Celona AerLoc

One identity, one security model across every radio — security built into the converged wireless fabric.

/ CONTENTS

/ THE PROBLEM

The security model hasn't kept up

Every time wireless crosses a new threshold in the enterprise, it brings a new security model — and that moment is here again. As factories, warehouses, and energy sites move critical operations onto wireless, this layer now carries the business's most operationally critical traffic. Yet the security around it is still assembled from siloed parts: the divide between IT and OT, and the disconnect between perimeter and cloud-based security services, have produced fragmented, inefficient architectures that restrict operational flexibility and drive up cost.

That fragmentation is worst where it matters most. IT needs flexibility; OT needs strict, deterministic control — and legacy systems force teams to bridge the two with duplicate infrastructure and bolted-on controls. Identity, segmentation, and isolation get added after the fact, radio by radio, instead of living in the network itself.

As enterprises design the next generation of wireless — private 5G and Wi-Fi together — they have a chance to redefine security architecture: converge IT, OT, and every radio into one fabric, with **identity and isolation built in from day one**.

Legacy disparate security architecture — the challenges

- Client-based ZTNA is unsuitable for headless OT devices.
- OT is constrained by wired-only infrastructure.
- OT apps aren't built for cloud-first ZTNA.
- Duplicated IT/OT infrastructure is costly to build and maintain.
- No single identity or security model spans every radio.

/ DESIGN PRINCIPLES

Key considerations for a converged secure access network

01

Convergence of access and security across IT, OT — and every radio

Converging access and security for IT and OT avoids the siloed solutions that have long plagued enterprise networks. A holistic framework supports diverse device types across IT and OT — and applies the same identity, segmentation, and policy whether a device is on private 5G or Wi-Fi. That reduces complexity and lowers operational cost.

02

Clientless zero trust

Managing VPN clients has always been a burden, and many OT and IoT devices are closed-box systems that can't run an agent at all. Zero-trust principles that require no client software meet the security demands of these devices — a strong, network-issued identity with nothing to install. This is essential for OT, where device constraints rule out traditional client-based models.

03

Security in the fabric, not bolted on

Modern enterprises are geographically dispersed, with operations at the edge and in the cloud. Identity, segmentation, and isolation therefore have to live in the network fabric — distributed and enforced close to the device — rather than added later at a single choke point. A model built into the fabric scales with the enterprise and protects hyperlocal edge and remote cloud resources alike, without compromising security.

/ THE SOLUTION

Introducing Celona AerLoc

AerLoc is the security paradigm built into Celona Orion — the converged wireless fabric spanning private 5G, Wi-Fi, and public mobile. It extends one identity and one security model across every radio, integrating with the network and security infrastructure enterprises already run. The result: private wireless that deploys securely across industrial and traditional enterprise environments — with no duplicate network to build or maintain.

Celona Orion · AerLoc — one identity for every device on the converged fabric: zero-trust identity, micro-segmentation with an IT/OT air-gap, and full visibility.

