TEVORA

VMware® Validated Design Compliance Kit for PCI DSS v3.2.1 Audit Guide

January 14, 2020

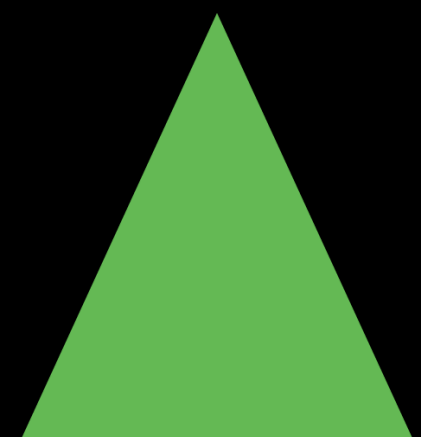

Table of Contents

Revision History

Date	Rev	Author	Comments	Reviewers
January 2020	1.0	Tevora	GA	Carlos Phoenix, Aleksandar Topuzov

Design Subject Matter Experts

The following people provided key input into this whitepaper.

Name	Email Address	Role/Comments
Christina Whiting	cwhiting@tevora.com	Co-Author
Brandon Richardson	brichardson@tevora.com	Co-Author
Carlos Phoenix	cphoenix1@vmware.com	Compliance and Cybersecurity SME, VMware

Trademarks and Other Intellectual Property Notices

VMware Validated Design for the Software-Defined Data Center

The VMware Validated Design architecture strives to balance security and innovation without sacrificing one for the other. Together, this by-design approach strengthens customers' confidence that, when they implement a VMware Validated Design for the Software-Defined Data Center (SDDC), they are getting a comprehensive software stack that not only supports their legislative and security needs but also helps meet the SDDC design objectives. In addition, the interoperability testing expected from a unified blueprint was extended to include compliance risk assurance through a comprehensive lifecycle development of the VMware Validated Design Compliance Kit for PCI DSS v3.2.1.

VMware Validated Design: Software-Defined Data Center Layer	Key Products
Virtual Infrastructure	VMware ESXi™, VMware vCenter Server® Appliance™, VMware NSX® Data Center for vSphere®, VMware vSAN™, VMware Cloud Builder™
Operations Management	VMware vSphere® Update Manager™ Download Service, VMware vRealize® Operations Manager™, VMware vRealize® Suite Lifecycle Manager, VMware vRealize Log Insight™, VMware Skyline™
Cloud Management	VMware vRealize Automation™, VMware vRealize Business™ for Cloud, VMware vRealize Orchestrator™
Business Continuity	VMware Site Recovery Manager™, VMware vSphere Replication™

Disclaimer (Tevora)

The opinions stated in this audit guide concerning the applicability of VMware products to the PCI DSS v3.2.1 framework are the opinions of Tevora. All readers are advised to perform individual product evaluations based on organizational needs.

For more information about the general approach to compliance solutions, please visit VMware ISBU Compliance Solutions or view the VMware Whitepapers published to the Tevora website. This audit guide has been reviewed and authored by Tevora's staff of information security professionals in conjunction with VMware, Inc.

Disclaimer (VMware)

This document is intended to provide general guidance for organizations that are considering VMware solutions to help them address compliance requirements. The information contained in this document is for educational and informational purposes only. This document is not intended to provide regulatory advice and is provided "AS IS." VMware makes no claims, promises, or guarantees about the accuracy, completeness, or adequacy of the information contained **herein**. Organizations should engage appropriate legal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements.

Executive Summary

Overview

The adoption of virtualization technologies across data centers is altering the audit landscape. Information technology assessors encounter VMware products without substantial technical guidance from regulators and standards bodies. The pace of innovation has caused assessors to develop their own best practices to assess virtualization technologies. VMware engaged Tevora to develop this audit guide to address compliance and technical concerns associated with virtual environments.

Implementing a virtual system is not the same as auditing a virtual system. The two viewpoints might have the technology in common, but they are often purposed with different objectives. To bridge this divide, VMware and Tevora are combining efforts to publish documentation as compliance kits to address both audiences. Each compliance kit is built to address a regulation, standard, or framework. The kit contains a configuration guide that supports the implementation of the VMware Validated Design, while the audit guide supports the auditing of the deployed solution.

Audit Guide Objective

The audit guide strives to empower key stakeholders with responsibilities for IT compliance (i.e., CISO, security administrator, internal audit, external audit) with information and guidance to evaluate security controls within the VMware Validated Design for the Software-Defined Data Center. The goal of this document is to make diverse stakeholders feel confident that the configuration of their SDDC will align with the intent of PCI DSS v3.2.1.

A key detail for the reader is that this guide supports but does not validate or concretely state an intended compliance outcome. The procedures outlined in the audit guide appendices can be used to produce evidence to audit the security configurations and leverage VMware's expertise to evaluate whether the SDDC is provisioned appropriately. Certifiable compliance is the responsibility of the organization and its designated parties.

How to Use This Audit Guide

The audit guide is constructed to be informative, comprehensive, and audit friendly. The authors not only are technologists but have also held positions responsible for IT compliance at various organizations. The guide assumes knowledge of the auditing process flow. Assessors can use this document to evaluate existing compliance requirements compared to the VMware Validated Design Compliance Kit for PCI DSS v3.2.1, identify control requirements necessary to meet compliance, and test security configurations.

