Cloud Security Solutions You Can Trust

Intel and VMware security solutions for business computing in the cloud

Embrace Cloud Computing with Intel and VMware Security Solutions

Cloud computing offers your business many benefits: increased flexibility, agility, efficiency, and cost savings. To move your data center to the cloud, however, you need security solutions that you can trust. You can deploy a cloud infrastructure confidently by safeguarding your sensitive data and strengthening regulatory compliance with cloud security solutions from Intel and VMware. With Intel® Trusted Execution Technology (Intel® TXT) and VMware® vSphere™ working together, you can create trusted platforms with security rooted in the hardware.

Meet the Cloud Security Challenge with Trusted Compute Pools

Cloud computing can expose sensitive data to new types of attacks where the platform, rather than just the software, becomes increasingly virtual, abstracted, and distant from IT administrators. Attackers see this as an opportunity and use stealth techniques to seek and gain control of the platform. Other cloud security challenges include protecting the virtual machines from potential tampering, isolating co-tenant virtual machines from one another, and protecting data from unauthorized viewers, which might include cloud administrators (more likely to be a third party). All of this affects compliance, audit, reporting, and policy enforcement, which all become more complex in a cloud environment.
Traditional tools and security models are not adequate to handle this virtual and complex security landscape and cannot be relied on to protect against the increasingly sophisticated software-based attacks that threaten integrity, confidentiality, reliability, and availability of systems. To embrace cloud computing, you need to address the increasing and evolving security threats across physical and virtual infrastructures. You can create trusted compute pools by using Intel TXT and VMware vSphere to implement trusted pools of server platforms and to create trust-aware security policies. These trusted compute pools are comprised of systems that protect virtualization environments at the hardware level, which allows increased security throughout the data center, enhances workload controls, and makes auditing and regulatory compliance easier.

Cloud Solutions from Intel and VMware
With Intel and VMware cloud solutions, you can transform your organization and align IT with your organization’s business needs by delivering infrastructure as a service (IaaS) solutions that help you virtualize any workload and simplify network provisioning and management.

You can build secure, flexible, and agile cloud infrastructures while lowering total-cost-of-ownership by combining VMware enterprise virtualization and management software with servers powered by the Intel® Xeon® processor E5 and Intel® Xeon® processor E7 families that include technologies such as Intel® Virtualization Technology (Intel® VT)® and Intel® Trusted Execution Technology (Intel® TXT). DynamicOps, a VMware company, provides additional capabilities for management and provisioning of IT resources in the cloud, including unified management and control over security capabilities.

Providing a Foundation for Cloud Security with Intel® TXT
The key to creating trusted compute pools is establishing a root of trust—the foundation on which trusted platforms can be built to protect against software-based attacks. The root of trust is a trusted, tamper-resistant configuration that each server can have; it can be used to evaluate the integrity of other system components. Many Intel® Xeon® processor E5 family and Intel Xeon processor E7 family platforms include Intel TXT, a hardware-based technology that provides a root of trust by creating a measured launch environment (MLE). The MLE is comprised of an accurate comparison of all the critical elements of the launch environment, which can be securely stored on the platform, attested, and used for comparison against a known good source. Intel TXT creates a cryptographically unique identifier for each approved launch-enabled component and uses hardware-based mechanisms to identify the launch of code that does not match approved code. Figure 1 illustrates how Intel TXT enables verification of a platform’s integrity before it is launched.

**Figure 1. How Intel® Trusted Execution Technology (Intel® TXT) works to enable host integrity verification**

**Establishing Trusted Compute Pools with Intel® TXT and VMware® vSphere™**

With virtual machine migration there is a real concern of moving a compromised virtual machine from one physical host to another, potentially compromising the receiving host and possibly impacting the virtual machines and workloads on the receiving platform. As a potential mitigation to this risk, companies are realizing that their critical data should be allocated to trusted compute pools only. To determine the trust status of a server, Intel TXT can work with VMware vSphere to measure hypervisor, firmware, BIOS, and other key software at boot time using the tamper-resistant root of trust and store the launch measurement results in the trusted platform module (TPM). These results can be securely queried (“attested”) and compared to the expected “known good” values to verify launch integrity and to flag unexpected results as possible security concerns. (To find server products with support for Intel TXT, see [Intel® Trusted Execution Technology Server Platforms Matrix](#).) This all allows Intel TXT and VMware vSphere to work together to establish trusted compute pools, which are groups of trusted hosts. Each host in a trusted compute pool has its integrity verified at launch time by Intel TXT. VMware® vCenter™ can work with third-party software such as the HyTrust Appliance® to apply policies that control the migration of virtual machines to and from...
trusted compute pools. For example, the HyTrust Appliance can read a platform's trust status from VMware vCenter and allow virtual machine migration to trusted compute pools from other trusted compute pools or trusted hosts only. The policy can prevent virtual machine migration from untrusted or unverified platforms to trusted compute pools and vice versa. With this policy, a virtual machine can be freely migrated within a trusted compute pool, maintaining the desired security profile for the workload while allowing for a dynamic virtual environment. Figure 2 shows a configuration of Intel TXT, VMware vCenter, and HyTrust Appliance in which they work together to establish and maintain trusted compute pools in a cloud environment.

