WHITE PAPER–NOVEMBER 2021

Security for Open RAN Architectures in 5G Telco Clouds

Protecting Open Radio Access Networks with Automation and Zero-Trust Architectures

vmware®

Table of Contents

Executive summary

Security risks and requirements are shifting as CSPs transition to 5G networks and an open RAN. 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 used in the radio access network (RAN) shift the security burden to virtual machines or the container runtime engine and the development and operations lifecycle. Kubernetes and cloud-native patterns require security enhancements to lock down API interfaces, manage microservices, and protect network end points.

This VMware white paper explains how VMware technology addresses the security risks and requirements that communications service providers face as they transition to open radio access networks by adopting virtualization, containerized network functions (CNFs), Kubernetes, and multi-cloud networks.

To protect the RAN for 5G, several guiding principles are applied:

- Open systems and open interfaces
- Multi-vendor networks
- Risk and threat assessment
- Zero-trust architecture
- Micro-segmentation
- Isolation of the management plane and other critical security functions
- Automation of security measures and automated management of security controls
- Roots of trust and code provenance
- Vulnerability management
- Strong security boundaries, especially those provided by virtual machines

IDENTIFYING OPEN RAN SECURITY RISKS AND REQUIREMENTS

To identify solutions for the security risks and requirements of an open RAN, this white paper relies on several standard-setting papers and the publications of standards organizations:

- Security Analysis for the UK Telecom Sector: Summary of Findings, by the National Cyber Security Centre of the United Kingdom, 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.
- The O-RAN Alliance, its architecture, and the publications of its security focus group.
- The publications of the Open RAN Policy Coalition.
- U.S. NIST Special Publication 800-207, Zero Trust Architecture.
- National Strategy to Secure 5G Implementation Plan of the National Telecommunications and Information Administration (NTIA) of the U.S. Department of Commerce.

Security Problems amid a Shifting RAN Landscape

With the shift toward 5G, the size of the radio access network is expanding significantly. With 5G, the RAN becomes denser with sites and systems from multiple vendors. As the number of edge locations, base stations, and antennae increases, so do the number of interfaces, attack vectors, and risks. The need to secure the RAN for 5G becomes paramount.

New use cases heighten the need to improve security. Customized on-demand services, enhanced mobile broadband (eMBB), massive machine-type communications (mMTC), and ultra-reliable low-latency communications (URLLC) all call for new or expanded security capabilities.

These changes in size, access, use cases, and the distribution of responsibilities contribute to a litany of security problems facing radio access networks for 5G.

Open RAN, the charge to disaggregate and open the RAN led by O-RAN Alliance, further shifts the responsibility for security to CSPs, which might in turn have to distribute security responsibilities across multiple vendors, segments, and possibly clouds. As a result, the number of technicians, contractors, and system administrators who need access, either remotely or on-site or both, is set to increase correspondingly with the growth of the RAN.

New approaches and components require a shift in focus.

5G, Virtualization, and the Path to Open RAN Security

An open radio access network seeks to adopt the industry trajectory toward virtualization and software-defined networking. The standards for 5G point toward a cloud-native future, and part of that future lies in a vision to disaggregate the RAN. Virtualization and

"From a security perspective, software-based networking and virtualization enables techniques such as sandboxing, microsegmentation, containerization, and network slicing. There are also important trust and security capabilities of virtualization enabled by modern hardware and processors. The end result is that through the advancements of hardware and virtualization, operators have more tools to ensure the security and resilience of the network."

5G AND OPEN RAN SECURITY: NEXT GENERATION TRUST, THE OPEN RAN POLICY COALITION

BUILT-IN SECURITY POWERS ZERO-TRUST ARCHITECTURES FOR RAN

Through the power of virtualization, VMware builds security into its RAN platform and fosters a zero-trust architecture for open RAN.

Security that is integrated with the software and built into the infrastructure helps solve the challenges of 5G by making security programmable, automated, adaptive, and context-aware. Built-in security improves visibility, reduces complexity, and focuses your defenses by letting you apply and automate measures like micro-segmentation in the right place.

software-defined networking enable CSPs to replace costly, purpose-built RAN hardware with common, commodity servers. By virtualizing and disaggregating RAN functions, CSPs can lower cost, deploy network functions for the RAN at their optimal locations, manage the functions at scale from a central location, and automate such things as elasticity and security.

The Open RAN Policy Coalition links open RAN to improved security: "Open RAN has the potential to build upon the security enhancements already enabled by 5G and allow the operator to fully control the security of the network, ultimately enhancing the operational security of their network. One benefit is greater visibility to security events: A network operator will have direct access to more data about network performance because the components are disaggregated and connected through open interfaces."[1]

With such visibility, CSPs can more readily detect and mitigate attacks and other security problems. The visibility that accompanies an open RAN improves the assessment and management of security risks.

Virtualization and software-defined networking enable the RAN to be protected by the following advanced security techniques:

- Containerization
- Micro-segmentation and network isolation
- Automation and orchestration
- Chains of trust, from container image repositories through deployment on hardware with roots of trust and security-enhanced processors
- Network slicing
- Shifting more security capabilities from core networks closer to the 5G edge and the access points of the RAN
- Stronger end-to-end encryption

Beyond bringing new security techniques and capabilities, an open RAN architecture diversifies the ecosystem of vendors and promotes interoperability with open interfaces.

Emerging Telecom Security Standards

To identify solutions for the key security risks and requirements of an open RAN, this paper relies on several standard-setting papers and organizations:

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. ybersecurity of 5G Networks EU Toolbox of Risk Mitigating Measures, published by the European Commission in January 2020.
4. The O-RAN Alliance, its architecture, and the publications of its security focus group.
5. The publications of the Open RAN Policy Coalition, including its 2021 paper on Open RAN security in 5G.
6. U.S. NIST Special Publication 800-207, Zero Trust Architecture.
7. National Strategy to Secure 5G Implementation Plan of the National Telecommunications and Information Administration (NTIA) of the United States Department of Commerce.

Other telecommunications standards organization, including 3GPP, GSMA, ETSI, and the Telecom Infrastructure Project (TIP), also provide standards, frameworks, and guidelines for helping CSPs deliver secure 5G networks.

1 See https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf

Security standards set the stage for CSPs to architecture radio access networks and processes that can proactively protect against and rapidly respond to threats, vulnerabilities, and exploits.

