HyTrust®
Virtualization Under Control

WHITE PAPER – August 2011

Passing Compliance Audit: Virtualize PCI-compliant Workloads with the Help of HyTrust and Trend Micro Deep Security

Contents

Virtualization in PCI DSS 2.0 3

PCI Requirements and Controls that are reported upon 6

Requirement 1: Install and maintain a firewall configuration to protect cardholder data 7

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters 8

Requirement 3: Protect stored cardholder data 9

Requirement 5: Use and regularly update anti-virus software or programs 10

Requirement 6: Develop and maintain secure systems and applications 11

Requirement 7: Restrict access to cardholder data by business need to know 12

Requirement 8: Assign a unique ID to each person with computer access 13

Requirement 9: Restrict physical access to cardholder data 14

Requirement 10: Track and monitor all access to network resources and cardholder data 15

Conclusion 16

Virtualization in PCI DSS 2.0

As more and more businesses begin to virtualize and move their operations to private, hybrid and public cloud environments, these businesses are struggling to understand what constitutes PCI compliance for virtual environments and are looking for comprehensive solutions to reduce the complexity of the audit process while ensuring that the security of their virtualized environments meets and exceeds the security of their legacy physical environments. The need for clarity and transparency around compliance in this context has never been greater.

Recently, new guidelines for virtualization compliance were issued by the PCI Security Standards Council based upon the work of the Virtualization Special Interest Group (VSIG), and these guidelines will play a critical role in defining the solutions required to make the shift to virtual environments safely, driving compliance while protecting customer data and company reputation.

10 Key Risks for Virtualization and compliance

1. Hypervisor environment is in scope
2. One function per server
3. Separation of duty
4. Mixing VM's of different trust levels
5. Dormant VMs and VM snapshots
6. Immaturity of monitoring solutions
7. Information leakage
8. Defense in depth
9. VM Hardening
10. Cloud Computing

Trend Micro and HyTrust have been active participants in VSIG since its inception in 2009, and have been at the forefront of developing solutions for virtualization security and management for VMware environments. As such, the two companies are uniquely poised to now offer a joint solution which covers many of the major guidelines issued by VSIG and which gives businesses the visibility and insight required to virtualize and move to the Cloud with confidence.

Virtualization guidelines supplement points out key risks that need to be considered when virtualization cardholder data environment (CDE). With this solution, HyTrust and Trend Micro take holistic view at the challenge of virtualizing compliance workload and come up with controls that address most of those risk and secures both the platform and the workloads hosting the CDE. The table below covers specific functionality that helps to mitigate the risks that were called out in the supplement.

Principle	Impact/Need	Trend Micro Deep Security	HyTrust Virtual Security Appliance
Hypervisor environment is in scope	— Hypervisor & components must be hardened — Restrict physical access — Security patches applied ASAP — Multi-factor authentication for admin functions — Enforce separation of duties — Logging and monitoring of hypervisor environment system events	Hardens VMs to reduce the risk of attacks from VMs to the hypervisor	— Automated hypervisor hardening and monitoring — Physical access restriction with root password vaulting — Two-factor authentication — Separation of duties, version monitoring and complete log of activities for all hypervisor management channels
One function per server	— No change from physical servers; no impact		
Separation of duty	— Requires role-based access control (RBAC)	— Roles based access control supported for all Deep Security Administrative functions	— Provides Role Based, Object based and Category based access control for least privilege access
Mixing VM's of different trust levels	— In order for in-scope and out-of-scope VMs to co-exist on the same hypervisor the VMs must be isolated from each other	— IDS/IPS supports firewall and VLAN controls by providing visibility into inter-VM traffic	— Logical partitioning of shared infrastructure per port-group and per host provides the isolation required to support mixed-mode VM deployments
Dormant VMs and VM snapshots	— Access to dormant VMs or snapshots should be restricted — Ensure that only authorized VMs are added and removed — Recognize that VMs are dynamic and state cannot be assumed	Deep Security's Agentless solution provides continuous and automated protection for existing and new VMs. Even VMs that have been paused or dormant are automatically protected using the latest protection eliminating the possibility of security gaps.	— VMs that do not meet policy cannot be powered on — Restricts what snapshots can be taken

