Palo Alto Networks and OneLayer

Asset Visibility, Management, and Zero Trust for Private Wireless Networks

Key Benefits

- **App-ID™**: See the applications on your network, and learn how they work, their behavioral characteristics, and their relative risk.
- **Network traffic security**: Analyze network traffic inline, and instantly stop known, unknown, and highly evasive threats.
- **Improved policy precision**: Policies are applied to devices based on real-time context.
- **Automated device segmentation**: Devices are automatically grouped and assigned the correct policies, based on property changes.
- **Unauthorized device activity**: Real-time detection of events like SIM swaps, geofencing events, and unauthorized devices.
- **Consistent security across networks**: Helps ensure seamless policy enforcement for cellular and enterprise networks.

The Challenge

As organizations embrace cellular wireless technology for their enterprise IT and OT networks, they introduce new attack vectors, new device types with different risk profiles, and new protocols never before seen on wired networks. Gaining device visibility and enabling a Zero Trust security posture are challenging as organizations embark on this digital transformation.

Devices often belong to certain organizations or groups, each with specific security rules and business requirements. If security policies don't have the necessary security constructs for each group and its unique device profiles and instead rely on IP addresses, policy configurations become overly complex and extremely challenging to manage. Furthermore, when anomalous or malicious traffic is detected, logs or data based only on the IP address of the affected device don't provide the context needed for effective remediation.

The Solution

Incorporating Zero Trust principles into private 4G/5G networks is achievable with advanced device-level insights and contextual security policies. This approach extends the capabilities of next-generation firewalls (NGFWs) by incorporating rich details about the device types and new protocols present in enterprise IT and OT networks. It allows for dynamic policy enforcement adaptable to location changes, IP fluctuations, or SIM swaps, enabling group-specific security rules.

Visibility into noncellular devices connected via cellular routers helps ensure comprehensive monitoring and security controls across an expanded attack surface. The result is a streamlined, proactive security approach that extends across all IT and OT infrastructure.

OneLayer Bridge

OneLayer Bridge™ closes the critical gap in private 5G/LTE network deployments by addressing asset management and security needs, enabling a Zero Trust approach. This software-only platform integrates seamlessly with the network's packet core, routers, and security products, providing a unified view through a single pane of glass. It generates OneID, a unique device identifier crucial for precise tracking of both cellular and noncellular devices, regardless of IP changes, SIM context, or network transitions. OneID facilitates seamless device management across networks and supports microsegmentation for enhanced network security. With

automatic device profiling and a comprehensive prevention cycle—covering profiling, classification, policy creation, monitoring, and enforcement—OneLayer Bridge enriches integrated products and enables actionable insights. The platform extends existing network policies to the cellular domain, helping ensure robust and comprehensive security management.

Palo Alto Networks NGFWs

Palo Alto Networks ML-Powered NGFWs offer a prevention-focused architecture that's easy to deploy and operate. The machine learning NGFW inspects traffic, including applications, threats, and content, and ties traffic to the user, regardless of location or device type. Automation reduces effort so security teams can replace disconnected tools with tightly integrated innovations and enforce consistent protection. Panorama® network security management empowers you with easy-to-implement, consolidated policy creation and centralized management features. Manage your network security with a single security rulebase for firewalls, threat prevention, URL filtering, application awareness, user identification, sandboxing, file blocking, access control, and data filtering. This simplification, along with App-ID technology-based rules, dynamic security updates, and rule usage analysis, reduces administrative workload and improves your overall security posture.

Palo Alto Networks and OneLayer

The integration of Palo Alto Networks and OneLayer extends Zero Trust security to private 4G/5G networks by providing critical device-level insights. The solution enables users to create and enforce policies based on detailed device context, helping ensure consistent application even when IP or SIM card changes occur. With OneLayer, users can create dynamic policies tailored to device context, including location shifts or hidden devices. Palo Alto Networks App-ID and dynamic grouping with OneLayer context-based auto-classification enables automated application-aware network segmentation that extends to private 4G/5G networks. It also helps ensure continuous updates to the NGFW for scenarios like geofencing, SIM swaps, and dynamic IPs, adapting policies without manual reconfiguration. Allowed applications are further secured by Content-ID™, which combines a real-time threat prevention engine to block a wide range of exploits, including malware as well as targeted and unknown threats.

