SOLUTION BRIEF

Data Center
Cloud and Software-Defined Infrastructre

Path to a Secure Compliant Cloud

Gain a trusted infrastructure with a solution from HyTrust, VMware, and Intel

Technology innovation can change not only how enterprises are run, but the way people work – and business is relying on IT as a collaborative partner in the transformation process.

Martin Guttmann
Principal Solution Architect;
World Wide Datacenter Solutions
Intel Corporation

Tamer Elsharnouby
Solution Architect;
World Wide Datacenter Solutions
Intel Corporation

Executive summary

Enterprises face more competition now than ever before. Innovative business models are disrupting the market, forcing even the largest organizations to radically transform the way they do business. Corporations need to innovate to stay ahead of the competition, deliver new services to attract and retain new customers, and keep their costs as low as possible.

At the heart of these projects lies a company's cloud. A well-designed cloud offers business decision-makers incredible levels of agility, which creates the opportunity for constant innovation through the rapid, iterative development of new services and business models. At the same time, IT gains increased operational efficiency while still meeting performance, cost, and elasticity requirements.

However, businesses must consider information security, regulatory compliance, server geolocations, geo-fencing, and trust as they build their virtualized cloud infrastructures. While these technologies can speed operations and reduce costs, they also introduce unique risks for security and compliance that companies need to address (see Figure 1). They directly impact data privacy and governance, because virtual workloads and their data may move among departments and geographies.

Security breaches of sensitive information can lead to disastrous business or legal consequences. When a breach occurs, it's up to IT to close it. To avoid those issues, companies should strive for a solution that can ensure that all their systems and hypervisors are trusted.

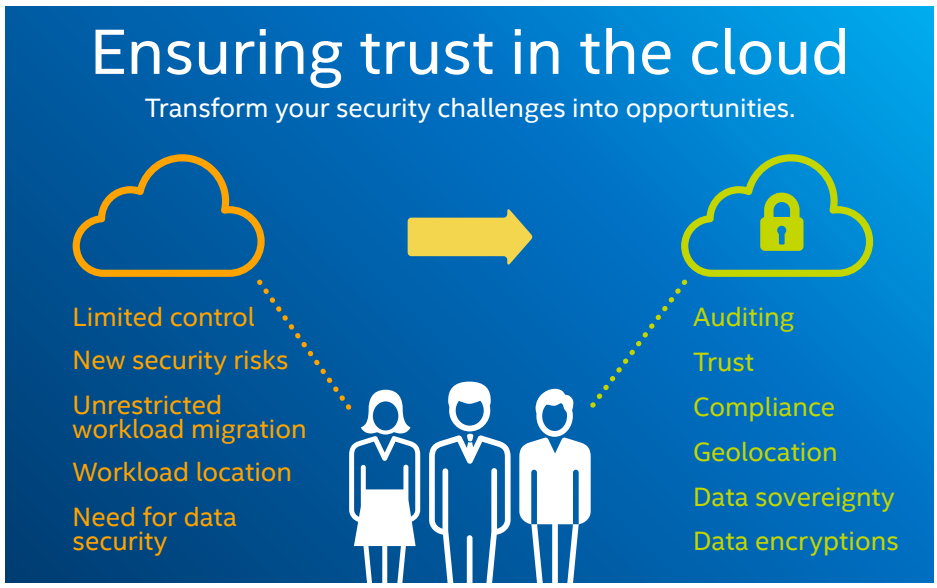

Figure 1. Moving cloud infrastructures towards increased compliance and trust. This solution can help enterprises address their security and compliance challenges.

Delivering on all these promises requires the cloud itself to be built upon the right architectural model. Industry consensus is moving towards the idea that a shift to a Software-Defined Infrastructure (SDI) fulfills this requirement. SDI is a vision for an environment entirely controlled by fast, adaptive software.

HyTrust, VMware, and Intel have teamed to offer a cloud solution that enables IT and business leaders to build a trusted, securely governed, virtualized infrastructure upon a capability known as a hardware root-of-trust. The root-of-trust, which is enabled by Intel® Xeon® processors, provides a foundation on which the system's other security elements can rely. With this solution, enterprises can increase the trust, security, and compliance of their IT infrastructure, while taking full advantage of the benefits of virtualization and the cloud.

The importance of trust in a virtualized infrastructure

For an infrastructure to be trusted, its hosts, data stores, hypervisor, and governance must also be trusted. That means hosts must be in known locations with expected configurations. Virtual data stores should be encrypted, and decryption should only be possible when both the workload and the host are also trusted.

By providing platform and hypervisor trust, Intel technologies and HyTrust cloud-aware products, HyTrust CloudControl* (HTCC) and HyTrust DataControl* (HTDC), offer the essential foundation for control, visibility, data security, management, and compliance in a VMware virtualized cloud infrastructure. With these solutions, IT can apply policies to have workloads run only on trusted platforms. Then, they can enforce geolocation, so data and workloads never launch in locations different than those expected. With defined policies in place, data can be encrypted and decrypted at trusted locations, and IT can run audits to ensure that all users and processes are following those policies.

