Celona Aerloc

Next-Generation Secure Access Network Architecture

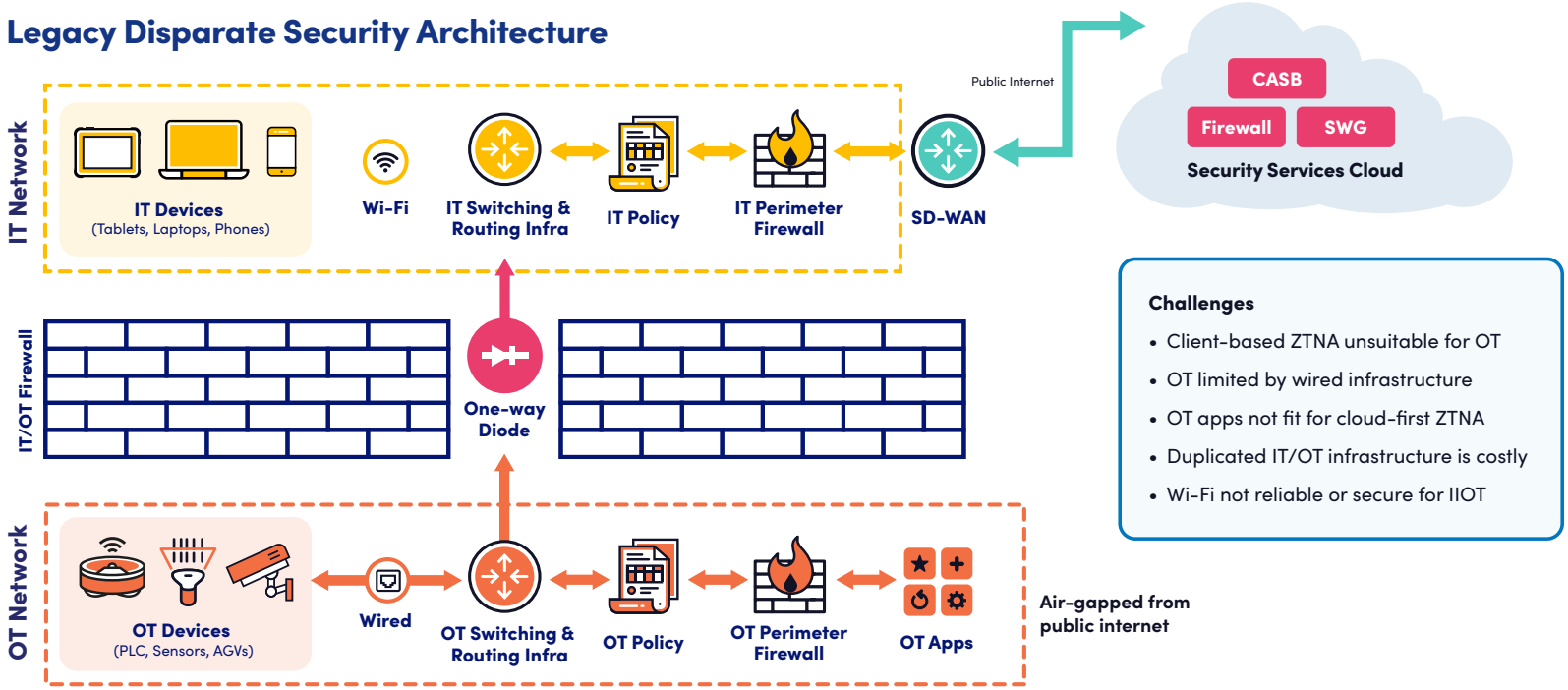
celona

PRODUCT BRIEF

Problem Statement

In today's rapidly evolving enterprise networking landscape, the integration of traditional IT environments with operational technology (OT) presents significant challenges. The existing siloed approach—whether it be the "great" divide between IT and OT or the disconnect between perimeter and cloud-based security services—has led to complex, fragmented, and inefficient security architectures. These disparate systems restrict operational flexibility and hamper productivity, particularly in industrial environments. The situation is further exacerbated by the complexity of legacy systems and the contrasting demands of IT (requiring flexibility) versus OT (requiring strict security standards).

