TEVORA™

VMware® Software-Defined Data Center (SDDC)

Product Applicability Guide for NIST 800-53 Rev. 4

March 11, 2021

Table of Contents

Revision History

Date	Rev	Author	Comments	Reviewers
December 2020	1.0	Tevora	Initial Draft	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
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,VMware vSphere®, VMware vSAN™, VMware vCloud Director Extender, VMware vCloud Usage Meter
Software-Defined Networking	VMware NSX®
Management and Automation	VMware vRealize Network Insight™, VMware vRealize Automation™, VMware vRealize Orchestrator™, VMware vRealize Log Insight™, VMware vRealize Operations Manager™, VMware vCloud Director®, VMware AppDefense™, Workspace One Access™
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 NIST 800-53 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 guarantees about the accuracy, completeness, or adequacy of the information contained herein. Organizations should engage appropriatelegal, business, technical, and audit expertise within their specific organization for review of regulatory compliance requirements.

Executive Summary

Background

In this Product Applicability Guide (PAG), we will provide an evaluation of VMware products that make up and support the Software-Defined Data Center (SDDC), and how they may support NIST 800-53 Rev. 4 (NIST 800-53) controls. These products virtualize and abstract the physical technology layers such as compute, storage, and network, the essence of a 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 ComplianceSolutions team developed a framework that incorporates SDDC product capabilities aligned to NIST 800-53 controls. Using NIST 800-53 as a foundational risk framework and security control catalog, the framework maps VMware products to control requirements to weave together VMware product capabilities with compliance requirements and cybersecurity controls.

NIST 800-53 provides organizations with a tested baseline of controls. It can be used to establish and refine a comprehensive data protection and cybersecurity program. Ultimately, the risks an organization faces are mitigated by controls, and the PAG provides one perspective on how VMware products can assist organizations with managing their cyber risks and implementing a stronger IT security control program.

VMware engaged Tevora, an independent third-party IT audit firm, to conduct a review of the SDDC and VMware Cloud™ solution's alignment to NIST 800-53. This document is the culmination of Tevora's discussions with VMware product teams to perform a thorough evaluation of VMware product capabilitiesmapped to NIST 800-53 controls.

Tevora is a leading security consulting firm specializing in enterprise risk, compliance, information securitysolutions, 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 NIST 800-53 standard and highlight applicable VMware product capabilities.

VMware SDDC and NIST 800-53

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 businessand compliance requirements.

VMware approaches compliance with a view that understands the complexity in environments and addresses those areas where virtualization can be leveraged to develop a more secure environment. Thisfocused view on compliance is reflected in the VMware Compliance Solutions framework, which allows fora 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 followsto weave in security through all stages of the product lifecycle, and not as an afterthought. A compliance-capable design follows the philosophy that mapping SDDC product capabilities to NIST 800-53 security requirements can result in a solution that has been vetted as compliance capable. This overlap between products and compliance requirements establishes a new level marrying security and non-security productcapabilities 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 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 toall aspects of 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 NIST?

The National Institute of Standards and Technology (NIST) was founded in 1901 and is now part of the U.S.Department of Commerce. NIST is one of the nation's oldest physical science laboratories. Today, NIST measurements support the smallest of technologies to the largest and most complex of human-made creations—from nanoscale devices so tiny that tens of thousands can fit on the end of a single human hair, up to earthquake-resistant skyscrapers and global communication networks. NIST also assists the federal government in issuing standards to meet the provisions and requirements such as the Federal Information Security Management Act (FISMA).

Introduction

What is NIST 800-53?

NIST Special Publication (SP) 800-53 Rev. 4 has been developed by NIST to further its statutory responsibilities under the Federal Information Security Management Act (FISMA), Public Law (P.L.) 107–347. It represents the culmination of a year-long initiative to update the content of the security controls catalog and the guidance for selecting and specifying security controls for federal information systems and organizations. The project wasconducted as part of the Joint Task Force Transformation Initiative in cooperation and collaboration with the Department of Defense, the Intelligence Community, the Committee on National Security Systems, and the Department of Homeland Security. The proposed changes included in Rev. 4 are directly linked to the current state of the threat space (i.e., capabilities, intentions, and targeting activities of adversaries) and the attack datacollected and analyzed over a substantial time-period. NIST 800-53 is an extensive catalog of information security controls.

While the initial intent of NIST 800-53 was to provide guidance and criteria for federal information systems, revisions have been made over the past few years for widespread adoption across various commercial andprivate industries.

The fifth revision draft was released in August 2017 and updates preceding publications within the areas of:

- Insider Threats
- Software Application Security (including web applications)
- Social Networking, Mobile Devices, and Cloud Computing
- Cross-Domain Solutions
- Advanced Persistent Threats
- Supply Chain Security
- Industrial/Process Control Systems
- Privacy

How does NIST 800-53 work?

The NIST 800-53 standard requires organizations to comply with a robust set of criteria. The criteria are brokendown into 20 control families (listed below) and provided ratings of impact to the business or organization.
Ratings are either Low-Impact, Moderate-Impact, or High-Impact. These risk ratings identify the specific controls to be implemented within each control family.

Ratings are either Low-Impact, Moderate-Impact, or High-Impact. These risk ratings identify the specific controls to be implemented within each control family.

- Access Control (AC)
- Awareness and Training (AT)
- Audit and Accountability (AU)
- Assessment and Authorization (CA)
- Configuration Management (CM)
- Contingency Planning (CP)
- Identification and Authentication (IA)
- Individual Participation (IP)
- Incident Response (IR)
- Maintenance (MA)
- Media Protection (MP)
- Privacy Authorization (PA)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Program Management (PM)
- Personnel Security (PS)
- Risk Assessment (RA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity

To derive the specific risk rating, a “Three-Tiered Risk Management” approach allows organizations a strategic viewpoint, not a solely compliance-based viewpoint, on security program development. The tiers are used to conclude the applicable risk rating that ultimately results in identifying the specific controls within each control family that are applicable. The risk is derived based on the following tiered risk approach:

- Tier 1 – Organization
- Tier 2 – Mission/Business Processes
- Tier 3 – Information Systems

All control families may not be applicable to an organization, depending on their size and scope of business.Each control takes the “Three-Tiered Risk Management” model into account and provides supplemental guidance on what a well-defined control looks like.

These controls will aid U.S.-based entities moving forward within a shifting regulatory landscape. While the standard is lengthy, it would be advantageous for any organization to define and/or align their security programagainst it, especially those organizations evaluating overseas expansion.

Scope and Approach

The SDDC and VMware Cloud platform covers a wide number of products and architectures. The platformsand each of their component products contain features that could be mapped to some NIST 800-53 controls. Of the 20 total control families, 17 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 limitedto those requirements supported either technically or through direct API integration. Additional technologies required in addition to VMware products are not identified. People and process controls are defined as administrative controls, in support of NIST 800-53 control intents.

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 NIST 800-53. It is up to each organization to identify the applicable NIST 800-53 controls and requirements that are in scope and, in addition, to determine the risk rating of NIST 800-53 High, Moderate, and Low impacts. The PAG focuses on capabilities of the SDDC product and VMware Cloud at the control family level, as each organization will need to identify its control scope based on risk ratings and to performits own risk rating and selection of controls based on the organization's scope and the relevance to its objectives. Thus, controls may vary within control families based on risk ratings. A technical whitepaper, to be released later, will compile information gathered within this PAG and apply to each individual NIST 800- 53 control.

Appendix B outlines specific product capabilities for SDDC and VMware Cloud, and their alignment to NIST800-53 control families.

In addition to the NIST 800-53 control families, we used eleven (11) security lenses that 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.

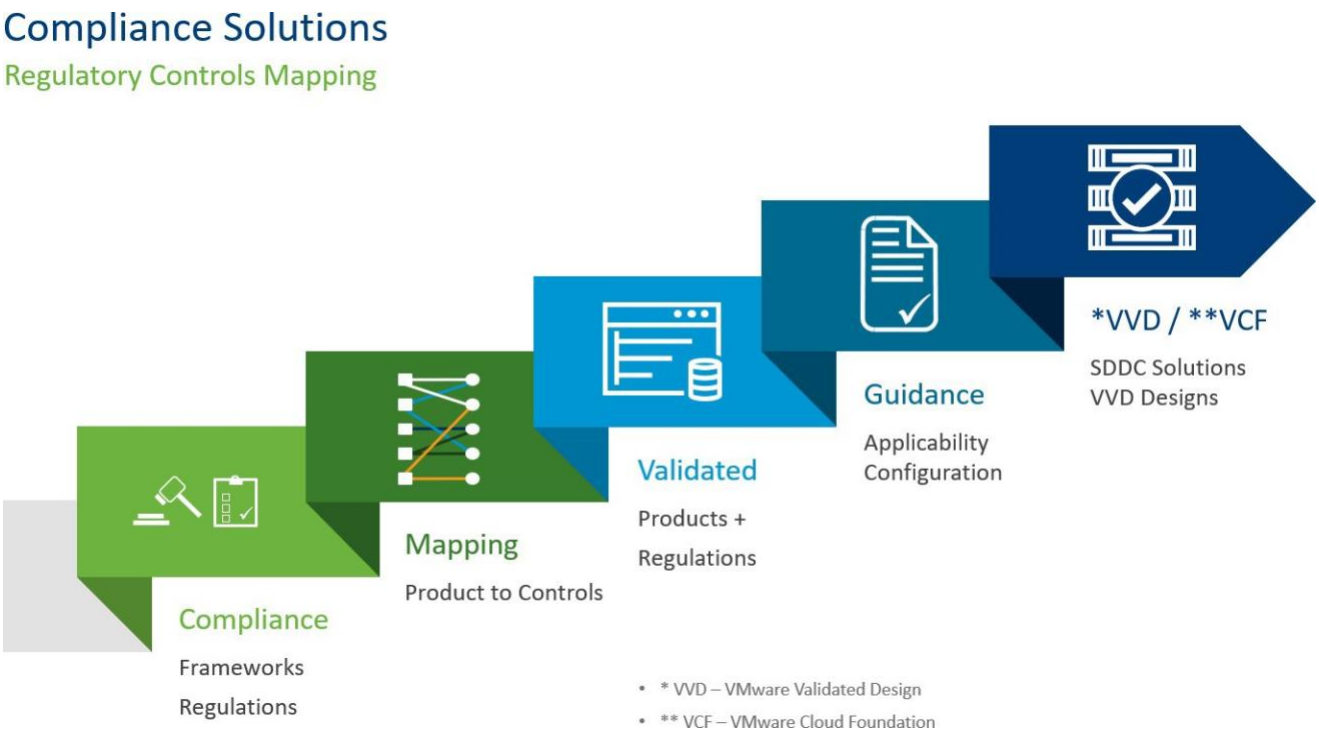

Exhibit 1: VMware Compliance Solutions Regulatory Controls Mapping

Outside of the process described above, these eleven (11) areas are broad categories of controls that areimplemented 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 (11) 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 andcompliance practitioners understand how products deliver the features required not only to support compliance with the NIST 800-53 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.

