WHITE PAPER

Celona 5G LAN Security and Privacy

Celona's 5G LAN keeps you in control of your data for private cellular.

MAY 2024

celona

CONTENTS

Introduction

Celona brings the resiliency and security of cellular technology to the enterprise network with its 5G LAN solution. A 5G LAN isn't a traditional cellular wireless network as it harnesses the power of cellular technology for use within the enterprise network. It is used to connect and secure mission-critical network applications such as those in healthcare, manufacturing, supply chain, and is a great alternative to Wi-Fi for enhanced security.

Cyber security remains a predominant concern among both technical and non-technical leaders, and that concern continues to intensify as organizations are hammered with the challenges of ransomware, insecure IoT devices, and insufficient resources to secure it all. Especially when such critical infrastructure is connected via the enterprise wireless network.

Celona's unique 5G LAN is industry's only turnkey solution that incorporates best-of-breed security from core to edge and one that integrates fully to the existing LAN. It is designed to guarantee privacy of data via device level network access controls and network segmentation. Ultimately, a secure 5G LAN enables organizations to bring mobile, IoT and new digital transformation initiatives into the enterprise network – without losing the ability for centralized visibility and control.

Not only does Celona's 5G LAN address the security and resiliency gaps of traditional mobile and IoT networks, but it also empowers organizations' zero trust strategies. This whitepaper demonstrates how a Celona 5G LAN services the objectives of confidentiality, integrity, and availability of the network and the enterprise data.

Supporting Your Zero Trust Strategy with a 5G LAN

Celona's 5G LAN supports zero trust strategies with strong device identification, authentication, granular end-to-end segmentation, and robust encryption -- plus integrations via APIs and secure authentication standards such as Security Assertion Markup Language (SAML) for privileged access management.

To date, IoT has been excluded from many zero trust scopes due to the complexity of managing non-user-based devices and the diversity of the connectivity models. Celona's 5G LAN gives enterprises centralized visibility and control of corporate-managed cellular devices, non-traditional endpoints, and IoT devices, alongside traditional endpoints.

For private cellular wireless network implementation, 5G LAN solution architecture that's tightly integrated with existing enterprise policies, user data plane and network infrastructure also enable a unified risk management approach, reduce gaps in visibility, and support even the most stringent regulatory requirements.

Strong device identification and authentication

One key challenge for securing the volume of disparate endpoints on any enterprise network is proper identification and classification of the device -- two tasks which must be completed before security controls can be implemented.

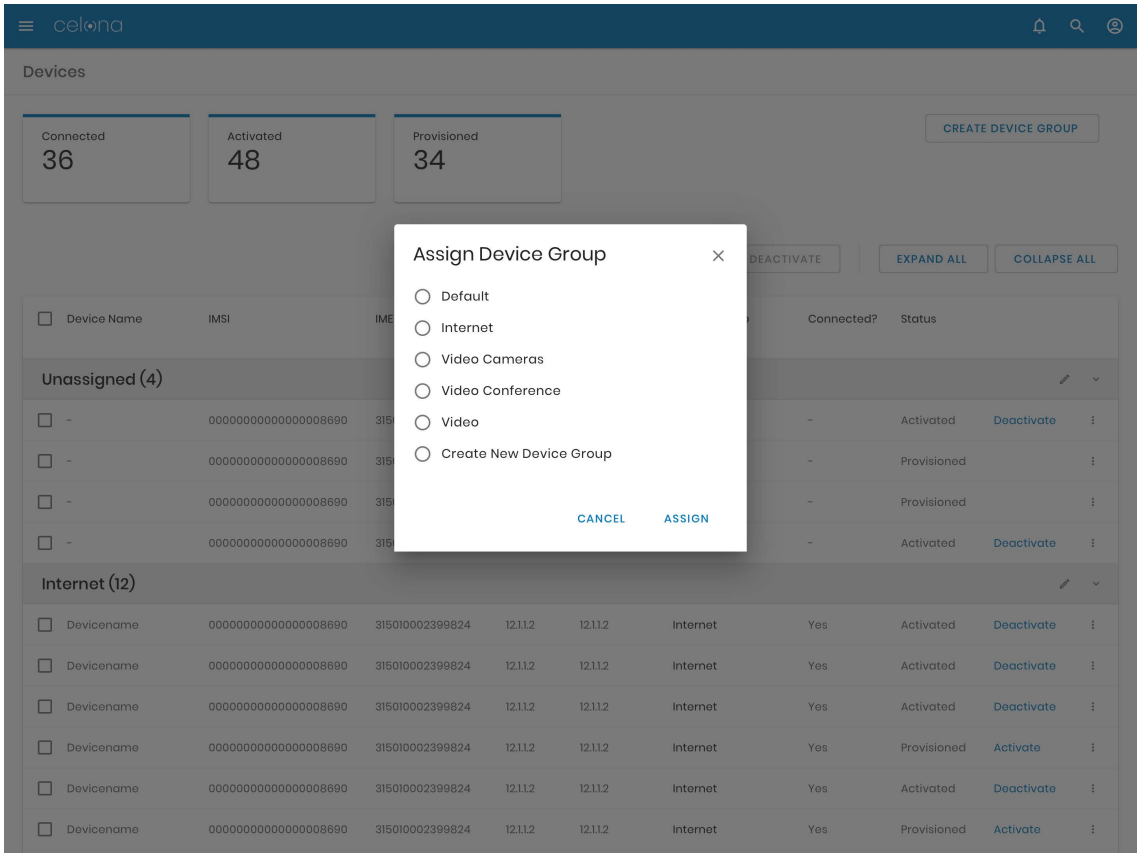
Celona's 5G LAN solution combines the deterministic and immutable identities inherent in cellular technologies with enterprise LAN security controls such as device specific policies, application service level objectives and VLAN segments.

