PCI-Compliant Cloud Reference Architecture

Cisco, HyTrust, VMware, Savvis and Coalfire have collaborated to construct a cloud reference architecture that addresses some of the unique challenges of the Payment Card Industry (PCI) Data Security Standard (DSS). Innovative technologies from Cisco, VMware, and HyTrust are used to implement the cloud architecture with a number of additional security controls to meet the intent of PCI DSS. The reference architecture was implemented in the Savvis lab and the team collaborated with Coalfire, which provided guidance as a PCI Qualified Security Assessor (QSA).

November 4, 2010

Introduction

Payment Card Industry (PCI) Data Security Standard (DSS) defines a set of requirements to protect payment cardholder data, and the environments in which cardholder data is stored, processed, or transmitted. These requirements apply to all "system components", with a system component defined as any network component, server, or application that is included in or connected to the Cardholder Data Environment (CDE). The challenge with the Data Security Standard (DSS) is that technology is constantly evolving and security and audit capabilities are built in after the initial foundation has been established.

In particular virtualized and cloud environments have some unique challenges, which include adequate segmentation, storage of cardholder data, access control, logging and alerting across all management activities, and use of the base platform layer (i.e. the hypervisor). PCI DSS Version 1.2.1 (the current effective standard) does not provide specific guidance to address the risks directly associated with virtual machines and cloud computing. It only empowers the PCI Qualified Security Assessors (QSAs) and vendors to work collaboratively to create a compliance approach to specific emerging technologies.

DSS will evolve to address technology and threat innovations, but likely will continue to remain vendor agnostic. This document is provided to give merchants, service providers, and assessors a basic framework and a practical implementation for building a PCI-compliant cloud. This document will evolve as DSS is updated, Special Interest Group (SIG) papers are published, and the PCI Security Standards Council Technical Working Group formally provides guidance on virtualization and cloud technologies.

The terms "virtualization" and "cloud computing" do not exist in PCI DSS Version 1.2.1. This version of DSS does not provide specific advice about whether CDE system components need to be physical. This is of no surprise as it was developed before virtualization technologies gained wide spread adoption. In PCI DSS Version 2.0 'System Components' include virtualization technology (hypervisors) and virtual system components such as virtual machines, virtual switches, routers and networks, virtual appliances, virtual applications and desktops.

Herein lies the first challenge: If an in-scope CDE system component is virtualized, can it be adequately protected to meet all the PCI DSS requirements? What else becomes within scope?

PCI DSS controls typically form the foundation for enterprise (both commercial and public sector) internal security practices. To reduce the burden and cost of an audit, PCI DSS suggests that network segmentation be used to isolate the CDE (i.e. protect the CDE from other networks and systems). The primary reason for virtualization adoption is cost reduction for both capital expenditures (CapEx) and operating expenditures (OpEx) through physical server consolidation.

Herein lies the second challenge: How can virtualized system components within a CDE be co-mingled with virtualized system components (servers, network components, security components, management and monitoring components, and such) used for non-CDE functions? Can CDE virtual system components reside on the same physical system as non-CDE virtual system components and still achieve PCI DSS compliance?

After enterprises have gained understanding of and confidence in virtualized infrastructures, adoption of other features, such as live migration for dynamic capacity management will become the norm and enterprises will rely heavily on the benefits from infrastructure elasticity and operational flexibility. How does PCI DSS view this dynamic mobility? Workloads are governed by PCI DSS. The environments that house these workloads are governed by PCI DSS. The people that access and manage these environments are governed by PCI DSS. The processes used are governed by PCI DSS. What about dynamic scaling: how should that be controlled and configured?

Herein lies the third challenge: How can adopters of emerging technology satisfy the intent of PCI DSS and adequately protect cardholder data without any specific guidance?

This document presents a reference architecture and additional controls needed to address the three cloud challenges mentioned above to achieve PCI compliance.

Architecture Use Case: E-Commerce Merchant

An example use case of an e-commerce merchant is presented in this reference architecture. This reference architecture can be equally applied to other use cases.

- The e-commerce merchant uses a cloud to host its e-commerce website. It receives payment via card-not-present transactions (e-commerce).

  Assume, for the purposes of this reference architecture, that the cloud infrastructure is provided by Savvis solely to this e-commerce merchant and resides in facilities owned and operated by Savvis. That is, the cloud (a virtual private datacenter) is not shared with any other merchant, and all virtual compute resources are dedicated to the merchant. However, physical compute, network and storage components are shared across many merchants.

- The cloud infrastructure is co-managed by the e-commerce merchant and Savvis. In addition, to reduce costs, the merchant uses the same cloud infrastructure to run a support forum; store its product catalog in a database; and operate the management, security and other infrastructure systems necessary for the application of these other systems. The merchant essentially needs to co-mingle CDE virtual machines with non-CDE virtual machines, sometimes referred to as a 'mixed-mode' environment.