The evaluation produced this guide to provide executives, technology experts, and security and compliancepractitioners 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.

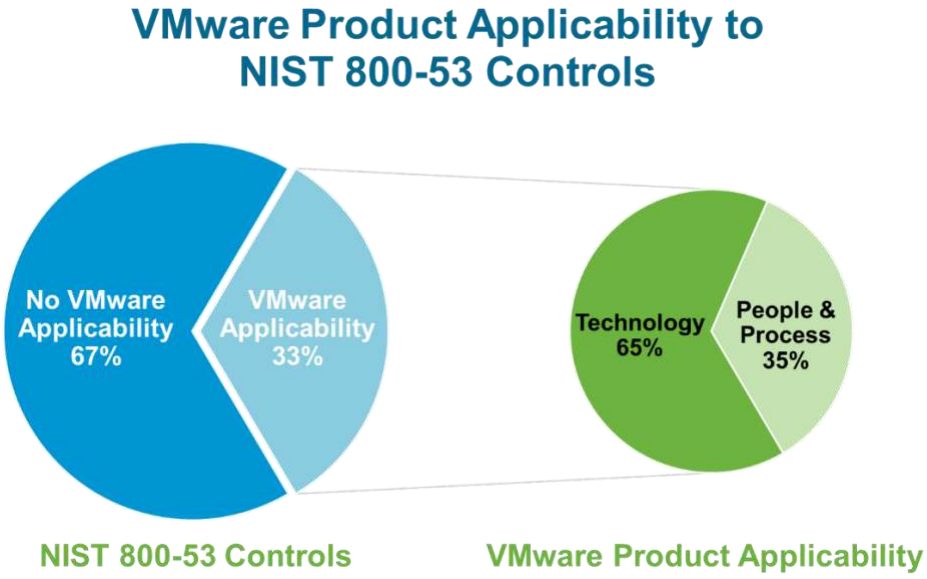

Exhibit 2: Percentage of SDDC Products that are capable of meeting the NIST 800-53 (Rev. 4) control objectives.

In-Scope VMware Product List

Software-Defined Data Center (SDDC)

VMware ESXi™ – 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 our customers.

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

Datacenter and Cloud Infrastructure

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

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

Networking and Security

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

VMware NSX® – NSX-v 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® -- NSX-T is a network virtualization program which creates, deletes, and restores software-based virtual networks. With network virtualization, the functional equivalent of a network hypervisor reproduces the complete set of Layer 2 through Layer 7 networking services (for example, switching, routing, access control, firewalling, QoS) in software.

Storage and Availability

VMware Site Recovery Manager™ – 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.

Hyperconverged Infrastructure

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

Cloud Management Platform

vRealize® Suite

VMware vRealize Operations Manager™ – 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™ – 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™ – 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™ – 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.

VMware vRealize Automation™ – vRealize Automation empowers IT to accelerate the provisioning and delivery of IT services across infrastructure, containers, applications, and custom services. Leveraging the extensible framework providedby vRealize Automation, you can streamline and automate the lifecycle management of IT resources from initial service model design through Day One provisioning and Day Two operations.

vCloud Suite

VMware vCloud Director® –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 – 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 – 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.

Digital Workspace

Workspace ONE™ -- Workspace ONE is an intelligence-driven digital workspace platform. It integrates access control, application management and multi-platform endpoint management into a single platform.

Business Continuity

VMware Site Recovery Manager™ – 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™ – vSphere Replication is an extension to VMware vCenter Server® that provides hypervisor- based virtual machine replication and recovery.

VMware vCloud Availability for vCloud Director® – vCloud Availability Cloud to Cloud DR 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 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 of 10pts per protected virtual machine per month, 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.

Overview of VMware and NIST 800-53 Best Practices and Requirement Mapping

.

Best Practice Area (Lens)	NIST 800-53	Capability Description	VMware Product Applicability
Automated Security	CP, RA	Automated Deployment, Automated Remediation	Site Recovery Manager vSphere Replication vRealize Operations vCloud Director vCloud Availability for vCloudDirector
Data Segmentation	PL, SA, SC, SI	Network & Host Firewall, Information Flow	NSX-v VMware Validated DesignvRealize Network Insight vRealize Operations vRealize Log Insight AppDefense vCloud Usage MetervCloud Director vCloud Director Extender vCloud Availability for vCloudDirector
System Hardening	CM, MP, PS, SA,SC, SI	Configuration Management, Patch Management, Vulnerability Management	vRealize Network Insight vRealize Operations vRealize Log Insight vSphere Update Manager NSX-v ESXi 6.7 AppDefense vCloud Usage MetervCloud Director vCloud Director Extender vCloud Availability for vCloudDirector
Compliance Validation	CM	Configuration Management	vRealize Network InsightvRealize Operations vRealize Log Insight NSX-v AppDefense vCloud Director

System Access	AC, AT, AU, IA, IR,PE, PL, PS, SC	Two-Factor Authentication, Identity and Access Management	vCenter NSX-v vRealize Network Insight vRealize Log Insight vRealize Operations ESXi 6.7 AppDefense vCloud Usage Meter vCloud Director vCloud Director Extender vCloud Availability for vCloud Director
System Monitoring	AT, AU, CA, CM, CP, IR, MA, PE, PL, PS,RA, SC, SI	Security Information Event Monitoring (SIEM),Database Monitoring	vRealize Log Insight vRealize Network Insight vRealize Operations Site Recovery Manager vSphere Replication vCenter vSphere Update Manager AppDefense vCloud Usage Meter vCloud Director vCloud Director Extender vCloud Availability for vCloud Director
Data Encryption &Protection	CA, IA, MA, SA, SC,SI, PA	Data at Rest Encryption, Data in Motion Encryption,System Backup & Restore	vSphere 6.7 VM Encryption feature vSAN 6.7 vSAN Encryption feature VMware vSphere vMotion® encryption NSX-v vRealize Operations vRealize Network Insight vRealize Log Insight vSphere VMware Validated Design vSphere Update Manager AppDefense vCloud Usage Meter vCloud Director vCloud Director Extender vCloud Availability for vCloud Director

Network Protection	AT, CA, CP, IR, PE,RA, SC	Intrusion Prevention System, Web Application Firewall	Site Recovery Manager vSphere Replication NSX-v vRealize Operations vRealize Network Insight vRealize Log Insight AppDefense vCloud Director vCloud Director Extender vCloud Availabilty for vCloud Director
Endpoint Protection	AC, CM	Endpoint A/V and Malware Prevention, File Integrity Monitoring, Data Leakage Protection, Mobile Device Management	NSX-v ESXi 6.7 vRealize Operations vRealize Network Insight vRealize Log Insight AppDefense vCloud Director vCloud Director Extender vCloud Availability for vCloud Director
Trusted Execution/Secure Boot	SC, SI	Execution Integrity	ESXi 6.7 NSX-v vRealize Log Insight vRealize Operations vRealize Network Insight vSphere Update Manager AppDefense vCloud Director vCloud Director Extender vCloud Availability for vCloud Director
Software Development Lifecycle (SDLC)	PL, SA	Configuration Integrity	VMware Validated Design

Exhibit 3 represents a high-level view of how VMware technology capabilities match up to best practices areas as well as NIST 800-53 requirement topics.

VMware Control Capabilities Detail

VMware Validated Design and Software Development Process

VMware has developed the VMware Validated Design (VVD) to allow organizations to implement the full SDDC platform using a design that is validated 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 VMwareCloud products (Exhibit 3). This principled approach to designing security, overseen by VMware Product Security from the start, is important to NIST 800-53 compliance, as the products utilized are required to have security interwoven through their underlying substructures, to be 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 using the NIST 800-53 risk-and-control framework. As further reference to 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 maturesecurity program addressing common areas of vulnerabilities.

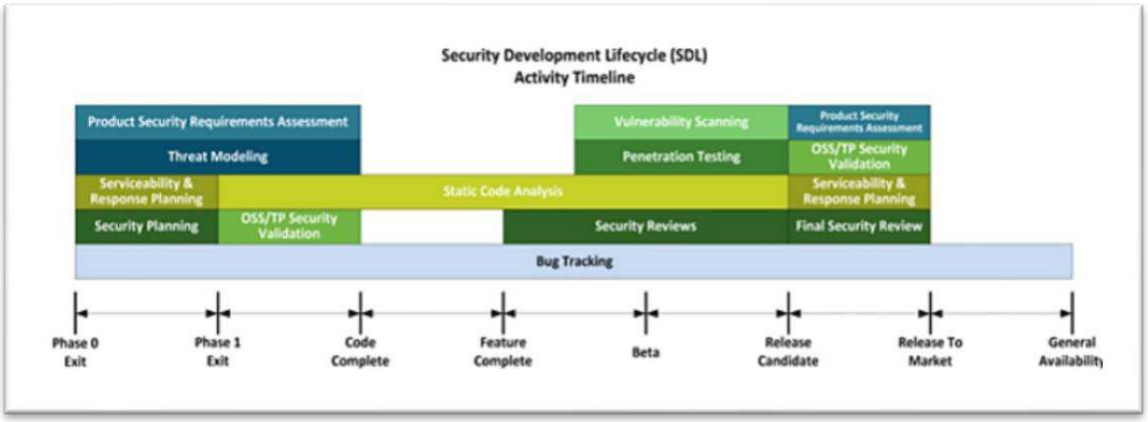

Exhibit 4: VMware SDLC Activity Timeline

Core and Administrative Control Categories

The NIST 800-53 authority document historically established “Security Control Class Designation” in the form of Management, Operational, and Technical references. These have been removed in the NIST 800-53 authority document. To streamline the delivery of this PAG and the intent of each control family, those categories were tailored into Core and Administrative. Core control families are those that address the mainstructure of a NIST 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 NIST Control Families

Many NIST control families establish policies and procedures requirements in the form of documentation, which may cite VMware products or rely on VMware technology capabilities. Other NIST controls may identify people or process requirements that are not specific to VMware products, but these too may rely on 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 will be able to deploy VMware products, apply the NIST 800-53 controls, and monitor them through the compliance- capable platform. In this way, implementing policy or operating procedures assists in maintaining a secureand compliant information architecture.

