WHITE PAPER–MARCH 2021

Intrinsic Security for Telco Clouds at the Dawn of 5G

An Integrated Approach to Helping CSPs Meet Emerging Security Standards

vmware®

Table of Contents

Introduction

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

The findings of the analysis led the NCSC to recommend the establishment of a robust security framework based on a new set of telecommunications security requirements, or TSRs, that are intended to drive communications service providers (CSPs) to operate secure networks. In the U.K., this security framework will be underpinned by legislation.

The NCSC's summary of these security requirements sets forth a standardized answer to some of the security concerns raised by the 5G PPP Security Working Group in a 2017 paper that identified 5G-specific 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 will be maintained and managed in 5G networks."

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

At the same time, network virtualization expands the application and management of security measures. "While network virtualization presents risk, it also allows advanced and flexible network protections," the NCSC writes in its findings.

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 will likely intensify the importance of centralized management and monitoring. Flexible, intrinsic, and automated approaches to imposing and enforcing security measures are becoming paramount.

This VMware white paper summarizes the security risks and requirements that communications service providers face as they transition to 5G networks and increasingly rely on virtualization and cloud computing, including network functions virtualization and cloud native technology like containers and Kubernetes.

To identify the key security risks and requirements in the changing telecommunications landscape, this paper relies on three standard-setting papers:

1. *Security Analysis for the UK Telecom Sector: Summary of Findings,* by the National Cyber Security Centre of the United Kingdom, published 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.

After discussing the risk factors and attack vectors of mixed 4G and 5G networks, this paper explains how VMware technology helps you implement security controls for the virtualization plane and its management and orchestration. The final section illustrates how to combine VMware technologies into an architecture that protects telecom networks with intrinsic security.

Risk Factors and Attack Vectors

Some risks are specific to 5G; others accompany the current infrastructure of most CSPs and are likely to remain during the transition to 5G. Risk factors are typically evaluated and prioritized based on how they might affect the three key aspects of information security:

- Integrity
- Availability
- Confidentiality

Sensitive functions warrant heightened protection. In its summary of findings, the NCSC considers the following functions to be critically sensitive:[1]

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

These functions warrant the highest levels of protection because a compromise could seriously undermine integrity, availability, or confidentiality.

Solving the trade-off between security and performance

A conflict undermines the security of some telecom networks: Security doesn't pay. Implementing it can be expensive, and there can be a trade-off between security and performance, a conflict that's not lost on the NCSC:

"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. That's unsustainable. So, the government decision to significantly uplift the baseline telecoms security and formalise the handling of high risk vendors putting it all on a robust footing is very welcome. It provides clarity for operators and transparency about what we expect for the security of our national networks. Externalising the security costs of particular choices (including vendor) will help operators make better security risk management decisions."[2] In the UK, 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.[3]

"If security is well managed, it can be a positive differentiator for CSPs."

PATRICK DONEGAN, PRINCIPAL ANALYST, HARDENSTANCE

Because prioritizing performance and revenue over security heightens risk and exposes more attack surface, such a trade-off is likely to prove damaging in the long run. The solution is to invest more in infrastructure that improves performance and scalability so that implementing security measures does not degrade network performance.

"If security is well managed, it can be a positive differentiator for CSPs," Patrick Donegan, Principal Analyst at HardenStance, writes in *Security Imperatives For Digital Transformation*.

There is a related problem that can make upgrading and patching difficult: Some CSPs run their equipment at such high levels of across-the-board utilization that it thwarts their capability to apply patches and perform rolling upgrades. This problem can also be addressed by investing more in infrastructure that enhances performance.

1 Security Analysis for the UK Telecom Sector: Summary of Findings, by the National Cyber Security Centre, January 2020. See https://www.ncsc.gov.uk/report/summary-of-ncsc-security-analysis-for-the-uk-telecoms-sector.
2 The future of telecoms in the UK, blog post by NCSC Technical Director Dr. Ian Levy, Published 28 January 2020. https://www.ncsc.gov.uk/blog-post/the-future-of-telecoms-in-the-uk
3 See the UK government's *Telecommunications Security Bill of 2020*.

"While network virtualization presents risk, it also allows advanced and flexible network protections. For this reason, a well-built virtualised network can be more secure and resilient than an equivalent network built on dedicated hardware."

SECURITY ANALYSIS FOR THE UK TELECOM SECTOR: SUMMARY OF FINDINGS, NATIONAL CYBER SECURITY CENTRE, JANUARY 2020

Virtualization plane

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 could enable an attacker to gain access to the entire virtualization fabric, including all hosts and virtual workloads, potentially compromising the whole network and affecting the availability and confidentiality of critical services.

Signaling plane and core network virtualization

The signaling plane risks being the recipient of malicious data, which could undermine the availability of the network.

5G-Specific threats and risk factors

The 5G PPP Security Working Group's white paper on the 5G security landscape identifies a number of 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 open up additional attack vectors.[4]

Here are some of the risks identified by the working group that are relevant to the VMware telco stack. This preliminary list will require 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 slice isolation, which could expose sensitive data to applications running in other slices through a side-channel attack
- 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 could make management complex and difficult, which 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 give rise to key security imperatives. In general, securing the virtualization plane and its management relies on your ability to do the following:

- Keep the virtualization fabric and virtual machines up to date.
- Maintain the fabric en masse 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.

4 5G PPP Phase 1 Security Landscape, Produced by the 5G PPP Security WG, June 2017. https://5g-ppp.eu/wp-content/uploads/2014/02/5G-PPP_White-Paper_Phase-1-Security-Landscape_June-2017.pdf

INTRINSIC SECURITY

With VMware Telco Cloud Infrastructure, security is intrinsic—integrated with the software and built into the infrastructure so that security is 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 like micro-segmentation in the right place.

- 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.

After a brief look at the layers of the VMware Telco Cloud, the next sections highlight security requirements and solutions for the virtualization and management of telecommunications networks.

Overview of the VMware Telco Cloud

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

- Infrastructure
- Automation
- Operations

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

Virtual infrastructure layer

The infrastructure layer supplies infrastructure as a service with VMware Telco Cloud Infrastructure™, which combines the following virtualization technology: VMware vSphere®, VMware NSX® Data Center, and (optionally) VMware vSAN™.

With VMware Telco Cloud Infrastructure, security is intrinsic—integrated with the software and built into the infrastructure so that security is 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 like micro-segmentation in the right place.

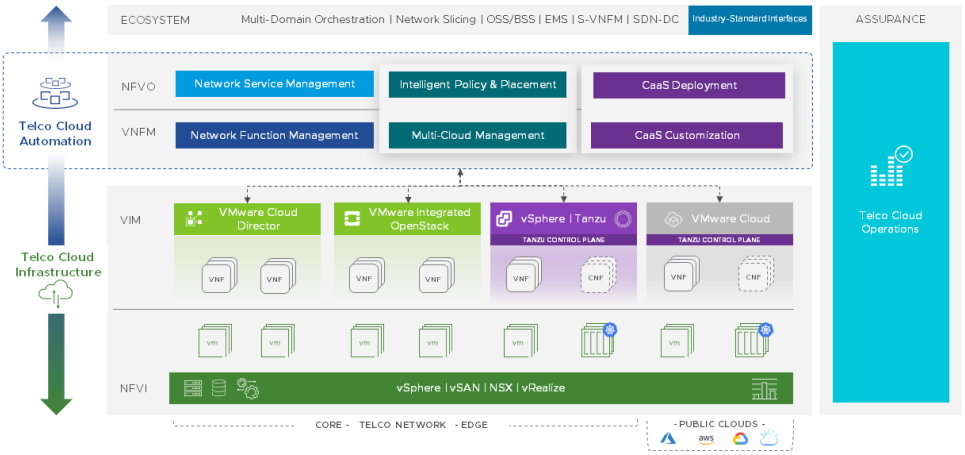


Figure 1: The VMware Telco Cloud includes three main products: VMware Telco Cloud Infrastructure, VMware Telco Cloud Automation, and VMware Telco Cloud Operations. A fourth product—VMware Telco Cloud Platform—combines compute and networking with VMware Telco Cloud Automation to form a cloud-native platform.

VMVWARE TELCO CLOUD INFRASTRUCTURE AT A GLANCE

VMware Telco Cloud Infrastructure simplifies, scales, and protects cloud services with consistent, fully integrated, multi-tenant infrastructure powered by field-proven compute, storage, networking, and management solutions. It can isolate multiple tenants within the same NFV infrastructure.

