WHITE PAPER
Intel® Trusted Execution Technology
Intel® Xeon® Processor
Secure Cloud Computing

Building Trust and Compliance in the Cloud with Intel® Trusted Execution Technology

The Taiwan Stock Exchange Corporation Develops a Secure Cloud Infrastructure

EXECUTIVE SUMMARY

The Taiwan Stock Exchange Corporation (TWSE) is a financial institution operating as a stock exchange that provides trading for 758 listed companies in Taiwan. Its primary business drivers include developing new financial products and boosting the number of services it offers. This paper highlights the systems, solutions, and approach Intel used in a joint proof of concept (PoC) with TWSE to address its business needs and increase the overall trust and security of its cloud infrastructure using Intel® Trusted Execution Technology (Intel® TXT), Cisco Unified Computing System* (UCS*) servers, and software solutions from HyTrust, McAfee, and VMware.

TWSE needed to build a more secure foundation for sensitive cloud workloads. It is using the components from these companies to establish trusted compute pools (TCP) providing the additional elements of security, visibility, and control needed to put more applications and workloads into its cloud infrastructure. From this initial proof-of-concept deployment, TWSE expects many other business units to be able to more effectively use cloud infrastructures to increase business agility, reduce costs, and improve asset utilization without compromising security considerations.

> Developing effective, efficient, and proven security and trust solutions to minimize the complexities of managing cloud infrastructures

Contributors

Intel Corporation
James J. Greene
Martin Guttmann
Kou-Hui Li
Jinn Parng
Raghu Yeluri

TWSE
Cheng-Yi Wu
Ken Wu

HyTrust
Hemma Prafullchandra
Ken Sigel

McAfee
Ed Reynolds

VMware
Gargi Keeling

Trust and Security Challenges

The rapid adoption and growing deployment of cloud infrastructure and solutions—internal, external, and/or federated—introduces new trust and security challenges.

In cloud infrastructure, systems are automatically provisioned. Applications are deployed and moved from system to system based on available IT resources. While this creates powerful efficiency and agility benefits, it often does so at the expense of creating new security and trust concerns.

There is very little visibility to the operating state of the infrastructure in this multi-tenant environment. Depending on the organization's industry segment, there may be many regulations that specify security controls, enforcement, and visibility to enable compliance.

Organizations need effective, efficient, and proven security and trust solutions to minimize the complexities of managing their cloud infrastructures and the workloads they wish to host there. They also need integration with existing IT systems and security tools. Finally, trust solutions need to enable automated security reviews and audits to ensure security and overall trust.

Fundamentally, organizations are searching for solutions and systems that behave in an expected way, ensuring that issues of trust are effectively addressed and managed.

A fundamental business and technical requirement for the cloud infrastructure under construction at TWSE was to provide secure systems and trusted compute environments. TWSE has established that it is crucial to integrate software application

Contents

solutions that will provide overall trust and security for its cloud infrastructure and fully use hardware-based security and provide root of trust and platform attestation. The goals for the organization were to enable:

- **Greater visibility** into the security states of the hardware platforms running infrastructure as a service (IaaS) for its private clouds
- **Production of automated, standardized reports** on the configuration of the physical and virtual infrastructure hosting customer virtual machines and data
- **Controls** based on the physical location of the server and location of the virtual machines and control the migration of these virtual machines onto acceptable servers, per specified policy
- **Collection of measured evidence** that services infrastructure complies with security policies and regulated data standards

To explore the capabilities and challenges of implementing such an infrastructure, TWSE engaged Intel and other key ecosystem members to develop a multi-phased proof of concept (PoC) implementation of a secure cloud based on familiar tools, platforms, and software. The capabilities the PoC needed to provide included:

- **Measured boot** for servers with platform attestation
- **Creation** of TCPs
- **Security-controlled workload placement** in the TCPs
- **Security controlled workload migration** in TCPs
- **Security and platform trust** Integrated and extended with McAfee ePolicy Orchestrator* (McAfee ePO*)

TWSE Business Needs and Priorities

To support its plans to deliver new business services for both internal and external brokers, TWSE decided to build a cloud infrastructure. A fundamental business and technical requirement for the infrastructure is to provide secure systems and trusted compute environments. Thus, it is crucial to integrate software application solutions that will provide TWSE with overall trust and security for its cloud infrastructure and fully use hardware-based security and provide root of trust and platform attestation.

In a cloud infrastructure, systems can be automatically provisioned based on needs. Applications are deployed and moved from system to system based upon available IT resources—not whether the systems have the required trust policies in place. TWSE requires appropriate trust policies. But tracking migration, reporting, applying policies, and auditing where and on what systems workloads are running can be a complex undertaking.

To address TWSE's overall business requirements in its cloud PoC infrastructure, solutions need integrated functionality for cohesive and greater overall trust and support for security, policy enforcement, audits, reporting, and compliance. For efficient operation, solutions need to provide:

- **Integration** for existing IT operational solutions including governance, risk, and compliance (GRC)
- **Security** information and event management (SIEM)
- **Security** and server management
- **Server** security risk dashboard

Figure 1 is an example of the integrated security and compliance elements of this PoC solution aligned to meet TWSE's business requirements, ranging from system deployment and provisioning and effective policy control to trust enforcement and audits.

Enabling Trust for Cloud Infrastructure

To address business and technical requirements for TWSE's cloud infrastructure, the organization worked with Intel on a joint, phased PoC. Goals were to demonstrate solutions, starting with hardware-based security, to provide root of trust platform verification and attestation. This included enabled hypervisor and software solutions that effectively manage and apply policies in the cloud infrastructure starting with known, trusted systems and a virtual machine manager (VMM) kernel.

Organizations that are using or want to use cloud services are starting to require cloud service providers to better secure the hardware layer and provide greater transparency into the system activities within and below the hypervisor. This means that cloud providers should be able to:

- **Give organizations greater visibility** into the security state of the hardware platforms running the IaaS for their private clouds.
- **Produce automated, standardized reports** on the configuration of the physical and virtual infrastructure hosting customer virtual machines and data
- **Provide controls** based on the location of the server and virtual machines and control the migration of these virtual machines onto acceptable servers per specified policy (e.g., FISMA and DPA requirements)
- **Provide measured evidence** that the services infrastructure complies with security policies and regulated data standards

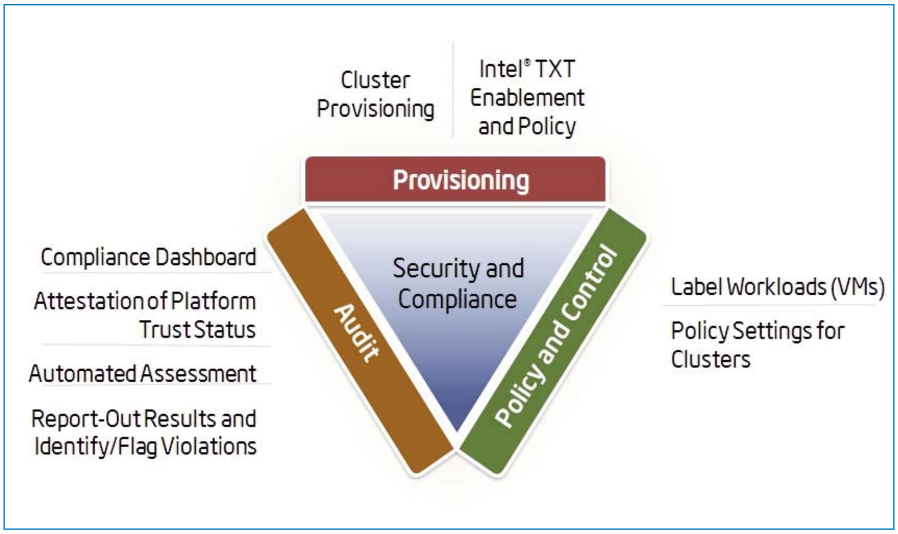

Cluster Provisioning
Intel® TXT Enablement and Policy
Provisioning
Compliance Dashboard
Attestation of Platform Trust Status
Automated Assessment
Report-Out Results and Identify/Flag Violations
Audit
Security and Compliance
Policy and Control
Label Workloads (VMs)
Policy Settings for Clusters

Figure 1. Components and Roles for Integrated Security and Compliance

What is needed is a set of foundational building blocks for developing more trustworthy clouds. These building blocks can be summarized as:

- **Creating a chain of trust** rooted in hardware that extends to include the hypervisor
- **Hardening the virtualization environment** using known best practices
- **Providing visibility** of assets, controls, and enforcement for compliance and audit
- **Using trust information** as part of the policy management for cloud activity
- **Using infrastructure and services** to address data protection requirements
- **Using automation** to bring it all together and achieve scale and management efficiency

Intel TXT: A Foundation for Trust, Visibility, and Control in the Cloud

Overall trust and security in a cloud computing infrastructure must begin with the servers and base compute systems. The basic elements of this trusted platform ideally (and in the case of Intel TXT) span hardware, firmware, and software to provide the best balance of tamper-resistance and functionality.

Intel TXT is available with many servers featuring the Intel® Xeon® processor E3, E5, and E7 families. Platform-level enhancements provide the building blocks to enable visibility, trust, and control in the cloud. As Figure 2 shows, Intel TXT includes support and capabilities in the microprocessor, chipset, I/O subsystems, and other platform components. Designed to measure the execution environment and protect sensitive information from software-based attacks, it operates with Trusted Platform Module* (TPM*), an industry-standard device that can securely store artifacts used to verify integrity of the platform.