Another key aspect of NIST 800-53 includes supplemental or complementary controls. As a framework,NIST 800-53 provides organizations with an opportunity to enhance controls using additional, complementary controls beyond the baseline of controls associated with each risk rating.

An example of an administrative control family is Incident Response Planning (IR). This control family mayrequire a documented incident response plan or a detailed runbook on audit procedures. Using VMware products such as NSX, vRealize Network Insight, or vRealize Log Insight to strengthen and accelerate discoveries and corrective actions during incident responses is possible because these products providemonitoring, troubleshooting, and remediation capabilities. However, this control family is more focused on the people and process. Thus, this guide will treat the control family as an administrative support control family instead of a core control family because VMware product capabilities support the administration of the control family rather than a core technology control.

The following Control Families fall within Administrative:

- Awareness and Training (AT)
- Contingency Planning (CP)
- Media Protection (MP)
- Physical and Environmental Protection (PE)
- Planning (PL)
- Personnel Security (PS)
- Incident Response (IR)
- Maintenance (MA)
- Risk Assessment (RA)

VMware Core Support for NIST Control Families

For those NIST control families where a technology will partially or fully satisfy a control requirement, VMware capabilities are identified as core to the NIST control family. These are the areas within NIST 800-53 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 NIST control family and their respective High-Impact controls. Each area defines the intention of the NIST family, 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.

VMware Core Support for NIST Control Families

For those NIST control families where a technology will partially or fully satisfy a control requirement, VMware capabilities are identified as core to the NIST control family. These are the areas within NIST 800-53 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 NIST control family and their respective High-Impact controls. Each area defines the intention of the NIST family, 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 virtualizationtechnology 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.

The following Control Families fall within Core:

- Access Control (AC)
- Audit and Accountability (AU)
- Assessment, Authorization, and Monitoring(CA)
- Configuration Management (CM)
- Identification and Authentication (IA)
- System and Services Acquisition (SA)
- System and Communications Protection (SC)
- System and Information Integrity (SI)

VMware Core Controls

Access Control (AC)

NIST Controls AC1–AC25

The Access Control family focuses on the ability of any user, at all permission levels, to reach key elements of the environment. It looks at coverage across subjects such as remote access, the protection of access and authentication, as well as the integrity of the entire authentication process.

Applicable Security Lens:

- System Access
- Endpoint Protection

Applicable VMware Product(s):

- VMware NSX for vSphere
- vSphere
- vRealize Automation
- vRealize Log Insight
- vRealize Network Insight
- vRealize Orchestrator
- vRealize Operations
- Site Recovery Manager
- (SRM)
- vSAN 6.7
- ESXi 6.7
- AppDefense
- vCloud Usage Meter
- vCloud Director Extender
- vCloud Director
- vCloud Availability for vCloud Director
- VMware NSX-T
- NSX-V

VMware Product Capabilities

For all products within the SDDC platform, Access Control can be implemented at a granular level. Thisis 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.

As an elevated protection, VMware has built third-party integration capabilities to allow organizationsto 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. The 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 ensure that only trusted IPs, subnets, or IP devices are allowed into the environment, vCenter andNSX provide access restriction to an organization's East–West traffic, or Virtual Machine (VM) to Virtual Machine communications.

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 VMware vSphereWeb Client.

Monitoring can be 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.

AppDefense allows for access rights to be established within vSphere, to restrict access to the AppDefense Manager and to provide the capability to log user activity for anyone with root access tothe monitored applications.

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, configure 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.

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

Audit and Accountability (AU)

NIST Controls AU1–AU16

The Audit and Accountability NIST control family discusses the implementation, governance, and operation of an audit program. As a function of the program, it calls for organizations to ensure theprotection of any logs and additional information associated with audit procedures.

Applicable Security Lens:

- Systems Monitoring
- System Access

Applicable VMware Product(s):

- vCenter
- vRealize Log Insight
- Site Recovery Manager(SRM)
- ESXi 6.7
- vRealize Operations
- vRealize Network Insight
- vSphere Replication
- vRealize Operations
- vRealize Automation
- NSX for vSphere
- vSAN
- AppDefense
- vCloud Usage Meter
- vCloud Director
- vCloud Director Extender
- vCloud Availability for vCloud Director
- NSX-T
- NSX-V

VMware Product Capabilities

The Audit and Accountability control family speaks to the need for a security program to conduct ongoing audits to maintain integrity and compliance. Implementing the SDDC through the VVD (VMware Validated Design) provides a reference architecture to identify security requirements throughout the virtual platform, from Hypervisor through to the User Interface that collects audit logdata.

Across all products, rich logging features exist to allow administrators to ascertain who logged in, theorigin, at what time (coordinated through NTP), and whether the attempt was a success or failure.
Logs can be pointed to third-party management tools through API integration if desired.
AppDefense can deliver alerts for all changes made within the environment. This can be configured through the provided “Scopes” feature, or through the vSphere Web Client.

Any logs generated by AppDefense canbe calibrated using both vSphere, and the AppDefense Manager, and access can be restricted to only an administrator. Additionally, vSphere supports capacity planning within configured environments and any location where AppDefense is installed.

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 tomost of the vCloud Director. vCloud Director is also integrated into the vSphere environment, with theability to be united with vCloud Availability for vCloud Director to guarantee functionality.

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 anyincidents 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 consistentbasis.

vCenter can be configured for specific-day retention. Tamper proofing can also be configured if leveraging vRealize Log Insight. vRealize Log Insight retains data based on defined storage capacity.vRealize Operations assists by monitoring the datastore's health and capacity, prompting the Administrator to determine how to proceed with further log archival if need be.

vRealize Network Insight contains the ability to adjust forensic data retention. Database storage can be adjusted to a specified limit up to 13 months. ESXi 6.7 affords administrators the ability to adjustthe richness and frequency of audit logs.

For advancing an organizational audit process, it is recommended that a Security Incident Event Management (SIEM) platform be coordinated through vRealize Log Insight to ingest logs. This can all be set through the REST API and will enable organizations to garner meaningful evidence to take real-time action.

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

Assessment, Authorization, and Monitoring (CA)

NIST Controls CA1–CA9

This control family establishes criteria and controls to ensure that only authorized connections are enabled throughout an organization's environment.

Applicable Security Lens:

- System Monitoring
- Data Encryption & Protection
- Network Protection

Applicable VMware Product(s):

- vRealize Network Insight
- vRealize Operations
- vRealize Log Insight
- vSAN 6.7
- ESXi 6.7
- NSX for vSphere
- vSphere Replication
- vCenter
- vCloud Director
- NSX-T
- NSX-V

VMware Product Capabilities

At its core, the Security Assessment and Authorization control family aims to certify that all systems support security in depth. The interconnections of systems, appropriate authorizations and the processes that support them are key. The applicable VMware products create an ease of configuration natively to support this intent.

NSX for vSphere 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 ensure security in depth. vSphere can be extended with vCloud Director, which includes monitoring functionality allowing audit logs to be produced that include environment analytics.

vRealize Operations and vRealize Log Insight, along with the other products that compose the SDDC suiteand VMware Cloud, can support the implementation of continuous monitoring when properly used. vRealize Operations gives administrators the ability to craft custom security tags that align with NIST 800-53 and other security frameworks to maintain up-to-the-minute assessment and authorization across the environment.

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

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

Configuration Management (CM)

NIST Controls CM1–CM12

This control family establishes management of information systems and software configurations within the environment and how those configurations and baselines are secured. Attention is given to identifying baseline configurations and how any changes to the configurations are managed with the security program.

Applicable Security Lens:

- System Hardening
- Compliance Validation
- System Monitoring
- Endpoint Protection

Applicable VMware Product(s):

- NSX for vSphere
- VMware NSX-T®
- vRealize Orchestration
- vRealize Operations
- vCenter
- ESXi 6.7
- vSphere Replication
- vSphere Update Manager
- vSphere 6.7 VM Encryption feature
- AppDefense
- vCloud Director
- NSX-T
- NSX-V

VMware Product Capabilities

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 for vSphere or NSX-T. 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 utilize REST API to deliver at scale and in real time. This is an advised strategy on environments deploying VMware vRealize Configuration Manager™. Endpoints should be configured to collect data and point information into vRealize Configuration Manager.

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 virtual machined within an organization via distributed firewall rules, along withedge gateway firewall capabilities.

Knowing that the protection of or adherence to standards is difficult without knowing what resides in thenetwork, vSphere and vRealize Automation have 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.

Identification and Authentication (IA)

NIST Controls IA1–IA12

This control family establishes how an organization should address and protect authentication. The familydelves into re-authentication requirements and cryptographic-enabled security. Overall, the intent of the family is to ensure that appropriate measures are employed for the operations and management of Identification and Authentication within an environment.

Applicable Security Lens:

- Data Encryption & Protection
- System Access

Applicable VMware Product(s):

- NSX for vSphere
- NSX-T
- vRealize Log Insight
- vRealize Network Insight
- vRealize Operations
- vSphere
- ESXi 6.7
- Site Recovery Manager(SRM)
- vSAN 6.7
- vCenter
- AppDefense
- vCloud Usage Meter
- vCloud Director
- vCloud Director Extender
- vCloud Availability for vCloud Director
- NSX-T
- NSX-V

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. To guarantee that no sessions remain unlocked, time-outs and re-authentication can be set across all SDDC products by following the standard VVD requirement. Both the vSphere 6.7 VM Encryption feature and the vSAN Encryption feature in vSAN 6.7 certify that all data stored within a customer's SDDC environment is encrypted to industry standards.

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 intents. Products can again harness Active Directory integration to maintain vigilance over authentications toproducts. 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.These instances are then logged within vSphere.

Natively, organizations can harness micro-segmentation to reduce the risk profile of their environment. For this control family, micro-segmentation is particularly important and can be implemented using NSX. Virtual machines (VMs) can be configured to only speak to other VMs in specified situations, based uponsecurity policies.

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 SDLCare 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.

Administrators viewing all passwords through the Graphic User Interface (GUI) will have passwords for allcredentials obscured or masked with asterisks.

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 CA that 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.

System and Services Acquisition (SA)

NIST Controls SA1–SA19

System and Services Acquisition spans the underlying makeup of an organization's SDLC and theapplication 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
- Software Development Lifecycle (SDLC)

Applicable VMware Product(s):

- vSAN 6.7
- ESXi 6.7
- NSX-T

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 System and ServicesAcquisition (SA) NIST control family fulfills requirements including process isolation at both personnel level and code level, encryption protocols in transmission, and permission granularity.

