SOLUTION BRIEF

Intel® Select Solutions
Enterprise Data Center Infrastructure
June 2019

Intel® Select Solutions for Hardened Security with Lockheed Martin

Help protect high-value data at runtime through a hardened full-stack security solution.

Intel® Select Solutions for Hardened Security with Lockheed Martin offer a hardened, full-stack security solution that isolates and protects virtual machines (VMs) at runtime and ideally allocates compute resources for more consistent performance. These verified solutions on 2nd Generation Intel® Xeon® Scalable processors simplify deployments and help to protect your most valued data at the edge and in the data center with:

- **Boot Protections**: Boot protections and a chain of trust from power-on through the launching of your most critical applications at runtime. Verifies and maintains system integrity at boot.
- **Runtime Security**: 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.
- **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 your time, cost, and complexity of evaluating and integrating hardware and software.

Hardened Security by Intel and Lockheed Martin

Intel Select Solutions for Hardened Security with Lockheed Martin represent a combination of Intel and Lockheed Martin developed technologies to deliver capabilities from system power on, through boot, BIOS load, and the runtime of applications in a VM environment. Intel Select Solutions for Hardened Security with Lockheed Martin provide hardware-enforced firewalling that helps separate sensitive data from untrusted workloads, providing cross-domain protection against leakage, modification, and privilege escalation. Partitioning and isolation of shared resources (such as cache, cores, memory, and devices) in the virtualized environment supports your confidentiality, integrity, and availability, and provides more consistent application performance. Isolation techniques create more runtime security domains within a trusted virtualization environment. The solutions are resistant to unauthorized modifications with advanced security features to help mitigate information leakage outside of each isolated runtime security domain.

Verified by Intel 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. Intel Select Solutions for Hardened Security with Lockheed Martin are tested and verified by Intel 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

User controls over VM security capabilities and resource assignment significantly increase your agility for deploying and managing secure virtualized workloads.

Hardware Selections

Intel Select Solutions for Hardened Security with Lockheed Martin pair Intel® processor capabilities and Lockheed Martin expertise to deliver a new level of reliable security and advanced QoS for VM environments. Intel compute, storage, and networking hardware enable businesses to quickly deploy hardened security on a performance-optimized infrastructure.

2nd Generation Intel® Xeon® Scalable Processors

Intel Select Solutions for Hardened Security with Lockheed Martin are available on 2nd Generation Intel Xeon Scalable processors. Intel Xeon Gold processors provide Intel Select Solutions for Hardened Security with Lockheed Martin with an excellent performance-to-cost ratio. These 2nd Generation Intel Xeon Scalable processors provide performance to support hardened virtualization and encryption protection. In addition, 2nd Generation Intel Xeon Scalable processor–based technologies further boost VM performance and security.

Intel® SSD Data Center Family

Intel Select Solutions for Hardened Security with Lockheed Martin are validated on Intel® Solid State Drive (SSD) DC P4510 drives. Storage latency and size can be bottlenecks for VM and container performance, and Intel SSD DC P4510 drives are recommended for data storage. Based on Intel® 3D NAND technology, these enterprise data center SSDs use the NVM Express* (NVMe*) protocol over the PCIe* interface to provide superior performance, outstanding quality, reliability, advanced manageability, and serviceability to minimize service disruptions. Intel SSD DC P4510 drives comply with the Opal v2.0* specification for self-encrypting drives published by the Trusted Computing Group. This specification manages drive encryption and authentication to protect the confidentiality of stored user data against unauthorized access.

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 in order to give end customers a simpler, more consistent deployment experience.

Intel® Ethernet Connections and Intel® Ethernet Adapters

The 25Gb Intel® Ethernet 700 Series Network Adapters accelerate the performance of Intel Select Solutions for Hardened Security with Lockheed Martin. The Intel Ethernet 700 Series delivers validated performance ready to meet high-quality thresholds for data resiliency and service reliability with broad interoperability.[1] All Intel Ethernet products are backed by worldwide pre- and post-sales support and offer a limited lifetime warranty.

The Intel® Ethernet Converged Network Adapter X710 Series provides 10 gigabit Ethernet (GbE), with 40 GbE available for the most demanding workloads. These network adapters provide intelligence and performance for network packet processing and flexible, scalable input/output (I/O) virtualization and intelligent offloads to improve the performance and efficiency of virtualized environments.

