Palo Alto Networks and Claroty

Securing Industrial Control Systems

Benefits of the Integration

Together, Palo Alto Networks and Claroty offer:

- Full visibility into OT networks, enabling users to assess, monitor, and mitigate potential threats to these networks more effectively and efficiently.
- Accelerated incident response capabilities, including automatic detection and blocking of threats to OT networks.
- Real-time, contextual alerting with root cause analysis to reduce alert fatigue, improve OT threat hunting accuracy, and strengthen process integrity and cyber resilience.

The Challenge

Protecting industrial enterprises and critical infrastructure from cyberattacks requires full visibility into the operational technology (OT) networks on which organizations' industrial processes and machinery rely. Due to the prevalence of proprietary protocols, legacy systems, and unfamiliar assets in OT networks, however, full visibility is exceedingly difficult to attain. Without it, security teams cannot accurately detect, respond to, or remediate threats, nor implement the fundamental security controls necessary to minimize the risks such threats pose to OT availability, reliability, and safety.

Claroty Continuous Threat Detection

Claroty Continuous Threat Detection (CTD) is the foundation of the Claroty Platform. Rooted in the principle that you cannot protect what you cannot see, CTD grants complete visibility into OT networks, the ability to easily discover and manage all assets within those networks, and continuous monitoring of all threats and vulnerabilities relevant to those assets and networks.

Specifically, CTD leverages Claroty's proprietary deep packet inspection (DPI) engine to extract precise details about each asset on the OT network, profile all communications and processes, and generate a fine-grained behavioral baseline that characterizes legitimate traffic. CTD also alerts you in real time to baseline deviations and the presence of indicators of compromise (IOCs), known and zero-day threats, and exact-match vulnerabilities.

Palo Alto Networks

Palo Alto Networks Next-Generation Firewalls offer a prevention-focused architecture that is easy to deploy and operate. Automation reduces manual effort so your security teams can replace disconnected tools with tightly integrated innovations, focus on what matters, and enforce consistent protection everywhere.

Palo Alto Networks and Claroty

Palo Alto Networks and Claroty have integrated the Next-Generation Firewall and CTD to offer security and operational personnel a scalable solution that seamlessly bridges the cybersecurity gap between IT and OT environments.

With this integration, CTD automatically discovers, baselines, and monitors all OT network assets, communications, and processes. Detection of baseline deviations and other anomalous activity, including threats, triggers the creation of a new rule within the Next-Generation Firewall, which then automatically blocks or limits the source of the threat. As a result, users gain extreme visibility into the deepest levels of their OT networks, more efficient and effective OT threat detection, and stronger protection of OT availability, reliability, and safety.

Use Case: Combating Self-Propagating Ransomware

WannaCry and NotPetya are self-propagating ransomware variants that were both used in attacks that caused global disruption and massive damage to organizations' OT networks, yet were not targeting those networks directly.

Challenge

A hallmark of self-propagating ransomware is its ability to rapidly spread across networks and connected devices. The presence of unsecured pathways between IT and OT networks—which are exceptionally common among industrial enterprises and critical infrastructure—can exacerbate this threat because it enables the ransomware to easily spill over from IT into OT. Unfortunately, many organizations lack the requisite telemetry across OT networks to identify anomalous and potentially malicious activity, and thus they tend to face a higher risk of compromise. Historically, such compromises have resulted in lengthy downtime periods and devastating damages for impacted organizations.

Solution

Close integration between CTD and Palo Alto Networks Next-Generation Firewall enables detailed policy and segmentation recommendations based on baseline behavior, including mapping of the assets, protocols, and ports used for OT-specific communications, to be sent from CTD to the Next-Generation Firewall. This empowers users to proactively and automatically block or limit specific communication protocols or commands to prevent malicious activity, such as that associated with self-propagating ransomware, from penetrating and spreading across OT networks.

Use Case: Network Segmentation

Challenge

Many organizations lack the OT visibility needed to understand normal operational process workflows, expected network communication paths, and all network assets. Even with visibility, traditional segmentation projects can be extremely difficult and time-consuming to implement due to the often vast, widely distributed, and geographically isolated nature of OT networks.