Legacy Disparate Security Architecture



Challenges

- Client-based ZTNA unsuitable for OT
- OT limited by wired infrastructure
- OT apps not fit for cloud-first ZTNA
- Duplicated IT/OT infrastructure is costly
- Wi-Fi not reliable or secure for IIOT

The introduction of Private 5G into enterprise environments has added layers of complexity, becoming a key factor in delaying the widespread adoption of this transformative technology. As we design and develop the next generation of enterprise networks, we are presented with a crucial opportunity to redefine network and security architecture. By converging IT, OT, and Private 5G into a seamless, unified solution, we can overcome existing challenges and unlock the full potential of Private 5G.

© Copyright 2024 Celona Inc. All rights reserved.

Introducing Celona Aerloc

The Celona 5G LAN Aerloc architecture has been meticulously crafted with these considerations in mind.

Designed to integrate effortlessly with existing network and security infrastructures, it paves the way for widespread deployment of Private 5G across both industrial and traditional enterprise environments.

Key Considerations for Designing Next-gen Secure Access Network

1. Convergence of Access & Security for IT and OT

The convergence of access and security for both IT and OT environments is crucial to avoid the siloed solutions that have traditionally plagued enterprise networks. This unified approach not only simplifies operations but also eliminates the unnecessary overhead that comes with maintaining separate systems. A holistic access and security framework provides organizations with an integrated solution that supports diverse device types across both IT and OT, reducing complexity and operational costs.

2. Clientless Zero Trust

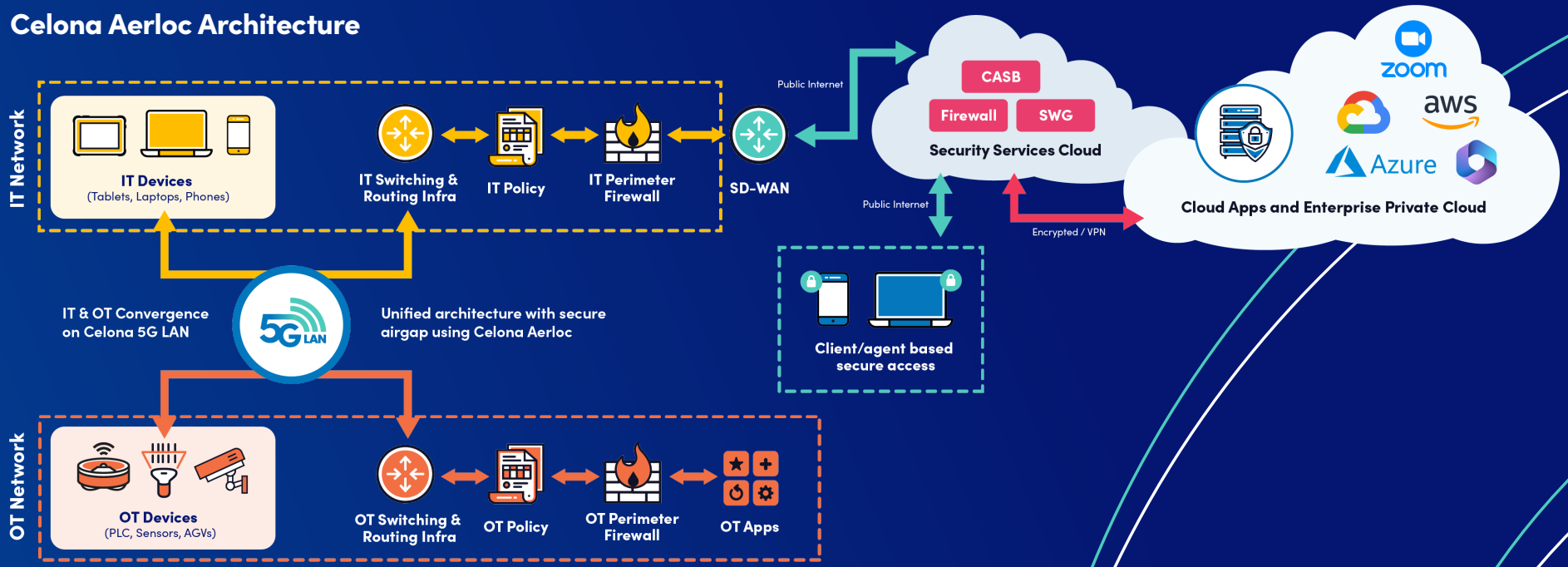
Managing VPN clients has long been a hassle for IT teams, especially when maintaining large, diverse networks. Furthermore, many OT and IoT devices are closed-box systems that do not support additional software clients or agents. By employing Zero Trust principles that do not require client software, enterprises can meet the unique security demands of these systems. This approach is particularly beneficial for OT environments, where security cannot rely on traditional client-based models due to the constraints of the devices themselves.

