TECKNEXUS

WHITEPAPER

SPONSORED BY

ONELAYER

PRIVATE NETWORK SECURITY

4 Pillars for Securing Private 5G, LTE & CBRS Cellular Networks

TABLE OF CONTENTS

INTRODUCTION TO PRIVATE NETWORK SECURITY

Why Enterprises Need It

The move toward private mobile networks is transforming how enterprises manage connectivity for mission-critical operations. Across industries such as manufacturing, utilities, airports, ports, logistics hubs, and large campuses, organizations are deploying private 5G, LTE, and CBRS networks to gain secure, local control over their wireless infrastructure.

Unlike traditional public mobile networks operated by national operators, private mobile networks are enterprise-owned, giving organizations direct control over spectrum, coverage, security, data sovereignty, and devices. This local ownership opens the door to Industry 4.0 use cases, from autonomous robots and connected workers to real-time telemetry and edge AI.

But with this flexibility comes a new set of risks.

Enterprises that deploy private mobile networks are responsible for securing them end-to-end. Unlike enterprise Wi-Fi or legacy wired networks, these next-generation private cellular environments blend IT, OT, and IoT into a single fabric, with connected machines, smart sensors, SIM-based devices, non-SIM devices connected via cellular routers or dongles, remote operators, and critical data flows that often-run 24/7.

And yet, many enterprises assume that simply adding encryption or firewalls to the core is enough. In reality, private network security demands a deeper strategy, one that spans everything from SIM and device lifecycle management to zero trust segmentation, real-time threat detection, OT asset visibility, and edge workload protection.

In this whirepaper, we break down the core capabilities that every enterprise should look for when evaluating private network security solutions.








WHY PRIVATE NETWORK SECURITY DEMANDS A NEW APPROACH

Enterprise private networks expand the traditional threat surface in ways many organizations underestimate. Public mobile networks place the burden of end-to-end security on licensed operators, who provide centralized cores, national roaming controls, and telecom-grade identity management.

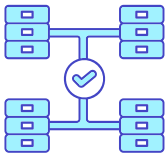
But with private 5G, LTE, and CBRS, enterprises inherit that responsibility. They operate their own local RAN and core. They choose spectrum bands, provision SIMs and devices, run on-site or cloud-based cores, and often interconnect with corporate IT and cloud services.

A single site might have:

SIM-ENABLED IOT SENSORS AND PRODUCTION MACHINERY ON THE SHOP FLOOR

LEGACY OT SYSTEMS THAT NEED TO INTERCONNECT WITH NEW WIRELESS GATEWAYS

REMOTE WORKERS USING SECURE SIM-BASED LAPTOPS, TABLETS, OR HANDHELDS



MULTI-ACCESS EDGE COMPUTE (MEC) NODES PROCESSING SENSITIVE WORKLOADS NEAR REAL-TIME

THIRD-PARTY CONTRACTORS, SYSTEMS INTEGRATORS, AND ROAMING PARTNERS THAT NEED CONDITIONAL NETWORK ACCESS

Traditional enterprise firewalls, VLANs, or Wi-Fi Network Access Control (NAC) systems can't address the unique security layers required for a local cellular network. Private 5G/LTE networks need carrier-grade security measures plus enterprise-grade threat detection and policy enforcement that integrates with existing SOC/SIEM systems.

Key challenges include:

SECURE SIM AND DEVICE IDENTITY LIFECYCLE

Who issues, verifies, monitors, secures, revokes, and/or rotates SIM and device credentials – and ensures that the right device is the one connected.

SLICE ISOLATION

How do you ensure one use case (like autonomous vehicles) is segmented from another (like worker tablets)?

EDGE WORKLOAD SECURITY

How are data streams secured at MEC nodes or when backhauled to the cloud?

OT/IOT DEVICE TRUST

How do you profile, monitor, and block rogue industrial assets that weren't designed with built-in security?

Enterprises must combine the best of telecom security, such as encryption, signaling protection, and device-based authentication and access control, with enterprise zero trust, NAC, and SOC integration to close these gaps.

