Telco Cloud Platform - 5G Edition Intrinsic Security Guide

VMware Telco Cloud Platform 3.0

You can find the most up-to-date technical documentation on the VMware website at:

https://docs.vmware.com/

VMware, Inc.
3401 Hillview Ave.
Palo Alto, CA 94304
www.vmware.com

Contents

About this Telco Cloud Platform 5G Edition Intrinsic Security Guide

1

This Telco Cloud Platform 5G Edition Intrinsic Security Guide summarizes the security risks and requirements that Communications Service Providers (CSPs) face as they transition to 5G networks and increasingly rely on virtualization and cloud computing, including network functions virtualization and cloud-native technology such as Containers and Kubernetes.

This guide describes how VMware technology helps you to implement security controls for the virtualization plane and its management and orchestration. This guide also describes how to combine VMware technologies into an architecture that protects telecommunication networks with intrinsic security.

After providing a brief overview of the VMware Telco Cloud layers, this guide highlights security requirements and solutions for the virtualization and management of telecommunication networks.

Intended Audience

This guide is intended for telecommunications and solution architects, sales engineers, field consultants, advanced services specialists, and customers who are responsible for the design, deployment, and operations of Telco Clouds, Virtualized Network Functions (VNFs), Cloud Native Network Functions (CNFs). This guide helps you to understand, assess, and mitigate 5G cybersecurity risks.

Acronyms

The following table lists the acronyms that are used frequently in this security guide:

Acronym	Definition
CNF	Cloud Native Network Function
CSP	Communications Service Provider
DEK	Data Encryption Key
KEK	Key Encryption Key
KMS	Key Management Server
NCSC	National Cyber Security Centre
NCCoE	National Cybersecurity Center of Excellence

Acronym	Definition
NFV	Network Functions Virtualization
NFVI	NFV Infrastructure
NFVO	NFV Orchestration
NIST	National Institute of Standards and Technology
TSRs	Telecommunication Security Requirements
VDC	Virtual Data Center
VIM	Virtual Infrastructure Manager
VNF	Virtualized Network Function

Challenges in Transitioning to 5G

2

The National Cybersecurity Center of Excellence (NCCoE) at the National Institute of Standards and Technology (NIST) recognizes the challenges that organizations face in transitioning from 4G to 5G. The need to safeguard new 5G technologies is a concern while 5G development, deployment, and usage are evolving. Some aspects of securing and using 5G components lack standards and guidance, making it challenging for 5G network operators and users to know what must be done and how to accomplish it.

To help organizations effectively manage 5G security risks, NCCoE developed the 5G Cybersecurity project to provide sample approaches for securing 5G networks through a combination of 5G security features defined in the 5G standards and third-party security controls.

In a landmark analysis at the dawn of 5G, the National Cyber Security Centre (NCSC) of the United Kingdom (UK) published a January 2020 paper that summarizes the findings of its analysis of the UK telecommunication sector. According to the report, "The potential economic and social benefits of 5G and full-fibre digital connectivity can only be realized if we have confidence in the security and resilience of the underpinning infrastructure."

The NCSC recommends the establishment of a robust security framework based on a new set of Telecommunication Security Requirements (TSRs) that are intended for Communications Service Providers (CSPs) to operate secure networks. In the U.K., this security framework is underpinned by legislation. The NCSC's summary of these security requirements addresses some of the security concerns raised by the 5G PPP Security Working Group in a 2017 paper that identified 5G security risks.

The challenges that 5G networks face in supporting new business requirements "have rendered current network security approaches inadequate," the 5G PPP Security Working Group wrote, calling for "a security makeover of how confidentiality, integrity, and availability is maintained and managed in 5G networks."

The use of network functions virtualization and the transition from 4G networks to 5G, coupled with the necessity to protect user information, only increases the complexity of the security landscape. The use of public clouds magnifies these trends.

At the same time, the network virtualization expands the application and management of security measures.

A 5G deployment might result in fragmented and difficult-to-manage security measures. The combinatorial nature of 5G, in which CSPs can mix elements of 4G and 5G networks, means that the application of network security measures might be uneven—the security measures are likely to evolve and shift with a network as it combines various 4G and 5G elements. New 5G network elements and the use of public clouds might intensify the importance of centralized management and monitoring. Flexible, intrinsic, and automated approaches to imposing and enforcing security measures are becoming important.

To identify the key security risks and requirements in the changing telecommunication landscape, this guide relies on the following standard-setting papers:

1. Security Analysis for the UK Telecom Sector: Summary of Findings, published by the National Cyber Security Centre of the United Kingdom in January 2020.
2. 5G PPP Phase 1 Security Landscape, published by the 5G PPP Security Working Group in June 2017.
3. Cybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures, published by the European Commission in January 2020.

Read the following topics next:

- Security Risk Factors and Attack Vectors

Security Risk Factors and Attack Vectors

Some security risks are specific to 5G, while other risks accompany the infrastructure of most CSPs and they might remain during the transition to 5G. Risk factors are evaluated and prioritized based on their impact on three key aspects of information security:

- Integrity
- Availability
- Confidentiality

Based on its findings, the NCSC considers the following functions to be critically sensitive. These functions require a high-level protection, and a compromise could undermine integrity, availability, or confidentiality.

- Virtualization infrastructure
- Controllers
- Orchestrators
- Internet gateways
- Routing and switching of IP traffic at the core
- Database functions
- Authentication, access control, and other security functions

Solving the trade-off between security and performance

A conflict undermines the security of some telecom networks. Implementing a secure network can be expensive, and there can be a trade-off between security and performance:

"In the last couple of years, the operators' commercial drivers have come into direct conflict with the NCSC's security advice," NCSC Technical Director Ian Levy writes in a January 2020 blog post on the future of telecoms. "Those operators who chose to follow our advice and requests were putting themselves at a commercial disadvantage which is unsustainable. So, the government's decision to significantly uplift the baseline telecoms security and formalize the handling of high-risk vendors putting it all on a robust footing is welcome. It provides clarity for operators and transparency about what we expect for the security of national networks. Externalizing the security costs of particular choices (including vendor) help operators make better security risk management decisions." In the UK, for example, eschewing robust security in the name of enhancing performance will not be a choice; the NCSC's telecom security framework will be underpinned by legislation.

Prioritizing performance and revenue over security increases risks and exposes more attack surfaces. The solution is to invest more in infrastructure that improves performance and scalability so that implementing security measures does not degrade network performance.

Some CSPs run their equipment at high levels of utilization across-the-board, causing challenges in applying patches and performing rolling upgrades. This can leave them vulnerable to cyber attacks that exploit known vulnerabilities. However, investing in infrastructure that enhances performance can address this problem.

Investing in infrastructure that improves performance and scalability is an effective way to addressing security risks without compromising network performance. This enables organizations to implement security measures without compromising network performance.

By striking a balance between performance, revenue, and security, organizations can build resilient and secure networks that can withstand cyber attacks and other threats.

Virtualization tier

Key risks to the virtualization plane include the following:

- Attacks that let a hacker bypass a hypervisor's enforced separation to control workloads running on the host or to move laterally to other hosts and applications
- Successful exploitation of the virtualization's fabric, orchestration system, or management functions enables an attacker to access the entire virtualization fabric, including all hosts and virtual workloads. This attack would keep the entire network at risk, affecting the availability and confidentiality of critical services.

Signaling plane and core network virtualization

The signaling plane is responsible for the exchange of control messages between different network elements, such as base stations and core network nodes, to set up and manage user sessions.

Vulnerabilities in the signaling plane related to the lack of proper authentication and encryption mechanisms, threats from insider attacks or new attack vectors, such as software bugs, misconfigurations can be exploited to gain unauthorized access to the network, compromise network elements, and launch distributed denial-of-service (DDoS) attacks.

Overall, the vulnerabilities in the signaling plane pose a significant risk to the availability, integrity, and confidentiality of 5G networks. To mitigate these risks, network operators need to implement robust security measures, such as end-to-end encryption, secure bootstrapping, network segmentation, access controls, and intrusion detection and prevention systems (IDPS). They also need to regularly audit their networks for security weaknesses and train their staff on cybersecurity best practices.

5G-specific threats and risk factors

The 5G PPP Security Working Group's white paper on the 5G security landscape identifies several 5G-specific security risks and their associated requirements. In general, the service-oriented architecture of the 5G core network introduces a broader range of data and services than 4G, increasing the attack surface. The common web protocols and APIs of 5G networks introduce more attack vectors.

The working group identified that the following risks are relevant to the VMware Telco Cloud Platform. This preliminary list requires updates during the transition to 5G.

- Unauthorized access or usage of assets
- Identity theft
- Identity cloning to gain access to sensitive resources
- Fraudulent use of shared resources
- Modification of subscriber credentials
- Weak 5G network slicing isolation
- Privacy Attacks using Side-channel Information
- Traffic capturing rerouting because of recursive or additive virtualization
- Lack of detection of alterations to the control plane or the user plane
- Difficulties in managing vertical SLAs and regulatory compliance

In addition, a lack of common security standards across multiple domains can make the management complex and challenging. This also increases the risk of configuration errors or other changes that expose vulnerabilities or attack vectors.

Key security imperatives for reducing risk

These risks and attack vectors increases the key security risks which demand immediate attention. In general, securing the virtualization plane and its management components relies on the ability to do the following:

- Keep the virtualization fabric and VMs up to date.

- Maintain the fabric as a group and at scale.
- Apply critical security patches quickly.
- Implement mitigations that neutralize known attack vectors.
- Control access to resources and the management layer by using the principles of least privilege and separation of duties.
- Isolate hypervisors and VMs with security domains and pools that prevent movement.
- Protect sensitive data through segmentation of workloads and storage.
- Encrypt data in transit and at rest.
- Architect the virtualized infrastructure by following best practices and patterns for automated provisioning, automated management, secure administration, and micro-segmentation.
- Architect the management of the virtualization plane to isolate it from other systems and networks.
- Strictly control access to and use of the virtualization plane's management layer.
- Monitor and audit the virtualization plane.
- Track access and changes to the management layer.

Overview of VMware Telco Cloud

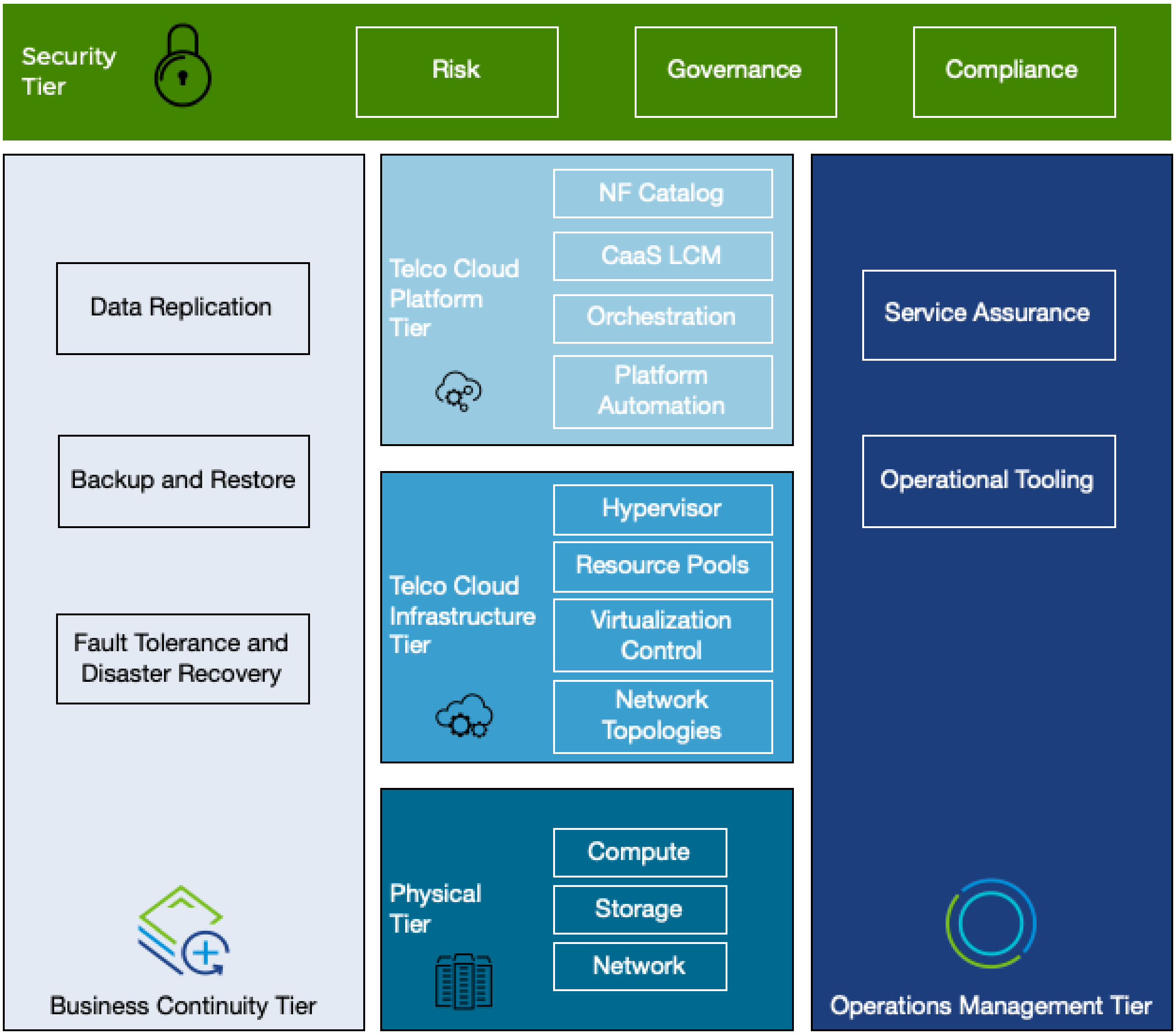
3

VMware Telco Cloud includes three main layers that span the edge network, radio access network, private network, and core network:

- Infrastructure
- Automation
- Operations

These layers form a complete telco stack that empowers you to deploy, automate, operate, and protect network services on a consistent horizontal infrastructure.