Verified Performance through Benchmark Testing

All Intel Select Solutions are verified through benchmark testing to meet a prespecified minimum capability level of workload-optimized performance. Intel Select Solutions for Hardened Security with Lockheed Martin provide a hardened virtualization platform addressing a full range of security controls. They offer improved availability through more deterministic QoS and protections from noisy neighbors, greater data confidentiality through VM encryption/isolation, and robust integrity with a chain of trust from boot through runtime. Using the LINPACK* and HammerDB* benchmark tests, Intel verified the solutions can provide up to 760 gigaFLOPs (GFLOPS) and up to 442,000 transactions per minute (TPM).[2]

Base Configuration

Intel Select Solutions for Hardened Security with Lockheed Martin are available in a "Base" configuration, as detailed in Table 1. The Base configuration specifies the minimum required performance capability for the solutions.

To refer to a solution as an Intel Select Solution, a server vendor or data center solution provider must meet or exceed the defined minimum configuration ingredients and reference minimum benchmark-performance thresholds listed below.

Table 1. Base configuration for the Intel® Select Solutions for Hardened Security with Lockheed Martin

INGREDIENT	INTEL® SELECT SOLUTIONS FOR HARDENED SECURITY WITH LOCKHEED MARTIN **BASE CONFIGURATION**
SINGLE NODES	
PROCESSOR	2 x Intel® Xeon® Gold 6248 processor (2.50 GHz, 20 cores, 40 threads), Intel Xeon Platinum 8260 processor, Intel Xeon Platinum 8268 processor, Intel Xeon Platinum 8280 processor, or a higher number Intel Xeon Scalable processor
MEMORY	768 GB or higher (24 x 32 GB DDR4-2666)
BOOT DRIVE	2 x Intel® SSD DC S4510 (mirrored boot 240 GB, 2.5-inch) or higher
DATA TIER	2 x Intel SSD DC P4510 (1 TB, 2.5-inch, NVM Express* [NVMe*]) or higher, Opal* ready
DATA NETWORK	10Gb Intel® Ethernet Converged Network Adapter X710-DA2 SFP+
MANAGEMENT NETWORK PER NODE	Integrated 1 GbE port 0/RMM port
SOFTWARE	
OPERATING SYSTEM	CentOS 7.5*
SOFTWARE STACK	Security Runtime Environment 3.6
TRUSTED VIRTUALIZATION ENVIRONMENT	Lockheed Martin Trusted Virtualization Environment*
APPLIES TO ALL NODES	
TRUSTED PLATFORM MODULE (TPM)	TPM 2.0
FIRMWARE AND SOFTWARE OPTIMIZATIONS	Intel® Boot Guard enabled** Intel® Hyper-Threading Technology (Intel® HT Technology) disabled Intel® Turbo Boost Technology enabled P-states enabled** C-states enabled** Power-management settings set to performance** Workload configuration set to balanced** Intel® Memory Latency Checker (Intel® MLC) streamer enabled** Intel MLC spatial prefetch enabled** Data Cache Unit (DCU) data prefetch enabled** DCU instruction prefetch enabled** Last-level cache (LLC) prefetch disabled** Uncore frequency scaling enabled**
MINIMUM PERFORMANCE STANDARDS Verified to meet or exceed the following minimum performance capabilities:[2]	
	Mitigations against a *minimum* of 19 attack domains while delivering a *minimum* of 760 gigaFLOPs (GFLOPS) in a VM, as measured by LINPACK* 442,000 transactions per minute (TPM) in a VM, as measured by HammerDB*

**Recommended, not required

Technology Selections for Intel Select Solutions for Hardened Security with Lockheed Martin

In addition to the Intel hardware foundation used for Intel Select Solutions for Hardened Security with Lockheed Martin, other Intel technologies integrated in 2nd Generation Intel Xeon Scalable processors deliver further security, QoS, and reliability gains, including:

- **Intel® Advanced Vector Extensions 512 (Intel® AVX-512)**, which provides 512-bit instructions that can accelerate performance for demanding workloads and usages like artificial-intelligence (AI) inferencing
- **Intel® AES New Instructions (Intel® AES-NI)**, a set of built-in encryption instructions that can greatly improve the compute efficiency of cryptographic algorithms, such as those used in blockchain transactions, while offering greater performance and improved security
- **Intel® Boot Guard**, hardware-based boot-integrity protection that prevents unauthorized software and malware takeover of boot blocks critical to a system's function, thus providing an added level of platform security based on hardware
- **Intel® Virtualization Technology (Intel® VT)**, a growing portfolio of technologies to reduce the virtualization overhead occurring in cache, I/O, and memory while maintaining the isolation of co-located virtualized workloads
- **Intel® Resource Director Technology (Intel® RDT)**, which supplies visibility and control over how shared resources such as last-level cache and memory bandwidth are used by VMs and containers
- **Firmware Descriptor Verification (FD0V)**, a server-node management firmware technology that verifies CPU configuration and protects the platform from fusing attacks, helping to ensure a secure boot process

Deploy Hardened, Boot-to-Runtime Security Quickly and with Confidence

Proven to scale with 2nd Generation Intel Xeon Scalable processors, the tested and verified Intel Select Solutions for Hardened Security with Lockheed Martin are workload-optimized for boot-to-runtime security for VMs and containers and let your organization deploy hardened infrastructure with QoS quickly and efficiently in your data center or at the edge.