With a 5G LAN implementation, gone are the days of inconclusive endpoint profiling and guessing what a device is, who owns it, or what applications it's running. Endpoint devices are uniquely identified with immutable identities tied to the physical SIM and/or embedded SIM (eSIM). In a Celona 5G LAN, this identity is used to derive a LAN-friendly unique identity for each connected device, allowing identification of the device across both the private cellular wireless and the enterprise LAN.

Device identification is made possible by the nature of 5G LAN deployment. The enterprise IT network and security teams can easily add and authorize devices via SIM provisioning. This allows them to assign devices to specific groups of their choice based on use cases or applications.

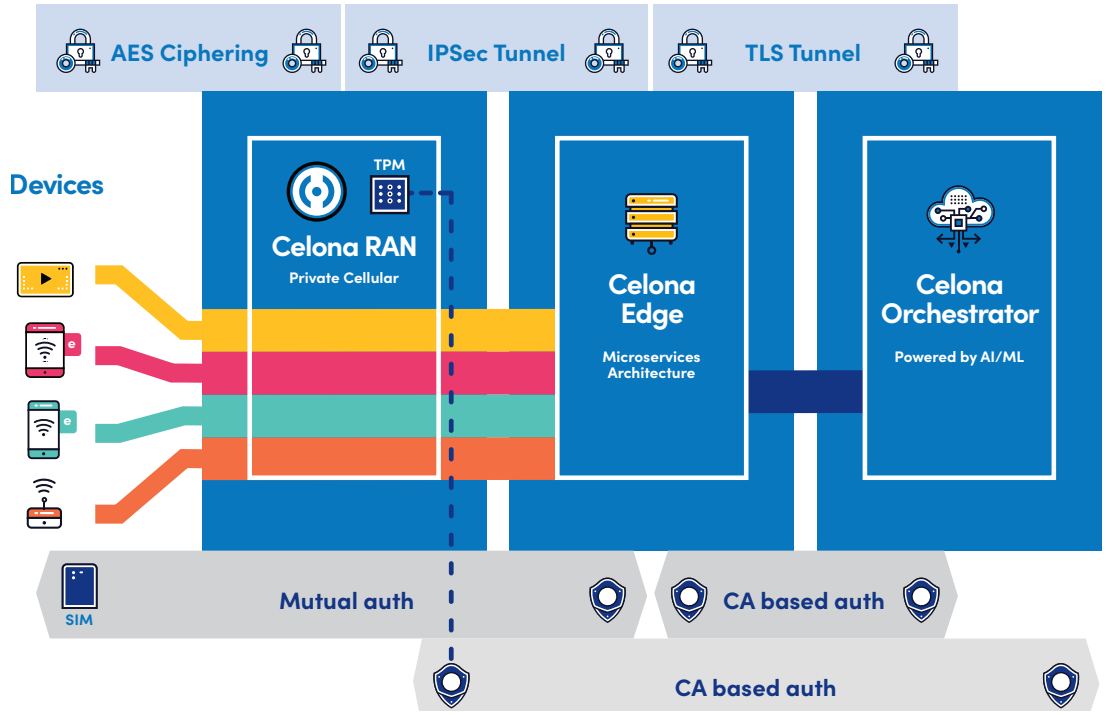
Support for software-based eSIM makes provisioning and maintenance a simple QR code scan / URL redirect with a profile download, allowing the IT team to update or issue new credentials to the endpoint securely over-the-air, without having to physically touch the device to swap physical SIM cards.