KEY BENEFITS AND CAPABILITIES

- Proven infrastructure stack deployed in production by some of the world's largest CSPs
- Seamless provisioning and consumption of infrastructure resources as code across geographically dispersed locations with VMware Cloud Director
- A fully supported OpenStack distribution (optional)
- Carrier-grade networking with high-performance virtualized switching, routing, firewalls, and load balancing
- Deployment of new services on-demand with real-time scaling
- Multi-tenant cloud environments with tenant isolation
- Fully isolated and protected workloads
- Guaranteed resource pools providing predefined SLAs to each tenant
- Service-based deployment, isolation, and security
- Provider- and tenant-based roles and service policies
- Proactive high availability through real-time performance analytics

Management and automation layer

The automation layer includes VMware Telco Cloud Automation™, which orchestrates network functions, services, and resources from a centralized location. It integrates with any virtual infrastructure manager (VIM) and Kubernetes to form a powerful multi-tenant environment to securely manage the application layer.

Our virtual infrastructure managers—you can select VMware Cloud Director® or VMware® Integrated OpenStack—let you impose role-based access control in a large-scale, multi-tenant telecommunications network.

Operations layer

The operations layer provides analytics, network intelligence, and assurance with VMware Telco Cloud Operations as well as such options as VMware vRealize® Log Insight™, VMware vRealize® Operations™, and VMware vRealize® Network Insight™.

To help communications service providers who are implementing 5G or transitioning to 5G by establishing a mixed non-stand-alone 5G and 4G network, VMware provides various bundles to support a variety of telco requirements, and you can choose the VIM that best suits your requirements. A telco-grade Kubernetes distribution from VMware can empower you to build, run, and manage containerized network functions (CNFs) and 5G services.

Protecting the Virtualization Plane and Containerized Environments

This section highlights how VMware fulfills key security requirements for the virtualization plane of telecommunications networks to reduce risk and limit the attack surface.

The following requirements and solutions for protecting the virtualization plane are divided 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, many of which are embodied in each subsection's heading, stem from the NCSC's summary of findings and the 5G PPP security working group's white paper cited earlier. VMware addresses these requirements by implementing settings, controls, and functions to protect virtualized infrastructure, including hypervisors, virtual machines, virtualized networking, and management functions.

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 bars virtual workloads from gaining access to or cutting through to the underlying hardware.

Keeping the virtualization fabric up to date

VMware vSphere Update Manager is at the core of keeping your virtualization fabric up to date. Update Manager centralizes patch and version management for VMware vSphere and supports VMware ESXi hosts and virtual machines. With Update Manager, you can upgrade and patch ESXi hosts, install and update third-party software on hosts, and upgrade virtual machine hardware and VMware Tools.

Upgrade Manager works either automatically or manually. It describes the tasks that you can perform to update your vSphere inventory objects and to enforce compliance with certain baselines.

VMWARE CLOUD DIRECTOR AT A GLANCE

VMware Cloud Director is a hyper-scale virtual infrastructure manager that helps CSPs provision cloud services, automate operations, maximize resource utilization, and dynamically scale infrastructure to meet changes in demand.

KEY BENEFITS

- Use a unified API-driven cloud platform to manage applications, services, containers, and virtual machines.
- Create virtual data centers from common or distributed infrastructure to cater to the heterogeneous needs of your customers.
- Stitch together complex custom telecommunications services and automate their operations.

VMWARE INTEGRATED OPENSTACK CARRIER EDITION AT A GLANCE

VMware Integrated OpenStack Carrier Edition is a VMware-supported OpenStack distribution for deploying NFV services. As part of VMware Telco Cloud Infrastructure, VMware Integrated OpenStack is a virtual infrastructure manager that accelerates time to market for new services, streamlines operations, and reduces infrastructure costs.

KEY BENEFITS

- Reduce operating expenses through extensive automation and continuous network performance optimization.
- Realize low capital expenditure per subscriber with a dense data center footprint and lower licensing costs.
- Run OpenStack at scale with support for multiple regions while complying with the OpenStack Foundation's 2018.02 interoperability guidelines.

A typical telecommunications operator should run Update Manager as a manual process to check for host patches and extensions at *regular intervals*. See the VMware vSphere Update Manager *documentation*.

The health checks in vSphere Health, which is set to be renamed Skyline Health in a future release, tracks the health of a vSphere environment, including possible security-related vulnerabilities in VMware vCenter Server® and ESXi. The health checks can help ensure that the virtualization fabric is up to date. For more information, see *VMware Security Advisories in vSphere Health* and *Introducing VMware Skyline Health for vSphere*.

Delivering critical security patches for quick deployment

VMware Security Advisories document remediation for security vulnerabilities that are reported in VMware products. VMware Security Alerts are posted at *https://www.vmware.com/security/alerts*.

The *VMware Security Response Policy* documents our commitments for resolving possible vulnerabilities in our products to assure our customers that any such issues will be corrected in a timely fashion. VMware will release a fix for the reported vulnerability. The fix may take 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 installed 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 that instructs users in adjusting the VMware product configuration to mitigate the vulnerability

Updating the virtualization fabric without affecting the network

The VMware virtualization fabric can be updated without affecting its availability.

The virtualization fabric can also be updated without affecting virtual network functions (VNFs) if they have been built with a fail-over capability, an active-active pattern, or another pattern that allows them to be moved with automation. VMware vSphere vMotion can thus use automation to move these VNFs from one set of hosts to another set so that the first set of hosts can be patched or updated without affecting the availability of the fabric or the VNFs running in the fabric.

To ensure that the VNF fabric can be updated without affecting the network, CSPs should require their vendors to supply VNFs that either have a built-in fail-over capability or can use vMotion as a failover mechanism.

Locking down hypervisors to restrict access

To increase the security of ESXi hosts, you can put them in lockdown mode. In lockdown mode, operations must be performed through vCenter Server by default. Starting with vSphere 6.0, you can select normal lockdown mode or strict lockdown mode, which offer different degrees of lockdown. 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 selected IP addresses. 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 the Preboot Execution Environment (PXE) to add only known hosts to the virtualization fabric.

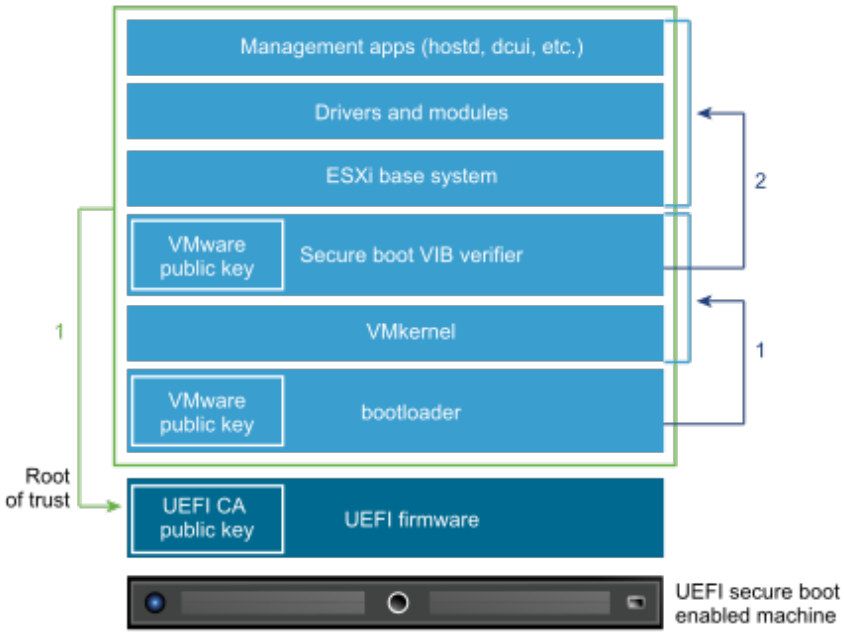


Figure 2: Secure boot in the VMware ESXi hypervisor.

Adding only attested hosts to the fabric

VMware cryptographically attests hosts in several ways:

- Secure boot. In vSphere, you can enable secure boot on the host to ensure that only digitally signed code is allowed to run.
- VMware AppDefense.

For CSPs, it is a security best practice to 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 refuses to load a UEFI driver or app unless the operating system bootloader is cryptographically signed. Starting with vSphere 6.5, ESXi supports secure boot if it is enabled in the hardware; as such, you should deploy hardware that supports and uses hardware roots-of-trust.

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

1. The ESXi bootloader contains a VMware public key. The bootloader uses this 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 VIB package that is installed on the system.

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

VMware AppDefense™ adds another form of attestation. AppDefense can be optionally embedded in ESXi to ensure the integrity of the operating system and the hypervisor. AppDefense verifies the reputation of executables and understands process-to-process communications on an NSX network.

By modeling known-good behavior, AppDefense helps you patch software sooner by continuously scanning workloads to detect changes and highlight vulnerabilities in the operating system and hypervisor.

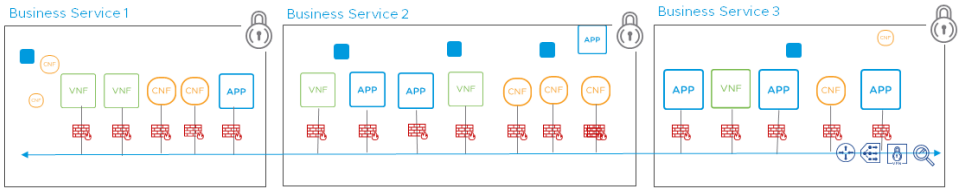


Figure 3: Distributed firewalls and micros-segmentation can isolate VNFs, CNFs, applications, and services.