Figure 3-1. Telco Cloud Layers



Virtual Infrastructure Tier:

The infrastructure layer supplies infrastructure as a service using VMware Telco Cloud Infrastructure™, which combines virtualization technologies such as VMware vSphere®, VMware NSX®, and (optional) VMware vSAN™.

With VMware Telco Cloud Infrastructure, security is intrinsic, programmable, automated, adaptive, and context-aware. Intrinsic security improves visibility, reduces complexity, and focuses your defenses by enabling you to apply and automate adaptive security measures such as micro-segmentation in the correct place.

VMware Telco Cloud Platform 5G Edition combines VMware Telco Cloud Infrastructure and VMware Telco Cloud Automation™. VMware Telco Cloud Infrastructure is an evolution of VMware vCloud® NFV™. VMware Telco Cloud Automation contains multi-domain orchestration and automation capability. VMware Telco Cloud Platform also embeds Tanzu Kubernetes Grid that allows CSPs to build, manage, and run containerized workloads across private, telco, edge, and public clouds.

Management and Automation Tier:

The Management and Automation tier in the VMware Telco Cloud Stack is a critical component that enables efficient management and automation of the cloud infrastructure.

VMware Telco Cloud Automation is a solution designed specifically for communications service providers (CSPs) to automate the deployment and management of virtualized network functions (VNFs) and services in their telco cloud environments improving service delivery, reduces operational costs, and increases agility.

It integrates with Virtual Infrastructure Manager (VIM) and Kubernetes to build a robust multi-tenant environment for securely managing the application layer.

Operations Tier:

The operations layer provides analytics, network intelligence, and assurance with VMware Telco Cloud Service Assurance and optional components such as VMware Aria Operations™ for Logs (formerly VMware vRealize® Log Insight™), VMware Aria Operations™ (formerly VMware vRealize® Operations™), and VMware Aria Operations™ for Networks (formerly vRealize® Network Insight™).

VMware Telco Cloud Service Assurance provides an integrated service monitoring and network management solution. It correlates physical devices such as hosts, switches, and routers with virtual environments such as NFV, VMs, SDN, and SD-WAN, providing CSP operations teams with rapid insight and automated actions.

To help CSPs who implement 5G or transition to 5G by establishing a mixed non-standalone 5G and 4G network, VMware provides different bundles to support various telco requirements. You can choose the VIM that suits your requirements. A telco-grade Kubernetes distribution from VMware helps you to build, run, and manage CNFs and 5G services.

Protecting the Virtualization Plane and Containerized Environments

4

VMware fulfills the key security requirements for the virtualization plane of telecommunication networks to reduce risk and limit the attack surface.

The requirements and solutions for protecting the virtualization plane are categorized into three areas:

- Securing the virtualization fabric and its components
- Configuring the virtualization fabric to secure the network
- Establishing trust domains and segregation

The security requirements are based on the NCSC's findings and the 5G PPP security working group's white paper. VMware addresses these requirements by implementing settings, controls, and functions to protect virtualized infrastructure, including hypervisors, VMs, virtualized networking, and management functions.

Read the following topics next:

- Securing the Virtualization Fabric
- Configuring the Virtualization Fabric for Network Security
- Establishing Trust Domains and Segregation

Securing the Virtualization Fabric

VMware supplies an underlying virtualization plane with vSphere, vSAN, and NSX. They provide virtualized infrastructure for compute, storage, and networking.

To protect the foundation of the virtualization plane, vSphere establishes a fully-abstracted virtualization layer by using the VMware ESXi™ hypervisor, which prevents virtual workloads from accessing or cutting through to the underlying hardware.

The holistic security architecture of ESXi achieves this goal by providing security mechanisms at multiple layers:

- Secure isolation of virtual machines at the virtualization layer. This includes secure instruction isolation, memory isolation, device isolation, and managed resource usage and network isolation.

- Configurable secure management of the virtualized environment. This includes secure communication between virtualization components through SSL; host protection using lockdown mode; and least privilege by a fine-grained, role-based access-control mechanism.
- Secure deployment of the ESXi software on servers through use of various platform-integrity mechanisms such as digitally signed software packages and Intel Trusted Platform Module (TPM)–based trusted boot.
- Rigorous secure software development life cycle that enables developers to create software using secure design and coding principles such as minimum attack surface, least privilege, and defense in depth.

Keeping the virtualization fabric up-to-date

vSphere Lifecycle Manager (also called VMware vSphere® Update Manager™) centralizes the patch and version management for VMware vSphere and supports VMware ESXi hosts and VMs. Using vSphere Lifecycle Manager (LCM), you can upgrade and patch ESXi hosts, install and update third-party software on hosts, and upgrade Virtual Machine (VM) hardware and VMware Tools™.

LCM works either automatically or manually. A telecommunication operator typically runs LCM manually to check for host patches and extensions at regular intervals. For more information, see About vSphere Lifecycle Manager.

Delivering critical security patches for quick deployment

VMware Security Advisories documents the remediations for security vulnerabilities that are reported in VMware products. VMware Security Response Policy outlines the commitments for resolving vulnerabilities in VMware products. VMware releases a fix for the reported vulnerability in one or more of these forms:

- A new major or minor release of the affected VMware product
- A new maintenance or update release of the affected VMware product
- A patch that can be applied on top of the affected VMware product
- Instructions to download and install an update or patch for a third-party software component that is part of the VMware product installation
- A corrective procedure or workaround to modify the VMware product configuration and mitigate the vulnerability

Updating the virtualization fabric without affecting the network

You can update the VMware Telco Cloud Infrastructure layer without affecting its availability by leverage feature within the vSphere software platform.

You can also update the VMware Telco Cloud Infrastructure layer without affecting Virtual Network Functions (VNFs) if they have a built-in fail-over capability, an active-active pattern, or another pattern that allows them to be moved with automation.

Feature within the vSphere software platform such as VMware DRS (Distributed Resource Scheduler) uses automation to move these VNFs from one set of hosts to another, accelerating the remediation process by determining the optimum number of hosts that can enter maintenance mode simultaneously based on current cluster conditions and demands without affecting the availability of the fabric or the VNFs running in the fabric.

To ensure that the VNF fabric are updated without affecting the network, CSPs require their vendors to supply VNFs with either a built-in failover capability or vSphere HA support as a failover mechanism.

Locking down hypervisors to restrict access

The security of ESXi hosts can be increased by keeping them in the lockdown mode. In the lockdown mode, operations are performed through vCenter Server by default. The Lockdown mode can be used to increase the security of an ESXi host by limiting the access allowed to the host. For more information, see Lockdown Mode.

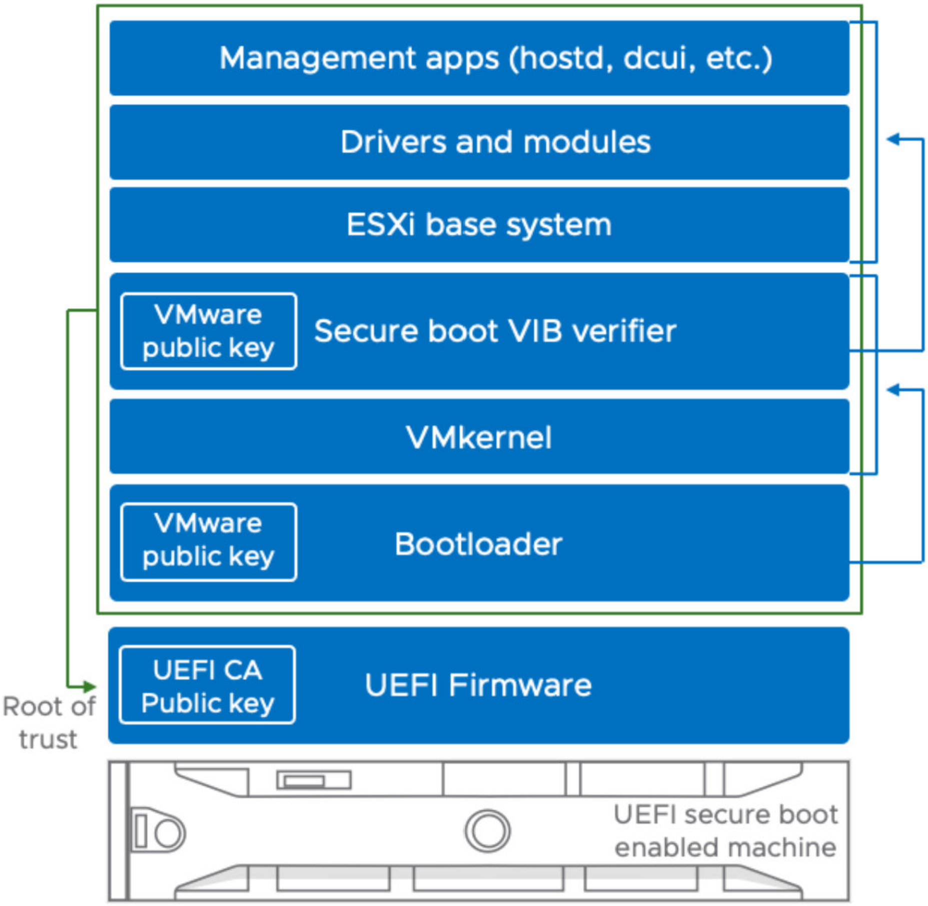
In addition, the vSphere Web Client and the VMware Host Client™ let you open and close firewall ports for each service or allow traffic from specific IP addresses. For more information, see Incoming and Outgoing Firewall Ports for ESXi Hosts.

Adding only known hosts to the fabric

In a VMware environment, you can use host profiles and Preboot Execution Environment (PXE) to improve security by enforcing consistent security configurations and ensuring that only trusted software is loaded on ESXi hosts.

Host profiles in VMware allow administrators to create standard configurations for ESXi hosts in a vSphere environment. These profiles can include security settings such as password policies, firewall rules, and network security configurations. By enforcing these standardized configurations across all ESXi hosts, administrators can ensure that security settings are consistent and up-to-date, reducing the risk of misconfigurations or security vulnerabilities.

Preboot Execution Environment (PXE) is a network boot protocol that allows a computer to boot from a server on the network rather than from its own hard drive. In the context of virtualization, PXE can be used to deploy virtual machines (VMs) to ESXi hosts. By using PXE to deploy VMs, administrators can ensure that the VMs are deployed with the latest security updates and configurations. This can reduce the risk of deploying VMs with outdated or vulnerable software. In addition, PXE can be used in combination with secure boot technologies to ensure that only trusted software is loaded on the ESXi host. Secure boot technologies, such as Unified Extensible Firmware Interface (UEFI) Secure Boot and Trusted Platform Module (TPM), can verify the integrity of the boot process and prevent the loading of unauthorized or malicious software.



Adding only attested hosts to the fabric

VMware uses a technology called Trusted Platform Module (TPM) to cryptographically attest hosts. A TPM is a microchip that is built into the computer's motherboard and is used to store cryptographic keys and measurements of the host's hardware and software configuration.

By using TPM-based attestation, VMware can ensure that only trusted hosts are allowed onto the network, and that the configuration of the hosts is consistent with a known and secure baseline. This helps to prevent unauthorized access, data breaches, and other security threats.