Solution

This integration reduces the complexity of segmentation by utilizing virtual rather than physical measures to segment OT networks. CTD automatically identifies and sends detailed virtual segmentation recommendations—based on the behavioral baseline created through visibility and continuous monitoring—to the Next-Generation Firewall. Users can then leverage the Next-Generation Firewall to quickly create segments while reducing the risk of disrupting connections that impact normal communication patterns and processes vital to operations. After initial segments are created, CTD continues to automatically discover new assets and connections as well as send updated recommendations to the Next-Generation Firewall to adjust and optimize segments as needed in real time.

Figure 1 shows an example of how this integration can be deployed in a converged IT/OT environment based on the Purdue model of a layered architecture. In this scenario, CTD analyzes I/O-level traffic while the Next-Generation Firewalls are placed in strategic detection and prevention points, allowing them to block or limit communications for a single node or between nodes to prevent operational disruption.

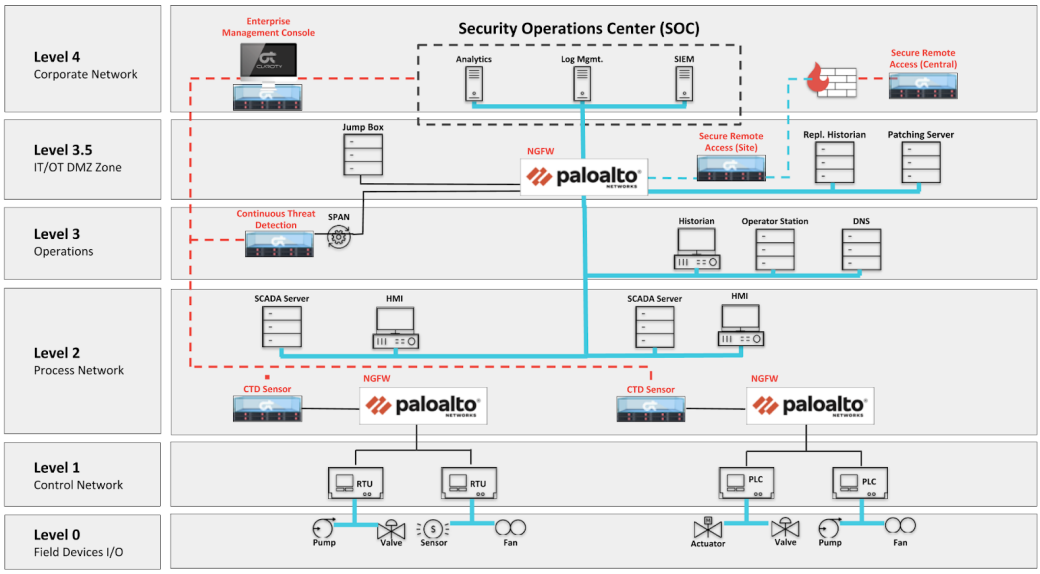

Figure 1: Palo Alto Networks and Claroty integration

About Claroty

Claroty bridges the industrial cybersecurity gap between information technology (IT) and operational technology (OT) environments. Organizations with highly automated production sites and factories that face significant security and financial risk especially need to bridge this gap. Armed with Claroty's converged IT/OT solutions, these enterprises and critical infrastructure operators can leverage their existing IT security processes and technologies to improve the availability, safety, and reliability of their OT assets and networks seamlessly and without requiring downtime or dedicated teams. The result is more uptime and greater efficiency across business and production operations.

Backed and adopted by leading industrial automation vendors, Claroty is deployed on all seven continents globally. The company is headquartered in New York City and has received $100 million in funding since being launched by the famed Team8 foundry in 2015. For more information, visit www.claroty.com.

About Palo Alto Networks

Palo Alto Networks, the global cybersecurity leader, is shaping the cloud-centric future with technology that is transforming the way people and organizations operate. Our mission is to be the cybersecurity partner of choice, protecting our digital way of life. We help address the world's greatest security challenges with continuous innovation that seizes the latest breakthroughs in artificial intelligence, analytics, automation, and orchestration. By delivering an integrated platform and empowering a growing ecosystem of partners, we are at the forefront of protecting tens of thousands of organizations across clouds, networks, and mobile devices. Our vision is a world where each day is safer and more secure than the one before. For more information, visit www.paloaltonetworks.com.

paloalto NETWORKS

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