HYTRUST intel IBM

The Road to a Secure, Compliant Cloud

The Road to a Secure, Compliant Cloud

Build a trusted infrastructure with a solution stack from Intel®, IBM Cloud SoftLayer,* VMware,* and HyTrust

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

A teamed solution: Agility, flexibility, trust, and compliance

Enterprises face more competition now than ever before. Innovative business models are disrupting the market, forcing even the largest organizations to transform the way they do business. Corporations must 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 corporate goals lies a company's business processes and intellectual property – their workloads and data. The infrastructure that enables the security and compliance of those workloads and data is the virtualized cloud. A well-designed virtualized cloud offers business decision-makers incredible agility in terms of available resources for their workloads and data. In turn, that creates opportunities for innovation through rapid, iterative development of new services and business models. In addition, IT groups gain increased operational efficiency while still meeting corporate requirements for performance, cost, and flexibility.

Elements of a trusted cloud infrastructure

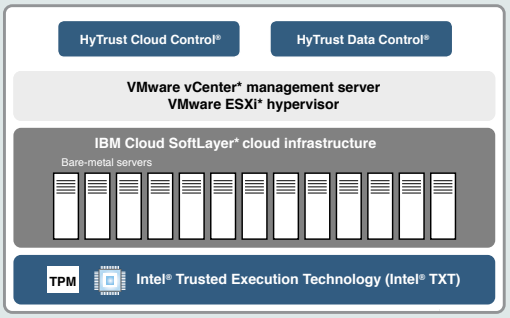

Figure 1. *Moving towards increased compliance and trust. The combined solution from Intel®, IBM Cloud SoftLayer (SoftLayer),* VMware,* and HyTrust* establishes a robust chain of trust from hardware up through hypervisor and applications.*

New challenges for the virtualized cloud

Along with virtualization benefits come new challenges and unique risks for security and compliance. For example, in a virtualized cloud, workloads and data can migrate between hosts that might not be in authorized configurations or even in authorized locations.

Security breaches of sensitive information can lead to disastrous business and legal consequences. When a breach occurs, it's up to IT to identify and close the breach as rapidly as possible. However, traditional IT solutions cannot automatically govern or resolve virtualization challenges or protect effectively against today's risks. Instead, businesses must build their virtualized clouds with new, robust solutions that help ensure both in-house security and compliance with other rules and regulations.

Companies must now strive for a solution in which they can trust all managed systems, from hardware up through hypervisor, for use cases such as data privacy, geolocation (data location), boundary control, geo-fencing, and intelligent decryption.

Look inside the trust solution

Delivering on the promise of trust and compliance requires that virtualized clouds be built upon the right architectural model. Intel®, IBM Cloud SoftLayer (SoftLayer),* VMware,* and HyTrust* have teamed up to resolve that critical challenge. The result of this extensive collaboration is a solution stack that enables leading concepts -- such as trusted compute pools -- and powerful new use cases. IT and business leaders can now build a trusted, securely governed infrastructure, while taking full advantage of the benefits of virtualization and the cloud. The architecture of this trusted cloud is built on:

- Intel® Xeon® processors
- Intel® Trusted Execution Technology (Intel® TXT)
- Trusted Platform Module (TPM) 1.2
- Intel® Advanced Encryption Standard - New Instructions (Intel® AES-NI)
- IBM Cloud SoftLayer (SoftLayer)* bare-metal servers
- VMware vCenter* management server
- VMware ESXi* hypervisor (the virtualization OS)
- HyTrust CloudControl (HTCC)*
- HyTrust DataControl (HTDC)*

When you order your SoftLayer bare-metal servers with Intel TXT and TPM, SoftLayer automatically performs initial configurations and provisions the server for you. This includes enabling and setting up the trust technologies to ready them for your deployment environment. Once enabled, Intel TXT is always "on," automatically providing the root of trust for each server.

Above the hardware, HyTrust and VMware solutions provide centralized security management and enhance IT control and visibility of data. First, VMware provides the virtualization layer of the cloud, through the VMware vCenter management server and the VMware ESXi hypervisor (the OS). VMware offers strong, across-the-board virtualization capabilities and simple, unified hypervisor management. Many companies already use VMware virtualization to manage their cloud environments, which makes HyTrust simple to integrate into existing VMware infrastructures.