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, third-party firewalls that work with VMware virtualization solutions can be incorporated to help meet uncommon performance requirements.[5] Virtual firewalls can be combined with micro-segmentation to separate all types of traffic, virtual machines, and workloads.

Micro-segmentation divides a virtual data center and its workloads into logical segments, each of which contain a single workload. You can then apply security controls to each segment, restricting an attacker's ability to move to another segment or workload.[6] This approach reduces the risk of attack, limits the possible damage from an attack, and improves the overall security posture.

Micro-segmentation uses the following capabilities to reduce risk and improve security:[7]

- Distributed stateful firewalling, which can protect each application running in the data center with application-level gateways that are applied on a per-workload basis.
- Topology-agnostic segmentation, which protects each application with a firewall independent of the underlying network topology.
- Centralized ubiquitous policy control of distributed services, which controls access with a centralized management plane.
- Granular unit-level controls implemented by high-level policy objects, which can create a security perimeter for each application without relying on VLANs.
- Network-based isolation, which implements logical network overlays through virtualization.
- Policy-driven unit-level service insertion and traffic steering, which can help monitor network traffic.

The micro-segmentation capabilities of NSX also satisfy[8] the security recommendations for protecting virtualized workloads set forth in NIST Special Publication 800-125B, Secure Virtual Network Configuration for Virtual Machine (VM) Protection.

Storing secrets and keys in secure hardware-backed storage

An external Key Management Server (KMS) provides the keys for encrypting virtual machines in vSphere and the vSAN datastore. Because the KMS is an external system, it can be a secure hardware-backed storage system. The use of an external KMS creates a requirement for operators to obtain robust third-party hardware in which to store keys.

Configuring the virtualization fabric to ensure 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,

5 With NSX-T Data Center, vSphere includes an N-VDS Enhanced mode for switching that improves performance. The N-VDS Enhanced mode uses vertical NUMA compute alignment capabilities to accelerate workloads. See the *Reference Architecture* Guide for VMware Telco Cloud Infrastructure.
6 For more information about what micro-segmentation is and what it isn't, see Micro-Segmentation for Dummies, by Lawrence Miller and Joshua Soto, published by John Wiley & Sons, Inc. 2015.
7 VMware NSX Micro-segmentation Day 1, by Wade Holmes, published by VMware Press, 2017; https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-microsegmentation.pdf
8 VMware NSX Micro-segmentation Day 1, by Wade Holmes, published by VMware Press, 2017; https://www.vmware.com/content/dam/digitalmarketing/vmware/en/pdf/products/nsx/vmware-nsx-microsegmentation.pdf.

SECURITY AT THE EDGE

VMware NSX implements network and security services—such as security groups, firewalling, and micro-segmentation—directly into the hypervisor, enabling a least-privilege model for an edge site. Micro-segmentation and virtual firewalls can segment internal and external network traffic at an edge site to prevent threats from moving laterally within the environment.

Similarly, an NSX security group can contain multiple types of objects from vSphere, such as logical switches, virtual NICs, and virtual machines. For example, all virtual machines with the security tag "edge-site-7B" are automatically placed in a security group at the edge site to establish a security pool of virtual machines that act as edge hosts to run public-facing VNFs in their DMZ, reducing exposure of the virtualization plane and simplifying monitoring of external network interfaces.

NSX security groups, tags, policies, and other capabilities can isolate virtual workloads in edge trust domains, and you can then manage those domains by their risk and sensitivity levels. This separation can further limit the attack surface of an edge site.

In general, VMware can also apply the same types of security measures to the hypervisors and virtual machines running at an edge site as those running at other sites, Depending on the security and performance requirements of an edge site, other VMware products, such as VMware Carbon Black, may be used to implement additional security measures.

and routing. NSX embeds the networking and security functionality typically handled by hardware directly in the ESXi hypervisor.

This abstraction, in turn, makes possible levels of security and efficiency that were previously infeasible. You can, for example, apply micro-segmentation with distributed stateful firewalling and dynamic security policies attached directly to individual workloads.

In addition, vSphere includes a number of settings to manage the allocation of IP addresses, ports, and encryption. VMware technology excels at blocking the access of hypervisors and virtual machines to the underlying hardware.

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

vSphere provides several schemes for automatic allocation of MAC addresses in vCenter Server. You can select the scheme that best suits your requirements. For example, you can use generated MAC addresses that are assigned by vCenter Server or assigned by the ESXi host, and you can use a range-based or a prefix-based allocation scheme to generate MAC addresses. For vSphere, 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 traffic that a virtual machine receives. When the Mac address changes 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 virtual machine adapter used to send the request is disabled and the virtual machine 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. See *MAC Address Changes*.

Port mirroring, otherwise known as span ports, is turned off by default in vSphere. You have to explicitly turn it on by creating a port mirroring session. See *Working with Port Mirroring*.

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

A vSphere Distributed Switch can mirror traffic from one port to another to allow packet capture devices to collect specific traffic flows. This mirrored traffic contains the full data in the packets captured and can result 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 vSphere, see *General Networking Security Recommendations*.

Encrypting data at rest

VMware vSphere and vSAN store data at rest to prevent the exfiltration of data. VMware vSphere uses the ESXi hypervisor to perform the encryption without modifying the virtual machine. 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, providing a common method of encryption across any operating system supported by vSphere.
- No specialized hardware or infrastructure is required—the encryption works with existing storage devices and storage fabrics.
- Policy-based enforcement that is supported by the vSphere SDK and tools such as VMware vSphere PowerCLI. This support provides 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 has been applied, the VM is automatically encrypted. The encryption policy can be applied on the Storage Policy screens in the vSphere Web Client instance 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 it 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 allowed to run.

Two 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.

The vCenter Server system transfers VM KEKs to an ESXi host when the host requires a key. The ESXi host uses the KEK to encrypt the DEK, and it stores the encrypted internal key on disk. The ESXi host does not store the KEK on disk. If a host reboots, the vCenter Server instance requests the KEK with the corresponding ID from the external KMS and makes it available to the ESXi 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 vSAN encryption is turned on, all files are encrypted, which protects virtual machines and their corresponding 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 device is removed from the cluster.

The 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.

Here's how vSAN uses encryption keys:

- 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.

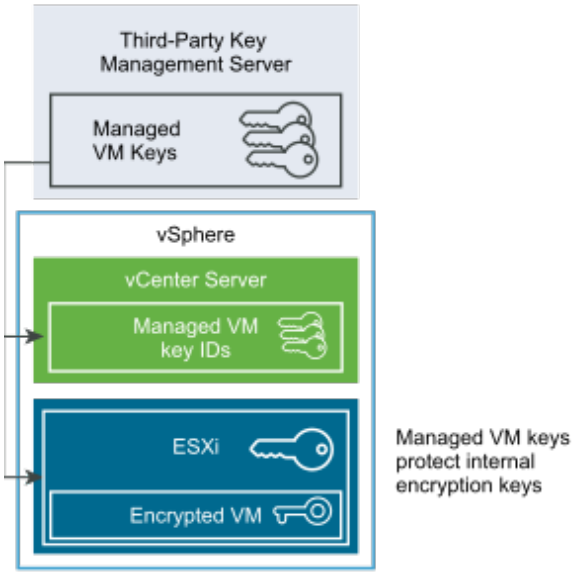


Figure 4: Securely storing keys in an external Key Management Server.

- 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*.

There are some more technical and operational details about encryption of data in the virtualization fabric, and the technical and operational mechanism might vary with the version of vSphere or vSAN and other VMware technology that's in use; for more information, see *VMware vSphere Virtual Machine Encryption*.

With VMware 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 still maintaining operational efficiencies inherent in the vSphere platform, all while preserving the security of the virtual machine.

Encrypting data in transit

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

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

Encryption is performed by the industry-standard OpenSSL libraries and algorithms described in *VMware vSphere Virtual Machine Encryption*. VM encryption does not impose any new hardware requirements, but using a processor that supports the AES-NI instruction set accelerates encryption and decryption operations.

Using both vSAN datastore encryption and VMcrypt might impair performance for some use cases because of the processing cost involved in encryption; 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 vs. VMcrypt Encryption*.

Blocking access to the underlying hardware

By default, virtual machines are configured to block direct access to the underlying physical hardware. VMware holds contests in which hackers are challenged to find a security hole in a virtual machine through which they can escape or cut through to the physical hardware to execute code on the hardware. You should make sure that you tightly control privileged access to the VMware ESXi host by using the principles of separation of duties and least privilege.

