TRUSTED WORKLOAD MIGRATION WITH EMC, RSA, INTEL, AND HYTRUST

- Nondisruptive trusted workload migration between data centers
- Active enforcement of hardware-level security policy compliance
- Enhanced logging and auditing capabilities for hardware-level security

EMC Solutions Group

Abstract

This white paper presents a solution jointly developed by EMC, RSA, Intel, and HyTrust for trusted workload migration with active security policy enforcement. EMC® VPLEX®, Intel Trusted Execution Technology, RSA Archer, and HyTrust Appliance are used to enhance service provider cloud environments.

May 2013
# Table of contents

**Executive summary** ................................................................. 5  
  Business case ................................................................................. 5  
  Solution overview ........................................................................ 5  
  Key results and recommendations ............................................... 6  

**Introduction** ............................................................................... 7  
  Purpose ......................................................................................... 7  
  Scope ............................................................................................ 7  
  Audience ....................................................................................... 7  
  Key technologies overview ........................................................ 7  

**Challenges in trusted workload migration** .................................... 9  
  VMware vMotion and Storage vMotion ......................................... 9  
  Security and integrity of hosts ..................................................... 9  

**EMC VPLEX storage solution** ...................................................... 11  
  New storage management challenges ........................................ 11  
  EMC VPLEX solution overview ............................................... 12  
  VPLEX family ............................................................................... 13  
  VPLEX Metro ............................................................................... 13  
  VPLEX Metro with VMware ....................................................... 14  

**Intel Trusted Execution Technology hardware security solution** ........ 15  
  Infrastructure security challenges ............................................. 15  
  Hardware security ........................................................................ 15  
  Intel TXT solution ......................................................................... 15  
  Intel TXT features ......................................................................... 16  
  Summary ....................................................................................... 17  

**HyTrust Appliance security policy enforcement solution** ................. 18  
  Security policy enforcement challenges ...................................... 18  
  HyTrust solution .......................................................................... 18  
  Features ........................................................................................ 18  

**RSA Archer Cloud Security and Compliance solution** ....................... 21  
  Security management and compliance challenges ....................... 21  
  RSA Archer Cloud Security and Compliance solution .................. 21  
  Architecture ................................................................................ 22  
  RSA Cloud Security and Compliance with Intel TXT .................... 22
<table>
<thead>
<tr>
<th>Chapter</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overall solution architecture for secure workload migration</td>
<td>24</td>
</tr>
<tr>
<td>Review of key components</td>
<td>24</td>
</tr>
<tr>
<td>High-level architecture</td>
<td>25</td>
</tr>
<tr>
<td>Setting up the hosts</td>
<td>25</td>
</tr>
<tr>
<td>Implementing the components</td>
<td>26</td>
</tr>
<tr>
<td>Enabling and using Intel TXT</td>
<td>26</td>
</tr>
<tr>
<td>Implementing HyTrust Appliance</td>
<td>27</td>
</tr>
<tr>
<td>Implementing RSA Archer</td>
<td>27</td>
</tr>
<tr>
<td>Use case demonstrations</td>
<td>28</td>
</tr>
<tr>
<td>Viewing Intel TXT trust status</td>
<td>28</td>
</tr>
<tr>
<td>Reporting on trust status in RSA Archer</td>
<td>29</td>
</tr>
<tr>
<td>Actively blocking virtual machine migration to an untrusted host</td>
<td>30</td>
</tr>
<tr>
<td>Enforcement actions from HyTrust displayed in RSA Archer</td>
<td>31</td>
</tr>
<tr>
<td>Conclusion</td>
<td>33</td>
</tr>
<tr>
<td>Summary</td>
<td>33</td>
</tr>
<tr>
<td>Findings</td>
<td>33</td>
</tr>
<tr>
<td>References</td>
<td>34</td>
</tr>
<tr>
<td>White papers</td>
<td>34</td>
</tr>
<tr>
<td>Other documentation</td>
<td>34</td>
</tr>
</tbody>
</table>
Executive summary

Business case

Enterprises and service providers are dealing with the challenges and risks inherent in moving their workloads from legacy IT infrastructures to cloud environments and, ultimately, to cloud environments located in geographically diverse data centers.

Enterprises can benefit from moving their application workloads from one of their data centers to another or to a service provider’s data center. To ensure against downtime, they could also run the same application across multiple active/active data centers.

Service providers who have the option of migrating workloads for their internal systems between data centers can more efficiently avoid or recover from disaster. They might want to offer their customers seamless migration of their applications between the customer’s data center and their own or among the service provider’s data centers. They can also benefit from the ultimate scalability that comes with being able to grow their cloud infrastructure, not only within the walls of one data center, but to expand their cloud environment across multiple facilities with environments that are active at the same time.