Address trust – across all clouds

System attestation is a critical process designed to measure and establish the trustworthiness of systems and hypervisors. As the server boots up, solutions from HyTrust and VMware, Intel® Trusted Execution Technology (Intel® TXT), and Trusted Platform Module (TPM) utilize a secure attestation process to measure whether or not the system and hypervisor are trusted. The TPM—often described as a hardware root-of-trust—is essentially a cryptographic processor that allows for the storage, retrieval, and attestation of keys and measurements.

Utilizing HyTrust software on top of the trusted infrastructure, administrators can define trusted compute pools and provide workload placement, verification, remediation, and reporting in the cloud. Trusted compute pools allow IT to gain the benefits of a dynamic cloud environment while enforcing higher levels of protection for their higher-value, critical workloads. They can also enable the separation of those workloads from commodity application workloads. Based on policies and trust information, these solutions ensure that specific workloads and data stay within pre-defined geographic boundaries.

Security administrators can set and apply consistent policies and boundaries at the virtual workload level, so only administrators can use certain systems and access certain data. Taking advantage of the solutions' auditing and logging capabilities make it possible to review the actions of privileged administrators with the fine-grained detail that is essential for security-forensic analysis.

Look inside the solutions

The trusted cloud solutions comprise VMware virtualization software; HyTrust CloudControl and HyTrust DataControl products that run on physical or virtualized servers; TPM; and Intel TXT, a technology inside Intel® Xeon processors. TPM is supported on most enterprise-level computers sold today, while Intel TXT is available by default in most Intel Xeon processor-powered servers supplied by leading server OEMs. VMware has enabled VMware vSphere* and VMware ESXi* base capabilities with direct and integrated support for Intel TXT, TPM, and HyTrust solutions.

Intel TXT provides an inherently trusted execution process. It uses a combination of hardware and software to establish a hardware root-of-trust. HTDC and HTCC use information gained from attestation as the essential foundation for cloud control, visibility, and management to enable an increased level of security.

Server, BIOS, and hypervisor measurement (including the server's asset tag, which contains its geographic location) are stored in the TPM. Each time a server boots up, HyTrust Trust Attestation Service uses Intel TXT to establish comprehensive, hardware-based trust by cryptographically comparing the launch measurements of BIOS, OS, asset tag, and other components against a database of known good values. If the measurements during system launch match the expected values for the BIOS, firmware, and hypervisor, the system is labeled as trusted; if they do not, it is labeled untrusted. HTCC utilizes the results to enable administrators to set policies, including workload placements, onto groups of servers known as trusted compute pools.

Intel Xeon processors also include Intel® Advanced Encryption Standard New Instructions (Intel® AES-NI), a specialized instruction set designed to boost performance during cryptographic data operations. Encryption, decryption, and rekeying processes detect and automatically use these instructions.

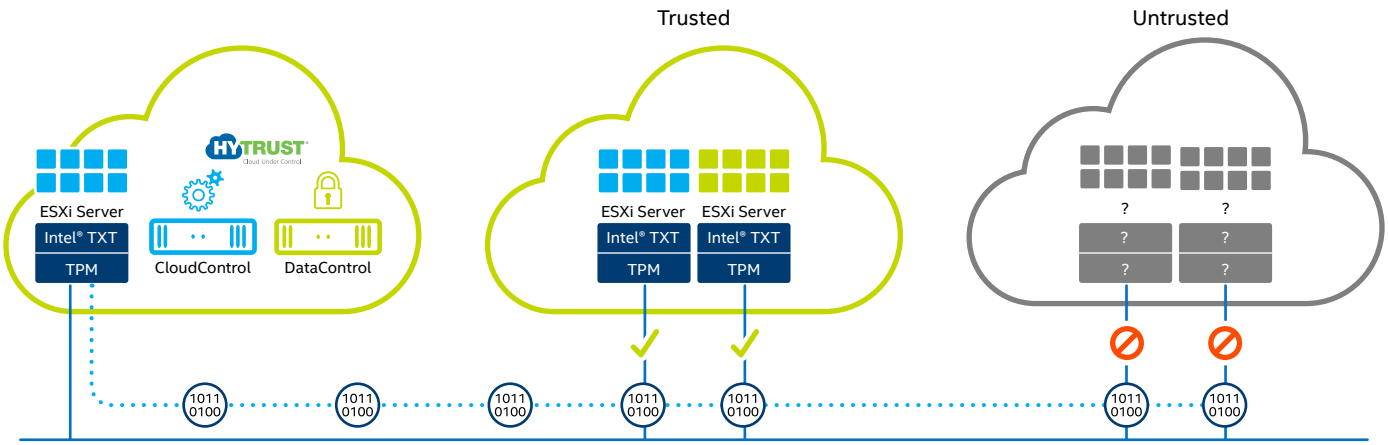

Figure 2. Intel, VMware, and HyTrust technology combine to ensure that data and workloads can move to and be processed by only trusted servers.