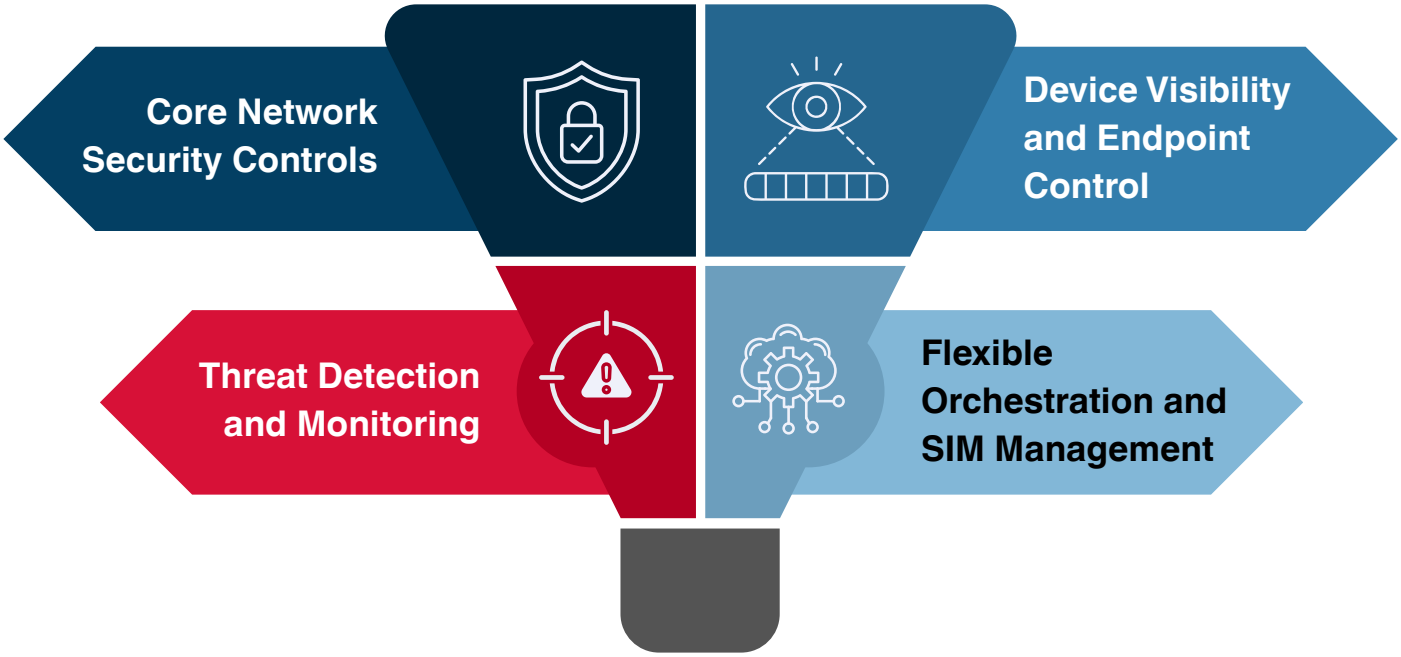
4 ESSENTIAL PILLARS OF ENTERPRISE PRIVATE NETWORK SECURITY

Protecting a private 5G, LTE, or CBRS network at enterprise scale requires more than basic encryption or traditional perimeter firewalls. Modern private mobile networks blend cellular infrastructure with enterprise IT systems, operational technology, and distributed edge computing. Each layer introduces new security demands that must work together under a unified strategy.

Drawing on real-world deployments, these four pillars define the essential areas every organization must address:

- Core Network Security Controls
- Device and Endpoint Visibility and Control
- Detection, Monitoring, and Response
- Flexibility and Orchestration

In the next sections, each pillar is broken down into the specific capabilities that matter most and how they shape practical vendor requirements when planning or expanding your private mobile network.



1 Core Network Security Controls for Private 5G & LTE

Securing a private 5G, LTE, or CBRS network starts with strong controls at the core. This pillar covers the capabilities that protect user and control plane traffic, authenticate devices, enforce access rules, and ensure that only trusted identities can move across network slices. For CBRS deployments, this means core traffic and slice isolation should align with dynamic spectrum assignments to maintain secure, interference-free operations.

Each of these capabilities builds on the previous one — starting with strong device identity, advancing through granular access and segmentation, and culminating in encryption that secures data throughout its lifecycle.