Securing open systems vs. securing closed systems

Some vendors of purpose-built RAN hardware continue to fuel the misconception that open interfaces introduce security risks, a misconception that they presumably seek to promote to create the perception of a barrier to entry to RAN markets and to lock customers into their singular solution. Closed vertical stacks of purpose-built hardware are a towering problem for CSPs and, ultimately, consumers. CSPs have no visibility into the vulnerabilities and risks of a closed system. They must take it on faith that the whole vertical stack is patched, up to date, locked down, and free of vulnerabilities. When something goes wrong, though, it is the CSP that bears the burden of bad press, fines, lawsuits, and the erosion of trust.

Open RAN takes the opposite approach. It seeks to define open interfaces through technical specifications to "provide a foundation and architecture for improving security."[2]

The Open RAN Policy Coalition makes the point that "open standards help users and network operators better understand, align on, and demonstrate successful implementation of security requirements. This effectively grows the market for 5G solution suppliers as network operators have the option to choose from a variety of suppliers and providers to offer standardized interoperable solutions."[3]

In addition, when standardized open interfaces are combined with immediate public sharing of information about vulnerabilities and exploits, vendors and operators can take action to patch systems, mitigate damage, and prevent dwelling or lateral movement in a network. When a CSP's security operations team knows what is inside systems they are running, what those systems are composed of, and what there interface are, they can protect them better before an attack and respond with visibility and knowledge during an attack or when a vulnerability comes to light.

Government intervention to protect networks by requiring multiple vendors

A multi-vendor RAN stack and network is key to security. The security problems of using single-vendor RAN stack are compounded if the components are closed systems without software transparency for the operator and without rapid public announcements of discovered security vulnerabilities and their patches.

Multi-vendor environments that flourish through the adoption of standardized open interfaces and the resulting interoperability lead to better protected environments and more secure telecommunications infrastructure, so much so that federal governments are beginning to either require or support multi-vendor environments. For example, emerging 5G security standards like the telecom security requirements, or TSRs, from the U.K.'s National Cyber Security Center (NCSC) require the use of multiple vendors.

In the United States, the Cybersecurity and Infrastructure Security Agency (CISA) conducted an economic analysis of the 5G RAN market to determine whether certain policies would support supply chain innovation, new entrants, and support for trusted RAN suppliers. The CISA determined that establishing R&D grants for innovation would advance strategies to improve the supply of trusted RAN equipment, among other options.[4]

2 See https://www.openranpolicy.org/wp-content/uploads/2020/06/5G-and-Open-RAN-Security-Next-Generation-Trust.pdf
3 See https://www.openranpolicy.org/wp-content/uploads/2021/04/Open-RAN-Security-in-5G-4.29.21.pdf
4 See https://www.ntia.gov/files/ntia/publications/2021-1-12_115445_national_strategy_to_secure_5g_implementation_plan_and_annexes_a_f_final.pdf

According to the *Open RAN Policy Coalition's comments submitted to NTIA*, an open, interoperable RAN provides a secure network.

- Standards Drive Transparent and Vetted Security, Interoperability and Trust
- Cloud Architecture Ensures Resilience, Scalability and Segmentation and Allows the Introduction of Multi-Access Edge Computing (MEC).
- Segmentation, Containerization and Virtualization Provide Enhanced Security and Isolation from the Hardware Up.

In its white paper titled *5G and Open RAN Security: Next Generation Trust*, the Open RAN Policy Coalition maintains that "because an open RAN is a fundamentally open architecture, it opens the ecosystem to new suppliers, increasing the diversity of virtualized RAN solutions."[5]

Open RAN architecture and VMware Telco Cloud Platform RAN

This section presents a brief overview of the O-RAN Alliance's architecture and situates VMware Telco Platform RAN within it.

Overview of O-RAN architecture

The O-RAN Alliance's architecture extends the 3GPP's open RAN architecture to further disaggregate the radio access network. As such, the O-RAN architecture not only splits the distributed unit (DU) of the 3GPP into a DU and a radio unit (RU), it also introduces new components: the RAN intelligent controllers. These new components include some new interfaces.

The RICs are logical functions that take two forms:

- A non-real-time RIC. It is logically situated in the service management and orchestration function.
- A near-real-time RIC.

Both are virtualized or containerized components that control and optimize RAN elements and resources. The RIC accesses user context and data about user usage—sensitive data that requires extra protection—and the RIC exposes this sensitive data to RAN microservices and applications developed by vendors.

The near-RT RIC can contain extensible microservices from third-party vendors to manage RAN resources for network functions. The O-RAN Alliance calls these microservices "xApps." Similarly, the non-RT RIC can also contain applications, which the O-RAN Alliance calls "rApps."

- O-Cloud: A cloud computing platform that comprises a collection of physical infrastructure nodes meeting O-RAN requirements to host O-RAN network functions, whether virtualized or containerized, including the Near-RT RIC, the CU control plane (O-CU-CP), the CU user plane (O-CU-UP), and the O-DU. The cloud platform supports such components as operating systems, container runtimes, and management and orchestration functions.
- SMO: The Service Management and Orchestration component (SMO) manages the components and network functions of an open RAN.

The O-RAN architecture also includes the following network functions and applications:

- O-CU-CP/UP: The centralized unit of the RAN and its control plane and user plane.
- O-DU: The distributed unit of the RAN.
- O-RU: The radio unit processes radio frequencies from antennas and other equipment.

5 https://www.openranpolicy.org/wp-content/uploads/2020/06/5G-and-Open-RAN-Security-Next-Generation-Trust.pdf