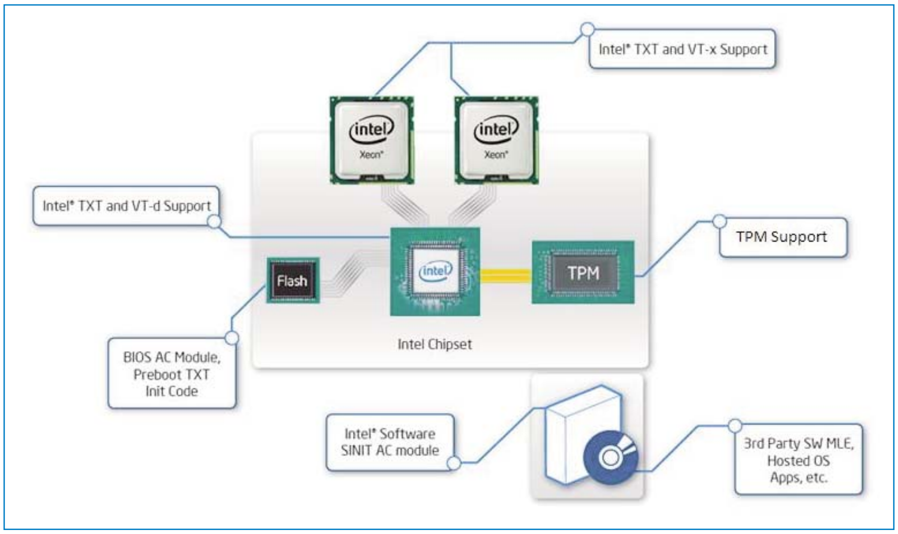

Intel® TXT and VT-x Support
intel Xeon®
intel Xeon®
Intel® TXT and VT-d Support
TPM Support
Flash
intel
TPM
Intel Chipset
BIOS AC Module, Preboot TXT Init Code
Intel® Software SINIT AC module
3rd Party SW MLE, Hosted OS Apps, etc.

Figure 2. Components of Intel TXT and its Solution Stack

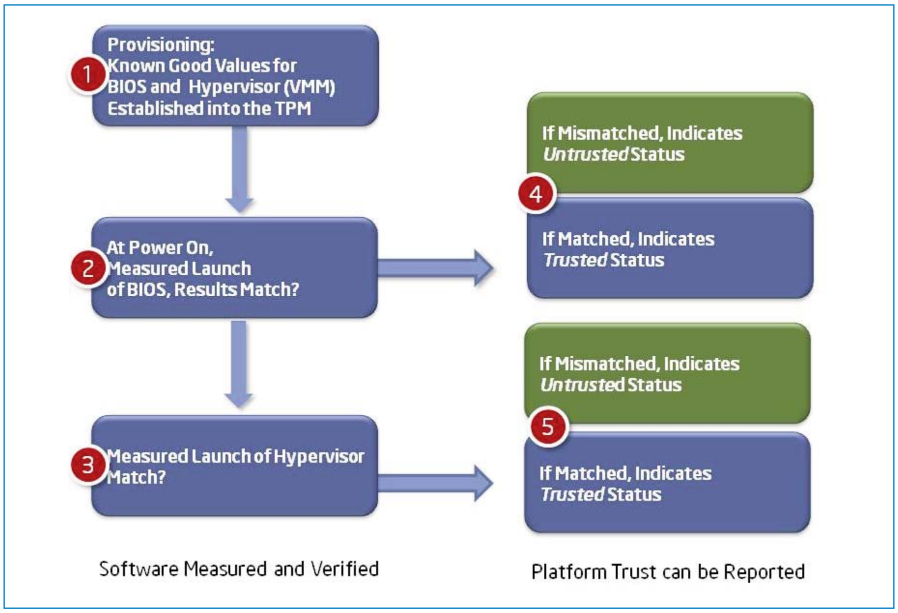

1 Provisioning: Known Good Values for BIOS and Hypervisor (VMM) Established into the TPM
2 At Power On, Measured Launch of BIOS, Results Match?
3 Measured Launch of Hypervisor Match?
If Mismatched, Indicates *Untrusted* Status
4
If Matched, Indicates *Trusted* Status
If Mismatched, Indicates *Untrusted* Status
5
If Matched, Indicates *Trusted* Status
Software Measured and Verified
Platform Trust can be Reported

Figure 3. Creating a Foundation of Trust with Intel TXT

Hardware-based root of trust—when coupled with an enabled operating system, hypervisor, and solutions—is the foundation for a more secure computing platform that can ensure hypervisor and VMM integrity at boot from rootkits or other low-level attacks. It establishes the trustworthiness of the server and host platforms. The hardware-based root of trust uses open industry standards developed by Trusted Computing Group (TCG) to establish and ensure platform trust and store measurements in a TPM.

The solution works by providing a root of trust—a processor-based, tamper-resistant environment that compares firmware, BIOS, and operating system or hypervisor code to known good configurations to establish a measured, trusted environment prior to launch. If integrity and trust are not verified in the launch process, Intel TXT identifies that the code has been compromised, which lets you protect the system and remediate the problem. The basic process for an Intel TXT launch process is shown in Figure 3.

Because Intel TXT can evaluate and report on platform integrity using attestation mechanisms, it can provide valuable insights and controls when used in the context of cloud computing models. This allows other key software—virtualization, cloud orchestration and management, and security policy applications—to understand and use platform integrity attributes to control workloads and data and better address security risks by keeping sensitive or regulated workloads separate from platforms with unknown integrity status. This is a concept that Intel and like-minded solution companies call TCPs. Numerous system and software vendors are developing solutions that integrate hardware-based root of trust capabilities, supporting Intel TXT to further extend and address security and trust issues for cloud infrastructure.

Enabling Platform Attestation

There are mechanisms to establish platform trust. The platform must have:

- **Root of trust for measurement (RTM).** This is provided by Intel TXT
- **Root of trust for reporting (RTR).** This is provided by the TPM
- **Root of trust for storage (RTS).** This is provided by the TPM

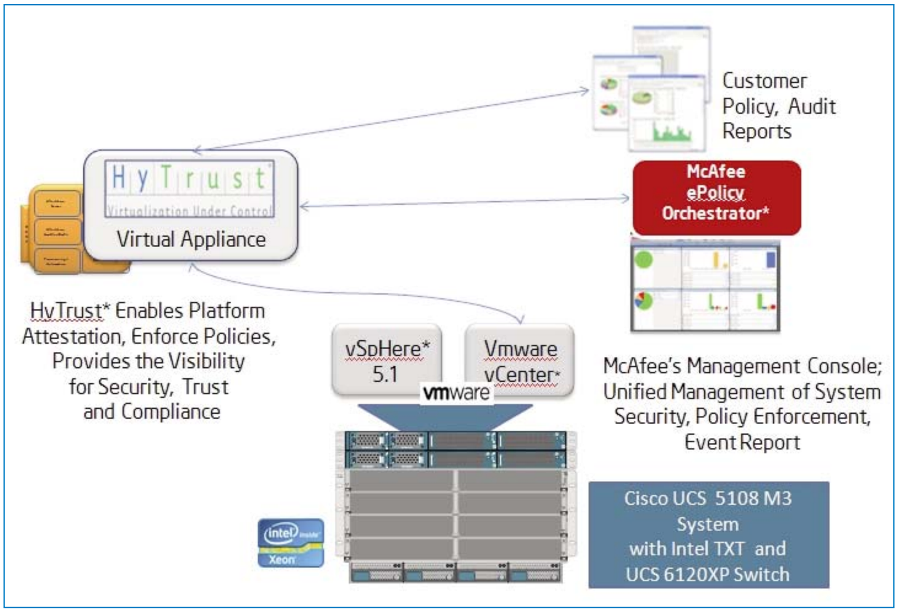

Customer Policy, Audit Reports
McAfee ePolicy Orchestrator*
HyTrust
Virtualization Under Control
Virtual Appliance
HyTrust* Enables Platform Attestation, Enforce Policies, Provides the Visibility for Security, Trust and Compliance
vSpHere* 5.1
Vmware vCenter*
vmware
McAfee's Management Console; Unified Management of System Security, Policy Enforcement, Event Report
intel inside Xeon
Cisco UCS 5108 M3 System with Intel TXT and UCS 6120XP Switch

Figure 4. TWSE PoC Systems and Solutions

RTM, RTR, and RTS are the foundational elements of a single platform. For use cases to be instantiated and delivered in a cloud, two key questions must be answered:

1. **How would** the entity needing this information know if a specific platform has Intel TXT enabled if a specific server has a defined or compliant BIOS or VMM running on it (i.e., can it be trusted)?
2. **Why should** the entity requesting this information (which, in a cloud environment, could be a resource scheduler or orchestrator trying to schedule a service on a set of available nodes or servers) trust the response from the platform?

The answers to these key questions determine:

- **How a given server** is added to a TCP
- **How a service** is placed on a server in a TCP
- **How and where a service** gets migrated in the pool

Attestation provides the definitive answers to these questions. Attestation elevates the operational value of roots of trust by making the information from the root of trust visible and usable by other entities. It is the process of providing a digital signature of a set of platform configuration registers (PCR)—a set of registers in a TPM that are extended with specific measurements for various launch modules of the software—and having the requestor validate the signature and the PCR contents. To validate, the requestor first invokes the TPM_Quote command, specifying:

- **An attestation identity key** to perform the digital signature
- **The set of PCRs** to quote
- **A nonce** to ensure freshness of the digital signature

Next, it validates the signature and makes a determination about the trust of the launched server by comparing the measurements from the TPM quote with known-good measurements. It is a critical IT operations challenge to manage the known-good measurement for hypervisors, operating systems, and BIOS software to ensure they are all protected from tampering and spoofing. This capability can be internal to a company, from a service provider, or delivered remotely as a service by a trusted third party (TTP), as shown in Figure 4.

TCP Overview

TCPs, as shown in Figure 5, are physical or logical groupings of computing platforms in a data center that have demonstrated integrity of key controlling components (e.g., BIOS and hypervisor) in the launch process. Intel TXT provides a hardware-based mechanism for verifying and reporting on platform trust as a foundation for creating trusted pools. Platform trust status is attested at launch. If the launch is trusted, that platform can be added to the trusted pool. Within this pool, systems and workloads can be tagged with security policies. The access and execution of apps and workloads can also be monitored, controlled, and audited.