Regardless of the need, the challenge lies in how to transfer those workloads in a nondisruptive fashion to avoid downtime for applications and end users, and to do so in a secure way that attests to the integrity of the underlying infrastructure running the virtual machines.

Solution overview

This white paper discusses the security and logistical challenges encountered by enterprises and service providers who are faced with application workload migration between data centers. It provides an overview of a solution jointly developed by EMC, RSA, Intel, and HyTrust that enables trusted workload migration between data centers using technology available from those companies.

The solution demonstrates two virtualized, active/active, geographically separated data centers managed and administered by the same service provider. The cloud environments in both data centers are active and include virtualized servers and storage. The solution meets several key goals of a workload migration project, as follows:

- Demonstrates immediate nondisruptive workload migration within and between data centers
- Enables hardware root of trust for cloud hosts to validate that the hosts running the virtual machines have not been compromised by attacks (such as BIOS rootkit attacks that run beneath the hypervisor)
- Provides an example of active security policy enforcement using hardware security data collected from the cloud hosts
- Implements audit and reporting capabilities so an enterprise or service provider can pull real-time reports showing an overall view of its cloud host integrity status
While the solution environment showcases a specific configuration, it has many elements in common with other multisite data center environments. Service providers and enterprises running multiple data centers will find key elements that can be applied to their environments.

This white paper shows demonstrates the following:

- Using solutions available from EMC and VMware, workload migration can be accomplished in an immediate, nondisruptive, and secure method using the technologies described herein.

- Hardware security can be enabled using the technology built into Intel Xeon processors. This allows for hardware trust attestation and ensures that the environment running beneath the virtual machines has been validated and is running known good configurations of firmware and hypervisor.

- Active security policy enforcement can be accomplished using a solution from EMC partner HyTrust.

- Full audit and reporting capabilities for the cloud environment can be made available using solutions from RSA.
Introduction

Purpose
The purpose of this white paper is to demonstrate methods of facilitating secure workload migration within and between data centers using EMC® VPLEX®, while implementing hardware-based security using Intel Trusted Execution Technology (Intel TXT). This solution allows the active enforcement of security policies based on Intel TXT using HyTrust Appliance and provides further audit and reporting capabilities through RSA Archer.

We demonstrate how to set up migration policies for a set of virtual machines, while staying within the confines of trusted infrastructure, and actively enforce security policies based on overall hardware trust status.

The integrated architecture implemented by EMC, RSA, Intel, and HyTrust successfully achieves these goals.

Scope
This paper presents a solution that showcases available options for addressing workload migration challenges faced by enterprises and service providers. It does not include detailed configuration recommendations.

Audience
This paper is intended for technical architects and strategists who are responsible for developing and implementing their organization’s workload migration strategies and the security policies governing those workloads. It is assumed that the reader has proficient knowledge of information security, governance, and cloud terminology.

Key technologies overview
In this paper, we highlight several solutions that allow secure, nondisruptive workload migration within and between data centers. Key benefits related to these solutions are as follows:

- EMC VPLEX enables nondisruptive workload migration within and between data centers using storage virtualization technologies that allow virtual storage volumes to be extracted from underlying heterogeneous storage arrays.

- Intel TXT provides the ability to establish hardware root of trust for cloud infrastructures, which can be compared against known good configurations.

- Intel has developed a trust attestation solution to extract hardware trust status from Intel TXT enabled hosts. The trust status can then be exported to policy enforcement and reporting systems through a set of APIs. Intel continues to develop this solution and provides best practices around using it to validate cloud environments, and it is working with partners who are also developing attestation solutions.

- The HyTrust Appliance sits between administrators and VMware vCenter/ESXi hosts to control administrative actions based on defined security policies. The HyTrust Appliance uses the overall trust status from Intel’s trust attestation solution to either permit or deny actions. For example, we demonstrate the ability to block a virtual machine migration from a trusted host to an untrusted host in the cloud environment.

- The RSA Archer Cloud Security and Compliance solution is a set of control procedures that provides a governance, risk, and compliance (GRC) framework
for VMware infrastructures. This allows you to assess, monitor, and report on the security and compliance status of your VMware cloud infrastructures. Using the APIs available in Intel's trust attestation solution, RSA Archer now has the ability to report host trust status on a dashboard, allowing you to monitor whether applications and virtual machines are running on hosts that have been validated against known good configurations.