Immaturity of monitoring solutions	— Traditional tools do not monitor inter-VM traffic — Virtualization specific tools are still immature compared to their physical counterparts	— VM specific IDS/IPS protection provides visibility into inter-VM traffic — Integrity Monitoring provides visibility into unauthorized changes to guest-VMs — Log Inspection provides visibility into security events occurring to guest-VMs	— Monitors the operations with virtual machines and the stack — Monitors hypervisor configuration
Information leakage	— Between logical network segments — Between logical components	— IDS/IPS provides visibility into inter-VM traffic — Integrity Monitoring provides visibility into unauthorized changes to guest-VMs — Log Inspection provides visibility into security events occurring to guest-VMs	— Provides separation of duties and “need to know” mechanism for the authorized users of virtualization
Defense in depth	— Traditional security appliances cannot protect virtualized environments — Traditional software-based security products can impact performance and functionality in dynamic VM environments	— New VMs automatically protected with a default security profile — Four protection technologies (AV, IDS/IPS, Integrity Monitoring, Log Inspection) integrated into a single comprehensive solution designed specifically for virtualized environments — No ‘gap’ in the protection of dormant VMs brought back online — Protection for physical, server VMs, VDI, hybrid cloud and public cloud	— Automated discovery of the infrastructure and proactive enforcement of policies

VM Hardening	— Harden VMs (OS & Apps) by disabling unnecessary services, ports, interfaces, and devices — Send logs off-board in near real-time — Establish limits on VM resource usage	— New VMs automatically protected with a default security profile — No 'gap' in the protection of dormant VMs brought back online — IDS/IPS shields unpatched vulnerabilities from attack — Integrity Monitoring provides visibility into unauthorized changes to guest-VMs in real-time — Log Inspection provides visibility into security events occurring to guest-VMs & forwards in real-time	
Cloud Computing	— Cloud service provider must provide sufficient assurance that the scope of PCI compliance is sufficient — Cloud service provider must provide the means for the customer to audit the environment — Customer is required to provide additional necessary controls	— Protects VMs regardless of their state or location — Can protect VMs in enterprise, hybrid cloud and public cloud environments	— Makes per-tenant infrastructure logs available

PCI Requirements and Controls That Are Reported Upon

PCI SSC calls out 12 major requirements for protecting the compliant infrastructure. Integrated HyTrust/Trend solution provides measurable controls for 9 of these requirements that concern the underlying technology, while the remaining 3 requirements are mostly process oriented.

Requirement 1: Install and maintain a firewall configuration to protect cardholder data.

Firewalls are vital for controlling traffic into and out of an organization's network – including internal segments related to the cardholder data environment. Legacy firewalls and related management solutions do not automatically extend to virtualized security zones and their related virtual firewalls and other virtual network devices. Technical controls are thus required to validate the configuration of a virtual firewall, and to detect and alert if tampering occurs.

Virtualization Considerations

- Examine multiple virtual layers.
- Use specialized solutions to monitor and restrict traffic.
- Ensure roles and responsibilities are assigned and enforced correctly.
- Be aware of dynamic network boundaries.
- Do not locate trusted and untrusted systems on the same hypervisor.

Best practice questions to ask for Requirement 1:

- Describe your virtual firewall capabilities.
- Describe the process for determining where your solution places virtual firewalls in the network system.
- How does your solution enforce infrastructure segmentation based on policies? Does your solution provide protection from VM escape or VM hopping? Does your solution provide cardholder data protection on the network packet level, for example, how does it discriminate against inappropriate and/or malicious traffic using networking communications effective for the environment (e.g., if bridging is used instead of routing).
- How does your solution prevent tampering with and/or disabling
- virtual firewalls?
- Describe how your solution prevents the accidental or non-authorized act of turning power off on servers running virtual firewalls?
- How does your solution integrate with legacy firewalls and firewall management systems?
- Provide details of your role-based management capability for virtual firewalls.

