CTONE

Protecting Open RAN-Powered Next-Generation Mobile Networks

Securing Open RAN deployments is critical to managing growing attack surface risk

The global Open Radio Access Network (O-RAN) market is projected to experience significant growth, increasing from USD $1.1 billion in 2022 to USD $15.6 billion by 2027, with a remarkable CAGR of 70.5% during the forecast period. This growth is closely tied to the transformation in network architectures, shifting from proprietary or closed radio access networks towards open and interoperable systems.

As a part of next-generation communication technologies (CT), O-RAN emphasizes the adoption of open interfaces, software-defined networking (SDN), and virtualization to enable multi-vendor interoperability and enhance flexibility in deploying and managing radio access networks. Embracing O-RAN principles empowers operators and system integrators to avoid vendor lock-in, foster innovation, and cultivate a more open and competitive telecommunications ecosystem.

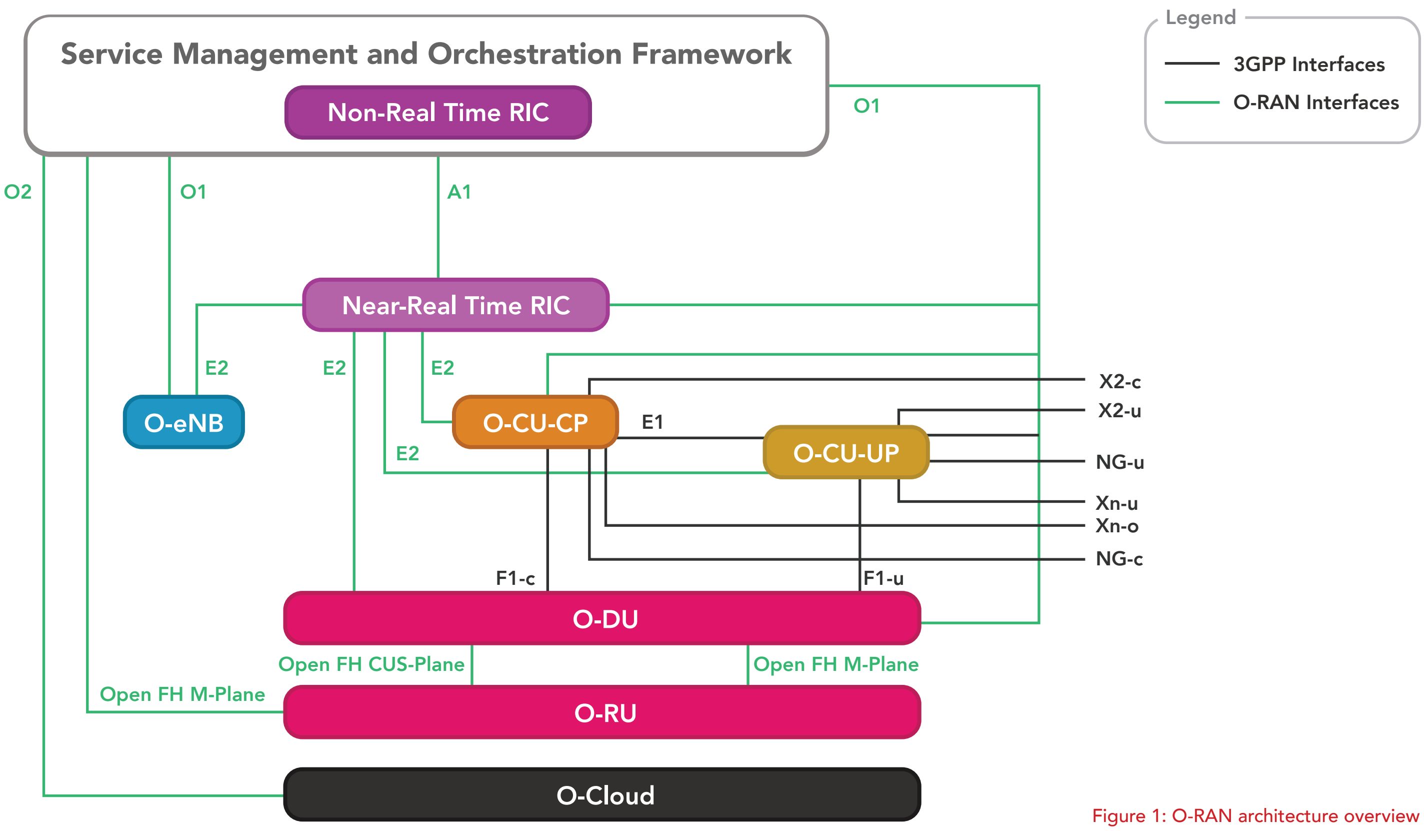


Figure 1: O-RAN architecture overview

What Does Security Mean for O-RAN?

Security in the context of O-RAN refers to the measures and practices implemented to protect the network infrastructure, components, and data from risk, including unauthorized access, malicious attacks, and potential vulnerabilities. Security measurement plays a pivotal role in ensuring the network's integrity, confidentiality, and availability, making it an essential element of O-RAN deployments. With the growth of next-generation mobile networks, the widespread utilization of Open Radio Access Network (O-RAN) signifies