3. Decentralized and Scalable approach to network access & posture assessment

Modern enterprises operate in geographically dispersed environments, with applications and operations taking place both at the network edge and in cloud-hosted environments. A decentralized security model aligns with this distributed nature, enabling secure and scalable access to resources across all enterprise touchpoints. This strategy ensures that both hyperlocal edge applications and remote cloud resources are protected, giving enterprises the flexibility to adapt to the demands of modern operations without compromising security.

© Copyright 2024 Celona Inc. All rights reserved.

Celona Aerloc Architecture



Benefits

- 5G LAN for secure and reliable alternative to wired and Wi-Fi
- Unified 5G LAN Infrastructure with secure IT/OT airgap reduces cost
- SIM-based authentication for clientless zero trust and full network visibility
- Native integrations with security services including third-party firewalls and NAC
- Dynamic security policy enforcement

© Copyright 2024 Celona Inc. All rights reserved.

Key Elements of Celona Aerloc Architecture

SIM-based Secure Authentication with Unified Zero Trust Enforcement

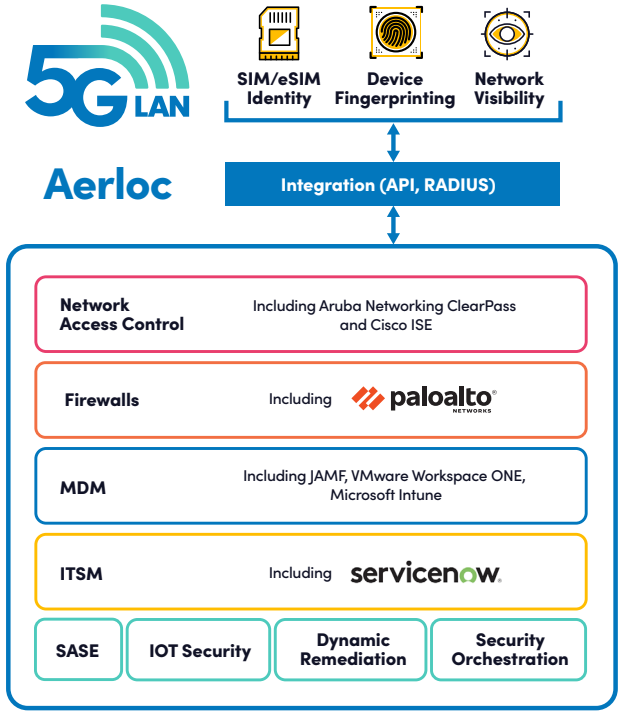
Celona's architecture employs a SIM-based secure authentication for both IT and OT devices, eliminating the need for device-side software or agents. An Open API approach provides native integration with best-in-class security services, such as firewalls, network access control (NAC) systems, SD-WAN solutions, agnostic to their deployment – whether in the cloud, on-premises, or a hybrid setup.

Dynamic & Distributed Policy Enforcement

Further extending the Open API approach to integrate with posture assessment tools, IoT security solutions, and security orchestration automation platforms, Aerloc provides a collaborative security architecture enabling localized and responsive policy enforcement at a granular level– down to the individual device or user – and at the very edge of the network, significantly reducing the attack surface.

Air-gap between IT & OT traffic

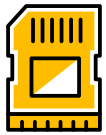
Through Celona MicroSlicing™ technology, IT and OT traffic can be securely segmented, physically and logically, within the shared 5G LAN, over the air, using 3GPP standards and extending to Enterprise LAN infrastructure. This unique intent-based segmentation of IT and OT traffic ensures the separation of critical operational data from general enterprise traffic, maintaining security and performance integrity across both environments.



