Multi-Operator Core SASE with Prisma SASE 5G and Aeris IoT Watchtower

Extend Best-in-Class SASE Security to All Your Wireless-Connected Assets

Key Benefits

- **Unified security visibility:** Extend SASE security policies to the wireless edge through a single pane of glass.
- **Proactive threat response:** Enable extended protection via Aeris® IoT Watchtower™ and Palo Alto Networks Prisma® SASE for real-time monitoring and zero trust control across networks and the entire device lifecycle.
- **Global connectivity at scale:** Tap into the Aeris consortium of nearly 30 leading mobile network operator partners, delivering connectivity through one platform.
- **Accelerated deployment:** Reduce friction in validating security interoperability, allowing for faster time to market for global IoT initiatives.
- **Future-proof infrastructure:** Leverage built-in support for 5G-enabled applications requiring high bandwidth and mission-critical responsiveness.
- **Seamless experience:** Implement a consistent, unified security approach across IT systems and wireless-connected devices.

The Challenge

Enterprises have successfully standardized on Palo Alto Networks Prisma SASE to provide secure connectivity to internet, SaaS, and private applications for their remote users, branches, and headquarters. However, the explosive growth of wireless-connected assets—from business-critical IoT devices to a distributed remote workforce—has created a major security blind spot. A growing percentage of enterprise devices operate out of band on wireless networks, making them invisible to corporate security infrastructures.

Also, many wireless devices cannot support traditional security agents due to hardware or OS limitations. Deploying security agents is often impractical due to operational problems. That is, users with bring your own devices (BYODs) might resist or disable them, while many wireless-connected IoT devices use custom operating systems that aren't designed for standard security clients. This situation leaves these assets unprotected, creating an open attack surface that undermines your security posture and complicates compliance efforts, making a network-based approach essential.

The Solution

Palo Alto Networks and Aeris have partnered to deliver a unified security solution that seamlessly extends the industry-leading protection of Prisma SASE to the wireless edge. This cloud-native service, powered by Prisma SASE 5G and Aeris IoT Watchtower, forwards wireless data traffic from any device, anywhere in the world, to your local Prisma SASE security node.

Through this solution, organizations gain comprehensive visibility of wireless-connected devices, security processing, and policy enforcement. The powerful integration behind it offers an agentless approach to security, closing the visibility and security gap and enabling organizations to protect every enterprise asset through a single, unified security platform.

The Aeris Global IoT Network

Aeris owns and operates a unique network of networks—the first global, telco-grade IoT network built on a software-defined core with unified management and user experience. Built on the Aeris IoT Accelerator (IoTA) platform, this multicarrier ecosystem provides seamless connectivity localization, ensuring optimal performance and compliance

with regional data sovereignty regulations. This architecture unifies nearly 30 mobile network operator (MNO) partners into a single, cohesive global network, providing reliable, borderless connectivity in over 180 countries.

The Aeris distributed core network provides control and flexibility to intelligently route wireless traffic to the Prisma SASE cloud. Aeris IoT Watchtower provides the foundational network-level security (Layer 3 and Layer 4). This unique integration enables Palo Alto Networks to apply advanced Layer 7 security, making Aeris IoT Watchtower the ideal platform to extend the power of Prisma SASE to the wireless edge.

Palo Alto Networks Prisma SASE 5G

Palo Alto Networks best-in-class cybersecurity solutions address security risks with cloud-based solutions—powered by Precision AI®—providing seamless zero trust security for connected enterprises. Prisma SASE 5G applies the capabilities of Prisma SASE and extends it to 5G endpoints to provide industry-leading security for enterprises connected to service provider 5G networks. Service and connectivity providers can enhance security for their enterprise customers with SASE security for 5G networks.

Palo Alto Networks and Aeris

Palo Alto Networks and Aeris address the market need for a unified and secure connectivity solution for mobile devices across multiple connectivity providers. This solution combines reliable IoT connectivity from Aeris mobile network operator partners with Palo Alto Networks Prisma SASE 5G for zero trust security with SIM-based authentication and comprehensive security with granular policies based on 5G device identifiers like IMSI and IMEI. Adopting this solution leads to secure connectivity for all 5G devices, apps, and users, anytime, anywhere—increasing customer retention.

Use Case 1: Securing Agentless IoT and OT Devices

Challenge

Critical infrastructures, from utility meters and medical devices to manufacturing sensors, are increasingly wireless-connected but cannot support security agents. They are left vulnerable to attack, making it difficult to prove regulatory compliance.

Solution

The Aeris and Palo Alto Networks solution provides best-in-class SASE network security for wireless-connected devices. Wireless traffic from these devices is routed automatically through Prisma SASE 5G for deep packet inspection and policy enforcement, securing them without any agents and ensuring they adhere to corporate security and compliance mandates.

Use Case 2: Simplifying Security for the Remote Workforce

Challenge

Securing a remote workforce is difficult, particularly in BYOD environments. Users are often resistant to installing corporate security agents or mobile device management (MDM) software on their personal devices. Even when adopted, these agents can be easily disabled by the user, leaving the device unprotected and adding significant management complexity and cost for IT teams.