Particularly important for this control family is that the ability to meet security requirements can be metduring 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.

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.

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

System and Communications Protection (SC)

NIST Controls SC1–SC41

The System and Communications control family addresses the need for protecting information throughout its lifecycle within the environment. It assesses how traffic travels from outside to inside anorganization's network and the layers in between.

Applicable Security Lens:

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

Applicable VMware Product(s):

- NSX for vSphere
- NSX-T
- vRealize Automation
- vRealize Network Insight
- vRealize Orchestrator
- vRealize Operations
- vRealize Log Insight
- vCenter
- Site Recovery Manager (SRM)
- ESXi 6.7
- vSphere Replication
- vSAN 6.7
- vCloud Usage Meter
- vCloud Director
- vCloud Availability for vCloud Director
- vCloud Director Extender
- NSX-T
- AppDefense
- NSX-V

VMware Product Capabilities

One main objective within this control set is minimizing the development of covert channels. VMware conducts peer reviews during each development cycle to plug all potential back doors. VVD requirementsforce security requirements to maintain 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.

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 to defined protocols, i.e., SSH and RDP.

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

VMware NSX Edge™ gateways give boundary protection and network isolation to user environments. Through its Dynamic Host Configuration Protocol (DHCP) service, 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 utilizing multi-tenant cloudenvironments.

For enhanced visibility, organizations can leverage 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 sync with RBAC to restrict access based on specified group names. The information contained within these data flows are then secured atrest with the vSAN Encryption feature in vSAN 6.7 and with the vSphere 6.5 VM Encryption feature. ESXi 6.5 further segments processes within resource pools. vCloud Director supports native integration into NSX Distributed Firewall to provide application isolation. vCloud Usage Meter provides further protectionby 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 takes effect throughout the development process and isdeveloped into products. 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.

System and Information Integrity (SI)

NIST Controls SI1–SI1

Maintaining integrity within the system and information it provides is paramount. This control family requires that organizations implement protections concentrated on three key areas: System Monitoring; Software, Firmware, and Information Integrity; and Flaw Remediation.

Applicable Security Lens:

- Data Segmentation
- System Monitoring
- System Hardening
- Data Encryption
- Trusted Execution/Secure Boot

Applicable VMware Product(s):

- ESXi 6.7
- vSphere Replication
- vSAN 6.7
- vRealize Log Insight
- NSX for vSphere
- vRealize Automation
- vRealize Network Insight
- vRealize Operations
- vSphere Update Manager
- vCenter
- AppDefense
- NSX-T
- NSX-V

VMware Product Capabilities

Through the lens of the VVD “secure by default” directive and the guidance of the security criteria held within the SDLC, VMware SDDC and VMware Cloud platform components consistently prioritize systemintegrity and the information it holds.

To highlight, ESXi 6.7 maintains a secure boot protocol utilizing vSphere Installation Bundles (VIBs). Harnessing the Unified Extensible Firmware Interface (UEFI), the hypervisor refrains from loading unless the signature database (containing the whitelisted and blacklisted signatures) validates. vCenter supports alerts to prevent unauthorized execution within the environment, and AppDefense can detect unauthorizedcode execution, send alerts, and address anomalies directly.

If signatures are not validated, the hypervisor fails to activate. ESXi 6.7 does not report system intelligenceback on the failure to the session’s origin. This is crucial as it protects the integrity of an organization’s virtual servers from adversaries targeting intelligence to exploit. NSX natively includes defined guest introspection framework that allows administrators to conduct analysis on the data plane level from North–South traffic flows.

Adding strength to the secure boot protocol are vRealize Log Insight and vRealize Network Insight features that can be configured to notify the security team in the event 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.

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, as well as 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.

Finally, all VMs can be configured for destruction upon end of life, defined by the administrator.

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

VMware Administrative Controls

Awareness and Training (AT)

NIST Controls AT1–AT5

This control family is managed through Administrative action on the client side and is not applicable toVMware natively.

Applicable Security Lens:

- System Monitoring
- System Access
- Network Protection

Applicable VMware Product(s):

- vRealize Log Insight
- vRealize Network Insight
- vRealize Operations
- ESXi
- vSphere Replication
- vCenter
- vCloud Director Extender
- NSX-T
- AppDefense
- vCloud Director

Individual Participation (IP)

NIST Controls IP1–IP6

Individual Participation in accordance with NIST 800-53 Rev 5 will be governed by Administrative policy. Individual participation focuses on the development and assignment of policies and procedures to protect privacy. It looks at coverage around consent to processing personally identifiable information prior to its collection, redress information that has been reported inaccurately, and the inclusion of privacy notice on organizational forms. This control family is managed through Administrative action on the client side and is not applicable to VMware natively.

Applicable Security Lens:

- System Monitoring
- System Access
- Network Protection

Contingency Planning (CP)

NIST Controls CP1–CP13

Contingency Planning in accordance with NIST 800-53 will be governed by Administrative policy. VMwareproducts such as Site Recovery Manager and vSphere can support the need for data backups or site replication as detailed within the organization's policy when properly used. Site Recovery Manager can also house contingency plans and drive any automated corrective actions needed to sustain required operating levels working in coordination with other products (vSphere Replication) as configured.

Further, for components of the control family relating to Predictable Failure and System Recovery & Reconstitution, vRealize Operations has been designed to support high availability. This means that if one virtual machine fails, vRealize Operations can be configured, at the organization's discretion, to automatically fail over to an alternative VM (or deploy a new one) to ensure uptime as required by SLAs orother operating needs. Replication can additionally allow for a new VM to be constructed automatically upon trigger. vSphere Replication is a replication tool completely autonomous from the underlying storage. It acts as the transport mechanism for the VM to the failover site.

Applicable Security Lens:

- System Monitoring
- Network Protection
- Automated Security

Applicable VMware Product(s):

- Site Recovery Manager (SRM)
- vRealize Operations
- vSphere Replication
- vCenter
- vCloud Director
- vCloud Availability for vCloud Director
- NSX-T

Incident Response (IR)

NIST Controls IR1-IR10

The Incident Response control family is driven by the creation of organizational policies that addresshow 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.

AppDefense provides continuous detection at the hypervisor level of vSphere, allowing it to block, suspend, or shutdown 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 ofapplications to determine when malicious activity is present.

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):

- ESXi 6.7
- vSphere Replication
- vCenter
- AppDefense
- vCloud Director
- NSX-T

Maintenance (MA)

NIST Controls MA1–MA6

Most controls listed underneath this control family are performed in accordance with organizationalpolicy. vSphere Update Manager and vRealize Operations allow for maintaining up-to-date patching. When configured accordingly, products such as vCenter assist in the updates and patching for complementary VMware products, e.g., ESXi 6.7.

Moreover, all products are pre-inspected prior to ingestion/deployment and are hashed to elevate security protocols at the deepest levels of the virtual stack.

Lastly, proof of maintenance within NIST is required to ensure that all procedures are being followedas stated in governing policies. All products can generate logs that highlight when maintenance didoccur on the component.

Applicable Security Lens:

- System Monitoring
- Data Encryption & Protection

Applicable VMware Product(s):

- NSX for vSphere
- vRealize Automation
- vRealize Log Insight
- vRealize Network Insight
- vRealize Operations
- vSphere Update Manager
- ESXi 6.7
- vSphere Replication
- Site Recovery Manager (SRM)
- vCenter
- vCloud Usage Meter
- NSX-V

Media Protection (MP)

NIST Controls MP1–MP8

VMware products can support the controls of this family through organizationally developed policy when properly used. Products within the SDDC do not natively provide features that directly apply tothe family's intent. Natively, the vSAN Encryption feature provides two media functions within its datastore for cache and capacity to protect media if this feature is activated.

Applicable Security Lens:

- System Hardening

Applicable VMware Product(s):

- ESXi 6.7
- vSAN Encryption feature of vSAN 6.7

Physical and Environmental Protection (PE)

NIST Controls PE1–PE22

VMware products can support the controls of this family through organizationally developed policy when properly used. All SDDC platform components provide backup and recovery capabilities, whichwill aid the employment of the policy for requirements such as data protection, recovery time objectives (RTO), and recovery point objectives (RPO).

Applicable Security Lens:

- System Access
- System Monitoring
- Network Protection

Applicable VMware Product(s):

- ESXi 6.7
- vSphere Replication
- vCenter
- NSX-T

Privacy Authorization (PA)

NIST Controls PA1–PA4

Privacy authorization determines the legal authority that permits the collection, use, maintenance, and sharing of personally identification information. This control is managed through Administrative actionon the client side and is not applicable to VMware natively.

Applicable Security Lens:

- System Monitoring
- System Access
- Network Protection

Planning (PL)

NIST Controls PL1–PL11

VMware products can support the controls of this family through organizationally developed policy when properly used. Across all products, VMware employs secure information-sharing processes, natively available throughout the Cloud suite. These processes are critical elements of the VVD andinclude the need for strict design testing requirements.

Applicable Security Lens:

- Data Segmentation
- System Access
- System Monitoring
- Software Development Lifecycle (SDLC)

Applicable VMware Product(s):

- ESXi 6.7
- vSphere Replication
- vCenter
- NSX-T

Personnel Security (PS)

NIST Controls PS1–PS8

VMware products can support the controls of this family through organizationally developed policy when properly used. Products within the SDDC natively provide features that support the family's intent. These features include general user review reports and log intelligence capabilities.

Applicable Security Lens:

- System Access
- System Hardening
- System Monitoring

Applicable VMware Product(s):

- vRealize Network Insight
- vSAN 6.7
- Site Recovery Manager (SRM)
- ESXi 6.7
- vSphere Replication
- vCenter
- vCloud Director
- NSX-T
- vRealize Log Insight

Risk Assessment (RA)

NIST Controls RA1–RA9

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 aidthe employment of a policy's requirements such as data protection and being able to meet recovery time objectives (RTO) and recovery point objectives (RPO). Site Recovery Manager and vSphere Replication can support the assurance of meeting RTO and RPO criteria. vRealize Network Insight assists risk assessmentsthrough visibility into network traffic throughout the environment.

Applicable Security Lens:

- System Monitoring
- Network Protection
- Automated Security

Applicable VMware Product(s):

- vRealize Network Insight
- Site Recovery Manager
- vSphere Replication
- vCenter
- AppDefense
- vCloud Director

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 has focused on developingmethodologies that set this tone.