Creating TCPs is a way to aggregate trusted systems and segregate them from untrusted resources. It provides an infrastructure to support the separation of higher-value, more sensitive workloads from commodity applications and data. The principle of operation is to:

- **Create a part of the cloud** to meet the specific and varying security requirements of users
- **Control access** to an identified portion of the cloud so that only approved workloads and applications get deployed there
- **Enable audits** of that portion of the cloud so that users can verify compliance

Such TCPs enabled by Intel TXT allow IT to gain the benefits of the dynamic cloud environment while still enforcing higher levels of protection for critical workloads. Also, use of TCPs eliminates the need for air-gapped clusters of servers.

Multi-Phased Cloud Infrastructure PoC

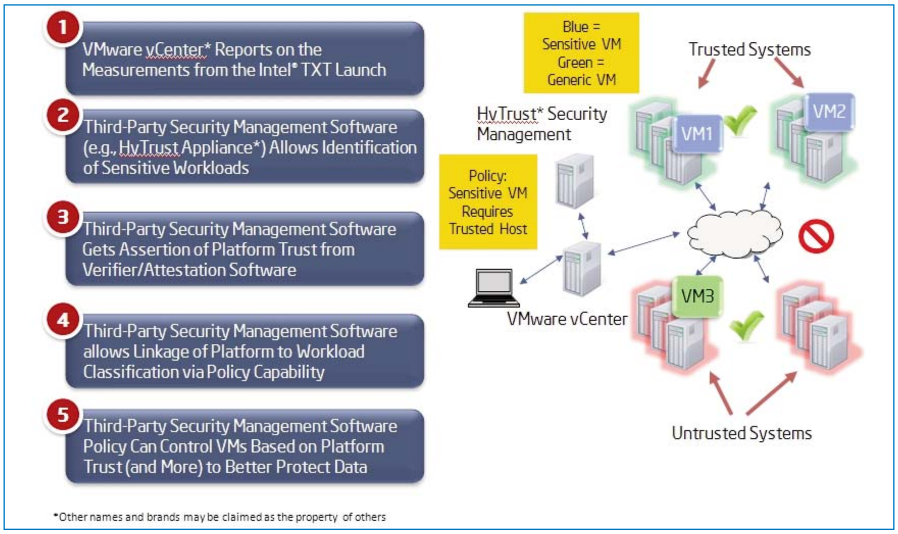
The objective of the comprehensive PoC was to highlight solutions and systems that will effectively address TWSE's needs and enable broader, policy-based trust for its planned cloud infrastructure. TWSE also needed to integrate and test solutions that would support overall trust and security for its IT and operations.

A skilled team participated in the PoC, from planning to execution. It included participants from TWSE, Cisco, HyTrust, Intel, McAfee, Systex, and VMware with expertise from infrastructure engineers, solution experts, IT operations, security architects, and business leads.

The PoC needed to clearly define a critical set of operational use cases, which it characterized under an umbrella concept of creating TCPs based on Intel TXT-enabled platforms. It also wanted to showcase software solutions, trust, and security functionality, so a critical part of the PoC was to highlight seamless integration of hardware root of trust, platform attestation, and policy security solutions with TWSE's cloud Infrastructure to address comprehensive trust and security.

Defining PoC Use Cases

The team began by defining use cases for creating TCPs with Intel TXT. These use cases were started by enabling trust from compute platforms via Intel TXT and then extending the trust and security throughout operational software solutions and systems to create the base TCPs. From there, they established use cases that would be integral to these TCPs (Figure 6). The


1
VMware vCenter* Reports on the Measurements from the Intel® TXT Launch
2
Third-Party Security Management Software (e.g., HyTrust Appliance*) Allows Identification of Sensitive Workloads
3
Third-Party Security Management Software Gets Assertion of Platform Trust from Verifier/Attestation Software
4
Third-Party Security Management Software allows Linkage of Platform to Workload Classification via Policy Capability
5
Third-Party Security Management Software Policy Can Control VMs Based on Platform Trust (and More) to Better Protect Data
Blue = Sensitive VM
Green = Generic VM
Trusted Systems
HyTrust* Security Management
VM1
VM2
Policy: Sensitive VM Requires Trusted Host
VMware vCenter
VM3
Untrusted Systems

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

Figure 5. Creating the TCPs

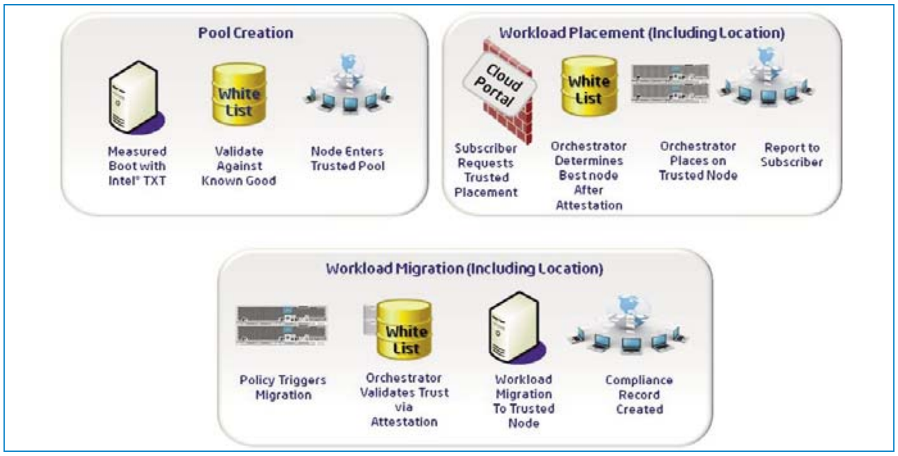

Pool Creation
White List
Measured Boot with Intel® TXT
Validate Against Known Good
Node Enters Trusted Pool
Workload Placement (Including Location)
Cloud Portal
White List
Subscriber Requests Trusted Placement
Orchestrator Determines Best node After Attestation
Orchestrator Places on Trusted Node
Report to Subscriber
Workload Migration (Including Location)
White List
Policy Triggers Migration
Orchestrator Validates Trust via Attestation
Workload Migration To Trusted Node
Compliance Record Created

Figure 6. TCPs Use Cases

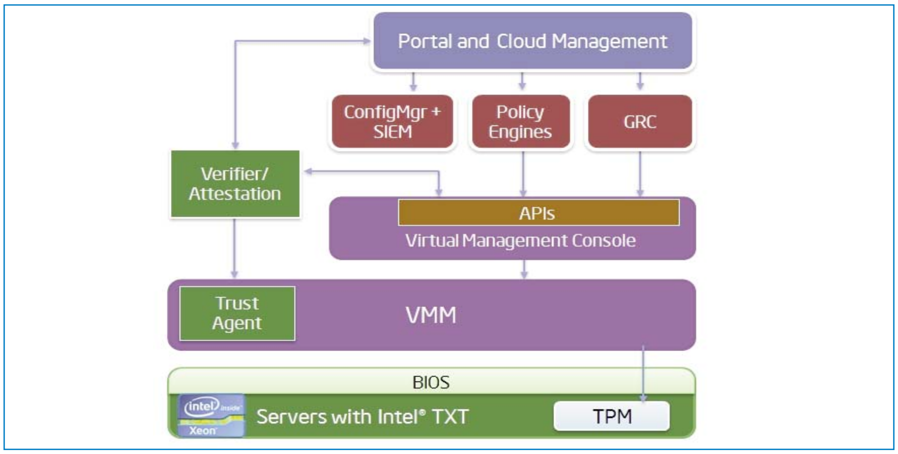


Figure 7. Intel TXT Trusted Compute Cloud Solution Reference Architecture

evolution of the phased approach is described in Table 1.

Table 1. Evolution of the Phased Approach

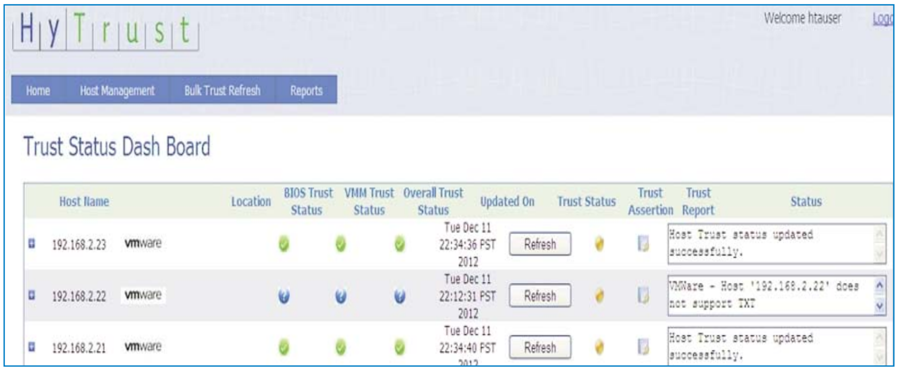
PHASE	DESCRIPTION	STEPS
1	**Measure boot for servers**	A. Measure launch of the server BIOS and VMM of Intel TXT-enabled servers.
		B. Validate measured vs. expected server measurements as known-good values or whitelist measurements against measured data.
		C. Report the trust status of the server as trusted or not trusted based on the results of the measured launch process.
2	**Perform platform attestation and create trusted complete pools**	A. Add only trusted server to the TCPs of servers based on policy.
3	**Place workloads in the TCPs**	A. When a cloud service/VM is provisioned, the service owner requires (and requests via policy) a placement of the service in a trusted pool.
		B. Orchestration software will place workload on servers in the trusted pool.
4	**Migrate workloads to compute pools**	A. Migration of workloads is triggered (for planned or unplanned reasons); the orchestration software determines the optimal set of servers to migrate workloads.
		B. Migration policies are examined for the trusted servers.
		C. Allow or disallow workload migration based on policy; the migration is completed or aborted.
5	**Integrate and extend security and platform trust with McAfee ePO**	A. Ensure security is up-to-date to conform to security compliance
		B. Verify & report on integrity of security technology in the Trusted Pool

Trust System and PoC Solutions Architecture

For the PoC, the team designed a system and solutions architecture and phased set of activities as defined above. The PoC examined TWSE's current solutions and systems and its overall enterprise operational and management solutions. It also examined the Intel TXT Trusted Compute Pools Cloud Solution Reference Architecture (Figure 7) as a baseline for building the PoC architecture. Since trust and security need to go from bottom to top, it is crucial to know the trust levels of the hardware platform and the hypervisor, as discussed previously. For the PoC implementation, the team selected a number of systems and solutions based on TWSE current and future directions and business needs. As shown in Figure 4, these included:

- **Cloud system and infrastructure supported by Cisco.** This included a fabric-based converged UCS M3 server with the Intel Xeon processor E5 family and Intel TXT enabled, equipped with the TPM. For testing, the PoC used three blades to be able to establish a mix of trusted and untrusted platforms in the PoC environment.
- **Virtualization solutions supported by VMware.** Managing the virtualized infrastructure was VMware vCenter Server* 5.1 with VMware ESXi* 5.1 hypervisor, which allows enterprises to use their own security certificates when securing remote sessions. VMware ESXi 5.1 also provides full, integrated support and functionality for Intel TXT and enables remote platform attestation measurements to detect possible malicious changes to BIOS and other critical base software components of the servers. VMware ESXi 5.1 measures the critical components of the hypervisor stack when the system boots and stores these measurements in the PCR of the TPM on the platform. The measured elements include the VMkernel*, kernel modules, drivers, native management applications that run on ESXi, and any boot-time configuration options.