The audit guide appendices outline how the SDDC can address PCI DSS v3.2.1 requirements across the high-impact level. Readers of the audit guide can gain an important tool to address regulatory needs and can apply the knowledge in gathering documentation to support security configurations often required to complete audit tasks.

The appendices are structured to support an audit strategy that focuses on evaluating the security configuration details on how the SDDC features conform to the control sets defined within. Assessors should marry this approach

and details to exhume product capabilities that provide evidence for use in formal audits. It is important to reiterate that although VMware Validated Design for the Software-Defined Data Center provides some capabilities to meet PCI DSS v3.2.1, it does not carry responsibility for certifying compliance.

By performing detailed reviews at multiple stages of your implementation process, you will find yourself well positioned to align your program with PCI DSS v3.2.1. No two organizations, industries, or frameworks are identical. Different needs, deployments, and configuration possibilities mean that there is no "one-size-fits-all" approach to securing or auditing an environment. This audit guide should be leveraged in addition to your internal Governance, Risk Management, and Compliance (GRC) program rather than substituted for it.

Anyone using this audit guide should make sure that they conduct regular internal reviews and understand internal requirements outlined by their organization and the requirements of outside assessors. Readers should also be aware of any specific details relating to their software deployments and their regulatory compliance needs of their organization. This guide should be leveraged throughout your implementation and then again post deployment to foster alignment to all in-scope PCI DSS controls.

These reviews should follow a similar pattern to what is shown in the following figure:

Figure 1: Internal Review Process

Tips for Auditing an SDDC

To complete an audit evaluation of the SDDC, it is imperative that you understand the architecture used to develop the VMware Validated Design Compliance Kit for PCI DSS v3.2.1. The kit uses a verifiable blueprint and model of security that supports PCI DSS v3.2.1. The SDDC is software based, which benefits from a level of abstraction that can be configured with granularity and precision without sacrificing operational efficiency.

Key Characteristics of a Virtual Environment

To better understand how to audit an SDDC, it is important to know how it differs from a traditional physical environment. Technical cornerstones such as servers, firewalls, and even storage arrays, while possessing features analogous to their physical counterparts, have several differences. Before diving into specific differences, understanding the basic breakdown of a virtual environment is important:

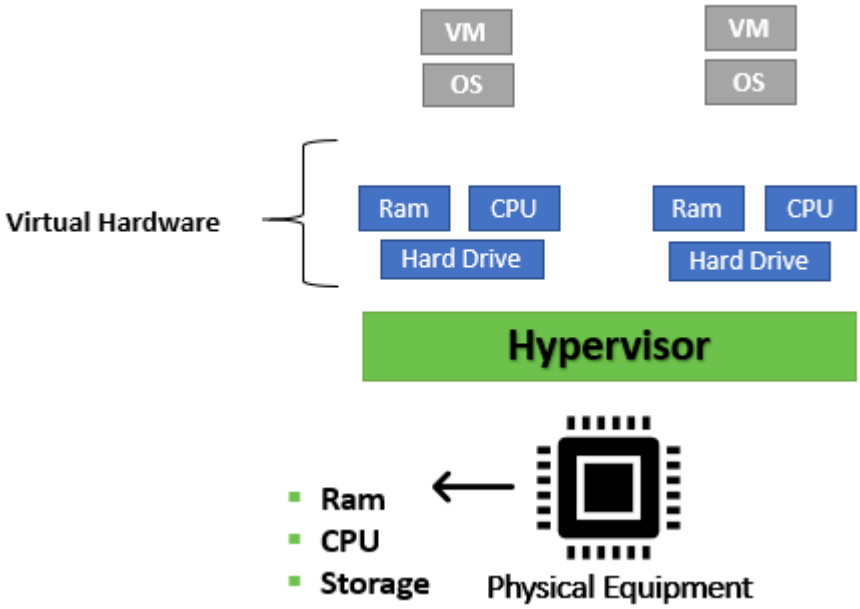

Figure 2: Breakdown of a Virtual Environment

At the core of any virtual environment, there is a physical server that is operating what is known as a "hypervisor." A hypervisor is simply the software that leverages the physical hardware, either directly or via a standard operating system (OS), to create and manage virtual machines (VMs). These machines can be workstations, servers, backup devices, or anything else you might require. Each virtual device is assigned virtual resources, which are segments of the overall physical equipment, which allow for specific OS, applications, or other tools to operate. Functionality is determined by the cloud provider, whether that is a private cloud hosted internally or services provided by AWS,Azure, or other public cloud provider, but the basic operations are similar.

With enough physical resources, namely RAM and disk space, there is effectively no limit to what you can host with a single server. Today, all critical components of IT infrastructure have some level of virtual counterpart. From

firewalls to switches to long-term storage devices, there is very little that can be achieved with a physical infrastructure that cannot be emulated by a virtual environment.

In practically every scenario, virtual counterparts are both cheaper and easier to deploy, although not necessarily to configure, than physical alternatives. The following is a breakdown of key differences between a few common technological components and their virtual counterparts:

Virtual Machines and Servers
Unlike physical machines, you can easily provision or deprovision VMs with any type of operating system you need, usually within minutes. This applies to additional storage or raw compute power as well, making tasks such as long-term data storage or load balancing simple. Securing these machines is easier as well because after a secure template is developed, you can leverage it across every other deployment of similar system down the line.