What is reported on by the solution

Trend: Firewall Active
Trend: Firewall rules assigned
Trend: # firewall events
Trend: IDS/IPS active
Trend: IDS/IPS rules assigned
Trend: IDS mode
HyTrust: host firewall active
HyTrust: detected virtual firewalls
HyTrust: list of portgroups

Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters.

Trying default passwords is the easiest way for hackers to access your cardholder data environment. Some vulnerability management tools can spot the use of default passwords, but their capability may stop with virtual environments where entire networks of virtual machines are hidden from legacy solutions. The use of virtualization in the cardholder data environment also requires password controls for hypervisor and virtual infrastructure management utilities.

Virtualization Considerations

- Use specialized hardening standards and methods across all virtualization layers.
- Be aware of security parameters specific to virtualization technology.
- Be aware of out of band non-console access to virtualized elements such as individual VMs, appliances and other hosted components and additional risk introduced by the new virtual components.

Best practice questions to ask for Requirement 2:

- Describe how your solution provides root password vaulting to eliminate the need for our administrators to know root passwords.
- How does your solution support the implementation and assurance of a secure configuration baseline for the hypervisor hosts?
- Describe how your solution uses industry best practices to govern how it hardens hosts and VM containers.
- How does your solution monitor configuration drift in the hardening posture of any virtual device?
- Explain the automation processes controlling remediation of non-compliant hosts.
- Requirement 2.2.1 notes: “Where virtualization technologies are in use, implement only one primary function per virtual system component.” Does your solution comply with this requirement? If not, explain how your solution will comply as a Compensating Control.

What is reported on by the solution

HyTrust: hosts with remote root login enabled
HyTrust: number of controls for all host configurations
HyTrust: number of configuration scans
HyTrust: Remediation mode
HyTrust: number of rules configured for VMConsole access

Requirement 3: Protect stored cardholder data.

Cardholder data is all information printed, processed, transmitted or stored in any format on a payment card. The PCI DSS urges no storage of cardholder data unless absolutely necessary, and deleting it immediately after use is a safe precaution. However, deletion is challenging to verify in a virtualized environment with VM mobility, data replication, and storage virtualization spreading cardholder data across connected storage subsystems. Secure deletion requires perfect knowledge of the location of all data copies. The process of secure deletion is only possible through the destruction of entire storage arrays or erasure of encrypted storage keys. It's mandatory to make all stored cardholder data unreadable by using encryption or tokenization and key management. It's much easier to "delete" Virtualized stored cardholder data by erasing the associated key.

Virtualization Considerations

- Be aware of the dormant and off-line VMs, VM snapshots, and cashed memory images that may maintain critical data.
- Separate logical access to encrypted files and protect privileged accounts that may expose cryptographic keys.
- Do not store the keys on the same hypervisor as encrypted data.
- Do not virtualized key management functions.
- Be aware that encryption may be applied against multiple virtualization layers.

Best practice questions to ask for Requirement 3:

- How does your solution address the problem of "remnants" of stored cardholder data on virtual resources? For example, memory that was previously stored only as volatile memory can, in virtual systems, be written to disk as "stored" by taking snapshots of systems. Describe how your solution knows that there are no remnants of stored data in virtual systems.
- How does your solution protect data exposed on internal networks, such as memory data transmitted during VMotion or on the connections to distributed storage such as NFS.
- How are cardholder data in virtual memory resources and other shared virtual resources protected from unauthorized access?
- Describe how your solution prevents unauthorized snapshotting of VMs in the cardholder data environment.
- Explain how your solution ensures deletion of cardholder data stored on virtual systems that are powered off.

What is reported on by the solution

Trend: IM active
Trend: IM real time
Trend: IM rules assigned
HyTrust: infrastructure segmentation report
HyTrust: list of restricted resources

Requirement 5: Use and regularly update anti-virus software or programs.

To comply with Requirement 5, your anti-virus software and signature updates must track the virtual machine lifecycle. Virtual infrastructure may be sensitive to performance issues associated with scheduled scan activities.

