Celona Security FAQ

Celona platform enables a highly secure, cloud-native hardware & software stack required to deploy and operate private LTE & 5G networks.

Contents

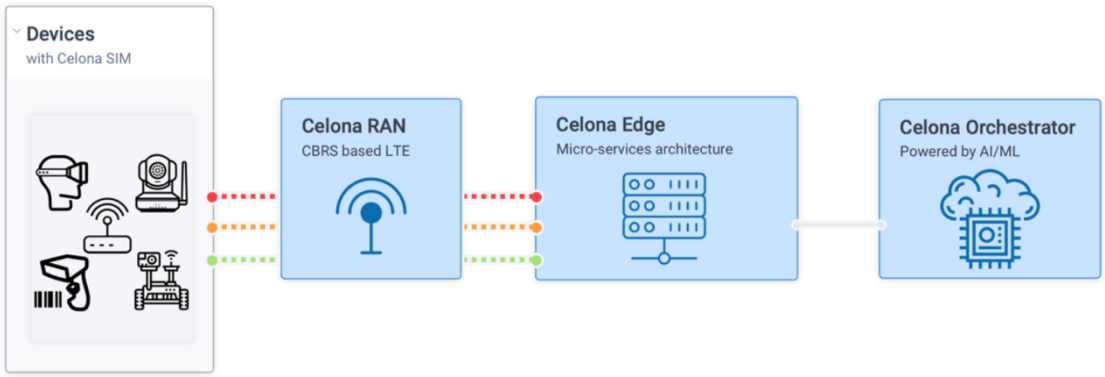
Introduction

Celona delivers a highly secure, cloud-native hardware & software stack required to deploy and operate private LTE & 5G networks. Celona solution delivers a multi-layered security architecture focused on end-user, back-end and application security employing secure access controls, logical isolation and adhering to state-of-the-art physical and cyber security standards.

Every piece of data collected and sent to the cloud management is documented and shared with customers. Data is securely sent to the cloud and is encrypted end to end over TLS. Penetration testing is performed regularly by a third-party and the company has implemented strict and documented controls around who can access data through mechanisms such as digital certificates, password policies, two-factor authentication and audit trails. For application security, Celona performs a range of vigorous tests protecting against incidents such as SQL injection, cross-site scripting and more.

Celona's solution architecture provides all components required to bring a private mobile network to life:

- Celona Radio Access Network (RAN) made up of indoor and outdoor CBRS LTE access points (APs) as a self-organizing enterprise wireless network.
- Celona Edge delivering edge compute services on-site including the Evolved Packet Core (EPC) functions as defined in the 4G LTE standard.
- Celona SIM cards on the connected devices for device level authorization and to enable centralized encryption with Celona Edge
- Celona Orchestrator enabling cloud orchestration for network operations and subscriber management, and integration with the SAS infrastructure



General FAQ

Where is Celona Orchestrator hosted?

Celona Orchestrator is hosted on AWS within their Virtual Private Cloud (VPC) environment.

What security measures exist for Celona Orchestrator?

Celona Orchestrator's backend infrastructure is hosted in Amazon Web Services (AWS) availability zones and regions that meet the following standards:

- SOC 1, Attestation Standard Section 801 (formerly SSAE 16)
- SOC 2 / SOC 3, Attestation Standard Section 101
- Data centers that feature state of the art physical & cyber security with reliable designs and strict access policies

Amazon Virtual Private Cloud (VPC)
Celona Orchestrator further leverages Amazon VPC with a provisioning construct that creates a logically isolated section within AWS. VPC provides complete control over virtual networking environment including IP address range selection and control, subnets, configuration of routing tables, and network gateways.

Encryption
Data in transit is encrypted over Transport Layer Security (TLS) over port 443.

Secure Access Controls
Access to backend servers are strictly controlled by role-based access via multi factor authentication (MFA) including user certificate, MFA token, and passphrase. Access logs are maintained and monitored for unauthorized system access, with an audit trail.

What are some of the automated security tools that you use?