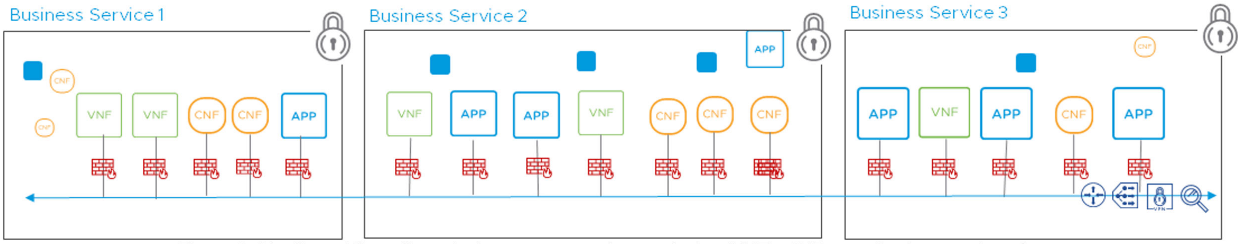
As a security best practice, CSPs must use hardware roots-of-trust to support Secure Boot technology for physical hosts. Secure boot is part of the UEFI firmware standard. With secure boot enabled, a machine does not load a UEFI driver or application unless the operating system bootloader is cryptographically signed. VMware Telco Cloud support ESXi secure boot if it is enabled in the hardware. VMware recommends that you deploy hardware that supports and uses hardware roots-of-trust.

With secure boot enabled, the boot sequence is as follows.

1 The ESXi bootloader uses a VMware public key to verify the signature of the kernel and a small subset of the system that includes a secure boot VIB verifier.

2 The VIB verifier checks every vSphere Installation Bundle (VIB) package that is installed on the system.

At this point, the entire System Boot with the root of trust in certificates that are part of the UEFI firmware.



Segmenting internal and external network traffic

VMware NSX segments internal and external network traffic in the virtualization fabric by implementing virtual firewalls and micro-segmentation. In addition, by incorporating third-party firewalls, you can enhance your virtual environment's security posture and protect your virtual machines from various types of cyber threats, including malware, unauthorized access, and data breaches. You must choose a reputable third-party firewall vendor that offers the features and functionalities that meet your organization's security requirements.

Virtual firewalls can be combined with micro-segmentation to separate all types of traffic, VMs, and workloads.

NSX micro-segmentation is a network security technology that allows you to divide a virtual data center and its workloads into smaller, more granular segments for better security and isolation. These segments are created using virtual firewalls and other security controls to provide network traffic filtering and policy enforcement between segments. You can then apply security controls to each segment, restricting an attacker’s ability to move to another segment or workload.
This approach can reduce the attack surface of your virtualized environment, prevent lateral movement of threats within the network, and limit the impact of a security breach by containing it within a smaller segment of the network.

Micro-segmentation uses the following capabilities to reduce risk and improve security:

- **Distributed stateful firewalling**: Protects each application running in the data center with application-level gateways that are applied on a per-workload basis.
- **Topology-agnostic segmentation**: Protects each application with a firewall independent of the underlying network topology.
- **Centralized ubiquitous policy control of distributed services**: Controls access with a centralized management plane.
- **Granular unit-level controls implemented by high-level policy objects**: Creates a security perimeter for each application without relying on VLANs.
- **Network-based isolation**: Implements logical network overlays through virtualization.

- **Policy-driven unit-level service insertion and traffic steering**: Helps monitor network traffic.

The micro-segmentation capabilities of NSX also meet the security recommendations for protecting virtualized workloads, as outlined in NIST Special Publication 800-125B, Secure Virtual Network Configuration for VM Protection.

Storing secrets and keys in secure hardware-backed storage

An external Key Management Server (KMS) provides the keys for encrypting VMs in vSphere and the vSAN datastore.

Using an external KMS allows for greater security, as the keys are stored in a separate, hardware-backed system that is designed specifically for secure key storage. This helps to protect against unauthorized access to the keys, which are critical for maintaining the confidentiality and integrity of the encrypted data.

However, setting up and maintaining an external KMS can require significant effort and investment, as it involves obtaining and configuring robust third-party hardware to store the keys. Also, Operators must follow proper security protocols and procedures to ensure the ongoing security and integrity of the key management process.

Configuring the Virtualization Fabric for Network Security

VMware NSX provides network virtualization for a software-defined data center, abstracting Layer 2 through Layer 7 networking functions such as switching, firewalling, and routing. NSX embeds the networking and security functionality (typically managed by hardware) in the ESXi hypervisor.

This abstraction enables security and efficiency that were previously infeasible. For example, you can apply micro-segmentation with distributed stateful firewalling and dynamic security policies attached directly to individual workloads.

In addition, vSphere includes several settings to manage the allocation of IP addresses, ports, and encryption. Through hypervisor, VMware decouples the virtual machines from the host providing fault and security isolation at the hardware level.

Preventing the use of hard-coded MAC addresses and virtual span ports

vSphere provides several schemes for automatic allocation of MAC addresses in vCenter Server. You can select a scheme that suits your requirements. For example, you can use generated MAC addresses that are assigned by vCenter Server or the ESXi host. You can also use a range-based or a prefix-based allocation scheme to generate MAC addresses. For more information, see MAC Address Management and MAC Address Assignment from vCenter Server.

With vSphere networking, the security policy of a virtual switch includes a MAC address changes option. This option affects the traffic that a VM receives. When this option is set to Reject, ESXi does not honor requests to change the effective MAC address to an address that differs from the initial MAC address. This setting protects the host against MAC impersonation. The port that the VM adapter used to send the request is deactivated, and the VM adapter does not receive any more frames until the effective MAC address matches the initial MAC address. The guest operating system does not detect that the MAC address change request was not honored. For more information, see MAC Address Changes.

Port mirroring, known as span ports, is turned off in vSphere by default. You can turn it on by creating a port mirroring session. For more information, see Working with Port Mirroring.

VMware recommends that you do not turn on port mirroring. If you turn it on, for example, to meet a compliance request or a monitoring requirement, ensure that distributed virtual switch port mirror traffic is sent only to authorized collector ports or VLANs.

A vSphere Distributed Switch can mirror the traffic from one port to another to allow the packet capture devices collect specific traffic flows. This mirrored traffic captures the entire data in the packets, resulting in total compromise of that data if misdirected. If port mirroring is required, verify that all port mirror destination VLAN, port, and uplink IDs are correct. For more information, see General Networking Security Recommendations.

Encrypting data at rest

VMware vSphere and vSAN store data at rest to prevent data exfiltration. VMware vSphere uses the ESXi hypervisor to perform encryption without modifying the VM. The security architecture of ESXi achieves this goal at the hypervisor layer to yield the following benefits:

- **No modification to VM operating systems**: No changes to existing applications are required. A common method of encryption is provided across any operating system supported by vSphere.
- **No specialized hardware or infrastructure is required**: Encryption works with existing storage devices and storage fabrics.
- **Policy-based enforcement**: vSphere SDK and tools such as VMware vSphere® PowerCLI™ supports policy-based enforcement, providing easy integration into current and future provisioning solutions.

Because all VM files that contain sensitive information are encrypted, the entire VM is protected. Only administrators with encryption privileges can perform encryption and decryption tasks.

The following types of files can be encrypted:

- VM files
- Virtual disk files
- Host core dump files

Encryption is a storage policy that is applied to a VM. After the policy is applied, the VM is automatically encrypted. The encryption policy can be applied on the Storage Policy screens in the vSphere Web Client or programmatically through the vSphere Storage APIs or vSphere PowerCLI. These encryption operations can be performed across many VMs simultaneously, regardless of the type of operating system.

Because of this policy-based enforcement, automation of VM encryption is simple, and it is easy to integrate with an overall provisioning workflow.

With VM encryption, there is assurance of the device doing the encryption, in this case the ESXi hypervisor. This assurance is accomplished in vSphere by enabling Secure Boot on the ESXi host to ensure that only digitally signed code is run.

The following types of keys are used for VM encryption:

- **Data Encryption Key (DEK)**: The ESXi host generates and uses internal keys to encrypt VMs and disks. These XTS-AES-256 keys are used as DEKs.
- **Key Encryption Key (KEK)**: The vCenter Server instance requests AES-256 keys from the KMS. vCenter Server stores only the ID of each KEK but not the key itself.

When an ESXi host requires a key, the vCenter Server system transfers VM KEKs to the host. The ESXi host encrypts the DEK using the KEK and stores the encrypted internal key on disk. The ESXi host does not store the KEK on disk. If an ESXi host reboots, the vCenter Server instance requests the KEK with the corresponding ID from the external KMS and makes it available to the host. The ESXi host can then decrypt the DEKs as needed.

Similarly, vSAN can perform data-at-rest encryption to protect data in a vSAN cluster.

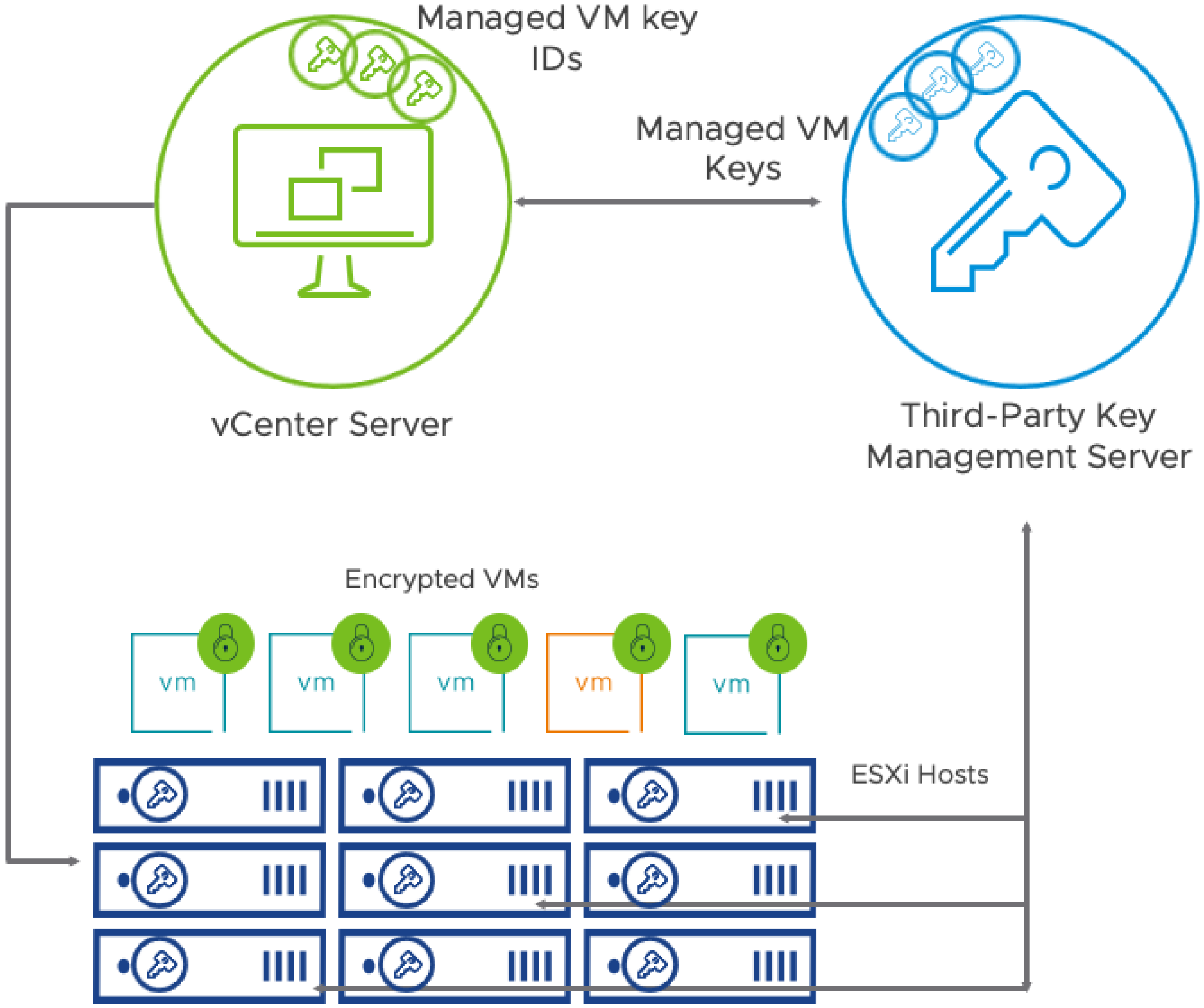
When the vSAN encryption is turned on, all files are encrypted, protecting VMs and their data. Only administrators with encryption privileges can perform encryption and decryption tasks. Data is encrypted after all other processing such as deduplication is performed. Data-at-rest encryption protects data on storage devices in case a storage device is removed from the cluster.

vCenter Server requests encryption keys from an external KMS. The KMS generates and stores the keys, and vCenter Server obtains the key IDs from the KMS and distributes them to the ESXi hosts. vCenter Server does not store the KMS keys, but keeps a list of key IDs.

To summarize vSAN uses encryption keys as follows:

- vCenter Server requests an AES-256 Key Encryption Key (KEK) from an external KMS. vCenter Server stores only the ID of the KEK, but not the key itself.
- The ESXi host encrypts disk data using the industry standard AES-256 XTS mode. Each disk has a different randomly generated Data Encryption Key (DEK).
- Each ESXi host uses the KEK to encrypt its DEKs and stores the encrypted DEKs on disk. The host does not store the KEK on disk. If a host reboots, it requests the KEK with the corresponding ID from the KMS. The host can then decrypt its DEKs as needed.
- A host key is used to encrypt core dumps, not data. All hosts in the same cluster use the same host key. When collecting support bundles, a random key is generated to re-encrypt the core dumps. You can specify a password to encrypt the random key.