It is also important to have the right hardware in place to be able to separate traffic to meet emerging industry security requirements. Emerging standards rely heavily on segmentation at various levels, including separating the management network from the data network. Buying and installing appropriate hardware with enough physical ports provides the flexibility to separate traffic in the management and data planes, as well as others. The use of hardware without enough physical ports can lead to problems in managing API management traffic and in separating management functions by security level.

If, for example, an application is granted permission to access the vSphere API at a highly privileged level, it creates an attack vector that could expose access to the underlying hardware. By applying the principles of least privilege and separation of duties, you can make sure that all systems, applications, and personnel have only 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.

Two examples illustrate the importance of tightly controlling privileged access to the virtualization plane. In an attempt to maximize utilization of hardware resources, some telco operators use an element manager to gauge the load of the underlying hardware in a vSphere environment. Such an approach, however, can expose a vector through which an attack could potentially gain access to the hardware.

Another example involves the Common Information Model (CIM) interface. For API-based hardware-level management through the CIM interface from remote applications via the VMware ESXi host, root credentials must not be used to access the CIM interface. Instead, you should create a less-privileged vSphere user account for these applications and use the VIM API ticket function to issue 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 inside the ESXi host.

To ensure that the CIM interface is secure, you should provide only the minimum access necessary to these remote applications. If you provision a remote application with a root or administrator account, and if the application is compromised, the virtual environment could become compromised. See *Control Access for CIM-Based Hardware Monitoring Tools*.

Establishing trust domains and segregation

Virtualized infrastructure plays a strong role in segregating workloads into trusted domains to reduce the risk of a breach spreading from a compromised host to other hosts. When you set up components of the management plane, such as a VIM and VMware Telco Cloud Automation, you can do so in a trusted location segmented from the rest of virtualization fabric. Establishing the management plane in a separate domain from the virtualization plane allows you to further protect it with firewalls, micro-segmentation, and other measures.

MICRO-SEGMENTATION

Micro-segmentation divides a virtual data center and its workloads into logical segments, each of which contain a single workload. You can then apply security controls to each segment, restricting an attacker's ability to move to another segment or workload. This approach reduces the risk of attack, limits the possible damage from an attack, and improves the overall security posture.

SECURE MULTI-TENANCY WITH TELCO CLOUD INFRASTRUCTURE

Multi-tenant CSPs must ensure that each tenant is fully secure from attacks, breaches, or insecure communications from other tenants. VMware Telco Cloud Infrastructure separates services in a multi-tenant environment across NFVI functions (virtual compute to networking) through the following means:

- NSX micro-segmentation with fine-grained access controls for provider and tenant administrators
- Transparent integration at the VIM layer
- Delegated role-based access control for fine-grained resource access
- Tenant-level operations management and visibility
- Cross-vCenter security policies, which empower operators to apply security policies consistently on objects across multiple VMware vCenter services

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

NSX architects network and security services—such as firewalling—directly into the hypervisor, enabling a least-privilege model for the network. The outcome is that a network security team can prevent threats from moving laterally within an environment by, for example, creating security groups, which can include dynamic membership criteria defined by security tags. Security groups can also be governed by a security policy. See *Working with Security Groups*.

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 a separate host pool, thereby limiting the attack surface.

Enforcing separation between trust domains

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

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

Hardware-assisted CPU virtualization assistance, called VT-x in Intel processors and AMD-V in AMD processors, automatically traps sensitive events and instructions in the VMware virtualization fabric, allowing trap-and-emulate style virtualization as well as providing assistance to reduce the overhead involved in handling these traps.

Hardware-assisted I/O MMU virtualization, 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, is an I/O memory management feature that remaps I/O DMA transfers and device interrupts. In the VMware virtualization fabric, this feature (which is, strictly speaking, a function of the chip set, rather than the CPU) can allow virtual machines to have direct access to hardware I/O devices, such as network cards, storage controllers (HBAs), and GPUs. Input–output memory management unit (IOMMU) can map virtual addresses to physical addresses. For more information, see *Performance Best Practices for VMware vSphere 6.7*.

Eliminating cross-host impacts

SpoofGuard prevents spoofing on an NSX logical switch. SpoofGuard lets you authorize the IP addresses reported by VMware Tools or IP discovery. 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, in turn, 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."[9]

To establish a strong security barrier for containers, VMware typically runs containers on virtual machines.

9 NIST Special Publication 800-190, Application Container Security Guide, by Murugiah Souppaya, Computer Security Division Information Technology Laboratory; John Morello, Twistlock, Baton Rouge, Louisiana; Karen Scarfone, Scarfone Cybersecurity, Clifton, Virginia. September 2017. This publication is available free of charge from https://doi.org/10.6028/NIST.SP.800-190

Running containers on VMs also lets you take advantage of security innovations in virtualization technology. AMD SEV-ES provides an example. 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) builds upon SEV to provide an even smaller attack surface and additional protection for a guest VM from the hypervisor even if the hypervisor is compromised. SEV-ES blocks attacks by encrypting and protecting all CPU register contents when a VM stops running to prevent the leakage of information in CPU registers to the hypervisor. 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 a VIM, that can manage containerized services programmatically at scale. Containers are addressed in more detail in a later section.

Protecting the Management of the Virtualization Plane

Protecting the management plane falls into three main areas of focus: its architecture, its administration network, and the access and privileges of administrators. Architecting a secure management plane puts in place the foundation upon which management elements, including the administrative network, can be isolated from other aspects of the virtual infrastructure and sets stage for successfully controlling and monitoring administrative access.

In architecting their management plane, operators can use a number of inter-related, generally interoperable solutions from VMware not only to manage their virtualized and containerized infrastructure but also to apply security measures in the management plane:

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

In addition, for managing cloud native functions and cloud network functions, VMware infrastructure integrates at strategic points with Kubernetes and other cloud native technology. VMware Telco Cloud Automation, for example, can securely deploy and orchestrate cloud native workloads on Kubernetes.

Architecture of the management plane

The architecture of the management plane establishes a trusted foundation for isolating management functions from the rest of the operator's network. When it is architected to enhance security, the management plane is segmented into discrete zones, bars movement across the plane, and restricts access to and exfiltration of network data. Management functions are considered critical security function that demand additional security controls, and operators should 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 a central orchestration tool: VMware Telco Cloud Automation, which integrates with VMware Telco Cloud Infrastructure. A VIM from VMware and the management interface for vSphere let you manage lower-level aspects of the management plane.

VMware architectures for CSPs isolate the management plane. The components and resources of the management plane, including vCenter Server and NSX Manager, are

TENANT AND MULTI-TENANCY IN SHARED VIRTUALIZED INFRASTRUCTURE

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

Scope multi-tenancy isolates resources and networks to deliver applications with quality for each tenant. Because multiple tenants share the same resource infrastructure, secure multi-tenancy can be enabled by using a VIM from VMware 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 both internal and external tenants over the common shared infrastructure so tenants can deploy and operate their respective workloads and services with virtualized network, compute, and storage isolation.

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 as well as 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 context can connect to the provider Tier-0 and manage east-west communications.

The Tier-0 will provide traffic termination to the cloud physical gateways and existing CSP underlay networks for inter-cloud traffic communication. Each organization in a virtual data center will 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. VNF element managers, for example, 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 furnishes a reference architecture for building, isolating, and protecting the management plane; see the *Reference Architecture* for VMware Telco Cloud Infrastructure, especially the sections on the management pod and the three-pod deployment option.

Protecting the administration network

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

VMware Telco Cloud Automation connects to a VIM from VMware over a secure channel so that you, as an administrator, can manage your telco virtualization fabric and its network functions from a single location.

VMware Telco Cloud Automation and a VIM control access with authentication and multi-tenant role-based access control. The VIM securely integrates with vSphere, NSX, and vSAN to establish a single management plane for the virtualization fabric.

Beyond the virtualization layer, it is important to have the right hardware in place to be able to protect the administration network by physically separating its traffic from the traffic of other networks with physical ports. Buying and installing appropriate hardware with enough physical ports provides the foundation for separating traffic at the physical layer and for segmenting traffic by sensitivity levels.

Separating administration from the virtualization fabric

Because the management functions that support the administration and security of the virtualization fabric are considered to be security critical functions, it is crucial that they be

rigorously separated from the rest of the virtualization fabric, protected with strong security measures, and closely monitored.

The *Reference Architecture* for the Cloud Director Edition of VMware Telco Cloud Infrastructure includes a three-pod design that completely separates the functional blocks by using a management pod, edge pod, and resource pod for their functions. 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 virtualization fabric.

In the reference architecture, 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 *Reference Architecture*, especially the sections on deployment options.

Protecting virtualization of security critical functions

The NCSC's paper summarizing the findings of its telecom security analysis emphasizes the protection of security critical functions. Security critical functions include orchestration systems for virtualization; management systems like jump boxes; firewalls protecting a security zone; directory services used for authentication and access control, such as Active Directory; 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 considered by the NCSC to be security-critical functions. The functions should take place in a trusted location secured by the following:

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

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

It is key to limit the attack surface of security critical functions. Within the virtualization fabric, you can segregate security critical functions in the virtualization fabric to reduce risk by using micro-segmentation with NSX. Micro-segmentation isolates security functions in their own trust domain.