We use automated security tools such as Qualys on a periodic basis and address issues that are found by the tools.

What are your incident response policies and procedures?

We run periodic scanning against the cloud service. Any vulnerability found is triaged as a low, medium, or high priority issue. High priority issues are immediately rolled into our development sprint and pushed out as soon as verification is completed.

Data Processing, Transport & Storage

What data is sent from the on-premise Celona Edge to the Orchestrator?

Celona collects only metadata and performance metrics from client devices, APs and Celona Edge clusters. Celona Edge is the sole collection point of all metadata.

Metadata is aggregated every minute and sent to the Orchestrator database. The metadata is used to provide customers insight into the operation and performance of the Celona private LTE/5G networks and the devices connecting to this network. Here is the list of data types that are processed:

Data Type	Description
Protocol Stats	Set of stats describing performance details of various networking protocols
Flow Stats	Statistics per flow: Src/dest IP, src/dest port, number of packets/bytes, session duration
Device Stats	Client device info: IMSI, ICCID, IP address, device type
Network Metrics (RAN)	Access point info – uptime, reboots, model, IP address RF stats for clients and APs: SNR, packet loss, noise floor, channel, channel width & utilization CPU & memory utilization of APs Clients associated to APs
Edge Health metrics	CPU & memory utilization of Edge Health stats of various Edge services

Protocols	Metrics
TCP / IP	TCP state machine analysis: Byte / packet counts, Round Trip time (RTT), retransmission error rate, timeouts and window size analysis, SYN/ACK relationships, sequence number timings, src/dest IP, src/dest port, DSCP tags
UDP	Jitter, session duration, src/dest IP, src/dest port

Do you process or store Personally Identifiable Information (PII)?

We process and store IP address, IMSI & ICCID associated with client devices. We do not store packets or payload information. Strong encryption of in-transit data from on premise Celona Edge clusters to the cloud-hosted Orchestrator is achieved using TLS communications.

How do you protect data in transit?

We use standard cryptographic protocols to encrypt all data in transit. The following protocols are used to transmit encrypted data:

- AP-to-Edge: IPSec
- Edge-to-Cloud Orchestrator: TLS port 443

How are system and network environments isolated to ensure separation of production and non-production services?

Our developers have access to non-production environments, while smaller subset of users (DevOps) have access to production environments. Production and non-production environments are not shared.

Confidentiality & Integrity

How is access to customer's account & data controlled?

We employ the principle of least privilege to limit access to the minimal level that will allow normal functioning: for instance, as part of technical support delivery.

How are production resources accessed?

Two Factor Authentication (2FA) is enabled for Celona engineers accessing the production environment. Access to production environment is via a VPN tunnel using secure certificates and MFA token. It is restricted to only certain users who have been granted access to the VPN tunnel. Finally, users access servers via SSH key and not manually entered password.

Do you audit/log access to production environment?

All access to backend production servers is logged by the VPN server and the server authentication logs. User access to the Orchestrator is also logged.

Who can access the on-premise Celona Edge & APs? Can customers restrict access to the on-premise components?

We employ the principle of least privilege to limit access to the minimal level that will allow normal functioning. Select Celona support engineers have this access for delivery of support, maintenance & software updates. Customers are notified in advance of making any software updates to the on-premise components.

Does Celona Orchestrator support role-based access?

Celona Orchestrator supports role-based access with the following user roles:

- Admin: ability to add users, make configuration changes, and set up user roles
- Observer: read-only access to specific parts of the Celona UI
- Installer: read-only access to specific parts of the Celona UI & CPI installation workflow

Conclusion

As highlighted above, Celona's solution architecture for private LTE & 5G networks take advantage of a secure cloud-native platform implementation. Combined with the always-on and device-level authorization of client devices with Celona SIM cards, centralized encryption of wireless client traffic with Celona Edge and role-based network access policies enabled by Celona's unique MicroSlicing™ technology, Celona private mobile networks are designed to enable highest levels of enterprise wireless security.