

# Payment Card Industry Data Security Standard (PCI DSS) Compliance and VMware

Tom McAndrew

1010101011  
101000001  
1010101011  
101000001



*This paper provides guidance to IT Auditors, QSAs, CIOs, System Administrators, Developers, and IT Auditors who are looking at virtualizing their Cardholder Data Environment (CDE).*

## 1. Executive Summary

Many organizations are looking to virtualize their IT environments but are concerned about how virtualization will impact their security and compliance. The Payment Card Industry Data Security Standard (PCI DSS) is one of the most challenging and specific set of standards established to date. It is used by many organizations as a standard to secure their systems. This paper provides guidance to IT Auditors, Qualified Security Assessors (QSAs), Chief Information Officers (CIOs), System Administrators, Developers, and IT Auditors who are looking at virtualizing their Cardholder Data Environment (CDE).

## 2. PCI and VMware Basics

This paper assumes the reader is familiar with the PCI DSS, Card Brand Requirements, and any specific guidance published by their acquiring bank or processor. The PCI DSS applies to all organizations that store, process, or transmit cardholder data, regardless of volume. This includes merchants, service providers, payment gateways, data centers, and outsourced service providers.

This paper also assumes that readers are familiar with the basics of virtualization and the VMware product line. Specifically, this paper focuses on solutions and configuration settings that address PCI requirements and will cover products such as ESXi, vSphere, vCenter Configuration Manager (VCM), vShield, etc.

Although this paper specifically addresses PCI compliance, the same basic tenants can be used for meeting other regulatory environment, such as GLBA, HIPAA, SOX, NERC CIP, FISMA, etc. For more information on PCI requirements or VMware's line of products, see the references at the end of this whitepaper.

*Organizations can be PCI compliant with virtual machines.*

*"System components" also include any virtualization components such as virtual machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.*

*- PCI DSS p.10*

## 3. Can Virtual Environments be PCI Compliant?

Yes, virtualization can be used in PCI environments and many organizations have already implemented virtualization. Although virtualization has been around for decades, the term "virtualization" was not specifically addressed in the PCI DSS until version 2 was released in October 2010. In DSSv2, PCI first acknowledged that virtualization can be used. Specifically, it mentions that organizations should ensure any system components that are part of the Cardholder Data Environment (CDE) include "any virtualization components such as virtual

*machines, virtual switches/routers, virtual appliances, virtual applications/desktops, and hypervisors.”* In addition, Self Assessment Questionnaire C-VT was released which specifically addresses virtual terminals.

*“Securing Virtual Payment Systems” is a supporting document released by the PCI SCC to provide additional guidance for assessors and organizations that use virtual environments.*

However, many auditors and organizations requested additional guidance and assessment criteria for evaluating virtual environments. Several years ago, the Council established Special Interest Groups (SIGs) comprised of leading experts in the industry, to provide thought leadership and guidance for various technologies such as virtualization. These SIGs were guided by the Council and provide industry input which was used to publish whitepapers. The PCI Security Standards Council is due to release a Virtualization Information Supplement in Q1 of 2011 with some additional clarification. Users are encouraged to check the Council’s website for the most recent guidance.

Virtual environments can be PCI compliant and are being deployed throughout the payment card industry in a variety of means. The PCI DSS and supporting SIG whitepapers provide vendor-agnostic guidance for implementing virtual environments. This paper provides guidance from Coalfire, a leading Qualified Security Assessor, and was written to specifically address the VMware suite of products. As the leading vendor of virtualization and cloud infrastructure solutions, VMware has established several controls and products designed to meet the unique requirements of PCI environments.

#### **4. All virtual environments are not the same**

The first step in architecting a PCI compliant environment is to determine what environment would be most appropriate based on the business and risk of the organization. While there are infinite numbers of options, there are three common ways organizations typically implement VMware.

##### Option #1: Direct conversion of all systems in the CDE

The simplest type of conversion for any organization is to simply virtualize all the physical components that are currently “in-scope” and deploy them as virtual machines (VMs) on a dedicated set of hardware. This hardware should be appropriately segmented from non-CDE systems, typically through the use of a hardware-based firewall. In this option, all the previous PCI controls would apply to the same virtual systems that were previously non-virtual. In addition, the hypervisor level would need to be appropriately hardened to meet PCI requirements (such as logging, monitoring, access control, patching, etc.). This is the simplest approach for organizations that are going through an initial virtual conversion

*The simplest approach to virtualizing an environment is to virtualize all systems onto a dedicated set of hardware that is logically isolated from the rest of the organization’s environment by a firewall.*

and have no business constraints for ensuring all virtual components and physical hosts can meet PCI controls.

#### Option #2: Mixed-Mode Environments

Mixed-mode environments are virtual environments where some VMs are designed to meet PCI controls, and some VMs are not. These environments are not recommended for simple or high risk deployments as they add complexity to the scope, segmentation requirements, and validation procedures used by auditors. These environments should only be pursued by sophisticated IT organizations that understand the risks and challenges with mixed-mode and have a clear business need to run CDE and non-CDE systems in the same hypervisor and hardware.