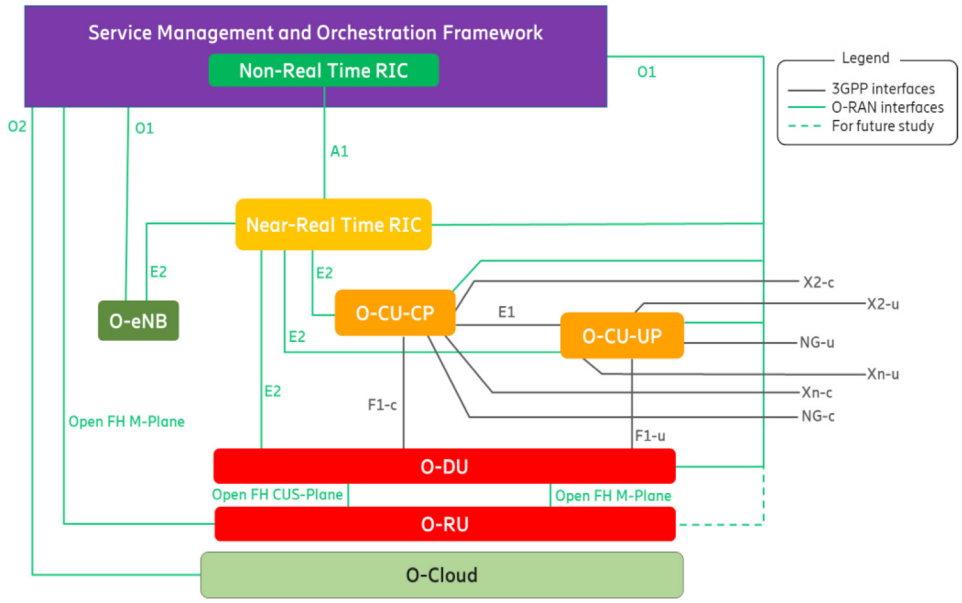

Figure 1: The O-RAN logical architecture and interfaces.

- O-eNB: The open evolved NodeB refers to hardware supporting 4G RAN.

In the O-RAN architecture, the following interfaces come into play; some of them are specified by the 3GPP:

- A1 Interface between Non-RT RIC and Near-RT RIC to enable policy-driven guidance of Near-RT RIC applications and functions and to support AI/ML workflowS
- O1 Interface connecting the SMO to the Near-RT RIC, one or more O-CU-CPs, one or more O-CU-UPs, and one or more O-DUs
- O2 Interface between the SMO and the O-Cloud
- E2 Interface connecting the Near-RT RIC and one or more O-CU-CPs, one or more O-CU-UPs, one or more O-DUs, and one or more O-eNBs
- Open Fronthaul CUS-Plane Interface between O-RU and O-DU
- Open Fronthaul M-Plane Interface between O-RU and O-DU as well as between O-RU and SMO

By supporting virtualized and containerized network functions, these interfaces let you apply security controls with micro-segmentation and other techniques.

Some of these components, network functions, or interfaces are irrelevant to VMware Telco Cloud Platform RAN because they are governed by the components or network functions of vendors. The next section situates VMware Telco Cloud Platform in the O-RAN Alliance architecture. Later sections describe the security principles and security measures that VMware technology can implement to apply and automate security for an open RAN.

VMware Telco Cloud Platform RAN and the O-RAN Alliance Architecture

In the O-RAN architecture, VMware Telco Cloud Platform RAN or VMware Telco Cloud Automation supply aspects of the cloud computing platform (O-Cloud), the service management and orchestration system (SMO), and the ability to connect these components with other components, clouds, and network functions, including the CU, the

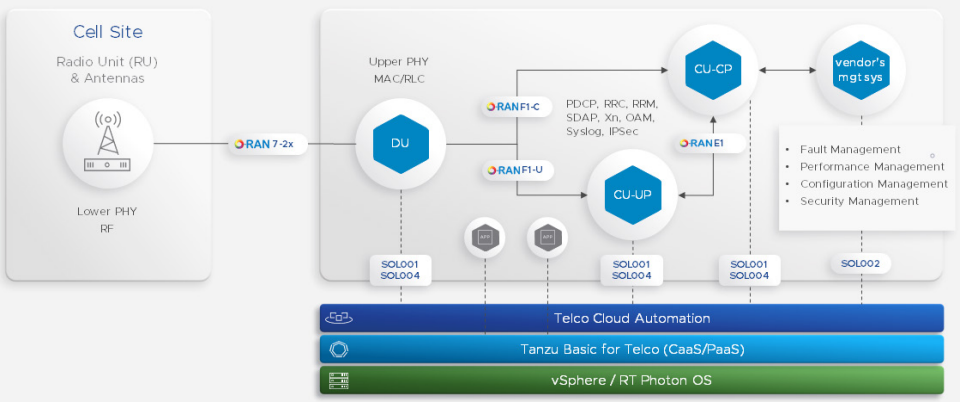

Figure 2: The O-RAN logical architecture and interfaces with VMware Telco Cloud Platform RAN running the CU, DU, and other RAN components from a hypothetical vendor.

DU, and the RICs. VMware Telco Cloud Platform RAN runs DUs, CUs, and virtualized baseband functions in accordance with stringent RAN performance and latency requirements. VMware Telco Cloud Platform RAN automates lifecycle management of Kubernetes clusters, RAN functions, and 5G services. The platform also optimizes the placement of DUs and CUs through programmable resource provisioning.

VMware Telco Cloud Platform RAN includes a security-hardened Linux host called Photon OS that is optimized for running containers on VMware vSphere.

VMware Telco Cloud Operations and VMware RIC can optionally be added to a RAN stack to supply subsets of SMO.

Risks, Threats, and Vulnerabilities in an Open RAN

Security risks and requirements are shifting as CSPs transition to 5G networks. 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 expose more attack vectors. Containers used in the RAN shift the security burden to virtual machines and the development and operations lifecycle. Kubernetes and cloud-native patterns require security enhancements to, for example, lock down API interfaces, manage microservices, and protect network end points.

Like any other telecommunications system, an open RAN faces security challenges, including similar challenges to those faced by existing RAN systems. With more devices being able to connect with a 5G network through the RAN, there is a greater need to thwart denial of service attacks and attempts to subvert authentication systems.

With a standalone 5G system, the trust model has also evolved. The 3GPP has noted that trust within the network for a standalone 5G system can be seen as decreasing as aspects of the system move farther away from the core, and this change in the trust model can affect the risk profile for the RAN, especially for DUs deployed in the public domain. CUs are seen as being deployed at sites with more restricted access.[6]

With a non-standalone 5G system that also supports different access networks, including previous generations like 4G, the non-standalone system will inherit many of the risks of those previous generations. As such, rigorous threat modeling and risk analysis will be required for the RAN by industry groups creating specifications, such as the O-RAN Alliance, and by CSPs implementing radio access networks for 5G.

6 See https://www.3gpp.org/news-events/1975-sec_5g

VMWARE TELCO CLOUD PLATFORM RAN

VMware Telco Cloud Platform RAN is optimized to run virtualized baseband functions, virtualized distributed units (vDUs), and virtualized central units (vCUs) in accordance with RAN performance and latency requirements. VMware Telco Cloud Platform RAN paves a clear path to RAN modernization by enabling CSPs to evolve from their traditional RAN to vRAN and, eventually, open RAN.