For all intents and purposes, a virtual server is a VM assigned to a specific task. It might run specialized software, akin to physical servers, or might simply be leveraged to manage a database or other dedicated service. VMs used as virtual servers will likely have more resources allocated to them, but there is no checkbox that transforms a regular VM into a server or vice versa.

Virtual Networking
There are virtual technologies that can replicate switches, firewalls, and network segmentation as a whole. These components, along with other tools, allow for a data center to direct and reconfigure traffic flows to best suit their compliance and operational needs. We have provided a brief outline of the different options and some additional features provided by virtual networking technology in the following sections.

Firewalls
Virtual firewalls are a type of software that can be placed at various areas within the virtual network, such as between VLANs or individual VMs. The virtual firewall can prevent the transmission/transfer of data, or files, by either unauthorized users or malicious insiders. Virtual firewalls are significantly cheaper than their physical counterparts, although they handle less network throughput. These firewalls can also be centrally managed and can have standardized configurations applied immediately without need for direct user interaction.

Switches
Along with the standard features such as packet forwarding, virtual switches can provide significant additional benefits not present within a physical switch. The biggest difference is that virtual switches can maintain the security and configuration standards of VMs as they move between physical hosts, eliminating a key risk facet associated with virtual systems.

VLANs
Virtual technology allows for segmentation that is strict enough to comply with all relevant legislation or industry requirements outlined in frameworks such as PCI DSS and ISO without requiring separate physical sets of networking equipment. Segmenting entire departments, or individual workstations, is easy and effective with virtualization and allows for both greater security and additional network control. This can all be accomplished without requiring several different sets of physical equipment, cables, and overall maintenance.

Additional Benefits and Risks

While virtual environments provide numerous benefits and cost savings, this does not mean that they are overall less risky than a physical setup would be. Instead, the risks are different. If a public cloud provider, such as Amazon, is being used, some areas such as physical security and hardware maintenance diminish as concerns, while other areas such as operating system selection or patch management become even more critical. Auditing virtual environments also brings new challenges, because direct access to the infrastructure in use by public cloud providers is not permitted.

Within virtual environments, east–west traffic describes the traffic within a data center such as server-to-server traffic. North–south traffic describes the traffic between a client and a server, which is the traffic between the data center and the network outside of the data center. In an SDDC, east–west traffic grows exponentially because many physical limitations are not present. A single server can host dozens or hundreds of workstations, services, or other critical infrastructure components that can all be communicating with each other. Processes such as VM migration greatly increase the amount of communication that exists within an SDDC, as VMs are moved between physical hardware components within the provider's environment. Accordingly, the opportunity for attackers or outsiders to obtain sensitive data is increased as well.

If the SDDC is operating within a public cloud environment, the differences are even more significant, as these providers usually operate on a co-tenant model. In a co-tenant model, physical equipment that is shared by VMs, communication infrastructure, routers, or any other virtual technology would then also be further segmented by individual tenants. This can create issues in managing specific devices and in patch management; however, these issues will be specific to each provider and each contract.

Virtual technology also produces a few specific technical risks that are unique to themselves. We have seen a rise in so-called "side-channel" attacks in recent years, which have taken on many forms. A common side-channel attack leverages the shared cache memory between VMs to obtain sensitive data such as encryption keys without compromising the host system. This means that even if your system is secure and hardened, attackers can still access critical information.

The feature set within the SDDC allows you to configure by default or selectively, to greatly reduce or even eliminate these risks within their environment. Some other common risks that persist across any type of virtual environment, regardless of scope and location, are outlined in the following sections.

Configuration Risk

Given that the VMware SDDC is entirely software based, the primary risk to this environment is from either software-specific vulnerabilities or from misconfigurations. Misconfigurations are one of the greatest threats associated with any environment, but they take greater precedence in a digital environment.

The VMware Validated Design was developed with software versions that are implemented in accordance with select best practices that help achieve the stated design objectives. This solution is tested for interoperability and scalability. A key goal with this approach is to minimize misconfigurations—thus, the need for such a detailed blueprint. The VMware Validated Design includes known issues, installation guidelines, software component lifecycles, as well as many other relevant implementation insights. If you operate in a highly regulated

industry or are processing personal information (i.e., subject to PCI DSS or CCPA), this risk can have major significance.

Software-Vulnerability Risk

VMware takes extensive steps to protect its offerings from security flaws and other vulnerability risks. Internal security programs and best practices operate “by design” to evolve methodologies of protection against new threats as they are discovered. This approach is followed throughout the development process. Products are also subject to intensive vulnerability scans and penetration tests prior to any full release or version update.

Architectural Risk

To help balance the threat posed by architectural misconfiguration or poor implementation, VMware created the Validated Design Compliance Kit for PCI DSS v3.2.1. The VMware Validated Design helps you implement a well-architected environment, decrease the risk of configuration errors, and provide procedures to audit your security configurations. Using the VMware Validated Design as a foundational architecture component, the approach outlined in the configuration guide can enhance the deployment of virtual architecture components.

To address architectural risk, use the procedures included in the audit guide appendices. The processes crafted by VMware act as constant reverification of the configuration and implementation steps necessary to secure an SDDC instance, while also meeting compliance needs for customers. Both built-in functionality and enhanced configurations are outlined in the appendices.