The process is further simplified by Celona's intuitive platform, requiring no specialized cellular expertise to onboard new devices and provision device groups per policy. Only known and authorized devices are allowed to connect to a Celona 5G LAN, ensuring accurate inventory and asset management, and allowing for centralized control of which device can access what parts of the private cellular network, under what conditions and when.



Along with their immutable identities, Celona-connected devices join the network using strong mutual authentication -- a process that authenticates both the endpoint to the network and the network to the endpoint, mitigating man-in-the-middle attacks and spoofed or rogue devices. Note that the Celona infrastructure components arrive already hardened and use certificate-based authentication, including the TPM-enabled cellular APs.

The device authentication protocols in Celona's 5G LAN include 5G-AKA and EAP-AKA that bring enhanced flexibility and security to the authentication process by adding signaling and data integrity and confidentiality.



Robust encryption

Data confidentiality and integrity are paramount, especially over wireless communication mediums. While prior generations of cellular technology relied on cryptographically weak algorithms and key lengths, 5G technology offers secure 128-bit AES encryption over-the-air, on par with the latest Wi-Fi WPA3 security standards.

Plus, Celona's 5G LAN will further extend protection with 256-bit AES, offering a cryptographic strength equal to the 192-bit Wi-Fi WPA3 advanced algorithms approved for use in the world's most secure environments.

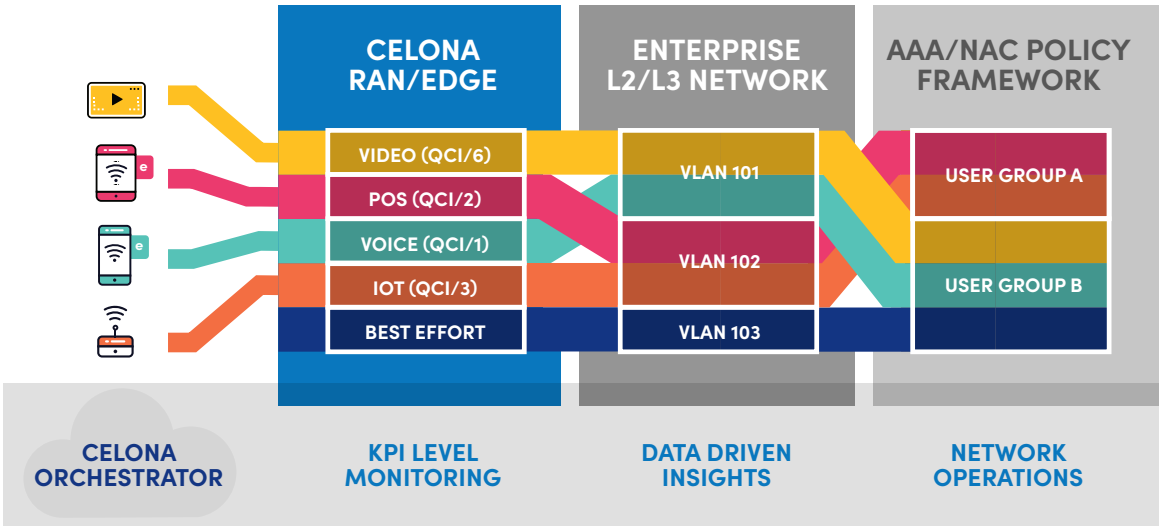
Celona's 5G technology also offers enhancements for key derivation and rotation -- the master key is never shared or exposed, and the device's identity is concealed for enhanced privacy.

