CTONE

Securing Enterprise Private Mobile Networks

CT Security:
The Often-Overlooked
Frontier in Cybersecurity

When enterprises consider digital
transformation, 5G technology plays a crucial
role in achieving their objectives by leveraging
its advantages and benefits.
However, CT (Communication Technology)
becomes a new attack vector for hackers to
infiltrate and steal sensitive data.
Despite 5G being inherently more secure than
other wireless communication technologies,
Network Function Virtualization, Open-Source
Software, Openness of 5G, and numerous
unprotected IoT devices expose 5G to different
types of vulnerabilities and potential attacks.

Hence, the scope of security deployment should
encompass not only IT and OT but also CT,
emphasizing the holistic protection of all aspects
of the enterprise's digital infrastructure.

The increased adoption of 5G opens up avenues for growth and innovation. With stable and reliable 5G wireless networks, enterprises can adopt more agile and flexible production line deployments to diverse customers' needs.

Undoubtedly, CT (Communication Technology) plays a pivotal role in bridging IT and OT networks, enabling seamless digital transformation within enterprises through the utilization of 5G technology.

However, the ubiquitous and invisible wireless coverage breaks down the well-defined boundary between OT and IT networks, creating openings for cyber threats to propagate across poorly designed, mismanaged, and unprotected 5G private mobile networks.

Optimizing Enterprise 5G Security: Protecting What Matters

THE RUNNING APPLICATION IN PRIVATE MOBILE NETWORKS

Our objective is to safeguard the uninterrupted operation of applications, such as AR/VR/ML, across various vertical markets that utilize private mobile networks, protecting them from potential disruptions or interference caused by attackers.

THE SENSITIVE DATA OF ENTERPRISES

Ensuring the security and privacy of communications within wireless networks includes confidential information, digital assets, trade secrets, personal data of employees or customers, and other sensitive data transmitted or stored.

COMMUNICATION SAFETY

It is crucial to ensure communication safety due to the potential threat of hackers exploiting vulnerabilities in technologies such as 4G, 5G, and Wi-Fi. These wireless connections can serve as attack vectors for common threats like DDoS attacks, malware infiltration, and ransomware.

O-RAN SYSTEM

The transition from closed to open architecture in Open RAN enables a more flexible, cost-effective approach for constructing wireless networks, but meanwhile, it also introduces new attack surfaces & SBOM profiling necessity.

THE CRITICAL INFRASTRUCTURE IN PRIVATE NETWORKS

With the gradual ITization by standard x86 server w/virtualization & cloud environment of the CT field, the occurrence of IT threats in wireless networks also exists, and it is crucial to protect the infrastructure and key elements in private mobile networks.

From Application to Security:
Securing Private Mobile Networks for Enterprises in Vertical Markets

Smart Manufacturing

Smart Logistics

Smart Healthcare

Energy & Utility

Military & Defense

What We Offer:
Unleashing Advantages of the Solution

CTOne`s solution offers a turnkey approach to private mobile network security for enterprises & operators. Providing robust protection against diverse and evolving cyber threats across 4G/LTE and 5G networks.

1 TAILOR-MADE SOLUTION

A tailor-made solution integrating IT and CT domain security for entire private mobile networks.

2 END-TO-END PROTECTION WITH ZERO TRUST & JOINT DEFENSE

A comprehensive cybersecurity solution covering Endpoint, RAN, MEC, and 5GC is essential for private mobile networks with zero trust management & joint defense strategy.