CAPABILITY	WHAT IT DELIVERS
Secure SIM Lifecycle Management	SIMs are the foundation of identity in private cellular networks, but SIM credentials alone aren't enough. Enterprises must manage the entire SIM lifecycle — issuance, activation, rotation, and revocation — and bind each SIM to a broader, continuously monitored device identity. This approach ensures that credentials remain valid only for trusted devices and users, reducing the risk of cloned or compromised SIMs being used to access the network.
Policy Enforcement and Access Control	Dynamic policy engines define who and what can connect — and under what conditions. Role-based controls, real-time blocking, and contextual policies make it harder for rogue devices or unauthorized endpoints to remain connected. These controls complement device-based identities by adding behavioral and situational context to access decisions.
Zero Trust Segmentation	Zero Trust principles require strict segmentation to prevent lateral movement. By dividing network traffic into micro-segments and enforcing least-privilege access, enterprises ensure that even if a device is compromised, it cannot move freely between network slices, applications, or workloads.
Integrated with Core Vendor	The most effective private network defenses are built into the mobile core itself. When traffic inspection, policy enforcement, and segmentation are natively integrated with the core stack, enterprises gain real-time protection, streamlined management, and fewer blind spots. This integration also supports compliance and simplifies coordination between telecom and enterprise security teams.
Encryption and Data Protection	Encryption protects data in motion and at rest — but it's the final layer, not the first. End-to-end encryption between devices, edge nodes, and applications ensures that even if a connection or credential is compromised, the data remains unreadable. Encryption standards in the private mobile core safeguard telemetry, video, and control data from interception or tampering.

2 Device Visibility & Endpoint Control in Private Networks

A secure core is only part of the story. After SIM identities and access policies are established, enterprises must maintain continuous visibility into every device interacting with the network — from modern IoT gateways to legacy industrial machines. Visibility ensures that authentication isn't treated as a one-time event but as part of an ongoing trust model, where every connected asset is continuously monitored, profiled, and verified throughout its lifecycle. This pillar focuses on the ability to discover, profile, and protect all assets, both cellular and non-cellular, ensuring that each device remains trustworthy and behaves as expected within its operational context.

CAPABILITY	WHAT IT DELIVERS
Comprehensive Device Discovery & Fingerprinting	With thousands of cellular and non-cellular assets connecting simultaneously, enterprises need continuous discovery. Fingerprinting uses network behavior, hardware identifiers, and SIM bindings to confirm that each asset is genuine. This eliminates blind spots and enables real-time tracking of devices as they join or leave the network.
Unified Device Identity (Cellular + Non-Cellular)	Private networks often host both SIM-enabled and legacy non-cellular devices behind gateways or CPE. Extending identity and policy visibility to those endpoints ensures consistent enforcement — even when assets connect via Ethernet, Wi-Fi, or industrial fieldbus interfaces.
Contextual Device Behavior Monitoring	Authentication alone doesn't guarantee security over time. Continuous behavioral monitoring detects deviations from expected patterns — such as abnormal traffic volumes, repeated authentication attempts, or protocol misuse — before they escalate into incidents.
OT and IoT Context Awareness	Industrial environments include PLCs, sensors, and legacy OT devices that were never designed for modern security. Solutions must interpret OT-specific protocols, detect unsafe commands, and isolate vulnerable systems without disrupting production. This contextual awareness allows the network to recognize "normal" process behavior and react intelligently when anomalies appear.
Automated Response and Enforcement Integration	The value of visibility lies in the ability to act. When an anomaly is detected — such as an unauthorized firmware update or rogue gateway — automated enforcement can quarantine the asset, revoke its SIM credentials, or adjust network policy instantly. Integration with the policy and segmentation layers established in the core ensures rapid, coordinated response.

By unifying identity, visibility, and enforcement, enterprises gain a living inventory of trusted assets — the foundation for intelligent threat detection, automated remediation, and true zero trust operations.

3 Threat Detection & Monitoring for Private 5G and LTE

Even the best core and device controls mean little without strong situational awareness and the ability to act quickly when something goes wrong.

After enterprises establish identity, access, and continuous device visibility, the next critical step is detecting and responding to threats in real time. Visibility tells you what is on the network — detection tells you what it's doing and whether that behavior is safe. Private 5G, LTE, and CBRS networks introduce unique layers — from the RAN to edge nodes and core slices — where threats can emerge and spread quickly if not continuously monitored. This pillar focuses on bridging operational visibility with real-time analytics, ensuring that every event, anomaly, and behavioral shift can trigger an informed, coordinated response across IT, OT, and cellular domains.

