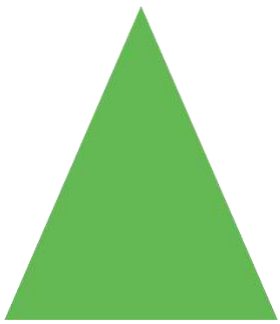
TEVORA™

# VMware® Software-Defined Data Center (SDDC) Product Applicability Guide for PCI DSS

March 11, 2021







# Table of Contents

# Revision History

| Date | Rev | Author | Comments | Reviewers |
|---|---|---|---|---|
| May 2019 | 1.0 | Tevora | Initial Draft | VMware |
| Oct 2020 | 1.1 | Tevora | Yearly Updates | VMWare |

# 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 |
| Anir Desai | adesai@tevora.com | Co-Author |
| Mikayla Bartell | mbartell@tevora.com | Co-Author |
| Carlos Phoenix | cphoenix1@vmware.com | Global Cyber Strategist, VMware |
| Jerry Breaud | jbreaud@vmware.com | Director, Product Management, Compliance Solutions, VMware |

# Trademarks and Other Intellectual Property Notices



| Solution Area | Key Products |
|---|---|
| Software-Defined Compute | VMware ESXi™, VMware vCenter®, VMware Cloud Foundation™, VMware vSAN™, VMware vCloud Director®, VMware vCloud Director Extender, VMware vCloud ® Usage Meter |
| Software-Defined Networking | VMware NSX®, VMware NSXT® |
| Management and Automation | VMware vRealize® Network Insight™, VMware vRealize Automation™, VMware vRealize Orchestrator™, VMware vRealize Log Insight™, VMware vRealize Operations Manager™, VMware AppDefense™, VMware Identity Manager™ |
| Disaster Recovery Automation | VMware Site Recovery Manager™, VMware vSphere®Replication™, VMware vCloud Availability for vCloud Director® |

## Disclaimer (Tevora)

The opinions stated in this guide concerning the applicability of VMware® products to the PCI DSS 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 Solution Exchange: Compliance and Cyber Risk Solutions. This whitepaper 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 assurances 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

## Background

This Product Applicability Guide (PAG) will provide an evaluation of VMware products that make up and support the Software-Defined Data Center (SDDC), and how they may support the Payment Card Industry Data Security Standard, v3.2.1 (PCI DSS/PCI) controls. These products virtualize and abstract the physical technology layers such as compute, storage, and network, the essence of an SDDC. The changing technology landscape that is modernizing the data center is also modernizing the virtual desktop environment and mobile device management while making inroads to consolidate and automate Information Technology (IT) resources. VMware prioritizes data protection and system security features within the SDDC. The VMware Compliance Solutions team developed a framework that incorporates SDDC product capabilities aligned to PCI DSS controls. The product capabilities and framework of this PAG used NIST 800-53 as their foundational security framework to create a series of standards. These standards have then been used to illustrate how VMware products and their capabilities apply to other industry frameworks such as NIST 800-171 and PCI DSS.

VMware engaged Tevora, an independent third-party IT audit firm, to conduct a review of the SDDC and VMware Cloud™ solution's alignment to PCI DSS. This document is the culmination of Tevora's discussions with VMware product teams to perform a thorough evaluation of VMware product capabilities mapped to PCI DSS requirements.

Tevora is a leading security consulting firm specializing in enterprise risk, compliance, information security solutions, and threat research. Tevora offers a comprehensive portfolio of information security solutions and services to clients in virtually all industries. This PAG will navigate readers through the PCI DSS standard and highlight applicable VMware product capabilities.

## VMware SDDC and PCI DSS

Today's infrastructures are heterogeneous in nature, built upon collaborations between internally constructed products and third-party sourced components, all guided by a customer's complex business and compliance requirements.

VMware approaches compliance with a view that understands the complexity in environments and addresses those areas where virtualization can be used to develop a more secure environment. This focused view on compliance is reflected in the VMware Compliance Solutions framework, which allows for a wide-ranging adoption of regulatory controls.

The phrase "security by design" identifies architectural decisions and default settings inside VMware products that are integrated into the product lifecycle. This approach reflects the process VMware follows to weave in security through all stages of the product lifecycle, and not as an afterthought. This overlap between products and compliance requirements marries security and non-security product capabilities in an improved way to also achieve operational innovation. Due to the breadth of the NIST compliance framework, VMware selected NIST 800-53 as its foundation for all future PAGs including PCI DSS and as the acknowledgment across industry standards that have been derived from the larger NIST risk framework.

## What is SDDC?

The Software-Defined Data Center architecture creates a completely automated, highly available environment for any application, and any hardware. SDDC can be used in any type of cloud model, and extends the existing concepts associated with the cloud such as abstraction, pooling, and virtualization across the cloud environment. Features of the SDDC can be deployed as a suite or can also work independently to allow for a controlled deployment over time.

## What is PCI DSS?

The Payment Card Industry Data Security Standard (PCI DSS) is an information security standard for organizations that handle branded credit cards from the major credit card brands. The standard was created to increase security around cardholder data and protect consumers. This standard applies to any organization that stores, processes or handles cardholder data.

Cardholder data can consist of several items, including:

- Primary Account Number (PAN)
- Name of the cardholder
- The Card's expiration date
- The Card's service code

An individual business interaction with cardholder data will vary depending on their defined operations. This underscores that there is no one-size fits all recommendation to secure a cardholder data environment (CDE). The responsibility resides with the individual business to certify they appropriately assess what requirements fit their environment to adequately protect cardholder data along PCI DSS standards.

Validation of compliance is performed annually, either by an external Qualified Security Assessor (QSA) that creates a Report on Compliance (ROC) for organizations handling large volumes of transactions, or by Self- Assessment Questionnaire (SAQ) for companies handling smaller volumes.

As with many security standards, PCI DSS takes a variety of its intentions from NIST 800-53 as guidance for defense in depth security within the cardholder environment.

# Introduction

## What is PCI DSS v3.2.1?

PCI DSS v3.2.1 is an updated version of the PCI Data Security Standard originally developed by PCI Standards Council in 2004. This version considers evolving technologies and threat vectors to consumers, merchants, and other entities within the transaction chain.

## How does PCI DSS work?

The PCI DSS standard requires organizations to comply with a robust set of requirements. The criteria are broken down into 6 objective areas and 12 requirements (listed below). Each requirement has a set of controls, the necessary testing procedures to certify that they are implemented appropriately with expert guidance.

- Build and Maintain a Secure Network and Systems
  - Requirement 1: Install and maintain a firewall configuration to protect cardholder data
  - Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Protect Cardholder Data
  - Requirement 3: Protect stored cardholder data
  - Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Maintain a Vulnerability Management Program
  - Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
  - Requirement 6: Develop and maintain secure systems and applications
- Implement Strong Access Control Measures
  - Requirement 7: Restrict access to cardholder data by business need to know
  - Requirement 8: Identify and authenticate access to system components
  - Requirement 9: Restrict physical access to cardholder data
- Regularly Monitor and Test Networks
  - Requirement 10: Track and monitor all access to network resources and cardholder data
  - Requirement 11: Regularly test security systems and processes.
- Maintain an Information Security Policy
  - Requirement 12: Maintain a policy that addresses information security for all personnel.

The scope of the PCI environment varies from organization to organization. VMware products help enforce controls configured by each client based on their individual environment. Organizations need to define the scope of their cardholder environment and controls.

# Scope and Approach

The SDDC and VMware Cloud platform covers a wide number of products and architectures. These platforms and each of their component products contain features that can be mapped to some PCI DSS requirements. Of the 12 total requirements, 10 had mapping overlaps to VMware software capabilities. This guide expands to account for all products underneath the SDDC umbrella. The scope of this guide is limited to those requirements supported either technically or through direct API integration. People and process controls are defined as administrative controls in support of PCI DSS requirement intents.

## What Is a Cardholder Data Environment?

The CDE is the key area in question within PCI DSS. The CDE can be described as any computer system or network that either processes, stores, or transmits cardholder data or other sensitive payment information. The environment extends to include any device that maintains a direct connection to the devices located within a CDE as outlined above.

The CDE can include but is not limited to any of the following devices:

- Firewalls
- Switches
- Routers
- Access Points
- Point-of-sale (POS) Systems
- Point-of-interaction (POI) Devices
- Servers (including web servers, application servers, or database servers)
- Any application that accepts payments
- Any associated virtual components (including virtual machines (VMs) and virtual networking devices)
- Third-party support staff or systems

## Our Approach

This Product Applicability Guide (PAG) is intended to provide information for all security and compliance practitioners on Tevora's recommended usage of the VMware technical stack to address regulatory compliance obligations and enhance the security of their services through the security and compliance framework of PCI DSS. It is up to each organization to identify how their compliance will be stated and the expanse of their CDE. The PAG focuses on capabilities of the SDDC product and VMware Cloud at the requirement level. A technical whitepaper, to be released later, will compile information gathered within this PAG and apply to each individual PCI DSS requirement and their underlying controls.

Appendix B outlines specific product capabilities for SDDC and VMware Cloud, and their alignment to PCI DSS requirements.

In addition to the PCI DSS standard requirements, 11 security lenses were used to serve as a baseline to evaluate SDDC and VMware Cloud products. From the ground up, VMware strives to design, define, and deliver compliance solutions to customers. The compliance solution begins with a compliance context (e.g., requirements from the appropriate standards in question). Next, the technical requirements applicable to the VMware products are mapped to in-scope compliance requirements. Finally, an independent audit evaluation of the design is conducted. The output is a solution that has interwoven compliance requirements into the end solution available to customers. Below is an overview of this process.

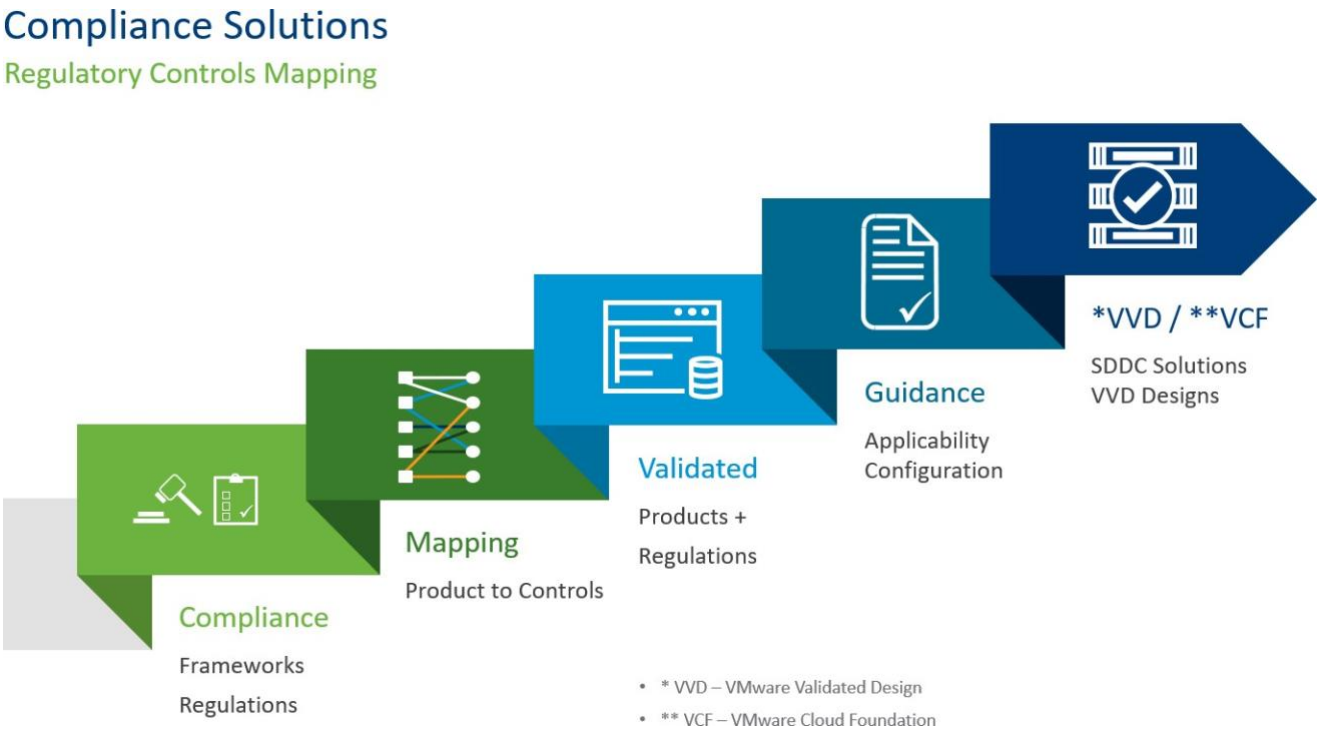



Exhibit 1: VMware Compliance Solutions Regulatory Controls Mapping

Outside of the process described above, these 11 areas are broad categories of controls that are implemented within today's security programs. They can be used to further understand the broader technology concepts used to build security architectures and to implement controls to mitigate risks.

The eleven security lenses include:

- Automated Security
- System Hardening
- Compliance Validation
- System Access
- Data Segmentation
- System Monitoring
- Data Encryption & Protection
- Network Protection
- Endpoint Protection
- Trusted Execution/Secure Boot
- Software Development Lifecycle (SDLC)

Evaluating the SDDC and VMware Cloud through the additional layer of security lenses helps security and compliance practitioners understand how products deliver the features required not only to support compliance with the PCI DSS standard but also to comport with general security best practices.

Tevora reviewed the high-level product design, followed by a detailed examination of data flows, features, architectures, and capabilities across all in-scope products to identify applicable controls. The testing considered all potential configurations that allow SDDC products to support each requirement.

This guide provides executives, technology experts, and security and compliance practitioners with insight to enhance security and compliance postures using VMware products. The SDDC's flexibility in feature deployment allows for connection with preexisting systems to further fortify security, privacy, and compliance. Understanding this flexibility is key to then understanding how VMware products can be deployed with continuous compliance in mind.