Encryption isn't just over-the-air; data is protected at each segment of the Celona infrastructure from the endpoint to cellular APs, to Celona Edge and Celona Orchestrator.

End-to-end segmentation and QoS

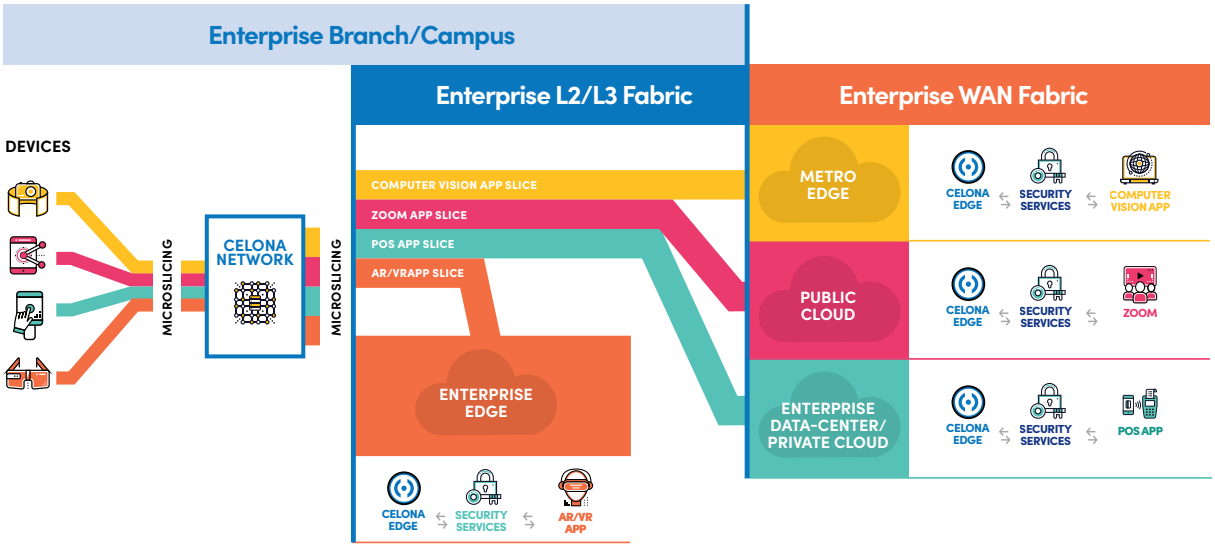
Another key element of a zero-trust architecture is segmentation, and a Celona 5G LAN expands on the standard 5G network slicing concept to delivery granular control and security for devices or applications.

Through its patented MicroSlicing™ technology, Celona allows enterprises to not only segment but separately encrypt groups of devices or applications as granularly as on a per-IP flow basis, offering an unequaled granularity of segmentation.



In addition, the Celona MicroSlicing Policy extends from the 5G LAN and can be mapped directly to enterprise network segments, such as VLANs, VxLANs, firewall zones, or other enforcement points. In order to deliver on service level objectives, set for minimum throughput, maximum latency and average packet error rate, MicroSlicing policies enforce quality of service (QoS) as well as segmentation for critical enterprise applications.

Celona MicroSlicing can be used to extend network segmentation and QoS to the enterprise LAN, to the enterprise WAN, or even to the cloud, via deployment of mobile network services within Celona Edge across these compute environments.



Integration support

Zero trusts strategies are best served by products and technologies that are extensible and scalable – two features powered by integrations with best-in-class technology solutions. The ecosystem of zero trust requires orchestration of systems, services and applications. Celona supports this capability with programmable APIs and secure privileged access authentication based on SAML.

Maintaining Your Data Privacy with a 5G LAN

Data privacy on public 5G networks continues to remain a top and growing concern for organizations. In a private 5G LAN, Celona puts the organization in full control of its data and traffic forward, ensuring data privacy and supporting compliance initiatives.

With Celona's architecture, whether you choose to connect secure data tunnels on-premises, at a remote datacenter, or in the cloud – your data is never visible to, inspected by, nor available for monetization by any third party, including Celona.