*There is a lack of consensus among assessors on how mixed-mode environments can be properly deployed and assessed. If an organization is considering mixed-mode, they should compare the risks and complexities of mixed-mode with the business drivers and work closely with their assessor and acquirer.*

Organizations must work closely with their assessors as currently there is no guidance from the PCI SSC on how mixed-mode environments can be deployed and assessed. Some organizations/assessors believe that there is too much risk in allowing a non-PCI compliant VM to reside on the same hypervisor. They are concerned about “VM escape” or other exploits which could allow an attacker to jump from a non-CDE VM to a VM in the CDE. Other organizations/assessors believe that there are appropriate ways of addressing the risk of mixed-mode through the use of various segmentation methods such as the use of VLANs, virtual firewalls, virtual switches, and other products. In either case, it is important for the assessor to provide their guidance on what will be assessed and what rationale the assessor will use when conducting their assessment.

PCI strongly encourages organizations to implement network segmentation “through a number of physical or logical means, such as properly configured internal network firewalls, routers with strong access control lists, or other technologies that restrict access to a particular segment of a network.”<sup>1</sup> Segmentation is encouraged, but PCI does not require it. However, for the vast majority of organizations, segmentation is necessary to reduce the scope and risk of their environments. Limiting the number of systems required to meet PCI standards is effective in increasing security and reducing costs to meet compliance.

Ultimately it is up to the organization, its assessor, and acquirer/card brand/processor to determine if the risks of mixed-mode can be sufficiently addressed with additional controls and business requirements. It should also be noted that the

---

<sup>1</sup> PCI Data Security Standard v2.0.

forthcoming Virtualization Information Supplement will provide guidance for mixed-mode environments.

### Option #3: Multi-Tenancy Environments

Multi-tenancy environments are virtual environments where more than one organization (tenant) resides on the same virtual platform(s). This is typically used in environments such as hosted data centers and service providers which sell products/services for multiple companies.

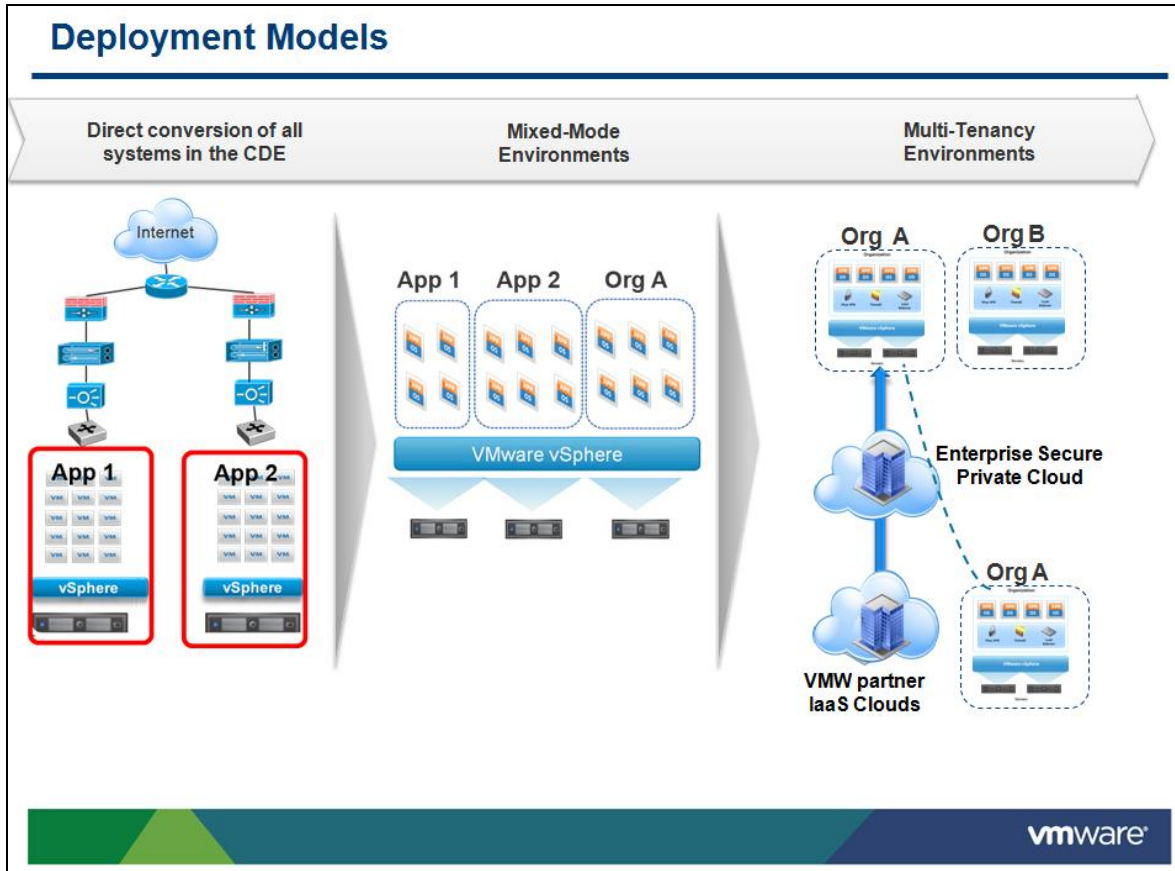
*Service providers with access to cardholder data (or cardholder data components such as VMs), must actively manage and monitor their compliance with the PCI DSS.*

This architecture provides the most benefit for small organizations that want to completely outsource their CDE and host at a data center or service provider that is contractually responsible for meeting specific PCI controls that are outsourced. If an organization outsources to a service provider in a multi-tenancy environment, they should ensure that they meet the contractual requirements of PCI DSS 12.8, specifically ensuring that the service provider clearly understands what services impact the security of cardholder data and ensuring PCI compliance for those services at all times. They must also meet all of the requirements of PCI DSS Appendix A-Additional PCI DSS Requirements for Shared Hosting Providers.