Through the eleven (11) security lenses and in accompaniment of the VMware Validated Design, the SDDCplatform components and VMware Cloud provide users with a virtualization stack that adheres to the comprehensive requirements of NIST 800-53.

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.

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 theirarchitecture and NIST 800-53 security program.

Bibliography

1. Himanshu Singh. April 17, 2018. Accessed November 18, 2019. https://blogs.vmware.com/vsphere/2018/04/introducing-vmware-vsphere-6-7.html
2. "NIST Special Publication (SP) 800-53 Revision 5 Draft." National Institute of Standards and Technology. August 2017. Accessed November 10, 2019. https://csrc.nist.gov/publications/detail/sp/800-53/rev-5/draft
3. "VMware Product Security: An Overview of VMware's Security Programs and Practices."VMware. Accessed December 1, 2019. https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/whitepaper/vmware - product-security-white-paper.pdf

Appendix A: NIST 800-53 Control Mapping

VMware Product	NIST 800-53 Control Families Supported
VMware NSX-V	AC, SC, SI, CM, MA, IA, AU, CA
VMware vRealize Log Insight	AU, MA, IA, AC, AT, SC, SI
VMware vRealize Network Insight	AU, MA, SC, IA, SI, RA, CA, AC, PS, AT
VMware vRealize Orchestration	SC, CM, AC, MA
VMware vRealize Operations	MA, SC, AC, IA, CA, CM, CP, AT, AU
VMware vSAN	AC, AU, SC, PS, IA, SI
VMware vCenter VMware ESXi VMware vSphere Replication VMware vSphere Update Manager VMware vSphere VM Encryption feature	AC, AU, CM, SC, SI, CP, MA, MP
VMware Site Recovery Manager	CP, AU, SC, MA, AC, IA, PS
Common across all Products/Administrative	AT, CA, CP, IR, MA, MP, PE, PL, PS, RA
VMware AppDefense	AC, AT, AU, CM, IA, IR, SI, RA
VMware vCloud Usage Meter	AC, AU, IA, MA, SC
VMware Cloud Platform	AC, AT, AU, CM, CP, CS, IR, IA, PS, RA, SC
VMware NSX-T	AC, IA, SC, CP, CM, AU, CA, SI, IR, PL, PE

Appendix B: SDDC Product Capability Relationship with NIST 800-53

Product	Capability ID	Product Capability	NIST Control Family
ESXi	ESXi_001	Login attempts can be logged.	AC – Access Control
	ESXi_002	Concurrent sessions can be limited on web clients virtual machine consoles.	AC – Access Control
	ESXi_003	ESXi can be integrated with Active Directory, or LDAP to employ unique user identifiers, instead of using the root account.	IA – Identification and Authorization
	ESXi_004	A proof of maintenance log is available to report on archived maintenance activity.	AU -- Audit and Accountability MA – Maintenance
	ESXi_005	Remote access to ESXi via SSH, or vSphere Web Client or API over HTTPS, can be configured as these cure communication protocol. Session identifiers are invalidated after session termination.	AC – Access Control SC- System and Communications Protection
	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 will be managed via the external authentication solution (minimum password, account lockout, and account lockout threshold, etc.).	IA – Identification and Authorization AC – Access Control
	ESXi_007	ESXi will perform the encryption on virtual machines that have been configured by vCenter to support VM Encryption. A third-party key manager solution is required to manage encryption keys. ESXi supports virtual machine encryption but requires a third-party integration.	SC – System and Communications Protection MP – Media Protection AU – Audit and Accountability

	ESXi_008	ESXi can push logs to be stored in an external log repository that supports syslog, including vRealize Log Insight. In the event vRealize Log Insight is used, it can then apply tamper protection of logging that can be used during after-the-fact investigations without altering the event logs.	AU – Audit and Accountability AC – Access Control
	ESXi_009	ESXi supports the Secure Boot feature to monitorfirmware to validate version control and authorization. If the violation is detected during boot, the system will not boot up. If the violation is detected during run-time, the command will be rejected and not boot.	CM – Configuration Management SI – System and Information Integrity
	ESXi_010	ESXi has inherent capabilities to log events and specify frequency. The richness of logging can be adjusted, and the log retention based on disk space can be enhanced, through use of a separate logging repository via syslog or vRealize Log Insight.	AC – Access Control AU – Audit and Accountability
	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.	AU – Audit and Accountability IR – Incident Response SI – System and Information Integrity
	ESXi_012	ESXi can be configured to display a login bannerbefore granting access to the system.	AC – Access Control
	ESXi_013	ESXi provides memory safeguards to protect it from executing unauthorized code.	SI – System and Information Integrity
	ESXi_014	ESXi limits the use of resources through Resource Pools, which can be constrained or prioritized based on Priority.	VMware Best Practice

	ESXi_015	ESXi has the capabilities to establish firewalls using VLAN, to deny traffic by default, and to allow only explicitly designated traffic.	SC – System and Communications Protection CA – Security Assessment and Authorization
	ESXi_016	ESXi patching is performed via vCenter using vSphere Update Manager.	CM – Configuration Management SA – System and Services Acquisition SI – System and Information Integrity
	ESXi_017	The vSphere 6.75 Security Configuration Guide provides support for ESXi and vCenter hardeningprocedures.	CM – Configuration Management
	ESXi_18	Logon authentication technique includes Two Factor Authentication	AC – Access control IA – Identification and Authorization
	ESXi_19	ESXi supports configuration of access control via Single Sign-On, or Active Directory services, such as requiring new users to change password on first logon, minimum password age, account lockout threshold or account lockout duration. Logon authentication techniques includes Two Factor Authentication.	AC – Access control IA – Identification and Authorization
	ESXi_20	ESXi can use Secure Boot integrated with AirWatch for asset management and UEM for Windows to detect and isolate rogue devices.	CM – Configuration Management

AppDefense	AD_001	AppDefense monitors all application endpoints within an environment utilizing its Intended State Engine (ISE), which is located in the virtualization layer. Since AppDefense is installed in the vSphere hypervisor, which is a tamper evident environment, ensuring secure communication throughout the environment. AppDefense actively monitors endpoints within the environment for any changes to their intended state. It correlates the changes with a snapshot of the endpoint to discern If the changes are permitted.	AC – Access Control
	AD_002	Access rights corresponding to AppDefense canbe established through vSphere, which has the ability to prevent users from accessing AppDefense Manager.	AC – Access Control
	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.	AC – Access Control
	AD_004	Logs and records generated through AppDefense are reliant upon functionality provided by vSphere. Event capturing can be completely fine-tuned utilizing both the vSphere Web Client and the AppDefense Manager.	AU – Audit and Accountability
	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.	AU – Audit and Accountability
	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.	AU – Audit and Accountability

	AD_007	AppDefense compiles event logs through its "Alarms" tab and can be reviewed at any time.	AU – Audit and Accountability
	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.	AU – Audit and Accountability
	AD_009	Access to AppDefense logs can be configured to only be accessible via an admin account and can be further secured by utilizing configuration setting through vSphere.	AU – Audit and Accountability CM – Configuration Management
	AD_010	AppDefense is integrated within the vSphere environment, which includes a full view 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 it's "Learning Mode". When malicious activity is suspected within the environment AppDefense can suspend, or completely shut down, any application and device.	CM –Configuration Management
	AD_011	Changing user identifiers is possible within the vSphere Web Client, of which AppDefense heavilyrelies on. AppDefense can block untrusted network protocols, resulting in a secure environment.	IA –Identificationand Authorization
	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 utilizes a "Learning Mode" to identify the desired functionality of applications within the environment.	IR – IncidentResponse RA – Risk Assessment
	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.	SC – System and Communications Protection

	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 utilized to restore functionality to compromised applications.	SC – System and Communications Protection
	AD_015	AppDefense lies within the hypervisor of vSphere, affording it the ability to isolate various elements of applications.	SC – System and Communications Protection
	AD_016	Unauthorized code execution can be mitigated via AppDefense's detection capabilities. If anomalies are detected within the environment, such as unauthorized code execution, AppDefense will alert and respond.	SI – System and Information Integrity
	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.	SI – System and Information Integrity
	AD_018	AppDefense detects any changes within the network. Any changes, such as configuration changes and suspicious anomalies, will triggeralerts that can be viewed win the AppDefense Manager.	SI – System and Information Integrity IR – Incident Response
	AD_019	AppDefense can be fully automated and can issue automated responses when various anomalies are detected, such as leveraging virtualization processes like suspending and shutting down the environment.	SI – System and Information Integrity
	AD_020	AppDefense can be fully automated and can issue automated responses when various anomalies are detected, such as leveraging virtualization processes like suspending and shutting down the environment.	SI – System and Information Integrity

NSX for vSphere	NSX_V_001	Information protection can be implemented using policies that restrict access information flow based on network micro-segmentation.	AC – Access Control SC – System and Communications Protection
	NSX_V_002	Within the data plane, the guest introspection framework (host based) or Network Extensibility (redirect network flow to 3rd party appliances/tools) is supported by NSX, which can be accessed by 3rd party tools to support Intrusion Detection System (IDS) and/or Intrusion Prevention System (IPS) systems.	SI – System and Information Integrity
	NSX_V_003	NSX identify firewall supports Role Based Access Controls (RBAC) to limit permissions that restrict viewing virtual machines (VM). 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.	SC – System and Communications Protection
	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 vRLI.	AU – Audit and Accountability MA – Maintenance PE – Physical and Environment Protection
	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, Edge, or Controller. By default, SSH access is disabled. This includes controlling remote access through an existing access control and authentication solution, and invalid rating session identifiers upon session termination.	AC – Access Control SC – System and Communications Protection
	NSX_V_006	Session lockouts are enforceable and require users to re-authenticate after a session time-out.	AC – Access Control

	NSX_V_007	Account lockout threshold can be altered.	AC – Access Control
	NSX_V_008	NSX can push logs to be stored in Syslog audit repositories, including vRLI. 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.	AU – Audit and Accountability
	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 NSX's Application Rule Manager can monitor enforcement of Security Rules and Firewall policies. NSX's Endpoint Monitoring enables Guest Introspection Framework capabilities to monitor endpoint processes specifically on Windows Virtual Machines.	SI – System and Information Integrity AC – Access Control AU- Audit and Accountability
	NSX_V_010	NSX provides monitoring of the system using event logs and other security logs to identify abnormal activity. NSX's Net X feature can redirect network traffic flow to be redirected to 3rd party Intrusion Detection System (IDS) solution on a per security policy basis to support granular event logging.	AU – Audit and Accountability AC- Access Control
	NSX_V_011	NSX can deny access to rogue devices that have not been approved using Spoof Guard. Also, a default deny with a list of approved devices can be established to further prevent rogue devices.	AC- Access Control SC – System and Communications Protection
	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.	CM – Configuration Management