Celona Aerloc architecture enables applying existing IT/OT security policies to Private 5G devices using provides open API/Radius integrations.

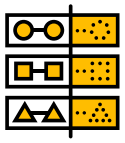
© Copyright 2024 Celona Inc. All rights reserved.

Additional Capabilities of Celona 5G LAN Aerloc



SIM-based Mutual Authentication

Devices connecting to the network via Celona use SIM-based mutual authentication, validating both the endpoint and the network to each other. This process, which includes protocols like 5G-AKA and EAP-AKA, strengthens security against man-in-the-middle attacks and rogue devices, providing enhanced flexibility and protection.

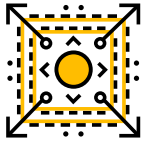


Granular End-end Traffic Segmentation

Celona 5G LAN provides granular segmentation of traffic down to a per-flow level, over both the air and the wire. Celona 's MicroSlicing™ technology maps individual IP traffic flows to pre-defined enterprise network segments, such as VLANs or firewall zones, ensuring that devices and applications are securely segmented and protected.

Enhanced User Confidentiality

To prevent unauthorized access and eavesdropping, Celona utilizes Subscription Permanent Identifier (SUPI) and Subscription Concealed Identifier (SUCI) technology. These cryptographic methods conceal subscriber identities, ensuring user anonymity and confidentiality.



Direct Accessibility to Non-cellular Endpoints

Using intelligent 5G LAN routing & Supernetting, 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/OT staff can monitor and adequately secure these devices.

Zero-touch eSIM Onboarding via MDM

Enterprises managing hundreds or thousands of devices with Mobile Device Management (MDM) systems can benefit from Celona's automated eSIM onboarding workflow. By integrating with incumbent MDM systems through custom APIs, Celona simplifies the provisioning of cellular-capable devices for Celona 5G LANs. This automation enhances flexibility, convenience, and security, allowing IT/OT staff to remotely provision devices while protecting against tampering and unauthorized access.

Strong Device Identification & Authentication

Celona Aerloc leverages deterministic and immutable identities from cellular technologies, such as Subscriber Identity Modules (SIMs or eSIMs), International Mobile Equipment Identity (IMEI), and Embedded Identity Document (EID). By locking authorized SIMs to authorized devices (IMEI/EID to ICCIDs), Celona eliminates the risk of unauthorized devices accessing the network.

© Copyright 2024 Celona Inc. All rights reserved.

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.

Device Fingerprinting for Enhanced Compliance

Celona's system supports device fingerprinting, identifying device types based on unique signatures available to the network. This information is accessible through APIs, allowing enterprise security systems to leverage device context and enhance security-policy compliance.

Robust API Integrations with Third-party Security Systems

Celona 5G LANs integrate with existing firewalls, IoT security systems, and Network Access Control (NAC) systems ClearPasslike Aruba Clearpass and Cisco ISE via APIs. This allows dynamic, zero-touch authorization changes in response to detected threats, enabling automatic blocking or quarantining of malicious devices.

Secure Cloud-based Management

All management data is securely stored and accessible in the cloud, with encrypted transport layer security (TLS) tunnels from the Celona Edge to the Celona Orchestrator. Support for SAML v2-based single sign-on (SSO) allows enterprises to use their existing identity providers (IdP) for role-based access control, ensuring adherence to security and compliance policies like multi-factor authentication (MFA).

© Copyright 2024 Celona Inc. All rights reserved.

Conclusion

Celona's Aerloc represents a paradigm shift in enterprise networking. By seamlessly integrating IT and OT environments through a unified, SIM-based secure authentication, clientless Zero Trust, and granular traffic segmentation, Celona enables enterprises to deploy scalable and secure private 5G networks. These networks are designed to support the distributed nature of modern enterprises while maintaining rigorous security and compliance standards.

This architecture not only solves today's challenges but also future-proofs organizations with a comprehensive, flexible, and scalable solution for next-generation enterprise networks.

For more information visit celona.io/aerloc

celona celona.io

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