- **Trust and policy solution supported by HyTrust and HyTrust Appliance***. The team used HyTrust Appliance 3.5 beta version, which provides extensive support for Intel TXT. The HyTrust Appliance verifies the integrity of the physical hardware of the host to ensure the underlying platform is fully trusted and can implement powerful policies based on this information. It can ensure that specified workloads are only permitted to be instantiated on specific hosts or clusters. It also intercepts all administrative access and change requests, determines whether a request is in accordance with the organization's defined policy, and permits or denies the request as appropriate. The HyTrust Appliance is not a physical piece of hardware; it is a VMware vSphere*-compatible virtual appliance deployed alongside the rest of the virtual infrastructure. The HyTrust Appliance uses the vSphere APIs to build out the functionality and the integrated verifier that measures the base software components of the servers, and also possible tampering of the hypervisor image, by comparing the measurement data provided by Intel TXT through vSphere APIs with expected known-good values. Finally, it provides direct sharing of trust and security information with McAfee ePO.
- **Security management solution supported by McAfee.** McAfee ePO unifies security management through an open platform, simplifies risk and compliance management, and provides security intelligence across endpoints, networks, data, and compliance solutions. It helps to manage security, streamline and automate compliance processes, and increase overall visibility across security management activities. McAfee with HyTrust ePO extensions enables communication with the HyTrust Appliance.



Trust Status Dash Board

Host Name		Location	BIOS Trust Status	VMM Trust Status	Overall Trust Status	Updated On		Trust Status	Trust Assertion	Trust Report	Status
192.168.2.23	vmware		✓	✓	✓	Tue Dec 11 22:34:36 PST 2012	Refresh	●	▯		Host Trust status updated successfully.
192.168.2.22	vmware		?	?	?	Tue Dec 11 22:12:31 PST 2012	Refresh	●	▯		VMWare - Host '192.168.2.22' does not support TXT
192.168.2.21	vmware		✓	✓	✓	Tue Dec 11 22:34:40 PST 2012	Refresh	●	▯		Host Trust status updated successfully.

Figure 8. Trust Status Dashboard Indicating Two Trusted and One Untrusted Host

Measured Boot for Cisco UCS Systems: Platform Attestation

The PoC used the Cisco UCS M3 blade server, which is a cornerstone for TWSE's cloud computing infrastructure. As noted, the Cisco UCS blade systems are fully Intel TXT-enabled and can establish and provide attestation of the integrity and trust of the server and platforms.

Optionally, the TPM provides facilities for providing the trust status to external entities such as management tools, security apps, etc. As discussed, the process of establishing the integrity of the platform is called remote attestation. By providing evidence of the hardware and software configuration of a platform to an authorized remote party, remote attestation allows the remote party to establish trust on an Intel TXT-enabled platform. For the PoC, the team disabled Intel TXT on one of the Cisco UCS blades to highlight this differentiation and control capability. A step-by-step summary of how to enable Intel TXT on a Cisco UCS server is included in Appendix A.

Although all of the Cisco blades used in this PoC are fully Intel TXT-capable, it was important to have a contrast of trusted and untrusted servers to differentiate our trusted pools and prove the controls and status reporting mechanisms. For this reason, the team disabled Intel TXT in the system BIOS configuration settings in one of the Cisco UCS blades to prohibit the system from executing a trusted launch. For the PoC, the team used a prerelease version of the HyTrust Appliance that fully integrates remote attestation capabilities. As shown in Figure 8, the trust status dashboard of the HyTrust Appliance shows an unknown BIOS trust status, unknown VMM status, and overall unknown status for the second Cisco UCS blade, on which the team had consciously disabled the Intel TXT support.

For virtualization, the team used VMware vCenter Server 5.1 running on VMware ESXi 5.1, which provides full support and functionality for Intel TXT. As discussed earlier, Intel TXT enables platform measurements to detect possible malicious changes to BIOS and other critical base software components of the servers. When executed on an Intel TXT-enabled system, VMware ESXi measures the critical components of the hypervisor stack when the system boots and stores these measurements in the PCR of the TPM on the platform. The measured elements include the VMkernel, kernel modules, drivers, native management applications that run on ESXi, and any boot-time configuration options.

The next critical component of the PoC architecture is the HyTrust Appliance, which provides extensive support for Intel TXT and also includes the robust policy control functionality for this use case. It essentially establishes the parameters and policies that define the TCP.

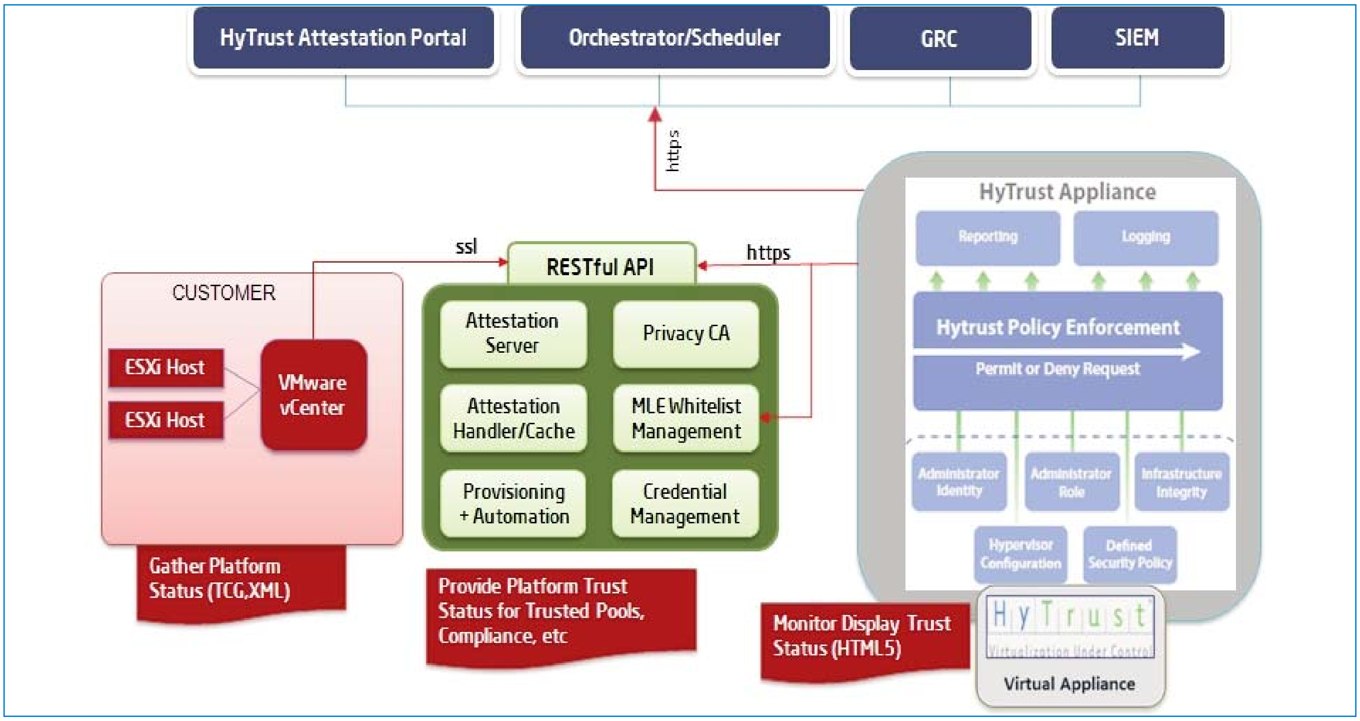
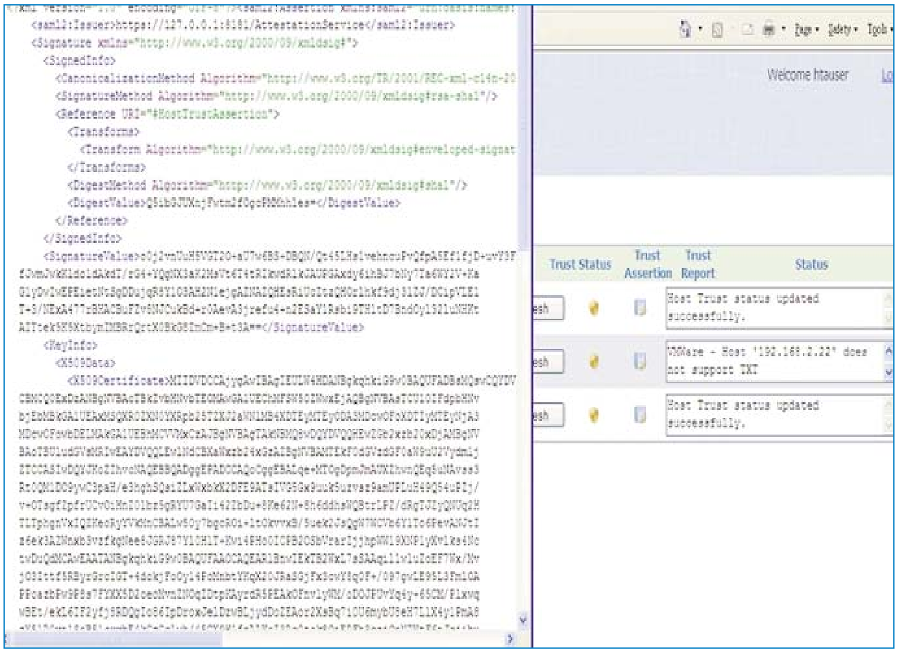