Components of the VMware Validated Design for the SDDC

There are four key objectives:

- Accelerate time to market
- Increase efficiency
- Improve IT agility
- De-risk deployments and operations

With key areas of virtualization designed to enhance efficiency and reduce risk at the software and architectural levels, the consistency provided in the VMware Validated Design stands as the backbone for virtualization best practices in a digital marketplace.

VMware Validated Design provides a detailed overview of several foundational software components related to launching and operating an SDDC. The VMware Validated Design also provides various use cases that can be used as templates to create an SDDC that addresses specific business concerns or compliance requirements.

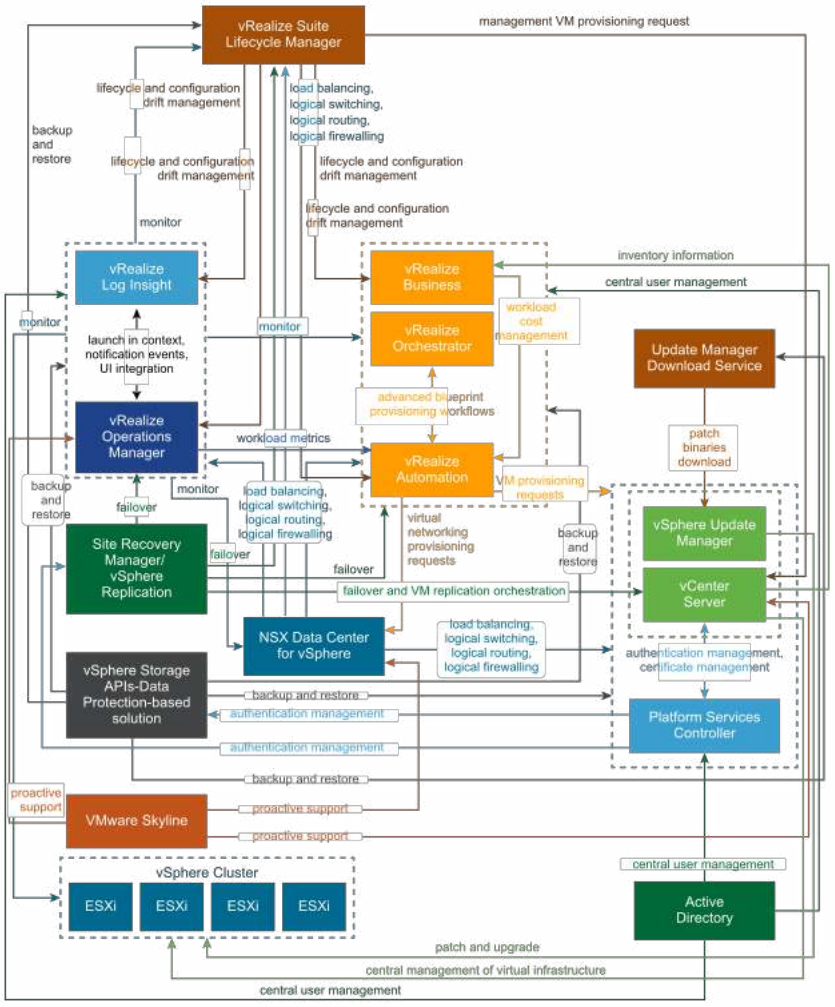

Figure 3: VMware Validated Design Depiction of SDDC Deployment

SDDC – People, Process, and Technology

VMware Validated Design Compliance Kit for PCI DSS v3.2.1 provides a technology solution to customers rather than the implementation of a PCI DSS v3.2.1 compliance program. Thus, the people and process components of this standard are not a major component of the kit. Features within the SDDC that enable organizations to enhance or craft a process based on compliance requirements can be classified as people or process controls.

As outlined in the PCI DSS v3.2.1 Product Applicability Guide (PAG), not all technology controls defined by PCI DSS are directly addressed by VMware technology. Some capabilities in the VMware Validated Design might support people and process controls, which are identified as "administrative" in nature because they relate to internal operational practices and not to specific technology capabilities. Further details on these categories and the aligned PCI DSS control families can be found in the PAG at https://www.tevora.com/wp-content/uploads/2019/05/VMware_PCIDSS_SDDC_PAG.pdf.

SDDC – Scope Based on Core and Administrative Controls

PCI DSS V3.2.1 outlines twelve (12) categories of controls defined as Requirements. The twelve Requirement sections each include sub-requirements related to achieving and maintaining the overarching control. As each Requirement must be either in-place or not applicable to achieve compliance, assessors (Qualified Security Assessors or QSAs) must address all Requirements during their assessment.

In addition to the PCI DSS, the PCI Security Standards Council (SSC) publishes a complementary report titled Information Supplement: PCI DSS Virtualization Guidelines (https://www.pcisecuritystandards.org/documents/Virtualization_InfoSupp_v2.pdf). The supplement is disseminated to help assessors, merchants, and service providers to understand, implement, and review virtualization technologies as they relate to the criteria established in the PCI DSS. The Information Supplement breaks down virtualization into five major categories: operating system (OS), hardware/platform, network, data storage, and memory. These categories, and their relation to the PCI DSS Requirements, help define how the features of different virtualization technologies impact compliance.