- Enforcement actions taken by HyTrust Appliance can be brought into the RSA Archer Incident Management module through the use of a security information and event management (SIEM) solution, such as RSA Security Analytics for Logs. This allows both trust status and enforcement actions to be presented through a single GRC platform.
Challenges in trusted workload migration

Workload migration is defined simply as the process of moving application workloads from one physical host to another. Administrators might migrate workloads for reasons such as the following:

- Perform maintenance on one host while allowing the application to continue running during maintenance.
- Recover from a disaster and bring the applications up on a new host.
- Avoid a disaster, such as an approaching hurricane, by migrating their applications to a facility outside the path of the approaching threat.
- Move some application workloads from their own data centers to a service provider data center.

The challenge is to accomplish workload migration without causing downtime to applications or end users, thus avoiding lost productivity and revenue.

Traditionally, when service providers or enterprises were tasked with the challenge of migrating data and applications between geographically-diverse data centers, they had to go through a series of manual, error-prone tasks and activities. They would either make physical backups or use data replication services to transfer application data to the new location. Applications had to be stopped and could not be restarted until testing and verification was complete.

In today’s virtualized data centers, administrators can take advantage of VMware vMotion, which makes possible the live migration of running virtual machines from one host to another with zero downtime, continuous service availability, and complete transaction integrity. A stretched storage area network (SAN) allows you to transfer a virtual machine from a host in one data center to a host in another data center. This type of configuration uses VMware vMotion and VMware Storage vMotion, which enable live migration of the virtual machine and migration of virtual machine disk files within and across storage arrays. This stretched SAN makes the storage available at the distant site but significantly adds to the time needed for failover, so moving virtual machines from site to site has its limitations.

In addition to confronting the challenges of migrating workloads between hosts in a nondisruptive manner, service providers must ensure that the hosts running those applications are continually secure. As enterprises choose to move more of their workloads to cloud service providers or to build their own cloud infrastructures, they are asking questions like these:

- How will this cloud infrastructure be verified and validated from a hardware security perspective?
- How will I know that the hosts running my virtual machines are secure?
- Will I be able to satisfy my audit and compliance requirements for this environment?
Before virtualization, if a single host was compromised, only the applications running on that host were compromised. That is no longer the case. Today, if a single hypervisor is compromised using something like a BIOS rootkit attack, dozens of systems in an enterprise cloud (or dozens of customers in a multitenant cloud provider environment) can be compromised. Attacks at this level are specifically designed to evade typical runtime security protection like anti-virus software. Organizations must provide a secure level of hardware trust attestation to ensure confidence that the environment beneath their hypervisors has not been compromised.
In the past, users have relied on traditional physical storage to meet their information needs. Developments such as server virtualization and the growth of multiple sites throughout an enterprise or service provider's network have placed new demands on how storage is managed and how information is accessed.

To keep pace with these new requirements, storage must evolve to deliver new methods of freeing data from a physical device. Storage must be able to connect to virtual environments and still provide automation, integration with existing infrastructure, consumption on demand, cost efficiency, availability, and security.

Figure 1 depicts the evolution of server and storage virtualization, bringing us from standalone models to ones using pools of cooperation.
The EMC VPLEX family is the next-generation solution for data mobility and access within or across data centers. VPLEX is the first platform to deliver local and distributed federation, whereby resources are pooled and made to cooperate through the stack.

- Local federation is the transparent cooperation of physical elements within a site.
- Distributed federation provides access between two locations across distance.

VPLEX removes physical barriers, allowing users to access a single copy of data at different geographical locations, and enables geographically stretched virtual or physical host clusters. The removal of physical barriers facilitates transparent load sharing among multiple sites while providing the flexibility of relocating workloads between sites in anticipation of planned events. Furthermore, in case of an unplanned event that could cause disruption at one of the data centers, the failed services can be restarted at the surviving site with minimal effort, minimizing time to recovery. In the case of VPLEX Metro with the optional VPLEX Witness and Cross-Connected configuration, applications continue to operate in the surviving site with no interruption or downtime.

VPLEX completely changes the way IT is managed and delivered—particularly when deployed with server virtualization. By enabling new models for operating and managing IT, VPLEX allows resources to be federated, and applications and data can be moved dynamically across geographies and service providers. The VPLEX family breaks down technology silos and is a critical element that helps deliver IT as a service.

Figure 2 shows how storage virtualization allows all underlying storage to be presented to the hosts as virtualized storage volumes.
The VPLEX family consists of the following three products:

- **EMC VPLEX Local** delivers local federation, which provides simplified management and nondisruptive data mobility across heterogeneous storage arrays within a data center.

- **EMC VPLEX Metro** delivers distributed federation, which provides data access and mobility between two VPLEX clusters within synchronous distances.

- **EMC VPLEX Geo** delivers data access and mobility between two VPLEX clusters within asynchronous distances.

Figure 3 highlights the VPLEX products and functions.

For the joint solution detailed in this white paper, we used EMC VPLEX Metro to demonstrate storage virtualization between two data centers within synchronous distances of each other with an approximate latency maximum of 10 ms or less for the VMware environments.