Figure 9. HyTrust Appliance with Remote Trust Attestation Architecture

As shown in Figure 9, the HyTrust Appliance manages:

- **Critical platform attestation** functionality
- **Whitelisting** of known good measurements
- **Trust operation and report dashboards** for TCPs
- **A broad set** of other virtualization security controls for workloads, servers, and administrators

Ensuring security and access control installation of any software—including the HyTrust Appliance and all other solutions—requires authentication and access approval. The HyTrust Appliance and solutions were used to detect, measure, and report the trust of both the server platforms and the hypervisor and to implement workload controls (e.g., VM migration) based on required platform trust attributes.



```
<?xml version="1.0" encoding="UTF-8"?><saml2:Assertion xmlns:saml2="urn:oasis:names:
  <saml2:Issuer>https://127.0.0.1:8181/AttestationService</saml2:Issuer>
  <Signature xmlns="http://www.w3.org/2000/09/xmldsig#">
    <SignedInfo>
      <CanonicalizationMethod Algorithm="http://www.w3.org/TR/2001/REC-xml-c14n-20
      <SignatureMethod Algorithm="http://www.w3.org/2000/09/xmldsig#rsa-sha1"/>
      <Reference URI="#HostTrustAssertion">
        <Transforms>
          <Transform Algorithm="http://www.w3.org/2000/09/xmldsig#enveloped-signat
        </Transforms>
        <DigestMethod Algorithm="http://www.w3.org/2000/09/xmldsig#sha1"/>
        <DigestValue>Q5ibGJUXnjFvtm2f0goPMMhhles=</DigestValue>
      </Reference>
    </SignedInfo>
    <SignatureValue>o0j2vnUuH5VGT20+aU7v6B3-DBQN/Qt45LHslvehncuPvQfpA5Ef1fjD+uvY3F
fOvmJvkKldoldAkdT/rG4+YQgNX3aK2MaVt6T4tRIkwdRlkGAURGAxdy6ihBJ7bNy7Ta6WY2V+Ka
GlyDvIvEFEietNtSgDDujqR8Y1O3AH2NlejgAZNAIQHEsRiUsItzQH0rlhKf3dj3l2J/DCipVLE1
T-3/NExA477rBHACBuFZv6NJCuKBd-r0AevA3jrefu4-n2E3aY1Rsbi9TH1tD7Bnd0y1321uNHKt
AITtek5K5XtbymIMBRrQrtX0BkG8ImCm+B+t3A==</SignatureValue>
    <KeyInfo>
      <X509Data>
        <X509Certificate>MIIDVDCCAjygAwIBAgIEULN4HDANBgkqhkiG9w0BAQUFADBsMQswCQYDV
CBMCQ0ExDzANBgNVBAcTBkZvbHNvbTEOMAwGA1UEChMFSW50ZWwxEjAQBgNVBAsTCU1OIFdpbXNv
bjEbMBkGA1UEAxMSQXR0ZXN0YXRpb25TZXJ2aWNlMB4XDTEyMTEyODA3MDcwOFoXDTIyMTEyNjA3
[illegible]
```

	Trust Status	Trust Assertion	Trust Report	Status
esh				Host Trust status updated successfully.
esh				VMWare - Host '192.168.2.22' does not support TXT
esh				Host Trust status updated successfully.

Figure 10. Trust Attestation Service: Trust Report View

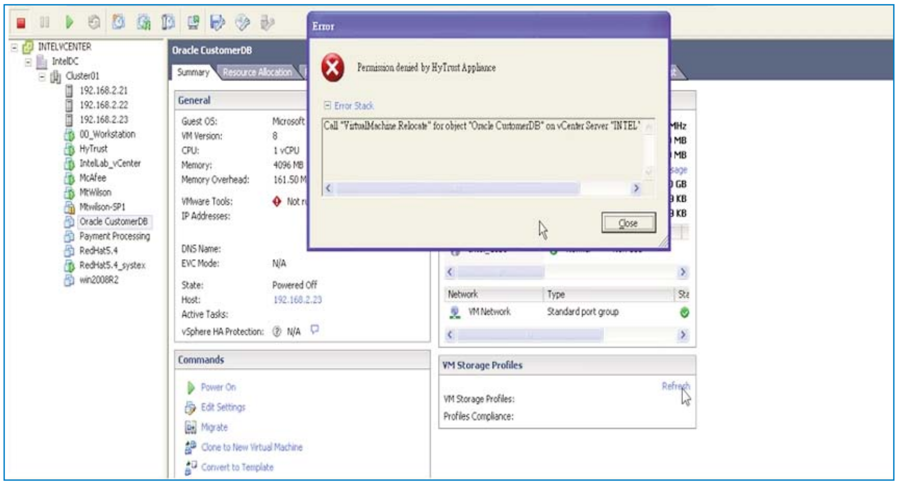
The team used the HyTrust Appliance to execute the remote attestation process to gather trust data. The results of the platform attestation are represented in the HyTrust Appliance trust status dashboard. As described in the previous section, the remote attestation process provides an independent evaluation of the integrity measurements of the firmware, BIOS, and VMM against known-good (whitelist) and securely makes that assertion available to the HyTrust Appliance policy enforcement and reporting components. The evaluation of the measurements is comprehensive and covers:

- **The core** of the BIOS
- **The BIOS** configurations
- **The VMM** kernel
- **Various VMM modules** that are loaded as part of the VMware ESXi launch

Figure 10 shows a snapshot of the actual measurements of an ESXi server and the whitelist values. Finally, McAfee ePO unifies security management through an open platform and simplifies risk and compliance management. Dashboards provide security intelligence across endpoints, networks, data, and compliance solutions. It helps to manage security, streamline and automate compliance processes, and increase overall visibility across security management activities. This is the final component needed to meet the security management objectives of the PoC and the business needs of TWSE.

Creating TCPs and Workload Migration

The robust software and functionality of the HyTrust Appliance enabled the team to securely measure trust for both the Cisco UCS server platforms and the VMware ESXi (hypervisor). The ability to measure the hypervisor software at boot time and store these measurements in the TPM proved the trustworthiness of the servers, using the integrated hardware root of trust and Intel TXT to complete the verification of the BIOS and VMM.



Oracle CustomerDB

General

Guest OS: Microsoft
VM Version: 8
CPU: 1 vCPU
Memory: 4096 MB
Memory Overhead: 161.50 M
VMware Tools: Not r
IP Addresses:
DNS Name:
EVC Mode: N/A
State: Powered Off
Host: 192.168.2.23
Active Tasks:
vSphere HA Protection: N/A

Network	Type	Sta
VM Network	Standard port group	✓

VM Storage Profiles

VM Storage Profiles:
Profiles Compliance:

Error

Permission denied by HyTrust Appliance

Error Stack

Call "VirtualMachine.Relocate" for object "Oracle CustomerDB" on vCenter Server "INTEL"

Figure 11. Displaying the Denied Migration Response for Trust Policy Violation

The PoC team took a systematic approach to test each aspect of the TCP use cases. Knowing the trust status of both the servers and hypervisors enabled the team to highlight to TWSE the platform trust information and then define a full and appropriate set of operational policies and controls. The team applied HyTrust Appliance, which provided tight integration with VMware vSphere and McAfee ePO. This made it possible to fully demonstrate the operational details of the TCPs use cases:

- **Creation** of TCPs
- **Workload placement** in the TCPs
- **Workload migration** in the TCPs
- **Integration** with McAfee ePO

The robust functionality of HyTrust Appliance enables the team to:

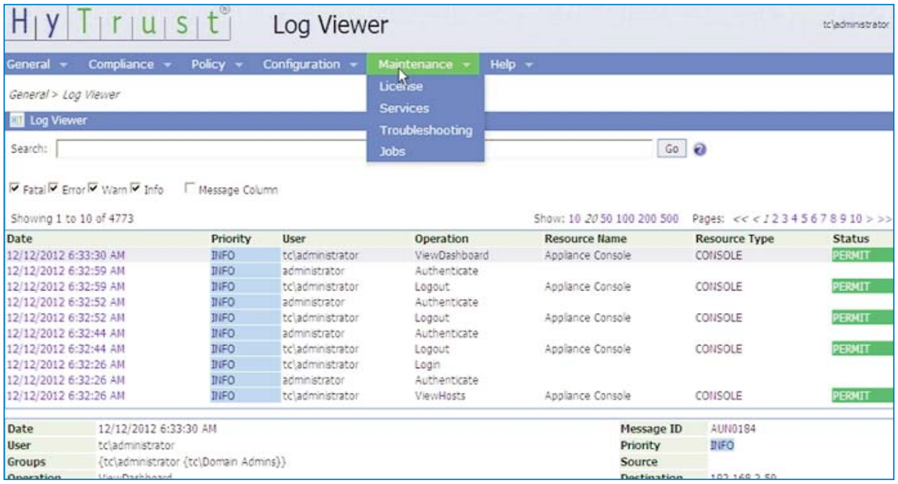
- **Intercept** all administrative requests for the virtual infrastructure
- **Determine** whether the request was in accordance with defined policy
- **Permit or deny** the request
- **Record** all administrative access and change requests

To apply effective end-to-end trust policies for the cloud infrastructure, the team:

- **Created TCPs** with Intel TXT
- **Identified and labeled** the sensitive workloads that required protection
- **Configured trust policies** to establish trust requirements
- **Assigned and managed** workload migration based on defined trust polices
- **Enforced** trust policies end-to-end
- **Recorded all activities**, including audit and compliance, and provide reporting

HyTrust automatically assigns the applicable trust status to compute servers and then ensures the separation between trusted and untrusted pools by continuously enforcing policies that identify the trust status.