Concerns over public 5G privacy

Confidentiality and privacy routinely rate in the top security concerns when it comes to the use of public 5G for enterprise connectivity. Fears over an increased attack surface, lack of visibility, and limited in-house knowledge are recurrent themes cited by enterprises.

In public 5G networks, the collective concern is that with faster and more capable networks, Mobile Network Operators (MNOs) will simply have more access to more data, including corporate data through 5G-connected devices.

In the absence of strict privacy laws and governance, users of public 5G networks remain at the mercy of the MNO as to how their private data is used. Often, data and metadata are monetized by way of data correlation and trend analysis for marketing purposes.

Data privacy within a 5G LAN

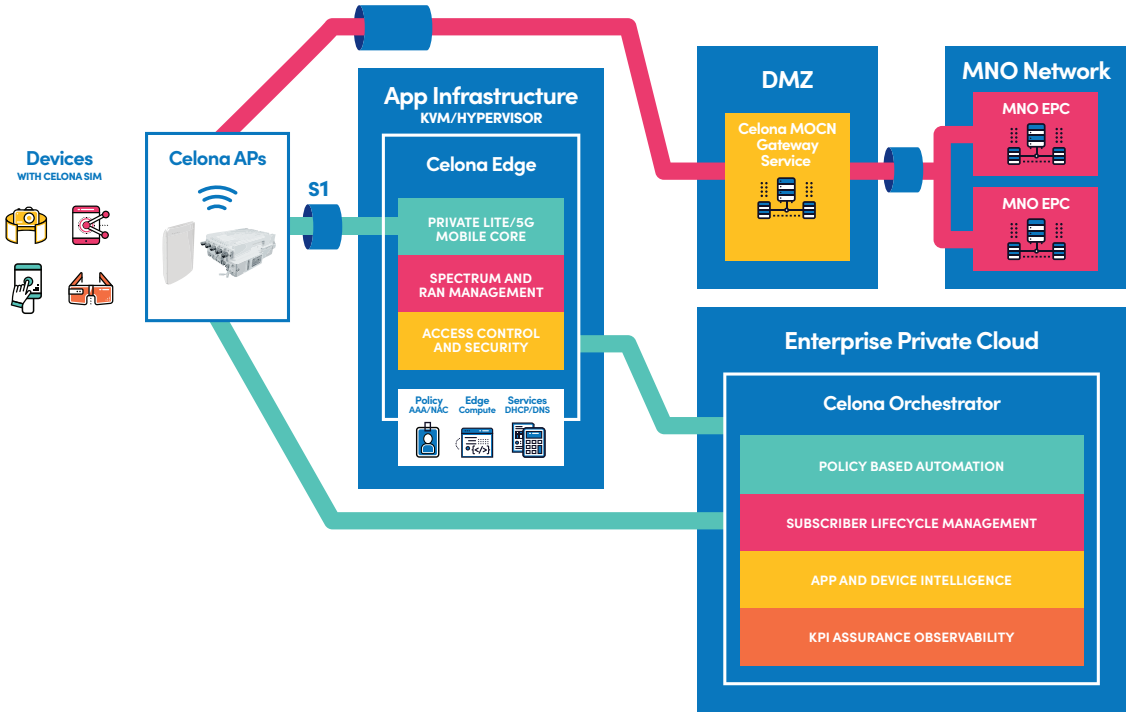
Knowing that mobile network operators may have access to corporate data across both public and MNO-managed private networks, enterprises are seeking options that are more secure and offer better data privacy controls.

Celona's private 5G LAN solves the privacy and confidentiality concerns intrinsic in public 5G connectivity via tight integration of its cellular access points and mobile network services within the enterprise LAN footprint. It can be configured by enterprise IT network and security teams with any custom policy and traffic forwarding rules required at any time. The configuration of the system can be changed only by them or by their authorization via their services partner. This provides them full control over their own data, management and accessibility of such data via the connected IoT and mobile infrastructure and the data path end-to-end.

An organization's data is never visible to Celona as it is a fully private network connectivity within the networked enterprise environment. All endpoint payloads are secured and contained within the enterprise 5G LAN – encrypted from the device to the core of the network. Only metadata and system performance metrics are sent securely to the cloud-hosted Celona Orchestrator – face of the Celona platform – where metrics on MicroSlicing policies offer application delivery teams and wireless network engineers the visibility into critical application performance. Such customer metadata is never used for monetization and not provided to third parties.

