Unified Zero Trust Edge-to-Core Security Platform

SEMTECH AND PALO ALTO PARTNER BRIEF

KEY BENEFITS

- End-to-end, context-aware security with local link protection, encrypted transport, application visibility, and threat prevention.
- Automated onboarding, configuration, fleet monitoring, and over-the-air (OTA) updates across thousands of devices.
- Unified visibility, logging, and policy enforcement across edge and firewall deployments.
- Open standards, no vendor lock-in—IPsec, EST, and REST APIs integrate easily with existing security infrastructure.
- Seamless public key infrastructure (PKI) and certificate lifecycle management (CLM) automate certificate provisioning and renewal, strengthening IPsec preauth and preventing expiry outages.

THE CHALLENGE

Organizations increasingly rely on a mix of fixed, mobile, and industrial IoT assets that operate across diverse and sometimes untrusted networks, including wired, cellular, and satellite connections. These environments introduce varying levels of visibility, fluctuating identifiers, and unpredictable connectivity conditions that make it difficult to maintain con-sistent security policies and continuous oversight. Devices may move, roam, or change state, and physical access can-not always be controlled—increasing the risk of configuration drift, delayed updates, and undetected anomalies.

As deployments scale to thousands of distributed endpoints, the complexity of managing strong and unique device authentication further complicates security, visibility, and operational consistency—heightening exposure to threats and service disruption.

THE SOLUTION

A zero trust solution across fixed and mobile environments continuously verifies every device, connection, and action—regardless of location or connectivity. Each device is assigned a hardware-bound cryptographic X.509 certificate that is used to authenticate each device to ensure secure onboarding and continuous authentication.

Certificate lifecycle automation integrated with modern PKI solutions eliminates manual effort and complexity. IPsec secures data in transit, while centralized oversight simplifies configuration, monitoring, and policy enforcement at scale. Visibility into apps, protocols, and potential threats within traffic enables network resilience and operational continuity by allowing for rapid, automated response to security risks.

Semtech AirLink® Edge Routers and Network Management Solutions

Semtech AirLink routers deliver secure, resilient 5G, 5G RedCap and 4G/LTE connectivity for fixed, mobile, and industrial IoT deployments. Designed for mission-critical environments, they support cellular, satellite, LAN, and wired links with built-in protection and multi-WAN failover. Rugged, military-grade hardware enables reliable performance in harsh and remote conditions, aligned with zero trust at the edge.

AirLink Network Management Solutions—available in the cloud or on premises—provide centralized fleet control with remote provisioning, automated onboarding, configuration templates, OTA updates, monitoring, and lifecycle management. It enables fleetwide updates, device health visibility, and security-aligned controls with enterprise PKI integration.

The portfolio includes AirLink Management Service (ALMS) for cloud, AirLink Manager (AM) for fixed on-premises deployments, and AirLink Mobility Manager (AMM) for mobile fleets, on-premises, or hosted—delivering unified, secure connectivity and consistent control.

Palo Alto Networks Next-Generation Firewalls and Next-Generation Trust

Palo Alto Networks Next-Generation Firewalls (NGFWs) offer a prevention-focused architecture that is easy to deploy and operate. The machine learning-powered NGFWs inspect all apps, threats, and content, and tie that traffic to the user and device. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focusing on what matters most.

Centralized policy management and logging help ensure consistent zero trust across mobile, remote, and industrial environments. A unified management plane provides end-to-end visibility into app behavior and security posture—simplifying operations across data center, cloud, and edge.

Next-Generation Trust Security (NGTS) and Zero Touch PKI (ZTPKI) deliver full lifecycle automation, visibility, and policy control for digital certificates that establish machine identity. Integrated into the network layer, they eliminate manual renewals, prevent outages from expired certificates, and reduce operational complexity.

Palo Alto Networks and Semtech: Unified Zero Trust Edge-to-Core Security

The integrated solution combines Palo Alto Networks zero trust security with Semtech AirLink secure 4G/5G edge connectivity to protect remote, fixed, and mobile assets across fleets, field sites, and industrial IoT environments. AirLink routers deliver encrypted connectivity over cellular, satellite, and wired networks via IPsec, while providing device and network context.