HyTrust Appliance assigns and manages workload migration based on the defined trust polices, checking to see if the predefined trust and operational policies are met before it allows workload migration. Besides displaying the denial information (Figure 11) to allow the request onto an untrusted system, it is critical to point out HyTrust Appliance also applied enforcement policy and did not allow the workload to be migrated due to the established trust security policy. All requests and actions were recorded for future policy reviews, audits, and reporting.

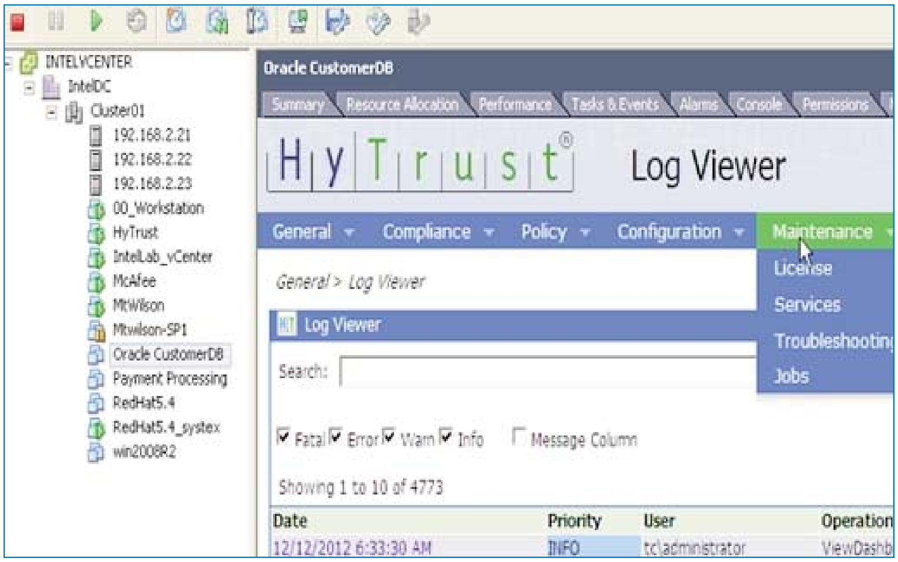


Showing 1 to 10 of 4773

Date	Priority	User	Operation	Resource Name	Resource Type	Status
12/12/2012 6:33:30 AM	INFO	tc\administrator	ViewDashboard	Appliance Console	CONSOLE	PERMIT
12/12/2012 6:32:59 AM	INFO	administrator	Authenticate			
12/12/2012 6:32:59 AM	INFO	tc\administrator	Logout	Appliance Console	CONSOLE	PERMIT
12/12/2012 6:32:52 AM	INFO	administrator	Authenticate			
12/12/2012 6:32:52 AM	INFO	tc\administrator	Logout	Appliance Console	CONSOLE	PERMIT
12/12/2012 6:32:44 AM	INFO	administrator	Authenticate			
12/12/2012 6:32:44 AM	INFO	tc\administrator	Logout	Appliance Console	CONSOLE	PERMIT
12/12/2012 6:32:26 AM	INFO	tc\administrator	Login			
12/12/2012 6:32:26 AM	INFO	administrator	Authenticate			
12/12/2012 6:32:26 AM	INFO	tc\administrator	ViewHosts	Appliance Console	CONSOLE	PERMIT

Date	12/12/2012 6:33:30 AM	Message ID	AUN0184
User	tc\administrator	Priority	INFO
Groups	{tc\administrator {tc\Domain Admins}}	Source	

Figure 12. HyTrust Appliance Log Viewer in the vCenter Plug-in



Showing 1 to 10 of 4773

Date	Priority	User	Operation
12/12/2012 6:33:30 AM	INFO	tc\administrator	ViewDashb

Figure 13. McAfee ePO with Host Trust Status indicated by HyTrust Appliance ePO Extension

For the end-to-end enforcement of trust policies—including reporting, audit, and compliance—the team examined an array of functional scenarios. It reviewed functionality including assigning and managing policies, access level privileges to enable role-based access, hypervisor and guest container hardening templates, and policy resources. It also migrated workloads of both trusted and untrusted compute systems (according to policies) and pools including extending security for overall password control, with use of strong authentication and root password vaulting.

It is important to note that the HyTrust Appliance is integrated with VMware vCenter Server by using the open, plug-in architecture; however, the console for the HyTrust Appliance provides a significantly more detailed set of information for overall policy reporting, auditing, and overall compliance and management functionality. As an example, Figure 12 shows the HyTrust Appliance log viewer, including specific details related to administrator activity.

Integrated and Extended Security and Platform Trust with McAfee ePO

To address TWSE's requirements for overall policy, broader overall trust, security management, and detailed reporting of its cloud infrastructure, the team used the HyTrust Appliance, which provides extended trust information and enables direct support and reporting with the leading security information and event management (SIEM) and governance, risk management, and compliance (GRC) solutions.

The PoC used the HyTrust Appliance to extend and integrate trust information for each hypervisor and the virtualized resource functionality to the McAfee ePO console. This provided TWSE with another common and aggregated management view for its cloud infrastructure.

The direct integration of the HyTrust Appliance dashboard shows users the Intel TXT trust status of the host on which each VM is running. The HyTrust Appliance assesses compliance by comparing a host's current configuration with a hardening configuration template that was customized based on TWSE requirements to meet particular regulation requirements for control. It then provides assessment data into the master McAfee ePO dashboard for reporting and analysis. HyTrust Appliance gives McAfee ePO a record of all administrative activities, including a unique user ID and operations attempted by the privileged user, including denied or failed attempts. Figures 13 through 15 show the HyTrust Appliance integration with McAfee ePO.

McAfee ePO's flexible automation capability streamlines workflows, dramatically reducing the cost and complexity of security and compliance administration.

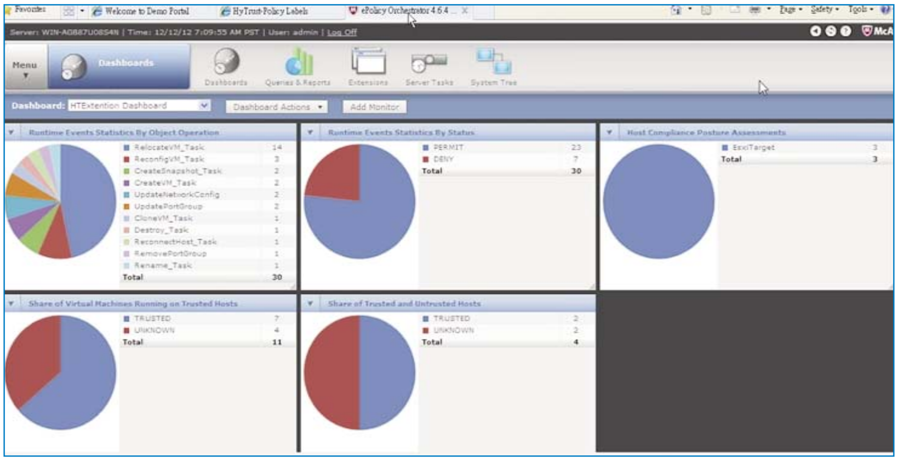
Summary

The PoC completed by a team from TWSE, Systex, Intel, HyTrust, McAfee, VMware, and Cisco successfully highlighted TCP use cases including integrated trust solutions and trust-aware, policy-driven functionality, which are an important foundation for enhanced cloud security. The outcome of the PoC helped TWSE to gain confidence that such an implementation could help it:

- **Address** its requirements
- **Increase** visibility
- **Gain** efficiencies
- **Strengthen** protection
- **Significantly** increase overall trust

McAfee ePO's flexible automation capability streamlines workflows, dramatically reducing the cost and complexity of security and compliance administration.

The PoC team took a systematic approach to design, implement, and test each aspect of a set of capabilities that began with establishing and verifying platform integrity and evolving through incremental TCP use cases. Establishing the trust status of both the servers and hypervisors gave the TWSE team new visibility into the status of the host platforms in the cloud. It was then able to define and implement a new set of appropriate operational policies and controls. The implementation allowed for:



Runtime Events Statistics By Object Operation

■ RelocateVM_Task	14
■ ReconfigVM_Task	3
■ CreateSnapshot_Task	2
■ CreateVM_Task	2
■ UpdateNetworkConfig	2
■ UpdatePortGroup	2
■ CloneVM_Task	1
■ Destroy_Task	1
■ ReconnectHost_Task	1
■ RemovePortGroup	1
■ Rename_Task	1
Total	30

Runtime Events Statistics By Status

■ PERMIT	23
■ DENY	7
Total	30

Host Compliance Posture Assessments

■ EsxiTarget	3
Total	3

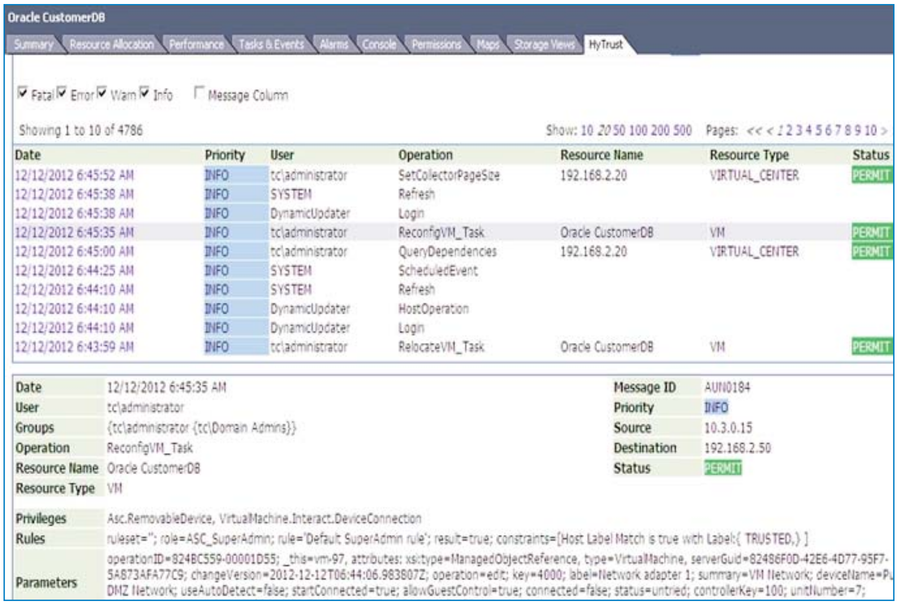
Share of Virtual Machines Running on Trusted Hosts

