Intrinsic Security for Telco Clouds

Protect infrastructure with built-in measures

VMWARE TELCO CLOUD AT A GLANCE

We help communications service providers build, manage, and protect telco cloud infrastructure to transform their networks, accelerate the delivery of modern services, and thrive in a multi-cloud world.

Our consistent infrastructure establishes a modern foundation for operating all generations of cellular and fixed-line technology. Solutions for automation, visibility, and optimization light up the path to launching 5G networks and monetizing 5G services.

With the VMware Telco Cloud, the imposition of security is adaptive, automated, and context-aware so CSPs can quickly and economically capitalize on new market opportunities while improving the security of their virtualized network and its management.

IDENTIFYING 5G SECURITY RISKS AND REQUIREMENTS

Three standard-setting papers identify the key security risks and requirements for CSPs transitioning to 5G:

- *Security Analysis for the UK Telecom Sector: Summary of Findings*, by the U.K. National Cyber Security Centre, published in January 2020.
- *5G PPP Phase 1 Security Landscape*, published by the 5G PPP Security Working Group in June 2017.
- *Cybersecurity of 5G networks EU Toolbox of risk mitigating measures*, published by the European Commission in January 2020.

Introduction

In a landmark analysis at the dawn of 5G, the United Kingdom's National Cyber Security Centre published a January 2020 paper that recommends the establishment of a new set of telecommunications security requirements, or TSRs, that are intended to drive communications service providers (CSPs) to operate secure networks.

"The potential economic and social benefits of 5G and full-fibre digital connectivity," the NCSC's report says, "can only be realised if we have confidence in the security and resilience of the underpinning infrastructure."

The use of network functions virtualization and the transition from 4G networks to 5G, coupled with pressure to protect customer information, increases the complexity of the security landscape for CSPs. The combinatorial nature of 5G, in which service providers can mix elements of 4G and 5G networks, can result in an uneven application of network security measures, which are likely to evolve and shift as the network combines various 4G and 5G elements. The use of public clouds will likely intensify the importance of centralized management and monitoring.

Security 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.

Risk Factors and Attack Vectors

Security risks and requirements are shifting as telecommunications providers transition to 5G networks and increasingly rely on virtualization and cloud computing, including network functions virtualization, containers, and Kubernetes.

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 more attack vectors. Containers shift the security burden to virtual machines and the development and operations lifecycle. Kubernetes and cloud native architectures require security enhancements to lock down API interfaces, manage microservices, and protect network end points.

The shift to 5G thus brings new or heightened security risks:

- Unauthorized access or usage of assets
- Identity cloning to gain access to sensitive resources
- Fraudulent use of shared resources
- Modification of subscriber credentials
- Undetected alterations to the control plane or the user plane

"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

- Weak slice isolation, which could expose sensitive data to applications running in other slices through side-channel attacks
- Difficulties in managing vertical SLAs and regulatory compliance

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. There are also risks specific to the virtualization plane:

- 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
- Traffic capturing rerouting because of recursive or additive virtualization
- 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 hosts and virtual workloads, potentially compromising the whole network and affecting the availability and confidentiality of critical services

Key security imperatives for reducing risk

These risks and attack vectors give rise to key security imperatives for protecting the virtualization plane, securing the management plane, and monitoring and auditing infrastructure and operations. Reducing risk relies on your ability to do the following:

- Keep the virtualization fabric, container images, and VMs up to date and patched.
- Maintain the virtualization fabric en masse and at scale.
- Implement mitigations that neutralize known attack vectors.
- Isolate hypervisors and VMs with security domains and pools to prevent movement.
- Protect sensitive data through segmentation of workloads and storage.
- Encrypt data in transit and at rest.
- Architect the virtualized infrastructure by using automated provisioning, automated management, secure administration, and micro-segmentation.
- Isolate the management of the virtualization plane from other systems and networks.
- Strictly control access to and use of the virtualization plane's management layer by using the principles of least privilege and separation of duties.
- Monitor and audit the virtualization plane.
- Track access and changes to the management layer.

A higher-level risk stems from the perceived cost of implementing security controls for some of these attack vectors.

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."

Because prioritizing performance and revenue over security heightens risk and exposes more attack surface, such a trade-off could prove damaging in the long run. Improving security by investing in performance might, in the end, increase the return on investment in the additional infrastructure. "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*.

5G SECURITY RISKS AND THREATS

A 2017 white paper by 5G PPP Security Working Group identified 5G-specific 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."

VMWARE TELCO CLOUD INFRASTRUCTURE AT A GLANCE

VMware Telco Cloud Infrastructure is a consistent, fully integrated, modular, multi-tenant infrastructure solution powered by field-proven compute, storage, networking, and management to simplify, scale, and protect telco cloud services. It can isolate multiple tenants within the same NFV infrastructure.