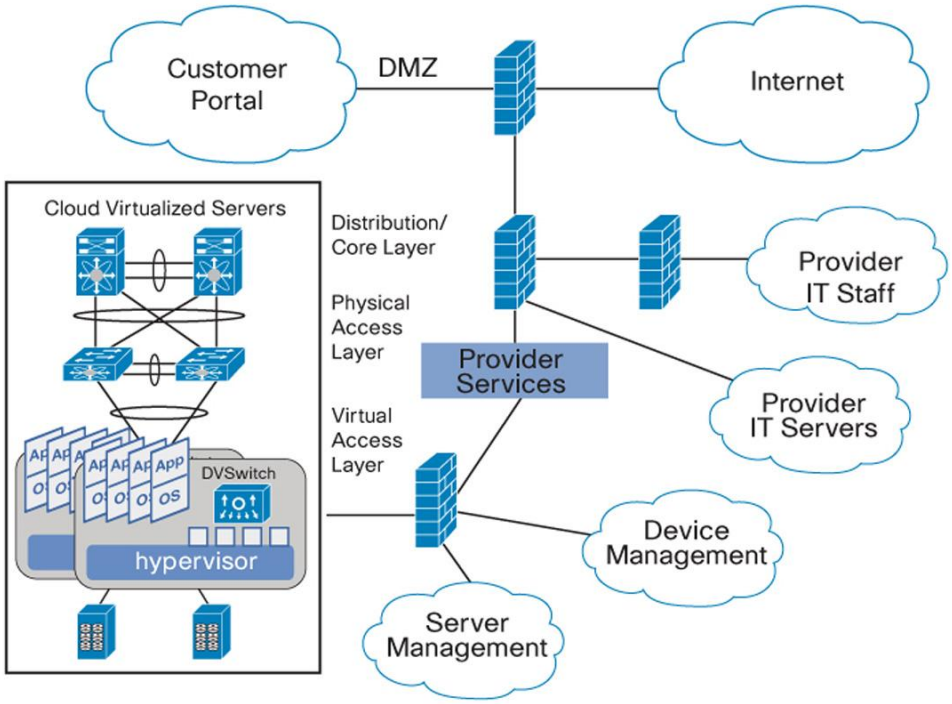
- Different types and tiers of workloads are co-mingled on the same hypervisor. Payments are processed through a third-party payment processor managed and operated by the third-party in its own facility.

- The cloud environment provided by the cloud provider is validated as PCI compliant and the required 12.8 service provider verbiage is contained within the merchant's contract. However, since there is co-management of the cloud environment by the merchant and cloud provider, each entity has the ability to impact the security of the merchant's cardholder data. Therefore the merchant must provide PCI validation of all system components that the merchant directly manages as well as a partial validation of system components that are co-managed. Validation requirements for co-managed environments are not specifically addressed by the PCI DSS and opinions are likely to vary as to the extent of the "co-validation" necessary, including documentation and ongoing monitoring records.

Scope of Work and Approach Taken

The reference architecture implemented in the Savvis lab is based on the Internet access point, the physical system components, the virtualization platforms, the virtualized infrastructure components, the virtual machines, the Storage Area Network (SAN) and physical storage, as shown in Figure 1 below.

Figure 1: Cloud Provider Network Scope Diagram



A disaster recovery (DR) instance of the same functional reference architecture is housed in a geographically separated datacenter lab, and provides redundancy. The same administrators that manage the primary reference architecture also manage this instance. The DR instance is not addressed in this document.

In this cloud environment a number of segmented networks are created to provide separation of access and a layered defense for each cloud. Physical and virtual firewalls are both used to implement physical and virtual network segmentation. All system components (virtual and physical) that are shared such as load balancers, routers/switches, and firewalls are considered in-scope for the CDE, and their configurations are reviewed. Only a sample set is assessed to reduce the amount of validation performed. Sampling is allowed for PCI DSS as long as processes and personnel demonstrate that system components are consistently managed and monitored – the sample set accurately represents the whole.