Beyond virtualization, protecting security critical functions also requires appropriate hardware—hardware with disks that can be encrypted and a sufficient number of 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 should be isolated from other networks and be closely monitored to track access and changes. Security critical functions can be separated by using a separate vSphere cluster of the ESXi hypervisor and virtual machines. NSX can then further isolate security critical functions by implementing firewalls and applying micro-segmentation.

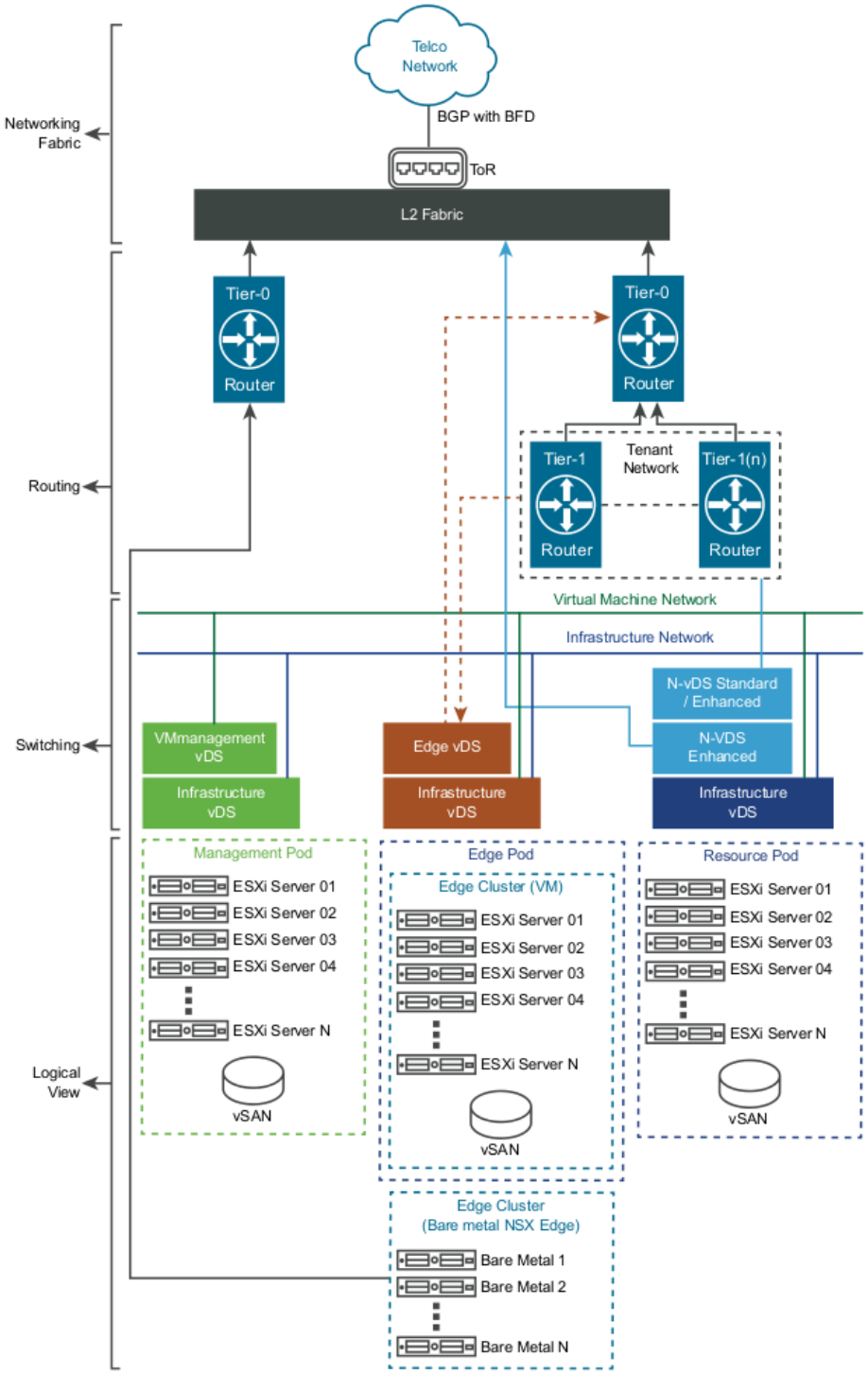


Figure 5: This diagram depicts the physical representation of the compute and networking connectivity and the logical layers of the switching and routing fabric. This flexible, scalable three-pod design uses a management pod to separate administration from the virtualization fabric.

Because containers alone are an inadequate security boundary, they should not be used 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, can authenticate and authorize users with Microsoft Active Directory or LDAP. These security systems are to be considered security critical functions. As such, a system like 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 too must be isolated in its own local, trusted security domain, not within the corporate security domain.

AppDefense can help defend isolated security functions. AppDefense can monitor the behavior of ESXi hypervisors and virtual machines running security critical functions by profiling their known good state, detecting anomalies, and responding when they deviate into an unknown state.

AppDefense also enhances the effectiveness of micro-segmentation by providing additional workload context to NSX. From inside the vSphere hypervisor, AppDefense profiles the behavior of data center endpoints to identify when changes are made. This contextual intelligence helps you distinguish threats from legitimate changes.

When a threat is detected, AppDefense can trigger vSphere and NSX to orchestrate the correct response without manual intervention. Responses can include the following:

- Block process communication
- Snapshot an endpoint for forensic analysis
- Suspend an endpoint
- Shut down an endpoint

As for the monitoring of security critical functions, Log Insight can ingest syslog messages. Log Insight includes a built-in syslog server that is active when the vRealize Log Insight service is running. The syslog server listens on ports 514/TCP, 1514/TCP, and 514/UDP; it is ready to ingest log messages sent from other hosts. Ingested messages become searchable in vRealize Log Insight in near real time to help monitor security critical functions. See *vRealize Log Insight as Syslog Server*.

To protect sensitive information gathered by vRealize Log Insight, you can place the server on a management network segment protected by a firewall from the rest of the internal network. See *vRealize Log Insight Firewall Recommendations*. Security controls can safeguard vRealize Log Insight; see *Security Considerations for vRealize Log Insight*.

Securing access to the management plane

The UK's NCSC sets forth several principles that drive requirements for securing user access to the management plane. Operators should tightly control access to the management plane by using the principles of least privilege and separation of duties, and each user is to 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, you should also block virtualization administrators from accessing workloads running in the virtualized environment.

The security of the orchestration system is paramount. Access to 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. See *Understanding vCenter Server Two-Factor Authentication* and *Configuring Smart Card Authentication for ESXi*.

Automating administration

NSX Data Center can automate 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. See *Network Automation*.

Blocking non-management devices from the management plane

In the past, some telecommunications networks have neglected to maintain a clear boundary between the management plane and other planes, allowing non-management devices to access the management plane. There should, however, be no access to devices outside the management plane, and devices without a management function should be barred from accessing the management network to minimize the attack surface.

NSX can use distributed firewalls, micro-segmentation, and security policies to cordon off the management plane and block the access of non-management devices.

In addition, Cloud Director can control access and cloud administration rights with Active Directory, allow lists, and other measures. By using Cloud Director with Active Directory, for example, you can limit access to only specific workstations—those devices set aside as privileged access workstations for connecting 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. You can 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. 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. See *Specifying Accounts with Access Privileges in Lockdown Mode*.

vSphere 6.0 and later supports an Exception User list, which is for service accounts that have to log in to the host directly. Accounts with administrator privileges that are on the Exception Users list can log in to the ESXi Shell. In addition, those users can log in to a host's DCUI in normal lockdown mode and can 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

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

- Dynamic resource discovery. Distributed and complex topologies require dynamic resource and service discovery. The platform 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 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 profile and monitor traffic segments, types, and destinations to recommend security rules and policies for traffic. 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. The main components are vRealize Operations Manager, vRealize Log Insight, and vRealize Network Insight. An additional component is VMware Telco Cloud Operations. The following sections describe how these components satisfy emerging telco security requirements.