For more information, see Using Encryption on a vSAN Cluster.



The technical and operational mechanism of data encryption in the virtualization fabric might vary with the version of vSphere or vSAN and other VMware technology that is in use. For more information, see VMware vSphere Virtual Machine Encryption.

With vSphere, VMware has built one of the most secure and robust virtualization platforms. Encryption is now available through software policies that are independent of the operating system and applications, while maintaining operational efficiencies inherent to vSphere and preserving the security of VMs.

Encrypting data in transit

The ESXi host manages several aspects of the encryption workflow, including encrypting data in transit by using VMcrypt:

- Performs the encryption of VM disks
- Ensures that the guest data for encrypted VMs is not sent over the network without encryption.

Encryption is performed using the industry-standard OpenSSL libraries and algorithms described in VMware vSphere Virtual Machine Encryption. VM encryption does not require new hardware, but a processor that supports the AES-NI instruction set is required to accelerate the encryption and decryption operations.

Because of the processing cost involved in encryption, using both vSAN datastore encryption and VMcrypt might impair performance for some use cases. You might have to evaluate the performance trade-off of encryption in relation to the security context, the type of data, your hardware, compliance regulations, and other requirements. For more information, see Understanding vSAN Datastore Encryption versus VMcrypt Encryption.

Blocking access to the underlying hardware

By default, VMs are configured to block direct access to the underlying physical hardware. Hence, hackers cannot find a security vulnerability in a VM and run code directly on the physical hardware. You must tightly control privileged access to the ESXi host by using the principles of separation of duties and least privilege.

Emerging security standards rely on segmentation at various levels, including the separation of the management network from the data network. Installing appropriate hardware with sufficient physical ports provides the flexibility to separate traffic in the management and data planes. The hardware without sufficient physical ports can lead to problems in managing API management traffic and separating management functions by security level.

For example, if an application is granted permission to access the vSphere API at a highly privileged level, it creates an attack vector exposing access to the underlying hardware. By applying the principles of least privilege and separation of duties, you can ensure that all systems, applications, and users have the appropriate level of access to the virtual infrastructure. With vSphere and a VIM from VMware, you can use role-based access control to tightly control privileged access in a multi-tenant environment.

The following examples illustrate the importance of tightly controlling privileged access to the virtualization plane:

- To maximize the use of hardware resources, some telco operators use an element manager to gauge the load of the underlying hardware in a vSphere environment. However, this approach can expose a vector through which an attacker could gain access to the hardware.
- For API-based hardware-level management through the Common Information Model (CIM) interface, root credentials must not be used to access the Input–Output Memory Management Unit (IOMMU) interface. Instead, create a less-privileged vSphere user account for these applications and use the VIM API ticket function to generate a sessionId or ticket to this less-privileged user account for authenticating to the CIM.

VMware writes CIM providers that monitor server hardware, ESXi storage infrastructure, and virtualization-specific resources. These lightweight providers run within the ESXi host.

To ensure that the CIM interface is secure, provide only the minimum access necessary to these remote applications. If you provision a remote application with a root or administrator account and the application is compromised, the virtual environment might also be compromised. For more information, see Control Access for CIM-Based Hardware Monitoring Tools.

Establishing Trust Domains and Segregation

To reduce the risk of a breach spreading from a compromised host to other hosts, virtualized infrastructure is critical for segregating workloads into trusted domains. Set up the management plane components such as a VIM and VMware Telco Cloud Automation in a trusted location that is segmented from the rest of the virtualization fabric. By establishing the management plane in a separate domain from the virtualization plane, you can protect it further with firewalls, micro-segmentation, and other techniques.

Placing hypervisors in a security pool and tagging workloads with a trust domain

NSX distributes network and security services to the hypervisor, enabling a new level of control and operational agility. Thus, a network security team can prevent threats from moving laterally within an environment by, for example, creating security groups that include dynamic membership criteria defined by security tags. Security groups can also be governed by a security policy. For more information, see Configuring Security Policy.

NSX security groups, tags, policies, and other capabilities can isolate virtual workloads in trust domains by their risk and sensitivity levels. For example, such a trust domain lets you place sensitive functions in one host pool and vulnerable functions in another host pool, thereby limiting the attack surface.

Enforcing separation between trust domains

Most processors from Intel and AMD include the following features to assist virtualization and improve performance:

- Hardware-assisted CPU virtualization
- MMU virtualization
- I/O MMU virtualization

Hardware-assisted CPU virtualization assistance is called VT-x in Intel processors and AMD-V in AMD processors. It automatically traps sensitive events and instructions in the VMware virtualization fabric, allowing trap-and-emulate style virtualization and reducing the overhead in managing these traps.

Hardware-assisted I/O MMU virtualization is called Intel Virtualization Technology for Directed I/O (VT-d) in Intel processors and AMD I/O Virtualization (AMD-Vi or IOMMU) in AMD processors. Hardware-assisted I/O MMU virtualization is an I/O memory management feature that remaps I/O DMA transfers and device interrupts. In the VMware virtualization fabric, this feature is a function of the chipset instead of the CPU. This feature enables VMs to have direct access to hardware I/O devices such as network cards, storage controllers (HBAs), and GPUs. IOMMU maps virtual addresses to physical addresses. For more information, see Performance Best Practices for VMware vSphere.

Eliminating cross-host impacts

SpoofGuard prevents spoofing on an NSX logical switch. Using SpoofGuard, you can authorize the IP addresses reported by VMware Tools or IP discovery. For more information, see Prevent Spoofing on a Logical Switch and Using SpoofGuard.

Running containers on VMs to enforce trust domains with hypervisors

Containers alone are inadequate security boundaries. A compromised workload on a container can compromise the host operating system and all other workloads running on that host operating system.

The NIST Application Container Security Guide, also known as NIST Special Publication 800-190, says containers “do not offer as clear and concrete of a security boundary as a VM. Because containers share the same kernel and can be run with varying capabilities and privileges on a host, the degree of segmentation between them is far less than that provided to VMs by a hypervisor.”

To establish a strong security barrier for containers, VMware runs containers on VMs. By running containers on VMs, you can leverage security innovations in virtualization technology. The Secure Encrypted Virtualization (SEV) technology integrates memory encryption with AMD-V virtualization to support encrypted VMs, which are ideal for multi-tenant environments.

SEV with Encrypted State (SEV-ES) reduces the attack surface and provides increased protection for a guest VM from the hypervisor even if the hypervisor is compromised. When a VM stops running to prevent information leakage from CPU registers to the hypervisor, SEV-ES blocks attacks by encrypting and protecting all CPU register contents. SEV-ES can detect and prevent malicious modifications to the CPU register state.

For more information, see CNFs on Virtual Machines or Bare Metal, Securing, Managing, and Optimizing CNFs and 5G Services at Scale.

VMware supplies technology such as Kubernetes and VIM that can manage containerized services programmatically at scale.

Protecting the Management of the Virtualization Plane

5

The management plane protection is focused on three primary areas: management plane architecture, its administration network, and the administrator access and privileges. Architecting a secure management plane provides the foundation for isolating management elements, including the administrative network, from other aspects of the virtual infrastructure and for controlling and monitoring administrative access successfully.

To architect the management plane, operators can use several inter-related, interoperable solutions from VMware to manage the virtualized and containerized infrastructure and also to apply security measures in the management plane:

- VMware Telco Cloud Automation
- VMware Cloud Director or VMware Integrated OpenStack
- VMware Telco Cloud Infrastructure and VMware NSX
- VMware vSphere

In addition, VMware infrastructure integrates with Kubernetes and other cloud native technology to manage cloud native functions and cloud network functions. For example, VMware Telco Cloud Automation can securely deploy and orchestrate cloud native workloads on Kubernetes.

Read the following topics next:

- Architecture of the Management Plane
- Protecting the Administration Network
- Separating Administration from the Virtualization Fabric
- Protecting Virtualization of Security-Critical Functions
- Managing Security-Critical Functions in Isolation
- Securing Access to the Management Plane
- Automating Administration
- Blocking Non-Management Devices from the Management Plane
- Administering the Virtualization Fabric with Emergency Access

Architecture of the Management Plane

The management plane architecture establishes a trusted foundation for isolating management functions from the rest of the Operator's network. When the management plane is architected to enhance security, it is segmented into discrete zones, prevents movement across the plane, and restricts access to and exfiltration of network data. Management functions are critical security functions that require additional security controls. Operators must scan the management network to detect anomalies in configurations and operations.

With the VMware telco stack, you can manage the higher-level virtualization fabric through VMware Telco Cloud Automation (a central orchestration tool) that is integrated with VMware Telco Cloud Infrastructure. You can manage lower-level aspects of the management plane using a VIM from VMware and the management interface for vSphere.

VMware architectures for CSPs isolate the management plane. The components and resources of the management plane, including vCenter Server and NSX Manager, are isolated from the virtualization plane. vCenter Server provides the infrastructure for fine-grained allocation and partitioning of compute and storage resources.

VMware Telco Cloud Infrastructure also provides abstraction layers for multi-tenancy. The concept of tenancy introduces shared administrative ownerships. A CSP administrator can allocate a resource pool and overlay networking for a tenant. With a VIM from VMware, multiple tenants can be defined with assigned RBAC privileges to manage resources and VNF onboarding.

The networking model of NSX isolates traffic paths across workloads and the tenant switching and routing fabric. Advanced security policies and rules can be applied at the VM boundary to further control access to the management plane. NSX Data Center uses a two-tiered routing architecture that manages networks at the provider (Tier-0) and tenant (Tier-1) tiers. The provider routing tier is attached to the physical network for north-south traffic, while the tenant routing can connect to the provider Tier-0 and manage east-west communications.

Tier-0 provides traffic termination to the cloud physical gateways and existing CSP underlay networks for inter-cloud traffic communication. Each organization in a virtual data center have a single Tier-1 distributed router that provides intra-tenant routing capabilities. The router can also deliver stateful services such as firewall and NAT. VMs belonging to a tenant can be connected to multiple logical interfaces for layer 2 and layer 3 connectivity.

By using these and other constructs of NSX such as firewalls, micro-segmentation, and VLANs, you can segregate the management plane by device type and function. For example, VNF element managers can be separated with micro-segmentation and blocked from communicating with one another and with elements that they do not manage to prevent man-in-the-middle attacks.

VMware provides a reference architecture for building, isolating, and protecting the management plane. For more information, see the management pod and three-pod deployment sections in the VMware Telco Cloud Reference Architecture Guide.

Protecting the Administration Network

VMware provides two key interfaces that form a management plane to administer the virtualization fabric and VNFs: a VIM from VMware and VMware Telco Cloud Automation. Both use secure, encrypted channels to administer VMs, VNFs, and the ESXi hypervisor.

Telco Cloud Automation connects to the VIM over a secure channel so that you can manage the telco virtualization fabric and its network functions from a single location. Telco Cloud Automation and the VIM control access with authentication and multitenant role-based access control. The VIM securely integrates with vSphere, NSX, and vSAN to establish a single management plane for the virtualization fabric.

In addition to the virtualization layer, protecting the administration network require appropriate hardware with sufficient physical ports to separate the administration network traffic from other network traffic and to segment traffic by sensitivity levels at the physical layer.

Separating Administration from the Virtualization Fabric

The management functions that support the administration and security of the virtualization fabric are security-critical functions. These functions must be separated from the rest of the virtualization fabric, protected with strong security measures, and closely monitored.

VMware Telco Cloud Infrastructure™ - Cloud Director™ Edition Reference Architecture includes a three-pod design that separates the functional blocks by using a management pod, edge pod, and resource pod. The initial deployment of a three-pod design consists of three vSphere clusters, with one cluster for each pod. Clusters can be scaled up by adding ESXi hosts, and pods can be scaled up by adding clusters.

The separation of management, edge, and resource functions in individually scalable pods lets you plan capacity by function. This strategy promotes operational flexibility and scalability while separating the management functions from the virtualization fabric.

The management pod hosts all the NFV management components. Its functions include resource orchestration, analytics, business continuity and disaster recovery, third-party management, and NFV operations.

For more information about separating administration from the virtualization fabric, see the Telco Cloud Reference Architecture Guide.

Protecting Virtualization of Security-Critical Functions

The NCSC’s findings on telecom security emphasize the protection of security-critical functions. Security-critical functions include orchestration systems for virtualization, management systems such as jump boxes, firewalls protecting a security zone, directory services such as Active Directory used for authentication and access control, IPSec security gateways, and monitoring and auditing systems.