The Cardholder Data Environment

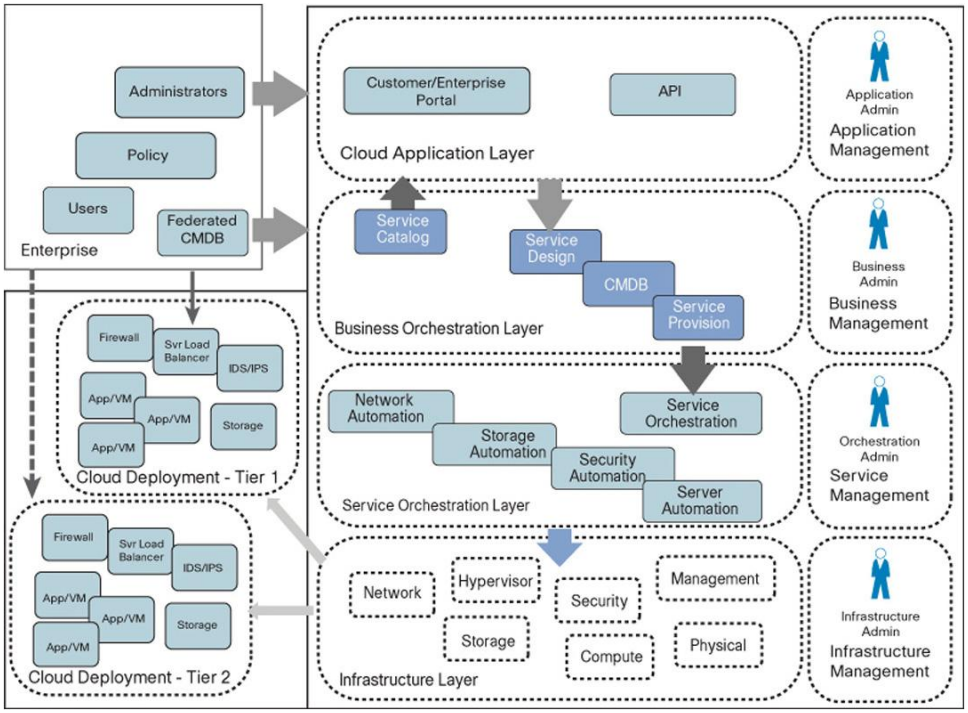
The cloud environment is co-managed by the e-commerce merchant and the cloud provider. The merchant is allowed to perform a limited set of administrative activities through the customer portal (for example, to start and stop a virtual machine and to administer the application running on it), as shown in Figure 1. The customer/enterprise portal limits visibility to each customer, authenticates and authorizes each access, and has detailed monitors for abuse. The provider is responsible for most of the management tasks and maintains separation-of-duties from a business and technical perspective. Each logical business layer is separated through network segmentation and firewall(s), as shown in Figures 1 and 2.

The cloud provider environment consists of individual Virtual Private Data Centers (VPDCs), which are a collection of network, security, storage and compute resources and processes that exist “in the cloud.” The resources and processes provided by the VPDCs were specifically designed to support multi-tenant deployment infrastructure in separate logical containers. Effectively each VPDC is dedicated to the merchant but the underlying infrastructure supports multi-tenancy. These VPDCs support multiple levels of service options including network service level agreements (SLAs), security SLAs, compute SLAs, quality of service (QoS), and backup.

The cloud provider environment consists of the following elements (see Figures 1 and 2):

- Network access: Represents the configuration elements related to authentication and authorization zones (internet, DMZ, internet optimized, private, and private optimized).
- Perimeter security: Represents the configuration elements related to segmentation policies from the internet including web application firewall, perimeter firewall, data leakage prevention, threat management, messaging, and URL filtering policies.
- Redirection: Represents the configuration elements related to the site/data-center selection methods (virtual or dedicated).
- Network delivery: Represents the configuration elements related to server availability (basic or high availability).
- Compute Tiers: Represents the configuration elements associated with the server tiers, including: CPU, memory, resource management, application configuration, security hardening, and associations.
- SAN connected to tier-3 media (SATA drives): Represents the configuration elements related to data access, protection, and storage latency.
  - Data access: Block base storage using radial placement technology and automated RAID migration. All writes are on RAID 10 and then migrated to RAID 6.
  - Data protection: Uses failure consistent Subnetwork Access Protocol (SNAP) copies or customer created SNAP copies.
  - Secondary data protection using enterprise backup technology.
  - Storage I/O latency cannot be guaranteed in a multi-tenant environment. However, volumes with this profile type will normally have the highest average latency when compared to the other two profiles. These volumes reside on SATA drives only and have the highest Virtual Machine File System (VMFS) to Virtual Machine Disk (VMDK) file ratio.
- Server tiers security: Represents the configuration elements related to the compute tier firewall policies, CMDB, and administrative access.
- Tier availability: Represents the availability configuration elements (no high availability, high availability and disaster recovery).
- Application performance: Represents the performance configuration elements (server monitoring, application monitoring, and end-user response time).

Figure 2: Business Layers and Co-management



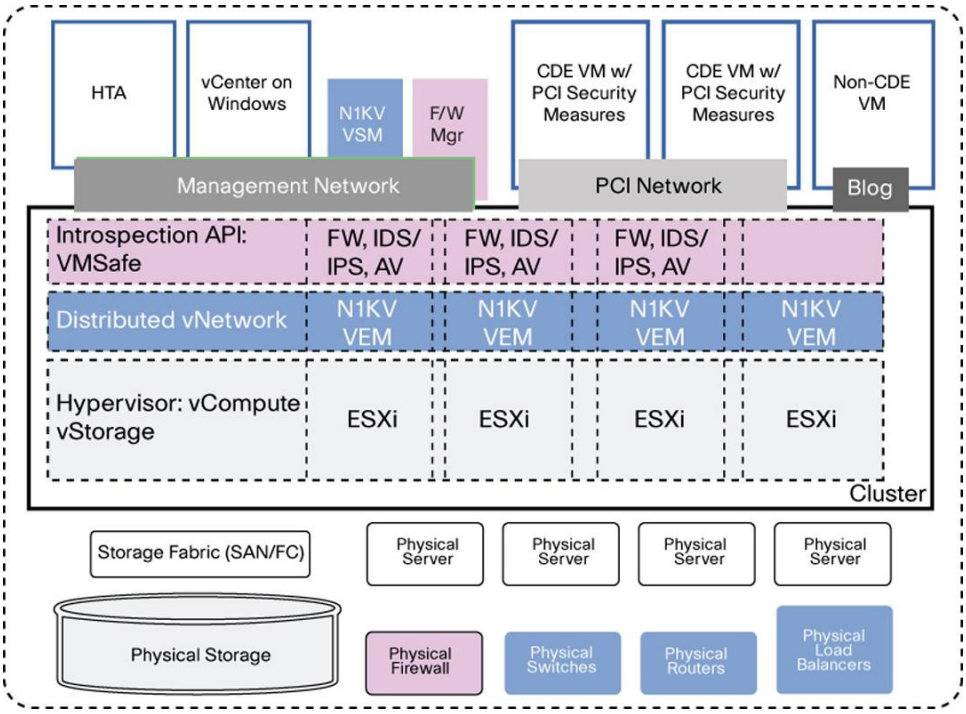
The reference architecture, shown in Figure 2, consists of the following logical business layers:

- Cloud application: Represents the external interface with which the enterprise administrators of the cloud can interact and manage. These administrators are authenticated and authorized at this layer, and have no (direct or indirect) access to the underlying infrastructure. They interact only with the business orchestration layer.
- Business orchestration: Represents both the configuration entities of the cloud and the governance policies for controlling the cloud deployment. It consists of:
  - Service catalog: Represents the different service levels available and their configuration elements.
  - Service design: Represents the service level and specific configuration elements along with any policies defined.
  - Configuration management database (CMDB): Represents the system of record, which may be federated with enterprise CMDB.
  - Service provisioned: Represents the final configuration specification.
- Service orchestration: Represents the provisioning logic for the cloud infrastructure. This layer consists of an orchestration director system and automation elements for network, storage, security, and server/compute.
- Infrastructure layer: Represents the physical and virtual compute, network, storage, hypervisor, security and management components.

The abstraction of these layers and the security controls built into these layers is critical to helping ensure role-based access control (RBAC) and segregation of duties. All cloud provider administrator accounts are maintained in a central repository and two-factor authentication is used. The different tiered cloud deployments (VPDCs) are available to the enterprise users.

The infrastructure layer detailed in Figure 3 includes the following physical components: storage, storage fabric, servers, firewalls, switches, routers and load balancers.

Figure 3: Implemented PCI Measures



Legend: HTA: HyTrust Appliance; N1KV VSM: Cisco Nexus 1000V VSM; N1KV VEM: Cisco Nexus 1000V VEM; CDE VM: Cardholder Data Environment Virtual Machine; FW: Firewall; IDS/IPS: Intrusion Detection System, Intrusion Prevention System; AV: Antivirus; ESX: VMware ESX; ESXi: VMware ESXi.

The implemented cloud reference architecture comprises of a cluster of physical servers running a type I hypervisor (VMware vSphere 4.0 ESX/ESXi) that are connected to the physical storage via the storage fabric. These are referred to as hosts. Hosts are hardened according to VMware's hardening best practices using the HyTrust Appliance. They are also routinely assessed for configuration drift, and automatically remediated depending on policy.

All administrative access, regardless of access method (Secure Shell (SSH)to host, VMware vSphere client to host or VMware vCenter or any of the programmatic or command-line interfaces(CLIs)), is controlled by the HyTrust Appliance (HTA). HTA provides two-factor authentication and role-based access control, virtual infrastructure segregation, root password vaulting, and audit-quality logs of every attempted access.

A distributed virtual switch, such as the Cisco Nexus 1000V spans across all the hosts in the cluster and provides three virtual networks for management, PCI and Blog traffic. The virtual appliances providing infrastructure/management services such as VMware vCenter, HyTrust Appliance, Cisco Nexus 1000V VSM and virtual firewall managers are all connected to the management network. The CDE VMs with the PCI security measures are connected to the PCI network and the Non-CDE VM running the merchant support forum is connected to the Blog network.

In-scope CDE system components are required to implement the following PCI security measures as appropriate:

- Virtual firewall
- File integrity monitoring

- Hardened configuration
- Role-based access control
- Privileged account management
- Anti-virus protection
- Web application firewall
- Intrusion detection system/intrusion prevention system
- Logging/Audit Trail

Some of these PCI security measures can be implemented in an optimized mode using the introspection APIs available in the hypervisor, for example, antivirus, firewall, and intrusion detection and prevention solutions as shown in Figure 3.

Conclusion

With PCI DSS version 2.0 system components may be virtual or physical. Detailed guidance on how to adequately secure the CDE with virtual system components will be provided by the Virtualization Special Interest Group (SIG) as an Information Supplement. All the authors of this reference architecture whitepaper are participating in the SIG.

At a minimum the hypervisors on which CDE Virtual Machines (and any other virtual system components) run, are in scope, as is the storage system where the VM image is stored when it is inactive. The virtualized infrastructure components providing services to a CDE-VM, such as network switches, firewalls and other security solutions are in-scope, together with their respective management servers. This means all these components need to satisfy the PCI DSS requirements and be validated.