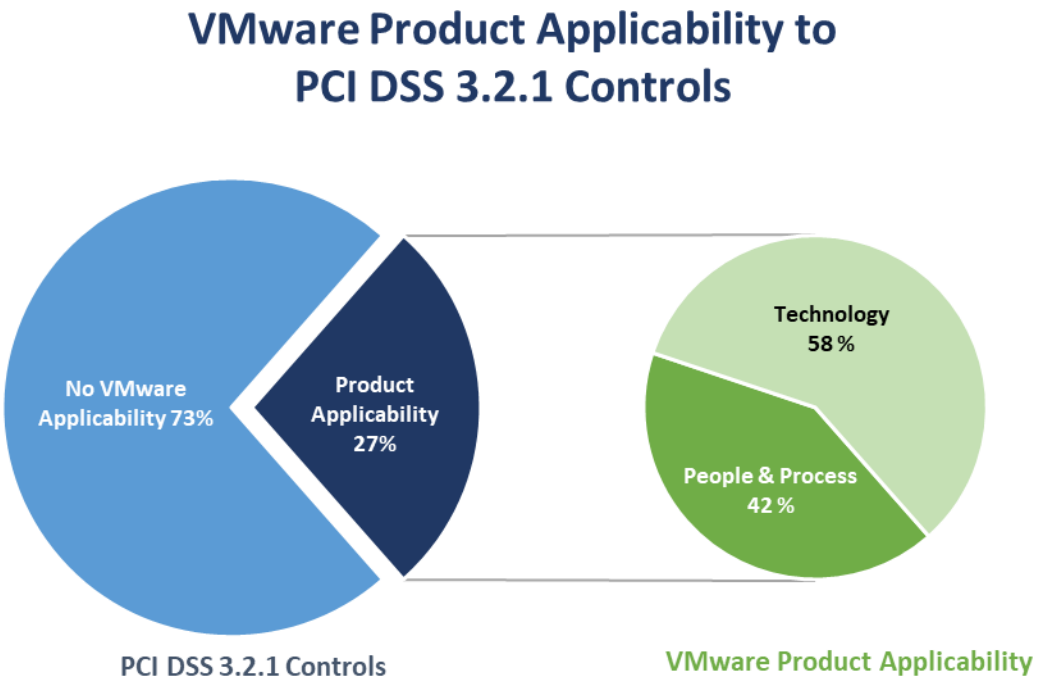



Exhibit 2: Percentage of SDDC Products that are capable of meeting the PCI DSS (v. 3.2.1) control.

# In-Scope VMware Product List

## Software-Defined Data Center (SDDC)

**VMware ESXi™6.0 update 3, 6.5, 6.7 update 2 – ESXi** is a purpose-built bare-metal hypervisor that installs directly onto a physical server. With direct access to and control of underlying resources, ESXi is more efficient than hosted architectures and can effectively partition hardware to increase consolidation ratios and cut costs for customers.

**VMware vCenter® 6.0 update 3, 6.5, 6.7 update 2 – vCenter** provides centralized management of VMware vSphere® virtual infrastructure. IT administrators can prioritize security and availability, simplify day-to-day tasks, and reduce the complexity of managing virtual infrastructure.

**VMware vSAN™ 6.2, 6.5, 6.6, 6.7 update 3 – 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.

## VMware Cloud Provider Platform

**VMware vCloud Director® 8.2, 9.1, 9.5, 9.7, 10.0 – vCloud Director** is the VMware flagship cloud management platform for cloud providers. vCloud Director enables cloud providers to deliver differentiated cloud services on their VMware cloud infrastructure and provides enterprises with self-service cloud capabilities.

**VMware vCloud Director Extender 1.1 – vCloud Director Extender** provides the ability to connect vCenter environments on-premises to a cloud based on vCloud Director to securely migrate virtual machines and extend virtual networks to the cloud. vCloud Director Extender provides seamless hybridity between on-prem and cloud environments based on vSphere.

**VMware vCloud Usage Meter 3.6.1, 4.1 – vCloud Usage Meter** helps cloud providers access VMware resources on a consumption-based monthly subscription, including vCloud Usage Insight, a SaaS tool that provides automated usage reporting, simple onboarding, secure data transfer and aggregation of usage across all contracts and sites.

**VMware vCloud Availability 3.0-** provides vSphere native replication of workloads for disaster recovery or migration purposes between vCloud Director organization virtual data centers. The solution is compatible to the vCloud Director self- service user interface (UI) or standalone and features symmetric source or destination execution of replication, migration, failover and failback of workload virtual machines and VMware vSphere vApps™ within vCloud Director. Using a consumption model, cloud providers are able to monetize their infrastructure by driving more breadth in their portfolios by offering additional managed or self-service disaster recovery and contingency planning services between cloud instances on a tiered basis and drive professional service opportunities.

## Virtualized Networking

**VMware NSX® (NSX-V) 6.3.5, 6.4.5, 6.4.6 – NSX** is the network virtualization and security platform for the Software- Defined Data Center (SDDC), 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.

**VMware NSX-T® 2.4, 2.5 –** NSX is the network virtualization and security platform for the Software-Defined Data Center (SDDC), 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.

## VMware vRealize® Suite

**VMware vRealize Operations Manager™ 6.6, 7.5, 8.0 – vRealize Operations Manager** is designed to automate and simplify the performance, troubleshooting, capacity, cost planning, and configuration management of applications and infrastructure across physical, virtual, and cloud environments.

**VMware vRealize Log Insight™ 4.5, 4.6, 4.7, 4.8 – vRealize Log Insight** delivers heterogeneous and highly scalable log management with intuitive, actionable dashboards; sophisticated analytics; and broad, third-party extensibility, providing deep operational visibility and faster troubleshooting.

**VMware vRealize Network Insight™ 3.4, 4.0, 4.1, 4.2, 5.0 – vRealize Network Insight** delivers intelligent operations for software-defined networking and security. It helps customers build an optimized, highly available, and secure network infrastructure across multi-cloud environments. It accelerates micro-segmentation planning and deployment, enables visibility across virtual and physical networks, and provides operational views to manage and scale NSX deployments.

**VMware vRealize Orchestrator™ 7.3, 7.4, 7.5, 7.6, 8.0 – vRealize Orchestrator** is a powerful automation tool designed for system administrators and IT operations staff who must streamline tasks and remediation actions and integrate these functions with third-party IT operations software.

## Business Continuity

**VMware Site Recovery Manager™ 6.5, 8.2 – Site Recovery Manager** is the industry-leading solution to enable application availability and mobility across sites in private cloud environments. It is an automation software that integrates with an underlying replication technology to provide policy-based management, non-disruptive testing, and automated orchestration of recovery plans. This provides simple and reliable recovery and mobility of virtual machines between sites, with minimal or no downtime.

**VMware vSphere Replication™ 6.5, 8.1, 8.2 – vSphere Replication** is an extension to VMware vCenter Server® that provides hypervisor-based virtual machine replication and recovery.

## VMware AppDefense

**VMware AppDefense™ 2.2, 2.3 – AppDefense** is a data center endpoint security product that protects applications running in virtualized and cloud environments.

## Digital Workspace

**Workspace One Access™ (formerly VMware Identity Manager™) 3.0, 3.1, 3.2, 3.3 –Workspace One Access** is an identity as a service (IDaaS) offering that provides single sign-on (SSO) capabilities and user-based controls for web, cloud, and mobile applications.

Appendix B in this guide showcases the capabilities of all products in alignment with PCI DSS intents.

# Overview of VMware and PCI DSS Best Practices and Requirement Mapping

| Best Practice Area (Lens) | PCI DSS Requirement(s) | Capability Description | VMware Product Applicability |
|---|---|---|---|
| Automated Security | Req. 10, Req. 11 | Automated Deployment, Automated Remediation | Site Recovery ManagervSphere Replication vRealize Operations vCloud Director<br>vCloud Availability for vCloudDirector<br>Workspace One Access |
| Data Segmentation | Req. 1, Req. 3, Req. 11, Req.<br>12 | Network & Host Firewall, Information Flow | Network Virtualization andSecurity<br>VMware Validated DesignCloud Foundation vRealize Network Insight<br>vRealize Operations<br>vRealize Log Insight<br>AppDefense<br>vCloud Usage MetervCloud Director<br>vCloud Director Extender<br>vCloud Availability for vCloud Director |
| System Hardening | Req. 1, Req. 3, Req. 4, Req. 6,<br>Req. 12 | Configuration Management, Patch Management, Vulnerability Management | vRealize Network Insight<br>vRealize Operations<br>vRealize Log Insight<br>vSphere Update Manager Network Virtualization and Security<br>ESXi<br>AppDefense<br>vCloud Usage MetervCloud Director<br>vCloud Director Extender<br>vCloud Availability for vCloud Director |
| Compliance Validation | Req. 6, Req. 12 | Configuration Management | vRealize Network Insight<br>vRealize Operations<br>vRealize Log Insight<br>Network Virtualization andSecurity<br>AppDefense<br>vCloud Director |

| Best Practice Area (Lens) | PCI DSS Requirement(s) | Capability Description | VMware Product Applicability |
|---|---|---|---|
| System Access | Req. 7, Req. 8 | Multi-factor Authentication, Identity and Access Management | vCenter<br>Network Virtualization andSecurity<br>vRealize Network InsightvRealize Log Insight vRealize Operations<br>ESXi<br>AppDefense<br>vCloud Usage MetervCloud Director<br>vCloud Director Extender<br>vCloud Availability for vCloudDirector<br>Workspace One Access |
| System Monitoring | Req. 10, Req. 11 | Security Information Event Monitoring (SIEM), Database Monitoring | vRealize Log Insight<br>vRealize Network InsightvRealize Operations<br>Site Recovery Manager<br>vSphere Replication<br>vSphere Update ManagervCenter<br>AppDefense<br>vCloud Usage MetervCloud Director<br>vCloud Director Extender<br>vCloud Availability for vCloudDirector<br>Workspace One Access |
| Data Encryption & Protection | Req. 1, Req. 3, Req. 4, Req. 6 | Data at Rest Encryption, Data in Motion Encryption, System Backup & Restore | EXSi VM Encryption featurevSAN Encryption feature VMware vSphere vMotion®encryption<br>Network Virtualization andSecurity<br>vRealize Operations<br>vRealize Network Insight vRealize Log Insight VMware Validated DesignCloud Foundation vSphere Update Manager<br>AppDefense<br>vCloud Usage MetervCloud Director<br>vCloud Director Extender<br>vCloud Availability for vCloud Director |

| Best Practice Area (Lens) | PCI DSS Requirement(s) | Capability Description | VMware Product Applicability |
|---|---|---|---|
| Network Protection | Req. 1, Req. 3, Req. 6, Req. 11 | Intrusion Prevention System, Web Application Firewall | Site Recovery Manager<br>vSphere Replication<br>Network Virtualization andSecurity<br>vRealize Operations<br>vRealize Network InsightvRealize Log Insight AppDefense<br>vCloud Director<br>vCloud Director Extender<br>vCloud Availability for vCloud Director |
| Endpoint Protection | Req. 2, Req. 3, Req. 5, Req. 6,<br>Req. 7, Req. 8, Req. 11 | Endpoint A/V and Malware Prevention, File Integrity Monitoring, Data Leakage Protection, Mobile Device Management | Network Virtualization andSecurity<br>ESXi<br>vRealize Operations<br>vRealize Network InsightvRealize Log Insight AppDefense<br>vCloud Director<br>vCloud Director Extender<br>vCloud Availability for vCloudDirector<br>Workspace One Access |
| Trusted Execution/SecureBoot | Req. 3,<br>Req. 6 | Execution Integrity | ESXi<br>Network Virtualization andSecurity<br>vRealize Operations<br>AppDefense<br>vCloud Director<br>vCloud Director Extender |
| Software Development Lifecycle (SDLC) | Req. 6 | Configuration Integrity | VMware Validated DesignCloud Foundation |

Exhibit 3 represents a high-level view of how VMware technology capabilities match up to best practices areas and PCI DSS requirement topics.

# VMware Control Capabilities Detail

## VMware Validated Design and Software Development Process

VMware developed the VMware Validated Design (VVD) to allow organizations to implement the full SDDC platform using a design that is authorized and provides the detail required to confidently deploy SDDC. The VVD is available to anyone and is published on the VMware website.

The VMware Software Development Lifecycle (SDLC) designs security into all phases of SDDC and VMware Cloud products (Exhibit 4). VMware Product Security oversees this principled approach to designing security, as it is important for PCI DSS compliance. The products used have security interwoven through their underlying substructures and are supported by administrative policy.

With compliance and security woven into the SDLC, VMware improves the quality of its products and solution platforms that can support organizations needing to achieve PCI compliance.

To further elaborate on the primary purposes of a control family, each detail segment provides the applicable security lens defined within the VMware approach. These lenses are hallmarks of a mature security program addressing common areas of vulnerabilities.

