celona × ONELAYER

SOLUTION BRIEF

Secure, High-Performance Private 5G/LTE with Unified Visibility and Control

Growing interest in private 5G/LTE for industrial operations is driven by the need for greater network performance, reliability, and secure connectivity across IT and OT environments.

The Challenge:

Extending Enterprise Visibility into Private Cellular Networks

As private LTE and 5G become foundational to enterprise operations, organizations increasingly rely on the cellular core as a secure, policy-enforced control point for mission-critical connectivity across IT and OT environments. Unlike traditional IP networks, private cellular networks are built around SIM-based identity, introducing new operational models for onboarding, access control, and segmentation.

As enterprises connect groups of devices behind routers and gateways, they require a way to extend cellular visibility and policy beyond the SIM itself. Without native mechanisms to expose device identity and policy context beyond the SIM, organizations risk losing the fine-grained control and observability that private 5G/LTE is designed to deliver, making it challenging to align cellular operations with existing IT and OT security workflows, asset inventories, and Zero Trust initiatives.

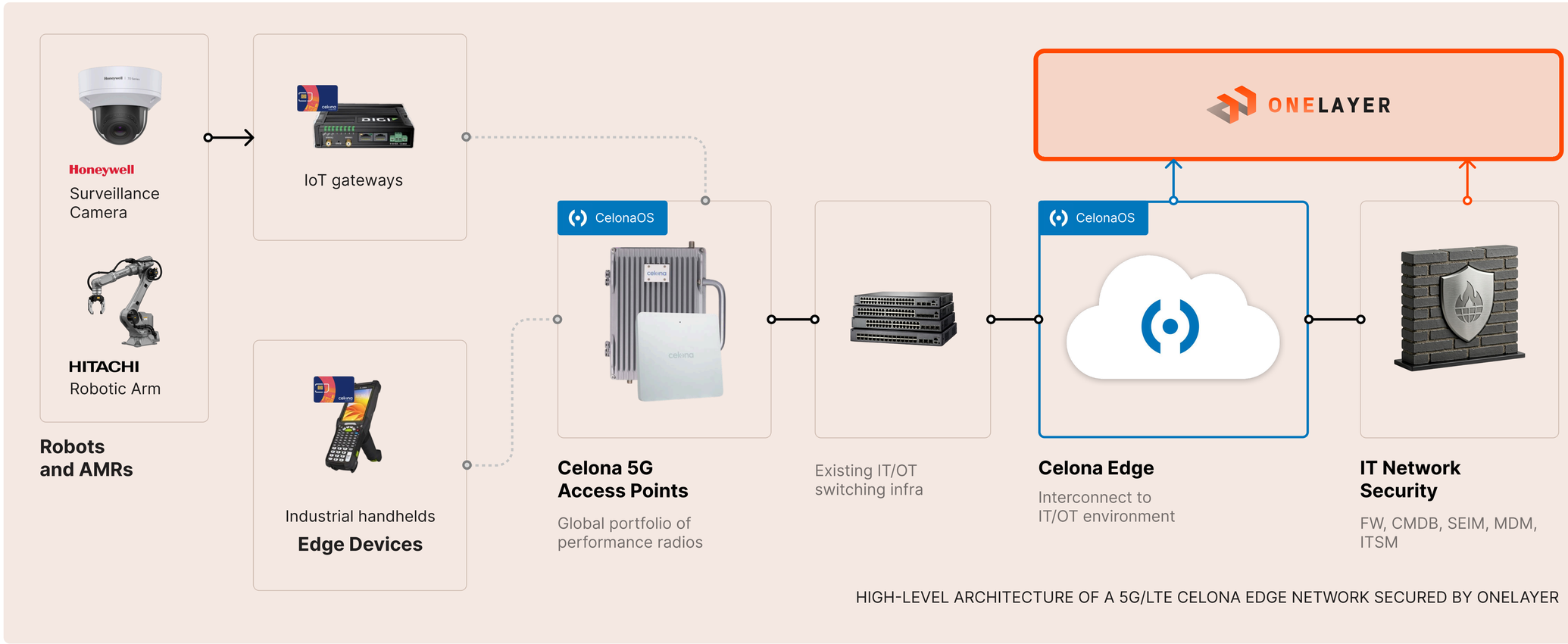
The Solution:

A Unified Foundation for Secure Private Wireless

Celona's AerLoc architecture delivers a secure-by-design private wireless platform that provides native IMEI/IMSI-based device identification, access control, and the built-in MicroSlicing™ feature enables network-based segmentation enforced directly at the cellular core. This foundation enables enterprises to deploy high-performance private LTE and 5G networks with deterministic security, predictable behavior, and centralized policy control. Celona further extends this foundation with Supernetting, a core-native capability that enables visibility, policy enforcement, and segmentation for multiple devices operating behind a single cellular connection.

