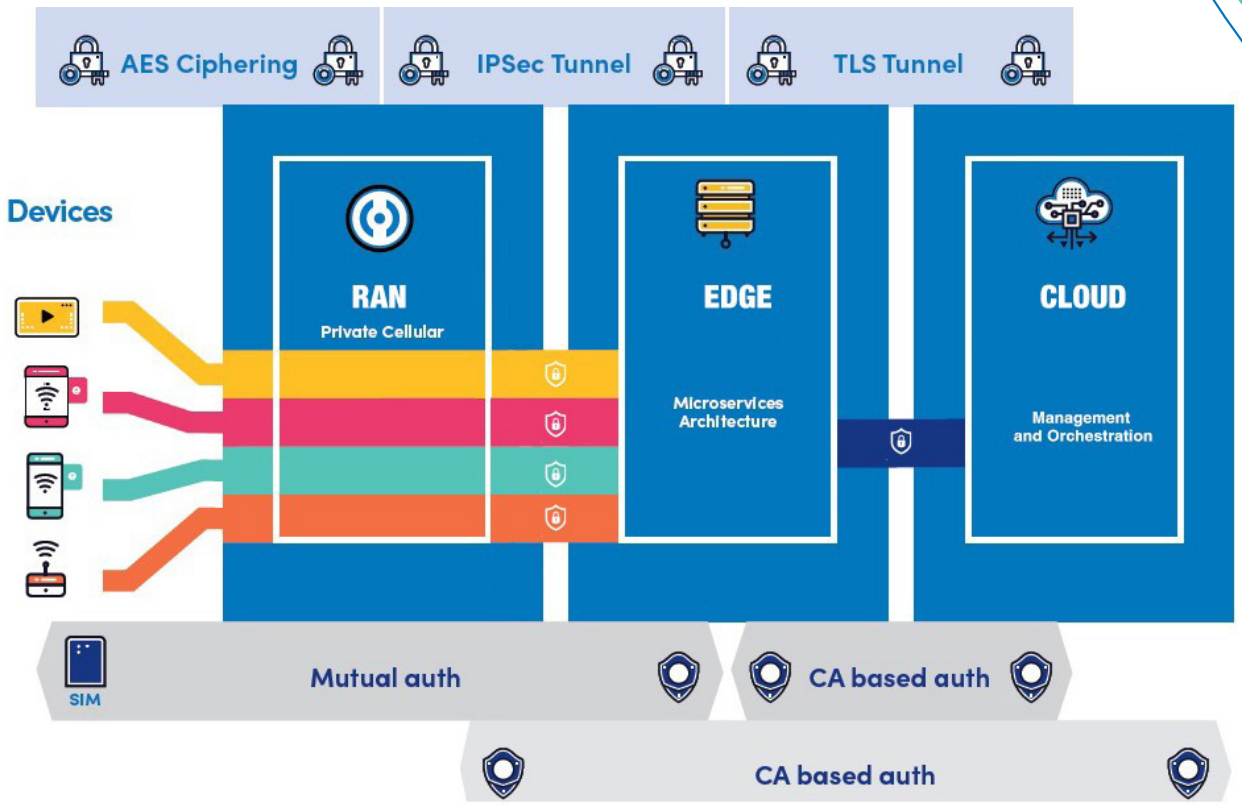
Security Feature brief

New 5G LAN technology from Celona offers the industry's most comprehensive suite of security capabilities across the full IP protocol stack, giving organizations the highest levels of user confidentiality and data privacy possible from the RAN across the enterprise L2/L3 LAN.



Data privacy with full stack L1-L7 encryption

Unlike Wi-Fi, Private wireless networks utilize modern cellular technology that encrypts radio signals at the physical layer transmitted between APs and user devices. Celona provides 128-bit AES ciphering over the air, offering quantum resistant cryptography that meets the NSA's CNSA 2.0 requirements. 5G technology brings enhancements in key derivation and rotation where the master key is never shared or exposed, and the device's identity is concealed for enhanced privacy. All enterprise data remains under complete control of the enterprise.