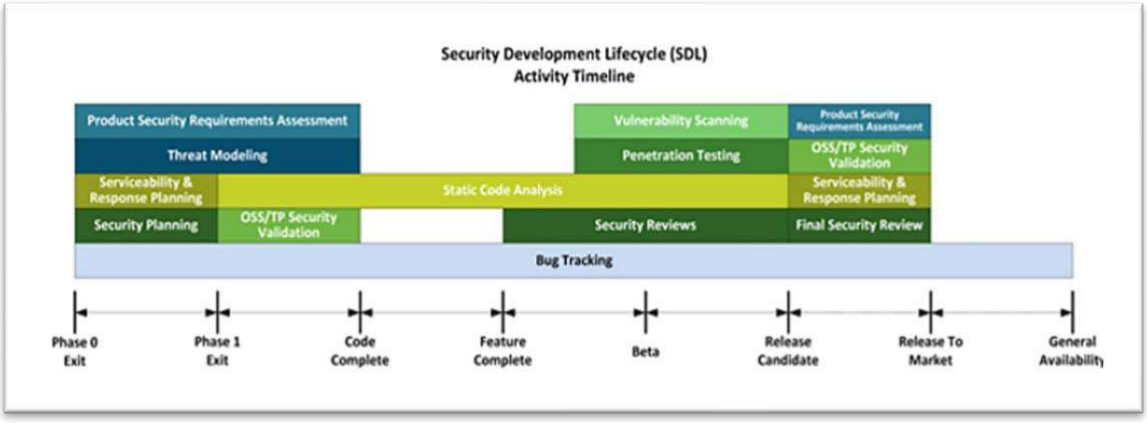



Exhibit 4: VMware SDL Activity Timeline

## Core and Administrative Control Categories

Enforcing defense in depth throughout a CDE requires a combination of technical and process or policy-based controls. This results in PCI DSS requirements covering a wide spectrum of control types. To streamline the delivery of this PAG and the intent of each control family, controls were sorted into two categories: core and administrative. Core control families are those that address the main structure of a PCI program through technical features and capabilities. Administrative control families support multiple control areas through policy development and general program, people, and process management tasks. Further details on these categories and the aligned control families can be found in the following sections.

## VMware Administrative Support for PCI Requirements

PCI DSS establishes requirements for technical and operational controls, procedures, or other security standards, which can be met by using VMware products or VMware technology capabilities. Other PCI controls may identify physical or operational requirements that are not able to be met by software alone. However, these controls may rely on or be supported by underlying VMware product capabilities. While VMware products do not map neatly to these controls, they support their fulfillment through alerts, scripting, and monitoring.

This is a common thread throughout the capabilities discussed below. An organization can deploy VMware products, apply the PCI DSS requirements, and monitor them through the compliance-capable platform. In this way, implementing policy or operating procedures assists in maintaining a secure and compliant information architecture.

An example of an administrative requirement is Requirement 12. This requirement requires a documented information security policy or set of detailed security procedures. Using VMware products such as NSX or vRealize Log Insight, a company can enforce standards defined by existing policies and then monitor endpoints against those standards and be alerted as soon as a system deviated. In this way, VMware can support the definitions of Requirement 12, while not fulfilling the specific controls laid out in the requirement. Requirement 12 is more focused on the people and process behind the policy itself. Thus, this guide will treat the requirement as an administrative support requirement instead of a core requirement because VMware product capabilities support the administration of the requirement rather than actually fulfilling a control item.

The following requirements are classified as administrative:

- Requirement 9: Restrict physical access to cardholder data
- Requirement 12: Maintain a policy that addresses the information security for all personnel

## VMware Core Support for PCI Requirements

For those PCI requirements where a product can partially or fully satisfy a control requirement, VMware capabilities are identified as core to the requirement in question. These are the areas within PCI DSS that best highlight how each product provides capabilities to strengthen the security and support a compliance-capable platform.

The details below showcase the SDDC and VMware Cloud components that support or apply to each PCI control requirement and their respective high-impact controls. Each area defines the intention of the PCI requirement, aligning security lenses as described in the “Our Approach” section (above), and the specifics of the product and their native features that meet control standards. Exhibit 2 (above) illustrates this information.

This guide provides organizations with the opportunity to harness the capability of modern virtualization technology to enhance their security program and processes. Organizations can be confident in their decision to elevate the sophistication of techniques needed to meet complex requirements and secure modern technology infrastructure.

While all controls described within the PCI DSS must be adhered to for compliance, the following requirements are defined as "core" controls as native VMware features support or execute the intent of specific aspects of the requirement and underlying controls as shown in Appendix B:

- Requirement 1: Install and maintain a firewall configuration to protect cardholder data
- Requirement 2: Do not use vendor-supplied defaults for system passwords and other security parameters
- Requirement 3: Protect stored cardholder data
- Requirement 4: Encrypt transmission of cardholder data across open, public networks
- Requirement 5: Protect all systems against malware and regularly update anti-virus software or programs
- Requirement 6: Develop and maintain secure systems and applications
- Requirement 7: Restrict access to cardholder data by business need to know
- Requirement 8: Identify and authenticate access to system components
- Requirement 10: Track and monitor all access to network resources and cardholder data
- Requirement 11: Regularly test security systems and processes

# VMware Core Controls

# Requirement 1: Install and Maintain a Firewall Configuration to Protect Cardholder Data

## PCI DSS Controls 1.1 – 1.5

Requirement 1 addresses the requirements for creating and maintaining firewalls and their configurations in the protection of cardholder data. This requirement details the protections required to prevent unauthorized access to sensitive data through the proper use and management of firewalls or similar components.

Applicable Security Lens:

- Data Segmentation
- System Hardening
- System Monitoring
- Network Protection
- Data Encryption & Protection

Applicable VMware Product(s):

- Cloud Foundation
- ESXi
- NSX
- NSX-T
- vCenter
- vCloud Availability for vCloud Director
- vCloud Director
- vCloud Director Extender
- vCloud Usage Meter
- vCloud Automation
- vCloud Operations
- vCloud Orchestrator

# VMware Product Capabilities

NSX can be configured to deny all traffic by default, restricting outbound traffic and protecting corporate devices from malicious traffic entering the environment. Exceptions can be defined granularly to further enahance security in depth. vCloud Director can be used to also provide additional monitoring functionality allowing audit logs to be produced that include environment analytics.

Micro-segmentation allows logical domain segmentation at a granular isolation level. For DDoS attacks, NSX builds in capabilities to perform malware analysis. These attributes supplement vulnerability scanning capabilities that exist within the SDLC. NSX and other SDDC products grant administrator functionality to restrict remote access todefined protocols, e.g., SSH and RDP. vCloud Usage Meter has transport layer security (TLS) enabled by default for all communications and conducts checksum verification for generated reports.

Beyond protocol restriction, vRealize Automation contains multiple default roles that segment information based on roles at scale. Coupled with vRealize Log Insight, this segmentation enables authentication to be authorized granularly across a designed environment without third-party integration. Similar to vRealize Automation, vRealize Operations permits the creation of groups using RBAC to define segregation of certain areas or devices within an environment.

VMware NSX gateways give boundary protection and network isolation to user environments. Through its Dynamic Host Configuration Protocol (DHCP) service, VMware NSX Edge™ gateways set a static binding. By doing so, unique identifiers are set prior to any execution, fortifying an information system against malicious activity and defining a virtual boundary for organizations using multi-tenant cloud environments.

For enhanced visibility, organizations can use vRealize Network Insight to provide context on information flow within the environment. vRealize Network Insight uses platform and proxy use certificates to restrict flow within an infrastructure. NSX and its micro-segmentation can then enforce defined information flow guidelines. VMware NSX Manager™ can synchronize with RBAC to restrict access based on specified group names. The information contained within these data flows is then secured at rest with the vSAN Encryption feature in vSAN and with the ESXi VM Encryption feature. ESXi further segments processes within resource pools. vCloud Director supports native integration into NSX Distributed Firewall to provide application isolation. vCloud Usage Meter provides further protection by allowing users to be segmented into three groups: root Unix user, non-root Unix user, and UI user, who has no system access.

VMware security programs and practices establish requirements “by design” to evolve methodologies of protection against new “in-the-wild threats.” This approach is followed throughout the development process. Products are tested by first-class vulnerability scans and penetration tests prior to any full release or version update.

For further information, please visit:
https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/VMware-Product-Security.pdf.

Additional product capability details can be found at the VMware Compliance IDs listed in Appendix B.

# Requirement 2: Do Not Use Vendor-Supplied Defaults for System Password and Other Security Parameters

## PCI DSS Controls 2.1 – 2.6

Requirement 2 provides guidance on removing any and all default settings or account information provided by vendors or third parties prior to production-level use within an organization's PCI environment.

Applicable Security Lens:

- System Hardening
- System Access
- System Monitoring
- Network Protection
- Data Encryption & Protection
- Trusted Execution/Secure Boot

Applicable VMware Product(s):

- Cloud Foundation
- ESXi
- NSX-T
- vCenter
- vRealize Automation
- vRealize Log Insight
- vSphere Replication

# VMware Product Capabilities

VMware products provide numerous integration opportunities with existing access control software such as Active Directory to assist removing default account information. NSX can apply configuration requirements, while also removing unnecessary functions. vRealize Automation provides similar features, allowing for default services and settings to be disabled by default for any new infrastructure equipment or virtual machines that are created through its portal.

All products can reset default passwords for their associated accounts. vRealize Operations can be configured to force root users to reset their passwords during their initial login. All products in accordance with the VVD and SDLC are required to have minimum password standards that are stored in an encrypted fashion, never maintained in clear text format.

Additional product capability details can be found at the VMware Compliance IDs listed in Appendix B.

# Requirement 3: Protect Stored Cardholder Data

## PCI DSS Controls 3.1 – 3.7

Requirement 3 outlines requirements for storing and protecting sensitive cardholder data, including requirements for encryption and access.

Applicable Security Lens:

- System Hardening
- System Access
- System Monitoring
- Network Protection
- Data Encryption & Protection
- Data Segmentation

Applicable VMware Product(s)

- ESXi
- NSX
- NSX-T
- vCenter
- vCloud Availability for vCloud Director
- vCloud Director
- vCloud Director Extender
- vCloud Usage Meter
- vSAN

# VMware Product Capabilities

SDDC requires the use of AES256 cryptographic protocols. To assist with user authentication, Active Directory can be integrated for central management of credentials. The vSphere VM Encryption feature supports encryption so that all data stored within a customer's SDDC environment can be encrypted to meet industry standards and the requirements of PCI. vSphere VM Encryption uses XTS-AES-256 based data encryption and AES256 based key encryption.

Both vSphere VM Encryption and VMware vSAN encryption also allows for additional cryptographic management features such as key rotation, additional API integration, Key Management System (KMS) integration, and generally enabling or disabling encryption as appropriate. vSphere 6.7 encryption is FIPS 140-2 validated. NSX uses Root Certification Authority to support Public Key Infrastructure within the virtual network platform.

Additional product capability details can be found at the VMware Compliance IDs listed in Appendix B.

# Requirement 4: Encrypt Transmission of Cardholder Data Across Open, Public Networks

## PCI DSS Controls 4.1 – 4.3

Requirement 4 provides guidance for protecting cardholder data when it is transmitted over public networks thatare accessible by malicious actors or when it is outside of the organization's administration.

Applicable Security Lens:

- System Monitoring
- Network Protection
- Data Segmentation
- Data Encryption & Protection

Applicable VMware Product(s):

- Cloud Foundation
- ESXi
- NSX
- NSX-T
- Site Recovery Manger
- vCenter
- vCloud Director
- vCloud Usage Meter
- vCloud Automation
- vRealize Log Insight
- vRealize Network Insight
- vRealize Orchestrator
- vRealize Operations
- vSAN
- vSphere Replication

# VMware Product Capabilities

VMware considers encryption to be a core feature of a secure environment and integrates modern standards into products where appropriate.

vCenter and ESXi support the encryption of VMs and integrate with existing third-party key management systems to manage the keys associated with these VMs. The cryptographic management features offered by vSAN also apply to data in transit.

Additional product capability details can be found at the VMware Compliance IDs listed in Appendix B.

# Requirement 5: Protect All Systems Against Malware andRegularly Update Anti-Virus Software or Programs

## PCI DSS Controls 5.1 – 5.4

Requirement 5 details the guidance for deploying, updating, and monitoring anti-virus or malware programs, or software with similar features.

Applicable Security Lens:

- System Hardening
- Data Encryption & Protection
- System Monitoring
- Network Protection

Applicable VMware Product(s):

- ESXi
- NSX-T
- vRealize Automation
- vRealize Log Insight

# VMware Product Capabilities

Several VMware products and capabilities are relevant to this requirement. Harnessing the Unified Extensible Firmware Interface (UEFI) and Secure Boot, the hypervisor refrains from loading unless the signature database (containing the whitelisted and blacklisted signatures) authenticates. At each stage of the boot process, components of the hypervisor are authenticated using digital signatures. This includes each vSphere Installation Bundle (or VIB). ESXi creates an in-memory filesystem that maps to the contents of the digitally signed VIB. This whole process certifies that when Secure Boot is enabled that the hypervisor will only run code that is signed by VMware and VMware partners. If signatures are not authenticated, the hypervisor fails to activate. vCenter supports alerts to prevent unauthorized execution within the environment.

In the case of system failure or misconfiguration, no detailed error information is reported to the end-user or session, thereby reducing the opportunity for malicious actors to exploit known weaknesses or gather intelligence. NSX natively includes defined guest introspection framework that allows administrators to conduct analysis on the data plane level from North–South traffic flows.

In addition to the functionality provided by Secure Boot, vRealize Log Insight and vRealize Network Insight provide features that can be configured to notify the security team if a root account is being accessed, brute force attack, or attempt to attack an ESXi host. All alerts can be sent via email, allowing security personnel to intercept incidents at their earliest stages.

Natively, VMware products host multiple features and capabilities (as described above) that prevent the exploitation of malware-related attacks. It is important for organizations to certify that alternative

measures are in place to protect these incidents occurring in other scope-related quadrants of an environment.

# Requirement 6: Develop and Maintain Secure Systems and Applications

## PCI DSS Controls 6.1 – 6.7

Requirement 6 establishes controls related to the creation and maintenance of secure systems, applications, and policies. This family spans the underlying makeup of an organization's SDLC and the application of security. It focuses on understanding resource allocation; the security engineering principles employed; supply chain protection; and how developers, engineers, and other product development personnel are prepared to perform the duties defined by the organization.

Applicable Security Lens:

- Data Segmentation
- Data Encryption & Protection
- System Hardening
- Network Monitoring
- Software Development Lifecycle (SDLC)
- System Monitoring

Applicable VMware Product(s):

- AppDefense
- Cloud Foundation
- ESXi
- NSX
- NSX-T
- Site Recovery Manager
- vCenter
- vRealize Orchestrator
- vSAN

# VMware Product Capabilities

The VMware approach to security extends into its development process. While constant iteration is a priority, security is interwoven into every stage from ideation and design to development and into production. Static code analysis, security, and privacy considerations at the design phase run through multiple levels of approval, in addition to performance-level assessments. Developers participate in extensive secure code training and regularly attend working sessions in collaboration with security compliance and privacy teams to stay abreast of evolving trends and vulnerabilities.