■ TRUSTED	7
■ UNKNOWN	4
Total	11

Share of Trusted and Untrusted Hosts

■ TRUSTED	2
■ UNKNOWN	2
Total	4

Figure 14. McAfee ePO Displaying Administrator Activity and Trust Status Captured by HyTrust Appliance



☑ Fatal ☑ Error ☑ Warn ☑ Info ☐ Message Column

Showing 1 to 10 of 4786 Show: 10 20 50 100 200 500 Pages: << < 1 2 3 4 5 6 7 8 9 10 >

Date	Priority	User	Operation	Resource Name	Resource Type	Status
12/12/2012 6:45:52 AM	INFO	tc\administrator	SetCollectorPageSize	192.168.2.20	VIRTUAL_CENTER	PERMIT
12/12/2012 6:45:38 AM	INFO	SYSTEM	Refresh			
12/12/2012 6:45:38 AM	INFO	DynamicUpdater	Login			
12/12/2012 6:45:35 AM	INFO	tc\administrator	ReconfigVM_Task	Oracle CustomerDB	VM	PERMIT
12/12/2012 6:45:00 AM	INFO	tc\administrator	QueryDependencies	192.168.2.20	VIRTUAL_CENTER	PERMIT
12/12/2012 6:44:25 AM	INFO	SYSTEM	ScheduledEvent			
12/12/2012 6:44:10 AM	INFO	SYSTEM	Refresh			
12/12/2012 6:44:10 AM	INFO	DynamicUpdater	HostOperation			
12/12/2012 6:44:10 AM	INFO	DynamicUpdater	Login			
12/12/2012 6:43:59 AM	INFO	tc\administrator	RelocateVM_Task	Oracle CustomerDB	VM	PERMIT

Date	12/12/2012 6:45:35 AM	Message ID	AUN0184
User	tc\administrator	Priority	INFO
Groups	{tc\administrator {tc\Domain Admins}}	Source	10.3.0.15
Operation	ReconfigVM_Task	Destination	192.168.2.50
Resource Name	Oracle CustomerDB	Status	PERMIT
Resource Type	VM		
Privileges	Asc.RemovableDevice, VirtualMachine.Interact.DeviceConnection		
Rules	ruleset=''; role=ASC_SuperAdmin; rule='Default SuperAdmin rule'; result=true; constraints=[Host Label Match is true with Label:{ TRUSTED,}]		
Parameters	operationID=824BC559-00001D55; _this=vm-97, attributes: xsi:type=ManagedObjectReference, type=VirtualMachine, serverGuid=82486F0D-42E6-4D77-95F7-5A873AFA77C9; changeVersion=2012-12-12T06:44:06.983807Z; operation=edit; key=4000; label=Network adapter 1; summary=VM Network; deviceName=Pu DMZ Network; useAutoDetect=false; startConnected=true; allowGuestControl=true; connected=false; status=untried; controllerKey=100; unitNumber=7;		

Figure 15. McAfee ePO Displaying Drill-Down of Administrator Activity Chart

- **Creation of TCPs** to segregate high-integrity servers from those with unknown integrity properties
- **Workload identification** and policy-based placement of sensitive workloads in the TCPs
- **Controlled workload migration** with sensitive workloads maintained within the TCPs
- **Integration with McAfee ePO** to provide a consolidated management view of security controls and events

The PoC successfully demonstrated a fully operational, fabric-based Cisco UCS M3 server secured with a hardware root of trust enabled by the Intel TXT feature available in Intel Xeon processors. VMware vSphere 5.1 and VMware ESXi 5.1 provided a crucial foundation and base functionality for Intel's hardware root of trust security capabilities and Intel TXT.

The built-in capabilities in vSphere 5.1 can also increase performance and streamline antivirus and antimalware deployment. Policy-based solutions from HyTrust will enable organizations to address and account for the trust of systems and apply effective, comprehensive, automated policies to manage the provisioning, deployment, and movement of workloads.

HyTrust Appliance provided robust functionality and capabilities that addressed TWSE's overall trust and security requirements. The extended functionality provides, in a secure way, direct and integrated support with VMware vSphere and leading GRC, SIEM, and McAfee ePO solutions.

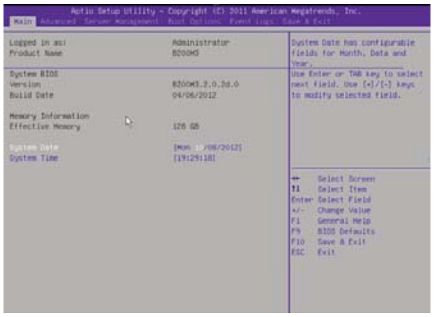
As it considers how to build out its cloud infrastructure to meet evolving business needs, TWSE has demonstrated with this PoC that a hardware-assisted, trust-enabled infrastructure can provide powerful new capabilities and controls to address security concerns with the cloud. Other businesses and organizations will be able to benefit from Intel TXT-enabled systems and integrated solutions such as TCPs that enable businesses to address their critical business requirements by providing greater overall trust and support for security, policy enforcement, reporting, compliance management, and audits.

In response to the learnings from this PoC, and to address growing demands and mandates form end users and government entities for increased security controls for cloud deployments, cloud providers and software vendors, along with a growing ecosystem of technology vendors, are collaborating to develop systems, software, and interoperable solutions to support deployment and enablement of trusted computing infrastructure. The goal of this emerging infrastructure is to provide greater visibility, control, and compliance capabilities for the cloud, with a strong, bottom-up security posture based on hardware and complemented by new, extensible software solutions.

Find the solution that's right for your organization. Contact your Intel representative, visit Intel's Business Success Stories for IT Managers (www.intel.com/Itcasestudies), or explore the Intel.com IT Center (www.intel.com/itcenter). Learn more about Intel TXT at www.intel.com/txt.

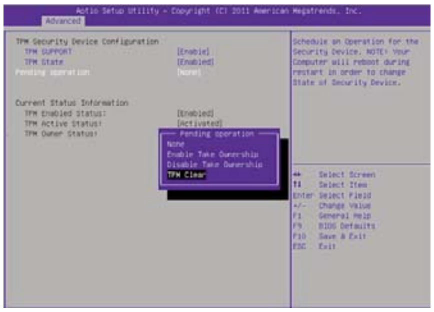
Appendix A: Overview of Steps for Intel TXT and TPM Configuration for Cisco UCS Systems

Below are primary steps to manually provision Intel TXT in the BIOS and establish the appropriate TPM configuration of a Cisco UCS blade server. Please note, if this is a new Cisco blade server being deployed, you do not have to clear TPM ownership. Please go directly to Step 5. Once systems are configured and Intel TXT is enabled on a Cisco UCS blade server, you are ready to install a trusted hypervisor or operating system kernel to establish a server configuration that is rooted in hardware trust.



```
Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.
Main  Advanced  Server Management  Boot Options  Event Logs  Save & Exit

Logged in as:            Administrator        System Date has configurable
Product Name             B200M3               fields for Month, Data and
                                              Year.
System BIOS                                   Use Enter or TAB key to select
Version                  B200M3.2.0.3d.0      next field. Use [+]/[-] keys
Build Date               04/06/2012           to modify selected field.

Memory Information
Effective Memory         128 GB

System Date              [Mon 10/08/2012]
System Time              [19:29:18]
                                              ↔     Select Screen
                                              ↑↓    Select Item
                                              Enter Select Field
                                              +/-   Change Value
                                              F1    General Help
                                              F9    BIOS Defaults
                                              F10   Save & Exit
                                              ESC   Exit
```

Step 1: F2 to Enter BIOS



```
Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.
     Advanced

TPM Security Device Configuration             Schedule an Operation for the
  TPM SUPPORT              [Enable]           Security Device. NOTE: Your
  TPM State                [Enabled]          Computer will reboot during
Pending operation          [None]             restart in order to change
                                              State of Security Device.
Current Status Information
  TPM Enabled Status:      [Enabled]
  TPM Active Status:       [Activated]
  TPM Owner Status:    ── Pending operation ──
                       None
                       Enable Take Ownership
                       Disable Take Ownership
                       TPM Clear
                                              ↔     Select Screen
                                              ↑↓    Select Item
                                              Enter Select Field
                                              +/-   Change Value
                                              F1    General Help
                                              F9    BIOS Defaults
                                              F10   Save & Exit
                                              ESC   Exit
```

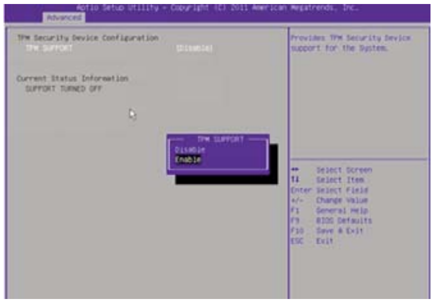
Step 2: Advanced > Trusted Computing > Pending Operation > TPM Clear

Step 3: F10 Save and Exit

Step 4: F2 to enter BIOS

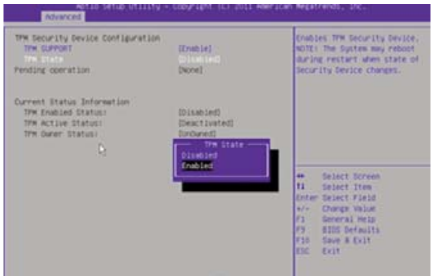
Step 5: Advanced > Trusted Computing > TPM Support > Enable