the clear demand for open and interoperable systems. However, it is important to recognize that this approach may introduce increased attack surface risk, including new vulnerabilities as vendors construct the network for private/public use. This broadened attack surface highlights the need for implementing O-RAN security solutions as a part of a secure network deployment. By proactively addressing potential business risks, organizations can safeguard and build resilience into their mobile network infrastructure.

Managing Growing Attack Surface Risk in the O-RAN World

It is crucial to address these challenges to ensure the security and integrity of O-RAN deployments.

1 **TRANSITIONING FROM CLOSED TO OPEN SYSTEMS**
Next-generation mobile deployments using O-RAN expand the attack surface that hackers can use to target the O-RAN system, presenting increased business and security risks.

2 **EXPANDING ATTACK SURFACE WITH O-RAN**
New interfaces like A1, E2, O1 etc., are emerging as a part of the growing attack surface found within O-RAN architectures.

3 **MULTI-VENDOR INTEROPERABILITY RISK**
The shift from single-vendor reliance to a multi-vendor supply chain introduces increased risk of attack and compromise.

4 **RAN VIRTUALIZATION AND CLOUDIFICATION**
The widespread adoption of virtualization and cloud technologies on commercial off-the-shelf (COTS) servers for O-RAN deployments can lead to more security risks from IT technologies.

5 **OPEN SOURCE ADOPTION**
The increasing use of open-source components exposes O-RAN systems to potentially serious vulnerabilities without the ability to easily discover or mitigate them.