KEY BENEFITS AND CAPABILITIES

- Optimize the placement of DUs and CUs through programmable resource provisioning
- Use the same common platform to virtualize the RAN now and migrate to open RAN in the future
- Deploy and operate both RAN and non-RAN workloads on a horizontal platform
- Transform the RAN into a 5G multi-services hub
- Use a security-hardened Linux host called Photon OS optimized for running containers on VMware vSphere®
- Automate lifecycle management of infrastructure, Kubernetes clusters, vRAN functions, and 5G services

VMWARE RAN INTELLIGENT CONTROLLER (RIC)

Combined with VMware Telco Cloud Platform RAN, VMware RIC paves a simple, flexible path toward open RAN without disrupting your business operations or overhauling your network design. With VMware RIC, you can build an integrated open RAN with solutions from a vibrant ecosystem of partners while providing RAN programmability and intelligence. The VMware hypervisor continues to deliver operational flexibility and layers of security. The VMware RIC SDKs power a rich application ecosystem to enable you to quickly create innovative services that maximize business growth. Centralized RAN Intelligence simplifies RAN operations and optimizes network utilization.

Risks and attack vectors in an open RAN

Here are some risks and attack vectors that deserve special attention in an open RAN:

- The major supply-chain attacks on commercial software vendors during the past two years heightens the need for vendors and CSPs to use secure development processes, DevSecOps approaches, end-to-end protection for CI/CD pipelines, signed code provenance, and other forms of protection.
- The use in the RAN of emerging technology like artificial intelligence can introduce new risks and expose new attack vectors.
- The rise of IoT and the proliferation of connected devices increases the risk of attacks by compromised devices.

Potential risk and vulnerabilities in O-RAN

The O-RAN Alliance's architecture for an open RAN potentially includes additional risks or potential vulnerabilities:

- The disaggregation of the CU and DU presents a potential new attack vector in the open fronthaul interface that operates in the lower-layer split (LLS) interface.
- Unauthorized access to a component or a control or user plane, such as the DU or the CU control plane, to degrade RAN performance or attack network availability
- Disabling over-the-air ciphers to eavesdrop on traffic.
- Strict latency requirements can affect how security controls like encryption are implemented and managed on the Open Fronthaul Interface.
- An O-RAN architecture includes a real-time intelligent controller. The RIC is a new component that accesses user context and data about user usage -- sensitive data that requires extra protection. The RIC exposes this sensitive data to RAN applications developed by multiple vendors. Another potential vulnerability is Near-RT RIC conflicts with O-gNB, or conflicts between third-party applications.
- RAN applications and microservices running in or connected to the near-real time and the non-real-time intelligent controllers, or RICs require code signing, isolation, secure lifecycle management and patching, vulnerability management and scanning, monitoring, and tight security controls to protect access to network and subscriber data.

Vulnerabilities and exploits that can be exposed with insufficient security

Vulnerabilities also arise if components, network functions, or applications are deployed without following security best practices:

- Disaggregation can present vulnerabilities if hardware roots of trust and code provenance are not in use.
- Unprotected or poorly isolated management interfaces.
- The inadvertent use of insecure designs, architectures, or interfaces.
- Misconfiguration, insufficient isolation, weak authentication, or imprecise access control for applicable components and interfaces.
- Kubernetes, containers, the Linux container host operating system, the container image registry, and other cloud-native technology call for new skill sets. If improperly deployed or managed, CNFs and Kubernetes, like any other technology, can expose vulnerabilities or present new attack vectors.
- Container images for CNFs and 5G services require code provenance and protection as they move through a CI/CD pipeline. If container images are not stored securely, protected by role-based access control, scanned for vulnerabilities, and signed as trusted, container images can contain vulnerabilities or exploits that surface after deployment.

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 containerized network functions (CNFs) on virtual machines.

Protecting against threats in an O-RAN architecture with VMware

The O-RAN Threat modeling and remediation analysis, v1.0 by the O-RAN Alliance Security Focus Group, March 2021, contains a comprehensive list of potential vulnerabilities and threats. Vulnerabilities and threats that are specific to VMware Telco Platform RAN or other VMware technology are addressed in the sections below.

Built-In Security

When security is built into an open RAN platform, security is, in effect, inherent in the system, and automation can deploy security controls for layers, APIs, virtual machines, and other elements.

VMware Telco Cloud Platform RAN has built-in security. Security controls that are integrated with the software and built into the infrastructure help solve the challenges of 5G RAN by making security programmable, automated, adaptive, and context-aware. Built-in security improves visibility, reduces complexity, and focuses your defenses by letting you apply and automate adaptive measures like micro-segmentation in the right place, such as interfaces between RAN network functions and the service management and orchestration layer.

With VMware Telco Cloud Platform RAN, you can architect the infrastructure with built-in security by using automated provisioning and automated management. In addition, when you opt to use VMware Telco Cloud Operations with VMware Telco Cloud Platform RAN, you can monitor the layers of a 5G network, including an open RAN, to help protect availability, integrity, and confidentiality. VMware Telco Cloud Operations uses machine learning and closed-loop automation to analyze data and proactively help thwart security threats and attacks.

Applying security principles and controls

The following sections describe the security principles and controls that VMware Telco Cloud Platform RAN uses to protect an open RAN from security risks, threats, and vulnerabilities. The following key principles guide the application of security controls in an open RAN:

- Zero-trust architecture and zero-trust networking
- Automating network management
- Vulnerability management
- Micro-segmentation
- Secure boot, roots of trust, code signing, and certificates
- Isolation of the RAN management plane and other critical security functions
- Monitoring and auditing of the RAN
- Strong security boundaries, especially those provided by hypervisors and virtual machines
- Security for cloud-native development and CNF deployments

Zero-Trust Architectures and Zero-Trust Networking

The service-based architectures and cloud-based computing that accompany the adoption of 5G enables greater use of zero-trust architectures and networking. With a zero-trust model, no trust is implicitly granted to system elements, resources, assets, network perimeters, or network connections. Verification is key. Before a session begins or a connection is established, authentication and authorization discretely govern access to networks and resources. A zero-trust model deploys multiple layers of verification to prevent data breaches and limit lateral movement within a system or network.