**Benefits of VPLEX Metro:**

- Helps transparently move and share workloads—including entire virtual machines—consolidate data centers, and optimize resource use across data centers

- Provides nondisruptive data mobility, heterogeneous storage management, and improved application availability

- Supports up to two clusters, which can be located in the same data center or at two different sites within synchronous distances

- Enables you to mirror volumes within and across locations, providing continuous application availability in the event of a disaster
VPLEX Metro, in combination with VMware vSphere and VMware vMotion, provides a unique capability that enables you to transparently move and relocate virtual machines—with their corresponding applications and data—within synchronous distances.

Figure 4 shows VPLEX Metro providing virtualized storage pooling within synchronous distances between two data centers.
Intel Trusted Execution Technology hardware security solution

**Infrastructure security challenges**

In today’s technology landscape, as organizations are being asked to evolve their data centers to serve new and more demanding needs that challenge existing security practices, service providers and enterprises must use the most secure building blocks available in the foundations of their solutions. As a data center becomes increasingly virtualized, workloads from different lines of business and many customers in a multitenant environment are shared across a common physical infrastructure. Where traditional physical isolation is no longer possible, a more trusted infrastructure is vital to maintaining the increased security demands of the data center.

**Hardware security**

The penalties and costs for lost or compromised customer, employee, or financial data dictate that service providers and enterprises maintain control of their systems and implement the best tools available to continually protect their infrastructure and validate the integrity of the computing environment. Establishing a root of trust is essential. This involves validating that each server component is running in a known good state, from the BIOS and system firmware to the system hypervisor. The server components must behave as expected and provide a description of the platform characteristics and an assessment of its trustworthiness.

**Intel TXT solution**

Intel TXT establishes the root of trust that provides the vital underpinnings for successful evaluation and protection of the computing platform. The root is optimally small and difficult to defeat or alter, and it allows for flexibility and extensibility to measure platform components in the boot and launch environment (such as BIOS, OS Loader, and Virtual Machine Managers). The root provides a trusted position for evaluating the integrity of the other components, enabling assurance through a secure comparison against expected measurements. By allowing such comparison during the boot and launch sequence, IT managers can detect the launch of unrecognized software that does not match known good launch-time configurations.

After a basic root of trust and a secure basis for measurement and evaluation is established, it becomes possible to further extend these capabilities and the technologies that enable them. For example, to protect other aspects of the system, mechanisms can be created to seal and protect secrets in memory, as well as provide local or remote attestation (proof) of system configuration.
Intel TXT is a feature of the Intel Xeon processor that works with enhanced hardware components on a server designed to protect sensitive information from software-based attacks. Intel TXT works with features in the chipset, I/O subsystems, and other platform components, including the Trusted Platform Module and BIOS. When coupled with an enabled operating system, hypervisor, and enabled applications, these features provide trust, confidentiality, and integrity of data in the face of increasingly hostile environments.

Intel TXT incorporates several secure processing innovations, including the following:

- Trusted extensions integrated into silicon (processor and chipset)
- Authenticated code modules (ACMs), which authenticate platform-specific code to the chipset and execute it in a trusted environment within the processor to perform secure tasks
- Launch control policy (LCP) tools

Third parties provide some of the required components for the Intel TXT secured platform, including the following:

- Trusted Platform Module (TPM) (third-party silicon) 1.2 or later — A hardware device that that stores authentication credentials in platform configuration registers (PCRs) issued by Intel TXT
- BIOS, firmware, operating system, and/or hypervisor environments enabled by Intel TXT

Intel TXT features include the following:

- **Protected execution:** Allows applications to run in isolated environments within the TPM, preventing unauthorized software from observing or tampering with operational information. Each of the isolated environments is executed using dedicated resources managed by the platform.
- **Sealed storage:** Provides the ability to encrypt and store keys, data, and other sensitive information within the hardware, with decryption allowed only by the platform that encrypted it.
- **Attestation:** Enables a system to provide assurance that the protected environment has been correctly invoked and to take a measurement of the software running in the protected space. The information exchanged during this process is known as the attestation identity key credential and is used to establish mutual trust between parties.
- **Protected launch:** Allows for the controlled launch and registration of critical system software components in a protected execution environment. Rather than relying on the detection of malware, Intel TXT works before malware can be launched as it builds trust into a known software environment, thereby ensuring that the software being executed hasn't been compromised. This advances security to address key stealth attack mechanisms used to gain access to parts of your cloud. Intel TXT works with Intel Virtualization Technology (Intel VT) to create a trusted, isolated environment for virtual machines.
Summary

Intel TXT uses a staged approach to establish a hardware-based root of trust by measuring and evaluating launch components against expected measurements stored in and protected by the TPM. The result is a carefully evaluated launch process called a measured launch environment (MLE).