*Multi-tenancy environments should carefully consider, document, and demonstrate they are meeting PCI DSS Requirement 2.4 which states that “shared hosting providers must protect each entity’s hosted environment and data.”*

If an organization is building a mixed-mode environment internally, they should be aware that all the risks of Option #1 and Option #2 above also apply. There is even a greater need for controls since a security incident could potentially impact not just one organization, but possibly all organizations hosted in the mixed-mode environment. Multi-tenancy environments should carefully consider, document, and demonstrate that they are meeting PCI DSS Requirement 2.4 which states “*shared hosting providers must protect each entity’s hosted environment and data.*”

These options are also outlined in more detail in VMware’s Security Journey, in which we are seeing the adoption of physically segmented virtual environments, to mixed-mode, to multi-tenancy.



### 5. Eight questions to ask in all virtual environments.

*There are eight critical questions all organizations should ask and answer for any virtual cardholder data environment.*

1. *How is the hypervisor protected?*
2. *How is access control managed?*
3. *How is the CDE segmented?*
4. *How is change control managed?*
5. *What is being logged and how is it monitored?*
6. *How is encrypted Data at rest and in motion managed?*
7. *How is File Integrity Monitoring implemented?*
8. *How is security implemented on virtual hosts?*

When architecting and assessing a virtual environment, organizations must be aware of the unique risks and additional controls required in a virtual environment. Simply put, the virtual environment should be able to demonstrate a similar level of security and compliance as its physical counterparts. This means all virtualized systems (servers, switches, firewalls) and any additional virtual components (i.e. the hypervisor) must be configured in accordance with the PCI DSS, if in scope.

While all PCI requirements apply to virtual environments, the following are eight critical questions that auditors and organizations should ask for any virtual environment:

#### 1. How is the hypervisor protected?

The hypervisor provides the keys to the kingdom, managing and protecting all access between virtual components. Organizations should ensure that they have implemented security hardening guidelines.

**2. How is access control managed?**

There are additional access methods to CDE systems through the hypervisor, virtual network devices, and storage of virtual machines (snapshots). All access control systems should be clearly documented and understood for all virtual system components.

**3. How is the CDE segmented?**

Ensuring that non-CDE systems cannot impact the security of CDE systems is critical. In a virtual environment, there are multiple paths to access and alter virtual components. All these paths should be carefully understood, mitigated, and documented. Particular attention should be paid to virtual components such as virtual switches, and virtual firewalls or access controls systems such as local accounts, VLANs and port groups. A virtual network diagram should be created that shows all connections and restrictions.

**4. How is change control managed?**

Virtual environments are much more dynamic than their physical counterparts. Systems can be duplicated, access resources, and altered or deleted dynamically on the fly. It is critical that organizations manage change control for virtual components and the hypervisor.

**5. What is being logged and how is it monitored?**

Section 10 of the PCI DSS has specific logging and monitoring requirements for all systems in the CDE. Historically, meeting these logging requirements was very challenging for virtual environments since the logs were originally designed for troubleshooting and IT system administration. Today many logs are now in standard formats that can integrate into common logging tools, enabling organizations to effectively log critical components and monitor systems.

**6. How is encrypted Data at rest and in motion managed?**

PCI requires data at rest to be encrypted (PCI Req 3.2), but does not require internal traffic to be encrypted. In a virtual environment, data that was previously never stored (such as encryption keys in memory) could be converted to virtual traffic and routed through non-CDE systems if not properly configured (e.g. vMotion).

**7. How is File Integrity Monitoring implemented?**

File Integrity Monitoring (FIM) is challenging in any environment, including virtual environments. Organizations must ensure that critical system files are reviewed and monitored for consistency to approved images and baselines.

## 8. How is security implemented on virtual components?

There are unique challenges with managing security requirements (such as logging, anti-virus, patching, etc.) in virtual environments. For example, if all systems are set to run daily A/V scans at the same time, there is a risk that the systems could consume a lot of processing power and crash the system. As a result, there are tools to assist organizations to run security through agent-less applications. As virtualization becomes more prevalent, additional tools will be developed which will impact the way security and compliance is assessed.

The following sections provide more detailed guidance addressing technical configurations specifically for the VMware suite of products.

## 6. Protecting the Hypervisor

*Only ESXi architectures should be used for PCI environments. While older versions of ESX can be compliant, they have additional complexities and nuances which are not addressed in this whitepaper.*

The hypervisor is the software that partitions and controls the flow of information among the different virtual machines. The ability of one machine to create several isolated environments allows companies to capture some of the inefficiencies lost with separate physical machines. Hypervisors are the most critical components to any virtual environment.