3 SECURITY VISIBILITY & VISUALIZATION

Providing a comprehensive and transparent network topology that includes multiple endpoint devices and offers a visible security status.
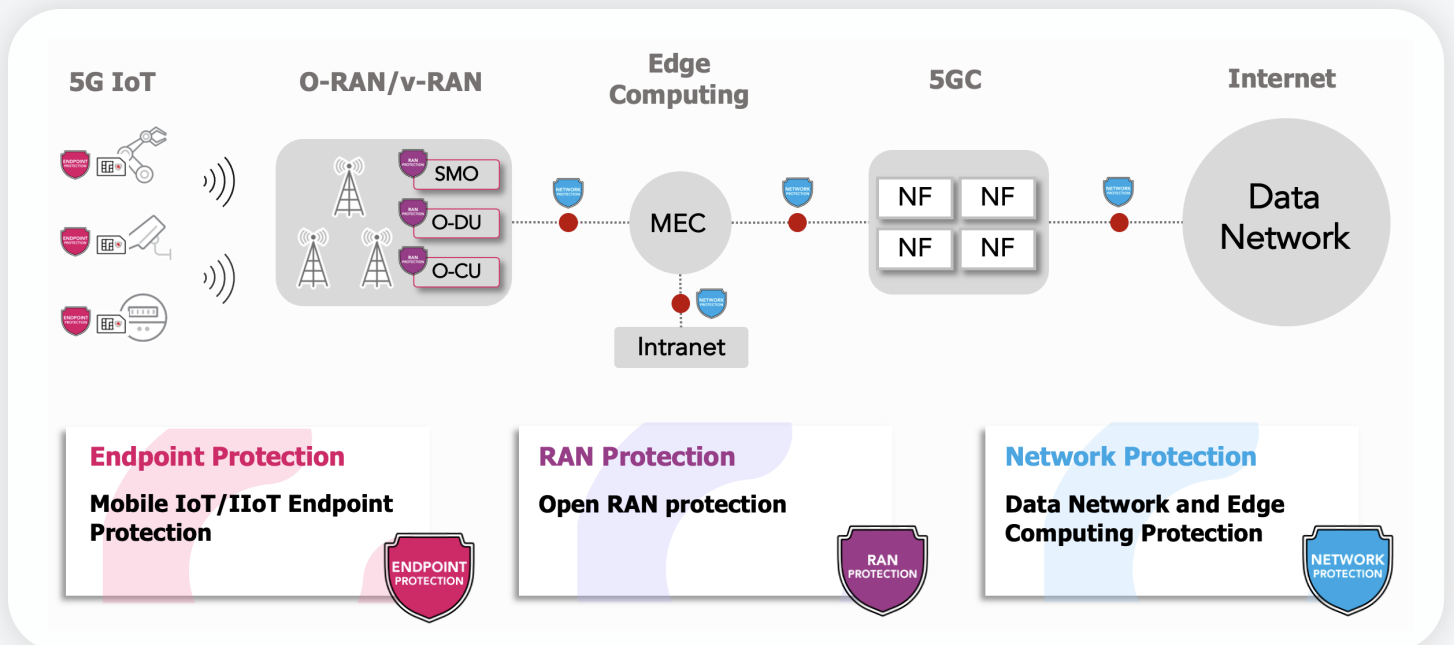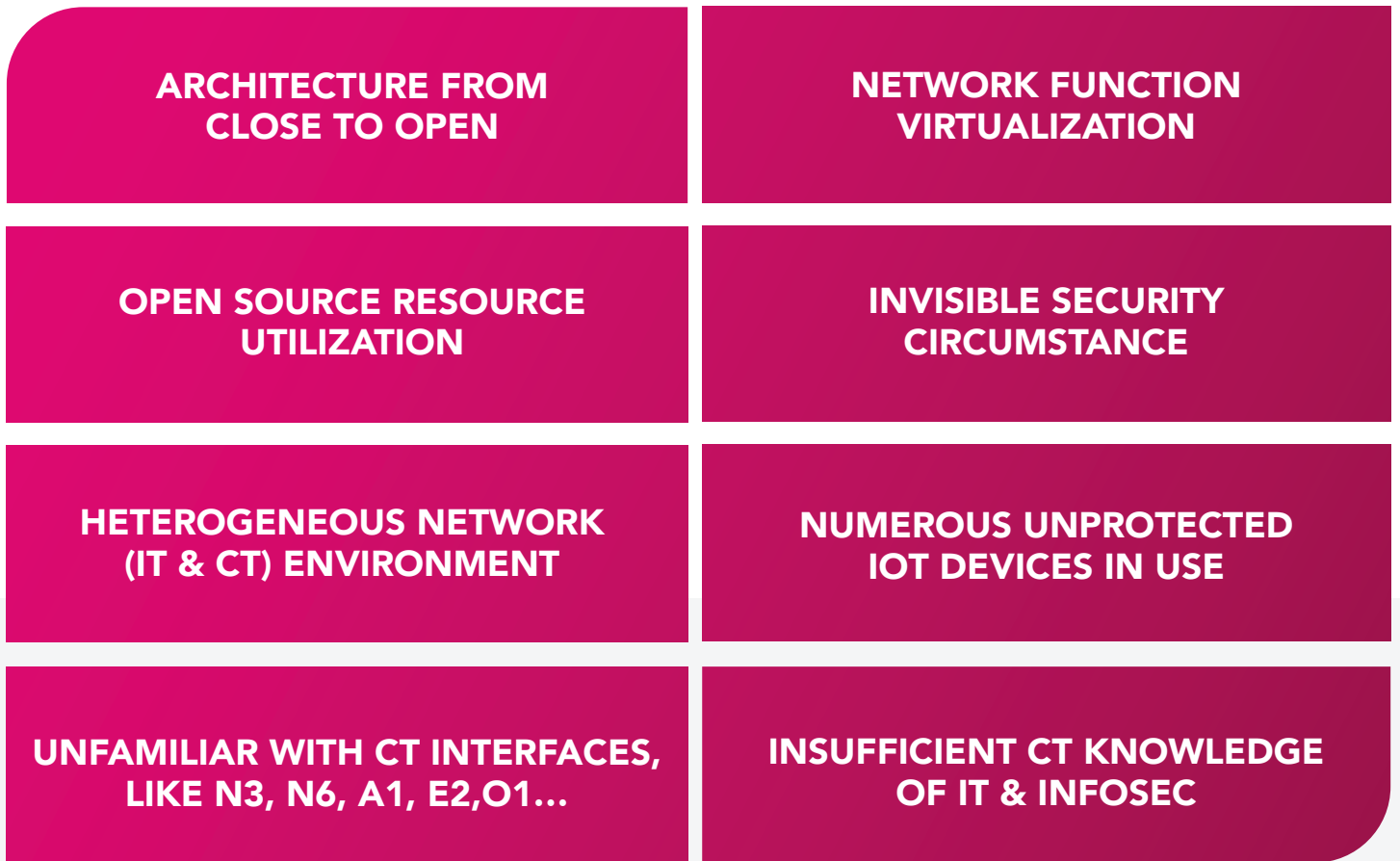
4 CENTRALIZED & USER-FRIENDLY CONSOLE