“Enabling and using Intel TXT” on page 26, provides specifics about enabling Intel TXT.
HyTrust Appliance security policy enforcement solution

Security policy enforcement challenges

One of the key security issues in managing cloud infrastructures is inadequate governance of privileged user rights in the virtualized data center. In some cases, privileged users have administrative access to every virtual machine, virtual network interface, and virtual security appliance, as well as the underlying hypervisor. They can copy, migrate, power off, or delete a production virtual machine—accidentally or intentionally—with a few clicks. The result can be operational downtime or compliance violations, both of which can mean significant expense to the organization. VMware does not provide a viable way to require additional approval of requested operations that could have major consequences. Given the minimal visibility provided by the virtualization platform, linking responsibility for changes to resources with the users who made the changes can be nearly impossible.

HyTrust solution

HyTrust Appliance enables enterprises to virtualize their mission critical applications while maintaining availability, integrity, and compliance. HyTrust Appliance provides needed security controls for compliance and visibility of the virtual infrastructure.

Figure 5 provides an overview of HyTrust Appliance.

Features

HyTrust Appliance has the following features:

- Fine-grained authorization
  - Enforces consistent separation of duties and infrastructure segmentation policies with an optional secondary approval requirement
  - Permits or denies changes made by privileged users to the virtual infrastructure based on enterprise-defined policies
  - Enforces consistent policies for administrative access across all access methods (vSphere Client, SSH, Web, CLI) to vCenter and direct-to-host
  - Supports both role-based and asset-based access control rules to meet any operational, security, or compliance need
  - Integrates with the active directory for efficient role definition
• Audit quality logs
  ▪ Are based on granular, user-specific data for all virtual infrastructure operations performed by administrators
  ▪ Aggregate detailed logs of every user request in a uniform format
  ▪ Provide a unique user ID for every access using root password vaulting, increasing accountability and compliance
  ▪ Record essential audit data not available from vCenter, including records of denied requests, source IP addresses, and details of virtual machine reconfigurations
  ▪ Automatically send log data to SIEM platforms, which can then parse critical information to be sent to an organization’s GRC solution

• Strong, multifactor authentication
  ▪ Is used for virtualized infrastructure, converged infrastructure (such as Cisco’s Unified Computing System [UCS]), and physical and virtual network devices based on NX-OS
  ▪ Integrates with RSA SecurID and other third-party strong authentication software, preventing stolen administrator login credentials from compromising cloud security

• Hypervisor hardening, trust verification, and infrastructure governance
  ▪ Relies on Intel TXT to ensure platform integrity and root password vaulting of the privileged root accounts on the hypervisors
  ▪ Verifies host and hypervisor root of trust using Intel TXT, defeating rootkit attacks
  ▪ Identifies and remedies hypervisor misconfiguration, reducing vulnerabilities
  ▪ Allows organizations to define operational policies that are validated against the Intel TXT trust status of each host
Figure 6 shows how the HyTrust Appliance verification process works.

Figure 6. HyTrust Appliance verification process
RSA Archer Cloud Security and Compliance solution

As companies look to extend the benefits of virtualization to business-critical applications, new security management and compliance concerns emerge.

While the process for security management and compliance is similar for both physical and virtual environments, virtualization presents the following unique challenges:

- Virtual machines are frequently brought online and offline or moved from one server to another as a result of the rapid rate of change in the virtual infrastructure.
- When security and compliance teams are not involved in the planning stages of virtualization projects, visibility and control of the virtualized environment can be less manageable than it was in the physical environment.

If security and compliance issues associated with virtualization and cloud computing are not addressed proactively, they can result in unnecessary costs to the business, including the following:

- Unrealized capital and operational savings when virtualization projects are delayed over security and compliance concerns
- Regulatory audit failures and fines that result from insecure virtualized infrastructure
- Impact to brand and shareholder confidence that stems from security breaches
- Lack of a detailed understanding of the organization’s security posture

The RSA Archer Cloud Security and Compliance solution addresses these challenges by enabling a GRC framework to provide security and compliance visibility into the VMware infrastructure.

Using the RSA Archer Cloud Security and Compliance solution, you can do the following:

- Assess, monitor, and report on the security and compliance posture of your VMware infrastructure.
- Manage compliance against security policies.
- Remediate noncompliant controls.
- Track implementation of controls through workflows.