Adhering to zero-trust tenets

According to NIST SP 800-207, a zero-trust architecture adheres to seven technology-agnostic tenets:

1. All data sources and computing services are considered resources.

2. All communication is secured regardless of network location.

3. Access to a resource is granted on a per-session basis.

4. Access to resources is determined by a dynamic policy.

5. The integrity and security posture of all assets are monitored.

6. Dynamic authentication and authorization govern resource access.

7. The current state of assets, network infrastructure, and network traffic is tracked to improve security policies, context awareness, and enforcement.

For more information, see *NIST SP 800-207*.

For an open RAN, adopting a zero-trust model can protect interfaces and APIs, obtain telemetry across clouds, and impose context-specific security measures through network slicing.

Implementing a zero-trust architecture

For practicality, efficiently implementing the far-reaching tenets of a zero-trust architecture entails three prerequisites:

1. A common horizontal multi-cloud platform.

2. Security mechanisms and controls that are built into the RAN stack and its network.

3. Automation to dynamically apply and adjust security measures.

In VMware Telco Cloud Platform RAN, management interfaces and APIs are secured by using the built-in security features of VMware vSphere, including authentication, access control, authorization, and certificates.

To support VNFs and CNFs, aspects of a zero-trust model can be implemented by using automation to create and manage Kubernetes clusters and to onboard, deploy, and update RAN network functions.

Automating network management

Misconfiguration of RAN resources or network functions can expose known attack vectors or vulnerabilities. With open RAN and the use of APIs, programmable resource provisioning and other techniques can automate network management to decrease incidences of human error or malicious activity. Automation can help avoid misconfigurations and insecure configurations, such as deploying a CNF in a container with elevated privileges.

Applying security patches at scale

VMware Telco Cloud Platform RAN automates network management to reduce the risks of misconfiguration and to improve security patching at scale:

- Simplify the onboarding of RAN functions with validated, standards-compliant packages optimized for the platform.
- Reduce misconfiguration by automating the provisioning of RAN sites based on standardized templates describing appliances and configurations.

- Automatically discover, register, and create Kubernetes clusters from a centralized location to manage thousands of distributed components life-cycle management and patching.
- Automated lifecycle management applies security patches to infrastructure elements, Kubernetes clusters, RAN functions, and the Linux container host.
- Programmatically adjust the underpinning platform availability and resource configuration, based on the requirements of RAN functions at the time of instantiation.

The platform's CI/CD pipeline onboards and deploys RAN functions quickly and reliably, removing time-consuming and error-prone integration work.

Optimizing resource placement

With VMware Telco Cloud Platform RAN, programmable resource provisioning optimizes where to locate DUs and CUs. When you onboard a virtualized RAN function, you can programmatically adjust the underpinning platform availability and resource configuration based on the function's requirements to reduce human error and possibility of misconfiguration.

Vulnerability management

The automated lifecycle management in VMware Telco Cloud Platform RAN radically increases the speed and efficiency with which you can apply, from a centralized location, security patches to operating systems, container hosts, Kubernetes clusters, and RAN functions.

Security advisories

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*.

Resolving vulnerabilities

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

Micro-segmentation

NIST SP 800-207 defines zero trust and a zero-trust architecture as follows:

"Zero trust (ZT) provides a collection of concepts and ideas designed to minimize uncertainty in enforcing accurate, least privilege per-request access decisions in information systems and services in the face of a network viewed as compromised. Zero trust architecture (ZTA) is an enterprise's cybersecurity plan that utilizes zero trust concepts and encompasses component relationships, workflow planning, and access policies. Therefore, a zero trust enterprise is the network infrastructure (physical and virtual) and operational policies that are in place for an enterprise as a product of a zero trust architecture plan."

Such a definition gets to the heart of protecting an open RAN from several potential vulnerabilities:

- Unauthorized access to a DU, CU-CP, or CU-UP to undermine performance or execute a broader attack to undermine network availability.
- Unauthorized access by RAN applications running in the RICs to network and subscriber data.

Shielding resources from unauthorized access

A zero-trust architecture for the networking of the CNFs that make up an open RAN can be implemented by using micro-segmentation, which can shield resources from unauthorized access. With VMware Telco Cloud Platform RAN, automated provisioning deploys Kubernetes worker nodes that use Calico and Multus for networking.

- With Calico, you can create and enforce policies for micro-segmentation of container networking. Access can in effect be controlled by policy and then enforced at a specific point in the network—a policy enforcement point, or PEP, in the NIST zero-trust architecture.
- With Multus, security policies can establish micro-segmentation by constraining network connections between workloads to limit lateral movement if a network is breached.
- With the telco-grade Kubernetes distribution in VMware Telco Cloud Platform RAN, VMware Tanzu for Telco, you can apply Kubernetes network policies to limit network traffic between CNFs in Kubernetes pods and Kubernetes clusters.

Reconfiguring security points when needed

NIST SP 800-207 says that "the key necessity to this approach is that the PEP components are managed and should be able to react and reconfigure as needed to respond to threats or change in the workflow." Because VMware Telco Cloud Platform RAN helps automate aspects of provisioning and management for container networking for Kubernetes clusters, the policy enforcement points can be reconfigured as needed.

Secure boot, roots of trust, code signing, and certificates

Secure boot, hardware roots of trust, code signing, and certificates help establish a chain of trust that protects the infrastructure, components, and applications in a RAN stack.

Secure boot and hardware roots of trust

VMware vSphere can cryptographically attest hosts with secure boot. In vSphere, you can enable secure boot on the host to ensure that only digitally signed code is allowed to run.

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 application unless the operating system bootloader is cryptographically signed.

With vSphere in VMware Telco Cloud Platform RAN, 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.

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.

