aruba
a Hewlett Packard Enterprise company

CLAROTY
Clarity for OT Networks

PARTNER SOLUTION OVERVIEW

ARUBA & CLAROTY

Protecting the Industrial Internet of Things with Enhanced Access Control

The current reality of the Internet of Things (IoT) is that it is fundamentally untrustworthy. The operational technology (OT) vendors that build IoT machinery are experts in robustness and reliability, but not cybersecurity. The divide between OT and IT forms an attack surface that leaves enterprise organizations open to risk when they don't know how, or choose not, to address it.

The most efficient way to close this gap is with uniform security policies and uniform visibility that spans from I/O on the factory floor to the CEO suite leaving no gaps, shadows, or unexposed surfaces.

WHY ARUBA & CLAROTY?

- Certified interoperability
- Granular device information for up-to-date asset inventory data
- Enforcement of secure OT and IoT access policies
- Fast incident response time based on real-time OT device status, device attributes, and network communications
- Blocks unwanted user access to secure OT networks

WHAT YOU SEE IS WHAT YOU CAN PROTECT

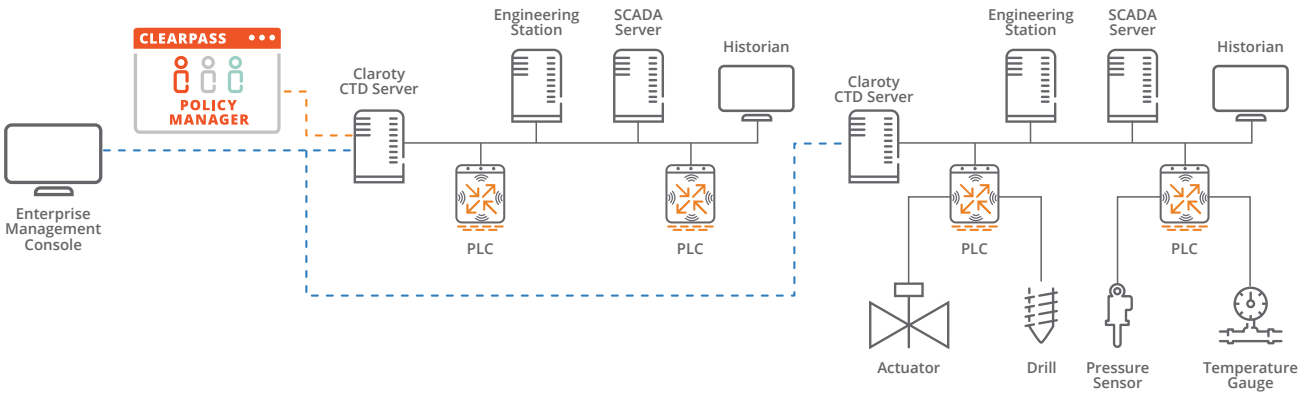
Aruba's 360 Security Architecture delivers the visibility and security to close the gap. This architecture uses ClearPass Device Insight to identify new IoT devices attempting to connect to the network and ClearPass Policy Manager to define and enforce access policies.

ClearPass Policy Manager interfaces with more than 150 different security vendors whose products include next generation firewall, SIEM, EMS, IDS, MDM, and analytics systems. OT devices are a unique case because they use physical layers, protocols, and operating modes unlike anything commonly seen in the IT world.

Aruba has partnered with Claroty to bring visibility and security to a broad range of OT devices. This integration extends the capabilities of ClearPass to reach OT devices and industrial control systems across a broad range of industries.

Claroty's Continuous Threat Detection (CTD) Software works in conjunction with CTD Sensors to observe and monitor OT network traffic, device configuration, and change management. The solution has three operating modes to detect OT anomalies, threats, and operator errors: passive, active, and AppDB.

Claroty provides ClearPass with information about each OT asset on the network, including the vendor, role and model. Using these attributes, ClearPass policies can control OT asset authorization and security posture to the maximum extent permitted under OT operating guidelines for that enterprise.



For example, using OT attributes reported by Claroty, ClearPass can determine if an OT device adheres to the organization's security compliance policies. If not, then ClearPass can change an authorization policy, based on OT contextual information provided by Claroty, to limit the device's network access and reduce its potential security impact until remediation can be affected.

USE CASES

- **Assets and User Permission Policy Profiles:** asset inventory and baseline monitoring to manage device and user profiles using asset type, vendor, firmware, OS, supported protocols, and other parameters.
- **Unauthorized Access:** secure devices such as programmable logic controllers (PLCs) and remote terminal units (RTUs) from unwanted access.
- **System Misconfigurations or Vulnerabilities:** locate vulnerabilities and misconfigurations so they can be quickly remediated.

CAPABILITIES CHECKLIST

ClearPass can receive industrial network and device attributes being monitored by Claroty. Through alerts and context unique to the operations environment, ClearPass can adjust permissions and security policies to increase OT security without disruptions or impacting productivity in plants or processes.

CERTIFIED INTEROPERABILITY

We've taken the guesswork out of industrial network access control by certifying the interoperability of Claroty with ClearPass. Claroty's installation wizard used in conjunction with the ClearPass menu selections and filters make set-up a breeze.

SUMMARY

Claroty and Aruba have bridged the IT and OT gap with a joint solution that provides threat detection and policy enforcement to OT networks across a broad range of vertical markets. Contact your local sales representative to see how together we deliver the most secure solution for industrial and manufacturing industries.

To learn more about Aruba ClearPass, please visit: https://www.arubanetworks.com/products/security/network-access-control/

To learn more about Claroty, please visit: https://www.claroty.com/

Features	Claroty Continuous Threat Detection (CTD) and Aruba ClearPass
Device identity including IP address, vendor, model, firmware, serial number, virtual zone, site, industrial protocols, device name, firmware version, criticality, CVE/scoring, risk level, etc.	✓
OT device and OT network baseline deviations with context	✓
OT device and OT network protocols in use	✓
OT device and OT network CVE match/scoring	✓
Virtual zones and deviations in normal communication behavior	✓

aruba
a Hewlett Packard Enterprise company

PSO_Claroty_120619 a00090831enw