The RSA Archer GRC platform provides a library of policies, control standards, procedures, and assessments mapped to current global regulations and industry guidelines. Control procedures in the library are written specifically against the *VMware vSphere Security Hardening Guide* and are mapped to security policies and authoritative sources such as Payment Card Industry (PCI), Control Objectives for Information and Related Technology (COBIT), National Institute of Standards and Technology (NIST), Health Insurance Portability and Accountability Act (HIPAA), and North American Electric Reliability Corporation (NERC).
In addition, the library includes thousands of control procedures for operating systems, databases, network devices, and other infrastructure assets, which are mapped to the same laws, regulations, and industry standards.

The solution helps automate the measurement of the VMware infrastructure against VMware control procedures though the Automated Measurement Agent, a set of tools that discovers each VMware device and scans it for its configuration state.

Figure 7 is a simplified view of the architecture of the RSA Archer Cloud Security and Compliance solution.

![Architecture](image)

**Figure 7.** RSA Archer Cloud Security and Compliance solution architecture

This solution discovers new virtual infrastructure devices and interrogates them against the control procedures to verify that VMware security controls have been implemented correctly. The results of these automated discovery and configuration checks are fed directly into Archer for continuous monitoring across the cloud environment.

For this particular environment, in addition to the existing controls for VMware cloud environments, we have included control procedures related to Intel TXT. This gives us a high-level view of the overall hardware compliance added to the benefits inherent in the GRC system.

RSA Security Analytics for Logs ensures that log data and alerts on security events generated from resources within the environment are passed into RSA Archer, providing alerts for new security events that alter the compliance posture. In our demonstration, HyTrust Appliance feeds directly into RSA Security Analytics for Logs,
which then triggers alerts into RSA Archer for events of interest related to hardware root of trust.
Overall solution architecture for secure workload migration

Review of key components

In combination, the key technologies we have discussed complement each other to form an overall solution that enables secure workload migration between data centers. The following is a summary of the components:

- **EMC VPLEX Metro.** EMC VPLEX is an in-band storage virtualization device that allows you to simultaneously export virtual volumes from the underlying arrays. When deployed across two data centers, it gives an instant copy of the data at both locations. Moving virtual machines from one data center to another is simple with vMotion, because the data is already at both sites. You save the time it would take to migrate your storage and you have the ability to instantly move your workloads from one site to another in a nondisruptive manner. This avoids downtime to your applications and end users.

- **Intel TXT.** Intel TXT is a feature of the Intel Xeon processor that works with a set of enhanced hardware components on a server designed to protect sensitive information from software-based attacks. It uses a staged approach to establish a hardware-based root of trust. This is done by measuring and evaluating launch components against expected measurements stored in and protected by the TPM. The results of this carefully evaluated launch process can be attested to and reported into virtualization management and security management infrastructures.

- **HyTrust Appliance.** HyTrust Appliance enforces administrator-defined security policies for virtual infrastructures based on VMware and provides the visibility required for security and compliance. It sits between the administrators of the virtual infrastructure—the virtualization administrators, the network administrators, and the application owners—and the virtual infrastructure itself. From this centralized vantage point, HyTrust Appliance intercepts all administrative requests for the virtual infrastructure, determines whether or not the request is in accordance with the organization’s defined policies, and then permits or denies the request as appropriate.

- **RSA Archer Cloud Security and Compliance solution.** The RSA Archer Cloud Security and Compliance solution, built on RSA Archer, enables a GRC framework for VMware infrastructures, allowing you to assess, monitor, and report on the security and compliance posture of the VMware infrastructure. It discovers new virtual infrastructure devices and interrogates them against a set of control procedures to verify that VMware security controls have been implemented correctly. The results of these automated discovery and configuration checks are fed directly into Archer for continuous monitoring across the cloud environment.
Because this solution is aimed at service providers and enterprises with multiple data centers, we used a similar architecture for this demonstration. Figure 8 shows a high-level diagram of the environment used for the solution.

![High-level solution architecture](image)

**Figure 8.** High-level solution architecture

In this diagram, two data centers are represented with the hosts running VMware ESXi 5.1, storage using EMC VNX, and virtual distributed volumes enabled by EMC VPLEX.

Each host has an Intel Xeon processor with Intel TXT enabled, and we implemented a trust attestation and verification solution developed by Intel. “Enabling and using Intel TXT” on page 26 provides more details about this solution. A measured launch of the platform and hypervisor establishes root of trust for the hosts. Upon verification, each host in the environment is assigned a trusted or untrusted status that can then be used by security policy enforcement and reporting platforms.

In our demonstration, we used a total of four hosts and installed VMware ESXi 5.1 on three of them. On the fourth host we installed ESXi 5.0 to intentionally provide a host that differed from the known good configuration we set up.
Table 1 shows the setup of the hosts.