Evolution to Neutral Host

While a private 5G LAN may be just what's needed today, tomorrow may bring new use cases and opportunities. Enterprises that deploy a Celona 5G LAN today will have a seamless path to support "guest users" on the same network – by securely onboarding subscribers of public MNO networks. This is also known industry as "Neutral Host Network (NHN)" capability.



Within a Neutral Host, a Celona 5G LAN acts as a pass-through to the public cellular MNOs – enabling seamless and secure connectivity to public 5G service via the same cellular access points deployed within the enterprise facility. Users experience seamless roaming, and all cellular network authentication and data is secured and managed by each MNO.

Neutral Host approach is quickly becoming the preferred choice for enterprises seeking better public cellular coverage indoors given the numerous benefits over traditional approaches as there will be no need to:

1. share bandwidth with public cellular networks,
2. deploy expensive DAS infrastructure within buildings, or
3. expensive custom spectrum designs for each enterprise site.

Neutral Host capability is enabled within a Celona 5G LAN by extending the Mobile Operator Core Network (MOCN) services to the enterprise DMZ – from where the connections to multiple MNOs can be established. On a Celona 5G LAN, privacy for enterprise owned / operated infrastructure are protected by enforcing secure transport of public subscriber traffic from the Celona cellular access points to the MOCN gateway.

Thanks to its MicroSlicing technology, Celona can enable unique network segmentation policies for subscribers of different MNOs within the same 5G LAN – while also supporting private use cases with distinct MicroSlicing policies. Celona 5G LAN continues servicing internal enterprise endpoints while simultaneously offering logically segmented access for non-enterprise users to access their respective provider networks.

Integrating Your 5G LAN with Enterprise Policies

Within a Celona 5G LAN, private cellular wireless traffic forwarding principles can be translated to existing enterprise network segments, access control policies and application QoS requirements – thanks to its unique 5G LAN routing capabilities. This enables enterprise technology teams to utilize existing corporate policies and local area network (LAN) configuration to support new devices and users taking advantage of the private cellular connectivity on the 5G LAN.

Addressing existing security gaps

Celona's 5G LAN is designed to supplement current wired and wireless connectivity options, and in fact operates in airspace that doesn't interfere with Wi-Fi infrastructures, making it an ideal choice as an RF overlay in any location. By taking advantage of private cellular spectrum options (such as CBRS in the United States), it enables an interference free "clean" spectrum for critical applications that communicate with enterprise resources via the 5G LAN.

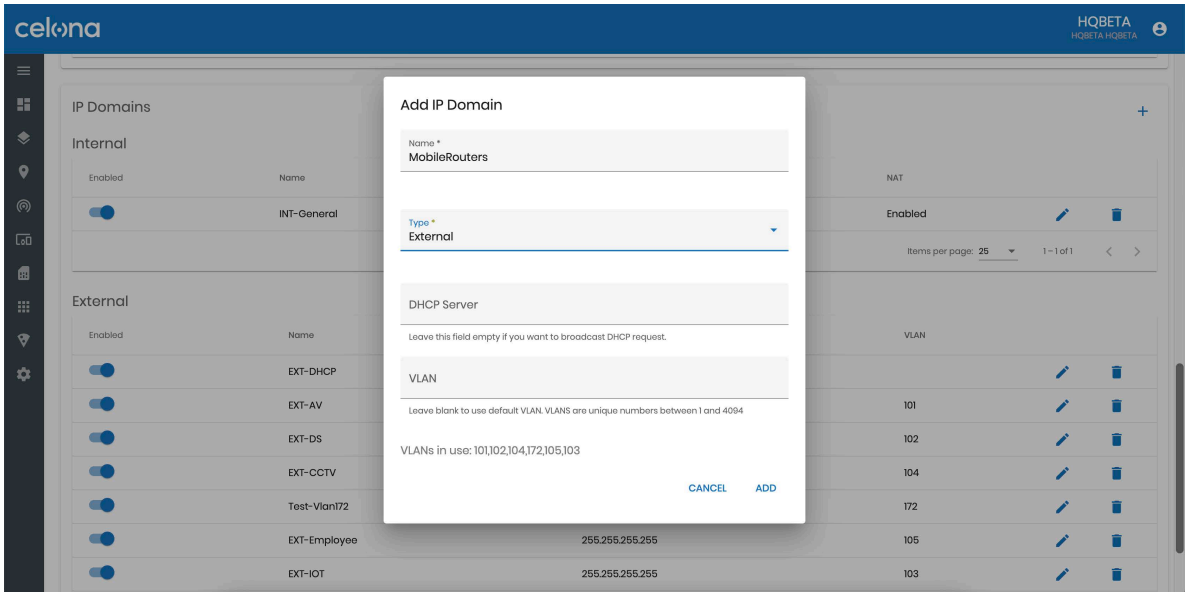
Although the 5G LAN isn't designed to replace current technologies, 5G is often better suited for subsets of needs including servicing mission-critical and latency-sensitive applications that have greater availability and security requirements than basic Internet-based traffic. Delivering a wired-like performance on wireless, a Celona 5G LAN can be configured on-demand for multiple MicroSlicing policies to ensure deterministic throughput, latency and packet error rate for applications across custom defined device groups.