Analyzing network data, topologies, and traffic

These four tools combine to provide a secure system for analysis of network data, topologies, routes, and traffic. Here is the role that each tool plays in analyzing network information:

- vRealize Operations Manager collects compute, storage, and networking data to provide performance and fault visibility over hosts, hypervisors, virtual machines, clusters, and sites.
- vRealize Log Insight captures unstructured data from the environment to provide log analysis and analytics. Platform component logs and events are ingested, tokenized, and mined for intelligence.
- vRealize Network Insight provides layer 2, 3, and 4 visibility into the virtual and physical networks, and it can help identify network anomalies and security policy gaps. The engine is integrated with the NFVI networking fabric to capture device and network configurations, IPFIX flow, and SNMP. vRealize Network Insight gives you visibility into traffic routing, sources and destinations, micro-segmentation, and possible security violations.
- VMware Telco Cloud Operations provides holistic monitoring and network management across all layers of the telco stack, both physical and logical, for rapid insights into configurations, interactions, and compliance. If a software component like SSL is out of date, VMware Telco Cloud Operations can detect it and raise an out-of-compliance notification. VMware Telco Cloud Operations complements the virtual capabilities of vRealize Network Insight by monitoring physical equipment, including routers, switches, and servers as well as the ESXi hypervisor and other VMware products, such as NSX. VMware Telco Cloud Operations fits into the VMware Telco Cloud by connecting to VMware Telco Cloud Infrastructure or VMware SD-WAN Orchestrator through an API integration. VMware Telco Cloud Operations connects to vRealize Operations to get events, topology information, and metrics.

Assessing compliance with line-item security requirements

vRealize Network Insight works with NSX Data Center to help assess compliance with telecommunications security requirements for the virtualization plane and its management. For example, vRealize Network Insight displays routing information for multi-tenancy and micro-segmentation, shows firewall rules and logical routers, and describes IPFIX flows.

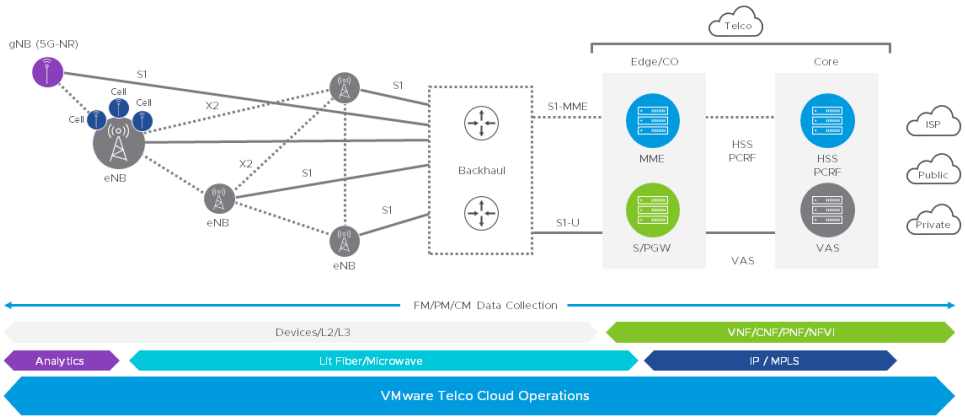


Figure 6: This diagram illustrates how VMware Telco Cloud Operations monitors the layers of a 5G network to help protect availability, integrity, and confidentiality.

Proactively identifying anomalies

vRealize Network Insight provides layer 2, 3, and 4 visibility into the virtual and physical networks, and it can help you identify network anomalies and security policy gaps. The engine is integrated with the NFVI networking fabric to capture device and network configurations, IPFIX flow, and SNMP. vRealize Network Insight gives you visibility into traffic routing, sources and destinations, micro-segmentation, and possible security violations.

VMware Telco Cloud Operations monitors all layers of the telco stack, both physical and virtual, for rapid insights into issues through its root-cause analysis engine. The host-based configurations and asset management information from VMware Telco Cloud Operations can be manually correlated with logging data from Log Insight to help investigate an anomaly.

Crucially, the combination of vRealize Network Insight and VMware Telco Cloud Operations enables you to monitor interfaces between networks that operate at different trust or sensitivity levels to help detect aberrant traffic.

Detecting unexpected changes to network equipment

VMware Telco Cloud Operations performs host-based configuration management and monitoring to help detect unexpected or unauthorized changes to network equipment and their settings. If a software or firmware release is out of date, VMware Telco Cloud Operations triggers an alert and can initiate automated updates if configured to do so. If a physical change adversely affects the network, VMware Telco Cloud Operations shows the issue's root cause and can trigger service workflows through integration with OSS tools, such as ServiceNow.

Protecting the Signaling Plane

A key risk in the signaling plane is receiving malicious data. VMware supplies the basis for one approach to reduce the risks involved in a signaling attack: After virtualizing the core network by using VMware technology, you can use NSX to segregate the core network by the services they offer, such as network slicing with 5G.

Cloud Native Approaches to Core Network Security

The primary areas of an environment that need to be considered for a secure cloud native environment are infrastructure, clusters, development, and workloads. Automation and orchestration help apply and optimize network security, and they are a clear recipe for

SECURITY FOR CNFS

As you work to develop and deploy containerized network functions (CNFs), you should consider how to secure the container lifecycle. Adopting 5G technology carries new risks and exposes systems to new threats. How will you do the following?

- Protect CNFs as they move through a continuous integration and deployment (CI/CD) pipeline
- Implement a trusted container image registry with role-based access control and vulnerability scanning
- Inspect containers against security benchmarks
- Automate security patching of containers
- Isolate, protect, and monitor the communications of CNFs and microservices
- Enforce policies governing CNF connectivity
- Protect your CNF supply chain by establishing end-to-end security from code provenance to CNFs running in production
- Embrace DevSecOps and new security principles to address emerging threats

VMWARE TELCO CLOUD AUTOMATION AT A GLANCE

VMware Telco Cloud Automation accelerates time to market for network functions and services while igniting operational agility through simplified automation—across any network and any cloud. VMware Telco Cloud Automation orchestrates and automates network functions in any format (physical, virtual, and containerized) and from any vendor whose functions comply with SOL001/004.

KEY BENEFITS

- Accelerate time to market of network functions and services.
- Gain operational efficiencies and avoid error-prone manual tasks.
- Enhance the service experience through workload mobility, dynamic scalability, closed-loop healing, and improved resilience.
- Improve service quality with integrated AI-driven workflows when you also use VMware Telco Cloud Operations.
- Optimize cloud resource utilization through VMware NFVO, G-VNFM and VIM/NFVI integrations.
- Use Kubernetes and cloud-native patterns.
- Minimize version validation efforts.

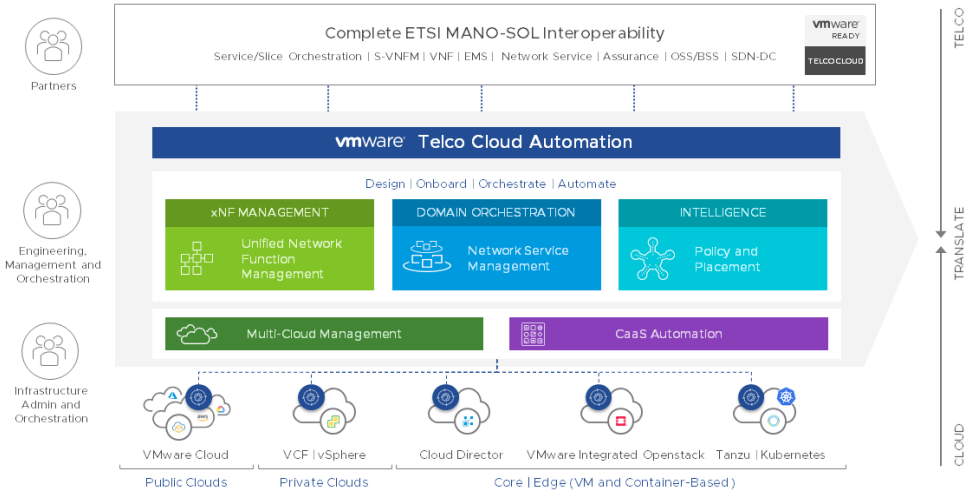


Figure 7: The capabilities of VMware Telco Cloud Automation.

achieving network transformation in the face of complex telco networks moving toward 5G and cloud network functions.

VMware Telco Cloud Automation puts in place orchestration and automation that can help secure telco network services and functions, including cloud native network functions (CNFs) and Kubernetes. More specifically, the platform's orchestration tool can help automate as many operational procedures as possible to avoid human error and configuration mistakes.

Securely orchestrating containerized applications

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

Checklist of countermeasures for cloud native security

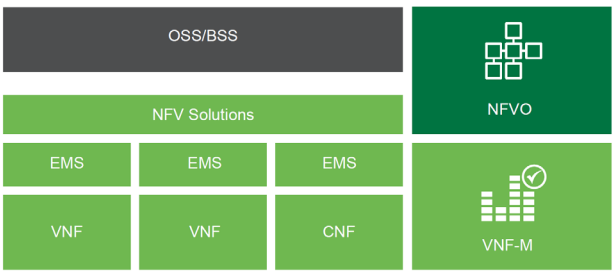
If you are implementing cloud native network functions or introducing containers and Kubernetes into your telco stack, here's a concise list of countermeasures that should be applied to the cloud native components. The checklist can help evaluate whether countermeasures are included in a platform or component by default or whether they must be put in place. In the end, however, the result should be the same: Cloud native technology that is protected from the top to the bottom with fully integrated security. 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, etc.
- 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
- Constrain network access from containers
- Profile and protect apps at runtime to ensure known good
- 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 thwart denial-of-service (DoS) attacks
- Monitor the cluster and network utilization
- Monitor for suspicious activity and analyze failed login and RBAC events
- Use recent versions of Kubernetes, which have stronger security than older versions
- Monitor configurations, such as dashboard access, for risks and vulnerabilities
- Routinely test for vulnerabilities and attack vectors by using standard tools

Conclusion: Example End-to-End Security Architecture

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.