Palo Alto Networks NGFWs enforce real-time App-ID™ classification and AI-driven threat prevention for consistent policy as assets move. Next-Generation Trust Security and Zero Touch PKI automate certificate lifecycle management—preventing downtime, enforcing strong cryptography, and ensuring full visibility. Integration with NGFW enables unified control across edge and security layers. Together, Palo Alto Networks and Semtech deliver end-to-end zero trust—improving resilience, simplifying operations, and securing distributed industrial and public sector environments.

USE CASE:
Zero Trust Protection for Distributed Industrial and Utility Field Sites

CHALLENGE

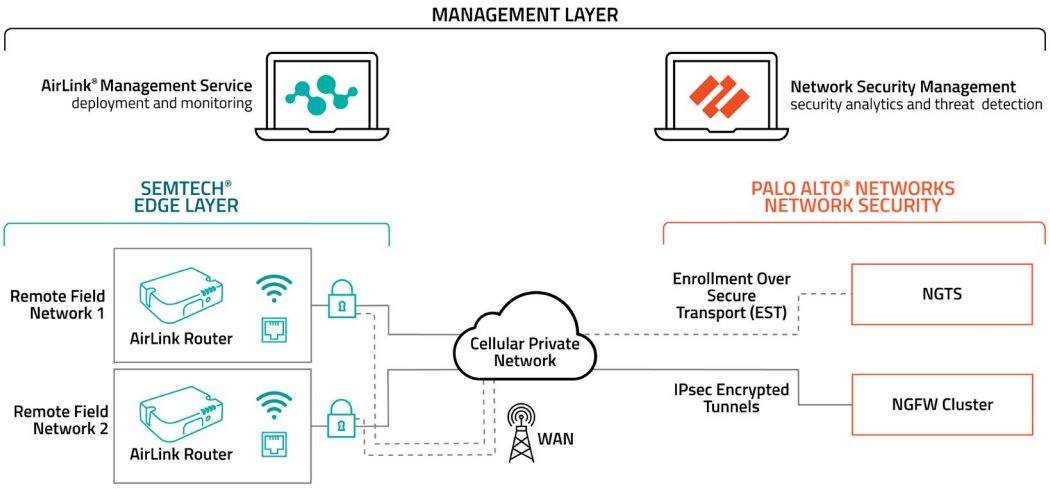
Remote industrial and utility sites rely on fixed assets operating across diverse, often untrusted networks where physical access can be compromised, exposing the broader environment. Maintaining consistent security, ensuring device integrity, and managing configurations across many unattended assets is challenging, increasing the risk of operational disruption and cyberthreats.

SOLUTION

AirLink routers deliver secure, reliable 4G/5G connectivity for field assets, with operational context enabling upstream zero trust enforcement. Encrypted local Ethernet protects on-site data integrity, while IPsec secures traffic across untrusted networks. ALMS ensures consistent configurations, OTA updates, and EST-based provisioning at scale.

Palo Alto Networks NGTS and ZTPKI automate certificate lifecycle management, enabling PAN-OS® to enforce identity-aware policies, real-time App-ID, and advanced threat prevention with unified visibility.

Together, this approach ensures continuous verification, simplifies operations, and strengthens protection for distributed industrial environments.



Key Benefits

- Robust encryption from edge to data center.
- Automated certificate management thwarts hacking.
- Layer 7 visibility and threat prevention for edge apps, devices.

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.

About Semtech

Semtech Corporation (Nasdaq: SMTC) is a leading provider of high-performance semiconductors powering AI data center networking, IoT connectivity and intelligent connected devices worldwide. Our global teams are committed to empowering solution architects and application developers to develop breakthrough products for the infrastructure, industrial and consumer markets. To learn more about Semtech technology, visit us at Semtech.com or follow us on LinkedIn or X.