Solution Brief
Intel® Trusted Execution Technology (Intel® TXT)

Foundational Security with Intel® TXT and Citrix XenServer®

How Intel and Citrix work together to protect sensitive data

In today's data-driven climate, your data is your business. Nearly every aspect of the enterprise—from the mailroom to the research and development lab—relies on some sort of access to corporate data. In addition to instant access to critical data, enterprises need the ability to adjust to changing market or regulatory conditions quickly while keeping IT costs down. To meet these competing demands, enterprises are adopting cloud strategies to maximize their agility while reducing infrastructure costs. But accelerated cloud-strategy adoption, combined with increasing regulatory constraints, can test the limits of even the most well-designed security strategies.

Intel and Citrix can help enterprises build secure cloud foundations that provide the agility, security, and costs savings they require. The combination of Intel® Trusted Execution Technology (Intel® TXT) and Citrix XenServer® can help ensure that your compute pools remain trusted with hardware-based security.[1]

New Technologies Equal New Security Challenges

As enterprises continue to adopt cloud technologies, security managers struggle to maintain server security policies and compliance, audit, and reporting enforcement in an increasingly abstracted computing environment. Data is no longer confined to discrete physical servers in bunker-like data centers. With cloud technologies, virtual machines (VMs) containing sensitive data can reside on any number of physical hosts in any number of physical locations.

In addition, cloud environments can complicate audit- and compliance-policy enforcement. In traditional physical-server deployments, the hardware, applications, and data can reside in the same physical space within the data center. With cloud deployments, an application might run on a physical server located in one data center, while that application's data might reside in a separate data center thousands of miles away.

This abstraction creates new opportunities for attackers to gain control of the underlying hardware platform. Once the platform is compromised, an attacker might be able to compromise any virtual machines running on the platform. An IT organization might have hardened operating systems and networks protecting its data, but an unsecured hardware platform can jeopardize even the best security implementation.

At a Glance: Intel® TXT and Citrix XenServer®

Intel and Citrix can help enterprises of any size secure their cloud platforms while virtualizing their most demanding workloads. With Intel TXT and Citrix XenServer, enterprises can realize the benefits of an agile infrastructure-as-a-service (IaaS) model with a root of trust built into the hardware.

With servers powered by Intel® Xeon® processors and Citrix XenServer, enterprises can better protect their cloud platforms from attacks that target a server host's BIOS, firmware, and hypervisor. Tools such as OpenStack* let cloud administrators create auditable security policies to help protect virtual machines and prevent them from starting and running on compromised hosts.

As enterprises in highly regulated industries such as government, healthcare, and finance embrace cloud technology, having a root of trust built into the hardware is crucial to conform to regulations and service-level agreements (SLAs) that require tighter data security, attestation of host integrity, and virtual machine location constraints.

Intel TXT and Citrix XenServer: The Building Blocks of a Secure Cloud

To meet these evolving challenges, Intel and Citrix have collaborated on secure cloud solutions that take advantage of hardware-assisted security to provide a foundation of trust. Large, complex cloud deployments provide more avenues for attackers to gain control of platforms. The combination of Intel TXT and Citrix XenServer helps protect the underlying platform from threats of BIOS, hypervisor, or other firmware attacks, in addition to software-based attacks such as root-kit installations.

To protect against sophisticated attacks, security must start at the cloud infrastructure's hardware level and extend to the software stack. Intel TXT, a hardware-based technology found on platforms powered by the Intel® Xeon® processor E5 v3 family and the Intel Xeon processor E7 v3 family, provides a hardware root of trust through:

- **Verified launch,** a hardware-based chain of trust that enables a host powered by an Intel Xeon processor to compare its startup environment to a known-good state. Any variation from the host's known-good state can be cryptographically detected and acted upon.
- **Sealed storage,** which protects a host's known-good state cryptographic values.
- **Protected execution and memory space,** where sensitive cryptographic values can be processed.
- **Attestation,** which confirms that the host configuration is either trusted or untrusted and provides this information for compliance and audit purposes.