Strong device identification and authentication

New 5G LANs combine the deterministic and immutable identities inherent in cellular technologies, such as the use of Subscriber Identity Modules (SIMs or eSIMS). Celona provides the locking of authorized SIMs to authorized devices (IMEIs to ICCIDs). This eliminates the ability to access the network using credentials not authorized for a given device.

Enhanced user confidentiality

To further prevent eavesdropping or unauthorized access within 5G LANs, Celona makes use of subscription concealed identifier (SUCI) technology that cryptographically hides subscriber identities during the initial connection setup and authentication process.

Certificate-based mutual authentication

Celona-connected devices join the network using certificate-based mutual authentication - a process that validates both the endpoint to the network and the network to the endpoint, mitigating man-in-the-middle attacks and spoofed or rogue devices. The authentication protocols in Celona's 5G LAN include 5G-AKA and EAP-AKA, which bring enhanced flexibility and security to the authentication process.

Granular end-end traffic segmentation

Celona 5G LANs not only segment but separately encrypt groups of devices or applications as granularly as on a per-flow basis – over the air and on the wire. Celona's 5G LAN solution combines the deterministic and unique identities inherent in cellular technologies with translated identities for integration with the enterprise LAN security controls such as VLANs and ACLs. Celona's patented MicroSlicing™ technology automatically maps individual IP traffic flows and groups devices directly to pre-defined enterprise network segments - such as secured VLANs, firewall zones, or other enforcement points.

Robust API integrations with third-party security systems

Celona 5G LANs support API integrations with existing firewalls, IoT security systems and Network Access Control (NAC) systems. This enforces a dynamic, zero-touch change of authorization (CoA) upon detection of malicious activity - allowing the system to automatically block or isolate misbehaving client devices.

Direct accessibility to non-cellular endpoints

Using intelligent 5G LAN routing, Celona provides full visibility of, and direct accessibility to, non-native cellular devices. These potentially vulnerable endpoints often connect to mobile gateways that place them on discrete VLANs or subnets not visible or accessible to IT staff. 5G LAN routing ensures IT staff can monitor and adequately secure these devices.

Device fingerprinting for enhanced compliance

Celona's 5G LAN system supports device fingerprinting that recognizes the type of device based on various device signatures available to the network. This information is available via APIs for enterprise security systems to consume and use device context to enhance security-policy compliance checks.

Consistent policy enforcement with static IP address pools

To further control and secure connected devices, Celona offers the ability to assign specific devices to a static IP address pool while still being reachable and visible from the rest of the enterprise network. This allows consistent accessibility to, and policy enforcement for, critical devices.

Secure cloud-based management

All management data is securely stored and accessible within the cloud using encrypted transport layer security (TLS) tunnels from the Celona Edge to the Celona Orchestrator. Celona Orchestrator supports the SOC type 1, 2 and 3 audit process attestation standards. Support for SAML v2 based single-sign-on enables enterprises to use their existing identity providers (IdP) for role-based access control to users within the organizations - while adhering to access control/password/MFA policies as defined by their Security and Compliance teams.

TANGIBLE BENEFITS

- Full end-end control over data and data path management
- Greater data integrity and confidentiality with strong L1-L7 end-end encryption
- Direct mapping and routing of policies to existing enterprise firewalls and security services
- Enhanced flexibility and security to the authentication process with 5G-AKA and EAP-AKA
- Elimination of inconclusive endpoint profiling through advanced SIM security
- Strong user privacy with EMEI to ICCID locking, and SUCI support prevents unauthorized access
- Mitigation of man-in-the-middle attacks and spoofed or rogue devices
- Direct accessibility to vulnerable non-cellular end devices through intelligent 5G routing
- Dynamic client blocking and isolation though open/RESTful API integrations with third party firewalls and NAC systems
- Consistent accessibility to, and policy enforcement for, critical devices with static IP pools
- Secure transport layer security (TLS) tunnels to cloud-based management.

Use Case studies

celona.io/case-studies

TCO and ROI Calculator

celona.io/tco-calculator

Comparison with Wi-Fi

celona.io/CS-Distr-MSB

Custom demo

celona.io/custom-demo

celona

celona.io

hello@celona.io

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