	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.	SC – System and Communications Protection
	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.	AC – Access Control
	NSX_V_015	Network access controls can be managed using NSX, which can also be integrated with 3rd party tools to support managing network access.	SC – System Communications Protection
	NSX_V_016	Using NetX API, NSX can support integration with 3rd 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.	SI – System and Information Integrity
	NSX_V_017	NSX can manage all internal network connections and provides documentation to describe the networking components available for deployment.	CA – Security Assessment and Authorization
	NSX_V_018	NSX can manage external network connections through the Edge Gateway, Firewall, VPN, or SSL through Load Balancer. This includes establishing aboundary defense.	SC – System and Communication Protection
	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.	SC – System and Communications Protection

	NSX_V_020	NSX can be implemented with a fault-tolerant architecture; documentation supporting this design is available.	CP– Contingency Planning SA – System and Services Acquisition SC – System and Communications Protection
	NSX_V_021	NSX can restrict inbound internet traffic inside the DMZ using ESG FW, distributed firewall, and the principles of DMZ Anywhere.	SC – System and Communications Protection
	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.	SC – System and Communications Protection
	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.	CM – Configuration Management SC – System and Communications Protection
	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.	CA – Security Assessment and Authorization SC – System and Communications Protection,
	NSX_V_025	NSX can leverage a Root Certification Authority tosupport Public Key Infrastructure within the virtualized network platform.	SC – System and Communications Protection
	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.	VMware Best Practice
	NSX_V_027	In the event of fail-safe procedures, NSX can move around machines to other recovery networks via automated quarantine actions.	SC – System and Communications Protection

	NSX_V_028	NSX provides a dashboard to monitor the platform's health, which can inform users around maintenance information of the platform itself.	MA – Maintenance SA- System and Services Acquisition
	NSX_V_029	NSX can be configured to protect against unauthorized data mining of the NSX postgres database.	AC – Access Control MP-Media Protection PL-Planning SC- System and Communications Protection
	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.	SA- System and Services Acquisition SC – System and Communications Protection
	NSX_V_031	NSX provides Stateful Firewall capabilities that can support adding devices requiring access control based on an Access Control List.	AC – Access Control SC- System and Communication Protection
	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).	AC – Access Control
	NSX_V_033	NSX can be architected to place firewalls between security domains, DMZ, and other network zones.	SC- System and Communication Protection
	NSX_V_034	NSX and vCenter architecture can be designed todistribute processing activities across multiple facilities, including using geographic separation.	VMware Best Practice
	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.	AC- Access Control IA – Identification and Authorization

	NSX_V_036	NSX provides and maintains a system hardening guide.	CM – Configuration Management
	SRM_001	Recovery can be included in simulated events as part of the larger continuity plan training. The simulated fail over 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).	CP – Contingency Planning
	SRM_002	SRM can push logs to be stored in vRLI. A content pack is provided to facilitate SRM logging and dashboard visualization of logging.	AU – Audit and Accountability AC- Access Control
Site Recovery Manager	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.	CP – Contingency Planning
	SRM_004	SRM can execute fail-safe procedures if initiated manually or via an API call. Additionally, if the source site is unavailable then automatic fail-over will occur.	SC – System and Communications Protection
	SRM_005	SRM 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. configuration of Windows event logging.	AC – Access Control AU – Audit and Accountability MA – Maintenance
	SRM_006	Access to SRM 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.	IA – Identification and Authentication
	SRM_007	Remote access is possible via Remote Desktop Protocol (RDP) to the SRM system. This can be managed through external authentication solutions. Use of SRM does not require RDP access mechanism and RDP is usually allocated for administrative access only.	AC – Access Control SC – System and Communications Protection

	SRM_008	SRM relies on vCenter to manage assign user access and manage user accounts, including assignment of roles to restrict functionality.	AC – Access Control PS – Personnel Security
	SRM_009	SRM can be configured to use Active Directory orvSphere domain accounts that adhere to organizational password standards, including forcing users to change their password upon first log on.	IA – Identification and Authorization
vCloud Usage Meter	UM_001	Proxy configuration is available during the initial setup of Usage Meter and also features full LDAP configuration.	AC – Access Control
	UM_002	Usage Meter retains a list of connections that are the subject of monitoring and usage collection. Usage Meter is installed within the vSphere environment, which is capable of full LDAP integration where user accounts can be controlled even further.	AC – Access Control
	UM_003	vSphere logs user activity and can be maintained for a set period of time. These logs can be secured via various methods, such as user account permissions.	AU – Audit and Accountability
	UM_004	Users can be uniquely identified through different aspects via the vSphere Web Client, as well as various methods derived from LDAP integration and configuration.	IA – Identification and Authorization
	UM_005	Usage Meter can be configured to utilize proxy services, in addition to leveraging LDAP integration to manage user ID's and passwords within a secure environment. This includes configuring the minimum and maximum password ages that can be applied to user accounts.	IA – Identification and Authorization
	UM_006	Any and all maintenance tools are controlled andmonitored through the vSphere Web Client, of which Usage Meter is integrated into.	MA – Maintenance

	UM_007	Separate user functionality from system management functionality.	SC – System and Communications Protection
	UM_008	Protect data from modification or loss while transmitting between separate parts of the system.Segregate applications and databases that contain restricted data or restricted information in an internal network zone. Enable encryption of a protected distribution system if sending restricted data or restricted information.	SC – System and Communications Protection
vCloud Director	vCD_001	vCloud Director has the ability to administrate user accounts, in addition to assigning those accounts various permissions, through the Administration Home Page and LDAP integration. Account management can also be accomplished through the vCloud API.	AC – Access Control
	vCD_002	Logging capabilities are configured and observed through vCloud Director's Manage and Monitor portal.	AC – Access Control
	vCD_003	Session lock capabilities can be employed, such as configuring the number of invalid logins before lockout occurs, through vCloud Director's Administration portal and also within the General System Settings.	AC – Access Control
	vCD_004	Configuring device and accounts that have access control permissions can be accomplished throughvCloud Director's Administration portal.	AC – Access Control
	vCD_005	System Administrator account permissions cannot be altered and encompass all existing rights, in addition to rights only associated with an Administrator role.	AC – Access Control
	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.	AC – Access Control

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.	AC – Access Control CA – Security Assessment and Authorization
vCD_008	An administrator account associated with vCloud Director can fully manage user accounts, including properly updating accounts and their access rights.	AC – Access Control PS – Personnel Security
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.	AU – Audit and Accountability
vCD_010	vCloud Director has the ability to monitor all assets within its environment, as well as produce reports that can later be utilized during forensic analysis.	AU – Audit and Accountability
vCD_011	Authentication measures are handled through the vSphere environment, of which vCloud Director is apart of.	IA – Identification and Authentication
vCD_012	vCloud Director can be coupled with vCD Availability to ensure proper contingency functionality within the vCloud Director environment, as well as other facets of the vSphere environment.	CP – Contingency Planning
vCD_013	AppDefense can be integrated into the vSphere environment, of which vCloud Director relies upon,to establish and maintain intrusion detection functionality.	IR – Incident Response
vCD_014	AppDefense can be integrated into the vSphere environment, of which vCloud Director relies upon,to implement and maintain incident management functionality.	IR – Incident Response
vCD_015	Intrusion detection procedures can be implemented within the vSphere environment, of which vCloud Director is integrated with, through the addition of AppDefense.	IR – Incident Response

	vCD_016	vCloud Director is responsible for tethering various cloud environments together, one of which can provide customer service business functionalities.	IR – Incident Response
	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 utilizing features afforded through AppDefense to vSphere, which encompasses vCloud Director.	IR – Incident Response
	vCD_018	While utilizing AppDefense within the vSphere environment, which contains vCloud Director, a user is afforded the ability of establishing and maintaining various incident response procedures.	IR – Incident Response SI – System and Information Integrity
vCloud Availability for vCloud Director	vCA_001	vCD Availability is integrated with vCloud Director, which is installed in the vSphere environment. In turn, users that are currently using vCD Availability services are subject to the termination of their session if idle for too long.	AC – Access Control
	VCA_002	It is possible to limit super user accounts to designated system administrators, if using LDAP through vSphere.	AC – Access Control
	VCA_003	Account lockout procedures can be configured by the use of LDAP services, which can be indirectly used in conjunction with vCD 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.	AC – Access Control
	VCA_004	vSphere has its own internal log management processes that can be utilized via any user, with applicable permissions, of vCD Availability. A user of vCD Availability can configure logging mechanisms within the vSphere environment that can be used for later analysis.	AU – Audit and Accountability

	VCA_005	The policy engine allows monitoring and event generation to react to changing conditions in the vRealize Orchestrator or plugged-in technology.	AU – Audit and Accountability
	VCA_006	Event logs stemming from the vSphere environment, of which vCD Availability is a part of,can be stored securely and protected from unauthorized access.	AU – Audit and Accountability
	VCA_007	A complete network overview can be reviewed via vSphere. This includes any ports, protocols, and services are currently active within the environment.	CM – Configuration Management
	VCA_008	When utilizing LDAP integration within the vSphere Environment, uniquely identifying properties can be employed to user accounts. This includes those who have access to vCD Availability through vSphere.	IA – Identification and Authentication
	VCA_009	Proxy measures can be implemented within the vSphere environment, in turn affecting vCD Availability, and can be configured to only allow access to properly identified and authenticated connections.	IA – Identification and Authentication
	VCA_010	The "Enable Password History" feature can be enabled via the vSphere Web Client, or through LDAP integration, and effects vCD Availability services due to access being derived through vSphere.	IA – Identification and Authentication
	vCAv_011	Various password settings can be configured through LDAP, which indirectly affects vCD Availability services.	IA – Identification& Authentication
	vCAv_012	System management is accomplished through the vShpere Web Client, which is completely separate from vCloud Director. vCloud Director governs services such as that of vCD Availability.	SC – System and Communications Protection

