Lanner

White Paper

Hardware-based Security with Lanner Network Appliances

Powered by Intel® Xeon® D-1700 & D-2700 (Ice Lake-D) Processors

Date of Release: 2022-06-14

Overview

As the edge computing market continues to grow and evolve, there is an even greater need for high-performance processors with IoT-centric features, however, the proliferation of Web-enabled wireless devices also makes managing security across myriad platforms more complicated. External threats are growing in complexity and precision, including firmware attacks, ransomware, identity theft, cyber espionage, and DDOS attacks, to name a few. Hardware-based security would be able to solve some of these legacy security issues by providing a foundational layer of protection that can help detect and prevent cyber threats at the software layer. Delivering performance and security while meeting power and space constraints is key to taking full advantage of network edge usage models for benefits such as low latency and reduced costs for backhaul bandwidth.

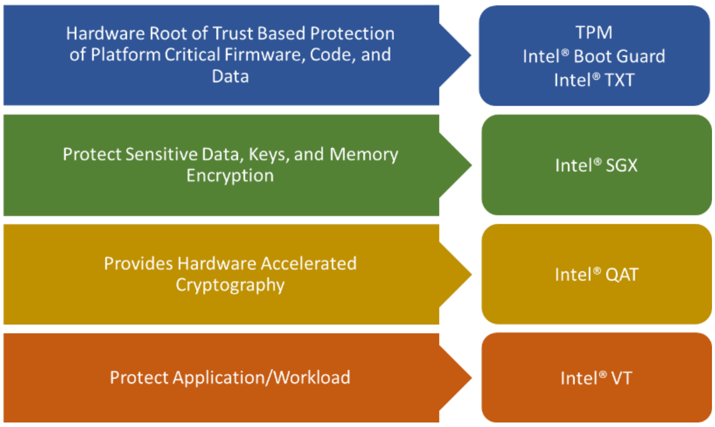
Lanner Network Appliance Powered by Intel® D-1700 & D-2700 Family

Lanner's NCA-4030 and NCA-4035 network appliance series are powered by Intel's Xeon® D-1700 and D-2700, a branch of Xeon processors optimized for delivering ultra-low power consumption and robust performance. The 1U rackmount network security appliance comes with the most innovative System-on-a-Chip built for the edge and is ideal for applications in networking, 5G, uCPE SD-WAN, and IoT/IIoT Edge computing, delivering improvement in packet processing performance, and network scalability in virtualized network functions.

Security Benefits of the Intel® D-1700 & D-2700 Family

The ongoing drive to process workloads closer to the point of data origin creates requirements for computing at the edge. The next-gen Intel® Xeon® D-1700/D-2700 processors deliver hardware-enhanced security features that help protect all layers in the computing stack, reducing physical and cyberattack surfaces and help prevent memory snooping in edge deployments.

Intel® Xeon® D-1700/D-2700 processors were designed for proactive protection of devices with hardware-based security for enhanced productivity.



Hardware Root of Trust Based Protection of Platform Critical Firmware, Code, and Data	TPM Intel® Boot Guard Intel® TXT
Protect Sensitive Data, Keys, and Memory Encryption	Intel® SGX
Provides Hardware Accelerated Cryptography	Intel® QAT
Protect Application/Workload	Intel® VT

Trusted Platform Module (TPM)

TPM (Trusted Platform Module) can securely store passwords, certificates, or encryption keys used to authenticate the platform. The nature of hardware-based cryptography ensures that the information stored in hardware is better protected from external software attacks. A TPM will store platform measurements that help ensure that the platform remains trustworthy through authentication and attestation, both are necessary steps to ensure safer and protected computing in all environments and layers of the network. TPM applications can make it much harder to access information on computing devices without proper authorization. If the configuration of the platform has changed as a result of unauthorized activities, access to data and secrets can be denied and sealed off. TPM is one of the fundamental hardware-based layers to offer a greater level of protection.

Intel® Boot Guard

Intel® Boot Guard attempts to protect the system before Secure Boot starts, by authenticating the initial BIOS code and extending the hardware root of trust. Intel Boot Guard provides hardware-based boot integrity to mitigate unauthorized BIOS boot block modifications.