*Hypervisors which rely on other operating systems are more vulnerable than bare metal installs. VMware recommends organizations only implement ESXi environments.*

VMware's hypervisor has evolved substantially over time. It was originally designed to operate as software which would run on top of a host operating system. This architecture had increased risk since vulnerability on the host operating system could cause a breach of the hypervisor. ESX is now designed as a bare-metal hypervisor with a Linux-based management console operating system. This still exposes risks as the hypervisor had both inherent risks of Linux and the ESX software. Today, VMware recommends organizations only use ESXi. ESXi's bare-metal architecture operates without any console operating system or the associated risks.

Bare-metal hypervisors improve security over their hosted counterparts. They provide two primary advantages:

1. Reduces the hypervisor's footprint, and
2. The hypervisor removes a layer of software creating a less complex system

*The hypervisor should be hardened according to the "VMware vSphere Security Hardening Guide."*

However, as with any software, the hypervisor must still be hardened and configured correctly. This includes configuring the hypervisor to manage access control through vSphere and vCenter Server, and hardening the hypervisor to hardening guidelines using vCenter configuration Manager (VCM).

VCM is able to evaluate hypervisor compliance with accepted security standards, such as DISA STIGs, CIS Benchmarks and vSphere Hardening Guidelines. This helps to automate the process and reduce errors in hardening the hypervisor. VCM will identify misconfigurations and users are able to use vCenter to remedy identified problems.

*Check the SHA-1 hash of any VMware software before installation.*

Before installing VMware software, always check the file against the current SHA-1 hash available from VMware to ensure that the software you are installing has not been altered.

## 7. Managing access control

*The ESXi host management network should not be accessible from remote systems on the Internet.*

Managing access control in a VMware environment requires knowledge of the tools and security solutions available from VMware.

*The ESXi host should be accessed through vSphere. vSphere should control access through the use of Groups and a centralized access control system such as Microsoft's Active Directory.*

Limiting access to the hypervisor is critical and is performed in ESXi through vSphere and locking down the ESXi host. The ESXi host can be configured to be accessed through any vSphere API client, such as vSphere Client, vCenter Server, and vCLI. Organizations should not allow access to the ESXi host management network from remote systems on the Internet. While this is not specifically prohibited through a PCI requirement, it is high risk. If an organization must have remote access, then it must implement PCI DSS 8.2 requirements and ensure processes enforce strong forms of authentication such as signed Digital Certificates from a Certificate Authority combined with strong two factor authentication and monitoring.

*By integrating vSphere to a third-party access control system, all user permissions, password requirements, and roles can be more easily reviewed and assessed.*

Where possible, access to the ESXi host should be centrally managed through an access control system. The preferred method for PCI compliance is through vCenter Server. vCenter Server creates logical containers which can be used for access and grouping. These groups can be governed through centralized authentication system (such as Microsoft Active Directory) to streamline the number of access control systems in use. By integrating vCenter Server to a third-party access control system, all user permissions, password requirements, and roles can be more easily reviewed and assessed, and can also be used to access VMs by leveraging the same central authentication system. When the use of local accounts on the ESXi host is necessary, organizations will want to consider using additional access controls which may include the use of two-factor authentication, splitting administrator responsibilities, or using jump boxes to manage secure access to the hypervisor.

A centralized authentication system is the first step to ensuring authentication requirements can be met, such as PCI DSS Section 8. Based on the architecture, number of systems, and number of users, organizations may want to consider implementing further controls.

*vCenter Configuration Manager (VCM) can also be used to manage access controls to guest VMs.*

vCenter Configuration Manager (VCM) can also be used to manage access controls to guest VMs. VCM can be used to ensure that any newly-established VMs are deployed and provisioned in a manner consistent with established baselines.

## 7. Segmenting the CDE

As mentioned in section 4 of this paper, there are three common deployment options for establishing a Cardholder Data Environment (CDE): virtualizing the entire CDE, creating mixed-mode environments, and establishing multi-tenancy environments. The first step for architecting and reviewing a network is to review the network architecture.

Standard networks generally have two network diagrams:

1. A cardholder data flow which outlines where data originates, how it is processed, and where it is sent out of the environment;
2. A traditional network diagram depicting all the different hardware and software within the CDE.

In a virtual environment, the cardholder data flow can be difficult to depict as it is more than simply a hardware diagram. Since all network communications must go through hardware at some point, there are natural network chokepoints and shared resources. Also, intra-VM traffic can be difficult to control and map in a virtual environment. The vShield line of solutions can assist organizations with common segmentation challenges in virtual environments.

### vShield

vShield has two primary solutions to assist organizations with establishing segmentation in a virtual environment, vShield Edge and vShield App. vShield Edge is used to provide segmentation at the perimeter (from the Internet to the internal network). vShield App is used to provide segmentation within the CDE. While both solutions have the ability to segment networks in a variety of ways, the following section should assist organization with understanding and architecting segmented solutions. While it is possible to attain PCI compliance without the vShield line of products, it is difficult and manpower intensive. Both vShield Edge and vShield App act as firewalls with stateful inspection of TCP, UDP and ICMP traffic (PCI

*Organizations should understand and utilize the vShield solutions to enforce PCI network segmentation.*

DSS 1.1, 1.2, and 1.3). vShield Edge provides an interface similar to a common border firewall, while vShield App provides a more detailed interface which can be used for additional internal segmentation.