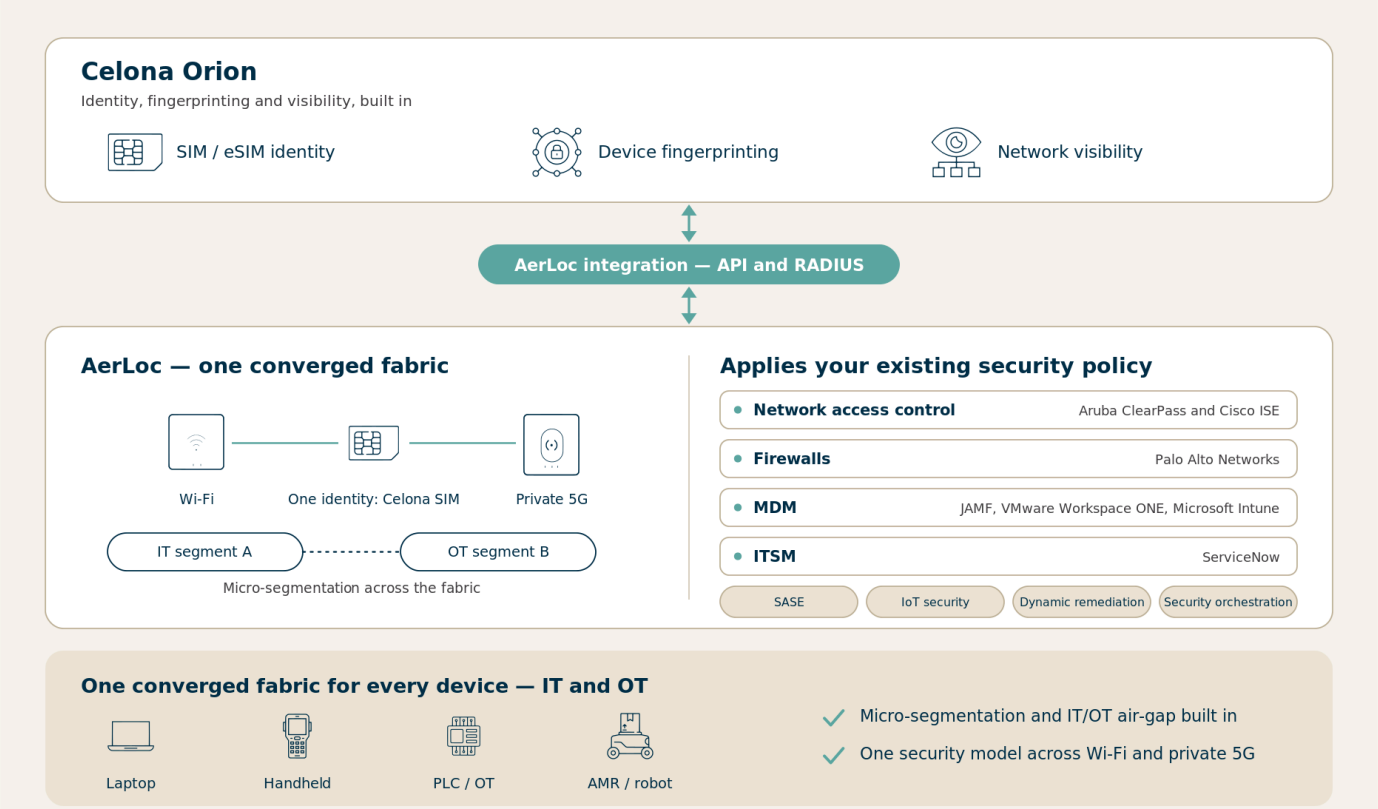
Trust designed in, not bolted on

AerLoc inherits the trust model of the platform it's built into. Celona Orion is a single trusted system, not assembled parts: Celona Orchestrator AI for secure agentic operations — bring your own LLM; a network edge whose entire software stack is written by Celona; and Celona access points that carry Wi-Fi 7 and public and private cellular through one trusted supply chain. End to end from a single source — built to carry your most critical traffic.

/ ARCHITECTURE

How AerLoc secures the converged fabric

AerLoc secures every device across the converged fabric through three layers — identity, segmentation, and integration — applying your existing IT/OT security policy across every radio.



AerLoc: the Celona SIM is one identity for every device across the converged fabric (Wi-Fi and private 5G), applying your existing security policy through open API and RADIUS.

Identity	Every device authenticates with a Celona SIM credential the network issues and trusts. It's clientless, so even unmanaged and headless OT devices get a strong identity with nothing to install — and there's no device-side software or agent to manage.
Segmentation and isolation	The fabric enforces micro-segmentation per device and keeps IT and OT traffic separated end to end. Through Celona MicroSlicing, that segmentation runs over the air using 3GPP standards and extends into the enterprise LAN — physically and logically separating critical operational data from general enterprise traffic. Segmentation is granular down to the individual traffic flow: MicroSlicing maps each IP flow to pre-defined enterprise network segments such as VLANs or firewall zones, over the air and on the wire.
Integration	Through open APIs and RADIUS, AerLoc applies your existing IT/OT security policies to wireless devices, so the tools you already run stay in control — NAC, firewalls, MDM, ITSM, and SASE, whether they run in the cloud, on-premises, or hybrid. Extending the same approach to posture-assessment and security-orchestration platforms enables localized, responsive enforcement at the edge, significantly reducing the attack surface. These integrations also enable dynamic, zero-touch authorization changes in response to detected threats — automatically blocking or quarantining compromised devices.

Because this lives in the fabric rather than in any single radio, the same identity, policy, and isolation apply whether a device is on private 5G or Wi-Fi — and follow it as it moves. Security and operations teams get full visibility into every device from one place.

Benefits

01 **One security model across every radio** — the same identity, segmentation, and policy reach Wi-Fi and private 5G alike.

02 **Lower cost, one infrastructure** — a built-in IT/OT air-gap on one converged network, with no duplicate to build or pay for.

03 **Clientless zero trust** — a strong, network-issued identity for every device, with full network visibility.

04 **Fits your security stack** — native integration with the firewalls, NAC, and security tools you already run.

05 **Dynamic policy enforcement** — localized, responsive enforcement at the edge, down to the individual device or user.

/ CAPABILITIES

Additional AerLoc capabilities

Beyond its core identity, segmentation, and integration layers, AerLoc brings cellular-grade security mechanisms — proven over decades in public mobile networks — to every device on the fabric.