Intel Boot Guard does not prevent access, instead, it requires verification of the code before the CPU runs the Initial Boot Block (IBB). The related keys and policies reside in fuses, further fortifying the Root of Trust, and thus stopping attacks on the root. When booting with Intel Boot Guard enabled, the boot integrity is unalterable since it is anchored in hardware fuses. Intel Boot Guard adds robustness to the chain of trust process where the UEFI boot process cryptographically verifies and/or measures each software module before executing it. The purpose of Intel Boot Guard process is to reduce the chance of malware exploiting the hardware or software components on the platform.

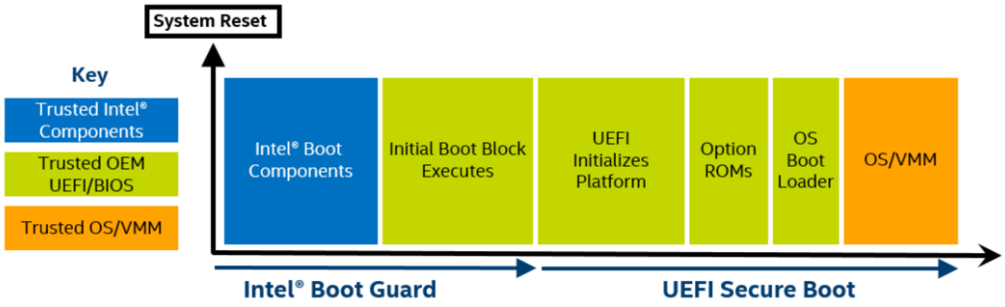


Figure 1. Secure Boot Flow

Source: Intel Cooperation, Application Note: Secure the Network Infrastructure – Secure Boot Methodologies

Intel Boot Guard establishes a strong, hardware-based Static Root of Trust for Verification and measurement. Both roots are established before control is passed to the reset vector (before executing a single BIOS instruction). This is accomplished in Intel Boot Guard by cryptographically verifying/measuring the first portion of BIOS code executed out of reset. The policies of Intel Boot Guard are rooted in Field Programmable Fuses, making them unalterable for the lifetime of a platform. Once provisioned, Intel Boot

Guard cannot be disabled, and the policies cannot be spoofed. Intel Boot Guard excludes the Serial Peripheral Interface (SPI) bus from the Trusted Computing Base, helping to detect corruption of the BIOS image in a Flash update or during transfer.

Intel® Trusted Execution Technology (Intel® TXT)

Intel® Trusted Execution Technology (Intel® TXT) is a set of hardware extensions to Intel® processors and chips that enhance the platform with security capabilities such as measured launch and protected execution. Intel® TXT provides hardware-based mechanisms that help protect against software-based attacks and protect the confidentiality and integrity of data created and stored.

Intel® TXT provides these mechanisms by enabling an environment where applications can run within their own space, protected from all other software on the system. Intel TXT initiates a measured and controlled launch of system software called the Measured Launch Environment (MLE), established generally at OS boot time. This MLE is a protected environment for itself and anything that may run within this space.

Intel TXT measures key components executed during the launch of MLE and allows the OS to check the consistency in behaviors and launch time configurations against a “known good” sequence. Using this verified benchmark, the system can quickly assess whether any attempts have been made to alter or tamper with the launch time environment.

