Securing Private Cellular Networks

Apply Enterprise Zero-trust Security to Private Wireless Networks with Ericsson and OneLayer

The Problem:

Private Wireless Network Visibility and Security Gaps

Private wireless networks now play a pivotal role in utilities innovation and growth. The Ericsson platform makes deploying secure private, mission-critical wireless networks simpler and more cost-effective than ever. At the same time, many enterprises struggle to extend their existing enterprise security tools and practices to 5G and LTE networks.

Most enterprise security tools were designed with IP networks in mind and cannot identify and classify cellular-connected devices effectively. Without this context, it is impossible to implement effective security measures based on each device category's unique risk profile. Differences between IP and cellular network topologies also render traditional network segmentation and security policy techniques ineffective.

The Solution:

Integrated Security and Threat Detection for 5G/ LTE Networks

Ericsson and OneLayer have integrated their capabilities to help utilities deploy private wireless networks that are inherently secure and fully integrated with existing enterprise security tools and workflows. The native security capabilities of the Ericsson platform ensure that every private wireless network has a secure foundation.

OneLayer further enhances 5G and LTE network security by identifying and fingerprinting cellular network-connected devices and extending existing security tools' visibility to cellular networks. Furthermore, OneLayer provides a set of advanced segmentation, threat detection, Zero Trust authentication, and geolocation capabilities.

How it works?

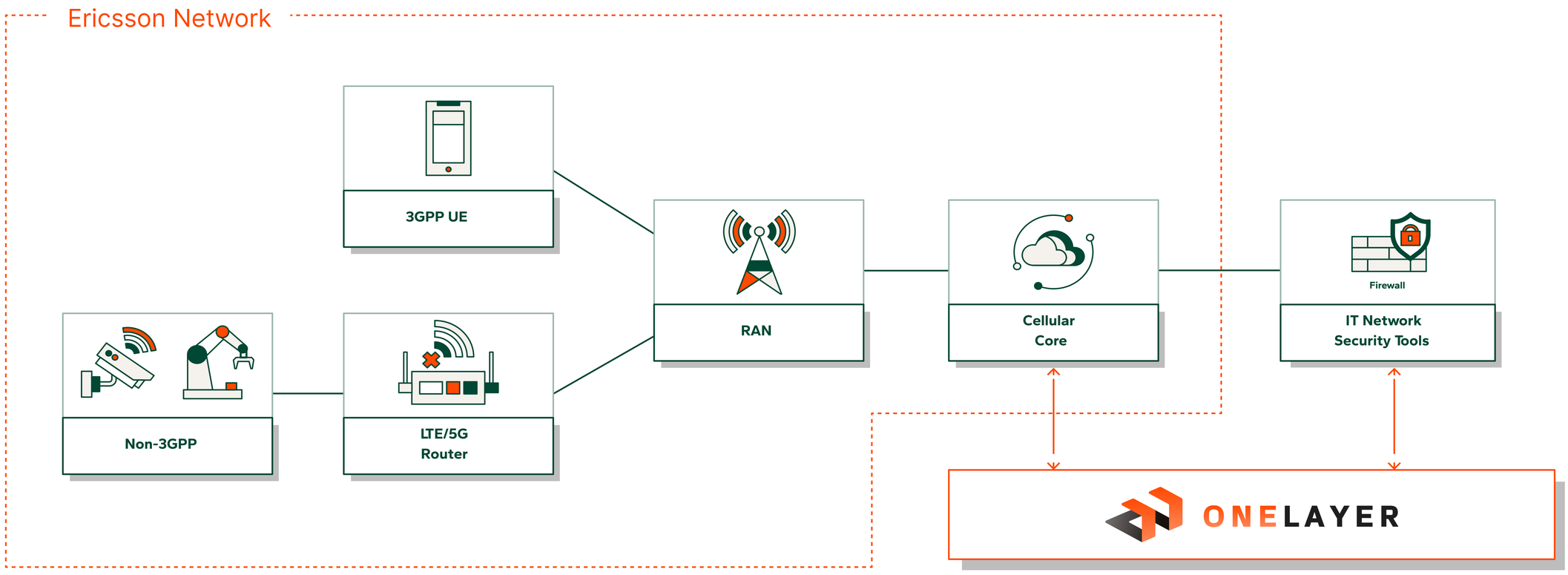
1.

Ericsson’s private cellular wireless solution allows global enterprises to own and operate their own private mobile networks. Ericsson provides several security capabilities natively.

2.

OneLayer integrates seamlessly with Ericsson containers on the Dual Mode LTE/5G packet core to enable critically enhanced security capabilities, including detailed asset visibility and fingerprinting, context-based segmentation, anomaly detection, Zero Trust authentication, and geo-fencing.

Enterprise Zero-trust Security to Private Wireless Networks with Ericsson and OneLayer



Immediate Benefits for Your Enterprise

- Deploy secure private wireless network infrastructure simply and cost-effectively.
- Discover, fingerprint, and apply context-based policies to all cellular-connected devices.
- Extend your trusted enterprise security tools and workflows to 5G/LTE networks.
- Bring enterprise segmentation best practices to your private wireless networks.
- Detect and respond to potential security threats quickly.
- Adapt protection dynamically based on geolocation.

Embrace Private Wireless Networks Securely

The combined capabilities of Ericsson and OneLayer will help you realize the business value of private mobile networks while anticipating and proactively mitigating potential risks.

- Simple deployment of private cellular infrastructure with strong native security.
- Seamless integration with the enterprise network and security policies.
- Granular device segmentation that is aligned with existing enterprise conventions.
- Advanced device discovery and fingerprinting, extending visibility to all assets in your ecosystem.
- Context-based segmentation policies that compartmentalize risk.
- Zero Trust network access control for your private wireless networks.
- Rapid detection and remediation of anomalous behavior.

Start Your Journey to Secure Private Wireless Networks

Contact OneLayer now to learn more about our Ericsson integration and enterprise wireless solution.

Visit onelayer.com to schedule a personalized demo or email us at contact@onelayer.com