End-to-End Security for Private Cellular Networks

As private LTE/5G, and cloud-native architectures accelerate digital transformation, service providers and critical infrastructure operators face rising cyber threats, increased regulatory pressure, and exponentially growing operational complexity.

Challenge:

The Complexity Behind Modernizing Mission-Critical Connectivity

In recent years, mission-critical organizations including power utilities, public safety, and rail have adopted a mix of private LTE/5G networks and Mobile Network Operator (MNO) access -providing connectivity to modernize operations, enhance network security, and support field communications.

However, many quickly encounter core challenges. Onboarding devices at scale in private networks is more complex and time-consuming than anticipated; cellular security introduces new and unfamiliar requirements, and temporary transitions to MNO environments result in fragmented visibility and limited control. This combination often leaves private networks underutilized and makes it difficult for teams to reliably support critical operations and maintain operational excellence.

Solution:

Unified Security from Devices to Core for Mission-Critical Networks

Together, OneLayer and ESM deliver end-to-end network security from devices, through the network infrastructure, helping mission critical organizations embed the security layer in their entire environment.

ERICSSON

Ericsson Security Manager (ESM):

Ericsson Security Manager strengthens security operations by providing continuous monitoring, automated assurance, and unified policy enforcement across the radio, transport, and core layers of private and public cellular networks. By giving security teams a centralized view of network posture, configurations, and anomalies, ESM helps operators detect threats earlier, validate compliance, and maintain resilient, mission-critical connectivity.

Identify and orchestrate

Dynamic risk and trust management

Protect

Automation of security configuration and compliance

Detect

Timely detection of known and unknown threats

Respond

Automation of security workflows and incident response

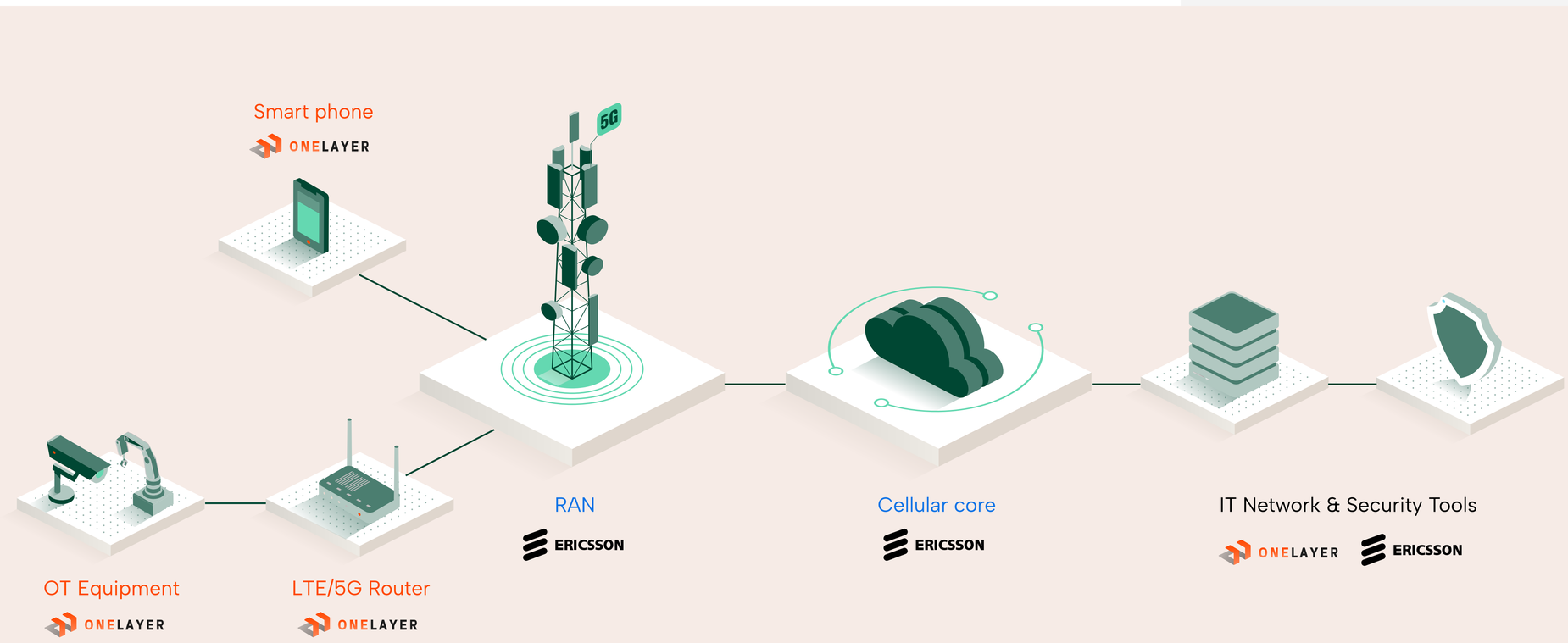
Recover

Predictive and automated security conditions recovery

ONELAYER

OneLayer Bridge:

OneLayer Bridge provides unified observability across every asset within private cellular networks. Using device fingerprinting, OneLayer discovers, classifies, and validates all connected assets, including those hidden behind routers and adapters. This deep device visibility enables continuous trackability throughout an asset's entire lifecycle, ensuring continuity in management even as the asset moves between private cores and APNs. Deep device visibility and identification enable OneLayer to detect anomalous device activity, rapidly troubleshoot device disconnections, and support granular access control policies based on identity and behavior context.



Better Together: Ericsson Security Manager + OneLayer Bridge

As private LTE/5G cellular networks become essential to mission-critical operations, organizations need clear visibility and consistent security across both infrastructure and devices. Ericsson Security Manager delivers network-wide governance and assurance, while OneLayer provides the device-level insight needed to understand what is connected and how it behaves, and enables security enforcement for those devices. Together, they enable earlier detection, more accurate risk assessment, and confident response, helping organizations strengthen security maturity and build a more resilient operational foundation.

1. Establish Network and Device Context

Ericsson Security Manager (ESM)	OneLayer Bridge	Customer Outcome
Visibility into network posture and configuration across core, RAN, and transport	Identifies every connected device including assets behind routers and adapters	Shared context across network and devices for effective security and operations

2. Detect Issues Early

Ericsson Security Manager (ESM)	OneLayer Bridge	Customer Outcome
Detects network threats with security EDR agents, misconfigurations and signaling, and wireless anomalies	Tracks device behavior, flags abnormal activity and troubleshoots disconnects	Earlier detection of risk before it impacts mission-critical operations

3. Respond to Incidents

Ericsson Security Manager (ESM)	OneLayer Bridge	Customer Outcome
Supports security compliance, and network-level policy enforcement	Applies access control based on device identity and behavior. Provides micro segmentation.	Faster response, stronger compliance, and secure operations

4. Support Ongoing Operations

Ericsson Security Manager (ESM) + OneLayer Bridge	Customer Outcome
Both solutions integrate with IT/OT and security solutions, including Firewalls, SIEM, SOAR, CMDB, ITSM, IDS/IPS, GRC, and MDM	Leverage existing workflows, increasing resource utilization