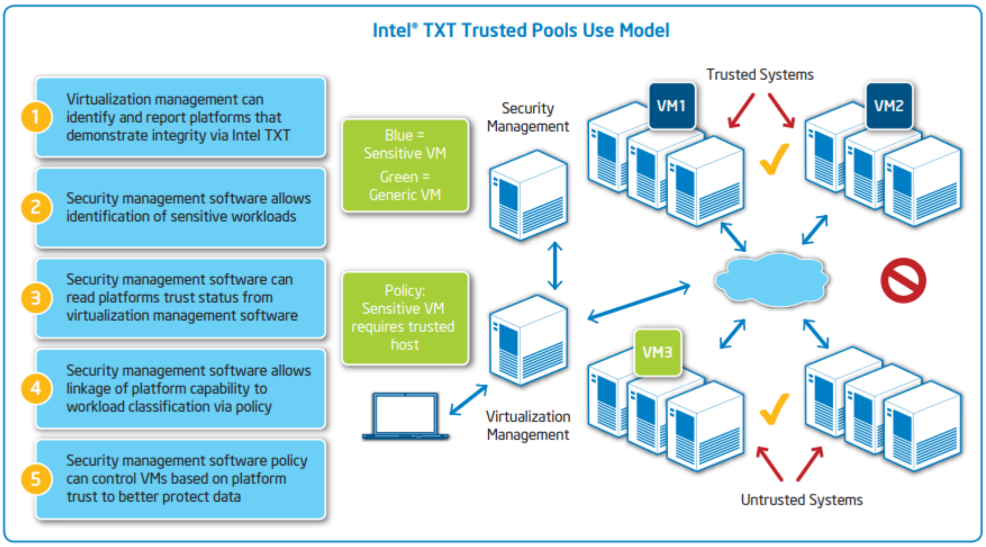

Intel® TXT Trusted Pools Use Model
1 Virtualization management can identify and report platforms that demonstrate integrity via Intel TXT
2 Security management software allows identification of sensitive workloads
3 Security management software can read platforms trust status from virtualization management software
4 Security management software allows linkage of platform capability to workload classification via policy
5 Security management software policy can control VMs based on platform trust to better protect data
Blue = Sensitive VM
Green = Generic VM
Policy: Sensitive VM requires trusted host
Security Management
Virtualization Management
Trusted Systems
VM1
VM2
VM3
Untrusted Systems

Figure 2. Intel TXT Trusted Pools Use Model

Source: Intel Cooperation, Whitepaper: Intel® Trusted Execution Technology

The measurement of this environment is the dynamic root of trust for measurement. It is a simpler measurement because firmware responsible for booting up the platform is excluded from the environment. The smaller the trusted computing base is, the stronger its trust will be. Software residing in a small trusted computing base can be more easily examined and tested.

Intel TXT provides the protection mechanisms, rooted in hardware, that are necessary to provide trust in the application’s execution environment. These mechanisms can protect vital data and processes from being compromised by malicious software running on the platform.

Intel® Software Guard Extensions (Intel® SGX)

Intel® Software Guard Extensions offers hardware-based memory encryption, a confidential computing solution that isolates specific application code and data within memory to protect data and applications while in-use. Intel® SGX helps protect data in use by allowing user-level code to allocate private regions of memory, called enclaves, which are designed to be protected from processes running at higher privilege levels. By protecting selected code and data from modification, developers can partition their application into hardened enclaves or trusted execution modules to help increase application security. When other system layers are compromised, the application data stored within the enclave itself is still protected and inaccessible to external, non-verified parties, and thus safe from being destroyed, manipulated, or edited by unauthorized users. SGX adds another layer of defense by reducing the attack surface of the system and helps protect against many known and active cybersecurity threats.

Intel® QuickAssist Technology (Intel® QAT)

Intel® QuickAssist Technology (Intel® QAT) offers a software-enabled foundation for symmetric and asymmetric encryption, authentication and compression/decompression, digital signatures, RSA, DH, ECC, and lossless data compression. Intel® QAT Gen 3 provides hardware acceleration to assist with the performance demands of securing and routing internet traffic and other workloads, such as compression and wireless 3G and 4G LTE algorithm offload, thereby reserving processor cycles for application and control processing; which in turn save cycles, time, and space of applications.

Intel® QAT significantly increases the performance and efficiency across applications and platforms. It supports encrypting/decrypting for applications such as Transport Layer Security (TLS) or IP Security (IPsec), supporting common ciphers and modes and authentication, as well as public-key cryptography and pseudorandom functions.

Intel® Virtualization Technology (Intel® VT)

Intel® virtualization technology is the processor’s hardware ability to divide and isolate its computing capacity for multiple host virtual machines and their operating systems, allowing multiple workloads to share a common set of resources. Virtual functions can be deployed on standard high-volume servers anywhere in the data center, network nodes, or cloud, and smartly co-located with business workloads. On shared virtualized hardware, a variety of workloads can co-locate while maintaining full isolation from each other, freely migrate across infrastructures, and scale as needed.

Virtualization of security and network functions enables developers, service providers, and businesses to gain significant capital and operational efficiencies because it leads to improved server utilization and consolidation, dynamic resource allocation and management, workload isolation, security, and automation. Virtualization makes possible on-demand self-provisioning of services and software-defined resource orchestration, scaling anywhere in a hybrid cloud on-premise or off-premise depending on specific business needs.

Memory virtualization features enable abstraction isolation and monitoring of memory on a per virtual machine (VM) basis. Example features include direct memory access (DMA) remapping and extended page tables (EPT), including their extensions: accessed and dirty bits, and fast switching of EPT contexts. These features also make live migration of VMs possible, add to fault tolerance, and enhance security.