The overlap in security emphasis between VMware internal SDLC processes and the Requirement 6 controls fulfills the requirements including process isolation at both personnel level and code level, encryption protocols in transmission, and permission granularity.

One main objective within this control set is minimizing the development of covert channels. VMware conducts peer reviews during each development cycle to secure all potential backdoor entry points for attackers. VVD requirements demand adequate levels of encryption, logging specifically through separating vRealize Log Insight from vRealize Network Insight and pushing security groups through NSX.

All pieces of VMware software include digital signatures and 256 MAC hashing.

Particularly important for this control family is that security requirements can be met during the acquisition process. For organizations looking to secure all levels of their infrastructure, the SDLC extends out into the supply chain and products that are acquired by VMware to deliver virtual solutions to the marketplace. Through Cloud Foundation (including both the vSAN Encryption feature in vSAN and ESXi VM Encryption feature), all elements of a virtualized environment are encrypted and secure throughout internetwork transit.

The VMware Compliance and Cyber Risk Solutions (CCRS) team develops whitepapers and other documentation to show the mapping between VMware product capabilities and compliance requirements. CCRS designed the VMware Compliance Capable Platform framework. On an ongoing basis, CCRS provides product engineering with feedback to further solidify product capabilities in support of compliance controls and cyber risk requirements. VMware product mappings and design architecture in support of a compliance-capable platform augment the value of acquiring VMware products.

The VVD architecture contains specified requirements for each component's configuration. This provides a "gold standard" for deployment across the entire suite of products. This standard is developed with security requirements through the SDLC.

To further protect any adjustments to information systems configuration, micro-segmentation can be defined through either NSX or VMware NSX-T Data Center™. Routing specifications can be set and protected by tamperproof logging. Active Directory can be integrated to enforce least privilege functionality, based on requirements across the user base. Devices can be isolated to eliminate rogue device infiltration. All configuration and isolation activities can use REST API to deliver at scale and in real time.

Endpoints can be further protected with AppDefense, which can comprehend the state of an environment and actively monitor changes in any applications, configurations, or system behavior. AppDefense can also be configured to block individual ports or protocols. Engaging vCloud Director can provide the ability to manage traffic between VMs within an organization via distributed firewall rules, along with edge gateway firewall capabilities.

Knowing that the protection of or adherence to standards is difficult without knowing what resides in the network, vRealize Automation has features to provide a database of virtual machines, which can be updated automatically. In conjunction, vRealize Operations provides organizations with the option to deploy agents to unearth deep, network-layer intel and monitor host configurations.

Additional product capability details can be found at the VMware Compliance IDs listed in Appendix B.

# Requirement 7: Restrict Access to Cardholder Data by Business Need to Know

## PCI DSS Controls 7.1 – 7.3

Requirement 7 focuses on the ability of any user, across all defined permission levels, to reach key elements of the environment. It looks at coverage across subjects such as remote access and the integrity of the entire authentication process.

Applicable Security Lens:

- System Access
- Endpoint Protection
- Data Encryption & Protection
- System Monitoring
- Data Segmentation

Applicable VMware Product(s):

- AppDefense
- Cloud Foundation
- ESXi
- NSX
- NSX-T
- Site Recovery Manager
- vCenter
- vCloud Availability for vCloud Director
- vCloud Director
- vCloud Director Extender
- Workspace One Access
- vRealize Automation
- vRealize Log Insight
- vRealize Network Insight
- vRealize Operations
- vRealize Orchestrator
- vSAN

# VMware Product Capabilities

For all products within the SDDC platform, access controls can be implemented at a granular level. This is presented through Role-Based Access Control (RBAC) mechanisms natively available. User management interfaces are provided to control password complexity and user profiles and to access review tasks. Products, for instance vCenter, enable complementary products with RBAC capabilities. This is particularly the case for Site Recovery Manager used in conjunction with vCenter.

Across all products, default passwords can be reset. vRealize Operations can be configured to force root users to reset their passwords during their initial login. All products in accordance with the VVD and SDLC are required to have minimum password standards that are stored in an encrypted fashion, never maintained in clear text format.

SDDC and VMware Cloud products across the suite allow for seamless 2FA deployment through third-party integrations.

As an elevated protection, VMware has built third-party integration capabilities to allow organizations to integrate single-sign-on (SSO) tools to strengthen authentication needs and restrict access. Organizations can also integrate their Active Directory (AD)/Lightweight Directory Access Protocol (LDAP) instance through use of VMware published Application Programmable Interfaces (API) to refine access at all levels of their virtual stack. vRealize Operations allows administrators to limit concurrent sessions and define account lockout parameters.

vCloud Usage Meter provides additional LDAP configuration and has HTTPS enabled by default, with support for SSH. vCloud Director provides the ability to administer user accounts via the administration page, the provided API, and LDAP integration. Further, vCloud Director provides multi-tenancy, isolation of tenants, and logically isolated switches. vCloud Director can be combined with vCloud Director Extender and vCloud Availability for vCloud Director to further expand the capabilities provided by vCloud Director, which further isolates, secures, and monitors the CDE.

Additional product capability details can be found at the VMware Compliance IDs listed in Appendix B.

# Requirement 8: Identify and Authenticate Access to System Components

## PCI DSS Controls 8.1 – 8.8

This control family establishes criteria and controls so that only authorized connections are enabled throughoutan organization's environment.

Applicable Security Lens:

- System Monitoring
- Network Protection
- Data Segmentation
- Endpoint Protection
- System Hardening
- Data Protection & Encryption

Applicable VMware Product(s):

- AppDefense
- Cloud Foundation
- ESXi
- NSX
- NSX-T
- Site Recovery Manager
- vCenter
- vCloud Automation
- vCloud Director
- vCloud Director Extender
- vCloud Usage Meter
- Workspace One Access
- vRealize Log Insight
- vRealize Network Insight
- vRealize Operations
- vRealize Orchestrator
- vSAN

# VMware Product Capabilities

VMware products support various forms of authentication and access controls to assist with the protection of systems and cardholder data. Only trusted IPs, subnets, or IP devices are allowed into the environment, vCenter and NSX provide access restriction to an organization's East–West traffic, or VM to VM communications.

All SDDC products can prevent sessions from remaining unlocked via the use of time-outs and re-authentication which can both be set by following the standard VVD requirement. By default, all session time-outs require user re-authentication. Typically set to 15 to 20 minutes, session time-out thresholds can be configured within the product and adjusted to meet control and requirement intents. Products can harness Active Directory integration to maintain vigilance over authentications to products.

AppDefense can manage and configure unique user identifiers within the operational console for any user logged into the AppDefense console. vCloud Usage Meter can be set to use LDAP for authentication.

NSX allows access control through the implementation of micro-segmentation via security policies. The NSX Identity Firewall feature enhances the access control down to the virtual networking level, permitting only approved users with need to access specific virtual machines. These authentication mechanisms can be managed through security groups and policies configured within the vCenter Web UI.

Within vCloud Director manage and monitor portals, various logging capabilities can be configured and reviewed. Additionally, servers can be configured into a log repository to hold logs from NSX components and hosts. The administration portal also offers the ability to configure account lockouts, devices and accounts with access control permissions based on compliance requirements. The system administrator account permissions encompass all existing rights, in addition to those associated with administrator accounts, which are immutable.

VMware Identity Manager provides additional controls for managing user access, including the ability to institute single sign on (SSO), assign unique session tokens, use VMware Verify for multi-factor authentication, and standard account controls. VMware Identity Manager provides a standardized reporting function available to administrators to facilitate user account reviews.

vRealize Operations and vRealize Log Insight, along with the other products that compose the SDDC suite and VMware Cloud, can support the implementation of continuous monitoring. vRealize Operations gives administrators the ability to craft custom security tags that align with PCI DSS and other security frameworks to maintain real-time assessment and authorization across the environment.

Beyond product applicability, organizations are advised to perform proactive penetration tests to meet the full extent of the control area.

Additional product capability details can be found at the VMware Compliance IDs listed in Appendix B.

# Requirement 9: Restrict Physical Access to Cardholder Data

## PCI DSS Controls 9.1 – 9.10

VMware products can support the physical security controls described in this requirement family by providing data and technical controls which can be combined with organizationally developed policies to create or support a secure physical environment.

Applicable Security Lens:

- System Access
- System Monitoring
- Network Protection

Applicable VMware Product(s):

- vCenter
- vRealize Automation
- vRealize Orchestration
- vSphere Replication

# Requirement 10: Track and Monitor All Access to Network Resources and Cardholder Data

## PCI DSS Controls 10.1 – 10.9

The Requirement 10 controls cover the implementation, governance, and operation of an audit program and logging systems. As a function of the program, it calls for organizations to confirm the protection of any logs and additional information associated with audit procedures.

Applicable Security Lens:

- Systems Monitoring
- System Access

Applicable VMware Product(s):

- AppDefense
- Cloud Foundation
- ESXi
- NSX
- NSX-T
- Site Recovery Manager
- vCenter
- vCloud Availability for vCloud Director
- vCloud Director
- vCloud Director Extender
- vCloud Usage Meter
- Workspace One Access
- vRealize Automation
- vRealize Log Insight
- vRealize Network Insight
- vRealize Operations
- vRealize Orchestrator
- vSAN

# VMware Product Capabilities

Requirement 10 speaks to the need for a security program to conduct ongoing audits to maintain integrity and compliance. Implementing the SDDC through the VVD provides a reference architecture to identify security requirements throughout the virtual platform, from hypervisor through to the UI that collects audit log data.

Across all products, rich logging features exist to allow administrators to ascertain who logged in, the origin, at what time, and whether the attempt was a success or failure. Logs can be pointed to third-party management tools through API integration if desired, although VMware also provides tools such as vRealize Log Insight to support log collection and integration into a SIEM. AppDefense can deliver alerts for all changes made within the environment. This can be configured through the provided “Scopes” feature, or through the vCenter Web UI. Any logs generated by AppDefense can be calibrated using the AppDefense Manager, and access can be restricted to only an administrator.

Monitoring is done using vRealize Network Insight, vRealize Log Insight, and vRealize Operations. vRealize Log Insight strengthens access security with forensic monitoring of the virtual/physical networking and flow. This also includes NSX stateful firewall and security group policies. Out of the box, vRealize Log Insight provides security dashboards that enable monitoring of associated VMware products.

Implementing vCloud Director can add additional benefits in the form of monitoring functionality, which produces audit logs on the environment and can be used to monitor all assets within the environment. Access to this functionality can be restricted, as administrators can restrict access to most of vCloud Director. vCloud Director can be combined with vCloud Availability for vCloud Director to entrust functionality.

VMware Identity Manager can integrate with vRealize Log Insight or a third-party logging system to promote log storage. In a cloud environment, VMware Identity Manager defaults to 90-day log storage, but it can be configured to push logs. On-prem instances storing recently generated logs, should be regularly pushed to an appropriate logstorage area for PCI compliance.

Further, vRealize Log Insight gives IT and IT security teams the ability to point all products in their stack (not only their VMware product stack) to vRealize Log Insight to help manage and correlate any incidents or perceived incidents through an audit dashboard and native log analysis. vCloud Usage Meter can store additional logs in the VMware vFabric® Postgres database of the appliance, which can be secured.

To support non-repudiation, administrators are advised to design strong access control surrounding administrator passwords. All administrative actions should be logged and reviewed on a consistent basis.

vCenter has the capability to push logs to up to three different external syslog receivers including vRealize Log Insight. vRealize Log Insight retains data based on defined storage capacity and can apply additional tamper protection. vRealize Operations assists by monitoring the datastore's health and capacity, prompting the administrator to determine how to proceed with further log archival if necessary.

vRealize Network Insight contains the ability to adjust forensic data retention. ESXi affords administrators the ability to adjust the richness and frequency of audit logs.

For advancing an organizational audit process, a SIEM platform can be coordinated through vRealize Log Insight to ingest logs to provide better alerting and log management.

To note, some controls only have partial matches but are supported across all products within the SDDC. These controls relate to authentication against a certificate authority (CA). The organization will need to identify the CAthat will then be assessed against during each user session.

Additional product capability details can be found at the VMware Compliance IDs listed in Appendix B

# Requirement 11: Regularly Test Security Systems and Processes

## PCI DSS Controls 11.1 – 11.6

Requirement 11 is driven by the creation of organizational policies that address how evolving disaster or security events will be addressed. SDDC components can assist in the research, auditing, and curtailing of those events attributed to technical elements through integration into IDS/IPS appliances or a SIEM.

In other respects, the breadth of the family is focused on developed administrative

policy. Applicable Security Lens:

- System Access
- System Monitoring
- Network Protection

Applicable VMware Product(s):

- AppDefense
- ESXi
- NSX
- NSX-T
- Site Recovery Manager
- vCenter
- vCloud Director
- vRealize Log Insight
- vRealize Network Insight
- vRealize Operations
- vSAN

# VMware Product Capabilities

To widen appliance coordination, vRealize Log Insight, vRealize Network Insight, vRealize Operations, and vRealize Orchestration can be combined to define an event occurrence–level alert. This capability will enable organizations to calibrate alerts so that critical alerts are noticed through visual dashboards and defined distribution lists. vSphere Update Manager and vRealize Operations can be configured to automate remediation on identified vulnerabilities. Third-party solutions can be inserted to combine both on-premises and cloud-based synchronization of updates.

AppDefense can, on its own, isolate threats as they appear and suspend the affected section of the environment. AppDefense actively monitors the environment from the hypervisor layer and can detect anomalies in application behavior or network traffic, and changes made to network configuration. Actions can be addressed automatically when alerts are triggered. It can also be integrated with the vSphere environment, which if used in conjunction with vCloud Director can be used to establish and maintain intrusion detection and management.