Intel® Xeon® Scalable Processors

2nd Generation Intel Xeon Scalable processors:

- Offer high scalability that is cost-efficient and flexible, from the multi-cloud to the intelligent edge
- Establish a seamless performance foundation to help accelerate data's transformative impact
- Support breakthrough Intel® Optane™ DC persistent memory technology
- Accelerate AI performance and help deliver AI readiness across the data center
- Provide hardware-enhanced platform protection and threat monitoring

Intel Select Solutions for Hardened Security with Lockheed Martin feature 2nd Generation Intel Xeon Gold processors.

Learn More

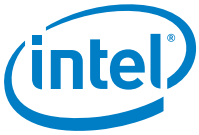
Intel Select Solutions: **intel.com/selectsolutions**

Intel Xeon Scalable processors: **intel.com/xeonscalable**

Intel SSD Data Center Family: **intel.com/content/www/us/en/products/memory-storage/solid-state-drives/data-center-ssds.html**

Intel Ethernet 700 Series: **intel.com/ethernet**

Intel Select Solutions are supported by Intel® Builders: **http://builders.intel.com**. Follow us on Twitter: **#IntelBuilders**



[1] The Intel® Ethernet 700 Series includes extensively tested network adapters, accessories (optics and cables), hardware, and software, in addition to broad operating system support. A full list of the product portfolio's solutions is available at intel.com/ethernet. Hardware and software is thoroughly validated across Intel® Xeon® Scalable processors and the networking ecosystem. The products are optimized for Intel® architecture and a broad operating system ecosystem: Windows*, Linux* kernel, FreeBSD*, Red Hat* Enterprise Linux (RHEL*), SUSE*, Ubuntu*, Oracle Solaris*, and VMware ESXi*. Supported connections and media types for the Intel Ethernet 700 Series are: direct-attach copper and fiber SR/LR (QSFP+, SFP+, SFP28, XLPPI/CR4, 25G-CA/25G-SR/25G-LR), twisted-pair copper (1000BASE-T/10GBASE-T), backplane (XLAUI/XAUI/SFI/KR/KR4/KX/SGMII). Note that Intel is the only vendor offering the QSFP+ media type. The Intel Ethernet 700 Series supported speeds include 10GbE, 25GbE, 40GbE.

[2] Based on Intel testing as of May 24, 2019. Results based on VM configurations with 15 vCPUs on the first of two sockets and 256 GB of RAM per VM. Configuration: 2 x Intel® Xeon® Gold 6248 processor, Intel Xeon Platinum 8260 processor, Intel Xeon Platinum 8268 processor, or Intel Xeon Platinum 8280 processor, 768 GB DDR4-2666 ECC RDIMM, 2 x Intel® SSD DC S4510 (240 GB), 1 x Intel SSD DC P4510 (1 TB, NVM Express* [NVMe*]), 10Gb Intel® Ethernet Network Adapter X710-DA2 SFP+, 10 GbE SFP+ switch, 1 GbE switch, CentOS 7.5*, Security Runtime Environment (SRE) version 3.6, running LINPACK* and HammerDB* benchmark tests.

Performance results are based on testing as of the date set forth in the configurations and may not reflect all publicly available security updates. See configuration disclosure for details. No product or component can be absolutely secure.

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark* and MobileMark*, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products. For more complete information visit intel.com/benchmarks.

Cost reduction scenarios described are intended as examples of how a given Intel- based product, in the specified circumstances and configurations, may affect future costs and provide cost savings. Circumstances will vary. Intel does not guarantee any costs or cost reduction.

Optimization Notice: Intel's compilers may or may not optimize to the same degree for non-Intel microprocessors for optimizations that are not unique to Intel microprocessors. These optimizations include SSE2, SSE3, and SSSE3 instruction sets and other optimizations. Intel does not guarantee the availability, functionality, or effectiveness of any optimization on microprocessors not manufactured by Intel. Microprocessor-dependent optimizations in this product are intended for use with Intel microprocessors. Certain optimizations not specific to Intel microarchitecture are reserved for Intel microprocessors. Please refer to the applicable product User and Reference Guides for more information regarding the specific instruction sets covered by this notice. Notice Revision #20110804

Printed in USA 0619/LU/PRW/PDF Please Recycle 338875-001US