Utilizing a user-friendly console for IT professionals or InfoSEC to minimize the learning curve bring the adoption of 5G technology.

5 TRANSPARENCY & VENDOR AGNOSTIC DEPLOYMENT

Enable transparent deployment within existing 5G infrastructure without compatibility problems.

Security Challenges in Private Mobile Networks:

ARCHITECTURE FROM CLOSE TO OPEN	**NETWORK FUNCTION VIRTUALIZATION**
OPEN SOURCE RESOURCE UTILIZATION	**INVISIBLE SECURITY CIRCUMSTANCE**
HETEROGENEOUS NETWORK (IT & CT) ENVIRONMENT	**NUMEROUS UNPROTECTED IOT DEVICES IN USE**
UNFAMILIAR WITH CT INTERFACES, LIKE N3, N6, A1, E2,O1...	**INSUFFICIENT CT KNOWLEDGE OF IT & INFOSEC**

CTOne offers a complete private 5G security solution for enterprises, protecting their entire network, including IIoT endpoint devices, O-RAN system, edge computing applications, core networks. This turnkey solution is designed to provide comprehensive protection without requiring substantial investments 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 4G/LTE and 5G networks.

CTONE

> **"** To Protect the Next-Generation Wireless Networks
> for Digital Transformation **"**

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.