Solution

Enterprises can now issue corporate devices with a SIM from Aeris MNO partners. Prisma SASE 5G protects wireless traffic from these devices, enforcing corporate policies without requiring an MDM client. This solution simplifies device management, reduces TCO, and provides a seamless user experience while ensuring a robust security posture.

Use Case 3: Securing Third-Party Wireless Gateways and FWA

Challenge

Many businesses in sectors like retail, finance, and healthcare use third-party wireless gateways for fixed wireless access (FWA) that are not Palo Alto Networks appliances. These devices often lack the advanced Layer 7 security needed to protect sensitive corporate data, creating significant compliance and security risks.

Solution

The Aeris and Palo Alto Networks integration secures traffic from any SIM-enabled wireless gateway, regardless of the hardware vendor. By routing wireless data through Prisma SASE, enterprises can enforce advanced threat prevention and data protection policies on this traffic, ensuring that all remote locations meet corporate security standards without costly hardware replacement.

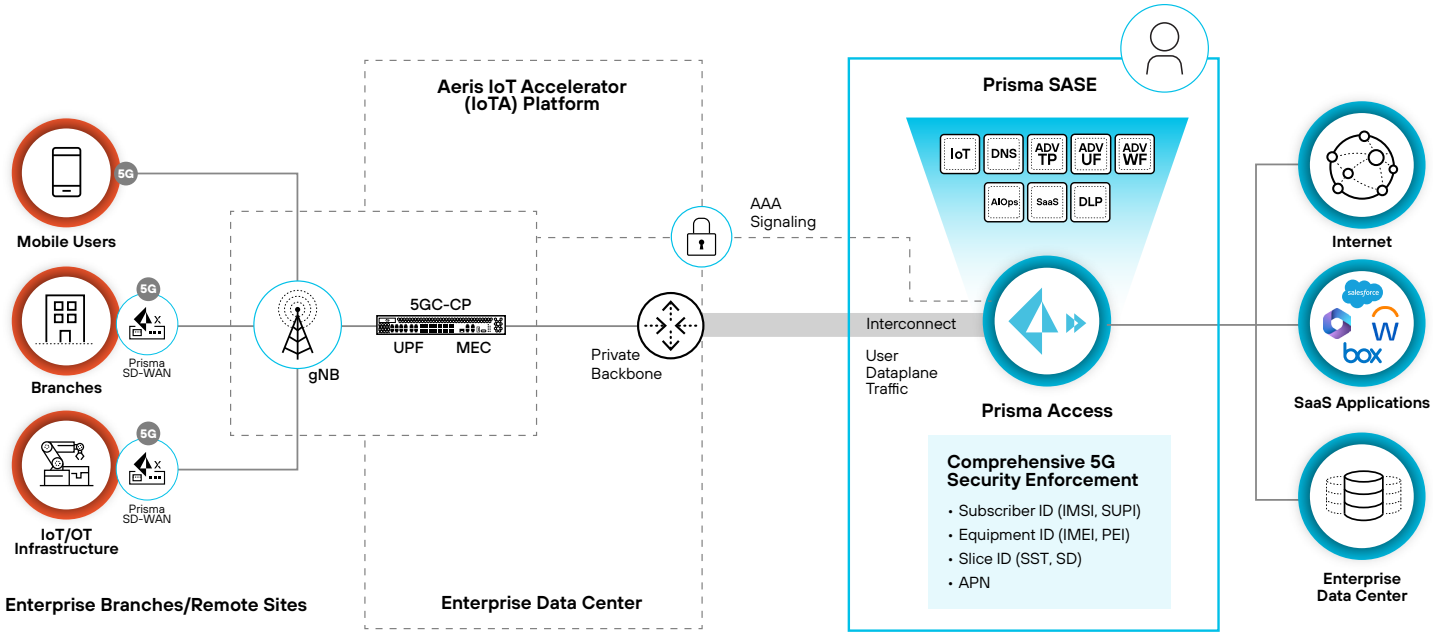


Figure 1. Prisma SASE with the Aeris IoT Accelerator platform

About Aeris

For more than three decades, Aeris has been a trusted global leader in wireless management platforms, security services, and connected vehicles programs. Our IoT technology expertise serves a global ecosystem of 7,000 enterprise customers, nearly 30 mobile network operator partners, and more than 100 million IoT devices across the world. Learn more at www.aeris.com.

About Palo Alto Networks

Palo Alto Networks (NASDAQ: PANW), the global AI cybersecurity leader, protects our digital way of life with a comprehensive portfolio of cybersecurity solutions and platforms across Network, Cloud, Security Operations, AI, and Identity. Trusted by more than 70,000 customers and powered by Unit 42® threat intelligence, our AI-driven platforms eliminate complexity, empowering enterprises to modernize with confidence and securing the speed of innovation. Explore the future of security at www.paloaltonetworks.com.

3000 Tannery Way
Santa Clara, CA 95054

Main: +1.408.753.4000
Sales: +1.866.320.4788
Support: +1.866.898.9087

www.paloaltonetworks.com

© 2026 Palo Alto Networks, Inc. A list of our trademarks in the United States and other jurisdictions can be found at https://www.paloaltonetworks.com/company/trademarks.html. All other marks mentioned herein may be trademarks of their respective companies.

parent_pb_aeris-iot-watchtower_021926