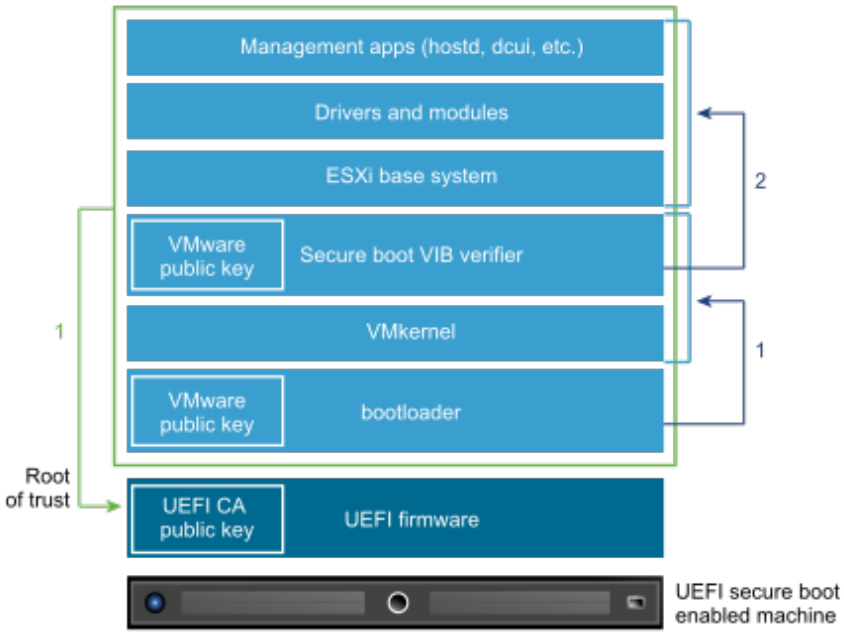

Figure 3: Secure boot in the VMware ESXi hypervisor.

Code signing

In addition to secure boot, code signing can help ensure the integrity of CNFs. The container image registry used with the CI/CD pipeline of VMware Telco Cloud Platform RAN can sign container images as trusted after scanning them for vulnerabilities and performing other actions to ensure code provenance.

Certificates

In the O-RAN architecture, the Fronthaul, O1, O2, A1, and E2 management interfaces are open interfaces that make an open RAN programmable. To identify services that interact in an open RAN and prevent the interception of sensitive data, interfaces in an open RAN are to use Transport Layer Security (TLS) (or SSH) to establish encrypted sessions between services verified by public key certificates. The architecture of 5G is based on a Public Key Infrastructure (PKI) system that uses cryptographic keys to establish identity. A public key and private key are created by a certification authority (CA) for each device.

The vSphere platform, which is part of VMware Telco Cloud Platform RAN, includes a component called the Platform Services Controller. It contains common infrastructure security services, including the VMware Certificate Authority and certificate management services. The VMware Certificate Authority can create and manage keys for the components of an open RAN that VMware Telco Cloud Platform RAN manages, especially for the RAN management plane and its interfaces.

By default, vSphere uses TLS/SSL certificates that are signed by VMware Certificate Authority (VMCA). These certificates are not trusted by end-user devices or browsers. As a security best practice, replace at least all user-facing certificates with certificates that are signed by a third-party or enterprise Certificate Authority (CA).

Isolation of the RAN Management Plane

Protecting the management plane for an open RAN falls into three main areas of focus: its architecture, its administration network, and the access solution and privileges of administrators.

THE SYNERGY OF CONTAINERS AND VIRTUAL MACHINES

VMs solve infrastructure-related problems by better utilizing servers, improving infrastructure management, and streamlining IT operations.

Containers solve application-related problems by streamlining DevOps, fostering a microservices architecture, improving portability, and further improving resource utilization.

Running containers on VMs produces a synergy that helps CSPs transition from 4G to 5G networks with ease.

BENEFITS OF HYPERVISORS AND VIRTUAL MACHINES FOR CNFs

- Onboard, deploy, and manage CNFs at scale through automation
- Establish strong security boundaries for containers
- Isolate workloads and apply built-in security measures like micro-segmentation
- Select the best Linux kernel version for your workload
- Optimize the performance of large Kubernetes clusters and mixed workloads on shared infrastructure
- Automate lifecycle management of Kubernetes clusters, RAN functions, and 5G services
- Optimize the placement and performance of CNFs with programmable resource provisioning
- Scale CNFs without the pain of adding, configuring, and managing physical hardware
- Streamline operations and reduce OpEx

An architecture with a secure management plane establishes 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 inter-related, generally interoperable solutions from VMware not only to manage their virtualized and containerized RAN infrastructure but also to manage security measures in the RAN management plane:

- VMware Telco Cloud Automation
- VMware 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 and its protection

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 regularly scan the management network to detect anomalies in configurations and operations.

With VMware Telco Cloud Platform RAN, you can manage the RAN virtualization fabric through a central orchestration tool: VMware Telco Cloud Automation. VMware Telco Cloud Platform RAN uses secure, encrypted channels to administer virtual machines, virtual network functions, and the ESXi hypervisor. VMware Telco Cloud Automation controls access with authentication and multi-tenant role-based access control.

VMware furnishes a reference architecture for designing, isolating, and protecting the RAN management plane; see the *Reference Architecture for VMware Telco Cloud Platform RAN*.

Protecting virtualization of critical security 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."

APPLYING CONSISTENT SECURITY WITH A COMMON HORIZONTAL PLATFORM

A common horizontal platform drives many security benefits. With a common platform, security operations become simpler, with faster, more agile responses.

- Isolate containerized network functions (CNFs) on virtual machines and the VMware hypervisor, VMware ESXi, to establish strong security boundaries and prevent lateral movement.
- Protect sensitive data by segmenting and encrypting workloads and storage.
- Keep the virtualization fabric, container images, and VMs up to date and patched.
- Use a security-hardened, real-time Linux host optimized for vSphere.
- Scan container images for vulnerabilities, sign them as trusted, and secure them with role-based access control.
- Architect the infrastructure with built-in security by using automated provisioning, automated management, secure administration, and micro-segmentation.
- Strictly control access to and use of management layers by using the principles of least privilege and separation of duties.