<table>
<thead>
<tr>
<th>Host</th>
<th>Intel TXT Enabled</th>
<th>ESXi Version</th>
<th>BIOS Same?</th>
<th>Overall Trust Status</th>
</tr>
</thead>
<tbody>
<tr>
<td>Hopkinton01</td>
<td>Yes</td>
<td>5.1</td>
<td>Yes</td>
<td>Trusted</td>
</tr>
<tr>
<td>Hopkinton02</td>
<td>Yes</td>
<td>5.1</td>
<td>Yes</td>
<td>Trusted</td>
</tr>
<tr>
<td>Boston01</td>
<td>Yes</td>
<td>5.0</td>
<td>Yes</td>
<td>Untrusted</td>
</tr>
<tr>
<td>Boston02</td>
<td>Yes</td>
<td>5.1</td>
<td>Yes</td>
<td>Trusted</td>
</tr>
</tbody>
</table>

With the trusted or untrusted status for each host established, we used HyTrust Appliance to define security policies based on the trust status and created enforceable actions relying on that data. As an example, we defined a policy that allowed an administrator to migrate a virtual machine from a trusted host to another trusted host, but prevented virtual machine movement to an untrusted host.

In addition to ensuring active enforcement based on hardware trust status, we imported the trust status into the RSA Archer GRC solution to provide a high-level view of compliance with defined security policies. This allowed us to quickly determine whether the cloud infrastructure met the organizational security policy and helped us identify any gaps that needed to be addressed.

Finally, we pulled the enforcement actions from HyTrust Appliance into RSA Archer’s dashboards by automatically sending log data to RSA Security Analytics for Logs, which parsed critical information to be sent to RSA Archer.

All of these components, when combined together in a fully integrated solution, provide a service provider or enterprise the ability to perform secure, nondisruptive workload migration between data centers.

### Enabling and using Intel TXT

A key component to providing a secure environment with established root of trust is the enabling of Intel TXT within the infrastructure. Following is a high-level overview of the steps required to enable Intel TXT, as well as a few points about harvesting that trust status for use by your enforcement and reporting platforms.


2. If necessary, update the BIOS and firmware to the latest version supporting Intel TXT.

3. Enable VT and VT-D, and set the TPM to enabled and activated for storing measurements.

4. Install the desired ESXi5 version, clear the TPM, and enable TXT in the BIOS.
Implementing HyTrust Appliance

Intel has developed a trust attestation solution, available from HyTrust, which provides the necessary components to perform verification of measurements associated with gaining the hardware root of trust. Components include the trust dashboard, management console, and whitelist portal, which constructs the known reliable configurations. When you have acquired the attestation solution, complete the following:

1. Deploy the trust attestation server OVF and follow the setup process.
2. Create the users for the trust dashboard, whitelist portal, and management console, and approve the users in the management console.
3. Configure your whitelist from the management console using the configuration on your known good host.
4. Check the trust dashboard and whitelist portal to verify that the host/Virtual Machine Manager (VMM) was added.
5. Go to the management console and register the hosts from vCenter, then check the trust status against your known good configuration.

HyTrust Appliance provides a key component for secure workload migration by actively enforcing organizational security policies defined by the service provider or enterprise administering the infrastructure.

In the demonstration, security policies restrict the movement of virtualized workloads based on whether or not the platform has attained trust status (using Intel TXT).

- If a host starts with known good configurations checked against the whitelist server within the measured launch environment, the host is given positive trust status and administrators can then move virtual machines to that host.

- If a host does not start with a known good configuration, it is labeled with a negative trust status. Administrators cannot move virtual machines to that host the host is brought into compliance with the organization’s security policies.

Implementing RSA Archer

HyTrust Appliance enables the service provider or enterprise to watch its defined policies being enforced within the cloud infrastructure. Using RSA Security Analytics for Logs, a SIEM tool that is capable of parsing important logs, classifying them based on priority, and then forwarding them to the GRC platform, events and all notable logs associated with the enforcement are sent to RSA Archer GRC for audit and compliance reporting.
Use case demonstrations

Viewing Intel TXT trust status

After the trust status is established on each host, the Trust Status Dashboard in Intel’s trust attestation solution allows you to monitor the trust status from each host in the environment. Figure 9 shows a view of the dashboard from our demo environment.

![Trust Status Dashboard](image)

Figure 9. Trust status dashboard

Both the BIOS and VMM must match the known reliable configuration for the host to achieve positive trust status. The dashboard shows that three of the four hosts in the environment have achieved a positive overall trust status. Because we installed a different version of ESXi on the fourth host as a test of our known good configuration, the fourth host has not achieved a positive trust status, as indicated by the red icons. Although the BIOS trust status is positive, the negative VMM trust status results in an overall negative trust status for that host.
The host trust status is reported in RSA Archer, which shows an overall compliance view for the cloud infrastructure. RSA Archer can tie directly into the APIs provided by Intel’s trust attestation solution so that the trust status information can be used by the same GRC platform used to report on other parts of the organization’s compliance posture. Figure 10 shows a view of the Cloud Security and Compliance dashboard, customized to display information related to Intel TXT trust status.