Summary

It takes a combination of software and hardware-based security features to keep an edge cloud infrastructure secure. By starting with a root of trust, security features can be strengthened at each layer to make the entire system or stack more secure. Intel® Boot Guard enables a hardware-based static root of trust for measurement and verification of boot integrity before the OS boots up. Intel® SGX isolates applications within trusted enclaves during runtime to help protect data. Intel® QAT offloads CPU to dedicated hardware acceleration for cryptography and data compression, enhancing security and compression performance in the cloud, networking, big data, and storage applications. Intel® TXT attests to the platform environment against the desired launch configurations defined. Intel® Virtualization Technology provides hardware assistance to the virtualization software by eliminating performance overheads and improving security.

Lanner has conducted benchmark tests for Intel® Xeon® Processor D-1700/D-2700 in Lanner's NCA-4030 and NCA-4035 platforms. NCA-4030 and NCA-4035 leverage the Intel® Xeon® D-1700/D-2700 Processor to deliver ultra-low power consumption and robust performance. This appliance is ideal for applications in networking, 5G, and IoT/IIoT Edge computing, delivering improvement in packet processing performance, and virtualized Customer Premise Equipment (vCPE) usages.

Disclaimer by Lanner

All product specifications are subject to change without notice. Lanner Electronics Inc. is not liable nor responsible for any damage of products caused by improper uses.

Copyright Disclaimer by Intel®

INFORMATION IN THIS DOCUMENT IS PROVIDED IN CONNECTION WITH INTEL PRODUCTS. NO LICENSE, EXPRESS OR IMPLIED, BY ESTOPPEL OR OTHERWISE, TO ANY INTELLECTUAL PROPERTY RIGHTS IS GRANTED BY THIS DOCUMENT. EXCEPT AS PROVIDED IN INTEL'S TERMS AND CONDITIONS OF SALE FOR SUCH PRODUCTS, INTEL ASSUMES NO LIABILITY WHATSOEVER AND INTEL DISCLAIMS ANY EXPRESS OR IMPLIED WARRANTY, RELATING TO SALE AND/OR USE OF INTEL PRODUCTS INCLUDING LIABILITY OR WARRANTIES RELATING TO FITNESS FOR A PARTICULAR PURPOSE, MERCHANTABILITY, OR INFRINGEMENT OF ANY PATENT, COPYRIGHT OR OTHER INTELLECTUAL PROPERTY RIGHT.

A "Mission Critical Application" is any application in which failure of the Intel Product could result, directly or indirectly, in personal injury or death. SHOULD YOU PURCHASE OR USE INTEL'S PRODUCTS FOR ANY SUCH MISSION CRITICAL APPLICATION, YOU SHALL INDEMNIFY AND HOLD INTEL AND ITS SUBSIDIARIES, SUBCONTRACTORS AND AFFILIATES, AND THE DIRECTORS, OFFICERS, AND EMPLOYEES OF EACH, HARMLESS AGAINST ALL CLAIMS COSTS, DAMAGES, AND EXPENSES AND REASONABLE ATTORNEYS' FEES ARISING OUT OF, DIRECTLY OR INDIRECTLY, ANY CLAIM OF PRODUCT LIABILITY, PERSONAL INJURY, OR DEATH ARISING IN ANY WAY OUT OF SUCH MISSION CRITICAL APPLICATION, WHETHER OR NOT INTEL OR ITS SUBCONTRACTOR WAS NEGLIGENT IN THE DESIGN, MANUFACTURE, OR WARNING OF THE INTEL PRODUCT OR ANY OF ITS PARTS.

Intel may make changes to specifications and product descriptions at any time, without notice. Designers must not rely on the absence or characteristics of any features or instructions marked “reserved” or “undefined.” Intel reserves these for future definition and shall have no responsibility whatsoever for conflicts or incompatibilities arising from future changes to them. The information here is subject to change without notice. Do not finalize a design with this information.

The products described in this document may contain design defects or errors known as errata which may cause the product to deviate from published specifications. Current characterized errata are available on request.

Contact your local Intel sales office or your distributor to obtain the latest specifications and before placing your product order.

Copies of documents which have an order number and are referenced in this document, or other Intel literature, may be obtained by calling 1-800-548-4725, or go to: http://www.intel.com/design/literature.html.

Intel and Xeon are trademarks of Intel Corporation in the U.S. and/or other countries.

*Other names and brands may be claimed as the property of others.