hyperthread sibling containment (enhanced and above)
- IC2.8 Contained within NUMA node (enhanced and above)
- IC2.9 Memory encryption (high only)
- IC2.10 Memory encryption and integrity (high only)
- IC2.11 Hardware entropy seeding and generation
- IC2.12 Hardware seeded keyed disk encryption (LUKS)
- IC2.13 Domain-based PCI* direct mapping, policy signing, and enforcement
- IC2.14 Policy-based revocation and version control per domain/tenant

CAPEC-3000: Domains of Attack

ID	TYPES OF ATTACK	LIKELIHOOD OF ATTACK	TYPICAL SEVERITY	CONTROL C HARDENED SECURITY CONTROL IDS
112	Brute Force	Undefined	High	Runtime IC2.2, IC1.4, IC2.11, IC2.12
115	Authentication Bypass	Undefined	Medium	Runtime IC2.2, IC1.4, IC2.11, IC2.12
125	Flooding	High	Medium	Runtime IC2.3, IC2.5, IC2.6
130	Excessive Allocation	Medium	Medium	Runtime IC2.3, IC2.5, IC2.6
131	Resource Leak Exposure	Medium	Medium	Runtime IC2.3, IC2.5, IC2.6
176	Configuration/Environment Manipulation	Undefined	Medium	Runtime IC2.12
184	Software Integrity Attack	Undefined	Low	Boot Time IC1.1, IC1.2, IC1.3, IC1.4, IC2.1, IC2.11
188	Reverse Engineering	Low	Low	Runtime IC1.4
21	Exploitation of Trusted Credentials	High	High	Runtime IC1.4, IC2.11
227	Sustained Client Engagement	Undefined	Undefined	Runtime IC2.3, IC2.5, IC2.6
240	Resource Injection	High	High	Boot Time IC1.1, IC1.2, IC1.3, IC1.4
242	Code Injection	High	High	Boot Time IC1.1, IC1.2, IC1.3, IC1.4
28	Fuzzing	High	Medium	Boot Time IC1.1
438	Modification During Manufacture	Undefined	Undefined	Boot Time IC1.1, IC1.2, IC1.3, IC1.4
439	Manipulation During Distribution	Undefined	Undefined	Boot Time IC1.1, IC1.2, IC1.3, IC1.4
440	Hardware Integrity Attack	Low	High	Boot Time IC1.1, IC1.2, IC1.3, IC1.4
507	Physical Theft	Undefined	Undefined	Runtime IC1.4, IC2.11, IC2.12
549	Local Execution of Code	Medium	High	Boot Time IC1.2, IC1.3, IC2.13
554	Functionality Bypass	Medium	High	Boot Time IC1.2, IC2.1
624	Fault Injection	Low	High	Boot Time IC2.3, IC2.4, IC2.5, IC2.6, IC2.7, IC2.8, IC2.9, IC2.10
123	Buffer Manipulation	High	Very High	Runtime IC2.5, IC2.9, IC2.10
233	Privilege Escalation	Undefined	Undefined	Runtime IC2.3, IC2.5, IC2.6
25	Forced Deadlock	Low	High	Runtime IC2.3, IC2.5, IC2.6
26	Leveraging Race Conditions	High	High	Runtime IC2.3, IC2.5, IC2.6
441	Malicious Logic Insertion	Medium	High	Boot Time IC1.1, IC1.2, IC1.3, IC1.4, IC2.1, IC2.11, IC2.14
607	Obstructon	Undefined	Undefined	Boot Time IC1.1, IC1.2, IC1.3, IC1.4, IC2.1, IC2.11, IC2.14

Figure 4: Hardened Security Controls: This table demonstrates which Hardened Security controls can be used to combat standard security attacks.

What are Intel® Select Solutions?

Intel Select Solutions are pre-defined, workload-optimized solutions designed to minimize the challenges of infrastructure evaluation and deployment. Solutions are validated by OEMs/ODMs, certified by ISVs, and verified by Intel.

Intel develops these solutions in extensive collaboration with hardware, software, and operating system vendor partners and with the world's leading data center and service providers. Every Intel Select Solution is a tailored combination of Intel® data center compute, memory, storage, and network technologies that delivers predictable, trusted, and compelling performance.

To refer to a solution as an Intel Select Solution, a vendor must:

1. Meet the software and hardware stack requirements outlined by the solution's reference-design specifications
2. Replicate or exceed established reference-benchmark test results
3. Publish a solution brief and a detailed implementation guide to facilitate customer deployment

Solution providers can also develop their own optimizations to give end customers a simpler, more consistent deployment experience.

Contact Us

For more information about Lockheed Martin Hardened Security or to get in contact with one of our team members, visit our website: ***www.lockheedmartin.com/hardenedsecurity.***