CAPABILITY	WHAT IT DELIVERS
Threat Detection and Response	Enterprises need to identify suspicious or malicious activity before it disrupts operations. Built-in threat detection analyzes device behavior, traffic flows, and control-plane messages for anomalies. When threats are found, automated response actions — such as isolating the asset or revoking SIM credentials — prevent escalation without manual intervention.
Network Visibility and Monitoring	Continuous monitoring of all network layers — RAN, edge, and core — provides a unified picture of traffic and performance. Deep inspection of both user and control planes helps identify unusual signaling, unauthorized slice access, or bandwidth anomalies that might indicate lateral movement or compromise.
Integration with Enterprise SOC/SIEM	Private networks must feed threat and telemetry data into the enterprise's broader security stack. Integration with existing SOC and SIEM tools enables faster detection, incident correlation, and response coordination across IT, OT, and cellular environments. This connection closes the gap between telecom security and enterprise cyber defense.
Managed Security Services	Many organizations lack in-house expertise to manage continuous 5G threat monitoring. Managed service providers can extend coverage with 24/7 threat hunting, incident response, and specialized telecom security knowledge — critical for industrial environments that operate around the clock.

With threat detection integrated into enterprise SOC workflows, organizations gain a unified operational view — where incidents from OT, IT, and private 5G domains can be triaged, correlated, and contained before impacting production.

4 Flexible Orchestration & SIM and Device Management for Private Networks

After enterprises establish core security, visibility, and real-time detection, the final pillar focuses on orchestration and adaptability — ensuring that private networks can evolve securely as operations expand. Enterprise private networks rarely stand still. They must continuously adapt to new sites, devices, partners, and regulatory requirements.

As these networks scale, so does the need for operational flexibility, multi-vendor interoperability, and automation that prevents complexity from becoming a security risk. This pillar highlights the capabilities that help enterprises scale securely, avoid vendor lock-in, and manage SIM and device lifecycles efficiently across distributed environments.

CAPABILITY	WHAT IT DELIVERS
Enterprise Focus	Not all network security solutions are built for large-scale or industrial realities. A strong enterprise focus means understanding multi-site management, regional compliance, and the need to integrate with existing IT and OT ecosystems. Solutions designed for enterprise operations align security with real-world workflows rather than theoretical carrier models.
Vendor Agnostic	Many organizations combine multiple RAN, core, and edge solutions to meet coverage, spectrum, or legacy needs. Vendor-agnostic orchestration maintains consistent security and policy enforcement, and single-pane-of-glass visibility across these heterogeneous environments, avoiding dependency on a single vendor's stack and preserving design flexibility as the network evolves.
Cloud and Edge Security	As private 5G and LTE deployments increasingly extend into distributed edge and hybrid cloud environments, security must follow workloads wherever they move. Protecting data and applications across MEC nodes, local data centers, and cloud instances ensures consistent enforcement for latency-sensitive and mission-critical operations.
Orchestration and SIM, and Device Management	One of the biggest operational differences between Wi-Fi and private cellular is the reliance on SIMs or eSIMs for device authentication. Enterprises need centralized tools to issue, activate, suspend, or revoke SIM credentials at scale – while validating that each profile matches the correct device. When mismatches occur, orchestration systems should automatically adjust profiles or deactivate the SIM or device to maintain security and ensure seamless, secure onboarding. Effective orchestration also governs network slicing, QoS, and policy updates — giving teams unified control over how devices connect, communicate, and consume resources.

In CBRS environments, where spectrum assignments can shift dynamically, orchestration tools are particularly vital. SIM and slice management systems must ensure that only authorized devices access licensed bands — maintaining compliance, resiliency, and operational continuity as network conditions change.

Together, these capabilities keep private mobile networks open, scalable, and adaptable. They enable enterprises to extend consistent security policies into new sites and workloads while automating repetitive management tasks that would otherwise overwhelm operational teams.

When an organization unites all four pillars - strong core controls, continuous device visibility, real-time detection and response, and flexible orchestration - it achieves an operationally mature, secure-by-design private 5G, LTE, or CBRS network that grows safely with the business.

KEY VENDORS FOR PRIVATE 5G, LTE AND CBRS SECURITY: WHO PROVIDES WHAT

PRIVATE NETWORK SECURITY VENDORS

Purpose-Built Private Network Security Vendors	Telco Core Vendors for Private 5G and LTE	Enterprise Security Vendors for Private Networks	SIM Provisioning and Orchestration Security Vendors	Edge Computing and Cloud Security Vendors
				
ONELAYER CTONE	NOKIA HUAWEI ZTE celona SAMSUNG	paloalto NETWORKS FORTINET zscaler NOZOMI NETWORKS cisco	Kigen THALES Giesecke+Devrient	HPE f5 allot ZABBIX NETSCOUT HIGHWAY 9 NETWORKS

SOURCE: TECKNEXUS

Securing a private LTE, 5G, or CBRS network takes more than a single vendor's tools. Most enterprises combine multiple layers, from carrier-grade core controls to zero trust policy engines, to protect traffic, devices, and critical workloads end-to-end.