SIM-based mutual authentication

Devices and the network validate each other using SIM credentials and 3GPP protocols such as 5G-AKA, EAP-AKA, and EAP-AKA′ (used for SIM-based authentication over Wi-Fi). Authenticating both sides of the connection hardens the fabric against man-in-the-middle attacks and rogue devices.

Strong device identification

AerLoc uses deterministic, immutable identities from cellular technology — SIM and eSIM (ICCID), device hardware (IMEI), and embedded identity document (EID). Locking authorized SIMs to authorized devices keeps credentials from moving to unauthorized hardware.

Enhanced user confidentiality

Subscriber identities are cryptographically concealed in transit using SUPI and SUCI, preventing eavesdropping and unauthorized tracking of users and devices.

Zero-touch eSIM onboarding via MDM

For fleets managed with MDM platforms such as JAMF, VMware Workspace ONE, and Microsoft Intune, Celona automates eSIM provisioning through API integration — so IT and OT staff can provision hundreds or thousands of devices remotely, with protection against tampering and unauthorized access.

Device fingerprinting for compliance

The fabric identifies device types from unique signatures visible to the network and exposes that context through APIs, giving enterprise security systems richer device context for policy compliance.

Full visibility of gateway-connected endpoints

Intelligent routing and supernetting give IT and OT staff direct visibility of, and accessibility to, endpoints behind mobile gateways — devices that would otherwise sit on discrete VLANs or subnets hidden from the teams responsible for securing them.

Consistent policy with static IP pools

Critical devices can be assigned to a static IP address pool while remaining reachable and visible from the rest of the enterprise network, ensuring consistent accessibility and policy enforcement.

Secure cloud-based management

Management data travels to the Celona Orchestrator over encrypted TLS and is securely stored in the cloud. SAML v2 single sign-on lets enterprises bring their existing identity provider for role-based access control, in line with security and compliance policies such as multi-factor authentication.

/ COMPARE

How AerLoc compares

The real question isn't which radio you run — it's whether one identity and one security model reach across all of them. With AerLoc, they do.

	LEGACY BOLTED-ON SECURITY	AERLOC — SECURITY IN THE FABRIC
IDENTITY	Passwords, certificates, or per-device agents; unmanaged and OT devices are left out.	A SIM credential the network issues and trusts; clientless, even for headless OT devices.
SEGMENTATION	Added after the fact at a choke point; often a duplicate IT/OT network.	Micro-segmentation in the fabric with a built-in IT/OT air-gap, on one network.
EVERY RADIO	A separate security model per radio.	One security model across Wi-Fi and private 5G alike.
INTEGRATION	Rip-and-replace or bolt-on point tools.	Open API and RADIUS apply the security tools you already run.
VISIBILITY	Partial; non-cellular endpoints hidden behind gateways.	Full visibility of every device from one place.

/ USE CASES

Technology use cases

AerLoc secures the wireless layer wherever operations are moving onto it — from the plant floor to the loading dock to regulated, high-security sites.

IT/OT convergence — run OT securely on the same infrastructure as IT, with a built-in air-gap. · MANUFACTURING

Clientless zero trust — strong identity for unmanaged and IoT/OT devices that can't run an agent.

The connected worker — one identity and one secure experience as people and devices move across the site.

Warehousing and logistics — secure connectivity for scanners, AMRs, and automation. · DISTRIBUTION AND LOGISTICS

Regulated, high-security environments — full visibility and segmentation where it's required. · HEALTHCARE· OIL AND GAS

/ THE PAYOFF

One security model, every radio

AerLoc represents a shift in enterprise networking: security built into the converged wireless fabric rather than bolted on afterward. By unifying IT and OT through SIM-based authentication, clientless zero trust, and granular segmentation — across private 5G and Wi-Fi alike — Celona lets enterprises deploy scalable, secure private wireless that carries their most operationally critical traffic. And that security rests on a platform where trust is designed in, not bolted on: from Orchestrator AI in the cloud to the network edge to the access point, built end to end by Celona on one trusted supply chain — a single trusted system, not assembled parts.

The real question isn't which radio you run — it's whether one identity and one security model reach across all of them. With AerLoc, they do — solving today's challenges while future-proofing the enterprise for what comes next.

/ REFERENCES

01 Network access control (NAC) integration — Cisco ISE

02 Network access control (NAC) integration — Aruba ClearPass

03 Celona eSIM / MDM lifecycle management

04 Palo Alto Networks alliance

05 Compliance and privacy

/ ABOUT CELONA

Celona is the company behind Celona Orion, the industry's first Agentic Converged Wireless Platform. Enterprises in manufacturing, logistics, mining, energy, and healthcare use Celona to connect the machines, sensors, autonomous systems, and people running their physical operations — with the deterministic performance, security, and enterprise control that off-the-shelf wireless can't deliver. For more information visit celona.io.

celona

hello@celona.io

900 E Hamilton Ave Suite 200, Campbell, CA 95008, United States