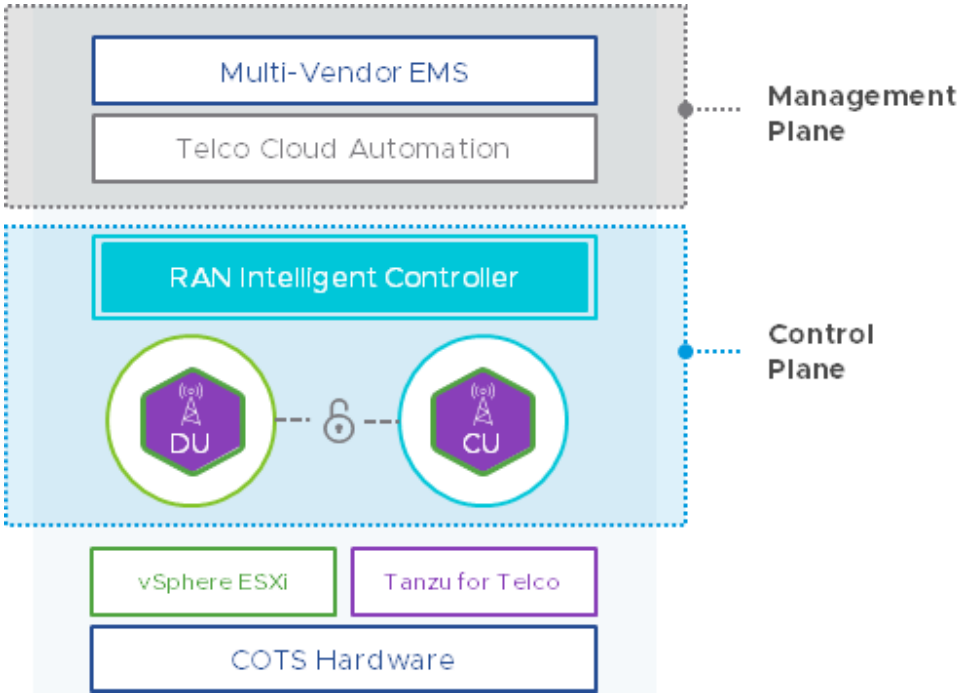

Figure 4: The reference architecture for VMware Telco Cloud Platform isolates the open RAN management plane.

It is key to limit the attack surface of security critical functions. To reduce risk, you can isolate security functions in their own trust domain.

Establishing trust domains

Virtualized infrastructure plays a strong role in segmenting workloads into trusted domains to reduce the risk of a breach spreading from a compromised host to others. When you set up components of the management plane, such as 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 as well as critical security functions with firewalls, micro-segmentation, and other measures.

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).

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 and vCenter.

Monitoring and Auditing for RAN Security

Monitoring and auditing are cornerstones of security. VMware Telco Cloud Operations is an optional component that supplies holistic monitoring and network management across the physical and logical layers of a RAN for rapid insights into configurations, interactions, and compliance. It can flag compliance gaps and security vulnerabilities. If a software

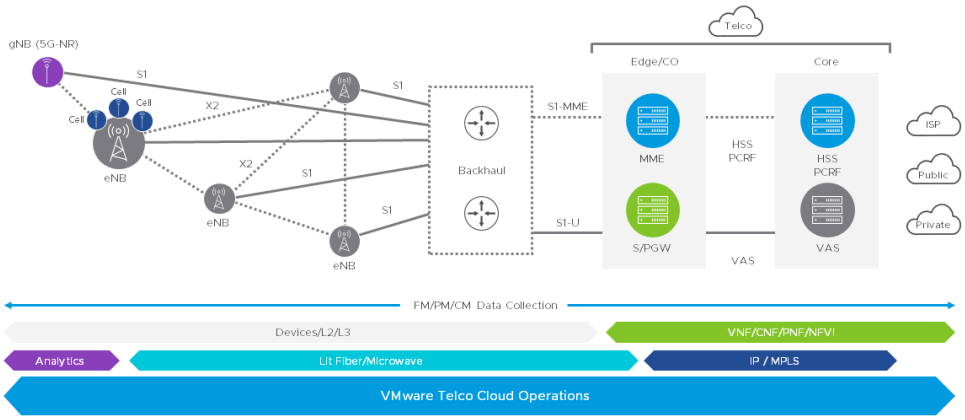

Figure 5: This diagram illustrates how VMware Telco Cloud Operations monitors the layers of a 5G network to help protect availability, integrity, and confidentiality.

component like SSL is out of date, for instance, VMware Telco Cloud Operations can detect it and raise an out-of-compliance notification. VMware Telco Cloud Operations can monitor physical equipment as well as the ESXi hypervisor and other VMware products

Optional components for the RAN management plane

In addition to VMware Telco Cloud Operations, you can deploy other optional components in the RAN management plane and centralize them across the cloud topology. The following optional 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 and helping satisfy emerging telco security requirements for open radio access networks.

- VMware vRealize Operations Manager collects compute, storage, and networking data to provide performance and fault visibility over hosts, hypervisors, virtual machines, clusters, and sites.
- VMware 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.
- VMware 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.

Gaining visibility into traffic routing and micro-segments

vRealize Network Insight gives you visibility into traffic routing, sources and destinations, micro-segmentation, and possible security violations. vRealize Network Insight works with NSX Data Center, which is also an optional component for the RAN management cluster, to help assess compliance with telecommunications security requirements for the virtualization plane and its management.

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.

Establishing Strong Security Boundaries for Containers

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.

"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

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."[7]

To establish a strong security barrier for containers, VMware typically runs containers on virtual machines. Deploying containers with VMs encases an application with a layer of strong isolation, an approach that is well-suited to cloud-style environments with multi-tenancy and multiple workloads. The major cloud providers, such as Google and Amazon Web Services (AWS), typically isolate the container workloads of tenants by using separate VMs.

Containers or the operating system of a physical host can easily be misconfigured, increasing the attack surface and the level of risk, the NIST Application Container Security Guide says. "Carelessly configured environments can result in containers having the ability to interact with each other and the host far more easily and directly than multiple VMs on the same host."

The abstraction, automation, and isolation of an operating system running on a VM in a hypervisor reduces the attack surface, adds layers of protection against lateral movement, and decreases the risk of a security breach.

Taking advantage of security innovations

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 on how virtual machines establish strong security boundaries for containers, see *CNFs on Virtual Machines or Bare Metal? Securing, Managing, and Optimizing CNFs and 5G Services at Scale*.

Security for cloud-native development and CNF deployments

The ability to host a multitude of network functions regardless of their locations and to automate operations across 5G networks are integral aspects of virtualizing the RAN. Offering new 5G services relies on the ability to develop, deploy, operate, and protect applications close to end customers, and the RAN is the prime location to do so. A common horizontal platform can scale the operation and protection of 5G services across distributed RAN sites.

As a common horizontal platform that is consistent with its corresponding 5G core platform, VMware Telco Cloud Platform RAN transforms the radio access network into a 5G multi-services hub that enables you to deploy and protect custom 5G applications alongside virtualized RAN functions.

This end-to-end consistency enables you to efficiently provision, operate, and protect 5G services tailored to different enterprise and consumer markets.