Intel TXT creates a measured launch environment (MLE) that cryptographically compares critical aspects of the hardware and software environment at startup to determine if any tampering has taken place. When a cloud administrator initially configures a host running Citrix XenServer, Intel TXT is used to create unique cryptographic identifiers for critical elements of the launch environment, including Citrix XenServer and the host's BIOS and firmware. Once Intel TXT creates each identifier, it securely stores the identifiers in the host's Trusted Platform Module (TPM),[2] a tamper-resistant cryptographic processor and protected-memory space built into the host's hardware. Together, these cryptographic signatures identify the host's known-good state.

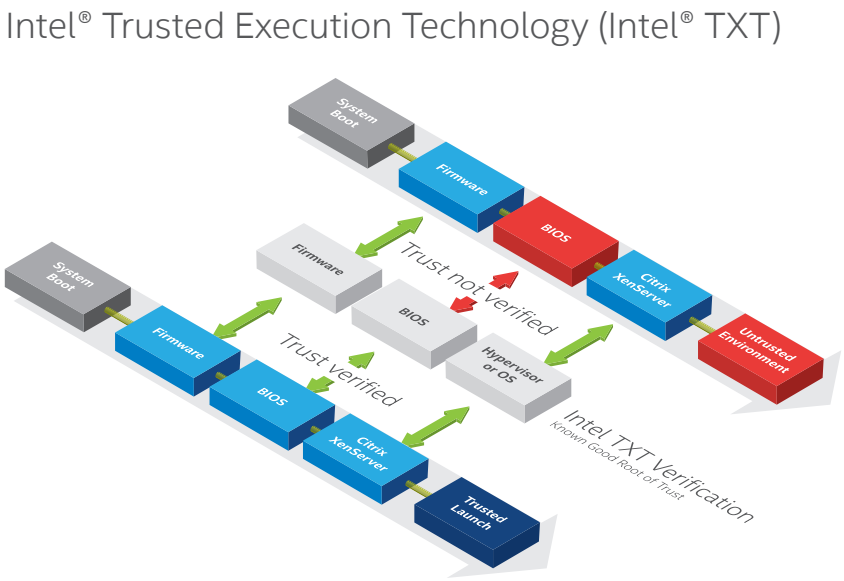

Figure 1. Intel® Trusted Execution Technology (Intel® TXT) and Citrix XenServer® work together to help ensure a chain of trust

Once a host's known-good state is stored in the TPM, Intel TXT measures each launch environment element at startup and compares the measured values with the known good–state values. If the values align, the host boots into a trusted state. If the values do not align, the host boots into an untrusted state. Intel TXT can flag unexpected attestation results, which can then be queried by remote attestation software to determine if additional scrutiny or security measures need to take place.

Building Upon a Secure Foundation

With Intel TXT and Citrix XenServer as the foundation, enterprises can create trusted compute pools—groups of hosts with verified security integrity—that can have sophisticated security, auditing, and reporting policies applied using third-party orchestration and reporting tools.

One of the benefits of a cloud infrastructure is the ability to seamlessly migrate virtual machines among pools of hosts using technologies such as the Citrix XenMotion® feature of Citrix XenServer. But if a virtual machine moves to a compromised host, an attacker could potentially compromise the virtual machine itself along with its data. Intel TXT and Citrix XenServer,[3] combined with tools such as OpenStack*, let cloud administrators create security policies to prevent virtual machines from being started on or migrated to untrusted hosts, maintaining the integrity of the virtual machine and its data.

While virtual machines can migrate anywhere within a trusted pool of hosts, cloud administrators might want to constrain virtual machine movement for various reasons. For example, financial or healthcare institutions might be bound by government regulations to keep sensitive data within specific geographic boundaries.