### **vShield Edge**

*vShield Edge acts as a firewall with stateful inspection of TCP, UDP and ICMP traffic (PCI DSS 1.1, 1.2, and 1.3). It is also used for Network Address Translation (PCI DSS 1.3.8).*

vShield Edge is a virtual appliance which bridges a designated security zone/network and all outside networks. All traffic that attempts to go in or out of the isolated VM/Zone must pass through the vShield virtual appliance. It can also be used for Network Address Translation (PCI DSS 1.3.8). vShield Edge can also be used to establish site-to-site VPN tunnels between different remote sites. This is particularly useful when the VMs are implemented across two geographic boundaries (such as a headquarters and a remote store).

### **vShield App**

*vShield App is useful for establishing and monitoring application-level segmentation, but should not be solely used to meet the “application firewall” requirement. (PCI DSS 6.6)*

vShield App is particularly useful for organizations that want to further segment their network behind the firewall. In many cases, there is not one CDE, but several different security zones. vShield App creates segmentation between various zones (such as databases, application servers, web servers, etc.).

It is an enhanced network segmentation tool that can be used to provide stateful packet inspection and blocking for internal segments. It is also useful for organizations looking to split up their PCI VLAN, or for monitoring the virtual traffic within a VLAN. vShield App provides additional security benefits such as preventing ARP spoofing and internal monitoring such as displaying all traffic and logging specific traffic that matches designated criteria.

### **Architecture #1 – Port Group Isolation**

*There are two different architectures for managing segmentation with vShield Edge. Organizations should understand the differences between Port Group Isolation (PGI) and VLAN's.*

One of the easiest ways to meet PCI segmentation requirements in a new virtual environment is to ensure that vShield Edge is deployed with Port Group Isolation (PGI). PGI is a module which runs on the hypervisor along with a service virtual appliance on each ESXi host. This configuration uses a proprietary Layer-2 encapsulation technology to isolate and segment the CDE network. Assessors should review the configuration of port groups and vShield Edge settings to ensure that segmentation has been appropriately established and implemented.

*Assessors should review the configuration of port groups and vShield Edge settings.*

### **Architecture #2 – VLAN Isolation**

The second option is to map port groups to specific VLANs. This tactic is commonly used by organizations that are currently using VLANs or have an existing VLAN architecture. Organizations must manage their VLANs in a physical network (switch) and then map those to virtual trust zones. Then each host must be individually

configured to a specific VLAN. This architecture adds additional management components to segmentation (switch, VLANs, and the hosts), but may be easier to manage for some organizations which already use VLANs.

## 8. Change control

*VMware has established vCenter Configuration Manager (VCM) as the solution to assist organizations with deploying and configuring “PCI Compliant” systems requirements.*

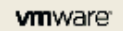
After an organization has implemented its virtual architecture and established a CDE, it must deploy and implement virtual components that are hardened to PCI requirements. PCI DSS requirement 2.2 requires organizations to “develop configuration standards for all system components.” VMware has developed vCenter Configuration Manager (VCM) as the solution to assist organizations with deploying and configuring PCI Compliant systems.

VCM has an established library of common templates and policies that are built from regulatory organizations (e.g. PCI), industry best practices, vendor recommendations (e.g. VMware Hardening Guidelines), and self-defined standards. VCM then allows organizations to leverage these security and compliance policies, or define their own, to assess all virtual and physical components against those policies.

VCM automatically collects tens of thousands of security and configuration settings from each vSphere, ESX, Windows, UNIX, and Linux server and workstation, then stores that configuration information in a centralized repository for analysis and reporting. This data is then checked against the assigned/desired security and compliance policies to show problems.

Users are able to remediate these problems to bring systems into compliance by either selecting the applicable correction or setting VCM to make corrections automatically. If configuration exceptions are necessary, users may denote these as well. Exceptions are tracked accordingly for auditing purposes but this can help organizations ensure that they are continually and actively managing their PCI compliance. VCM also allows auditors to see a snapshot of the current systems that are running ensuring that all system components are inventoried and accounted.

# Compliance Results



## Compliance by Asset Classification

Asset Class	# of machines	# of conditions	Compliant Conditions		Non-Compliant Conditions	
Vital	11	2,056	1,221	59%	41%	835
Significant	15	2,842	1,693	60%	40%	1,149
Average	10	1,956	1,144	58%	42%	812
Minor	9	1,809	1,040	57%	43%	769
Not Classified	2	410	249	61%	39%	161
<b>Total evaluated</b>	<b>47</b>	<b>9,073</b>	<b>5,347</b>	<b>59%</b>	<b>41%</b>	<b>3,726</b>

## Compliance by Rule Severity / Rule Group

Rule Severity	Rule Group	# of machines	# of conditions	Compliant Conditions		Non-Compliant Conditions	
<b>Critical</b>		<b>47</b>	<b>7,431</b>	<b>4,419</b>	<b>59%</b>	<b>41%</b>	<b>3,012</b>
	Payment Card Industry DSS Windows 2003 Server Controls v1.2.1	15	2,384	1,409	59%	41%	975
	Payment Card Industry DSS Windows 2008 Server Controls v1.2.1	13	1,947	1,201	62%	38%	746
	Payment Card Industry DSS Windows Vista Workstation Controls v1.2.1	11	1,770	1,075	61%	39%	695
	Payment Card Industry DSS Windows XP Workstation Controls v1.2.1	8	1,330	734	55%	45%	596

*PCI DSS requirement 6.1 - Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor-supplied security patches installed.*

VCM can be used to automate the patching process to ensure that all critical security patches are deployed (PCI DSS Requirement 6.1) across the physical and virtual OSs in the environment (Windows, Linux, UNIX, Mac, etc).