Additionally, AppDefense provides continuous detection at the hypervisor level allowing it to block, suspend, or shut down malicious behavior. It can also block or whitelist other activity within the environment based on its 'Learning Mode,' which assists with identifying the desired functionality of applications to determine when malicious activity is present.

Additional product capability details can be found at the VMware Compliance IDs listed in Appendix B.

# VMware Administrative Controls

# Requirement 12: Maintain a Policy That Addresses Information Security for All Personnel

## PCI DSS Controls 12.1 – 12.11.1

VMware products can support the controls of this family through organizationally developed policy when properly used. All SDDC platform components do provide backup and recovery capabilities, which will thus aid the employment of a policy's requirements such as data protection and being able to meet recovery time objectives (RTO) and recovery point objectives (RPO).

### Applicable Security Lens:

- System Monitoring
- Network Protection
- Automated Security

### Applicable VMware Product(s):

- AppDefense
- NSX
- NSX-T
- vCenter
- vCloud Director
- vRealize Log Insight
- vRealize Operations
- vRealize Orchestrator
- vRealize Replication

# Conclusion

To meet evolving regulatory needs, security programs now must define applicable controls at early stages. From ideation to design and through to the end of the product lifecycle, VMware focused on developing methodologies that set this tone.

Through the eleven (11) security lenses and in accompaniment of the VMware Validated Design, the SDDC platform components and VMware Cloud provide users with a virtualization stack that adheres to the comprehensive requirements of PCI DSS.

Organizations can seamlessly piece together full SDDC and VMware Cloud environments, or a subset made up of individual components, and be confident in the security and privacy measures employed in the products' support efforts to protect a cardholder data environment.

The considerations that VMware brings to bear on continuous compliance for clients comes from its development culture, which constructs requirements that balance functionality and security for all deployable products. These policies provide customers with the confidence to include the SDDC product suite within their architecture and PCI DSS security program.

# Bibliography


1. Holmes, Wade. VMware NSX Micro-segmentation Day 1. VMware Press, 2017.“Secure Boot for ESXi 6.5 – Hypervisor Assurance.”

2. Foley, Mike. May 4, 2017. Accessed July 20, 2017. HTTPs://blogs.vmware.com/vsphere/2017/05/secure-boot-esxi-6-5-hypervisor-assurance.html

3. “NIST Special Publication (SP) 800-53 Revision 4.” National Institute of Standards and Technology. April 2013. Accessed July 26, 2017.

4. https://doi.org/10.6028/NIST.SP.800-53r4.“NIST Special Publication (SP) 800-53 Revision 4.”National Institute of Standards and Technology. April 2013. Accessed July 26, 2017. https://doi.org/10.6028/NIST.SP.800-53r4.

5. “Official PCI Security Standards Council Site: Document Library.” Accessed October 30, 2018. https://www.pcisecuritystandards.org/document_library

6. “VMware Product Security: An Overview of VMware’s Security Programs and Practices.” VMware. Accessed July 26, 2017. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/VMwareProductSecurity.pdf.

7. “Information Supplement: PCI SSC Cloud Computing Guidelines,” PCI Security Standards Council – CloudSpecial Interest Group, Version 3.0. April 2018. Accessed February 8, 2019. https://www.pcisecuritystandards.org/pdfs/PCI_SSC_Cloud_Guidelines_v3.pdf

# Appendix A: PCI DSS 3.2.1 Control Mapping

| *VMware Product* | *PCI DSS 3.2.1 Control Families Supported* |
|---|---|
| VMware AppDefense | Req. 1, Req. 2, Req. 7, Req. 10, Req. 11, Req. 12 |
| VMware Cloud Foundation | Req. 1, Req. 2, Req. 6, Req. 7, Req. 8, Req. 10 |
| VMware Cloud Provider Platform | Req. 1, Req. 2, Req. 3, Req. 4, Req. 5, Req. 6, Req. 7, Req. 8, Req. 9, Req. 10, Req. 11, Req. 12 |
| - vCloud Availability for vCloud Director | |
| - vCloud Director | |
| - vCloud Director Extender | |
| - VMware vCloud Usage Meter | |
| VMware Identity Manager | Req. 7, Req. 8, Req. 9, Req. 10 |
| VMware NSX | Req. 1, Req. 6, Req. 8, Req. 12 |
| - VMware NSX-T | |
| VMware vRealize Automation | Req. 1, Req. 2, Req. 4, Req. 5, Req. 7, Req. 9, Req. 10 |
| VMware vRealize Log Insight | Req. 2, Req. 7, Req. 8, Req. 9, Req. 10, Req. 12 |
| VMware vRealize Network Insight | Req. 7, Req. 8, Req. 9, Req. 10, Req. 11 |
| VMware vRealize Orchestration | Req. 1, Req. 2, Req. 7, Req. 8, Req. 9, Req. 10, ReqQ.12 |
| VMware vRealize Operations | Req. 1, Req. 2, Req. 8, Req. 10, Req. 11, Req. 12 |
| VMware vSAN | Req. 3, Req. 4, Req. 6, Req. 7, Req. 8, Req. 10, Req. 11 |
| VMware Site Recovery Manager | Req. 4, Req. 7, Req. 8, Req. 10, Req. 11 |
| VMware vSphere | Req. 1, Req. 2, Req. 3, Req. 5, Req. 4, Req. 6, Req. 7, Req. 8, Req. 9, Req. 10, Req. 11, Req. 12 |
| - VMware ESXi | |
| - VMware vCenter | |
| - VMware vSphere Replication | |

# Appendix B: SDDC Product Capability Relationshipwith PCI DSS

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | | | |
| ESXi | ESXI_001 | Login attempts can be logged. | Req. 8 |
| | ESXI_002 | Concurrent sessions can be limited on web clients and virtual machine consoles. | Req. 7<br>Req. 8 |
| | ESXI_003 | ESXi can be integrated with Active Directory, or LDAPto employ unique user identifiers, instead of using the root account. | Req. 8 |
| | ESXI_004 | A proof of maintenance log is available to report on archived maintenance activity. | Req. 10 |
| | ESXI_005 | On ESXi and VMware vCenter Server Appliance™, the SSH service is disabled by default. Remote access to ESXi via SSH, or Web Client or API over HTTPS, can be configured as the secure communication protocol. Session identifiers are invalidated after session termination. | Req. 1<br>Req. 4 |
| | 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 root privileges. Password requirements willbe managed via the external authentication solution (minimum password, account lockout, and account lockout threshold). | Req. 7<br>Req. 8 |
| | 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 key manager. | Req. 3<br>Req. 4<br>Req. 8 |
| | ESXI_008 | ESXi can push logs to be stored in an external log repository that supports syslog, including vRealize Log Insight. If 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. | Req. 10 |
| | 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 be processed. | Req. 5<br>Req. 6<br>Req. 11 |