Securing O-RAN Deployments:
CTOne SecureRAN

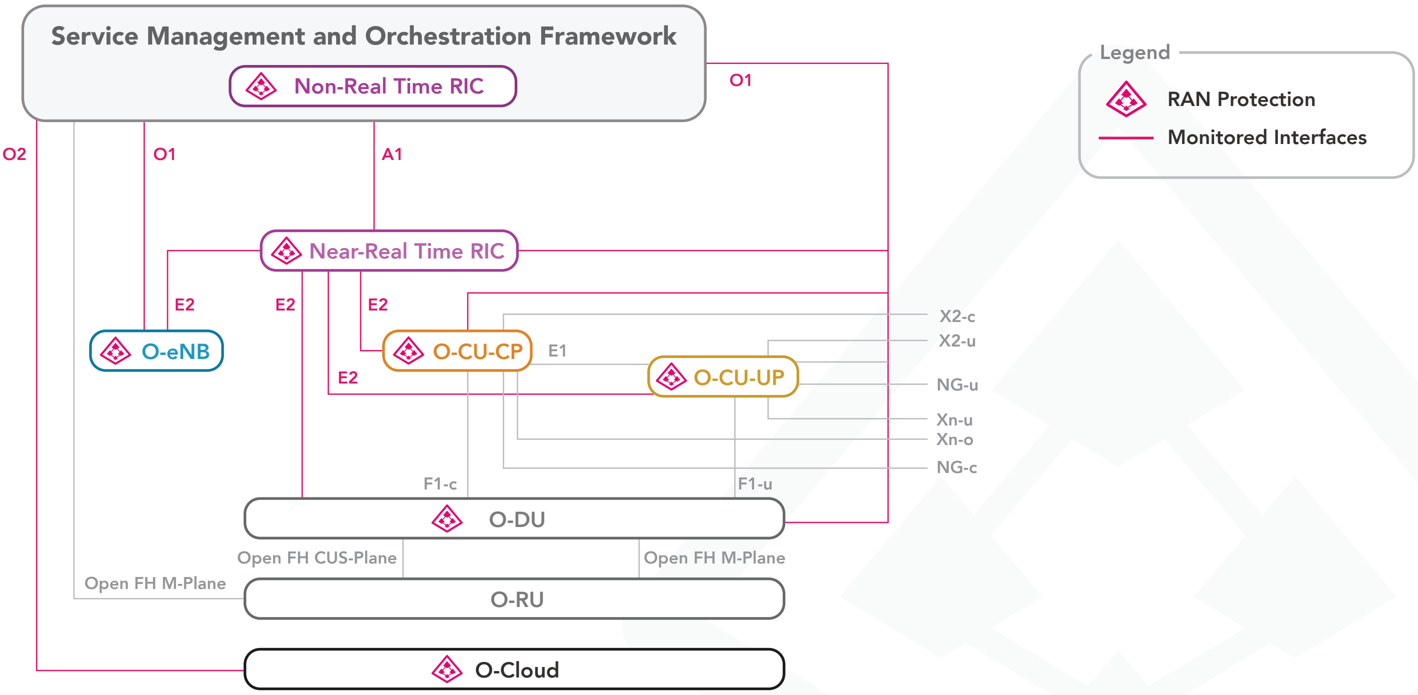
CTOne SecureRAN is a specialized cybersecurity solution that covers both IT and communication technologies (CT) domains, specifically designed for O-RAN systems, and deployed on the O-Cloud platform to protect key elements of an O-RAN system. It monitors the integrity of the O-Cloud server, detects O-RAN interfaces, and with built-in software component analysis (SCA), CTOne SecureRAN can monitor potentially risky components for more effective supply chain risk management (SCRM).

Visibility Across O-RAN Systems

Security visibility in O-RAN systems is crucial as it provides transparency into the network's security status, enabling proactive vulnerability management, helping to comply with regulations, and enhancing incident response. CTOne SecureRAN generates indicators of security risk and vulnerability exploit information, offering a comprehensive view of the O-RAN system's devices, interfaces, and applications.
The comprehensive insight supports informed decision-making, mitigates risks, and improves overall system resilience, safeguarding the network against evolving cyber threats.

Real-time Protection

CTOne SecureRAN delivers real-time security capabilities for private 5G deployments, reducing enterprise risk by monitoring critical system files and configurations for unauthorized changes or tampering. By continuously comparing the current state with trusted baseline values, CTOne SecureRAN can detect and stop potential security breaches, strengthening the integrity and security of next-generation wireless deployments.
In addition, SecureRAN helps with the identification and mitigation of potential network exploits within O-RAN software, making it an ideal solution for managing increasing cyber risk.



Realize the True Value of Next-Generation Wireless Networks

CTOne offers a complete private 5G security solution for enterprises, protecting the entire enterprise private 5G network, including IIoT endpoint devices, O-RAN systems, edge computing applications, and core networks. This turnkey solution is designed to provide comprehensive protection without requiring substantial investment or management costs. By bridging the gap between IT and CT, CTOne ensures the security of both network and endpoint layers, addressing the evolving cyber threats faced by businesses in private 5G networks.

> “ *Empowering Secure Connectivity in an Open World* ”

About CTOne

CTOne, a global cybersecurity leader in communication technology, offers enterprise cybersecurity solutions for next-generation wireless networks. A subsidiary of Trend Micro, CTOne enables digital transformation and strengthens the resilience of communication technology.

www.ctone.com