Step 6: F10 Save and Exit



```
Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.
     Advanced

TPM Security Device Configuration             Provides TPM Security Device
  TPM SUPPORT              [Disable]          support for the System.

Current Status Information
  SUPPORT TURNED OFF

                       ── TPM SUPPORT ──
                       Disable
                       Enable
                                              ↔     Select Screen
                                              ↑↓    Select Item
                                              Enter Select Field
                                              +/-   Change Value
                                              F1    General Help
                                              F9    BIOS Defaults
                                              F10   Save & Exit
                                              ESC   Exit
```

Step 7: F2 to enter BIOS

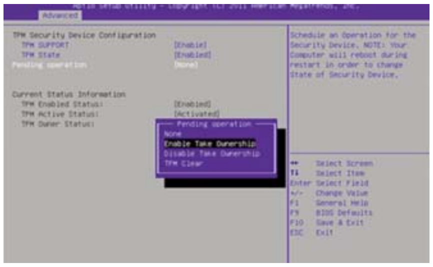


```
Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.
     Advanced

TPM Security Device Configuration             Enables TPM Security Device.
  TPM SUPPORT              [Enable]           NOTE: The System may reboot
  TPM State                [Disabled]         during restart when state of
Pending operation          [None]             Security Device changes.

Current Status Information
  TPM Enabled Status:      [Disabled]
  TPM Active Status:       [Deactivated]
  TPM Owner Status:        [UnOwned]
                       ── TPM State ──
                       Disabled
                       Enabled
                                              ↔     Select Screen
                                              ↑↓    Select Item
                                              Enter Select Field
                                              +/-   Change Value
                                              F1    General Help
                                              F9    BIOS Defaults
                                              F10   Save & Exit
                                              ESC   Exit
```

Step 8: Advanced > Trusted Computing > TPM State > Enable

Step 9: F10 Save and Exit

Step 10: F2 to enter BIOS



```
Aptio Setup Utility - Copyright (C) 2011 American Megatrends, Inc.
     Advanced

TPM Security Device Configuration             Schedule an Operation for the
  TPM SUPPORT              [Enable]           Security Device. NOTE: Your
  TPM State                [Enabled]          Computer will reboot during
Pending operation          [None]             restart in order to change
                                              State of Security Device.
Current Status Information
  TPM Enabled Status:      [Enabled]
  TPM Active Status:       [Activated]
  TPM Owner Status:    ── Pending operation ──
                       None
                       Enable Take Ownership
                       Disable Take Ownership
                       TPM Clear
                                              ↔     Select Screen
                                              ↑↓    Select Item
                                              Enter Select Field
                                              +/-   Change Value
                                              F1    General Help
                                              F9    BIOS Defaults
                                              F10   Save & Exit
                                              ESC   Exit
```

Step 11: Advanced > Trusted Computing > Pending Operation > Enable Take

Step 12: Advanced > Intel TXT (LT-SX) Configuration

Step 13: F10 Save and Exit

Appendix B: VMware Software Solutions

VMware delivers a comprehensive set of customer-proven solutions that help IT organizations better manage virtual environments while protecting critical data and workloads:

- **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 work flows, 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 vShield Zones** allow 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.

Appendix C: McAfee ePO

The solution provides end-to-end visibility through a unified view of your security posture. Drillable, drag-and-drop dashboards provide security intelligence across endpoints, data, mobile, and networks for immediate insight and faster response times. Simplified security operations help streamline workflows for proven efficiencies. Benefits include:

- **End-to-end visibility.** Get a unified view of your security posture. Drillable, drag-and-drop dashboards provide security intelligence across endpoints, data, mobile, and networks for immediate insight and faster response times.
- **Simplified security operations.** Streamline workflows for proven efficiencies. Independent studies show ePO software helps organizations of every size streamline administrative tasks, ease audit fatigue, and reduce security management-related hardware costs.
- **An open, extensible architecture.** Use your existing IT infrastructure. McAfee ePO software connects management of both McAfee and third-party security solutions to your LDAP, IT operations, and configuration management tools.

Appendix D: HyTrust Appliance

The HyTrust Appliance is a virtual appliance. VMware vSphere-compatible, it sits between the administrators of the virtual infrastructure—the virtualization administrators, the network administrators, the application owners—and the virtual infrastructure itself, in the management network.

HyTrust Appliance can verify the integrity of the physical hardware and hypervisor of the host to ensure that the platform is fully trusted. It provides the ability to label virtual machines, as well as other virtual resources, and then apply policies to those labels. Combined with hardware root-of-trust, HyTrust Appliance provides the ability to verify the trust of the hardware and hypervisor layer using Intel TXT and ensures total platform integrity of the virtual platform.

Figure D1 shows the HyTrust Appliance inline deployment.

The HyTrust Appliance has a robust array of extended functionality that addresses the overall TWSE business requirements and makes it possible for TWSE to apply trust policies and security operations for its cloud infrastructure.

Besides highlighting the use cases, the team also showcased how hardware-based security enabled with the HyTrust Appliance delivers extended capabilities including:

- **Verifying platform integrity** is trusted via Intel TXT
- **Ensuring the hypervisor is hardened** and the virtual infrastructure is trusted via Intel TXT
- **Enforcing consistent administrative access** and authorization policies covering all access methods
- **Providing granular**, user-specific, audit-quality logs of all administrative access
- **Enabling strong**, multi-factor authentication
- **Securing privileged** user access of the hypervisor through root password vaulting

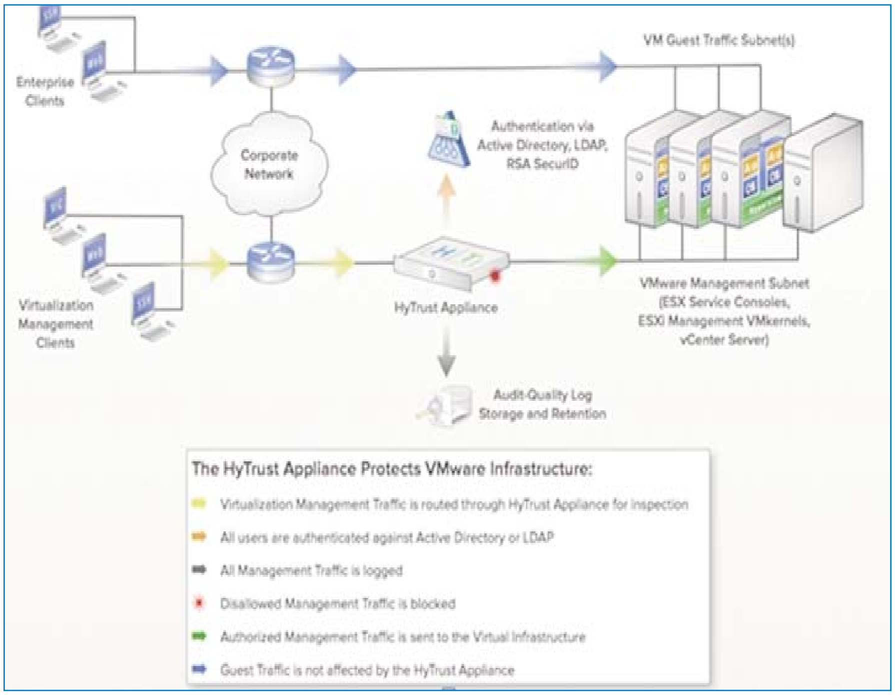

VM Guest Traffic Subnet(s)
Enterprise Clients
Corporate Network
Authentication via Active Directory, LDAP, RSA SecurID
Virtualization Management Clients
HyTrust Appliance
VMware Management Subnet (ESX Service Consoles, ESXi Management VMkernels, vCenter Server)
Audit-Quality Log Storage and Retention
The HyTrust Appliance Protects VMware Infrastructure:
Virtualization Management Traffic is routed through HyTrust Appliance for inspection
All users are authenticated against Active Directory or LDAP
All Management Traffic is logged
Disallowed Management Traffic is blocked
Authorized Management Traffic is sent to the Virtual Infrastructure
Guest Traffic is not affected by the HyTrust Appliance

Figure D1. HyTrust (Virtual) Appliance Inline Deployment

- **Enabling additional oversight** for highly sensitive operations via secondary approval
- **Enforcing infrastructure segregation** for trusted compute pools and multi-tenancy use-cases

With the HyTrust Appliance, there are no anonymous changes to the virtual infrastructure. All administrative access must first be authenticated, supporting two-factor authentication. Access to the entire environment may be tied back to a specific individual—a critical requirement in security and compliance-conscious data centers. As the central authority over all change requests, the HyTrust Appliance provides granular, user-specific log records that can be used for regulatory compliance, troubleshooting, and forensic analysis. It offers an unprecedented level of visibility into the state of the virtual infrastructure.

The HyTrust Appliance records all requests, which are critical for security purposes. Every request is tied to the identity of a specific user and all relevant information is collected. With total visibility from HyTrust, organizations can accomplish their audits and rely on their logs for forensics if needed.

Learn more at www.hytrust.com.

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-compatible measured launched environment (MLE). Intel TXT also requires the system to contain a TPM v1.s. For more information, visit http://www.intel.com/technology/security

Software and workloads used in performance tests may have been optimized for performance only on Intel microprocessors. Performance tests, such as SYSmark and MobileMark, are measured using specific computer systems, components, software, operations and functions. Any change to any of those factors may cause the results to vary. You should consult other information and performance tests to assist you in fully evaluating your contemplated purchases, including the performance of that product when combined with other products.

Results have been estimated based on internal Intel analysis and are provided for informational purposes only. Any difference in system hardware or software design or configuration may affect actual performance.

Intel does not control or audit the design or implementation of third-party benchmark data or Web sites referenced in this document. Intel encourages all of its customers to visit the referenced Web sites or others where similar performance benchmark data are reported and confirm whether the referenced benchmark data are accurate and reflect performance of systems available for purchase.

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.htm

0213/MG/SS