The requirement of one primary function per server can be satisfied even in a virtualized environment, with each virtual machine serving one primary function and the underlying hypervisor providing only the single function of virtualization. The hypervisor must be mature and must be able to demonstrate that it is not vulnerable to any known attacks and exploits, and that it can provide adequate isolation for each virtual machine. Hypervisor configuration needs to be hardened to prevent (accidental) abuse by virtual machines and administrators.

Multi-tenancy and mixed-mode: CDE VMs and non-CDE VMs can be co-mingled on a cluster of hypervisors as long as adequate controls are implemented and validated to ensure proper isolation. Network controls and communication must be tested in the same or similar fashion as physical environments to demonstrate segmentation. Refer to Appendix A for vendor specific detailed controls needed to meet each PCI DSS requirement.

Automatic movement of CDE-VMs to other hypervisors in a cluster is allowed. However, it brings into scope the hypervisors and the network over which migration (vMotion) traffic flows. Management and configuration of these capabilities should be carefully controlled due to exposure on the network. It must be authorized to only select administrative personnel.

In summary, a PCI compliant cloud can be achieved with technologies from VMware, Cisco and HyTrust

.

Appendix A: Controls In Place to Meet PCI DSS Requirements

The following table lists the controls in place to meet PCI DSS requirements.

PCI DSS REQUIREMENT	UNIQUE RISKS TO VIRTUAL AND CLOUD ENVIRONMENTS	HYTRUST	CISCO	SAVVIS	VMWARE
Executive Summary	Defining the CDE is particularly challenging in a virtual environment. Every physical and virtual "system component" should be carefully documented. Will this address multi-tenancy environment or use "mixed-mode" deployment? If "other technology" is used to segment systems (such as access control lists (ACLs) on virtual system components) they should be described in detail. The organization should also describe exactly how the system was isolated, how it was tested, and how an auditor can test that segmentation is in place and will remain in place over time.	All the in-scope CDE physical system components are subject to all the PCI DSS requirements. If a CDE system component is virtualized then the virtualization platform (hypervisor) it runs on or is connected to is ALWAYS in-scope. Any virtualized infrastructure or security components deployed on the in-scope hypervisor are pulled into scope, as are their management servers. Multi-tenancy (different owners of co-managed CDEs) and mixed-mode (different tiers of technology and/or trust) on a cluster of hypervisors, can be implemented: • Use of state-of-art, innovative technologies from VMware, Cisco and HyTrust, and • Technologies, processes and personnel training utilized by Savvis. The environment can be assessed with proper documentation from the tenant (e-commerce merchant) and the cloud provider, and tested by a PCI QSA skilled in virtualization and cloud computing, such as Coalfire.			

PCI DSS REQUIREMENT	UNIQUE RISKS TO VIRTUAL AND CLOUD ENVIRONMENTS	HYTRUST	CISCO	SAVVIS	VMWARE
	Three separate network diagrams should be available for the assessor: • Data flow diagram of the CDE • Logical diagram of physical components. • Logical diagram of virtual components.				
Requirement 1 **Install and maintain a firewall configuration to protect cardholder data.**	Most virtual and cloud environments rely on additional technology beyond a standard stateful network firewall to establish separate security zones. Virtual network interfaces cards (vNICs), virtual switches, virtual firewalls, and any other physical components that use software or hardware to create segmentation should be documented and included in section 1, as they are used to establish and maintain segmentation and protect cardholder data	Use the HyTrust Appliance to enforce infrastructure segmentation through label-based policies to prevent administrators from accidentally or otherwise connecting CDE-VMs and Non-CDE-VMs to incorrect portgroups or vswitchs or virtual networks, and to specify which group of administrators can perform specific change management activities to which virtual network and security components. Any virtualized network (Cisco Nexus 1000V Switch Virtual Supervisory Module) or	Use Cisco Nexus 1000V distributed virtual switch to establish private VLANs to segment CDE-VM and non-CDE-VM traffic. Configure vNIC to access specific port groups on a Cisco Nexus 1000V. Cisco Nexus 1000V is typically configured to span multiple hosts in a cluster. Make sure that the port groups map to the correct physical NICs and	Both physical and virtual firewalls and network components are used to segment CDE VMs from non-CDE VM: • Physical perimeter firewall • Physical Server tier firewall • Virtual VMSafe-enabled firewall Documented logical and physical network security zones are established.	VMware vShield App is a hypervisor-based application-aware firewall solution for virtual datacenters. vShield App plugs directly into VMware vSphere to protect against internal network-based threats and reduce the risk of policy violations within the defined security perimeter using application-aware firewalling with deep packet inspection and connection control based on source and destination IP