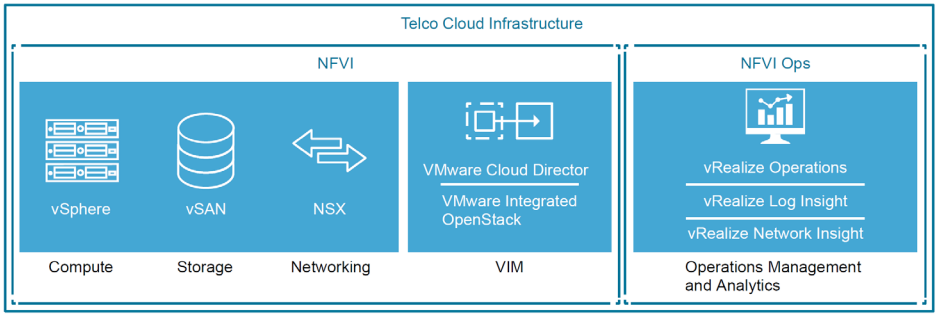


Figure 8: VMware components can be deployed in various ways to construct a comprehensive solution that meets your security goals. This example uses VMware Telco Cloud Infrastructure OpenStack Edition as the VIM and includes vSphere, vSAN, and NSX. The operational components are vRealize Operations, vRealize Log Insight, and vRealize Network Insight. A different combination could use Cloud Director as the VIM instead of OpenStack.

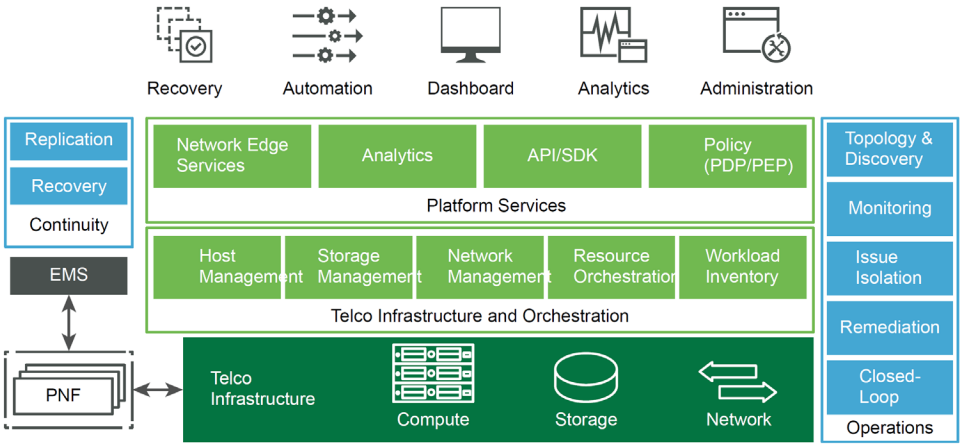


Figure 9: The logical components of VMware Telco Cloud Infrastructure.

In general, the components of VMware Telco Cloud Infrastructure can be combined to form an architecture with a core data center and multiple edge domains. This section discusses one way in which the components can be combined to create a multi-tenant architecture with quality of service and end-to-end security.

Multi-tenant consumption models and security

In this example, you can facilitate NFV transformation on a shared resource infrastructure environment with multi-tenant consumption models. Scope Multi-tenancy isolates resources and networks to deliver applications with quality. Because multiple tenants share the same resource infrastructure, secure multi-tenancy can be enabled 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 both internal and external tenants over the common shared infrastructure so tenants can deploy and operate their respective workloads and services. The result is network, compute, and storage isolation with quality of service.

Tenancy and quality of service

A unit of tenancy is called a tenant virtual data center, or vDC, within the scope of a project. A tenant vDC allows 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 defined as a composition of dedicated compute, storage, and network resources and as 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 many tenants. Services such as HSS and DNS are examples of shared tenancy. To avoid contention and starvation, compute, storage, and network isolation as well as 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 a combination of vSphere DRS and the 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 make sure that the resources are tuned and balanced dynamically.

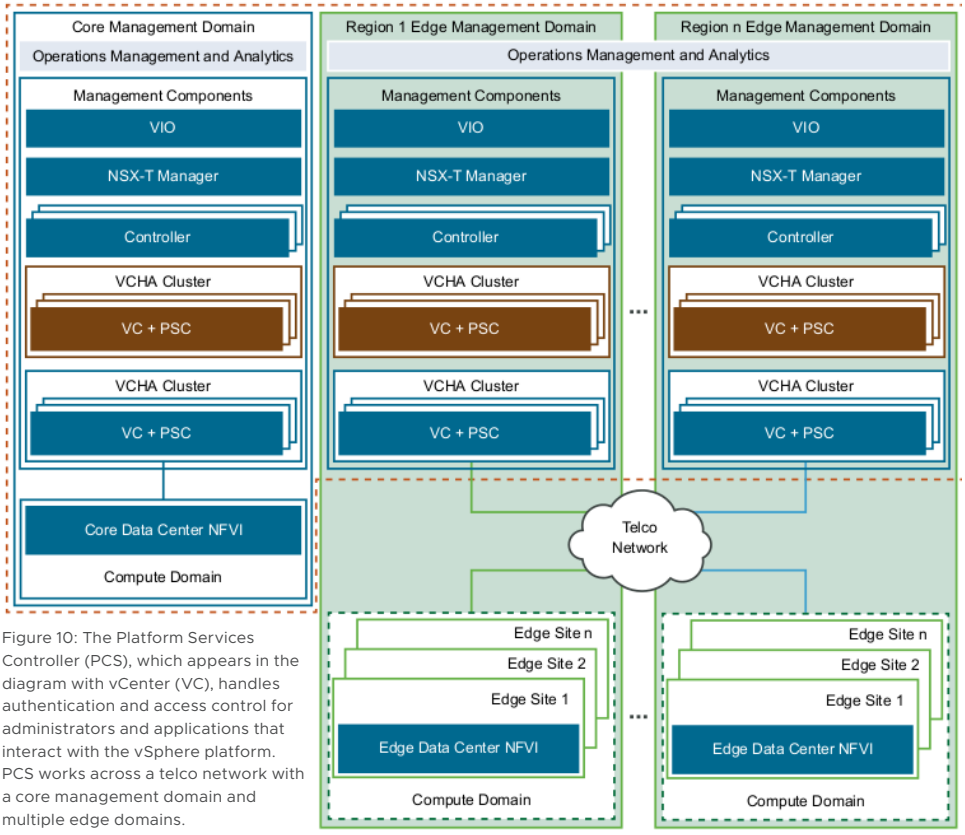


Figure 10: The Platform Services Controller (PCS), which appears in the diagram with vCenter (VC), handles authentication and access control for administrators and applications that interact with the vSphere platform. PCS works across a telco network with a core management domain and multiple edge domains.

Authentication and access control

The vSphere platform includes a component called the Platform Services Controller. It 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, which can securely connect to LDAP or Microsoft Active Directory for identity management, handles authentication and access control for administrators and applications that interact with the vSphere platform. The Platform Services Controller may be deployed as a load-balanced pair of appliances for each vCenter Server.

Management plane

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

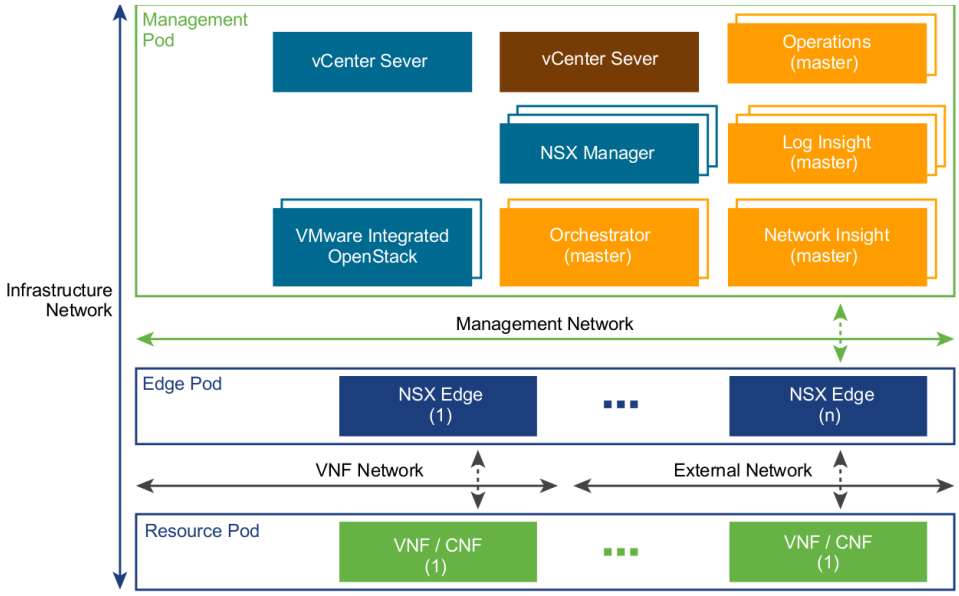


Figure 11: For security, the management pod and its functions are isolated from other elements of the telecommunications network, including the virtualized infrastructure.

resources as well as VNF onboarding. RBAC empowers you to implement the principles of least privileges and separation of duties in a hierarchy of tenants.