Because of the importance of the virtualization plane to telecom networks, the management and orchestration of those networks requires additional security. These management functions are security-critical functions by the NCSC and they must be secured by the following:

- Two-factor authentication
- Role-based access control that uses the principles of separation of duties and least privilege

The NCSC summary says “Operators use security-critical functions to enforce security controls in their networks and mitigate risk. As risks are mitigated, the options available to attackers are reduced, and the security-critical functions become the primary focus of attack. The Telecoms Security Requirements (TSRs) define additional controls for security-critical functions to ensure that they are resilient to targeted attacks from determined attackers.”

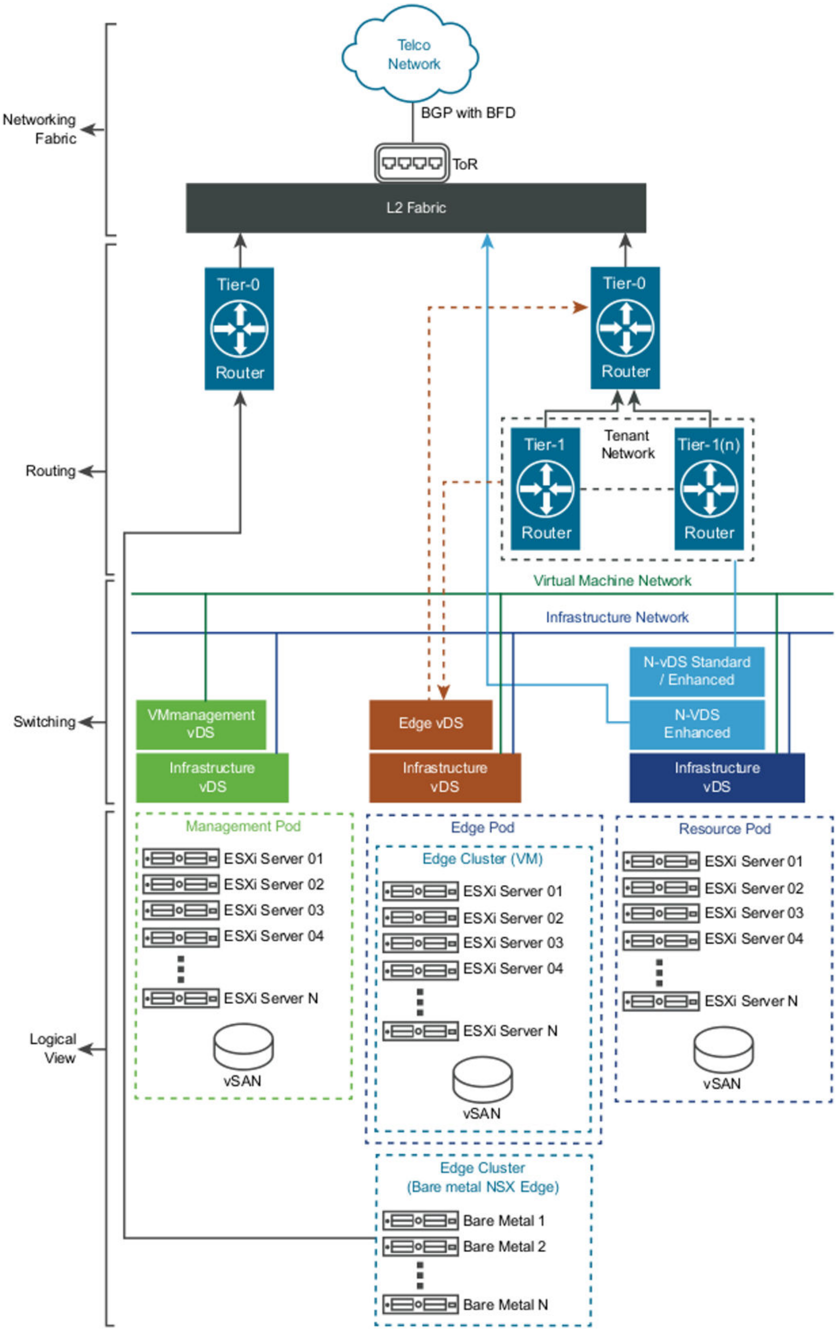
To limit the attack surface of security-critical functions and reduce risk, segregate security-critical functions in the virtualization fabric by using micro-segmentation with NSX. Micro-segmentation isolates security functions in their own trust domains.

In addition to virtualization, protecting security-critical functions also requires appropriate hardware with disks that can be encrypted and sufficient physical ports to separate traffic by type or sensitivity level.

Managing Security-Critical Functions in Isolation

The management and orchestration systems for the virtualization fabric must be isolated from other networks and closely monitored to track access and changes. Security-critical functions can be separated by using a separate vSphere cluster of the ESXi hypervisor and VMs. NSX isolates security-critical functions further by implementing firewalls and applying micro-segmentation.

The following diagram depicts the physical representation of the compute and networking connectivity and the logical layers of the switching and routing fabric. This flexible, scalable three-pod design uses a management pod to separate administration from the virtualization fabric.



Containers alone are an inadequate security boundary. Do not use containers to separate different security-critical functions or to separate security-critical functions from other workloads or functions.

VMware components of the management plane, such as vSphere and vCenter, authenticate and authorize users with Microsoft Active Directory or LDAP. These security systems are security-critical functions. A system such as Active Directory must be installed and isolated in its own trusted security domain, not the corporate domain, for the sole purpose of identity management and Kerberos authentication for the management plane. A system that provides multi-factor authentication for the management plane is also a security-critical function. It must also be isolated in its own local, trusted security domain and not the corporate security domain.

As for the monitoring of security-critical functions, VMware Aria Operations for Logs can ingest syslog messages. VMware Aria Operations for Logs includes a built-in syslog server that is active when the VMware Aria Operations for Logs service is running. The syslog server listens on ports 514/TCP, 1514/TCP, and 514/UDP. It ingests log messages sent from other hosts. Ingested messages become searchable in VMware Aria Operations for Logs in near real time to help monitor security-critical functions. For more information, see **VMware Aria Operations for Logs** as Syslog Server.

To protect sensitive information gathered by VMware Aria Operations for Logs, place the server on a management network segment that is protected by a firewall from the rest of the internal network. For more information, see **VMware Aria Operations for Logs** Firewall Recommendations. Security controls can safeguard VMware Aria Operations for Logs. For more information, see Security Considerations for **VMware Aria Operations for Logs**.

Securing Access to the Management Plane

The NCSC outlines several principles for securing user access to the management plane. Operators must tightly control access to the management plane by using the principles of least privilege and separation of duties. Each user must be authenticated with multi-factor authentication (MFA).

With a VIM from VMware, you can establish strict role-based access control for administrators in a multi-tenant context, limiting administrators to only the access required to fulfill their duties. As a best practice, block virtualization administrators from accessing workloads running in the virtualized environment.

The security of the orchestration system is important. VMware Telco Cloud Automation is secured with role-based access control to limit access to NFVO, VNFM, VNF Designer, and the API. Other components of the VMware management plane, such as vSphere and vCenter, can authenticate and authorize users with Microsoft Active Directory or LDAP. Multi-factor authentication can be added for ESXi, vCenter, and Cloud Director. For more information, see Understanding vCenter Server Two-Factor Authentication and Configuring Smart Card Authentication for ESXi.

Automating Administration

VMware NSX automates the provisioning and administration of virtualized infrastructure. The NSX API enables you to use an automated process to build the virtualization fabric with authorized API calls. For more information, see Network Automation.

Blocking Non-Management Devices from the Management Plane

Some telecommunication networks neglected to maintain a boundary between the management plane and other planes, allowing non-management devices to access the management plane. To minimize the attack surface, you must prevent the devices outside the management plane and the devices without a management function from accessing the management network.

NSX uses distributed firewalls, micro-segmentation, and security policies to segregate the management plane and block access by non-management devices.

In addition, VMware Cloud Director manages access and cloud administration rights with Active Directory. By using VMware Cloud Director with Active Directory, you can allow only specific workstations with privileged access to connect to the management plane.

Administering the Virtualization Fabric with Emergency Access

vSphere includes an Exception User list. Exception users do not lose their privileges when the host enters lockdown mode. Use the Exception User list to add the account of a third-party management solution that needs to access the host directly when the host is in lockdown mode. For more information, see Lockdown Mode.

You can specify service accounts that can access the ESXi host directly by adding them to the Exception Users list. A single user can be specified to access the ESXi host in a catastrophic vCenter Server failure. For more information, see Specifying Accounts with Access Privileges in Lockdown Mode.

vSphere 6.0 and later supports the Exception User list for service accounts that must log in to the host directly. Accounts with administrator privileges can log in to the ESXi Shell. In addition, those users can log in to a host's Direct Console User Interface (DCUI) in normal lockdown mode and exit lockdown mode. Exception users are host local users or Active Directory users with privileges defined locally for the ESXi host. Users that are members of an Active Directory group lose their permissions when the host is in lockdown mode.

Implementing Monitoring and Auditing for Security

6

VMware Telco Cloud Infrastructure can be integrated with an operations management suite for monitoring and remediation of the NFVI and VNFs. Some of the key capabilities are as follows:

- **Dynamic resource discovery**: Distributed and complex topologies require dynamic resource and service discovery. It provides continuous visibility over service provisioning, workload migrations, auto-scaling, elastic networking, and network-sliced multi-tenancy that spans VNFs, hosts, clusters, and sites.
- **SLA management**: Alerts can flag configuration and compliance gaps and security vulnerabilities.
- **Remediation**: Reduced MTTU and timely issue isolation for improved service reliability and availability. Prioritized alerting, recommendations, and advanced log searching enable the isolation of service issues across physical and overlay networks.
- **Security and policy controls**: Multi-vendor services operating in a shared resource pool can create security risks within the virtual environment. The management suite can recommend security rules and policies for traffic by profiling and monitoring traffic segments, types, and destinations. It can also identify violations of security policies or vulnerable configurations, performance impacts, and traffic routes.

The analytical data can also be queried and triggered by third-party components such as existing assurance engines, NMS, EMS, OSS/BSS, and VNF-M and NFV-O for closed-loop remediation.

You can deploy the operations management components in the management plane and centralize them across the cloud topology. VMware Aria suite of products including Aria Operations, Aria Operations for Logs, and Aria Operations for Networks are the main components. VMware Telco Cloud Service Assurance is an additional component.

The following sections describe how these components meet the emerging telco security requirements.

Analyzing network data, topologies, and traffic

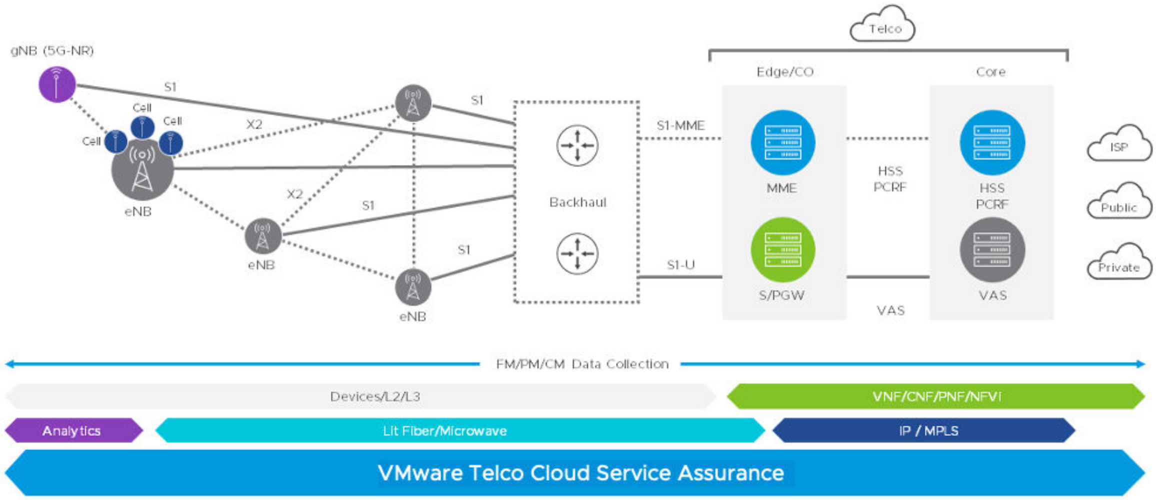
The following components together provide a secure system for the analysis of network data, topologies, routes, and traffic:

- **Aria Operations**: Collects compute, storage, and networking data to provide performance and fault visibility over hosts, hypervisors, VMs, clusters, and sites.
- **Aria Operations for Logs**: Captures unstructured data from the environment to provide log analysis and analytics. Logs and events of the Telco platform component are ingested, tokenized, and mined for intelligence.
- **Aria Operations for Networks**: Provides layer 2, 3, and 4 visibility into the virtual and physical networks. It helps identify network anomalies and security policy gaps. The Aria Operations for Networks engine is integrated with the NFVI networking fabric to capture device and network configurations, IPFIX flow, and SNMP. Aria Operations for Networks provides visibility into traffic routing, sources and destinations, micro-segmentation, and security violations.
- **VMware Telco Cloud Service Assurance**:Provide a holistic service assurance solution that allows Communications Service Providers (CSPs) and large enterprises to monitor and manage both the traditional physical infrastructure and new virtual and containerized network services together. The micro-services architecture enables flexibility and scale in VMware Telco Cloud Service Assurance. Telco Cloud Service Assurance provides end-to-end service assurance capabilities across multiple domains including the Network underlay, the virtualized infrastructure and service level monitoring of the 5G Core and RAN applications VMware Telco Cloud Service Assurance provides an automated approach to operational intelligence to reduce operational expenses, increase uptime, meet SLAs, and operationalize new services faster. It automatically discovers the topology of a complex, multivendor network including the physical, virtual, and services layers, and presents the user with a comprehensive, graphical topology view.