*VMware Update Manager (VUM) should also be used to monitor any new updates and security patches from VMware.*

With VCM, organizations can create software packages, push packages to systems and guests, automatically find missing software, and remediate and install required software to non-compliant systems.

VMware Update Manager (VUM) should also be used to monitor any new updates and security patches from VMware, and used to patch and update virtual components (e.g. ESXi).

*Historically, logging on virtual components was used only for troubleshooting, but has evolved to meet common logging requirements and can be exported as syslogs.*

## 9. Logging and Monitoring

Section 10 of the PCI DSS has specific logging and monitoring requirements for all systems in the CDE. Historically, meeting these logging requirements was very challenging for virtual environments

since the logs were originally designed for troubleshooting and IT system administration.

Today, the logs generated in virtual environments contain more information than the logs from several years ago. Many virtual components, such as ESXi and vShield, can be configured to integrate with centralized logging and monitoring solutions, as well as follow the industry “syslog” standard for exporting and consolidation. Additionally, VCM can be used to ensure that logging settings are uniform across the environment and collect and/or parse logs from the guest OS. PCI DSS section 10 defines logging requirements in detail, and the remainder of this section will map the specific logging requirements to the tools/processes used today with VMware.

*Do not store all logs for the hypervisor on a host residing on the hypervisor. If there is an incident and the hypervisor is accessed, any VMs on the hypervisor can be altered, including log servers.*

It is important to note, the ability to meet these requirements with the various logging solutions available to ESXi will require an additional log management as well as collection products due to the native un-centralized manner in the way the tools and logs are organized within ESXi. Do not store logs for the hypervisor on a host residing on the hypervisor. Logs for the hypervisor should be stored separate from the hypervisor and not on a host residing on the hypervisor. This will help ensure that all activity to the hypervisor is reflected in its logs and an attacker isn't able to alter logs after gaining access to the hypervisor.

*The best way to meet PCI DSS 10.1 is to establish a centralized role-based access control (RBAC) system and link vSphere groups. Using local accounts for accessing the ESXi host is not recommended for PCI compliance.*

**PCI DSS 10.1: Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.**

The mechanism available for linking system events to specific user accounts is available through centralized role-based account management that is available with vSphere. While ESXi itself allows for individual account creation and permissions assignment or users and groups through Active Directory, the preferred method is to use the Active Directory User Access Control mechanisms provided in vSphere via vCenter, when possible. With vCenter and ESXi hosts joined to an Active Directory domain, Role-Based User Access controls can be implemented which allows access to ESXi hosts and administrative functions to be assigned to individual user accounts. This eliminates the need to rely on the root account or other generic administrative accounts. If Active Directory cannot be used, organizations should consider the use of additional access controls.

*The best way to meet PCI DSS 10.1 is to establish a centralized role-based access control (RBAC) system and link vSphere groups. Using local accounts for accessing the ESXi host is not recommended for PCI compliance.*

**PCI DSS Req 10.2: Implement automated audit trails for all system components to reconstruct the following events: individual access to cardholder data, admin actions, log access, invalid access, logging mechanisms used, initializing audit logs, creation and deletion of system-level objects.**

*vCenter Configuration Manager (VCM) provides audit control by tracking changes to the environment, verifies that audit trails are set up correctly, provides guest OS system logfile monitoring across the environment, and verifies that file permissions are set up correctly.*

Audit trails are critical for reconstructing events during a suspected compromise. They can help demonstrate that cardholder data was not compromised and can help limit the liability and forensic investigation needed. Robust logs must be kept to monitor and reconstruct events such as administrative privilege use, audit trail access and initialization, logical access attempts, creation and deletion of system objects and the use of authentication mechanisms. Each ESXi host runs a syslog service that collects messages from various components such as the VMkernel. These settings can be individually managed on the host or centrally managed through vCenter. You can reference the [vSphere Datacenter Administration Guide](#) (Chapter 14) for further information on the various log files, their locations and types of data each log file contains.

vCenter Server records system events and exposes them for viewing and download, as well as making them available through an event monitoring API. These events include the creation/deletion of accounts, enabling/disabling of admin permissions, users added/removed from groups and password update events. Events for a particular host are collected by and accessible from the vCenter Server that manages the host. While the monitored events include both security and system-state events, it is a valuable source that can be used to audit ESXi.

*Event logs directly from ESXi and vCenter follow different formats but include the information needed to meet PCI DSS 10.3.*

**PCI DSS 10.3: Record an audit trail that includes: ID, event, date, time failure/success, name of affected data, system component, or resource.**

The event logs that are collected by vCenter Server cover these requirements as well; however the format is different from syslog formats and should be reviewed for differences in formatting.