Auditing a Virtualized Versus Traditional Environment

VMware Validated Design Compliance Kit for PCI DSS v3.2.1 uses a Software-Defined Data Center, which is a virtual environment rather than a traditional physical environment for infrastructure. Auditing a virtual environment introduces some limitations to conduct an audit and raises the need for new methods. This section will highlight some of these methods and provide guidance on incorporating these methods into your existing Governance, Risk, and Compliance (GRC) strategy.

Audits focused on a virtual environment are conducted by conforming controls and software settings using command-line interface (CLI) or a graphic user interface (GUI). To facilitate this, the audit guide appendices outline procedures to test the configurations. These commands are needed for you to conduct an audit of both built-in and enhanced configurations related to deployed software components. The virtual nature of the evaluation provides the assessor with the opportunity to conduct many tests on the components, in most cases using commands that are outlined in the appendix.

The audit guide exists to assist with audits of virtual environments. This guide helps you confirm that your environments are configured to the specifications outlined in the compliance kit. The guide does not cover physical equipment, physical security, or hardware functionality. Take care to exercise due diligence when selecting or auditing these additional aspects, as any failure of physical security or hardware can impact your compliance with PCI DSS requirements.

VMware integrates security throughout the phases of its product development and solution design. Responsibility also rests on customers to ensure that proper installation, configuration, and ongoing operations are performed. Access controls, physical or otherwise, are the sole responsibility of the customers, as are software-specific settings and configuration management. Addressing these last two items can be done either by applying provided software documentation and auditing guidelines or by engaging a third party.

In virtualized environments, risks posed by software errors and misconfigurations can pose a higher risk than in more standard environments. Configuration management is a top priority for any organization or audit, as this is where customers' responsibilities begin. Given the ease with which virtual environments can be created and copied, configuration drift is a serious risk that you must carefully manage.

Additional differentiation can be seen in the layout of a virtual network versus a physical network. With the VMware SDDC, the entire network infrastructure has been virtualized, from servers to firewalls to internal communication pathways. Assessors must take care to review every aspect of the environment and understand what the scope of the virtualized environment is for the organization they are auditing, to ensure that all areas receive appropriate reviews and tests.

Considerations When Assessing a Virtual Environment Utilizing VMware Products

As stated above, VMware Validated Design Compliance Kit for PCI DSS v3.2.1 uses a Software-Defined Data Center, which is a virtual environment rather than a traditional physical environment. There are many considerations when accounting for products in use within a SDDC. Predominantly, virtualization will impact how users and administrators interact with the machines they use. There is no single way to assess a virtual environment but below is a list of the primary considerations for assessing virtual environments using VMware products.

First and foremost, assessing access controls evolves into a multi-tiered access audit. Assessors must review both the native operating system's users and access permissions, such as Active Directory for Windows systems and Access Control Lists for Linux, and the operating system utilized within the hypervisor, known as the guest OS, and even VMware administrative features such as vCenter or ESXi.

In conjunction with the layers of access controls, another primary consideration is the use of VMware product features, such as Lockdown Mode, which limit access to the host, or VM host firewall which helps achieve system isolation. Enabling such features can help limit risks by hardening systems per the criteria outlined in Requirement 2 and set access restrictions per Requirements 7 and 8. Enabling these features does not guarantee compliance against PCI DSS. Often, these features are not required to achieve compliance. However, when enabled, assessors, merchants, and service providers can leverage these tools to prove that the Requirements outlined in the applicable sections of the PCI DSS have been met by configuring the settings appropriately. If the provided features are not configured, merchants and service providers can manually harden systems and configure system and network devices to be compliant with all applicable PCI DSS Requirements.

Networking is also impacted when utilizing virtualization technologies. Security tagging and vLAN/vSwitches applied to ESXi hosts can be used to implement network segmentation. Through this, merchants and service providers can define their cardholder data environments (CDEs) and any demilitarized zones (DMZs). Network connectivity, though still handled by network devices such as firewalls and routers, can be directly controlled by the port and protocol configurations within the virtual machines and their respective management interfaces.

In-Scope VMware Product List

Software-Defined Data Center (SDDC)

VMware ESXi™, the industry-leading virtualization platform, provides a powerful, flexible, and secure foundation for business agility that accelerates the digital transformation to cloud computing and success in the digital economy.

VMware vCenter® Server provides centralized management of vSphere virtual infrastructure. IT administrators can provide security and availability, simplify day-to-day tasks, and reduce the complexity of managing virtual infrastructure.

VMware vSAN™ is a core building block for the Software-Defined Data Center, delivering enterprise-class, flash-optimized, and secure storage for all of a user's critical vSphere workloads.

Virtualized Networking

VMware NSX® Data Center for vSphere® is the network virtualization and security platform for the Software-Defined Data Center, delivering the operational model of a virtual machine for entire networks. With NSX, network functions including switching, routing, and firewalling are embedded in the hypervisor and distributed across the environment.