| | | | |
|---|---|---|---|
| | ESXI_010 | ESXi and vCenter audit quality logging in 6.5 is enabled by default. Changing logging levels is only for troubleshooting logs used by GSS. | Req. 10 |
| | ESXI_011 | If ESXi has Secure Boot enabled, any attempt to execute unsigned binaries will be blocked. All shell commands are logged via syslog and the attempt to install unsigned binaries will be logged. | Req. 10 |
| | ESXI_012 | ESXi can be configured to display a log-on banner before granting access to the system. | Req. 8<br>Req. 10 |
| | ESXI_013 | ESXi provides memory safeguards to protect it from executing unauthorized code. | Req. 2<br>Req. 5 |
| | ESXI_014 | ESXI limits the use of resources through Resource Pools, which can be constrained or prioritized based on Priority. | Req. 2 |
| | ESXI_015 | ESXi has the capabilities to establish firewalls using vLAN and deny traffic by default and only allowing explicitly designated traffic. | Req. 1 |
| | ESXI_016 | ESXi patching is performed via vCenter using VMware vSphere Update Manager (VUM). | Req. 6 |
| | ESXI_017 | vSphere Hardening Guide provides support for ESXi and vCenter hardening procedures. | Req. 12 |
| | ESXI_018 | Logon authentication techniques includes multi-factor authentication. | Req. 8 |
| | 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 multi-factor authentication. | Req. 8 |
| | ESXI_020 | ESXi can use Secure Boot integrated with AirWatch for asset management and UEM for Windows to detect and isolate rogue devices. | Req. 11 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | | | |
| AppDefense | AD_001 | AppDefense monitors all application endpoints within an environment using its Intended State Engine (ISE), which is located in the virtualization layer. Since AppDefense is installed in the vSphere hypervisor, it is completely isolated, ensuring secure communication throughout the environment. AppDefense actively monitors endpoints within the environment for any changes to their intended state. It correlates to the changes with a snapshot of the endpoint to discern if the changes are permitted. | Req. 8<br>Req. 11 |
| | AD_002 | Access rights, corresponding to AppDefense, can be established through vSphere, which has the ability to prevent users from accessing AppDefense Manager. Now SaaS manager has independent light weight role-based access control (RBAC) available. | Req. 7 |
| | AD_003 | The AppDefense Manager is capable of logging activity from users with root privileges via any applications monitored by AppDefense. A user can configure multiple logging methods through the AppDefense Manager. | Req. 10 |
| | AD_004 | Logs and records generated through AppDefense are reliant upon functionality provided by vSphere. Event capturing can be completely fine-tuned using both the vSphere Web Client and the AppDefense Manager. | Req. 10 |
| | AD_005 | Substantial storage space can be configured via vSphere and applied through the AppDefense Manager. vSphere will notify the user if any storage is reaching maximum capacity and includes those environments where AppDefense is configured in. | Req. 6<br>Req. 11 |
| | AD_006 | AppDefense alerts to any and all changes within the environment including auditable event failure and can be configured through its “Scopes" feature. Additional configuration can be accomplished through the vSphere Web Client. | Req. 6<br>Req. 11 |
| | AD_007 | AppDefense compiles event logs through its "Alerts" tab and can be reviewed at any time. | Req. 10 |
| | AD_008 | AppDefense affords the user the ability to view all previous event logs at any time via the AppDefense Manager. This allows for the analysis of any questionable event. | Req. 10 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | AD_009 | Access to AppDefense logs can be configured to only be accessible via an admin account and can be further secured by using configuration setting through vSphere role-based access controls (RBAC). In SaaS, light weight RBAC has been provisioned on AppDefense with 2 roles - Admins AND Analyst. | Req. 8<br>Req. 10 |
| | AD_010 | AppDefense is integrated within the vSphere environment, which includes a full view of the ports and protocols in use. AppDefense includes a full list of application and services that are currently in use. AppDefense is capable of learning the intended state of the environment and can whitelist processes accordingly through its "Learning Mode" When malicious activity is suspected within the environment, AppDefense can suspend, or completely shut down, any application and device. | Req. 2<br>Req. 11 |
| | AD_011 | Unique identifiers are possible within the vSphere; AppDefense heavily relies on vSphere for this feature. Password policy management is via vCenter password policy. | Req. 1<br>Req. 8 |
| | AD_012 | AppDefense employs the use of a continuous detection system that is capable of responsive measures when malicious actions appear to be present. AppDefense responds by suspending, shutting down, and taking a snapshot of the environment. AppDefense also uses a "Learning Mode" to identify the desired functionality of applications within the environment. AppDefense prioritizes every vulnerability using real-time threat information collected from sensors around the world. AppDefense ingests this feed from Kenna Security to determine the overall risk for your environment. | Req. 11<br>Req. 12 |
| | AD_013 | The separation of various domains is accomplished via vSphere, of which AppDefense is integrated with. Users' privileges are applied to each separate domain. We can further define scopes and services for specific applications within the AppDefense manager. | Req. 7<br>Req. 8 |
| | AD_014 | During the course of a debilitating event, AppDefense will respond by isolating the threat and suspending that section of the environment. Fail- safe procedures take the form of snapshots of the environment, which can be used to restore functionality to compromised applications. It can monitor the integrity of the agent itself, kernel of ESXi and workload. | Req. 11<br>Req. 12 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | AD_015 | AppDefense lies within the hypervisor of vSphere, affording it the ability to isolate various elements of applications. | Req. 6<br>Req. 11 |
| | AD_016 | Unauthorized code execution can be mitigated via the detection capabilities of AppDefense. If anomalies are detected within the environment, such as unauthorized code execution, AppDefense will alert and respond. | Req. 5<br>Req. 6<br>Req. 11 |
| | AD_017 | AppDefense is installed within the hypervisor of vSphere (the virtualization layer),) and monitors various endpoints in the environment. These endpoints are the desirable attack vector, making this the effective area to monitor. | Req. 11 |
| | AD_018 | Suspension of the endpoint (in Virtual infrastructure) environment can occur if AppDefense detects the use of unauthorized, executable code. It has next gen anti-virus capabilities that can monitor integrity of system and suspicious activities. | Req. 2<br>Req. 6<br>Req. 11 |
| | AD_019 | AppDefense can be fully automated and can issue automated responses when various anomalies are detected, such as using virtualization processes such as suspending and shutting down the environment. Intended state engine prevents execution of untrusted binary code or programs. | Req. 11 |
| | AD_020 | AppDefense can be fully automated and can issue automated responses when various anomalies are detected. Suspending and shutting down the environment can be manually configured by an administrator. By default, all Integrity violations are alerted in vSphere dashboard / SaaS manager | Req. 11 |
| | AD_021 | AppDefense has the ability to automatically roll the appliance back to a stable state in case of failure. Automatic reversion increases comfort with turning on auto upgrade. | Req. 6 |
| | | | |
| | NSX_T_001 | NSX-T session time-out will terminate session after a defined period of inactivity (default is set to 15 minutes). | Req. 4<br>Req. 12 |
| | NSX_T_002 | NSX-T enables password enforcement rules such as setting Password Expiration (set to 3 months by default), Password Length (set to 12 characters by default), Password Complexity (turned on by default). Entering of passwords is masked. All stored passwords are encrypted. Password resets require the previous password to be provided. | Req. 10<br>Req. 11 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| NSX-T | NSX_T_003 | NSX-T supports segmentation through the use of firewall rules, port restrictions, and network segmentation via vLANs to restrict communication between VMs. This can provide additional security to applications and databases that are communicating over the network by enforcing isolation and security rules for security architecture using segmentation concepts. | Req. 1<br>Req. 7<br>Req. 8 |
| | NSX_T_004 | NSX-T can be configured to support two sets of standby facilities and replicate configurations across two data centers to support emergency, offsite relocation. | Req. 10 |
| | NSX_T_005 | NSX-T services are restricted from kernel level access, and from components further up the technology stack. Also, additional services can be restricted. | Req. 1<br>Req. 4<br>Req. 8 |
| | NSX_T_006 | Session lockouts are enforceable and require users to re-authenticate after a session time-out. | Req. 8 |
| | NSX_T_007 | Account lockout threshold can be altered. | Req. 8 |
| | NSX_T_008 | NSX-T supports logging and includes auditable event selections such as: privileged actions (who did what and when), system changes, configuration changes, administrative events, account management of both users (including account lockout and password expiration), and alerts to specify the configurations to monitor. This information can be sent via Syslog to vRLI, or another log repository solution. | Req. 10 |
| | NSX_T_009 | NSX-T can be used to monitor the network for inappropriate usage and security violations. Network activity and traffic can be logged and evaluated, along with firewall traffic. This can support system monitoring for inappropriate usage and other security violations. | Req. 10<br>Req. 11 |
| | NSX_T_010 | NSX-T closely monitors session IDs to minimize the risk of replay attacks. | Req. 10 |
| | NSX_t_011 | During a Panic Attack, the system will restart by default and potentially shut down after repeated failures. | Req. 7<br>Req. 8<br>Req. 12 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | NSX_T_012 | NSX-T provides two mechanisms to detect unauthorized components, or rogue devices. Natively, NSX-T can monitor VMs and Edge Devices (infrastructure gateways) and can isolate them if they are out of compliance. Using the Guest Introspection Framework, NSX-T can extend this capability to include mobile devices and endpoint devices. When NSX-T detects an authorized component, or rogue device, the system can then isolate or quarantine these form factors based on tagging rules or security policies. | Req. 8<br>Req. 12 |
| | NSX_T_013 | NSX-T can support the collection of Information Technology inventory by providing an inventory of VMs with access to the Software Defined Networking layer. | Req. 1<br>Req. 6<br>Req. 7<br>Req. 10 |
| | NSX_T_014 | NSX-T 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, and through configuration policies and firewall polices to manage internal information flow. | Req. 7<br>Req. 8 |
| | NSX_T_015 | Combined with Workspace One Access or another integrated Identity Access Management tool, NSX-T can support multi-factor authentication. | Req. 7<br>Req. 8 |
| | NSX_T_016 | NSX-T firewalls can be configured to include Intrusion Detection System (IDS) with policies that are set to ""default"" responses such as ""auto deny"" when an attack is detected. This can be an effective method to detect unrecognized devices, VMs placed in the DMZ, or other abnormal traffic. | Req. 11 |
| | NSX_T_017 | NSX-T can manage all internal network connections and provides documentation to describe the networking components available for deployment. This can assist in establishing a network security policy. | Req. 1 |
| | NSX_T_018 | NSX-T provides routing capabilities to manage all external communications in and out of the data center (using the constructs of Tier Zero and Tier One to denote the traffic pathways). This can be used to develop a boundary defense. | Req. 11 |
| | NSX_T_019 | NSX-T can distinguish between a Trusted Network and an Untrusted Network to support boundary protection. Rules can be assigned to protect the boundary and confirm external perimeter network access is managed accordingly. | Req. 1 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | NSX_T_020 | NSX-T can be implemented with a fault-tolerant architecture. This can be used to schedule backups and restore backups too. | Req. 6<br>Req. 11 |
| | NSX_T_021 | NSX-T can restrict external network connectivity so that external network access is restricted to a network segment (vLAN/IP pools) and firewall restriction to Deny or Allow access based on a range or list of IP Addresses. | Req. 1 |
| | NSX_T_022 | NSX-T documents product capabilities to support security architecture through publication and version maintenance in the Product Applicability Guide (PAG whitepaper). | Req. 1<br>Req. 7 |
| | NSX_T_023 | For NSX-T's underlying Operating System (Ubuntu) a series of integrity checks are performed. For example, this includes detecting for any kernel integrity violations, disk storage errors, or other alarms that fail an integrity check. | Req. 6<br>Req. 11 |
| | NSX_T_025 | NSX-T contains a trust store for storage of keys and certificates, but this is not a Key Management System. This can be used to configure support of self-signed certificates, and certificates signed by a certificate authority (CA signed), including Public Key certificates. This can also be used to house revoked public certificates to support certification revocation procedures, which can be used to support network traffic and data flow enforcement. | Req. 8 |
| | NSX_T_026 | NSX-T provides some capabilities to facilitate detection of malicious code traffic. Using stateful scan and firewall traffic monitoring is one capability identify malicious code. 3rd party vendors can integrate with NSX-T to enhance detection of malicious activity. | Req. 1<br>Req. 5 |
| | NSX_T_027 | NSX-T as a virtualized networking infrastructure canmove around machines to recovery networks to support fail-safe procedures. | Req. 6 |
| | NSX_T_028 | NSX-T provides visibility into the capacity of the system via dashboards to report usage and infrastructure capacity, including number of VMs supported, transport nodes supported, and the<br>overall health of the platform. | Req. 10 |
| | NSX_T_029 | NSX-T provides Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) based in the firewall. These capabilities can be used to support detection capabilities and incident response capabilities. | Req. 10<br>Req. 11 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | NSX_T_030 | NSX-T includes some Denial of Service (DoS) attackprevention mechanisms, which may support detection processes but will not monitor and detect DoS before the attack occurs. This includes firewall rules with tracking mechanisms to block a port or take other precautionary measures once a DoS attack is identified. | Req. 1 |
| | NSX_T_031 | NSX-T can provide firewall-based Access Control Listfunctionality to restrict access based on IP Addresses and VM names. | Req. 1 |
| | NSX_T_032 | NSX-T comes with pre-defined roles (13) that can be assigned to enable Role Based Access Control. In addition, new roles can be developed based on an inventory of functionality to be used as custom roles. This capability can support both Separation of Duties, and the concept of Least Privilege. | Req. 1<br>Req. 7 |
| | NSX_T_033 | NSX-T can restrict access based on configurations explicitly authorized such as protocols, ports, applications, and services based on an approved configuration standard. | Req. 1 |
| | NSX_T_034 | NSX-T provides and maintains a system hardening guide. | Req. 2 |
| | NSX_T_035 | NSX-T enables SSH access, and it is disabled by default. Access control via SSH includes enforcement of password parameters, such as password length, requiring password change upon first login, and account lockout duration. | Req. 4<br>Req. 8 |
| | NSX_T_036 | NSX-T includes three default accounts. The "root" user is disabled by default. The "admin" account can be disabled. The "auditor" account is restricted to read-only and can also be disabled. The system can enforce changing default passwords. | Req. 8 |
| | NSX_T_037 | In support of User Access Controls and in particular process controls such as adding, modifying, or removing users, NSX-T can be integrated with Active Directory to support access controls. | Req. 8 |
| | NSX_T_038 | NSX-T provides local authentication mechanisms that require a username and password. However, the preferred method is for external integration with user authentication mechanisms, such as tokenization using the O-AUTH framework. | Req. 8 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | NSX_T_039 | NSX-T supports application tagging at the network level to restrict information flow based on the data a VM is permitted to or restricted from sharing. This control policy can include information transmitted over network paths, restricted by environment, restricted by type of infrastructure, or explicit applications. | Req. 1 |
| | NSX_T_040 | NSX-T can restrict change management control by removing local admin access and granting it instead to the Admin Group, which can be authorized tomake changes to NSX-T based on the assignment of this group/role to approved user(s). | Req. 7 |
| | NSX_T_041 | NSX-T can encrypt network traffic and monitor for exceptions to support network confidentiality and data protection, including loss of data over the network. | Req. 4 |
| | NSX_T_042 | NSX-T provides the capability to enable System Entropy, a tool to monitor intel chip information and firmware integrity. This can be used to detect unauthorized changes to underlying chip firmware. | Req. 11 |
| | NSX_T_043 | NSX-T provides an alert dashboard to notify the administrator of any suspicious activity. Alerts can include firewall Intrusion Detection System (IDS). Integration with 3rd party tools can include email notification. | Req. 11 |
| | NSX_T_044 | NSX-T logging can be configured to protect logs from failure by enabling notification of failure. Logging can be set to specified retention period (30 days by default, or when sizing limit is reached), log sizing can be specified to either enable archiving of files or overwriting logs or redirecting logs to a log infrastructure such as vRLI or other logging repository via Syslog. Access to logging data can be restricted to the enterprise administrator role. Monitoring of logs for any unauthorized changes can also be enabled. | Req. 10 |
| | NSX_T_045 | NSX-T has the capability to redirect logs to a SIEM or copy logs and send them to another logging tool for analysis. Logging is collected across the software defined networking infrastructure and can be incorporated into system-wide time-correlated audit trails. Logging can be used to track audit trails across system components such as nodes, type of event, location, user, and correlated with other data to support adding additional elements. Data frequency and retention parameters can be set. | Req. 10 |