This trusted compute pool model enables the following features:

- Virtualization management provided by VMware vCenter can identify and report platforms that demonstrate integrity via Intel TXT.
- Third-party security management software such as HyTrust Appliance can do the following:
  - Allow identification of sensitive workloads
  - Read platforms’ trust status from virtualization management software
  - Allow linkage of platform capability to workload classification through policy
  - Control virtual machines based on platform trust to better protect data

**Proving the Cloud Can Be Trusted**

To adopt a cloud solution, you need to be able to prove to your organization that the cloud can be trusted, especially when the cloud infrastructure is owned and managed by a third party. IT managers need to be able to verify for themselves that the cloud infrastructure is secure and auditable. They need assurance of compliance with security policies and standards.

Intel TXT can provide platform measurement credentials to support compliance and audit activities. VMware vSphere can provide trust status through virtualization management consoles and can deliver that information to Security Information and Event Management (SIEM) and governance, risk management, and compliance (GRC) systems for more automated logging, reporting, and auditing.

The trusted foundation, however, is only part of the story. Of course, protections and controls are essential to have a more secure virtual infrastructure as an extension of a traditional IT infrastructure. To complement the trusted compute pool capabilities, VMware...
vSphere offers the following virtualization-layer features to support compliance and audit activities:

- VMware® ESX™ and VMware® ESXi hypervisors allow enterprises to use their own security certificates when securing remote sessions. The user name, password, and network packets sent to a VMware ESX server over a network connection when using the VMware Remote Console or the VMware Management Interface are encrypted in the VMware ESX server by default when medium- or high-security settings are activated for the server.

- VMware vCenter Server gives IT administrators unprecedented visibility and centralized control of every level of the VMware vSphere virtual infrastructure. It provides granular privilege management that limits who can deploy virtual machines to specific clouds and storage devices. Combined with well-defined operational processes and workflows, these capabilities can provide maximum mobility for virtual machines while managing risk.

- VMware vCenter Lifecycle Manager enables IT administrators to track ownership of virtual machines and to keep records of when virtual machines are created, deployed, and decommissioned.

VMware vSphere 5.0 is Common-Criteria certified at EAL4+, providing an objective measure of security that’s well understood by security professionals and compliance auditors.

VMware® vCloud™ Networking and Security allows for convenient, centralized management by providing highly granular views of the entire virtual machine and virtual network deployment, easing configuration of zone-based policies and reducing the risk of errors.

Move to the Cloud with Confidence

Trusted compute pools with Intel and VMware technologies can strengthen security and compliance from the core to the edges of your data center. They can give you the confidence you need to embrace cloud computing and let your business become more competitive with the increased flexibility, agility, efficiency, and cost savings that come with this critical transformation.

HyTrust Appliance*: Protecting the Keys to the Kingdom

HyTrust Appliance* is a virtual appliance that is compatible with VMware® vSphere™ and deployed right alongside the rest of your virtual infrastructure. The HyTrust Appliance can be deployed on the same hypervisor that it is actively protecting.

Where Does It Live?

HyTrust Appliance sits in the management plane of the virtual infrastructure, between the administrators of the virtual infrastructure and the virtual infrastructure itself.

What Does It Do?

HyTrust Appliance intercepts all administrative requests for the virtual infrastructure, determines whether or not the request complies with policy, and then permits or denies the request as appropriate.

What Policies Are Enforced?

The options are practically unlimited. HyTrust Appliance can ensure that certain workloads are only permitted to boot up on specific hosts or specific clusters. Working with Intel® Trusted Execution Technology (Intel® TXT), HyTrust Appliance can verify the integrity of the physical hardware of the host to ensure that the underlying platform is fully trusted. Through its unique ability to label virtual objects and then apply policies to those labels, HyTrust Appliance adds flexibility and control to your cloud security solution.

Additional Resources

www.hytrust.com/products/overview
www.vmware.com/go/vsphere
www.intel.com/txt

---

1 No computer system can provide absolute security under all conditions. Intel® Trusted Execution Technology (Intel® TXT) requires a computer with Intel® Virtualization Technology, an Intel TXT-enabled processor, chipset, BIOS, Authenticated Code Modules and an Intel TXT-enabled measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.2. For more information, visit www.intel.com/go/inteltxt.

2 Intel® Virtualization Technology requires a computer system with an enabled Intel® processor, BIOS, and virtual machine monitor (VMM). Functionality, performance, or other benefits will vary depending on hardware and software configurations. Software applications may not be compatible with all operating systems. Consult your PC manufacturer. For more information, visit http://www.intel.com/content/www/us/en/virtualization/technology/white-paper-virtualization-technology.html.

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. UNLESS OTHERWISE AGREED IN WRITING BY INTEL, THE INTEL PRODUCTS ARE NOT DESIGNED NOR INTENDED FOR ANY APPLICATION IN WHICH THE FAILURE OF THE INTEL PRODUCT COULD CREATE A SITUATION WHERE PERSONAL INJURY OR DEATH MAY OCCUR.

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 by visiting Intel’s Web site at www.intel.com.

Copyright © 2013 Intel Corporation. All rights reserved. Intel, the Intel logo, and Xeon are trademarks of Intel Corporation in the U.S. and other countries.

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

Printed in USA 0413SB/PRW/PDF Please Recycle 328730-001US