Appendix A: SDDC Product Capability Relationship with PCI DSS V3.2.1

Product	Capability ID	Product Capability	PCI DSS Requirements
ESXi	ESXI_001	Login attempts can be limited.	8.1.6
	ESXI_002	Concurrent sessions can be limited on web clients and virtual machine consoles.	8
	ESXI_003	ESXi can be integrated with Active Directory, or LDAP to employ unique user identifiers, instead of using the root account.	8.1, 8.1.1, 8.5.1, 8.8
	ESXI_004	A proof of maintenance log is available to report on archived maintenance activity.	10.2
	ESXI_005	Remote access to ESXi via SSH, or vSphere Web Client or API over HTTPS, can be configured as the secure communication protocol. Session identifiers are invalidated after session termination.	2.3
	ESXI_006	ESXi supports integration with external authentication solutions, such as Active Directory. Users that are members of a group that has been granted access to ESXi can sign in using single sign-on and will be able to log in using their user ID with elevated permissions.	8.1.7, 8.6
	ESXI_007	ESXi will perform the encryption on virtual machines that have been configured by vCenter to support VM Encryption. A third-party key manager solution is required to manage encryption keys. ESXi supports virtual machine encryption but requires a third-party integration.	4.3
	ESXI_008	ESXi can push logs to be stored in an external log repository that supports syslog, including vRealize Log Insight. In the event vRealize Log Insight is used, it can then apply tamper protection of logging that can be used during after-the-fact investigations without altering the event logs.	10.1, 10.2.2, 10.5, 10.5.2, 10.6, 10.6.1, 10.6.2
	ESXI_009	ESXi supports the Secure Boot feature to monitor firmware to validate version control and authorization. If the violation is detected during boot, the system will not boot up. If the violation is detected during run-time, the command will be rejected and not boot.	5.1.2, 6.6
	ESXI_010	ESXi has inherent capabilities to log events and specify frequency. The richness of logging can be adjusted, and the log retention based on disk space can be enhanced, through use of a separate logging repository via syslog or vRealize Log Insight.	10.2.2, 10.5, 10.5.2, 10.6, 10.6.1, 10.6.2
	ESXI_011	If ESXi has Secure Boot enabled, any attempt to execute unsigned binaries will result in an alert that will be sent to the vCenter instance.	10.1, 10.6, 10.6.1, 10.6.2
	ESXI_012	ESXi can be configured to display a login banner before granting access to the system.	8.6

	ESXI_013	ESXi provides memory safeguards to protect it from executing unauthorized code.	5.1
	ESXI_015	ESXi has the capabilities to establish firewalls using VLAN, to deny traffic by default, and to allow only explicitly designated traffic.	1.2.3
	ESXI_016	ESXi patching is performed via vCenter using vSphere Update Manager.	6.4.5, 12.11
	ESXI_017	The *vSphere 6.5 Security Configuration Guide* provides support for ESXi and vCenter hardening procedures.	12.1
	ESXI_018	Logon authentication techniques includes Two Factor Authentication.	8.3
	ESXI_019	ESXi supports configuration of access control via Single Sign-On, or Active Directory services, such as: requiring new users to change password on first logon, minimum password age, account lockout threshold or account lockout duration. Logon authentication techniques includes Two Factor Authentication.	8.2.6, 8.6
NSX for vSphere	NSX_V_001	Information protection can be implemented using policies that restrict access information flow based on network micro-segmentation.	4.1, 12.1
	NSX_V_002	Within the data plane, the guest introspection framework (host based) or Network Extensibility (redirect network flow to third-party appliances/tools) is supported by NSX, which can be accessed by third-party tools to support Intrusion Detection System (IDS).	10.2, 11.4
	NSX_V_003	The NSX Identity Firewall feature supports Role Based Access Controls (RBAC) to limit permissions that restrict viewing virtual machines. Also, micro-segmentation can be used to manage access to specific areas of the network using RBAC and minimize attack surface.	1.2, 1.3, 7.2, 8.1
	NSX_V_004	A proof of maintenance log is available to report on archived maintenance activity. These logs are captured at key components: NSX Manager (Management Plane) and vCenter (Data Plane). For a consolidated view, logs can be pushed to a syslog server or vRealize Log Insight.	10.1, 10.2
	NSX_V_006	Session lockouts are enforceable and require users to re-authenticate after a session time-out.	8.1.8
	NSX_V_007	Account lockout threshold can be altered.	8.1
	NSX_V_008	NSX can push logs to be stored in syslog audit repositories, including vRealize Log Insight. NSX supports multiple log repository servers to enhance tamper protection of logging that can be used during after-the-fact investigations without altering the event logs.	10.2
	NSX_V_009	NSX can be used to monitor the network using logging of firewalls and other traffic. This can be used to support monitoring the system for inappropriate usage and other security violations. Use of the NSX Application Rule Manager tool can monitor enforcement of access rules.	10.2
	NSX_V_010	NSX provides monitoring of the system using event logs and other security logs to identify abnormal activity. The	10.2, 11.4