*Logging is normally stored in UTC time, not the local time.*

**PCI DSS 10.4: Using time-synchronization technology, synchronize all critical system clocks and times and ensure that the following is implemented for acquiring, distributing, and storing time.**

Time synchronization facilities in ESXi are available through the use of Network Time Protocol (NTP). PCI DSS requirement 10.4 directs that organization implement time synchronization technology such as NTP. However, it is important to note that some virtual components, by default, log in UTC time, not the local time. Even though an organization may update and set the host's time zone, additional reviews should be performed to ensure the time zone in use (actually used in logs, audit trails, etc.) is accurate.

*All ESXi hosts should use a designated, centralized time source for time synchronization.*

For large deployments, a good alternative practice is to use UTC time zone across all ESXi hosts to maintain consistency. Access to time facilities can be limited through proper assignment of permissions and should be implemented through RBAC mechanisms available in

vSphere. All ESXi hosts should use a designated, centralized time source for time synchronization and ensure that the centralized time source itself uses established, external time sources (i.e. Tick and Tock).

**PCI DSS 10.5: Secure audit trails so they cannot be altered.**

Securing audit trail and logging data on ESXi can be implemented through proper assignment of permissions to individual accounts. However, as mentioned in Requirement 10.1 above, application of this logical control should be carried out as part of the RBAC mechanisms available in vSphere and managed in vCenter. By using these mechanisms, you can leverage consistent permission application across all managed servers.

Since ESXi logs in syslog format, there are a variety of third party logging solutions which will accept ESXi logs.

Centralized backup of log and audit data can be done through the use of centralized log collecting systems that can collect syslog formatted data. Since ESXi logs in syslog format, there are a variety of third party logging solutions which will accept ESXi logs. As with most syslog services, the log collecting IP and port can be individually set. Please note that the additional audit data provided through the collection of events by vCenter Server can be redirected (e.g. RSA envision). However, this event data is not stored on the individual ESXi host, but the database of the vCenter Server that manages the host.

**PCI DSS 10.6: Review logs for all system components at least daily.**

Daily review audit and log data can be performed individually on each ESXi host, but most organizations find that impractical. Instead, log review should be performed through a centralized log system, SIEM, or centralized systems such as vCenter Server (Event auditing can only be done on the vCenter Server). vCenter Server provides basic review capabilities such as regular expression use and other filter capabilities that include date/time and specific host. However, with today's centralized log repository solutions (both appliance and software), it should be considered the back-up to an organization's primary logging solution.

Log review should be performed through a centralized log system, SIEM, or through centralized systems such as vCenter server.

vCenter Server has an alerting infrastructure that allows for different types of alerts and actions to be taken in response to generated events. The alerting capabilities (email, running a script, raise an SNMP trap, etc.) can be customized at a very granular level. Since this control is dependent on the proper configuration of alerts, organizations should pay careful consideration to the rules and logic behind alerts.

vCenter has an alerting infrastructure that allows for different types of alerts and actions to be taken in response to generated events.

**PCI DSS 10.7: Retain audit trail history for at least one year, with a minimum of three months immediately available for analysis (for example, online, archived, or restorable from back-up).**

*ESXi log retention is set by file size and not date, so organizations should ensure they establish the appropriate size to meet the one year requirement if they are not using a third-party logging solution.*

As mentioned previously, current logging solutions allow for granular control over retention policies and log backup management (on the centralized logging server/appliance, not ESXi directly). However, administrators should also adjust ESXi logging facilities to store 90 days of logging data locally to facilitate timely forensic requirements. It is important to note that ESXi logging facilities only allow for retention settings based on file size and file count, not date/time. Because of this limitation, space availability will have to be considered when implementing these settings. It is important to change log file storage to a separate partition reserved for log storage purposes. Proper choices in partition size, individual log file size and number of log files to maintain 90 days of logs can only be made through a trial and error process that is closely reviewed and adjusted as needed.

## **10. Managing Encrypted Data at rest and in motion**

Virtualization brings two new challenges to ensuring that data is encrypted at rest and in motion. The first is that systems are generally stored on a shared storage device. These systems can be accessed or copied by people with access to the storage device. Each device has its own set of access controls which can be used to monitor and log access to systems. VCM can be used to ensure that when systems are pulled from the device, they match approved baselines before going live. Also, vSphere can be configured to manage access to datastores. Each data store and port group can be configured so that only the proper systems, processes, and people have access to sensitive VMs stored in the database. Organizations should ensure that they limit users who can put VMs into port groups, and who can manage/access running VMs. Organizations should ensure that they do not take running snapshots (also known as dirty snapshots), if they contain sensitive data (such as encryption keys, encrypted databases, credentials, etc.). Many of these processes run in memory, but will be written to disk if taken as a snapshot. This can significantly change the risk and attack vectors for malicious users trying to access sensitive data.

*Always ensure that vMotion and other intra-host traffic occurs over a secure network, such as a dedicated VLAN with no other endpoints.*

Another area to consider is how VMs move from hardware to hardware. Most organizations deploy virtual environments across multiple physical servers, in multiple geographic areas. vMotion does not encrypt data as it moves systems from one location to another. There is a risk that the entire VM can be compromised if moved across an unencrypted channel in an untrusted network. Organizations that use vMotion should ensure they understand the networks and systems that the VMs traverse and implement appropriate protection.