HyTrust and VMware solutions centralize security management and enhance control and visibility over data, wherever it is in the world. The web-based HyTrust solutions and the HTCC Management Console are used to customize configuration settings and set up policies that help safeguard the virtual environment. The console offers menus to set authentication options for virtual admins, manage vCenter Server* and hosts, define templates and policy checks to enforce security, and view logs. It captures highly detailed, real-time logs of every attempted, denied, or approved administrator action in the virtualized data center while it enforces company security policies.

VMware vSphere and VMware vCenter* offer strong across-the-board virtualization capabilities and simple, unified hypervisor management. Many companies already use VMware virtualization solutions to manage their cloud environments, making the HTCC solutions simple to integrate into existing VMware infrastructures.

HTCC, a virtual appliance compatible with VMware vSphere, has tight and integrated interdependencies with VMware vCenter. It sits between the infrastructure and its VM administrators, and when a request is submitted, it determines whether or not the request complies with the organization's security policies and permits or denies it accordingly (see Figure 2).

By logging all requests, it produces records that IT can use for auditing, troubleshooting, and analysis. HTCC provides support for private cloud, logging, active directory, root access, two-factor authentication, virtual infrastructure segmentation, host hardening, multi-tenant policy enforcement, secondary approval services, encryption, and key management.

HTDC software is a robust and flexible data security and data encryption/decryption solution. Its policy-based key management offers automated, centrally managed control over all policies. Because the software is part of a VM, encryption travels with the VM from one physical host to another. HTDC also provides a unique key management capability that allows the data owner to retain full ownership of the keys.

Taking advantage of the robust functional capabilities and flexibility provided by HTCC and HTDC, enterprises can assign trust and geolocation Boundary Controls. The use of hardware-based geolocation tags and policy enforcement can control where systems are located and where workloads and data are running. They can also ensure that data can only be decrypted and run on trusted systems and/or known-approved locations. Boundary Control enables a rich set of business use cases to ensure data security, including enforcement of specific policies to assure workload isolation.

Summary

The trust enabled by HyTrust, VMware, and Intel solutions underpins data security, geolocation, and data control for the virtualized cloud infrastructure. The solutions enable administrators to set and apply consistent policies and boundaries at the virtual workload level, so only privileged users can execute and use certain systems. Because each action is logged and available for auditing, the solutions' fine-grained controls ensure that administrators' and users' actions are within policies. Refer to Figure 3 to understand how HTCC and HTDC products connect to trusted compute pools in a secure cloud deployment.

When IT knows which systems and hypervisors in the virtualized infrastructure are trusted, they can effectively reduce risk and increase security. With these cloud solutions, enterprise IT organizations can build a trusted cloud infrastructure that helps them address their security and compliance needs for mission-critical business operations.

Regulatory requirements vary by country but typically share common goals. These include provision of data protection to mitigate risk in the event of loss or breach; visibility of and control over data location and movement, either at geographical or departmental level; and auditability of data access and usage.

Intel, VMware, and HyTrust have collaborated to offer a solution that enables IT and business leaders to take full advantage of the benefits of cloud computing while maintaining the strongest levels of data protection, visibility, and auditability necessary to protect the business.

To find the best solution for your organization, contact your Intel representative, register at IT Center, or visit www.intel.com/cloud.

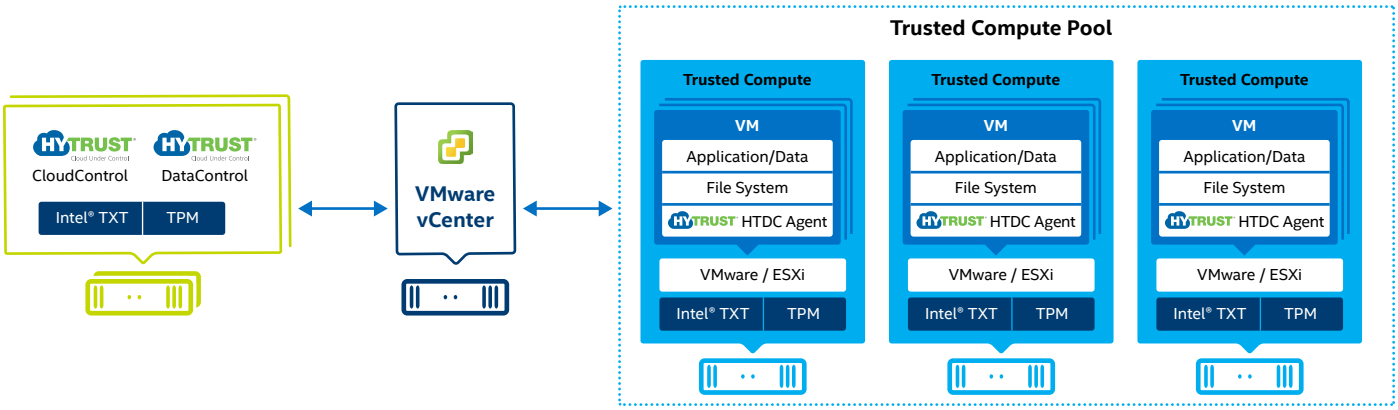

Figure 3. Interconnection of HTCC and HTDC to trusted compute pools.

0116/JMW/PT/PDF 333805-001US