Assessing compliance with line-item security requirements

VMware Aria Operations for Networks works with NSX Data Center to assess compliance with telecommunication security requirements for the virtualization plane and its management. For example, VMware Aria Operations displays routing information for multi-tenancy and micro-segmentation, shows firewall rules and logical routers, and describes IPFIX flows.

The following diagram illustrates how VMware Telco Cloud Service Assurance monitors the layers of a 5G network to protect availability, integrity, and confidentiality.



Proactively identifying anomalies

VMware Aria Operations provides layer 2, layer 3, and layer 4 visibility into the virtual and physical networks, and it helps identify network anomalies and security policy gaps. The VMware Aria Operations for Networks engine is integrated with the NFVI networking fabric to capture device and network configurations, IPFIX flow, and SNMP. VMware Aria Operations for Networks provides visibility into traffic routing, sources and destinations, micro-segmentation, and possible security violations.

Telco Cloud Service Assurance monitors all layers of the telco stack, both physical and virtual, for rapid insights into issues through its root-cause analysis engine. To investigate an anomaly, the host-based configurations and asset management information from Telco Cloud Service Assurance are manually correlated with logging data from VMware Aria Operations for Networks.

VMware Aria Operations for Networks and Telco Cloud Service Assurance together help monitor interfaces between networks operating at different trust or sensitivity levels and detect any traffic anomalies.

Detecting unexpected changes to network equipment

Telco Cloud Service Assurance performs host-based configuration management and monitoring to detect unexpected or unauthorized changes to network equipment and its settings. If a firmware or software is outdated, Telco Cloud Service Assurance triggers an alert and initiates automated updates if it is configured. If a physical change adversely affects the network, Telco Cloud Service Assurance shows the root cause of the problem and triggers service workflows through integrated OSS tools such as ServiceNow.

Protecting the Signaling Plane

7

A key risk in the signaling plane is receiving malicious data. After virtualizing the core network using VMware technology, segregate the core network based on its services, such as network slicing with 5G, by using VMware NSX.

Protecting the signaling plane using network slicing with 5G in conjunction with NSX involves implementing various security measures. These security measures ensure the integrity and reliability of the signaling messages.

Some of the security measures are as follows:

- **Network Slicing**: Use the network slicing capabilities of 5G to logically isolate and dedicate a specific portion of the network for signaling traffic. Hence, the signaling plane has dedicated resources and is not impacted by data plane activities.
- **Traffic Segmentation**: Implement traffic segmentation to isolate signaling traffic from user data traffic. NSX creates separate logical networks, ensuring that signaling messages traverse only the designated path.
- **Micro-Segmentation**: Apply micro-segmentation techniques to partition the signaling plane further into small security zones. This reduces the attack surface and prevents lateral movement of threats.
- **Firewalls and Access Control Lists (ACLs)**: Deploy firewalls and ACLs at strategic points within the signaling plane to filter and permit only authorized signaling traffic. NSX provides distributed firewall capabilities to enforce security policies at the virtual machine (VM) level.
- **Intrusion Detection and Prevention Systems (IDPS)**: Integrate IDPS solutions into the signaling plane to detect and prevent potential attacks or anomalies in real-time.
- **Encryption**: Implement end-to-end encryption for signaling messages to prevent unauthorized access or tampering. NSX facilitates encrypted communication between VMs.
- **Network Function Virtualization (NFV)**: Use NFV to virtualize network functions, including signaling-related elements. This enables flexibility and scalability while maintaining security.
- **Network Access Control (NAC)**: Enforce NAC policies to ensure that only authenticated and authorized devices can access the signaling plane.
- **Security Monitoring and Analytics**: Use advanced security monitoring and analytics tools to detect and respond to potential security incidents promptly.
- **Role-Based Access Control (RBAC)**: Implement RBAC mechanisms to control and restrict access to critical components within the signaling plane. Hence, only authorized personnel can make changes or access sensitive data.

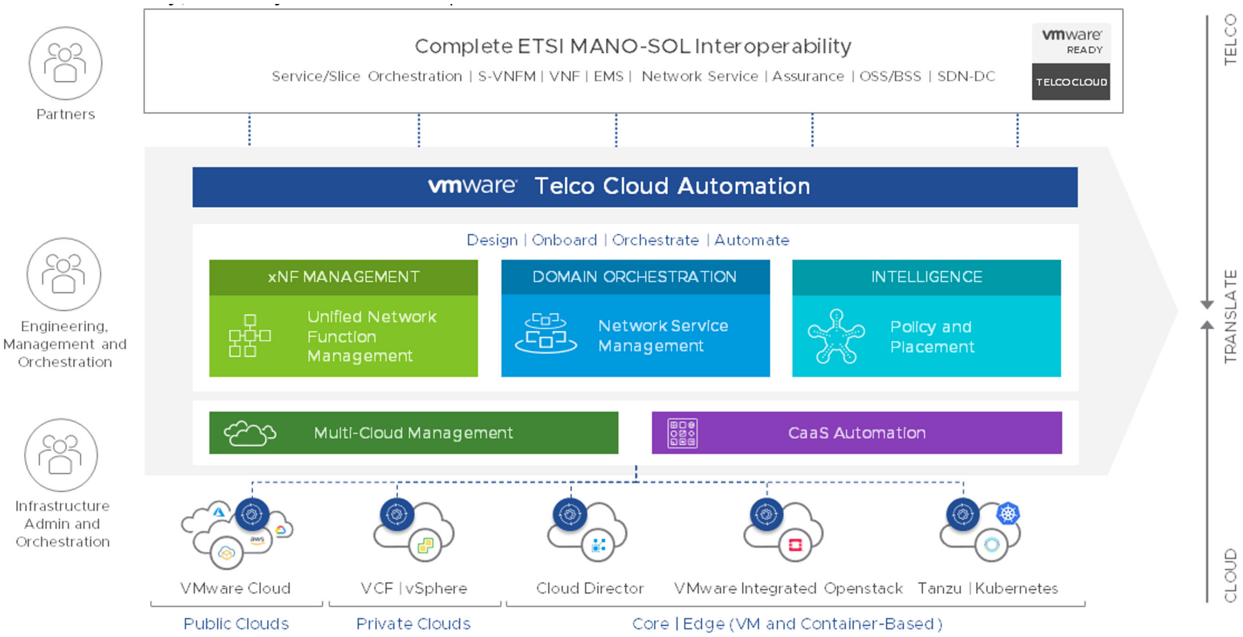
Note Implementation of these security measures depends on the 5G infrastructure, NSX features, and the overall security requirements of the network. Regular updates and patches to all software and network elements are also crucial to maintaining a secure signaling plane.

Cloud Native Approaches to Core Network Security

8

The primary areas for a secure cloud native environment are infrastructure, clusters, development, and workloads. With complex telco networks moving toward 5G and cloud network functions, automation and orchestration are required to optimize network security and achieve network transformation.

VMware Telco Cloud Automation provides orchestration and automation to secure telco network services and functions, including CNFs and Kubernetes. The platform’s orchestration tool automates several operational procedures to avoid configuration mistakes.


Partners
Complete ETSI MANO-SOL Interoperability
Service/Slice Orchestration | S-VNFM | VNF | EMS | Network Service | Assurance | OSS/BSS | SDN-DC
vmware READY
TELCOCLOUD
Engineering, Management and Orchestration
vmware Telco Cloud Automation
Design | Onboard | Orchestrate | Automate
xNF MANAGEMENT
Unified Network Function Management
DOMAIN ORCHESTRATION
Network Service Management
INTELLIGENCE
Policy and Placement
Multi-Cloud Management
CaaS Automation
Infrastructure Admin and Orchestration
VMware Cloud
VCF | vSphere
Cloud Director
VMware Integrated Openstack
Tanzu | Kubernetes
Public Clouds
Private Clouds
Core | Edge (VM and Container-Based)
TELCO
TRANSLATE
CLOUD

Securely orchestrating containerized applications

The Center for Internet Security (CIS) is a non-profit organization that relies on the IT community to safeguard private and public organizations against cyber threats. To set up Kubernetes clusters with a secure configuration, analyze their security posture using the CIS Kubernetes Benchmark.

Checklist of countermeasures for cloud native security

If you are implementing cloud native network functions or introducing containers and Kubernetes into your telco stack, apply the following list of countermeasures to the cloud native components. These countermeasures ensure that the cloud native technology is protected with fully integrated security.

Note Use this checklist to evaluate whether countermeasures are included in a platform or component by default or whether they must be applied. For more information, see the NIST Application Container Security Guide (NIST Special Publication 800-190).

- Implement container-specific countermeasures
- Integrate countermeasures into the container life cycle and pipeline, from build through the registry and runtime through orchestration
- Monitor containers across their life cycle and stack for full visibility
- Enforce security with policies, especially RBAC and policies for image use
- Use only the latest known, patched, scanned, and signed images
- Run images as non-privileged, immutable containers without SSH
- Manage containers through the orchestration engine, not the container host
- Securely store secrets, encrypted, in the orchestrator, not in the image
- Connect to registries and dashboards over secure, encrypted channels
- Tightly control access to registries, orchestrators, and dashboards with RBAC using principles of least privilege and separation of duties
- Control access to the Kubernetes API
- Federate existing accounts by using a standard directory service and implement single sign-on
- Log, monitor, and audit registry, orchestrator, and dashboard access
- Encrypt data at rest using container-specific methods
- Segment orchestrator network traffic into discrete virtual networks by sensitivity level
- Only mix workloads of the same sensitivity level and threat posture on the same host
- Use a patched, up-to-date runtime
- Limit network access from containers
- Profile and protect apps at runtime to ensure integrity
- Use an up-to-date container-specific minimalist OS to narrow the attack surface
- Set the root file system to read-only
- Limit, log, and audit host OS access to detect anomalies and privileged operations

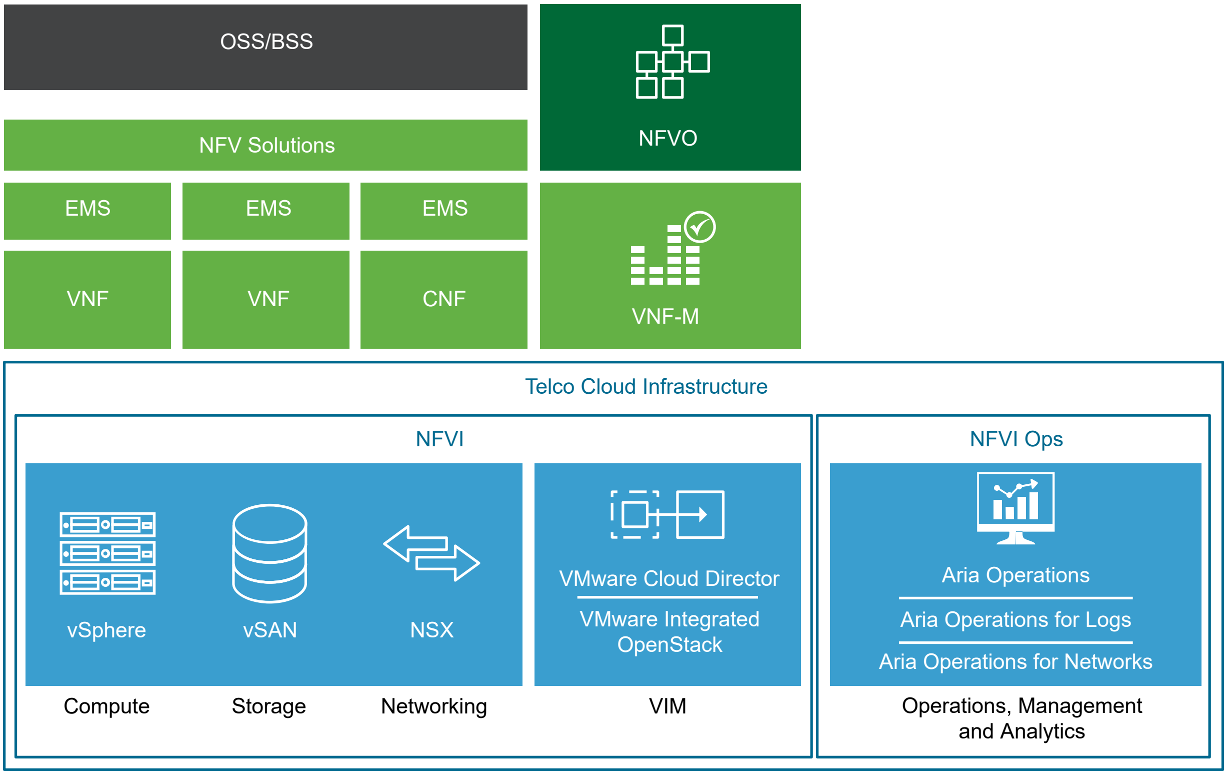
- Limit resource consumption of a container to prevent denial-of-service (DoS) attacks
- Monitor the cluster and network usage
- Monitor for suspicious activity and analyze failed login and RBAC events
- Use the latest versions of Kubernetes, which are more secure than older versions
- Monitor configurations, such as dashboard access, for risks and vulnerabilities
- Perform routine tests for vulnerabilities and attack vectors by using standard tools