Virtualization Considerations

- Multiple anti-malware protection mechanisms may be required to protect guests and hypervisors.
- Ensure that the selected anti-virus mechanism does not interfere with virtualization function and provides adequate protection.

Best practice questions to ask for Requirement 5:

- How does your solution distinguish whether virtual system components in the cardholder data environment are commonly affected by viruses and other malware, or if they are not susceptible to those risks?
- How does your solution identify virtual systems that have changed configurations, and require an anti-virus software or signature update?
- Describe how your solution ensures that anti-virus software on virtual system components in the cardholder data environment is properly configured and running the most recent version of software and signatures?
- What process does your solution follow for distributing patches to virtual system components?
- How does your solution protect VM management servers in the cardholder data environment?
- How will implementing your solution for updating anti-virus software or programs affect performance of our virtual infrastructure?

What is reported on by the solution

Trend: AV active
Trend: real-time protection
Trend: AV action
HyTrust: number of rules configured for VMConsole access

Requirement 6: Develop and maintain secure systems and applications.

Legacy vulnerability management does not automatically integrate with virtual asset and infrastructure databases. It is infeasible to assure vulnerability management without tight integration with virtualized asset configuration and inventory. Change control processes must be updated to support virtual machine mobility and provisioning. Application security must be integrated with virtual infrastructure inventory controls.

Virtualization Considerations

- Patching may require specialized tools to address multiple virtualization layers and stack elements.
- Development/test systems and data could be inadvertently moved to production.

Best practice questions to ask for Requirement 6:

- How does your solution address the problem of "VM Sprawl," which is creating more VMs than are necessary? Specify how your solution controls the building, copying, placement, and deletion of virtual images in the cardholder data environment?
- Explain how your solution controls who can power off VMs, move VMs to different hosts, and connect VMs to different networks.
- How does your solution support backup up of cardholder data in virtual systems?
- Describe how your solution supports the virtual systems component of disaster recovery and business continuity.

What is reported on by the solution

Trend: IM active
Trend: IM real time
Trend: IM rules assigned
HyTrust: infrastructure segmentation report

Requirement 7: Restrict access to cardholder data by business need to know.

Legacy access control systems do not automatically comply with Requirement 7 within the virtualized data center. System and application level access controls must be enforced throughout the virtualized cardholder data environment.

Virtualization Considerations

- Access controls and least privilege principle need to be implemented across multiple layers.
- Use specialized tools for effective and granular assignment of privileges including access to individual hosted components.

Best practice questions to ask for Requirement 7:

- How does your solution limit access to virtual system components and cardholder data only to those individuals whose job requires such access?
- Describe access controls provided by your solution for each virtual system component. Are they set to "deny all" unless specifically allowed?
- Detail the multi-factor authentication capability provided by your solution.
- Explain how your solution's access controls operate for different security zones in the virtual cardholder data environment.
- Specify granular capabilities for role-based and workload-based access and management.
- How does your solution control access by authorized administrators such that none are able to log into virtual systems as "administrator" or "root?"
- How does your solution enforce separation of duties for access to virtual servers as opposed to virtual networks? Ditto for separating virtual backup administration from management of virtual servers and management of virtual networks.
- Explain how your solution controls access to hypervisor management, particularly for restricting local access for administrators to hypervisor management via centralized console access only.
- Describe logging capabilities for every administrative access attempt (whether allowed or denied).

What is reported on by the solution

HyTrust: number of rules for access
HyTrust: number of users with access
HyTrust: number of attempted policy violations
HyTrust: number of users with access not subject to zone restriction
HyTrust: number of users with SuperAdmin access
HyTrust: RSA configuration report
HyTrust: Root password vaulting configuration

Requirement 8: Assign a unique ID to each person with computer access.

Legacy Identity and Access Management systems do not properly protect virtual data center management, particularly for "headless" hypervisors such as VMware ESXi. Secure access policy management must include capability for virtual inventory controls.

Virtualization Considerations

- Unique IDs and secure authentication is required across multiple layers.
- Additional access controls and specialized tools may be required due to high impact of unauthorized hypervisor access.
- Dormant VMs and snapshots also need to be under access control.