	VCA_013	Fall back procedures and services are provided via vCD Availability in the event of catastrophic failure of an environment through the use of various virtual machine replications.	SC – System and Communications Protection
	VCA_014	User privileges are dictated through configurations stemming from either vSphere, or LDAP integration, all of which affect vCD Availability due to being deeply entangled with vSphere through vCloud Director.	SC – System and Communications Protection
vCloud Director Extender	vCDX_001	vCD Extender is a plugin for vCloud Director, whichis integrated within the vSphere environment. vSphere is capable of establishing various access rights to the user through the vSphere Web Client.	AC – Access Control
	vCDX_002	Various roles and accounts can be configured through the vSphere Web Client, of which vCD Extender is inherently a part of.	AC – Access Control
	vCDX_003	The capturing of logs can be accomplished through the vSphere Web Client. Actions taken by the user with root privileges can be detailed within the vSphere Web Client.	AC – Access Control
	vCDX_004	Account lockout procedures can be configured via LDAP integration with vCloud Director, thus affording these same traits to vCD Extender.	AC – Access Control
	vCDX_005	vCD Extender retains information regarding all previously performed virtual machine migrations.	AT – Awareness and Training AU – Audit and Accountability
	vCDX_006	The preservation of logs can be accomplished through the vSphere Web Client, of which vCD Extender is inherently integrated with.	AU – Audit and Accountability
	vCDX_007	A list detailing the network configuration can be viewed within the vSphere Web Client where vCD Extender resides.	CM – Configuration Management

	vCDX_008	vCD Extender is innately apart of the vSphere environment, which has the ability to enforce uniquely identifying properties to various users.	IA – Identification and Authentication
	vCDX_009	The enforcement of password history requirements can be accomplished through LDAP integration, which can be successfully accomplished environment.	IA – Identification and Authentication
	vCDX_010	vSphere can be successfully integrated with LDAP, which enables the options of configuring minimum and maximum password age standards for its users. vCD Extender will inherit these properties due to its deep integration with vSphere via vCloud Director.	IA – Identification and Authentication
	vCDX_011	vCD Extender employs the use of the Replicator, which provides the data transfer and monitoring, to protect data with encrypted TCP traffic during a virtual machine migration.	SC – System and Communications Protection
	VCENTER_001	vCenter supports access control configuration including session timeout, logon attempts, account lockout threshold, account lockout duration, minimum password age, and requiring re- authentication.	IA – Identification and Authorization AC – Access Control
	VCENTER_002	Concurrent sessions can be limited on web clients and virtual machine consoles.	AC – Access Control
	VCENTER_003	vCenter employs unique user identifiers through Platform Services Controller (PSC), which manages integration with SSO. Unique user identifiers can be assigned using PSC.	IA – Identification and Authorization AC – Access Control
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 comb.	VMware Best Practice

	VCENTER_005	Super user capabilities in vCenter are a combinationof 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.	AC – Access Control
	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.	CP – Contingency Planning SA – System and Services Acquisition
	VCENTER_007	vCenter can list all the virtual machines and support creating an inventory of technology systems.	CM – Configuration Management
	VCENTER_008	Remote access to vCenter via SSH, or vSphere Web Client or API over HTTPS, can be configuredas the secure communication protocol. For the VMware vCenter Server Appliance™, it runs on Linux and can be restricted to accept only HTTPS. Session identifiers are invalidated after session termination.	AC – Access Control CA – Security Assessment and Authorization SC- System and Communications Protection
	VCENTER_009	vCenter can be configured to log out inactive sessions. By default, inactivity is set to log out after 15 minutes.	AC – Access Control
	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.	MP – Media Protection, AU – Audit and Accountability SC – System and Communications Protection
	VCENTER_011	vCenter can push logs to be stored in an external log repository that supports syslog, including vRealize Log Insight. In the event vRealize Log Insight is used, it can then apply tamper protection of logging that can be used during after-the-fact investigations without altering the event logs.	AU – Audit and Accountability AC – Access Control

	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.	SI – System and Information Integrity AC – Access Control MP-Media Protection PL – Planning SC- System and Communication Protection
	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.	AU – Audit and Accountability AC – Access Control
	VCENTER_014	vCenter can be configured to display a login banner to users before granting access to the system.	AC – Access Control
	VCENTER_015	vCenter supports enhanced logging of audit-level events to support third-party integration with tools such as Introduction Detection Systems (IDS).	AC – Access Control AU- Audit and Accountability SI – System and Information Integrity
	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.	SC- System and Communication Protection SI – System and Information Integrity
	VCENTER_017	Resources can be limited based on priority using pools, storage Input/output (IO) control, Network Input/output Control (NIOC), or Dynamic Resource Scheduling (DRS) reservation.	VMware Best Practice
	VCENTER_018	vCenter can be run on a Linux appliance that is configured to restrict network traffic through use of a software firewall, which is restricted to only necessary ports during the installation. However, if vCenter is run on a Windows appliance, the network traffic and firewall are inherited based on the user's configuration of the Windows appliance.	CA – Security Assessment and Authorization

	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.	SC – System and Communications Protection
	VCENTER_020	vCenter can push audit trail logs to be archived in an external log repository that supports Syslog, including vRLI.	AU – Audit and Accountability CP- Contingency Planning
	VCENTER_021	vCenter can patch ESXi hosts through VMware Update Manager (VUM).	CM- Configuration Management SI – System and Information Integrity SA- System and Services Acquisition
	VCENTER_022	vCenter can facilitate installation of critical security updates for ESXi. VMware 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).	CM- Configuration Management SA- System and Services Acquisition
	VCENTER_023	vSphere Hardening Guide provides support for ESXi and vCenter hardening - procedures. https://www.vmware.com/security/hardening-guides.html	CM – Configuration Management
	VCENTER_024	Logon authentication techniques includes Two Factor Authentication.	AC – Access Control
	VCENTER_025	vCenter natively can provide two-factor authentication techniques such as CAT Card and RSA2FA.	IA – Identification and Authorization
vRealize Log Insight	VRLI_001	Using 3rd party software, vRLI can be configured to support non-repudiation of log entries and monitor access to logs to ensure 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.	AU – Audit and Accountability

	VRLI_002	A proof of maintenance log is available to report on archival maintenance activity.	MA – Maintenance
	VRLI_003	Session lockouts are enforceable and require users to re-authenticate after a session time-out.	IA - Identification and Authentication
	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.	SI – System and Information Integrity AU – Audit and Accountability AC – Access Control
	VRLI_005	vRLI supports standard SYSLOG and secure SYSLOG. In addition, when using an internal vRLI agent, a secure, encrypted protocol is enforceable	AU – Audit and Accountability
	VRLI_006	Audit Dashboard is provided to analyze log data and support after-the-fact investigations. In addition, vRLI 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.	AU – Audit and Accountability
	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 timestamps to support event log correlation.	AU – Audit and Accountability
	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.	AU – Audit and Accountability
	VRLI_009	Logging uses the First in First out (FIFO) mechanism to avoid overwriting logs. If system capacity is reached, users are prompted to archive older log data. Users can define the retention policy.	AU – Audit and Accountability

	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.	AU – Audit and Accountability
	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 and retention and to protect logs from unauthorized activity.	AU – Audit and Accountability
	VRLI_012	Remote access to vRealize Log Insight is by default set to HTTPS. Session identifiers are discarded upon session termination.	AC – Access Control
	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 Platform Services Controller to enable enforcement of authentication parameters from Active Directory directly.	AC – Access Control
	VRLI_014	vRealize Log Insight provides management of user accounts through the Access Control panel, including managing users configured locally, as well as accounts created through an external authentication solution.	PS – Personnel Security AC – Access Control
	VRLI_015	vRLI 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. vIDM or an external authentication solution is required to administer this capability. vRLI can integrate authentication with vCenter's PSC to enable enforcement of authentication parameters from Active Directory directly.	SC – System and Communications Protection AC – Access Control
	VRLI_016	vRLI can manage an Access Control List via agent and host listings to manage devices, as well as restricting the logs a device can access. Role based access can limit access to specific log devices and log data.	AC – Access Control

	VRLI_017	If local accounts are created in vRLI, users can be required to change their password upon first logon.	IA – Identification and Authorization
	VRLI_018	Alerts are generated when agents are unresponsive, or offline after a defined period.	AU-Audit and Accountability IR- Incident Response
	VRLI_019	vRealize Log Insight collects logs in real time. Content packs to enhance dashboards and provide custom queries tailored to many VMware products.	AU – Audit and Accountability
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.	AU – Audit and Accountability
	VRNI_002	A proof of maintenance log is available to report on archived maintenance activity.	MA – Maintenance
	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 vRNI 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.	SC - System and Communications Protection
	VRNI_004	After fifteen minutes of inactivity, users are locked out and required to re-authenticate.	IA - Identification and Authentication AC - Access Control
	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.	AU – Audit and Accountability
	VRNI_006	vRealize Network Insight can be used to monitor data center traffic and provide visibility to support monitoring activities.	SI – System and Information Integrity AC – Access Control

	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.	RA – Risk Assessment CA – Security Assessment and Authorization
	VRNI_008	vRealize Network Insight logs network traffic with a default retention period of thirty days, which can be extended to thirteen months. This log data can provide audit trail support.	AU – Audit and Accountability
	VRNI_009	vRealize Network Insight can provide visibility into the information flow, including information flow insight for managing policies of the system and between interconnected systems.	AC - Access Control SC - System and Communications Protection CA - Security Assessment and Authorization AU - Auditand Accountability AT -Awareness and Training
	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), and password complexity can be configured.	AC - Access Control PS - Personnel Security SC - System and Communications Protection IA - Identification and Authentication
	VRNI_011	The vRealize Network Insight traffic between the Platform and Proxy servers can be encrypted using certificates.	SC - System and Communications Protection
	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.	SC - System and Communications Protection AC - Access Control

vRealize Orchestrator	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.	CM – Configuration Management
	VRO_003	A proof of maintenance log is available to report on archived maintenance activity.	MA – Maintenance
	VRO_004	vRealize Orchestrator supports multiple roles to separate user functionality from system management functionality, as well as the capability to support the principle of least privilege user access control.	AC – Access Control
vRealize Operations	VROPS_001	A proof of maintenance log is available to report on archived maintenance activity.	MA – Maintenance
	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. vRealize Operations user interface is only accessible via a secure URL. Upon session termination, session identifiers are invalidated.	SC – System and Communication Protection AC – Access Control
	VROPS_003	Session lockouts enforced by default and require users to re-authenticate after a session time-out.	IA - Identification and Authentication AC - Access Control
	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 content pack relies on vSphere to evaluate technical configurations and settings based on the compliance pack's baseline.	CM – Configuration Management CA – Security Assessment and Authorization
	VROPS_005	vRealize Operations has a maximum of concurrent sessions (6); this setting cannot be altered.	AC – Access Control