HyTrust provides automated, policy-based management of virtualized servers. This management layer consists of HyTrust CloudControl (HTCC) and HyTrust DataControl (HTDC) components. HTCC allows IT to customize configuration settings and set up policies that help safeguard the virtual environment from both external and internal threats. This includes setting authentication options for virtual administrators, managing VMware vCenter Server* and hosts, and establishing management and security policies. HTCC enforces policies and also captures highly detailed, forensic logs of every attempted, denied, or approved administrator action in the virtualized data center. This helps you comply more effectively with stringent audit and compliance requirements, and stop security threats as quickly as possible.

VMware capabilities include direct, integrated support for Intel TXT, TPM 1.2, HTCC, and HTDC. In turn, HTCC and HTDC include direct, integrated support for Intel TXT, TPM, and VMware solutions. HTCC has integrated with VMware vCenter for easy management. Functionally, HTCC sits between the virtualized cloud infrastructure and the VM administrators. When an VM administrator request is submitted, HTCC determines whether or not the request complies with security policies; then permits or denies the request accordingly (see Figure 2). HTCC can also determine whether an action requires additional approval (for example, the "four-eyes" principle). Also, by logging all requests, HTCC produces forensic-quality records for auditing, troubleshooting, and analysis. In this solution stack, HTCC provides trust-based support for logging, active directory services, virtual infrastructure segmentation, hypervisor hardening, and multi-tenant policy enforcement.

The second HyTrust component, HTDC, is a robust and flexible data security and encryption/decryption solution. HTDC provides IT with military grade encryption, as well as easy and scalable key management. (Hytrust encryption and key management are NIST FIPS 140-2 validated.) HTDC key management offers automated, central control over your encryption policies. Because an HTDC agent is installed within the VMs, encryption also travels with the VM from one physical host to another. This helps ensure that workloads can be encrypted on any on-premise or cloud platform. In addition, a unique key-management capability allows the data owner to retain full ownership of the keys -- a critical capability in the cloud.

HyTrust includes direct, integrated support for Intel Advanced Encryption Standard - New Instructions (Intel AES-NI). Intel AES-NI is built into Intel Xeon processors to enable smarter, faster, more effective encryption with almost zero performance overhead. HyTrust automatically detects and takes advantage of Intel AES-NI in the CPU to enhance HyTrust encryption, decryption, and rekeying processes. Enterprises can now afford to encrypt and secure all workloads and data, not just those that are highly sensitive.

The importance of trust in a virtualized infrastructure

In order to have trust in your infrastructure, you must be able to trust your hosts, data stores, hypervisor, and governance. That means knowing that your hosts are in their expected locations, with authorized configurations. It means knowing that your sensitive workloads and data run only on trusted hosts, and are transferred only between trusted hosts in appropriate locations. It also means knowing that decryption of your virtual data stores will be allowed only when both the workload and the host holding that data are also trusted and authorized to handle that data. Finally, it means knowing that your admins take only authorized actions, and that all actions requested or taken in the cloud -- whether deliberate, accidental, or caused by malfeasance -- are logged. The root of trust, and the use cases it enables, are key to the solution of the trusted cloud.