7 NIST Special Publication 800-190, Application Container Security Guide, September 2017. See https://doi.org/10.6028/NIST.SP.800-190

PROTECTING CNFS

As you work to develop and deploy 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 CI/CD pipeline
- Implement a trusted container image registry with role-based access control and vulnerability scanning
- Inspect Kubernetes clusters and 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 production
- Embrace DevSecOps and new security principles to address emerging threats

To protect 5G services running in the RAN and to help protect RAN functions, VMware Telco Cloud Platform RAN delivers the following security capabilities:

- Strong security boundaries by running containerized 5G services and CNFs on virtual machines (see the previous section)
- A security-hardened Linux container host called Photon OS that is optimized for running containers on vSphere
- A CI/CD pipeline with a secure container image registry called Harbor
- Automated lifecycle management and security patching for container hosts and Kubernetes clusters

These capabilities help protect cloud native network functions and 5G services by implementing countermeasures that should be applied to cloud native components. Cloud native technology should be protected from the top to the bottom of the RAN stack with fully integrated security. For more information, see the NIST Application Container Security Guide (NIST Special Publication 800-190).

- Implement container-specific countermeasures and integrate them into the container pipeline, image registry, life cycle, and orchestration platform
- Enforce security with RBAC and policies for image use
- Use only the latest known, patched, scanned, and signed images
- 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, dashboards, and the Kubernetes API by using RBAC and the principles of least privilege and separation of duties
- Segment orchestrator network traffic into discrete virtual networks by sensitivity level
- Use a patched, up-to-date container runtime
- Constrain network access from containers
- Use an up-to-date container-specific minimalist OS to narrow the attack surface
- Limit resource consumption of a container to thwart denial-of-service (DoS) attacks
- 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

Security-hardened Linux container host

VMware Telco Cloud Platform RAN uses Photon OS as its Linux container host for deploying CNFs. Photon OS provides a secure runtime environment for running containers, including CNFs, and a real-time kernel for RAN applications.

Photon OS features a kernel flavor called 'linux-rt' to support low-latency real-time RAN applications. linux-rt is based on the Linux kernel PREEMPT_RT patchset that turns Linux into a hard real-time operating system. In addition to the real-time kernel itself, Photon OS 4.0 supports several userspace packages such as tuned, tuna, stalld that are useful to configure the operating system for real-time workloads. The linux-rt kernel and the associated userspace packages together are referred to as Photon Real Time (RT).

The 5.10 kernel in Photon OS is configured according to the recommendations of the Kernel Self-Protection Project (KSPP); packages are built with hardened security flags; and the operating system uses secure EFI boot to start up with validated trust.

Security capabilities include SELinux, Security Encrypted Virtualization, and encrypted status and support for Intel Software Guard Extensions (SGX).

OPEN RAN 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 containers, virtual machines, hypervisors, and other components
- Conduct penetration testing on a regular basis
- Set up secure Kubernetes clusters by analyzing their security posture using the *CIS Kubernetes Benchmark*.

LEARN MORE

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

SELinux is an implementation of mandatory access controls (MAC) on Linux. Photon OS 4.0 provides an opportunity for the appliance to enable SElinux, either in Permissive or Enforcement mode. Photon OS includes a default policy that can be customized during build time. Photon also supports SELinux for containers.

Intel SGX is a set of instructions that protects application data and code from modification or disclosure. With SGX, developers can partition sensitive information into enclaves, which are areas of execution in memory with enhanced security.

Container image registry with security controls

The CI/CD pipeline of VMware Telco Cloud Platform RAN includes a trusted container image registry called Harbor. Harbor protects the container images for CNFs with security policies and role-based access control (RBAC), scans them for vulnerabilities, and signs them as trusted. In doing so, Harbor enhances compliance, performance, and interoperability to help you consistently and securely manage CNFs for VMware Tanzu for Telco RAN, a telco-grade Kubernetes distribution.

Conclusion

Through the power of virtualization, VMware addresses the security risks and requirements that communications service providers face as they move to open radio access networks and adopt CNFs, Kubernetes, and multi-cloud networks. VMware Telco Cloud Platform RAN protects open radio access networks with built-in security that enables you to apply and automate security controls to foster a zero-trust architecture.

References

National Strategy to Secure 5G Implementation Plan; see *https://www.ntia.doc.gov/5g-implementation-plan*.

Comments of the Open Ran Policy Coalition Before the National Telecommunications And Information Administration, Washington, DC, 20230 In the Matter of *The National Strategy to Secure 5G Implementation Plan*, Docket No. 200521–0144.

5G and Open RAN Security: Next Generation Trust, by the Open RAN Policy Coalition.

Open RAN Security in 5G, April 2021, by the Open RAN Policy Coalition.

The Open RAN Policy Coalition's *Statement on Senate Passage of the U.S. Innovation and Competition Act*, June 2021.

U.S. NIST SP 800-207, Zero Trust Architecture, August 2020.

NIST Special Publication 800-190, Application Container Security Guide, September 2017.

ISO/IEC 27005:2018, Information security risk management, July 2018.

O-RAN Alliance *specifications* and *resources*:

- O-RAN Security Protocols Specifications-V1.0, O-RAN Alliance, March 2021. See *https://www.o-ran.org/specifications*.
- O-RAN.WG1.O-RAN-Architecture-Description-v04.00. See *https://www.o-ran.org/specifications*.
- O-RAN Threat modeling and remediation analysis, v1.0, O-RAN Alliance Security Focus Group, March 2021. See *https://www.o-ran.org/specifications*.
- O-RAN white paper: *O-RAN Use Cases and Deployment Scenarios: Towards Open and Smart RAN*, February 2020.
- O-RAN white paper: *Minimum Viable Plan and Acceleration towards Commercialization*, June 2021.

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

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

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

Security Assurance Requirements for Linux Application Container Deployments, NIST.IR 8176, October 2017.

vSphere Security, December 2019.

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

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

VMware Security Hardening Guides

Security Best Practices and Resources for VMware Virtualization Infrastructure

vSphere Security Documentation, Guides, and Resources

Understanding vSphere Hardening and Compliance

The UK government's *Telecommunications Security Bill of 2020*

VMware technical white paper on telecom security (non-RAN)

Modernize to Monetize: Reimagine the Telco Cloud to Capitalize on 5G: Efficiently design, deploy, operate, and protect 5G networks with a common horizontal platform, by VMware.

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-ran-security-wp 11/21