		NSX NetX feature can redirect network traffic flow to be redirected to third-party Intrusion Detection System (IDS) solution on a per security policy.	
	NSX_V_012	NSX can isolate any devices that are out of compliance and restrict their access to the network, if the device is tagged as rogue and a policy defined to isolate devices that have this tag. NSX can quarantine any devices identified as rogue devices using the Guest Introspection Framework.	1.2, 10.1, 11.1
	NSX_V_013	NSX can use micro-segmentation to establish processing domains based on access rights and user privileges. Granularity around trust can be defined as a virtual NIC, or more broadly as a region, for both static infrastructure and dynamic logical objects.	1.3, 7.1, 7.2, 8.3
	NSX_V_014	NSX can restrict network traffic based on system security classification, which can be defined using static objects and dynamic objects. Access control for objects can be restricted based on security rules and tags.	1.3, 7.1, 7.2, 8.3
	NSX_V_016	Using NetX API, NSX can support integration with third-party intrusion detection systems (IDS) to support responses in network locations, or granular to VM/workflow between VMs. In addition, NSX can use Guest Introspection to further enhance IDS responses.	10.2, 11.4, 12.10
	NSX_V_017	NSX can manage all internal network connections and provides documentation to describe the networking components available for deployment.	1.2, 1.3, 2.4
	NSX_V_018	NSX can manage external network connections through the NSX Edge gateway, firewall, VPN, or SSL through Load Balancer. This includes establishing a boundary defense.	1.2
	NSX_V_019	Using the NSX Edge firewall, distributed firewall, Guest Introspection (within the VM) and third-party NetX API (network enforcement), NSX can prohibit systems from connecting directly to external networks.	10.2, 11.4
	NSX_V_020	NSX can be implemented with a fault-tolerant architecture; documentation supporting this design is available.	
	NSX_V_022	All capabilities of NSX can be programmatically created by Rest API to segregate applications and databases that can restrict information in an internal network zone.	1.2, 1.3.6
	NSX_V_023	NSX can apply configuration standards and remove unnecessary functionality using Rest API, Guest Introspection, and distributed firewall specifically to protocols, ports, applications, and services in the firewall and router configuration standard.	1.1, 2.2
	NSX_V_024	NSX can be used to configure traffic including firewall deny all traffic by default, explicit exceptions for designated traffic, restricting outbound traffic, protecting devices from outbound connections, protecting devices to deny inbound connections, managing IP addresses in DHCP, assigning or reserving static IP addresses in DHCP.	1.1, 1.2

	NSX_V_027	In the event of fail-safe procedures, NSX can move around machines to other recovery networks via automated quarantine actions.	12.10.1
	NSX_V_028	NSX provides a dashboard to monitor the platform's health, which can inform users around maintenance information of the platform itself.	10.6
	NSX_V_030	NSX includes some Denial of Service (DoS) attack prevention mechanisms, which may support detection processes but will not monitor and detect DoS before the attack occurs.	5.1, 6.5.5
	NSX_V_031	NSX provides stateful firewall capabilities that can support adding devices requiring access control based on an Access Control List.	1.2, 1.3, 7.2
	NSX_V_032	NSX supports least privilege around workloads and provides four different roles within NSX to support the principle of least privilege (enterprise administrator, NSX administrator, security administrator, and assessor/read only).	7.1, 7.2
	NSX_V_035	The NSX appliance provides access via SSH, which can also be disabled. Access control to the NSX appliances can enforce password parameters: length, requiring password change upon first login, and account lockout duration.	8.1, 8.2.3
	NSX_V_036	NSX provides and maintains a system hardening guide.	2.2
vCenter	VCENTER_001	vCenter supports access control configuration including session time-out, login attempts, account lockout threshold, account lockout duration, minimum password age, and requiring re-authentication.	8.1.6, 8.1.7, 8.2.6, 8.6
	VCENTER_002	Concurrent sessions can be limited on web clients and virtual machine consoles.	7.1, 7.1.1
	VCENTER_003	vCenter employs unique user identifiers through Platform Services Controller™, which manages integration with SSO. Unique user identifiers can be assigned using Platform Services Controller.	8.1, 8.1.1, 8.5.1, 8.8
	VCENTER_005	Assignment of elevated privileges can be restricted to only those users that are approved as designated system administrators.	7.1
	VCENTER_006	vCenter can support an organization's continuity plan by providing workload management in the event of a host system disruption. However, this capability is not a robust continuity planning solution.	6
	VCENTER_007	vCenter can list all the virtual machines and support creating an inventory of technology systems.	2.4, 9.9.1
	VCENTER_008	Remote access to vCenter via SSH, or vSphere Web Client or API over HTTPS, can be configured as the secure communication protocol. For the vCenter Server Appliance, it runs on Linux and can be restricted to accept only HTTPS. Session identifiers are invalidated after session termination.	8.6
	VCENTER_009	vCenter can be configured to log out inactive sessions. By default, inactivity is set to log out after 15 minutes.	