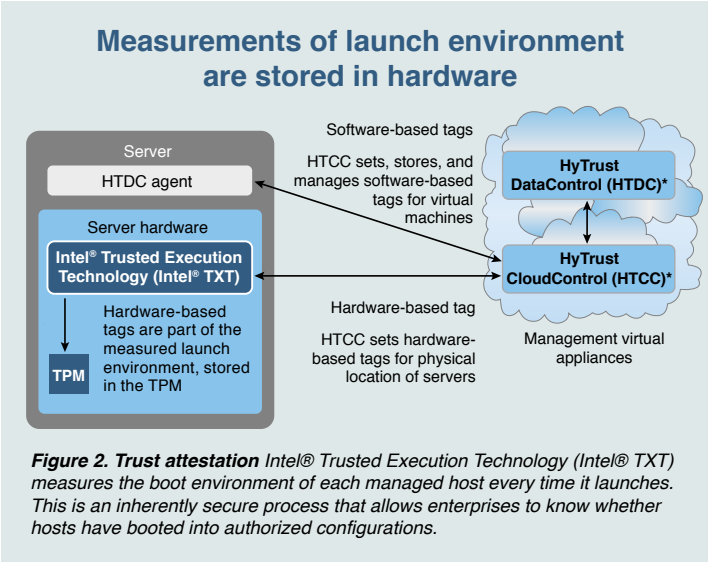

Figure 2. Trust attestation *Intel® Trusted Execution Technology (Intel® TXT) measures the boot environment of each managed host every time it launches. This is an inherently secure process that allows enterprises to know whether hosts have booted into authorized configurations.*

The root of trust

With today's security and regulatory requirements, the virtualized cloud requires a foundation of trust -- a root of trust. This foundation is based in hardware, and enabled by Intel TXT and TPM. In the trusted cloud, each time a server boots, Intel TXT measures the boot environment as it launches. Every element of the boot environment is measured: BIOS, OS, hypervisor, VMkernel,* and a subset of the loaded modules (VMware vSphere* installation bundles, or VIBs). Those measurements are stored in the TPM, in an inherently secure process.

The chain of trust is extended via HyTrust, which includes the Trust Attestation Service (TAS). HyTrust compares the measurements in the TPM to a white list stored in the TAS. If the host's launch measurements match the measurements in the TAS white list, then HyTrust labels the host as trusted. Basically, if the host boots into a configuration that is recognized as authorized, the host is considered trusted. If not, HyTrust labels the host untrusted. HyTrust can then use the trust status of the host to enforce IT-defined policies for workload and data migration, management, and decryption. For example, IT policies could specify that untrusted hosts are removed for maintenance, allowed to run only low-level applications, and so on.

Trust enables powerful use cases

Trusted compute pools. Intel TXT and HyTrust work together to verify whether hosts boot into trusted, authorized configurations. This is trust attestation, enabled by Intel TXT and the TPM. Once IT knows which hosts can be trusted, IT can use HyTrust to group those hosts into trusted compute pools. This is one of the leading concepts for managing a compliant, virtualized cloud. Trust-based compute pools help IT meet different business, security, and compliance needs for workloads, sensitive data, and cloud resources. For example, IT can now apply intelligent policies to workloads so that different, sensitive workloads run only on specific, trusted servers in specific, trusted groups. Commodity application workloads could be assigned to other, more typically secured hosts. For enterprise, trusted compute pools provide the benefits of a dynamic cloud environment while enforcing high levels of protection for higher-value, critical workloads

Accurate data location. Data location is knowledge of the actual, physical location of a host. With trust attestation and hardware-based policy tags, IT now has visibility of actual server locations across the virtualized cloud. The hardware-based tags are HyTrust descriptors that let you "tag" hosts by location, capabilities, compliance requirements, or other logical identifiers. Because these are hardware-based descriptors, they are part of the host's launch environment and are measured by Intel TXT each time the host launches. Servers can now verify, not just their configurations, but their actual, physical locations each time they boot.

Verified boundary control. Boundary control is the ability to restrict workloads and/or data to run only within a specified boundary. This can be a geographic boundary, such as a country's borders. It can also be a logical boundary, such as a boundary based on a logical grouping, capability, or compliance factor. Boundary control is enabled either by software-based tags or through the more robust security option via Intel TXT, hardware-based policy tags, and HyTrust. Once IT knows the actual, physical location of each host, IT can use HyTrust policies to restrict data and workloads to only authorized locations, and provide evidence-based reporting for those restrictions.

Additional geo-fencing. Geo-fencing is the ability to separate workloads within a trusted compute pool. For example, you can use trusted compute pools and boundary control to group trusted servers within a specific region. You could then use geo-fencing to separate workload types within that pool, such as fencing off accounting workloads from auditing workloads. Geo-fencing gives you even finer control to group servers within a trusted compute pool.