SECURE MULTI-TENANCY

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 secure multi-tenant environment across network functions through the following means:

- NSX micro-segmentation with fine-grained access controls for provider and tenant administrators
- Secure integration with the VIM
- Delegated role-based access control
- Tenant-level operations management and visibility
- Security policies that can be applied consistently to objects across multiple VMware vCenter services

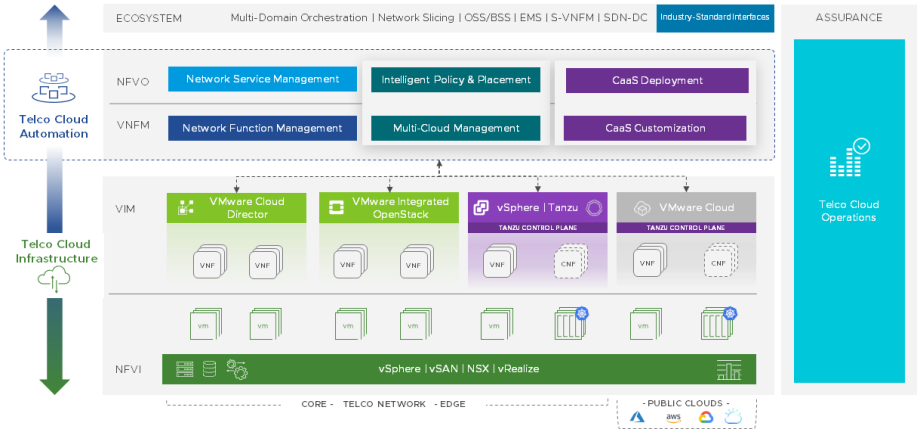

FIGURE 1: The VMware Telco Cloud includes three main products: VMware Telco Cloud Infrastructure, VMware Telco Cloud Automation, and VMware Telco Cloud Operations. A fourth product—VMware Telco Cloud Platform—combines VMware Telco Cloud Infrastructure with VMware Telco Cloud Automation into a cloud-native platform that runs and protects CNFs and VNFs on any cloud with visibility, orchestration, and operational consistency.

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:

- Telco Cloud Operations
- Telco Cloud Automation
- Telco Cloud Infrastructure

Operations

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

Automation

This layer includes VMware Telco Cloud Automation, which orchestrates network functions, services, containers, 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 choose VMware Cloud Director or VMware Integrated OpenStack—let you impose role-based access control in a large-scale, multi-tenant telecommunications network.

Infrastructure

The foundation of the VMware Telco Cloud supplies infrastructure as a service with the following virtualization technology:

- VMware vSphere®
- VMware NSX® Data Center
- VMware vSAN™

To help CSPs that are implementing 5G or transitioning to 5G by establishing a non-stand-alone 5G and 4G network, VMware Telco Cloud Infrastructure includes vSphere, NSX, and a VIM. VMware vSAN can optionally be added to this stack to supply distributed storage. This foundation empowers you to build, run, and manage containerized services by using Kubernetes and other cloud native technology.

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.

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

The VMware Telco Cloud lets you deploy, manage, automate, and protect network functions and services on consistent infrastructure with consistent operations.

Protecting the Virtualization Fabric

VMware addresses telecom security requirements for the virtualization fabric by implementing and automating controls, encryption, and policies that protect virtualized infrastructure, including hypervisors, virtual machines, virtual networks, and management functions. With VMware technology, intelligent automation can define, deploy, adapt, and remediate security policies based on your dynamic applications.

Segmenting network traffic with automation

VMware NSX provides network virtualization for a software-defined data center, abstracting Layer 2 through Layer 7 networking functions—such as switching, firewalling, and routing—on top of an existing physical network.

Virtual firewalls can be combined with micro-segmentation and dynamic security policies to separate and protect all types of network traffic, virtual machines, containerized applications, and workloads. Where necessary, third-party firewalls that work with VMware virtualization solutions can be incorporated to help meet uncommon performance requirements.

The ability to segment network traffic supplies the basis for one approach to reduce the risks involved in receiving malicious data: After virtualizing the core network by using VMware technology, you can use VMware NSX to segregate the core network by the services they offer, such as network slicing with 5G.

Programmatically encrypting data at rest and in transit

vSphere and vSAN can store data at rest and in transit to prevent the exfiltration of data. Encryption is available through software policies that are independent of the operating system and applications while maintaining operational efficiencies inherent in the vSphere platform and preserving the security of the virtual machine.

Encryption is performed by the industry-standard OpenSSL libraries and algorithms described in *VMware vSphere Virtual Machine Encryption: Virtual Machine Encryption Management*.

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.

Keeping the virtualization fabric patched and up to date

Our update manager centralizes patch and version management for VMware vSphere and supports VMware ESXi™ hosts and virtual machines. Health checks automatically track the health of the vSphere environment, including possible security-related vulnerabilities in VMware vCenter Server® and ESXi, to help ensure that the fabric is up to date and patched.

The VMware virtualization fabric can be updated without affecting its availability. The virtualization fabric can also be updated without affecting VNFs if the VNFs have been built with a fail-over capability, an active-active pattern, or another pattern that allows them to be moved with automation.