PCI DSS REQUIREMENT	UNIQUE RISKS TO VIRTUAL AND CLOUD ENVIRONMENTS	HYTRUST	CISCO	SAVVIS	VMWARE
	from access.	firewall management servers should be protected against accidental mis-management such as power-off using the HyTrust Appliance. HyTrust Appliance automatically configures protected hosts to accept only administrative traffic originating from it.	upstream physical switches and ports.		addresses.
Requirement 2 **Do not use vendor-supplied defaults for system passwords and other security parameters.**	The provisioning systems for creating new virtual components must include a way to help ensure that new components are hardened and to remove any default settings.	HyTrust Appliance provides: • Hypervisor root password vaulting. • Hardening of hosts and VM-containers based on industry best practices (e.g. Center for Internet Security or VMware hardening guide). • Monitoring of drift in the hardening posture. • Automatic remediation of non-compliant hosts.		All CDE-VMs are provisioned with hardened operating systems. Virtualized management servers are segmented onto a dedicated management network and are hardened according to vendor or industry best practices. Hypervisors and VM containers are hardened per custom PCI hardening template, and monitored for drift.	VMware ESX or ESXi is used as the hypervisor, which is a type 1 hypervisor, runs on bare metal and serves a single purpose. VMware “host profiles” is used to create templates for host configurations.

PCI DSS REQUIREMENT	UNIQUE RISKS TO VIRTUAL AND CLOUD ENVIRONMENTS	HYTRUST	CISCO	SAVVIS	VMWARE
Requirement 3 **Protect stored cardholder data.**	Memory that was previously stored only as volatile memory can now be written to disk as stored (by taking snapshots of systems). How are memory resources and other shared resources protected from access? (How do you know that there are no remnants of stored data?)	HyTrust Appliance prevents unauthorized administrative access to VMware ESX, ESXI, vCenter, ESX and VM consoles, Cisco Nexus 1000V, VMware vShield Manager and any other virtual management appliance it is configured to protect.	ACL, private VLAN, and anti-spoofing features of Cisco Nexus 1000V are used to protect against man-in-the-middle attacks and maintain network separation of the virtual infrastructure.	SAN security/encryption is used to separate and protect CDE-VMs. CDE-VM backups are encrypted. IDS/IPS data retention is limited and access is restricted to those that need-to-know.	Fully isolate the Vmotion network to ensure that as hosts are moved from one physical server to another, memory and other sensitive running data cannot be sniffed or logged.
Requirement 4 **Encrypt transmission of cardholder data across open, public networks.**	Is any part of the cloud environment considered a “public” network? How are risks to satellite communications, cellular networks, etc. addressed if the environment covers a large WAN?	All traffic between management clients and HyTrust Appliance; and between HyTrust Appliance and protected systems is over an encrypted channel (over SSH or SSL).		• Multiprotocol Label Switching (MPLS) backbone • SSL/VPN/IPsec used to encrypt all traffic between any two systems (virtual or physical) in the CDE as appropriate.	All traffic between any two systems (virtual or physical) including hypervisor in CDE is encrypted or isolated as appropriate. VMware vShield Edge is an edge network security solution for virtual datacenters. Among other capabilities, it provides site-to-site VPN services.

PCI DSS REQUIREMENT	UNIQUE RISKS TO VIRTUAL AND CLOUD ENVIRONMENTS	HYTRUST	CISCO	SAVVIS	VMWARE
Requirement 5 **Use and regularly update anti-virus software or programs.**	What components have anti-virus software and how do they report status and help ensure that newly provisioned systems have anti-virus software installed? If a component will not have anti-virus software installed, what is the justification for determining that it is not a system that is commonly affected by viruses?	The management servers of all VMware VMSafe-enabled solutions are protected by the HyTrust Appliance, for administrative access.		CDE-VMs that are susceptible are provisioned with an anti-virus solution.	No anti-virus solution is needed for VMware vSphere host as it is not a general purpose OS and hence is not widely affected by malware.
Requirement 6 **Develop and maintain secure systems and applications.**	This requirement is one of the most critical in the virtual or cloud environment. The process for creating, implementing, and maintaining the virtual or cloud environment is different than for a physical environment. Building images, backing up data, and building disaster recovery and business continuity systems introduce unique risks. How is VM sprawl addressed?	HyTrust Appliance limits who can create, snapshot or clone CDE-VMs, where they can be instantiated, and who can power-off, copy or delete them.	With the Cisco Nexus 1000V datacenter teams manage their virtual network with the same security policies and workflow that they use to manage their physical network. This capability reduces recertification and reworking.	Defined business process and automated orchestration for how systems are provisioned and who can provision, create snap-shot of, and clone systems. These systems have automatically hardened images and include all the necessary security solutions (see Figure 3). Also all systems (virtual and physical) are patched and kept-up-to-date using VMware Update Manager. Savvis subscribes to vendor specific vulnerabilities and patch notifications.	All hypervisor hosts should be patched and kept-up-to-date using VMware Update Manager. VMware provides: • Notifications when critical security vulnerabilities are discovered and patches are made available. • Guidelines for architecting and hardening