Enterprises can use asset tagging to define logical boundaries within or among trusted compute pools. With asset tagging, cloud administrators can assign unique values—such as geographic location—to each host within the trusted pool. Security administrators can then create security policies to constrain which hosts within the pool can run sensitive workloads. When a virtual machine is ready to migrate to another host, cloud-management software can use security policies and asset-tag information to restrict the virtual machine to a defined subset of the trusted-pool hosts.

Asset tagging can also enable intelligent workload distribution. Many enterprises require different levels of performance from their cloud infrastructures. Some compute pools might incorporate hosts designed around the Intel Xeon processor E5 v3 family for workloads such as email processing, while other pools might contain hosts built on the Intel Xeon processor E7 v3 family for more demanding workloads. Administrators can create policies and templates to restrict virtual machines to specific hosts based on the types of workloads running within the virtual machine.

At a Glance: Citrix XenServer®

Citrix XenServer is a bare-metal virtualization platform built on the open-source Citrix Xen® hypervisor. Used by many of the world's largest public-cloud service providers, Citrix XenServer can help you handle the most demanding workloads, and it is designed to scale with your business needs.

The Citrix XenServer hypervisor takes advantage of Intel® Virtualization Technology (Intel® VT), which further enhances the hypervisor's performance on servers powered by Intel® Xeon® processors. Combined with capabilities[1] such as high availability, VM protection and recovery, live VM migration, and dynamic memory allocation, Citrix XenServer delivers the performance and features that make it a clear choice for any size of enterprise.

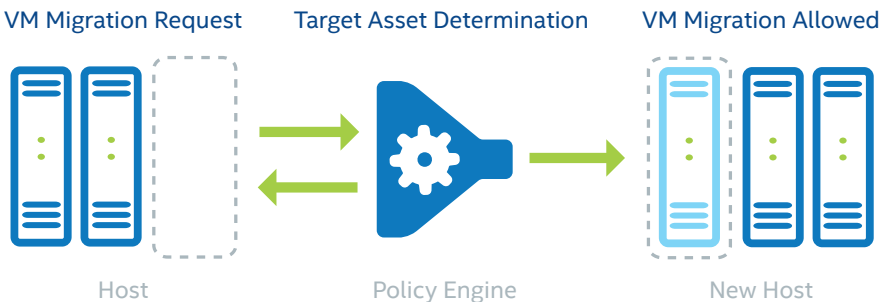

Figure 2. Asset tagging helps restrict virtual-machine movement to specific hosts

Compliance Peace of Mind through Auditing

Verifying the security of your hardware and where your data and workloads reside is as important as the security policies that constrain virtual-machine movement. In addition, government regulations in industries such as healthcare and finance require regular auditing of systems and data to help ensure data is kept safe from threats both within and outside the enterprise.

Intel TXT and Citrix XenServer provide the infrastructure for attestation of host integrity and auditing of virtual-machine health and location. With tools such as OpenStack, auditors and cloud administrators can quickly determine if hosts have been compromised and can take action automatically to isolate potentially compromised workloads.

Intel and Citrix: Enabling Secure Cloud Solutions for a Changing World

Cloud solutions from Intel and Citrix can provide enterprises with a more-secure foundation to help protect critical and sensitive workloads. With third-party support from solutions like OpenStack, enterprises can be confident that their cloud solutions will give them the capabilities they need to compete in increasingly competitive and regulated business environments.

Find Out More

Intel TXT:
www.intel.com/txt

Citrix XenServer:
http://www.citrix.com/products/xenserver/

OpenStack:
http://www.openstack.org/

CITRIX®

[1] Intel technologies' features and benefits depend on system configuration and may require enabled hardware, software or service activation. Performance varies depending on system configuration. No computer system can be absolutely secure. Check with your system manufacturer or retailer or learn more at www.intel.com.

[2] The Intel Trusted Platform Module (TPM) is based on standards created by Trusted Computing Group, an industry collaboration effort to implement security standards across multiple platforms.

[3] Intel® TXT support for Citrix XenServer® requires the Measured Boot Supplemental Pack.