Conclusion: Example End-to-End Security Architecture

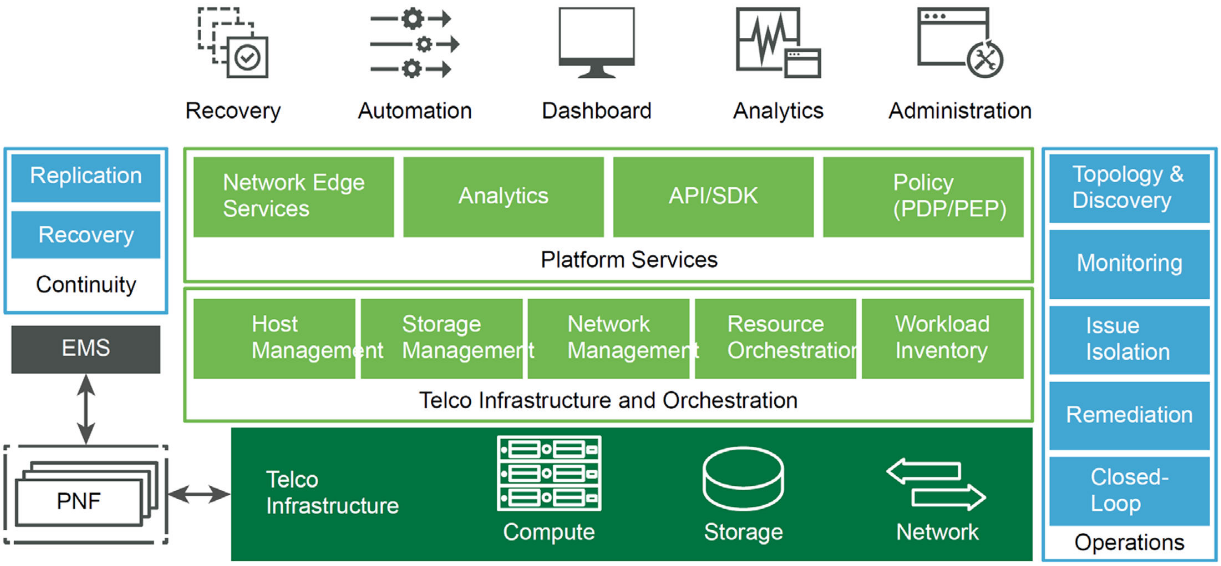
9

This section illustrates how a VMware Telco Cloud architecture can create a multi-tenant quality-of-service NFV platform with intrinsic security built into the virtual infrastructure, its components, and its management so that security is programmable, automated, adaptive, and context-aware.

VMware components can be deployed in several ways to construct a comprehensive solution that meets your security goals. This example uses VMware Telco Cloud Infrastructure OpenStack Edition as the VIM and includes vSphere, vSAN, and NSX. The operational components are Aria Operations, Aria Operations for Logs, and Aria Operations for Networks. You can also use VMware Cloud Director as the VIM instead of OpenStack in a different combination.



In general, the components of Telco Cloud Infrastructure are combined to form an architecture with a core data center and multiple edge domains. This section describes how the components are combined to create a multi-tenant architecture with quality-of-service and end-to-end security.



Read the following topics next:

- Multi-tenant Consumption Models and Security
- Tenancy and Quality of Service
- Authentication and Access Control
- Management Plane
- Compute Isolation
- Network Isolation
- Secure Multi-Tenancy and the VIM
- Embedded Analytics, Monitoring, and Intelligence for Security Assurance
- Intrinsic Security

Multi-tenant Consumption Models and Security

A tenant is a construct for providing appropriate resources for various constructs. A tenant can be a service. A shared resource infrastructure environment can provide an NFV consumption model with secure multi-tenancy. You can create one tenant to run VNFs from one vendor and another tenant to run VNFs from another vendor.

You can facilitate NFV transformation on a shared resource infrastructure environment with multi-tenant consumption models. Multi-tenancy isolates resources and networks to deliver applications with quality for each tenant. Because multiple tenants share the same resource infrastructure, you can enable secure multi-tenancy by using the VIM in a single cloud island and across distributed clouds.

Resource infrastructure can be converged across IT and network clouds by enabling a multi-tenancy IaaS. Consumption models can serve internal and external tenants over the shared infrastructure so tenants can deploy and operate their workloads and services. This results in the network, compute, and storage isolation with quality of service.

Tenancy and Quality of Service

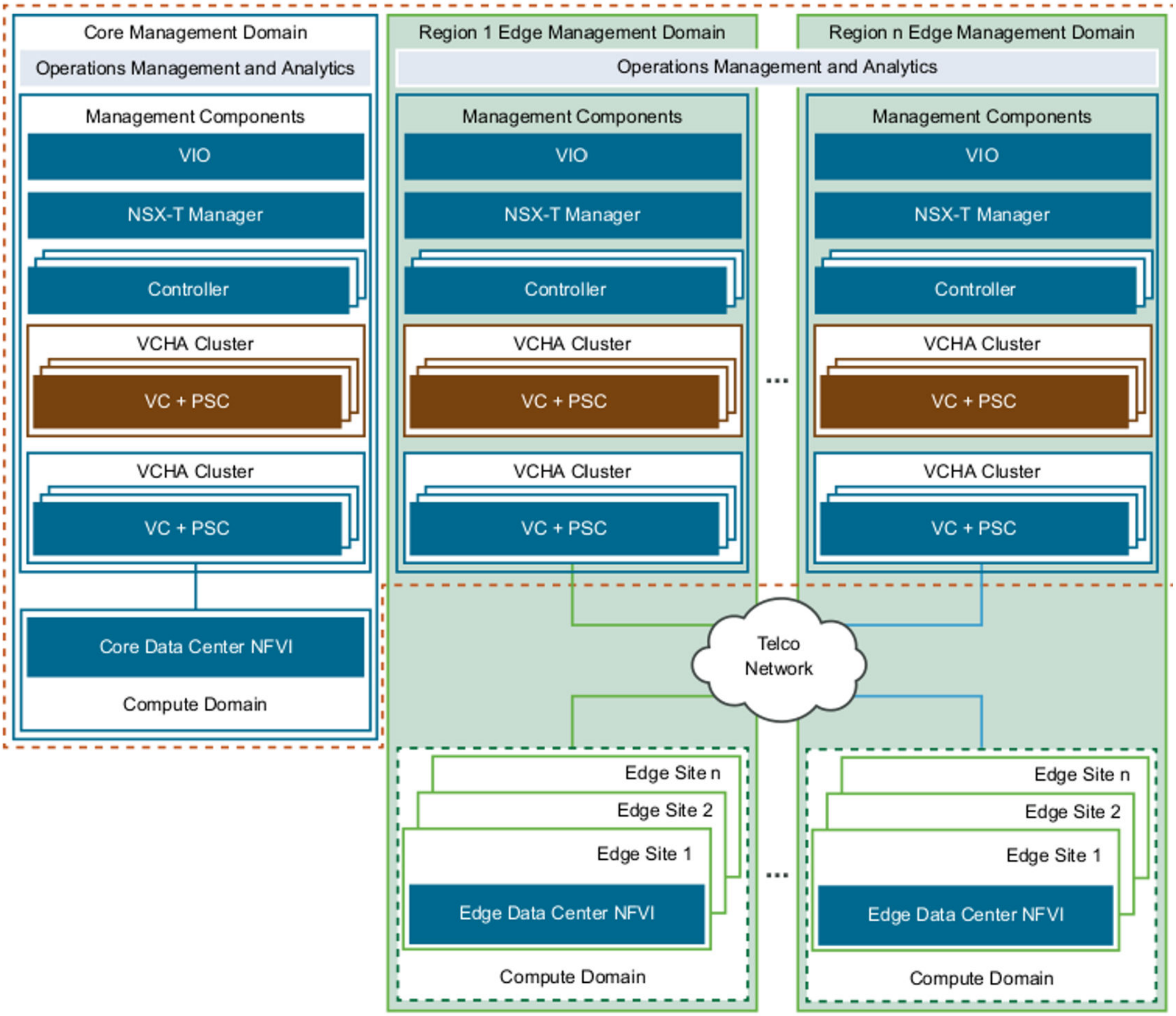
Within VMware vCloud Director, a unit of tenancy is called a tenant virtual data center (vDC) within the scope of a project. It is defined as a composition of dedicated compute, storage, and network resources and as workloads. A tenant vDC allows the creation of virtual data centers for tenants under different compute nodes that offer SLA levels for each telco workload. While quotas on projects set limits on the resources, tenant vDCs let you set resource guarantees for tenants and avoid noisy neighbor scenarios in a multi-tenant environment.

A tenant vDC is a composition of dedicated compute, storage, and network resources and workloads. The tenant is associated with a set of operational policies and SLAs. The tenant vDC can be bound to a single tenant or shared across multiple tenants. Services such as HSS and DNS are examples of shared tenancy. To avoid contention and starvation, compute, storage, and network isolation policies and QoS policies can be applied consistently to the workloads.

To meet the operational policies and SLAs for workloads, closed-loop automation is necessary across the shared cloud infrastructure.

VMware Telco Cloud Infrastructure OpenStack Edition uses vSphere DRS and Nova Scheduler to optimize the initial and runtime placement of workloads and to ensure the health and performance of the infrastructure. Tenant vDCs and workloads are monitored to ensure that the resources are tuned and balanced dynamically.

Platform Services Controller (PCS) manages authentication and access control for administrators and applications that interact with the vSphere platform. PCS works across a telco network with a core management domain and multiple edge domains.



Authentication and Access Control

The vSphere platform includes Platform Services Controller (PSC) that contains common infrastructure security services such as VMware vCenter single sign-on, VMware Certificate Authority, licensing, service registration, and certificate management services. The Platform Services Controller securely connects to LDAP or Microsoft Active Directory for identity management. It performs authentication and access control for administrators and applications that interact with the vSphere platform. You can deploy PCS as a load-balanced pair of appliances for each vCenter Server.

Management Plane

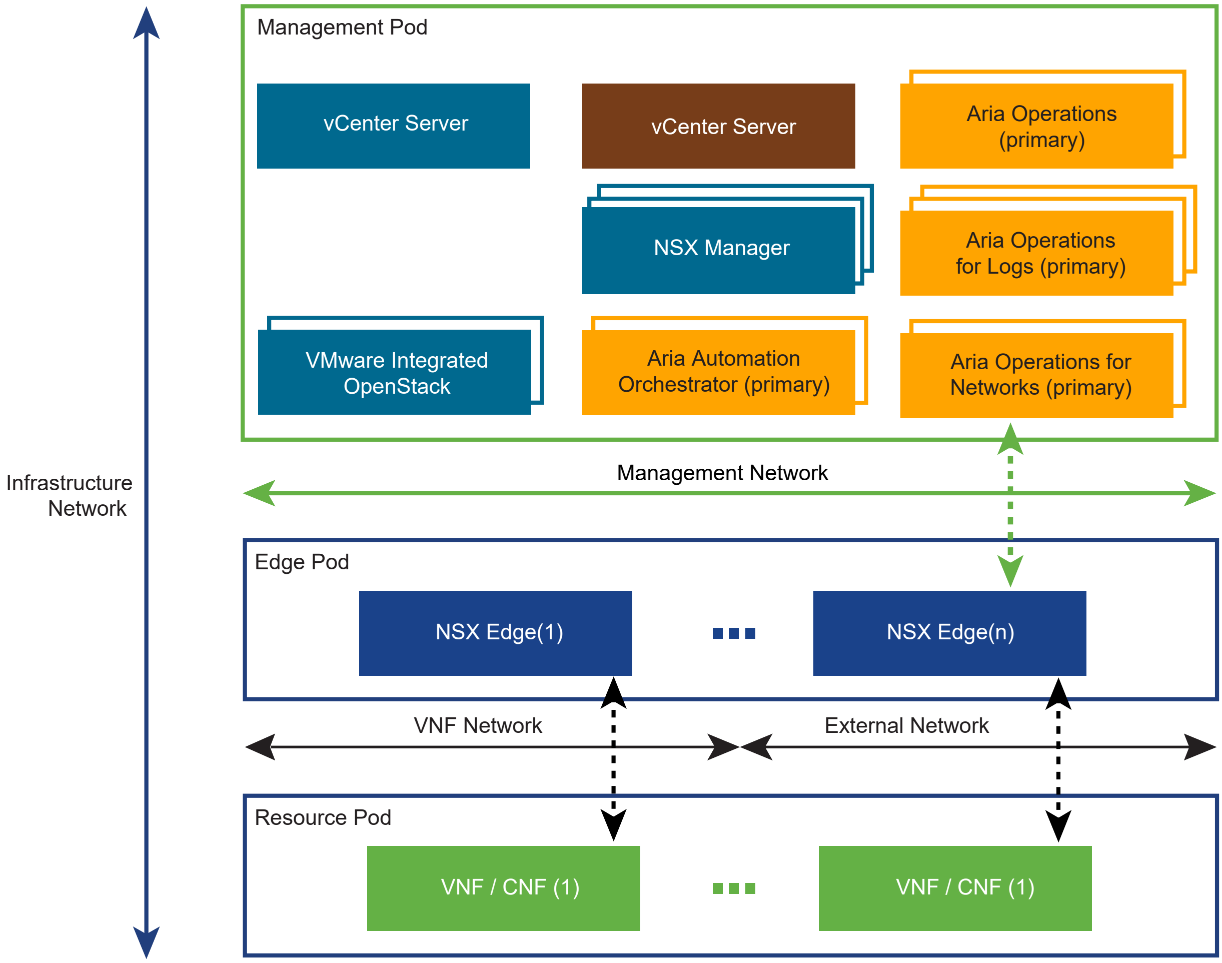
The management plane functions reside in an isolated management pod. These functions orchestrate resources and operations. They are local to each cloud instance to manage the infrastructure, virtual networks, and operations.