Best practice questions to ask for Requirement 8:

- How does your solution assign all users a unique user name before allowing them access to virtual system components or cardholder data?
- Specify the directory service used by your solution for authenticating administrator and user access to virtual systems in the cardholder data environment.
- What directory service is used when a virtual cardholder data environment is hosted by a cloud provider as opposed to a private cloud hosted on our in-house resources?
- Describe how your solution stores privileged account (root) passwords for all protected virtual hosts. Are these passwords perpetual or granted on a temporary basis to one individual at a time?
- Describe the multi-factor authentication used by your solution, and its integration capabilities with AD, RSA SecurID, and Smart Card.

What is reported on by the solution

HyTrust: number of rules for access
HyTrust: ESX accounts
HyTrust: AD configuration report

Requirement 9: Restrict physical access to cardholder data.

The virtual infrastructure client may allow remote users unrestricted physical access to virtual machine files. Remote network access to the hypervisor service console, CLI, storage management, or Virtualization Management Console may be exploited to grant a remote user the equivalent of physical access to virtualized systems. Traditional physical access controls also must be implemented and enforced for systems hosting virtual services for cardholder data.

Virtualization Considerations

- Physical access to a single hypervisor is equivalent to physical access to all the virtualized components running on it.
- Additionally, dormant components and backup need to be under physical access protection and monitoring.

Best practice questions to ask for Requirement 9:

- Describe how controls in your solution prevent access from a hypervisor to root passwords stored in the virtual cardholder data environment's Identity and Access Management system.

What is reported on by the solution

HyTrust: # of RPV events

Requirement 10: Track and monitor all access to network resources and cardholder data.

Legacy network security systems are unable to track asset and infrastructure access events between virtualized components residing within individual hypervisor nodes. This will result in a critical visibility gap across the virtual data center. Legacy audit systems do not provide fine grained auditing and controls for hypervisor management events, nor do they support virtual system forensics. Traditional application and system logs must be securely maintained for the virtual cardholder data environment.

Virtualization Considerations

- Logging mechanisms specific to the virtualization technology may be required to reconstruct the events required by PCI DSS Requirement 10.2.
- Specific system functions, API, objects and logs may be different for different technologies.
- Specialized tools may be required to capture and correlate audit log data.
- It may be difficult to capture, correlate or review logs in cloud-based deployments.

Best practice questions to ask for Requirement 10:

- Describe how your solution logs all access to virtual systems in the cardholder data environment – especially administrative access.
- Detail the types of data captured in logs, such as user identification, type of event, date and time, success or failure indication, origination of event, and identity or name of affected data, virtual system component or resource.
- What types of automated audit trails are created by your solution? Examples include all individual user accesses to cardholder data; all actions by any individual with root or administrative privileges to virtual systems; access to all audit trails; invalid logical access attempts; use of identification and authentication mechanisms; initialization of audit logs; creation and deletion of system-level objects.
- Where does your solution store log records?
- Describe the security controls protecting log records from alteration or deletion.
- Describe the time synchronization technology used by your solution.
- How does your solution comply with the requirement to retain audit trail history for at least one year, and to provide at least three months of history for immediate analysis?

What is reported on by the solution

HyTrust: log configuration report
HyTrust: hypervisor level access
HyTrust: attempted policy violations
HyTrust: VMConsole access
HyTrust: number of obfuscated operations
HyTrust: number of time affecting operations
HyTrust: number of unique IP address used for access
Trend: log inspection active
Trend: log inspection rules assigned

CONCLUSION

The Right Data at Your Fingertips
Clear, Simple, Measurable Compliance

By combining data from two cutting-edge products for VMware environments, Trend Micro's Deep Security and HyTrust's Security Virtual Appliance, we give the end user a tool that provides clear, simple and measurable compliance for PCI. In addition to providing detailed reports on critical compliance data, we score each area of compliance, then tally these scores to provide a high-level view on overall PCI compliance. This provides both the granular visibility into areas of compliance that need addressing, as well as a view of ongoing compliance status that makes reporting to execs a snap.