VMware Security *Advisories* and *Alerts* address remediation for vulnerabilities reported in VMware products. The VMware *Security Response Policy* documents our commitments for resolving possible vulnerabilities to correct any such issues in a timely fashion. VMware will release a fix for the reported vulnerability.

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

PATRICK DONEGAN, PRINCIPAL ANALYST, HARDENSTANCE

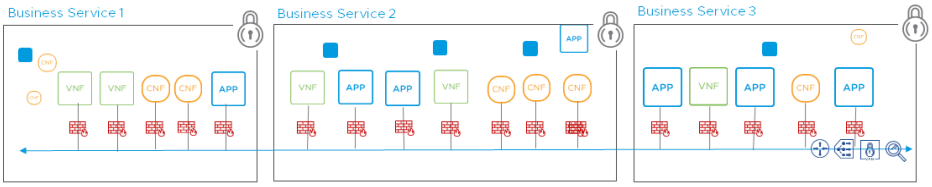

FIGURE 2: Distributed firewalls and micro-segmentation can isolate VNFs, CNFs, and services.

Blocking access to the underlying hardware

To protect the foundation of the virtualization plane, vSphere establishes a fully abstracted virtualization layer by using the ESXi hypervisor, which bars virtual workloads from gaining gain access to the underlying hardware.

Adding only attested hosts to the fabric

You can use host profiles and the Preboot Execution Environment (PXE) to add only known hosts to the virtualization fabric. VMware cryptographically attests hosts with secure boot. In vSphere, hardware roots-of-trust support Secure Boot for physical hosts to ensure that only digitally signed code is allowed to run. Secure boot is part of the UEFI firmware standard; with it enabled, a machine refuses to load a UEFI driver or application unless the bootloader is cryptographically signed.

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. Network security teams can prevent threats from moving laterally within their environments by, for example, creating security groups, which can include dynamic membership criteria defined by security tags and be governed by a security policy.

Similarly, a security pool of virtual machines can act as edge hosts to run public-facing VNFs in a DMZ, reducing exposure and simplifying monitoring of external network interfaces. NSX security groups, tags, policies, and other capabilities can also isolate virtual workloads in trust domains by their risk and sensitivity levels.

Protecting the Management of the Virtualization Plane

The VMware architecture for the management plane puts in place a trusted foundation upon which management elements, including the administrative network and the VIM, can be isolated from other aspects of the virtual infrastructure. The architecture sets the stage for successfully controlling and monitoring administrative access.

Management plane components, such as a VIM and VMware Telco Cloud Automation, can reside in a trusted location segmented from the virtualization fabric. Virtual firewalls, micro-segmentation, and security groups protect the trust domain.

The management interfaces use secure, encrypted channels to administer VMs, virtual network functions, and the ESXi hypervisor. Advanced security policies and rules can be applied at the VM boundary to further control access to the management plane.

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 VMware Telco Cloud *Reference Architecture*.

CRITICAL SECURITY FUNCTIONS

In its summary of findings, the NCSC considers the following functions to be critically sensitive:

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

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

PROTECTING CONTAINERS WITH STRONG SECURITY BARRIERS

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

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

Isolating and protecting critical security functions

It is key to limit the attack surface of critical security functions. Within the VMware virtualization fabric, you can segregate security functions to reduce risk by using a separate vSphere cluster. NSX can then further isolate security functions in their own trust domain by implementing context-aware virtual firewalls and applying adaptive micro-segmentation, which means that each workload can be individually isolated and protected.

VMware components of the management plane, such as the VIM and vCenter, can authenticate and authorize users with Microsoft Active Directory or LDAP. Critical security functions can be secured by role-based access control that applies the principles of separation of duties and least privilege.

A VIM from VMware securely integrates with vSphere, NSX, and vSAN for a single, secure management plane. Multi-factor authentication can be added for ESXi, vCenter, and Cloud Director. Access to VMware Telco Cloud Automation is also secured with role-based access control to limit access to NFVO, VNFM, VNF Designer, and the API.

Monitoring and Auditing Infrastructure and Operations

The VMware Telco Cloud integrates with an operations management suite for monitoring and remediation of the NFVI and VNFs. The platform provides continuous, context-aware visibility over service provisioning, workload migrations, auto-scaling, elastic networking, and network-sliced multi-tenancy across VNFs, hosts, clusters, and sites.

Alerts can flag configuration and compliance gaps and security vulnerabilities. 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 and traffic routes.

The following tools combine to provide context-aware analysis of network data, topologies, routes, and traffic:

- vRealize Operations Manager.
- vRealize Log Insight.
- vRealize Network Insight.
- VMware Telco Cloud Operations.

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. 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.

Conclusion

With the VMware Telco Cloud, security is intrinsic—integrated with the software and infrastructure to make security programmable, automated, adaptive, and context-aware. The result improves visibility, reduces complexity, and focuses defenses.

LEARN MORE

For more information about the VMware Telco Cloud, call 1-877-VMWARE (outside North America, dial +1-650-427-5000) or visit *https://telco.vmware.com/*