Smarter, faster decryption. The solution stack from Intel, SoftLayer, VMware, and HyTrust helps IT make sure that decryption occurs only at trusted locations on authorized servers. For example, in a traditional

Geo-fencing: Restrict workloads to specific servers within a trusted pool

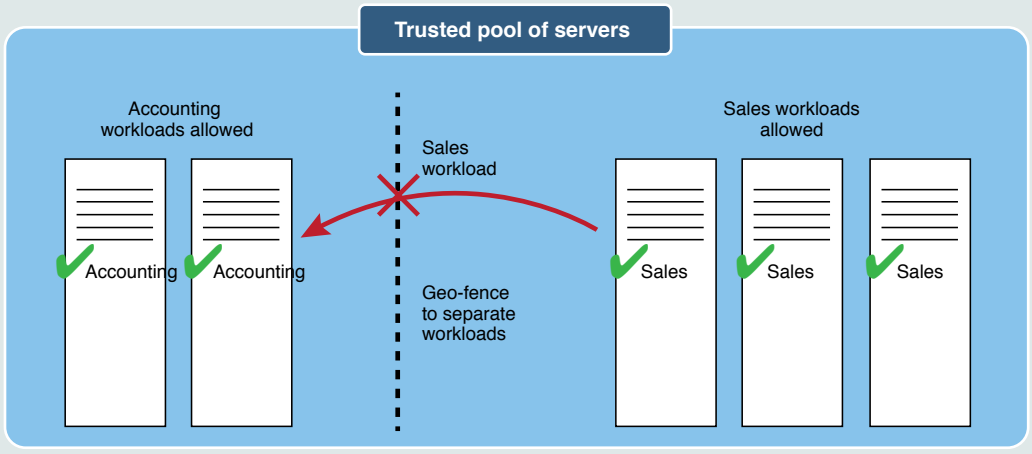

Figure 3 *Capabilities such as trust attestation enable trusted compute pools, boundary control, and geo-fencing, to help make sure data and workloads are handled only by trusted, authorized servers.*

cloud, it's possible for a virtual workload to be loaded onto an external drive, moved to an untrusted host, and decrypted. In contrast, in the trusted cloud, encryption is tied to the VM itself, and moves with the VM. Even if a workload is moved to an untrusted host, the workload cannot be decrypted without authorization. In addition, with trust attestation and data location, HyTrust policies can enforce and approve decryption requests only for authorized hosts that are physically located in authorized locations.

Evidence-based compliance. Regulatory requirements typically require data protection to mitigate risk in the event of a loss or breach. Compliance also usually requires control over data location and movement, and evidence-based audits of data access and usage. In this solution stack, Intel TXT and HyTrust allow security administrators to set and apply consistent, intelligent policies at the virtual workload level -- and provide visibility and logging of all virtualized activity. Fine-grained logging makes it possible to review the actions of privileged administrators with the detail that is essential for security analyses. In addition, HyTrust provides logging of administrator actions based on individuals, so that IT can now provide evidence-based audits and reports, and enable forensic-level analyses when required.

Summary

The trust attested by the combined solution from Intel, SoftLayer, VMware, and HyTrust enables powerful leading concepts and use cases: trusted compute pools, hardware-based policy tags, data location, boundary control, geo-fencing, and policy-based decryption. This robust solution stack allows administrators to set, apply, and enforce consistent, trust-based policies even at the virtual workload level. Trust attestation gives IT visibility of physical servers across any virtualized infrastructure so that IT can make sure that only authorized servers in authorized locations handle sensitive workloads. With trust, IT can better enforce only authorized administrator actions, and help make sure that all requested actions -- whether approved or denied -- are logged for reporting and compliance.

When IT knows which hosts can be trusted, IT can more effectively reduce risk and increase security. The solution stack from Intel, SoftLayer, VMware, and HyTrust enables a trusted cloud infrastructure that helps address in-house security needs as well as compliance requirements for mission-critical business operations. IT and business leaders can now take full advantage of the benefits of cloud computing while maintaining the strongest levels of data protection, visibility, and auditing necessary to protect the business.

To learn more about this solution and how to deploy it in SoftLayer, visit:
https://knowledgelayer.softlayer.com/learning/intel-trusted-execution-technology-txt