| | | | |
|---|---|---|---|
| | NSX_T_046 | NSX-T can be configured to prompt users with a loginbanner, or system use agreement that is displayed as a message. | Req. 7<br>Req. 8 |
| | NSX_T_047 | NSX-T can capture some events of unauthorized access, such as performing events that are not authorized. In some cases, the UI will prompt the user that sufficient permission is unavailable to perform the desired action. | Req. 7<br>Req. 10 |
| | NSX_T_048 | NSX-T system clocks can be synchronized to NTP to enable accurate and universal time source logging. | Req. 10 |
| | NSX_T_049 | NSX-T can use Edge Nodes to detect kernel accesstampering. NSX Manager can be configured to detect integrity of the kernel and shut it down by default. | Req. 11 |
| | NSX_T_050 | NSX-T monitors memory and takes precautions basedon best practices to safeguard memory from unauthorized code execution. | Req. 5 |
| | NSX_T_051 | NSX-T establishes session authenticity through Transport Layer Security (TLS) version 1 by default. 0 is disabled due to recent industry guidance that it has known vulnerabilities. Version 1.1 and 1.2 are supported and recommended. | Req. 4 |
| | NSX_T_052 | NSX-T can prioritize traffic to supporttelecommunications Service Level Agreements by using Quality of Service (QoS) customization. | Req. 4 |
| | NSX_T_053 | NSX-T can whitelist or blacklist applications from communicating VM to VM by using firewall rules to enforce communication access rules. | Req. 1 |
| | NSX_V_001 | Information protection can be implemented usingpolicies that restrict access information flow based on network micro-segmentation. | Req. 4<br>Req. 12 |
| | 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) and/or Intrusion Prevention System (IPS) systems. | Req. 10<br>Req. 11 |
| | NSX_V_003 | NSX identity firewall supports role-based access controls (RBAC) to limit permissions that restrict viewing virtual machines (VMVMs). Also, micro- segmentation can be used to manage access to specific areas of the network using RBAC and minimize attack surface by using NSX to isolate and segment workload and platform components. This includes configuring the system to restrict the development team from having access to the production environment. | Req. 1<br>Req. 7<br>Req. 8 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | | | |
| NSX-V | 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. | Req. 10 |
| | NSX_V_005 | Remote access to products can be restricted to just SSH, or other desired and secure communication protocols. Manually, the configuration files can be altered in NSX to further restrict access to specific components such as: NSX Manager, NSX Edge, or NSX Controller. By default, SSH access is disabled. This includes controlling remote access through an existing access control and authentication solution, and invalidating session identifiers upon session termination. | Req. 1<br>Req. 4<br>Req. 8 |
| | NSX_V_006 | Session lockouts are enforceable and require users to re-authenticate after a session time-out. | Req. 8 |
| | NSX_V_007 | Account lockout threshold can be altered. | Req. 8 |
| | 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. | Req. 10 |
| | 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 can monitor enforcement of security rules and firewall policies. NSX Endpoint Monitoring enables Guest Introspection Framework capabilities to monitor endpoint processes, specifically on Windows virtual machines. | Req. 10<br>Req. 11 |
| | NSX_V_010 | NSX provides monitoring of the system using event logs and other security logs to identify abnormal activity. The NSX NetX feature can redirect network traffic flow to be redirected to third-party Intrusion Detection System (IDS) solution on a per security policy basis to support granular event logging. | Req. 10 |
| | NSX_V_011 | NSX can deny access to rogue devices that have not been approved using SpoofGuard. Also, a default deny with a list of approved devices can be established to further prevent rogue devices. | Req. 7<br>Req. 8<br>Req. 12 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | 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. | Req. 8<br>Req. 12 |
| | 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. | Req. 1<br>Req. 6<br>Req. 7<br>Req. 10 |
| | 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. | Req. 7<br>Req. 8 |
| | NSX_V_015 | Network access controls can be managed using NSX, which can also be integrated with third-party tools to support managing network access. | Req. 7<br>Req. 8 |
| | 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. | Req. 11 |
| | NSX_V_017 | NSX can manage all internal network connections and provides documentation to describe the networking components available for deployment. | Req. 1 |
| | 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. | Req. 11 |
| | NSX_V_019 | Using the 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. | Req. 1 |
| | NSX_V_020 | NSX can be implemented with a fault-tolerant architecture; documentation supporting this design is available. | Req. 6<br>Req. 11 |
| | NSX_V_021 | NSX can restrict inbound internet traffic inside the DMZ using ESG FW, NSX Edge services gateway firewall, distributed firewall, and the principles of DMZ Anywhere. | Req. 1 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | 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. | Req. 1<br>Req. 7 |
| | 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. | Req. 1<br>Req. 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. | Req. 1<br>Req. 8 |
| | NSX_V_025 | NSX can use a Root Certification Authority to support Public Key Infrastructure within the virtualized network platform. | Req. 3<br>Req. 4 |
| | NSX_V_026 | NSX can support analytics to be used with third-party solutions to identify behavior and characterize malicious code, which would be supported via Guest Introspection. | Req. 10<br>Req. 11 |
| | NSX_V_027 | In the event of fail-safe procedures, NSX can move around machines to other recovery networks via automated quarantine actions. | Req. 4<br>Req. 6<br>Req. 11 |
| | NSX_V_028 | NSX provides a dashboard to monitor the platform's health, which can inform users around maintenance information of the platform itself. | Req. 6<br>Req. 11 |
| | NSX_V_029 | NSX can be configured to protect against unauthorized data mining of the NSX Postgres database. | Req. 2<br>Req. 7 |
| | 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. | Req. 6<br>Req. 10<br>Req. 11 |
| | NSX_V_031 | NSX provides stateful firewall capabilities that can support adding devices requiring access control based on an Access Control List. | Req. 7<br>Req. 8 |
| | 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 auditor/read only). | Req. 7 |
| | NSX_V_033 | NSX can be architected to place firewalls between security domains, DMZ, and other network zones. | Req. 1 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | 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, including length, requiring password change upon first login, and account lockout duration. | Req. 8 |
| | NSX_V_036 | NSX provides and maintains a system hardening guide. | Req. 6<br>Req. 12 |
| | | | |
| Site Recovery Manager | SRM_001 | Recovery can be included in simulated events as part of the larger continuity plan training. The simulated failover can be triggered manually. In addition, tier systems can be prioritized or omitted through the use of consistency groups (high impact versus low impact, for example). | Req. 6 |
| | SRM_002 | Site Recovery Manager can push logs to be stored in vRealize Log Insight. A content pack is provided to facilitate Site Recovery Manager logging and dashboard visualization of logging. | Req. 10 |
| | SRM_003 | Results of test run can be included in documentation to evidence results of continuity planning exercises. Recovery mode can be run within the test plan and export the results to showcase the outcome of every test run inside test mode. | Req. 6 |
| | SRM_005 | Site Recovery Manager is an application that runs in Windows and relies on events and standard maintenance logs provided by Windows. Proof of maintenance and archival of reports depends on configuration of Windows event logging. | Req. 10 |
| | SRM_006 | Access to Site Recovery Manager is only available via a web client using vSphere. The vSphere web client manages authentication and session handling. Upon session termination, session identifiers are invalidated. | Req. 8 |
| | SRM_007 | Remote access is possible via Remote Desktop Protocol (RDP) to the Site Recovery Manager system. This can be managed through external authentication solutions. Use of Site Recovery Manager does not require RDP access mechanism, and RDP is usually allocated for administrative access only. | Req. 4<br>Req. 8 |
| | SRM_008 | Site Recovery Manager relies on vCenter to manage and assign user access and to manage user accounts, including assignment of roles to restrict functionality. | Req. 7 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | SRM_009 | Site Recovery Manager can be configured to use Active Directory or vSphere domain accounts that adhere to organizational password standards, including forcing users to change their password upon first login. | Req. 8 |
| | | | |
| vCloud Usage Meter | UM_001 | Proxy configuration is available during the initial setup of Usage Meter and also features full LDAP configuration. | Req. 8 |
| | UM_002 | vCloud Usage Meter retains a list of connections that are the subject of monitoring and usage collection. vCloud Usage Meter is installed within the vSphere environment, which is capable of full LDAP integration where user accounts can be controlled even further. | Req. 8 |
| | UM_003 | vSphere logs user activity and can be maintained fora set period of time. These logs can be secured via various methods, such as user account permissions. | Req. 10 |
| | UM_004 | Users can be uniquely identified through different aspects via the vSphere Web Client, and various methods derived from LDAP integration and configuration. | Req. 8 |
| | UM_005 | vCloud Usage Meter can be configured to use proxy services, in addition to using LDAP integration to manage user IDs and passwords within a secure environment. This includes configuring the minimum and maximum password ages that can be applied to user accounts. | Req. 8 |
| | UM_007 | LDAP and various parameters derived from vSphere Web Client can be employed to maintain separation between user functionality and system management. | Req. 8 |
| | UM_008 | Data transmission can be secured through proxy configurations and are employed during the initial setup of vCloud Usage Meter. | Req. 1<br>Req. 4 |
| | | | |
| vCloud Director | vCD_001 | vCloud Director has the ability to administrate useraccounts, in addition to assigning those accounts various permissions, through the administration home page and LDAP integration. Accountmanagement can also be accomplished through the vCloud API. | Req. 7<br>Req. 8 |
| | vCD_002 | Logging capabilities are configured, and observed,through the vCloud Director's manage and monitor portal. | Req. 4<br>Req. 10 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | vCD_003 | Session lock capabilities can be employed, such as configuring the number of invalid logins before lockout occurs, through the vCloud Director's administration portal and also within the general system settings. | Req. 8 |
| | vCD_004 | Configuring device and accounts that have accesscontrol permissions can be accomplished through the vCloud Director's administration portal. | Req. 7<br>Req. 10 |
| | vCD_005 | System administrator account permissions cannot be altered and encompass all existing rights, in addition to rights only associated with an administrator role. | Req. 7<br>Req. 8 |
| | vCD_006 | The administrator account associated with vCloud Director has the capability of managing the access authorization list and is the only account that can do so. | Req. 7 |
| | vCD_007 | vCloud Director includes monitoring functionality, which can produce audit logs and cost reports, to provide insight regarding the overall statistics of the environment. | Req. 10 |
| | vCD_008 | The administrator account associated with vCloudDirector can fully manage user accounts, including properly updating accounts and their access rights. | Req. 8 |
| | vCD_009 | An administrator has the ability to restrict user access to nearly all facets of the vCloud Director environment, including log management and observation. | Req. 10 |
| | vCD_010 | vCloud Director has the ability to monitor all assetswithin its environment and produce reports that can later be used during forensic analysis. | Req. 10 |
| | vCD_011 | Authentication measures are handled through thevSphere environment, of which vCloud Director is a part of. | Req. 1 |
| | vCD_012 | vCloud Director can be coupled with vCloud Director Availability to achieve proper contingency functionality within the vCloud Director environment, and other facets of the vSphere environment. | Req. 12 |
| | vCD_013 | AppDefense can be integrated into the vSphere environment, which vCloud Director relies upon, to establish and maintain intrusion detection functionality. | Req. 10<br>Req. 11 |
| | vCD_015 | Intrusion detection procedures can be implemented within the vSphere environment, with which vCloud Director is integrated with, through the addition of AppDefense. | Req. 11 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | vCD_017 | An Incident Response program can be established within one of the cloud environments that vCloud Director is responsible for managing. Users are able to review and update the incident response procedures following the closure of such an event, while using features afforded through AppDefense to vSphere, which encompasses vCloud Director. | Req. 12 |
| | vCD_018 | While using AppDefense within the vSphere environment, which contains vCloud Director, a user is afforded the ability of establishing and maintaining various incident response procedures. | Req. 12 |
| | vCD_019 | User accounts can be provisioned with privileges based on the roles that they are expected to perform on the system. | Req. 8 |
| | | | |
| vCloud Availability forvCloud Director | vCA_001 | vCloud Director Availability is integrated with vCloud Director, which is installed in the vSphere environment. In turn, users that are currently using vCloud Director Availability services are subject to the termination of their session if idle for too long. | Req. 8 |
| | vCA_002 | It is possible to limit super user accounts to designated system administrators, if using LDAP through vSphere. | Req. 7 |
| | vCA_003 | Account lockout procedures can be configured by the use of LDAP services, which can be indirectly used in conjunction with vCloud Director Availability. The procedures that can be configured are account lockout threshold and duration, in addition to the set number of consecutive login attempts before such procedures are triggered. | Req. 8 |
| | vCA_004 | vSphere has its own internal log management processes that can be used via any user, with applicable permissions, of vCloud Director Availability. A user of vCloud Director Availability can configure logging mechanisms within the vSphere environment that can be used for later analysis. | Req. 10 |
| | vCA_006 | Event logs stemming from the vSphere environment, of which vCloud Director Availability is a part of, can be stored securely and protected from unauthorized access. | Req. 10 |
| | vCA_007 | A complete network overview can be reviewed viavSphere. This includes any ports, protocols, and services currently active within the environment. | Req. 1 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | vCA_008 | When using LDAP integration within the vSphere environment, uniquely identifying properties can be employed to user accounts. This includes those who have access to vCloud Director Availability through vSphere. | Req. 8 |
| | vCA_009 | Proxy measures can be implemented within the vSphere environment, in turn affecting vCloud Director Availability, and can be configured to only allow access to properly identified and authenticated connections. | Req. 1 |
| | vCA_010 | The "Enable Password History" feature can be enabled via the vSphere Web Client, or through LDAP integration, and affects vCloud Director Availability services due to access being derived through vSphere. | Req. 8 |
| | vCA_011 | Various password settings can be configured through LDAP, which indirectly affect vCloud Director Availability services. | Req. 8 |
| | vCA_012 | System management is accomplished through the vSphere Web Client, which is completely separate from vCloud Director. vCloud Director governs services such as that of vCloud Director Availability. | Req. 8 |
| | vCA_014 | User privileges are set through configurations stemming from either vSphere, or LDAP integration, all of which affect vCloud Director Availability due to being deeply entangled with vSphere through vCloud Director. | Req. 8 |
| | | | |
| | VCENTER_001 | vCenter supports access control configuration including session timeout, login attempts, account lockout threshold, account lockout duration, minimum password age, and requiring re-authentication. | Req. 8 |
| | VCENTER_002 | Concurrent sessions can be limited on web clients, and virtual machine consoles. | Req. 7 |
| | VCENTER_003 | vCenter employs unique user identifiers through Platform Services Controller (PSC), ™, which manages integration with SSO. Unique user identifiers can be assigned using Platform Services Controller. | Req. 8 |