PCI DSS REQUIREMENT	UNIQUE RISKS TO VIRTUAL AND CLOUD ENVIRONMENTS	HYTRUST	CISCO	SAVVIS	VMWARE
					virtual datacenters.
Requirement 7 **Restrict access to cardholder data by business need-to-know.**	Access controls are more complicated. In addition to hosts, there are now applications, virtual components, and storage of these components while they are waiting to be provisioned. Organizations should carefully document all the access controls in place, and help ensure that there are separate access controls for different security zones.	HyTrust Appliance provides granular RBAC for administrative access to VMware ESX/ESXi, vCenter, ESX and VM console access, and Cisco Nexus 1000V (Cisco NX OS CLI) based on business need-to-know, skill set, and resource classification. HyTrust Appliance is used to provide two-factor authentication for all administration access to ESX/ESXi, vCenter, ESX and VM consoles, and Cisco Nexus 1000V. Every attempted administrative access is recorded (whether allowed or denied).	Cisco Nexus 1000V ACLs and private VLANs are used to zone traffic to and from CDE-VMs to other system components in the environment.	The Savvis portal supports two-factor authentication and granular role-based access to the resources “owned’ by the e-commerce merchant, as shown in Figure 2.	The fine-grained access controls of vSphere limits who can access datastores and networks with credit card information.

PCI DSS REQUIREMENT	UNIQUE RISKS TO VIRTUAL AND CLOUD ENVIRONMENTS	HYTRUST	CISCO	SAVVIS	VMWARE
Requirement 8 **Assign a unique ID to each person with computer access.**	Every action that can affect the security of the virtual/cloud environment should be traceable back to a specific individual.	HyTrust Appliance is configured to use the cloud provider user directory and RSA SecurID server, which is where the administrator accounts and their credentials are managed. HyTrust Appliance vaults privileged account passwords for all protected hosts. Access to hosts with privileged account status (root) is granted only on a temporary basis to one individual at a time.		The e-commerce merchant administrators are provisioned in the Savvis enterprise portal to grant them limited access to perform specific operations to their (virtual) resources. The e-commerce application and support forum is managed within the merchants' cloud, and is completely the merchants' responsibility.	Microsoft Active Directory authentication should be used for both vCenter Server and ESX/ESXi host management, so that actions can be tied back to individual users.
Requirement 9 **Restrict physical access to cardholder data.**	This requirement is the same for a virtual or cloud environment as for a physical environment, however the risks are greater since physical access to the hypervisor could lead to logical access to every virtual component and storage.	Even with physical access to hypervisors, if root passwords are vaulted in HyTrust Appliance there is an ability to track access and accountability to an individual user.		Physical data center controls restrict who has physical access to the physical hardware and hypervisor console. Restricted physical access to CDE-VM snapshots and offline instances, which are kept on a SAN.	Physical server the hypervisor runs on is in scope.
Requirement 10 **Track and monitor**	Many virtual components do not have the robust logging	HyTrust Appliance is used to uniformly track and monitor	Without Cisco Nexus 1000V, port statistics are	HP Network Automation Logging and Validating all access and changes made to	Virtualization-related administrative

PCI DSS REQUIREMENT	UNIQUE RISKS TO VIRTUAL AND CLOUD ENVIRONMENTS	HYTRUST	CISCO	SAVVIS	VMWARE
all access to network resources and cardholder data.	requirements of their physical counterparts. Many systems are designed for troubleshooting, and not to create detailed event and system logs that provide sufficient detail to meet PCI logging requirements. Also, PCI requires logs to be stored in a central location that is independent of the systems being logged. (For example, VMware ESX(i) logs should not be stored on a virtual host on the VMware ESX server, as compromising the VMware ESX server could compromise the logs). The logs should be forensically sound.	administrative access to ESX, ESXi, vCenter, ESX and VM consoles, and Cisco Nexus 1000V. HyTrust appliance logs who in which role from where, performed what administrative operation on which resource, when, and the result (allowed or denied) for every management access. All log records generated are sent in near real-time to a central log repository that is on a separate physical system and is tamper-proofed.	reset each time a VM migrates from host to host using VMware vMotion, with Cisco Nexus 1000V port statistics are persistent, creating a clear audit trail. Auditing tools such as NetFlow and Encapsulate Remote Switched Port Analysis (ERSPAN) are also available and are persistent during VMware vMotion movement.	physical systems.	operations are tracked by both vCenter Server event auditing as well as ESX/ESXi logging.
Requirement 11 **Regularly test security systems and processes.**	How are scans conducted on virtual components, and how do organizations know that the scans that were run matched the inventory of all systems that were actually running at the time?	HyTrust Appliance is used to monitor drift from host hardening configurations, and is configured to automatically remediate nightly.	With Cisco Nexus 1000V testing procedures are the same for the physical as they are for virtual networks, reducing audit complexity and	Automated network and vulnerability scanning is performed against physical and virtual systems.	

PCI DSS REQUIREMENT	UNIQUE RISKS TO VIRTUAL AND CLOUD ENVIRONMENTS	HYTRUST	CISCO	SAVVIS	VMWARE
	Are new virtual components scanned before going live?		time taken.		
Requirement 12 **Maintain a policy that addresses information security for employees and contractors.**	All policies should be updated to include the unique risks of a cloud environment, including policies for forensics, employee background checks, and vendor agreements. Asset tracking processes and system should be updated to account for virtual assets.	HyTrust Appliance policy labels are used to include virtual 'asset' information such as owner, contact information, and purpose.	With Cisco Nexus 1000V port profiles and security profiles are maintained centrally in the VSM, and they migrate with each VM during VMware vMotion movement. Also a clear separation of duties can be enforced between the server and network administrators.	Maintain written policy and agreement per 12.8 regarding their responsibility for securing cardholder data.	
Appendix A **Shared hosting providers must protect the cardholder data environment.**	Shared hosting providers must be particularly clear about what their responsibilities are for ongoing controls (patching, logging, monitoring, scanning, etc.)				