	VCENTER_010	vCenter can configure encryption parameter designation on a VM-by-VM basis. ESXi performs the actual encryption on the VM. Third-party key manager solution is required for encryption key management.	4.3
	VCENTER_011	vCenter can push logs to be stored in an external log repository that supports syslog, including vRealize Log Insight. In the event vRealize Log Insight is used, it can then apply tamper protection of logging that can be used during after-the-fact investigations without altering the event logs.	10.1, 10.2.2, 10.5, 10.5.2, 10.6, 10.6.1, 10.6.2
	VCENTER_012	vCenter supports monitoring a set of standardized settings to monitor, which may indicate inappropriate usage or security violations. Alarms and alerts can be configured to notify users via email when triggered.	8.6, 10.1, 10.2.2, 10.5, 10.5.2, 10.6, 10.6.1, 10.6.2, 11.4, 12.3, 12.3.5
	VCENTER_013	vCenter has inherent capabilities to log events and specify frequency. The richness of logging can be adjusted, and the log retention based on disk space can be enhanced through use of a separate logging repository via syslog or vRealize Log Insight.	10.2.2, 10.5, 10.5.2, 10.6, 10.6.1, 10.6.2
	VCENTER_014	vCenter can be configured to display a login banner to users before granting access to the system.	8.6
	VCENTER_015	vCenter supports enhanced logging of audit-level events to support third-party integration with tools such as Introduction Detection Systems (IDS).	10.1, 10.2.2, 10.5, 10.5.2, 10.6, 10.6.1, 10.6.2
	VCENTER_018	vCenter can be run on a Linux appliance that is configured to restrict network traffic through use of a software firewall, which is restricted to only necessary ports during the installation. However, if vCenter is run on a Windows appliance, the network traffic and firewall is inherited based on the user's configuration of the Windows appliance.	1.2.3, 8.6
	VCENTER_019	vCenter can manage the encryption of virtual machines (applying encryption or removing encryption) and matching keys using a third-party key management solution.	4.3
	VCENTER_021	vCenter can patch ESXi hosts through vSphere Update Manager.	6
	VCENTER_023	The *vSphere 6.5 Security Configuration Guide* provides support for ESXi and vCenter hardening procedures.	6
vSAN	vSAN_001	Network encryption of the replication traffic data for new and existing replications can be enabled to enhance the security of data transfer .	6.4.2, 7.1.2, 7.1.3, 7.2.2, 8.1.2, 8.1.4
	vSAN_002	Logging capabilities can be enabled and customized to capture event information.	10.1, 10.2.2, 10.5, 10.5.2, 10.6, 10.6.1, 10.6.2
	vSAN_003	Logging can be synchronized to system clocks (NTP) and also capture a date and time stamp.	10.3.3, 10.4
	vSAN_004	vSAN can push logs to be stored in vRealize Log Insight. A default vSAN dashboard is available in vRealize Log Insight as a content pack.	9.9, 10.1, 10.2.2, 10.5, 10.5.2, 10.6, 10.6.1, 10.6.2

	vSAN_005	Session lockouts are enforceable and require users to re-authenticate after a session time-out, which are controlled by vCenter or ESXi.	8.1.8, 12.3.8
	vSAN_006	Encryption at rest can be performed for objects residing on the vSAN datastore (both in cache and long-term capacity storage media). However, a third-party key manager will be required to store and rotate keys.	4.3
	vSAN_008	Maintenance activity is logged and can be accessed via reports, which can be archived for historical reference. The maintenance logging information is captured at each component vCenter, ESXi, and vSAN, which can be holistically analyzed via vRealize Log Insight or customized.	9.9, 10.1, 10.5, 10.5.2, 10.6, 10.6.1, 10.6.2
	vSAN_009	Storage size can be adjusted to prevent exceeding capacity. This can be adjusted by adding physical devices or adding vSphere hosts, without a limit to file or block storage size.	
	vSAN_010	Cryptographic management features supported include rotation of keys via User Interface or API integration, changing Key Manage System (KMS) providers, and broadly enabling or disabling encryption. These capabilities can be used to support cryptographic procedures.	4.3

About VMware

VMware, a global leader in cloud infrastructure and business mobility, accelerates our customers' digital transformation journey by enabling enterprises to master a software-defined approach to business and IT.

With the VMware Cross-Cloud Architecture™ and digital workspace solutions, organizations are creating exceptional experiences by mobilizing everything; differentiating and responding faster to opportunities with modern apps hosted across hybrid clouds; and safeguarding brand and customer trust with a defense-in-depth approach to security.

The VMware Cross-Cloud Architecture extends the company's hybrid cloud strategy with new public and private cloud capabilities that enable enterprises to run, manage, connect, and secure their applications across clouds and devices in a common operating environment. As the world's most complete and capable hybrid cloud architecture, the VMware Cross-Cloud Architecture enables consistent deployment models, security policies, visibility, and governance for all applications, running on premises and off, regardless of the underlying cloud or hypervisor.

About Tevora

Tevora is a leading management consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. We offer a comprehensive portfolio of information security solutions and services to clients in virtually all industries and also serve institutional and government clients.

Tevora's leaders are professionals with years of experience and records of accomplishments in technology as well as business. This dual background means that we understand the importance of growth and profitability and our solutions are designed to enhance both.

As a consulting firm that has the ability to fully implement whatever it recommends, Tevora works with all of the industry's top vendors, yet is beholden to none. We are completely vendor-independent and select best-of-breed products tailored exclusively to our clients' needs. Security is our only business and our single-minded focus on anticipating and solving client problems has been described as "obsessive." We consider this a fair assessment.

Our hard work and dedication has established us as a reliable partner CTOs CIOs, and CISOs can depend on to help protect against threats, both internal and external. With Tevora as a partner, business leaders can devote their energies to enhancing the overall value of information technology to their enterprise.

Tevora is a Qualified Security Assessor (QSA) and Payment Application Qualified Security Assessor (PA-QSA) in good standing with the PCI Security Standards Council. Tevora is also a DVBE (Disabled Veteran Business Enterprise) certified by the California General Services Department (Cert REF# 32786).

For more information please visit www.tevora.com.

TEVORA

Go forward. We've got your back.

Compliance – Enterprise Risk Management – Data Privacy – Security Solutions – Threat Management