![Cloud Security and Compliance dashboard](image)

**Figure 10. Cloud Security and Compliance dashboard**

The dashboard shows that 75 percent of the infrastructure is in compliance, representing that three out of four hosts match the known good configurations for the cloud infrastructure.
The trust status can be used to define an organization’s security policy that ensures workloads are running on known good infrastructure.

Similar to the way RSA Archer ties into the APIs of Intel’s trust attestation solution, HyTrust Appliance obtains the hardware trust status for the hosts it is protecting. Once the trust status is obtained, the organization’s defined security policies can be actively enforced.

For this demonstration, the administrator has attempted to move a virtual machine from one of our three trusted hosts to the fourth host, which is not trusted. This looks exactly like a normal vMotion event until the migration is attempted by vCenter. Figure 11 shows the error displayed when the migration is attempted.

![Figure 11. Invalid-migration error message](image)

The error indicates that permission was denied by HyTrust Appliance. Registering HyTrust as a vCenter plug-in enables the display of the specific error message, which describes the reason permission was denied, as shown in Figure 12.

![Figure 12. Event details displayed in vCenter](image)
RSA Archer provides a high-level view of the overall compliance for hardware trust status in the GRC system as well as a view into specific events to confirm that active enforcement is taking place based on the trust status. RSA Archer provides a single place to view how the cloud infrastructure aligns with overall security policies and validation that protection mechanisms based on those policies are in place and working.

RSA Archer can be customized to display information about specific events. Figure 13 shows RSA Archer’s incident management dashboard displaying the same information that was displayed in the HyTrust plug-in in vCenter in Figure 12.

RSA Archer also allows you to view additional details for specific events, as shown in Figure 14 and Figure 15.
Figure 15 shows details of the Event Payload.

In the “Event Payload” section of the details, the last line indicates a failed check on the policy. The policy was checking that a trusted label existed on the virtual machine being migrated. Since the machine was not trusted, the check within the policy was false, and permission was denied when migration was attempted. Had the host been trusted, permission would have been allowed and normal vMotion operation would have been permitted.
Conclusion

Summary

This solution presents methods of facilitating secure workload migration within and between data centers through the following:

- Moving applications and data dynamically using EMC VPLEX
- Enabling hardware-based security using Intel TXT
- Allowing the active enforcement of security policies based on Intel TXT using HyTrust Appliance
- Providing additional audit and reporting capabilities using RSA Archer

This test case demonstrates how to set up migration policies for a set of virtual machines that stay within the confines of trusted infrastructure while actively enforcing security policies based on overall hardware trust status.

Combined in an integrated architecture put together by EMC, RSA, Intel, and HyTrust, the solution successfully achieves the stated goals.

Findings

This white paper highlights several solutions that enable secure, nondisruptive workload migration within and between data centers. The following is a summary of key findings related to these solutions:

- EMC VPLEX enables nondisruptive workload migration within and between data centers by utilizing storage virtualization technologies that allow organizations to extract virtual storage volumes from underlying heterogeneous storage arrays.
- Intel TXT provides organizations with the ability to establish hardware root of trust for their cloud infrastructures. It enables them to compare those infrastructures against known good configurations and use trust and integrity as a control point for virtual workloads.
- HyTrust Appliance monitors and controls administrative actions for vCenter based on defined security policies. HyTrust Appliance uses the overall host trust status from Intel's trust attestation solution to permit or deny actions.
- RSA Archer Cloud Security and Compliance solution is a set of control procedures that enables a GRC framework for VMware infrastructures, allowing organizations to assess, monitor, and report on the security management and compliance posture of their VMware cloud infrastructures. Host trust status is displayed in the RSA Archer dashboard through the APIs built into Intel's trust attestation solution, showing whether applications are running on hosts that have been validated against known good configurations.
- Enforcement actions taken by HyTrust Appliance are brought into RSA Archer's incident management module through the use of a SIEM solution, such as RSA Security Analytics for Logs, which displays both trust status and enforcement actions through a single GRC platform.
References

White papers

For more information, see the following white papers:

- Using VMware vSphere with EMC VPLEX – Best Practices Planning
- Intel Trusted Execution Technology
- Evolution of Integrity Checking with Intel Trusted Execution Technology: an Intel IT Perspective

Other documentation

For additional information, see the following:

- RSA Security Brief – Infrastructure Security: Getting to the Bottom of Compliance in the Cloud
- HyTrust Appliance product documentation