	VROPS_006	Using a management pack, vRealize Operationscan store information that is collected by agents via the use of plug-ins to collect data from guestOperating Systems running in virtual machines.	CM – Configuration Management
	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.	CP – Contingency Planning
	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.	IA – Identification and Authorization
	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.	AU – Audit and Accountability AT – Awareness and Training
	VROPS_010	vRealize Operations can be configured to support account lockout duration, number of failed attempts, and password length and complexity.	AC – Access Control
	VROPS_011	vRealize Operations can push audit trail logs to be archived in an external log repository that supports Syslog, including vRealize Log Insight.	AU – Audit and Accountability
	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)	SC – System and Communications Protection
	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.	CA - Security Assessmentand Authorization

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-crypto graphic user access to configuration of this feature.	SC – System and Communications Protection PS – Personnel Security IA – Identification and Authorization AU – Audit and Accountability AC – Access Control
	vSAN_002	Logging capabilities can be enabled and customized to capture event information.	AU – Audit and Accountability
	vSAN_003	Logging can be synchronized to system clocks (NTP) and capture a date and time stamp.	AU – Audit and Accountability
	vSAN_004	vSAN can push logs to be stored in vRealize LogInsight. A default vSAN dashboard is available in vRealize Log Insight as a content pack.	AU – Audit and Accountability
	vSAN_005	Session lockouts are enforceable and require users to re-authenticate after a session time-out, which are controlled by vCenter or ESXi.	AC – Access Control
	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.	MP – Media Protection AU – Audit and Accountability
	vSAN_007	vSAN can be patched via vCenter's VMware Update Manager patching capabilities. In addition, vSAN 6.7 has the ability to patch firmware controller drivers for participating vendors.	SI - System and Information Integrity
	vSAN_008	Maintenance activity is logged and can be accessed via reports, which can be archived for historical reference. The maintenance logging information is captured at each component vCenter, ESXi, and vSAN, which can be holistically analyzed via vRealize Log Insight or customized.	MA – Maintenance

	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.	AU – Audit and Accountability
	vSAN_010	Cryptographic management features supported include rotation of keys via User Interface or API integration, changing Key Manage System (KMS) providers, and broadly enabling or disabling encryption. These capabilities can be used to support cryptographic procedures.	SC – System and Communications Protection
	vSAN_011	vSAN utilization 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.	SC – System and Communications Protection
vSphere Replication	VSPHEREREPLICATION_001	Replication of virtual machine object and its data can be used to support continuity planning and provide a virtualization technology alternative to off-site vSphere environment storage using electronic media.	CP – Contingency Planning
	VSPHEREREPLICATION_002	vSphere Replication supports geographical separation through use of vSphere replicated infrastructure to provide timely and effective recovery operations.	CP – Contingency Planning
	VSPHEREREPLICATION_003	vSphere Replication integrates with Site Recovery Manager to enable mitigation during an outage ordisruption.	CP– Contingency Planning
	VSPHEREREPLICATION_004	Recovery policies can be set up to specified recovery point objectives (RPO), which can be selected from a range of 15 minutes to 24 hours. vSphere Replication (6.5) can be reduced to 5 minutes and up to 24 hours.	CP – Contingency Planning
	VSPHEREREPLI CATION_005	You can enable the network encryption of the replication traffic data for new and existing replications to enhance the security of data transfer	SC - System and Communications Protection

	VSPHEREREPLI CATION_006	vSphere has a management pack for integration with vRO and this integration helps automate the disaster recovery workflows with SRM integrationin place	CM - Configuration Management
Workspace One Access (WS1A) (WSA)	WSA_001	Access controls to objects and users is 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. WSA supports Single Sign On (SSO) and serves as a platform services controller for other VMware products.	IA - Identification and Authentication
	WSA_002	WSA supports VMware Verify, a two-factor authentication product. In addition, WSA can be integrated with 3rd party two-factor authentication solutions.	IA - Identification and Authentication AC - Access Control
	WSA_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 WSA in the cloud, the system is set to store event data for 90 days. For WSA 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.	MA - Maintenance
	WSA_004	Remote system management of WSA is bifurcated into Operational Access via SSH and Administrator Access via HTTPS. In both instances, session identifiers are invalidated upon session termination.	SC - System and Communications Protection AC - Access Control
	WSA_005	WSA issues session tokens (default value of 8 hours), which can be configured to force users to re-authenticate after the token expires.	IA - Identification and Authentication
	WSA_006	WSA can push logs to vRLI, or a 3rd party logging system that supports Syslog. For WSA in the cloud, the system is set to store logs for 90 days. For WSAon-prem, disk size may require recycling of logs. Therefore, for both cloud and on-prem instances, pushing log files	AU - Audit and Accountability

		to a proper log repository is recommended.	
	WSA_007	WSA supports configuration of access control setting such as: requiring new users to change password on first logon, minimum password age, account lockout threshold, account lockout duration.	AC - Access Control IA - Identification and Authentication
	WSA_008	User Account reviews is supported through a standardized reporting function available to WSAAdministrators.	AC - Access Control PS - Personnel Security
	WSA_009	WSA access can be assigned to roles such as Operator, Administrator, and User.	AC - Access Control SC - System and Communications Protection
NSX-T	NSX_T_001	NSX-T session time-out will terminate session after a defined period of inactivity (default is set to 15 minutes).	AC - Access Control
	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.	IA - Identification and Authentication
	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 leveraging segmentation concepts.	SC - System and Communications Protection
	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.	CP - Contingency Planning

NSX_T_005	NSX-T services are restricted from kernel level access, as well as from components further up the technology stack. Also, additional services can be restricted.	CM - Configuration Management
NSX_T_006	Session lockouts are enforceable and require users to re-authenticate after a session time-out.	AC - Access Control SC - System and Communications Protection
NSX_T_007	Account lockout thresholds can be altered. NSX-Tprovides 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.	AC - Access Control
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.	AU - Audit and Accountability
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 usageand other security violations.	AC - Access Control SI - System and Information Integrity
NSX_T_010	NSX-T closely monitors session IDs to minimize the risk of replay attacks.	IA - Identification and Authentication
NSX_T_011	During a Panic Attack, the system will restart by default and potentially shut down after repeated failures.	SI - System and Information Integrity

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.	CM - Configuration Management
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.	CM - Configuration Management
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 controls for objects can be restricted based on security rules and tags, as well as through configuration policies and firewall polices to manage internal information flow.	AC - Access Control, SC - System and Communications Protection
NSX_T_015	Combined with Workspace One Access or another integrated Identity Access Management tool, NSX-Tcan support two-factor authentication.	IA - Identification and Authentication
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.	SI - System and Information Integrity
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.	CA - Security Assessment and Authorization SC - System and Communications Protection

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.	SC - System and Communications Protection
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 ensure external perimeter network access is managed accordingly.	SC - System and Communications Protection
NSX_T_020	NSX-T can be implemented with a fault-tolerant architecture. This can be used to schedule backups and restore backups too.	CP - Contingency Planning SC - System and Communications Protection
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.	SC - System and Communications Protection
NSX_T_022	NSX-T documents product capabilities to support security architecture through publication and version maintenance in the Product Applicability Guide (PAG whitepaper).	SA - System and Services Acquisition PL - Planning
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.	SI - System and Information Integrity
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, as well as 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.	SC - System and Communications Protection IA - Identification and Authentication

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.	SI - System and Information Integrity
NSX_T_027	NSX-T as a virtualized networking infrastructure can move around machines to recovery networks to support fail-safe procedures.	CP - Contingency Planning PE - Physical and Environmental Protection
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 overall health of the platform.	CP - Contingency Planning
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.	SI - System and Information Integrity IR - Incident Response
NSX_T_030	NSX-T 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. This includes firewall rules with tracking mechanisms to block a port or take other precautionary measures once a DoS attack is identified.	SC - System and Communications Protection
NSX_T_031	NSX-T can provide firewall-based Access ControlList functionality to restrict access based on IP Addresses and VM names.	AC - Access Control
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, as well as the concept of Least Privilege.	AC - Access Control CM - Configuration Management SA - System and Services Acquisition SC - System and Communications Protection

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.	CM - Configuration Management
NSX_T_034	NSX-T provides and maintains a system hardening guide.	AC - Access Control SA - System and Services Acquisition CM - Configuration Management
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.	AC - Access Control
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 restrictedto read-only and can also be disabled. The system can enforce changing default passwords.	AC - Access Control IA - Identification and Authentication
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.	AC - Access Control
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.	IA - Identification and Authentication
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.	AC - Access Control

	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 to make changes to NSX-T based on the assignment of this group/role to approved user(s).	CM - Configuration Management
	NSX_T_041	NSX-T can encrypt network traffic and monitor forexceptions to support network confidentiality and data protection, including loss of data over the network.	SC - System and Communications Protection
	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.	SI - System and Information Integrity
	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.	SI - System and Information Integrity
	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.	AU - Audit and Accountability
	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.	AU - Audit and Accountability

	NSX_T_046	NSX-T can be configured to prompt users with a login banner, or system use agreement that is displayed as a message.	AC - Access Control PS - Personnel Security
	NSX_T_047	NSX-T can capture some events of unauthorizedaccess, such as performing events that are not authorized. In some cases, the UI will prompt theuser that sufficient permission is unavailable to perform the desired action.	SI - System and Information Integrity
	NSX_T_048	NSX-T system clocks can be synchronized to NTP to enable accurate and universal time source logging.	AU - Audit and Accountability
	NSX_T_049	NSX-T 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, or assigning or reserving static IP addresses in DHCP.	SC - System and Communications Protection CA - Security Assessment and Authorization SI - System and Information Integrity
	NSX_T_050	NSX-T monitors memory and takes precautions based on best practices to safeguard memory from unauthorized code execution.	SI - System and Information Integrity
	NSX_T_051	NSX-T establishes session authenticity through Transport Layer Security (TLS). By default, version 1.0 is disabled due to recent industry guidance that it has known vulnerabilities. Version 1.1 and 1.2 are supported and recommended.	SC - System and Communications Protection
	NSX_T_052	NSX-T can prioritize traffic to support telecommunications Service Level Agreements by using Quality of Service (QoS) customization.	CP - Contingency Planning
	NSX_T_053	NSX-T can whitelist or blacklist applications from communicating VM to VM by using firewall rules to enforce communication access rules.	CM - Configuration Management

About VMware

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

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

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

For more information on VMware security, visit security.vmware.com.

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 aswell as business. This dual background means that we understand the importance of growth and profitability and our solutions are designed to enhance both.

As a consulting firm that has the ability to fully implement whatever it recommends, Tevora works with all of the industry's top vendors, yet is beholden to none. We are completely vendor-independent and select best-of-breedproducts 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 tohelp 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