Secured 5G LANs also prohibit risky uncoordinated peer communications and overlay protocols designed to subvert enterprise networks (e.g., mDNS and zeroconf) traditionally found in enterprise Wi-Fi networks.

Celona's 5G LAN offers always on data encryption for any connected device, and device level authorization for network access via the use of SIM cards. In a 5G LAN, there is no concept of SSID broadcast over the air, no option for open or pre-shared key access, and no ability for end users to add additional network names to the end devices for connectivity due to tight enterprise controls. In the next section, we dive deeper on the topic.

Integration with the enterprise LAN

Under the hood, Celona is unique in its implementation of the 5G LAN, offering integration with external DHCP infrastructure that's already in place within the enterprise network. Custom device groups can be provisioned to interface with existing VLAN/VxLAN configurations outside the 5G LAN, and traffic forwarding between any IP subnet that already exist within the enterprise LAN. Existing network security solutions and infrastructure can gain access to device and application context that reside within the 5G LAN, enabling end-to-end visibility across Wi-Fi, wired and private cellular connectivity within the enterprise access network.



Turnkey architecture, designed for enterprises

Managing a secure Celona 5G LAN doesn't require special skills or a 5G expert. In fact, Celona's platform was designed to be used by enterprise IT teams and network admins. It comes as a turnkey package from cellular access points and SIM provisioning to mobile network services and network operations. This prevents the need to acquire and put together each of these essential elements from different technology vendors – reducing footprint possible security risks.

By utilizing a single software release for all components of its 5G LAN solution, Celona can enable rapid deployment of new capabilities or critical improvements. Instead, traditional solutions and managed services options that encompass multiple product lines come with the risk of having to work with multiple technology releases, product updates and support workflows.

Celona 5G LAN components are delivered fully hardened and maintained through the Celona platform throughout the lifecycle of the system. This model alleviates the need for the enterprise IT team to take on any additional tasks of maintaining security and hardening of multiple components that traditionally make up a private cellular network.

Enterprises find Celona Orchestrator intuitive to use, with familiar menu navigation, network, and endpoint configuration options. Provisioning can be as simple as a few clicks, or as granular as locking device assets to specific sites. Ease of operation reduces the risk of misconfiguration across multiple sites for network segmentation rules, device access policies and new infrastructure rollouts – and translates to time saved for implementation of higher value tactics and strategies for enterprise technology teams.

Conclusion

With a Celona 5G LAN, enterprises have the opportunity to enable deterministic wireless performance for their critical applications – while directly translating their existing corporate network access policies to strong device identity, authentication, and encryption.

Within the private cellular network, end to end data privacy is combined with the power of Celona's MicroSlicing technology deliver granular network segmentation for multiple use cases.

Celona 5G LAN improves upon your organization's zero trust strategy with centralized visibility and control of corporate cellular, non-traditional endpoints, and IoT devices alongside traditional endpoints. The entire platform is easily managed by the enterprise IT team on-demand with full ownership and data control or can be fully consumed as a managed service.

SEE THE CELONA TECHNOLOGY IN ACTION

Request a proof of concept and custom product demonstrations by visiting us at celona.io/journey.

hello@celona.io | celona.io

celona