OneLayer complements the Celona platform by adding extended device intelligence, including deep device fingerprinting, behind-router visibility, and behavioral context. This additional context enhances Celona's native capabilities by correlating SIM-based identity with device-level attributes, enabling more granular visibility and adaptive policy decisions across IT, OT, and cellular domains. Together, Celona and OneLayer enable enterprises to maintain core-level enforcement, segmentation, extended visibility, and orchestration into existing enterprise security and operations workflows. The result is a unified private wireless environment that combines performance, reliability, and native security with richer device context—eliminating operational blind spots without introducing complexity.

USE CASE	celona	ONELAYER	OUTCOME
Automated SIM & Device Onboarding	Full SIM lifecycle management with native IMEI/IMSI based onboarding	Device fingerprinting, SIM-to-device correlation, and automated remediation	Faster onboarding with verified SIM-to-device integrity and simplified issue resolution
Device Observability	Core-level visibility into cellular devices using SIM, radio, and IP session attributes including devices behind cellular routers/gateways	Extended visibility into devices behind routers and adapters	Eliminates blind spots beyond the cellular layer and strengthens asset management
Device Access Control	Native access control enforced at Celona Edge using IMEI/IMSI and network-level policies	Access control based on device identity and behavior, i.e. prohibi ted manufacturer, geo-fencing	Reduces risk from unapproved and rogue devices while improving security and compliance
Zero Trust Segmentation & Orchestration	Native Zero Trust segmentation enforced at the Celona Edge using network-based policies	Micro segmentation based on device identity and behavior, including Purdue-aligned models	Reduces security risk from lateral movement while preserving deterministic enforcement
Enforcement at the Core	Native policy enforcement at the Celona Edge with integration into enterprise security ecosystems	Anomaly detection and risk insights that trigger adaptive enforcement actions via the Celona Edge	Reduces reliance on external firewalls for cellular traffic, improving control and reducing complexity



HIGH-LEVEL ARCHITECTURE OF A 5G/LTE CELONA EDGE NETWORK SECURED BY ONELAYER

How it Works

1. Celona establishes the secure private wireless foundation, identifying and enforcing policy for connected devices using native SIM-based identity. OneLayer integrates with the Celona Edge to extend this visibility by discovering and fingerprinting all devices, including those behind routers and adapters, establishing broader asset awareness from day one.
2. Extended device identity and behavioral context from OneLayer augments Celona Edge, expanding visibility beyond IMEI/IMSI and enhancing Zero Trust access policies based on posture, behavior, and risk.
3. Segmentation is enforced natively by Celona Edge using network-based Zero Trust policies and is enhanced with additional device-level granularity from OneLayer, including Purdue-aligned models that adapt as devices move or change.
4. The unified device identity established and enforced by Celona, and enriched with additional context from OneLayer, powers orchestration across firewalls, NAC, OT security platforms, and ITSM/CMDB systems—aligning cellular operations with existing IT/OT controls.
5. Continuous monitoring of cellular signaling and device behavior enables anomaly detection and insights, triggering automated remediation and policy actions.

Better Together:

celona × ONELAYER

Celona and OneLayer combine to give enterprises a private 5G/LTE network that delivers high performance with unified visibility and control across IT, OT, and cellular domains. Celona provides the reliable, cloud-managed wireless foundation, while OneLayer adds device-level intelligence, adaptive security, and seamless integration into existing enterprise tools. Together, they eliminate operational blind spots and make onboarding, access control, and segmentation more precise and efficient, creating a private wireless environment that operates as a natural extension of the enterprise infrastructure.

Save time

with faster, error-free SIM & device onboarding

Strengthen asset management

with visibility behind routers

Improve network security

with granular device access control

Reduce risk of lateral movement

with perdue-aligned segmentation