Compute isolation

Allocation of compute and storage resources ensures that there is an optimal footprint available to each tenant, with room for expansion 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.

The 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

The networking model of NSX-T Data Center fully isolates and secures the traffic paths across workloads and the tenant switch and 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, with logical Tier-0 routers defining and isolating the provider tier and logical Tier-1 routers defining and isolating the tenant tiers.

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

Each tenant vDC will have 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 plumbed to multiple logical interfaces for layer 2 and layer 3 connectivity.

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

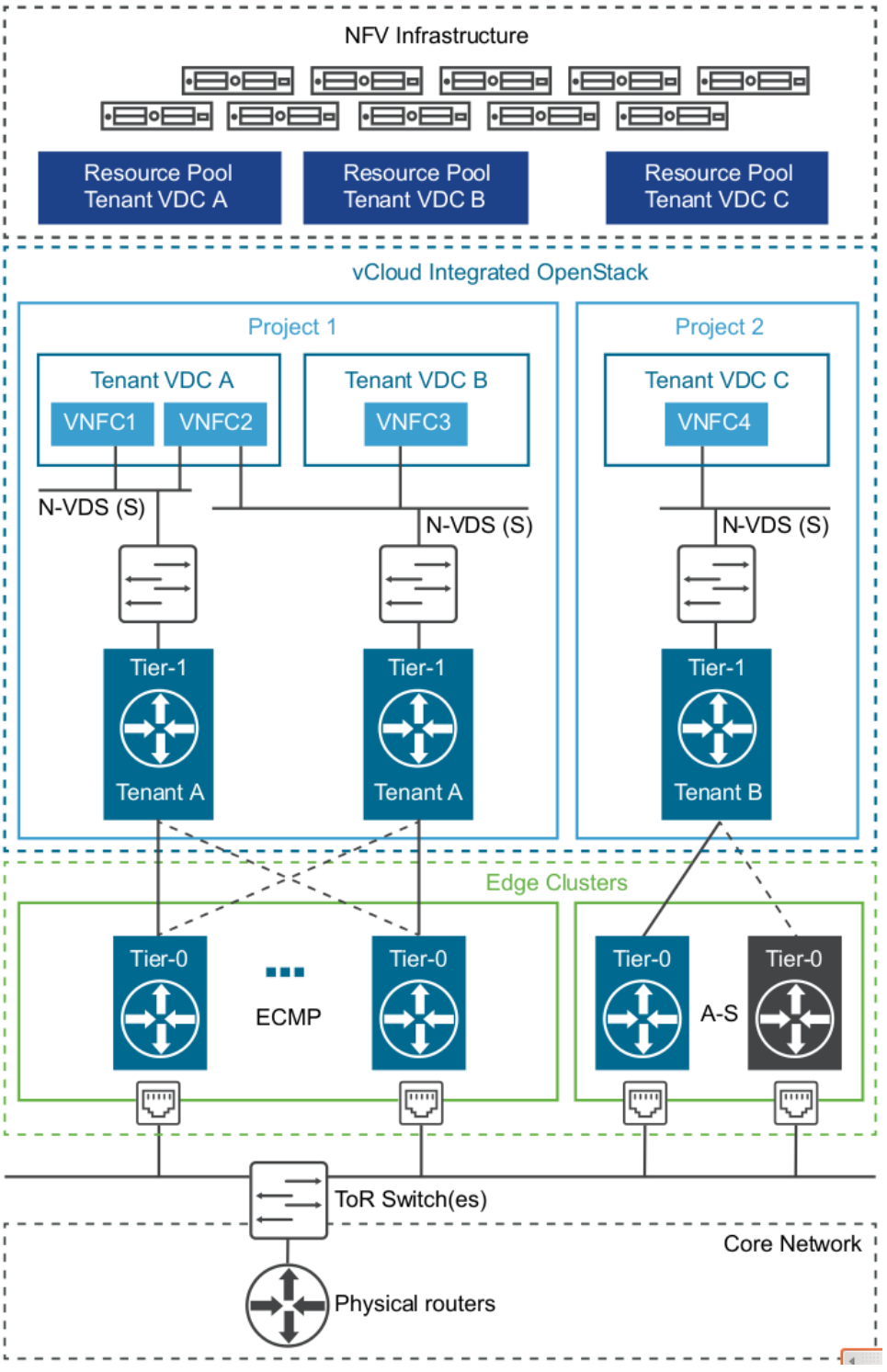


Figure 12: NSX-T Data Center uses a two-tiered routing architecture for network management, with logical Tier-0 routers defining and isolating the provider tier and logical Tier-1 routers defining and isolating the tenant tiers. The provider routing tier connects to the physical network for north-south traffic, and the tenant routing context can connect to the provider Tier-0 and manage east-west communications. The Tier-0 provides traffic termination to the cloud physical gateways and existing CSP underlay networks for inter-cloud traffic communication.

SECURITY BEST PRACTICES

Even with intrinsic security, best practices for security are still required. At a minimum, security best practices include the following:

- Identify and disable unnecessary functionality and software
- Identify interfaces that are not needed or wanted
- Remove all unnecessary accounts
- Follow the principles of least privilege and separation of duties for service and administrator accounts
- Disable unnecessary network services
- Audit open ports and their uses
- Harden virtual machines, hypervisors, and other components
- Conduct penetration testing on a regular basis

Secure multi-tenancy and the VIM

Together, the vCenter Server, NSX Manager, and the VIM form a secure multi-tenant platform. vCenter Server lets you allocate and partition compute and storage resources with precision, and 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, all of which can be used to isolate and secure network resources and services.

The VIM lets you create additional abstraction layers by dividing 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 first mapped to NFVI virtual resources—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. From there, you can reserve and allocate resources for tenants by using an organizational-level virtual data center.

Every organizational virtual data center can map to an underlying resource pool within the parent provider cluster. The resource settings of the resource pool are managed from the VIM according to the allocation settings of the organizational virtual data center to set aside resources without exceeding the resource limits.

Tenant edge devices that are deployed from the VIM can 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 data center. This separation of edge devices and VNF workload resources prevents one from starving the other.

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

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

Embedded analytics, monitoring, and intelligence for security assurance

The vRealize suite enriches the management pod with security assurance. vRealize Network Insight lets you visualize and plan micro-segmentation and security policy distribution into NSX-T to impose and enforce security across the virtual infrastructure. In general, the solution can monitor the infrastructure to help detect security policy violations.

Intrinsic Security

Security like this that is built into the software and infrastructure improves visibility, reduces complexity, and focuses your defenses by enabling you to apply and automate adaptive security measures like micro-segmentation in the right place. In this way, the VMware Telco Cloud emphasizes intrinsic security—integrated with the software and infrastructure so that security is programmable, automated, and context-aware.

References and Resources

Security Analysis for the UK Telecom Sector: Summary of Findings, by the National Cyber Security Centre, 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, Published 28 January 2020.

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

vSphere Security, December 2019.

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 2.4 Security Configuration Guide

vSphere Security Documentation, Guides, and Resources

Understanding vSphere Hardening and Compliance

Create an IP Pool with VMware NSX Data Center for vSphere

Security Considerations for Log Insight

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.

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

About the VMware Telco Cloud

VMware helps communications service providers build, operate, monetize, and protect their telco cloud. Our technology empowers CSPs to transform their networks into a 5G force, accelerate the delivery of innovative services, and compete in a multi-cloud world.

The VMware telco cloud creates a consistent foundation for operating all generations of cellular and fixed-line technology while leading the way to 5G adoption. Solutions for infrastructure, orchestration, automation, assurance, optimization, and security modernize your network from the core to the edge and RAN. VMware powers more than 100 telco networks in production worldwide. Customers such as Vodafone, Telia, and Millicom are deploying new services much faster while cutting OpEx by as much as 50 percent and CapEx by as much as 60 percent.

At the dawn of 5G, the VMware Telco Cloud combines consistent infrastructure with intrinsic security to give CSPs a strong foundation for digital transformation and rapid innovation.

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel 877-486-9273 Fax 650-427-5001 www.vmware.com Item No: vmw-telco-security-wp 3/21