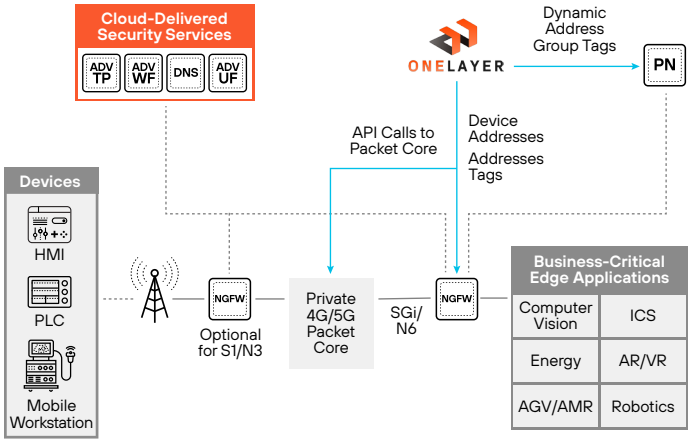

Figure 1: Palo Alto Networks and OneLayer high-level architecture

Use Case 1: Effective Zero Trust Security Through Device Visibility and Context

Challenge

Achieving effective Zero Trust security in private 4G/5G networks requires comprehensive device visibility and management based on device context, rather than static identifiers like SIM cards or IPs. While mobile network operators (MNOs) focus on SIMs, enterprises require more granular context about connected devices, their use, and their risks.

Solution

OneLayer overcomes the visibility and segmentation challenge with a sophisticated fingerprinting solution that integrates with Palo Alto Networks NGFWs, offering detailed insights into device attributes and context. This solution correlates multiple identifiers to maintain a consistent device identity under changing conditions, such as SIM swaps or location shifts. By employing automated, context-based classification, OneLayer enables dynamic policy enforcement without manual intervention. The integration with Palo Alto Networks helps ensure consistent policy enforcement and security across cellular and enterprise networks, boosting network efficiency and integrity.

Use Case 2: Enhancing Visibility and Threat Prevention for Hidden Devices

Challenge

Managing noncellular devices connected via adapters like routers, hotspots, or Bluetooth is crucial to eliminating security visibility gaps in cellular networks. These devices often inherit privileges, leading to potential security risks if not monitored accurately. Other solutions may overlook these connections, resulting in unauthorized access and compromised network integrity. Organizations need robust detection and response mechanisms to quickly address threats and maintain network security.

Solution

OneLayer enhances security by providing visibility into noncellular devices connected via adapters and integrating with Palo Alto Networks NGFWs for precise threat detection and response. This collaboration helps ensure all devices receive appropriate privileges, preventing security visibility gaps and unauthorized access. By continuously monitoring and gathering contextual data, OneLayer enables swift identification of threats, allowing Palo Alto Networks NGFWs to adjust network privileges and isolate at-risk devices automatically. This integrated approach helps ensure comprehensive security coverage, maintaining robust network integrity and adaptability against dynamic threats.

About OneLayer

OneLayer brings complete visibility, asset management, and Zero Trust security to all devices connected to private LTE and 5G networks to maximize operational excellence. The platform enables enterprises to treat their private cellular network as another enterprise network without the need to be cellular experts. For more information, visit www.onelayer.com.

About Palo Alto Networks

Palo Alto Networks is the global cybersecurity leader, committed to making each day safer than the one before with industry-leading, AI-powered solutions in network security, cloud security, and security operations. For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS | ONELAYER

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

parent_pb_onelayer_020325