*VMware products can leverage the vCenter Configuration Monitor File Integrity Service (CMFIS) to meet FIM requirements such as PCI DSS 11.5.*

## 11. File Integrity Monitoring

File Integrity Monitoring (FIM) is always challenging in any environment, including virtual environments. VCM can be used to check file and directory permissions and file checksums. This ensures that critical files are not altered, and match approved baselines. The FIM functionality of VCM can be used for Windows, Linux, and UNIX systems. Organizations can create templates of standard systems which can be compared to running systems. As the template is updated VCM can be used to dynamically check running systems.

*vShield Endpoint security can be deployed to meet PCI anti-virus requirements through an agent-less architecture. This enforces consistency and allows for great visibility across all VMs and hosts.*

## 12. Other Technology and Tools Available

VMware is constantly adding more tools and software to increase the security and compliance needs of the virtual community. One of the biggest challenges in a distributed and dynamic environment is ensuring that anti-virus solutions are running, active, updated, and logging. vShield Endpoint can be used to enforce and monitor agent-less anti-virus solutions on Windows VMs. Various anti-virus vendors have developed solutions which assist organizations with managing anti-virus on distributed VM environments. These agent-less solutions are more suited for PCI compliance as they are less prone to error and can be used by an assessor as a central location to ensure that anti-virus across all VMs and hosts is operating effectively.

More tools are continually being established and created to better address the unique challenges and opportunities for security in virtual environments.

## 13. Conclusion

Organizations can implement virtualization in PCI compliant environments. The simplest way is to virtualize all CDE components and run them on ESXi hosts that are segmented from the rest of the organization. Assessors and IT Administrators must be familiar with the unique risks of virtualization, and the benefits provided by different tools and products from VMware and other products which integrate with VMware's suite of tools.

*Conclusion: Organizations can use virtualization in PCI compliant environments if they are aware of the risks and tools available to manage security.*

Virtualization adds additional risks to their physical counterparts by adding additional layers and software which provides more attack vectors. However, with the proper configuration and tools, virtual environments can actually reduce the likelihood and impact of attacks, reduce the manual processes prone to human error, and can scale and validate compliance better than most physical environments.

## 14. About Coalfire

Coalfire is a leading assessor in the payment card space, validating PCI compliance across the largest service providers and merchants throughout the country. Coalfire conducts over 1,000 assessments each year, and is actively engaged with many of the leading technology vendors and service providers. For more information, go to [www.coalfiresystems.com](http://www.coalfiresystems.com). This whitepaper was authored by Tom McAndrew, with the assistance of Mike McGee and Josh Byrnes. For question or comments, please e-mail [virtualization@coalfiresystems.com](mailto:virtualization@coalfiresystems.com).

## 15. Resources

The following table provides a summary of common VMware products used to meet PCI compliance. An additional whitepaper will be released providing specific testing and configuration suggestions shortly.

For more information on compliance and VMware products:

[www.vmware.com/go/compliance](http://www.vmware.com/go/compliance)

For more information on the PCI DSS and other PCI guidance:

[www.pcisecuritystandards.org](http://www.pcisecuritystandards.org)

For more information on Coalfire Systems:

[www.coalfiresystems.com](http://www.coalfiresystems.com)

PCI DSS Req.	Description	VMware Product
1.1	Establish firewall and router configuration standards	vShield
2.1	Always change vendor-supplied defaults before installing a system on the network, including but not limited to passwords, simple network management protocol (SNMP) community strings, and elimination of unnecessary accounts.	vCenter Configuration Manager
2.2	Develop configuration standards for all system components. Assure that these standards address all known security vulnerabilities and are consistent with industry-accepted system hardening standards. Sources of industry-accepted system hardening standards may include, but are not limited to: Center for Internet Security (CIS) International Organization for Standardization (ISO) SysAdmin Audit Network Security (SANS) National Institute of Standards Technology (NIST)	vSphere Host Profiles vSphere VM Templates vCenter Configuration Manager
5.1	Deploy anti-virus software on all systems commonly affected by malicious software (particularly personal computers and servers).	vShield
6.1	Ensure that all system components and software are protected from known vulnerabilities by having the latest vendor supplied security patches installed. Install critical security patches within one month of release.	vCenter Configuration Manager vCenter Update Manager
6.2	Establish a process to identify and assign a risk ranking to newly discovered security vulnerabilities.	vCenter Configuration Manager vCenter Update Manager
7	Restrict access to cardholder data by business need to know	vCenter Server
8.1	Assign all users a unique ID before allowing them to access system components or cardholder data.	vCenter Configuration Manager vCenter Server ESXi
10.1	Establish a process for linking all access to system components (especially access done with administrative privileges such as root) to each individual user.	vCenter Configuration Manager vCenter Server vShield
10.2	Implement automated audit trails for all system components	vCenter Server vCenter Configuration Manager
11.5	Deploy file-integrity monitoring tools to alert personnel to unauthorized modification of critical system files, configuration files, or content files; and configure the software to perform critical file comparisons at least weekly.	vCenter Configuration Manager