Resource isolation for compute and networking design are enabled together with vCenter Server, NSX Manager, and the VIM.

- The VIM provides the abstraction layers for multi-tenancy.
- vCenter Server furnishes the infrastructure for fine-grained allocation and partitioning of compute and storage resources.
- NSX-T Data Center creates the network virtualization layer. The concept of tenancy also introduces multiple administrative ownerships that require RBAC.

A communications service providers (CSP) provider administrator can allocate a resource pool for a tenant. The tenant can then manage the underlying infrastructure and overlay networking. In the VIM, multiple tenants can be defined with RBAC to control access to the compute and network resources and VNF onboarding. RBAC empowers you to implement the principles of least privileges and separation of duties in a hierarchy of tenants.

For security, the management pod and its functions are isolated from other elements of the telecommunication network, including the virtualized infrastructure.



Compute Isolation

Allocation of compute and storage resources ensures that an optimal footprint is available to each tenant to meet future workload demand. Tenant vDCs provide a secured multi-tenant environment to deploy VNFs. Compute resources are defined as resource pools when a tenant vDC is created.

A resource pool is an allocation of memory and CPU from the shared infrastructure, assignable to a tenant vDC. More resources can be added to a pool as capacity needs grow. The tenant vDC can also stretch across multiple resource clusters residing in different physical racks.

Network Isolation

NSX-T Data Center isolates and secures the traffic paths across workloads, the tenant switch, and the routing fabric. Advanced security policies and rules can be applied at the VM boundary to further control unwarranted traffic.

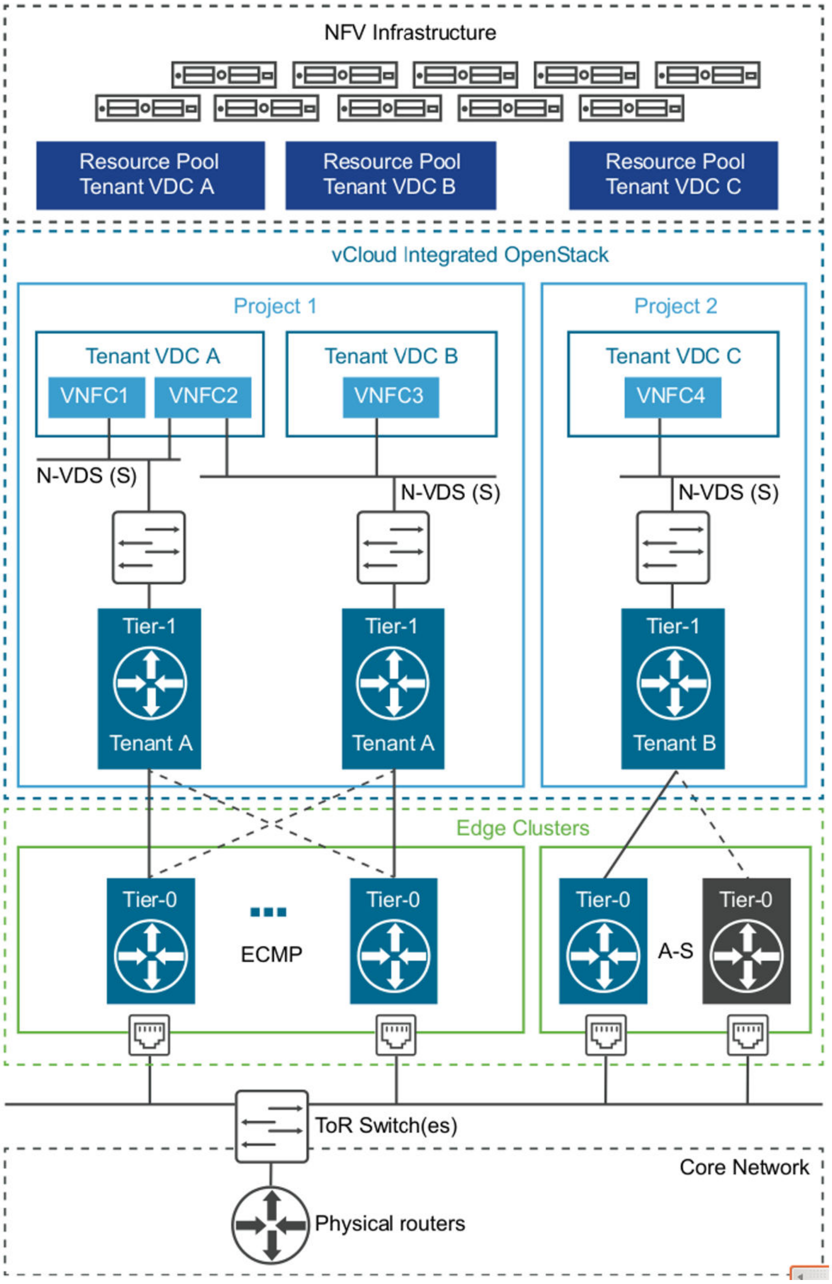
NSX-T Data Center uses a two-tiered routing architecture for network management:

- Logical Tier-0 router defines and isolates the provider tier.
- Logical Tier-1 router defines and isolates the tenant tiers.

The provider routing tier connects to the physical network for north-south traffic. The tenant routing context connects to the provider Tier-0 and manages east-west communications. The Tier-0 router provides traffic termination to the cloud physical gateways and existing CSP underlay networks for inter-cloud traffic communication.

Each tenant vDC has a single Tier-1 distributed router with intra-tenant routing capabilities. This distributed router can also be enabled for stateful services such as firewalls, NAT, and load balancers. VMs belonging to Tenant A can be connected to multiple logical interfaces for layer 2 and layer 3 connectivity.

By using VMware Integrated OpenStack as the IaaS layer, user profiles and RBAC policies can be used to restrict access to the networking fabric at the Tier-1 level.



Secure Multi-Tenancy and the VIM

vCenter Server, NSX Manager, and the VIM form a secure multi-tenant platform.

- vCenter Server lets you allocate and partition compute and storage resources precisely
- NSX creates the network virtualization layer with vSphere. The network virtualization layer is an abstraction between physical and virtual networks. NSX provides logical switches, firewalls, load balancers, and VPNs to isolate and secure network resources and services.

- VIM lets you create additional abstraction layers by distributing pooled resources among tenants. These abstraction layers provide a secure multi-tenant environment to deploy and run VNFs.

Physical compute, storage, and network resources are mapped to NFVI virtual resources such as clusters for compute resources, datastores for storage resources, and virtual switches for network resources. The VIM lets you map the virtual resources to a provider data center, which is a logical construct that pools the NFVI virtual resources for consumption by tenants. You can then reserve and allocate resources for tenants by using an organizational-level virtual data center.

Every organizational VDC maps to an underlying resource pool within the parent provider cluster. The VIM manages the resource pool according to the allocation settings of the organizational VDC and set aside resources without exceeding the resource limits.

Tenant edge devices that are deployed from the VIM use a dedicated resource pool nested within the provider resource pool. VNFs are deployed in a separate and dedicated resource pool nested within the organizational VDC. This separation of edge devices and VNF workload prevents exhaustion of resource.

Separation of network access between NFVI tenants is important for a secure multi-tenancy on a horizontally shared platform. The VIM integrates with vCenter Server and NSX to manage the creation and consumption of isolated Layer 2 networks.

Connectivity to external networks, such as the CSP Multi-protocol label switching (MPLS) network, must be manually set during the VNF onboarding process. Networks that are internal to an NFVI tenant or a VNF instance can be created using the VIM's user interface or API. BGP routing, ESG firewall rules, and additional services can be configured by the tenant administrator within the organizational VDC.

Embedded Analytics, Monitoring, and Intelligence for Security Assurance

VMware Aria Operations enriches the management pod with security assurance. Aria Operations lets you visualize and plan micro-segmentation and security policy distribution within NSX to enforce security across the virtual infrastructure. In general, the Aria Operations solution monitors the infrastructure for security policy violations.

Intrinsic Security

VMware Telco Cloud emphasizes the integration of intrinsic security with the software and infrastructure so that security is programmable, automated, and context-aware. Security that is built into the software and infrastructure improves visibility, reduces complexity, and focuses on security defenses. Intrinsic security enables you to apply and automate adaptive security measures such as micro-segmentation.

Even with intrinsic security, the following security best practices are necessary:

- Identify and deactivate unnecessary functionality and software
- Identify interfaces that are not required
- Remove all unnecessary accounts
- Follow the principles of least privilege and separation of duties for service and administrator accounts
- Deactivate unnecessary network services
- Audit open ports and their uses
- Harden VMs, hypervisors, and other components
- Conduct penetration testing regularly

References and Resources

10

US government 5G Cybersecurity Practice Guide, by National Cybersecurity Center of Excellence (NCCoE)

Trusted Cloud Security Practice Guide for VMware Hybrid Cloud Infrastructure as a Service (IaaS) Environments, NIST Special Publication 1800-19A.

NIST SPECIAL PUBLICATION 1800-33B, 5G Cybersecurity. Volume B: Approach, Architecture, and Security Characteristics

NIST SPECIAL PUBLICATION 800-190, Application Container Security Guide

UK government Telecommunications Security Bill of 2020.

Security Analysis for the UK Telecom Sector: Summary of Findings, by the National Cyber Security Centre, January 2020.

The future of telecoms in the UK, blog post by NCSC Technical Director Dr. Ian Levy, Published 28 January 2020.

5G PPP Phase 1 Security Landscape, Produced by the 5G PPP Security WG, June 2017.

The future of telecoms in the UK, blog post by NCSC Technical Director Dr. Ian Levy, 28 January 2020.

Security imperatives for digital transformation, By Patrick Donegan, published on TM Forum, August 2019.

vSphere Security, December 2023.

Protecting VM Register State with SEV-ES. AMD, David Kaplan, February 2017.

Secure Virtual Network Configuration for Virtual Machine (VM) Protection, NIST Special Publication 800-125B.

Application Container Security Guide, NIST Special Publication 800-190, by Murugiah Souppaya, Computer Security Division Information Technology Laboratory; John Morello, Twistlock, Baton Rouge, Louisiana; Karen Scarfone, Scarfone Cybersecurity, Clifton, Virginia. September 2017.

Security Assurance Requirements for Linux Application Container Deployments, NIST.IR 8176, by Ramaswamy Chandramouli, Computer Security Division, Information Technology Laboratory. October 2017.

VMware vSphere Virtual Machine Encryption: Virtual Machine Encryption Management, December 2017 white paper, VMware.

VMware Security Hardening Guides

Security Best Practices and Resources for VMware Virtualization Infrastructure

VMware NSX-T 3.2 Security Configuration Guide

vSphere Security Documentation, Guides, and Resources

Understanding vSphere Hardening and Compliance

Create an IP Pool with VMware NSX

Security Considerations for VMware Aria Operations for Logs

Micro-segmentation for Dummies, by Lawrence Miller and Joshua Soto, John Wiley & Sons, Inc. 2015.

VMware NSX Micro-segmentation Day 1, by Wade Holmes, VMware Press, 2017.