| | | | |
|---|---|---|---|
| vCenter | VCENTER_004 | Access is supported using Role Based Access Control (RBAC) through local operating system access control, or integration with Active Directory and federated services. vCenter access control is established through permissions, which are assigned by a combination of roles and privileges. Users are assigned to roles. Privileges are assigned to roles. Thus, access authorization is a combination of the role a user is assigned and the privilege a role is assigned. | Req. 8 |
| | VCENTER_005 | Super user capabilities in vCenter are a combination of privileges, which can be assigned to administrator roles. Assignment of elevated privileges can be restricted to only those users that are approved as designated system administrators. | Req. 7 |
| | 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. | Req. 12 |
| | VCENTER_007 | vCenter can list all the virtual machines and support creating an inventory of technology systems. | Req. 2<br>Req. 9 |
| | VCENTER_008 | Remote access to vCenter via SSH, or Web Client or API over HTTPS, can be configured as the secure communication protocol. For the VMware vCenter Server Appliance™, it runs on Linux and can be restricted to only accept HTTPS. Session identifiers are invalidated after session termination. | Req. 4<br>Req. 8 |
| | VCENTER_009 | vCenter can be configured to log-off out inactive sessions. By default, inactivity is set to log out after 15 minutes. | Req. 8 |
| | 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. | Req. 4 |
| | VCENTER_011 | vCenter can push logs to be stored in an external log repository that supports syslog, including vRealize Log Insight. If 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. | Req. 10 |
| | 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. | Req. 10<br>Req. 11 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | 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. | Req. 10 |
| | VCENTER_014 | vCenter can be configured to display a login banner to users before granting access to the system. | Req. 7<br>Req. 8 |
| | VCENTER_015 | vCenter supports enhanced logging of audit level events to support third-party integration with tools such as Introduction Detection Systems (IDS). | Req. 10<br>Req. 11 |
| | VCENTER_016 | vCenter has granular access control permissions that can be applied to virtual machines, VM clusters, and hosts. An organization can define the roles that can access these systems, such as bifurcating access between developers and production environments. | Req. 1 |
| | 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 networktraffic and firewall are inherited based on the user's configuration of the Windows appliance. | Req. 1<br>Req. 7 |
| | 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. | Req. 3<br>Req. 4 |
| | VCENTER_020 | vCenter can push audit trail logs to be archived in anexternal log repository that supports syslog, including vRealize Log Insight. | Req. 10<br>Req. 11 |
| | VCENTER_021 | vCenter can patch ESXi hosts through VMware vSphere Update Manager (VUM). | Req. 6 |
| | VCENTER_022 | vCenter can facilitate installation of critical security updates for ESXi. VMware vSphere Update Manager (VUM) alerts vCenter of any firmware issues that affect ESXi and can be used to install patches, and also automate installation of updates. vCenter has a manual feature to check to see if there are any updates available for vCenter without specifying the nature of the update (security, or operational). | Req. 6 |
| | VCENTER_023 | vSphere Hardening Guide provides support for ESXi and vCenter hardening procedures.<br>https://www.vmware.com/security/hardening-guides.html | Req. 2<br>Req. 12 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| vRealize Log Insight | VCENTER_025 | vCenter natively can provide multi-factor authentication techniques such as CAT Card and RSA SecurID. | Req. 8 |
| | VRLI_001 | Using third-party software vRealize Log Insight can be configured to support non-repudiation of log entries and monitor access to logs to certify transactions are reputable. The access restriction would be applied at the operating system and restrict access to the underlying file system/database, since super users administering the operating system would be able to access log information. | Req. 7<br>Req. 10 |
| | VRLI_002 | A proof of maintenance log is available to report on archived maintenance activity. | Req. 10 |
| | VRLI_003 | Session lockouts are enforceable and require users to re-authenticate after a session time-out. | Req. 8 |
| | VRLI_004 | Search queries can be configured to monitor the system for inappropriate usage, security violations, and other defined events. Monitoring tools include alerts and dashboards. Dashboards and interactive analytics are provided out-of-the-box, which can also be configured to enhance system monitoring. | Req. 10<br>Req. 11 |
| | VRLI_005 | vRealize Log Insight supports standard syslog and secure syslog. In addition, when using an internal vRealize Log Insight agent, a secure, encrypted protocol is enforceable. | Req. 10 |
| | VRLI_006 | Audit Dashboard is provided to analyze log data and support after-the-fact investigations. In addition, vRealize Log Insight can provide tamper protection by deploying a log system architecture configured to support multiple storage locations to minimize the risk of a central location from being corrupted or altered. | Req. 10 |
| | VRLI_007 | vRealize Log Insight can gather event logs across any device within the virtualized, or physical environment. Log data is stored in a centralized database. The logging database can be used to correlate system-wide audit trails. Security -related queries, dashboards, and alerts use time- stamps to support event log correlation. | Req. 10 |
| | VRLI_008 | vRealize Log Insight has a dashboard export feature to help distribute logs. In addition, a read-only view is available for designated users to log in and view the reports. | Req. 10 |
| | VRLI_010 | Backups of logs can be performed for all products using vRealize Log Insight. Remote archival of vRealize Log Insight logging data is supported. | Req. 10 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | VRLI_011 | Hosts can use a vRealize Log Insight agent or send logs via syslog to the centralized vRealize Log Insight log database to manage storage, retention, and protect logs from unauthorized activity. | Req. 10 |
| | VRLI_012 | Remote access to vRealize Log Insight is by default set to HTTPS. Session identifiers are discarded upon session termination. | Req. 4<br>Req. 8 |
| | VRLI_013 | vRealize Log Insight allows access control settings to be configured to manage sessions, including the following parameters: account lockout threshold, account lockout duration, and password policies. vRealize Log Insight can integrate authentication with the vCenter Platform Services Controller instance to enable enforcement of authentication parameters from Active Directory directly. | Req. 7<br>Req. 8 |
| | VRLI_014 | vRealize Log Insight provides management of user accounts through the Access Control panel, including managing users configured locally, and accounts created through an external authentication solution. | Req. 8 |
| | VRLI_015 | vRealize Log Insight allows users to be assigned to roles. The roles can be assigned granular access based on the organization's assignment of least privilege, or job responsibilities within the groups. VMware Identity Manager or an external authentication solution is required to administer this capability. vRealize Log Insight can integrate authentication with the vCenter Platform Services Controller instance to enable enforcement of authentication parameters from Active Directory directly. | Req. 7<br>Req. 8 |
| | VRLI_016 | vRealize Log Insight can manage an Access Control List via agent and host listings to manage devices and restricting the logs a device can access. Role - based access can limit access to specific log devices and log data. | Req. 7<br>Req. 8<br>Req. 10 |
| | VRLI_017 | If local accounts are created in vRealize Log Insight, users can be required to change their password upon first login. | Req. 8 |
| | VRLI_018 | Alerts are generated when agents are unresponsive, or offline after a defined period of time. | Req. 5<br>Req. 11 |
| | VRLI_019 | vRealize Log Insight collects logs in real time. Content packs to enhance dashboards and provide custom queries tailored to many VMware products. | Req. 10 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | | | |
| vRealize Network Insight | VRNI_001 | vRealize Network Insight receives NetFlow from VMware vSphere Distributed Switch (VDS) instances, which connect virtual machines. This can be used to monitor information flows and network flows. | Req. 10 |
| | VRNI_002 | A proof of maintenance log is available to report on archived maintenance activity. | Req. 10 |
| | VRNI_003 | Remote access to administrative features can be restricted to just SSH, or other desired and secure communication protocols. Manually the configuration files can be altered in vRealize Network Insight to further restrict access to vSphere. This includes controlling remote access through an existing access control and authentication solution, and invalidating session identifiers upon session termination. | Req. 7 |
| | VRNI_004 | After fifteen15 minutes of inactivity, users are locked out and required to re-authenticate. | Req. 8 |
| | VRNI_005 | vRealize Network Insight can push logs to syslog, or vRealize Log Insight. vRealize Log Insight can then apply tamper protection of logging that can be used during after-the-fact investigations without altering the event logs. | Req. 10 |
| | VRNI_006 | vRealize Network Insight can be used to monitordata center traffic and provide visibility to support monitoring activities. | Req. 11 |
| | VRNI_007 | vRealize Network Insight can be used to review network paths and troubleshoot components that are not communicating properly, such as a web server not reaching a database. This feature can also help in establishing distributed firewalls. | Req. 11 |
| | VRNI_008 | vRealize Network Insight logs network traffic with a default retention period of thirty (30) days, which can be extended to thirteen (13) months. This log data can provide audit trail support. | Req. 10 |
| | VRNI_010 | The vRealize Network Insight administrator can manage User Interface (UI) users. Users connect via a web portal UI. These user accounts can be reviewed, access control can be managed using roles (administrator, or read-only Member User) member user), and password complexity can be configured. | Req. 7<br>Req. 8 |
| | VRNI_011 | vRealize Network Insight traffic between the platform and proxy servers can be encrypted using certificates. | Req. 4 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | | | |
| vRealize Orchestrator | VRO_001 | Remote access to products can be restricted to just SSH, or other desired and secure communication protocols. Manually, the configuration files can be altered in vSphere to further restrict access to vSphere. This includes controlling remote access through an existing access control and authentication solution, and invalidating session identifiers upon session termination. | Req. 1<br>Req. 4 |
| | VRO_002 | vRealize Orchestrator can provide user information responsible for creating or modifying the virtual machine, virtual infrastructure asset information, or other information. This can be used to trace ownership, if the creation or modification are appropriate parameters to assist in deciphering ownership. | Req. 9<br>Req. 10 |
| | VRO_003 | A proof of maintenance log is available to report on archived maintenance activity. | Req. 10 |
| | VRO_004 | vRealize Orchestrator supports multiple roles to separate user functionality from system management functionality, and the capability to support the principle of least privilege user access control. | Req. 7<br>Req. 8 |
| | | | |
| vRealize Operations | VROPS_001 | A proof of maintenance log is available to report on archived maintenance activity. | Req. 10 |
| | VROPS_002 | Remote access to vRealize Operations is restricted by default. vRealize Operations appliance remote access can only be enabled to use SSH via the vCenter VM Console. vROPS user console. vRealize Operations UI is only accessible via a secure URL. Upon session termination, session identifiers are invalidated. | Req. 1<br>Req. 4 |
| | VROPS_003 | Session lockouts are enforced by default and requireusers to re-authenticate after a session time-out. User privileges can also be defined in the product. | Req. 8 |
| | VROPS_004 | Using a management pack, specific to the compliance area (PCI and HIPAA only at this time), vRealize Operations can be used to support a configuration management program. The contentpack relies on vSphere to evaluate technical configurations and settings based on the compliance pack's baseline. | Req. 6 |
| | VROPS_005 | vRealize Operations has a maximum of concurrent sessions (6); this setting cannot be altered. | Req. 8 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | VROPS_006 | Using a management pack, vRealize Operations can store information that is collected by agents via the use of plugins to collect data from guest operating systems running in virtual machines. | Req. 10 |
| | VROPS_007 | vRealize Operations can perform capacity planning, forecasting, and reporting. An input into this planning process can include comparing capacity between production and backup sites. | Req. 12 |
| | VROPS_008 | Initial login with the root account requires users to change the password. New users logging in for the first time can also be required to change their password upon initial login. | Req. 8 |
| | VROPS_009 | vRealize Operations can monitor the storage of vSAN (or another database) and upon running low, it can provide an alert and recommendation to adjust the storage capacity. The storage capacity data and alerts can be archived to support retaining records in accordance with applicable regulations. | Req. 11 |
| | VROPS_010 | vRealize Operationscan be configured to support account lockout duration, number of failed attempts, and password length and complexity. | Req. 8 |
| | VROPS_011 | vRealize Operations can push audit trail logs to bearchived in an external log repository that supports syslog, including vRealize Log Insight. | Req. 10 |
| | VROPS_012 | vRealize Operations permits creating roles and groups using Role Based Access Control (RBAC). Granularity can be applied to view or edit objects, run reports, and other functionality. Separate Administrative UI is available for the admin to perform actions related to vROPS infrastructure changes (like adding node , HA configuration). | Req. 7<br>Req. 8 |
| | VROPS_013 | vRealize Operations provides metrics and system performance reports that users can compare against organizational standards or industry benchmarks. The metrics include capacity planning, virtual machine sizing, and behavioral analysis. | Req. 8 |
| | | | |
| vSAN | vSAN_001 | Access to data storage in vSAN is managed by roles within vCenter. vSAN 6.5 introduced a new role to manage enabling/disabling encryption that can be further applied to restrict non-cryptographic user access to configuration of this feature. | Req. 7<br>Req. 8 |
| | vSAN_002 | Logging capabilities can be enabled and customized to capture event information. | Req. 10 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | vSAN_003 | Logging can be synchronized to system clocks (NTP) and also capture a date and time stamp. | Req. 10 |
| | 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. | Req. 10 |
| | vSAN_005 | Session lockouts are enforceable and require users to re-authenticate after a session time-out, which are controlled by vCenter or ESXi. | Req. 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. | Req. 3<br>Req. 4 |
| | vSAN_007 | vSAN can be patched via vCenter's VMware Update Manager patching capabilities. In addition, vSAN 6.6 has the ability to patch firmware controller drivers for participating vendors. | Req. 6 |
| | 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 instance, which can be holistically analyzed via vRealize Log Insight or custom API log reporting tool. | Req. 10 |
| | 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. | Req. 6 |
| | vSAN_010 | Cryptographic management features supported include rotation of keys via UI or API integration, changing key management system (KMS) providers, and broadly enabling or disabling encryption. These capabilities can be used to support cryptographic procedures. | Req. 3<br>Req. 4 |
| | vSAN_011 | vSAN use of public key infrastructure can be controlled by vCenter's RBAC Capability. Granular control can be provided or removed through the use of specific role-based permissions. | |
| | | | |
| vSphere Replication | VSPHEREREPLICATION_001 | Replication of virtual machine object and its data can be used to support continuity planning and can provide a virtualization technology alternative to offsite vSphere environment storage using electronic media. | Req. 12 |
| | VSPHEREREPLICATION_002 | vSphere Replication supports geographical separation through use of vSphere Replication Interceptors to provide timely and effective recovery operations. | Req. 12<br>Req. 9 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | VSPHEREREPLICATION_003 | vSphere Replication integrates with Site Replication Manager to enable mitigation during an outage, or disruption. | Req. 12<br>Req. 9 |
| | VSPHEREREPLICATION_004 | Recovery policies can be set up to specified Recovery Point Objectives (RPO), which can be selected from range of 15 minutes to 24 hours. vSphere Replication (6.5) can be reduced to 5 minutes and up to 24 hours. | Req. 12<br>Req. 9 |
| | VSPHEREREPLICATION_005 | You can enable the network encryption of the replication traffic data for new and existing replications to enhance the security of data transfer. | Req. 2<br>Req. 4 |
| | VSPHEREREPLICATION_006 | vSphere has a management pack for integration with vRO and this integration helps automate the disaster recovery workflows with SRM integration in place. | Req. 12<br>Req. 9 |
| | | | |
| Workspace One Access (previously vIDM) | vIDM_001 | Access controls to objects and users are supported using Role Based Access Control (RBAC) through integration with Active Directory and federated services. This includes limiting super user accounts, requiring unique user identifiers, and authentication methods. VMware Identity Manager supports Single Sign-On (SSO) and serves as a Platform Services Controller instance for other VMware products. | Req. 7<br>Req. 8 |
| | vIDM_002 | VMware Identity Manager supports VMware Verify, a multi-factor authentication product. In addition, VMware Identity Manager can be integrated with third-party multi-factor authentication solutions. | Req. 8 |
| | vIDM_003 | Maintenance logs are generated during upgrades and patches. However, logs are not automatically archived and should be stored in a logging repository to preserve the maintenance logs. For VMware Identity Manager in the cloud, the system is set to store event data for 90 days. For VMware Identity Manager on-prem, only the most recent log is maintained, and this should be pushed to a log repository to preserve data according to each organization's policy. | Req. 10 |
| | vIDM_004 | Remote system management of VMware Identity Manager is bifurcated into Operational Access via SSH and administrator access via HTTPS. In both instances, session identifiers are invalidated upon session termination. | Req. 7 |
| | vIDM_005 | VMware Identity Manager issues session tokens (default value of 8 hours), which can be configured to force users to re-authenticate after the token expires. | Req. 8 |

| Product | Capability ID | Product Capability | PCI Requirement |
|---|---|---|---|
| | vIDM_006 | VMware Identity Manager can push logs to vRealize Log Insight, or a third-party logging system that supports syslog. For VMware Identity Manager in the cloud, the system is set to store logs for 90 days. For VMware Identity Manager on-prem, disk size may require recycling of logs. Therefore, for both cloud and on-prem instances, pushing log files to a proper log repository is recommended. | Req. 10 |
| | vIDM_007 | VMware Identity Manager supports configuration of access control setting such as: requiring new users to change password on first login, minimum password age, account lockout threshold, account lockout duration. | Req. 8 |
| | vIDM_008 | User Account reviews is supported through a standardized reporting function available to VMware Identity Manager administrators. | Req. 7<br>Req. 8 |
| | vIDM_009 | VMware Identity Manager access can be assigned to roles such as operator, administrator, and user. | Req. 7 |

# About VMware

VMware, a leading innovator in enterprise software, powers the world's digital infrastructure.

Our cloud, app modernization, networking, security, and digital workspace platforms form a flexible, consistent digital foundation on which to build, run, manage, connect, and protect applications, anywhere.

A digital foundation built on VMware enables rapid, technology-driven innovation and continuous integration of emerging technologies. Organizations can move quickly without disrupting business operations, while maximizing return on investments in people, processes, and systems.

We help businesses become digital at their core—so they can meet the needs of customers and employees, and more quickly take advantage of market opportunities.

# 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 and 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 have 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