Appendix B: References

Payment Card Industry Security Standard Council Data Security Standard
https://www.pcisecuritystandards.org/security_standards/pci_dss.shtml

VMware Security and Compliance Center http://www.vmware.com/security/

Cisco Datacenter Solutions http://www.cisco.com/en/US/products/ps9902/index.html

Savvis Cloud Solutions http://www.savvis.com/en-US/infrastructure-services/Cloud/Pages/Home.aspx

HyTrust resources http://www.hytrust.com/resources/main/

Coalfire Systems PCI Services http://www.coalfiresystems.com/pci_compliance_services.html

Acknowledgements

Authors:

- Hemma Prafullchandra, HyTrust
- Ken Owens, Savvis
- Tom McAndrew, Coalfire Systems
- Charu Chaubal and Davi Ottenheimer, VMware
- Cuong Tran and Han Yang, Cisco Systems

We would like to thank the following contributors and reviewers for their invaluable input to make this whitepaper more comprehensive and accurate.

- Matt Springfield, AT&T Consulting Services
- Mark Weiner, Reliant Security
- Chris Richter, Savvis
- Phil Cox, System Experts
- Eric, Renata, Jason, Will, Julian, Russ and Borya at HyTrust
- Lisa Rice and Shefali Chinni, Cisco Systems

Disclaimer

The information presented in this paper is provided as guidance and was pulled together by the collaborative efforts of the authors. The authors do not accept any liability for any information that is found to be erroneous, incomplete or out-of-date. Best efforts were made to make the information as useful and detailed as possible.

About Cisco Systems, Inc.

Cisco, (NASDAQ: CSCO), the worldwide leader in networking that transforms how people connect, communicate and collaborate, this year celebrates 25 years of technology innovation, operational excellence and corporate

social responsibility. Information about Cisco can be found at http://www.cisco.com. For ongoing news, please go to http://newsroom.cisco.com. Cisco equipment in emerging markets is supplied by Cisco Systems International BV, a wholly owned subsidiary of Cisco Systems, Inc.

About Coalfire Systems, Inc.

Coalfire is a leading IT audit and compliance firm that provides audit, security, and compliance solutions for over 1,000 customers throughout North America. Coalfire delivers these services to companies in the retail, financial services, government, healthcare, education, legal, and public electric utility industries. Our solutions are adapted to requirements under emerging data privacy legislation including PCI, GLBA, HIPAA, NERC CIP, SOX, and FISMA. For nearly a decade, Coalfire has experienced consistent growth and profitability each year. We partner with our customers and establish long-term relationships that achieve business success. Coalfire has delivered more than 4,000 successful IT audits truly a proven track record. Coalfire's team of certified IT auditors and engineers has developed an online platform that guides your organization through the challenging task of establishing, assessing, and validating IT compliance with minimal cost and impact to your business today and into the future. Information about Coalfire can be found at http://www.coalfiresystems.com.

About HyTrust, Inc.

HyTrust®, headquartered in Mountain View, CA, is the leader in policy management and access control for virtual infrastructure. HyTrust empowers organizations to virtualize more - including servers that may be subject to compliance - by delivering enterprise-class controls for access, accountability, and visibility to their existing virtualization infrastructure. The Company is backed by top tier investors Granite Ventures, Cisco Systems (Nasdaq: CSCO), Trident Capital, and Epic Ventures; its partners include VMware; Symantec (Nasdaq: SYMC); Citrix (Nasdaq: CTXS); RSA (NYSE: EMC) and Intel Corporation (Nasdaq: INTC). Information about HyTrust can be found at http://www.hytrust.com.

About Savvis, Inc.

Savvis, Inc. (NASDAQ: SVVS) is a global leader in cloud infrastructure and hosted IT solutions for enterprises. More than 2,500 unique clients, including 30 of the top 100 companies in the Fortune 500, use Savvis to reduce capital expense, improve service levels and harness the latest advances in cloud computing. For more information, please visit http://www.savvis.net.

About VMware, Inc.

VMware (NYSE: VMW), the global leader in virtualization and cloud infrastructure, delivers customer-proven solutions that significantly reduce IT complexity and enable more flexible, agile service delivery. VMware accelerates an organization’s transition to cloud computing, while preserving existing IT investments and enabling more efficient, agile service delivery without compromising control. With more than 190,000 customers and 25,000 partners, VMware helps organizations of all sizes lower costs, preserve freedom of choice and energize business through IT while saving energy - financial, human and the Earth’s. Information about VMware can be found at http://www.vmware.com.

11-630607-00 11/10