PRIVATE NETWORK SECURITY VENDORS

Purpose-built security for private LTE, 5G, CBRS. Provides device fingerprinting, OT/IoT visibility, zero trust segmentation, and real-time policy enforcement inside local networks. Closes gaps that traditional firewalls or core controls don't cover.

ONELAYER CTONE

TELCO CORE VENDORS

Carrier-grade core networks for private mobile. Provide deep RAN/core integration, traffic encryption, slice isolation, and subscriber management. Typically partner with specialist security vendors for advanced device segmentation or SOC integration.

NOKIA HUAWEI ZTE celona SAMSUNG

ENTERPRISE SECURITY LEADERS

Mature zero trust access, SOC/SIEM integration, policy engines that extend enterprise IT security frameworks into local private mobile deployments. Often used to unify IT + OT security, but do not provide SIM or core-level traffic enforcement themselves.

paloalto NETWORKS FORTINET zscaler NOZOMI NETWORKS CISCO

SIM & ORCHESTRATION VENDORS

Experts in secure SIM, eSIM, and credential lifecycle management. Enable dynamic SIM provisioning, remote activation/suspension, and slice alignment for thousands of endpoints — essential for CBRS and flexible multi-site deployments.

Kigen THALES Giesecke+Devrient

EDGE & CLOUD SECURITY VENDORS

Secure traffic and workloads between private core, edge MEC nodes, and hybrid/cloud environments. Deliver workload protection, anomaly detection, network intelligence, and flexible monitoring. Often used to extend visibility and policy control beyond the core.

HPE allot See. Control. Secure. f5 ZABBIX NETSCOUT HIGHWAY 9 NETWORKS

Questions to Ask When Choosing Private Network Security Vendors

Once you understand the four pillars of private network security and how today's vendors align, the next step is knowing exactly what to ask when evaluating your shortlist. Clear questions help ensure that what looks complete on a slide meets your real-world needs in production. Here are a few practical questions every enterprise team should raise with potential partners:

COVER ALL FOUR SECURITY PILLARS

Do they truly cover all four pillars — core network security, device visibility and control, detection and response, and operational flexibility — or do you need additional solutions to close the gaps?

VENDOR-AGNOSTIC

Are their solutions vendor-agnostic enough to integrate smoothly with your chosen RAN, core, or edge platforms without locking you in?

INTEGRATION WITH EXISTING SYSTEMS

Can their security tools connect with your existing SOC and SIEM systems so you can manage incidents and compliance from one place?

SECURING OT AND IT ASSETS

How well do they secure OT and IoT assets that often have unique protocols, legacy limitations, and operational constraints?

MANAGED SECURITY

If your in-house security team has limited capacity, can they deliver managed security services to monitor, hunt, and respond 24/7?

ROBUST ORCHESTRATION

Do they provide robust orchestration for SIM lifecycle management, including provisioning, activation, suspension, and policy updates for devices across multiple sites?

Secure Your Private Network: Final Takeaways

Private 5G, LTE, and CBRS networks promise local control, industrial-grade reliability, and the flexibility to support complex, high-value use cases. Whether you deploy private LTE on licensed bands or CBRS shared spectrum, these same pillars apply, giving you local control, reliable coverage, and enterprise-grade security.

But realizing that promise takes far more than basic encryption or a secure core alone. True enterprise-grade security demands full-stack coverage, trusted device identity, continuous threat detection and response, tight integration with your SOC, and flexible controls that adapt as your network evolves.

Choosing the right mix of vendors and partners is mission-critical for industrial environments where OT and IoT assets, local edge workloads, and sensitive data flows must work together securely around the clock.

Whether you rely on one trusted provider or a small, well-integrated team, the key is knowing exactly who covers what, where the gaps are, and how each layer fits your operating reality.

SPONSORED BY

TECKNEXUS

ONELAYER

WHITEPAPER

For more information on OneLayer Private Network Security visit https://onelayer.com/

For inquiries about sponsoring content, please reach out to us at sales@tecknexus.com. We look forward to collaborating with you to deliver insightful and impactful content.

THANK YOU

This content was commissioned by **OneLayer** and independently written by TeckNexus. While commissioned by OneLayer, the TeckNexus team maintained full control over the content, ensuring an objective and well-researched analysis consistent with our commitment to analytical integrity.