CLAROTY | Mission Secure

INTEGRATION BRIEF

CLAROTY AND MISSION SECURE: COMPLETE OT VISIBILITY WITH ACTIVE POLICY ENFORCEMENT

The Next Step Toward OT Zero Trust

Operational technology (OT) networks, including ICS and SCADA systems common in critical infrastructure and manufacturing organizations, have become increasingly connected to IT networks. The convergence of these networks has led to the proliferation of the Extended Internet of Things (XIoT), the web of connected devices that span and support cyber-physical systems, ranging from both legacy and greenfield OT assets, to IT and IoT devices, to building management system equipment. While this connectivity has improved operational efficiency, it has also made OT systems more vulnerable to attacks and a more attractive target for threat actors.

Unlike attacks on IT devices that generally focus on data theft and monetary gain, a successful attack on OT or IIoT assets can alter physical processes, damage critical infrastructure, disrupt services, and endanger the health and safety of workers and the communities they serve.

As such, it has increasingly become the responsibility of IT security teams to oversee the cybersecurity programs for OT networks, as well as inform OT engineers of cyber and operational risks and the potential impact of these risks being exploited. In order to do this, organizations need to have unified visibility of their assets, network communications, and associated vulnerabilities at all times.

Organizations also need the ability to manage OT network traffic with the same degree of control they have over IT networks. Until now, this has been challenging—if not impossible—because OT environments are fundamentally different from their IT counterparts.

With a combined Claroty xDome and Mission Secure solution, organizations gain not only complete visibility into their OT networks, but the ability to enforce granular, context-aware cybersecurity policies—the next step on the road toward Zero Trust security practices in OT environments.

Key Benefits

Asset and Traffic Visibility, Down to Level 0 of the Purdue Model

Claroty xDome accurately identifies and discovers all XIoT assets to generate a centralized, dynamic, and enriched asset inventory. With the addition of Mission Secure's industry-leading Level 0 signal monitoring and validation technology, organizations gain a complete, real-time view of their entire operational environment, including the ability to correlate network activity with process variable changes.

Advanced Threat and Anomaly Detection

Effective vulnerability management and threat processing requires a deep understanding of the connected landscape. Detailed device attribution and knowledge of authorized device behavior is essential to detect unauthorized, anomalous behavior. All alerts are contextualized by xDome to optimize response and remediation before a threat can impact operations.

Segmentation and Policy Enforcement, Built for OT

Using comprehensive device information, communication profiles, and tailored risk scores from xDome, Mission Secure provides an intuitive interface for defining and enforcing communication policies throughout the OT environment. From basic network segmentation to granular policies based on vulnerability scores, patch status, asset states, or time and date, organizations can create tailored security policies that fit their unique operational requirements and security goals.

A New Model for OT Cybersecurity

OT cybersecurity is a specialized job, requiring specialized technology and domain-specific expertise. Together, Claroty and Mission Secure deliver a complete set of OT-native security capabilities, enabling organizations to minimize risk and address the rapidly-evolving threats facing industrial operations.

As the industry leader in OT visibility and vulnerability management, Claroty provides a complete picture of your organization's asset inventory and XIoT vulnerabilities with customized risk scoring as well as threat detection and network communication mapping. By integrating this data with Mission Secure's industry-first OT policy enforcement engine, organizations gain the ability to create and enforce policies based on hundreds of possible inputs. Connections can be allowed or blocked based on:

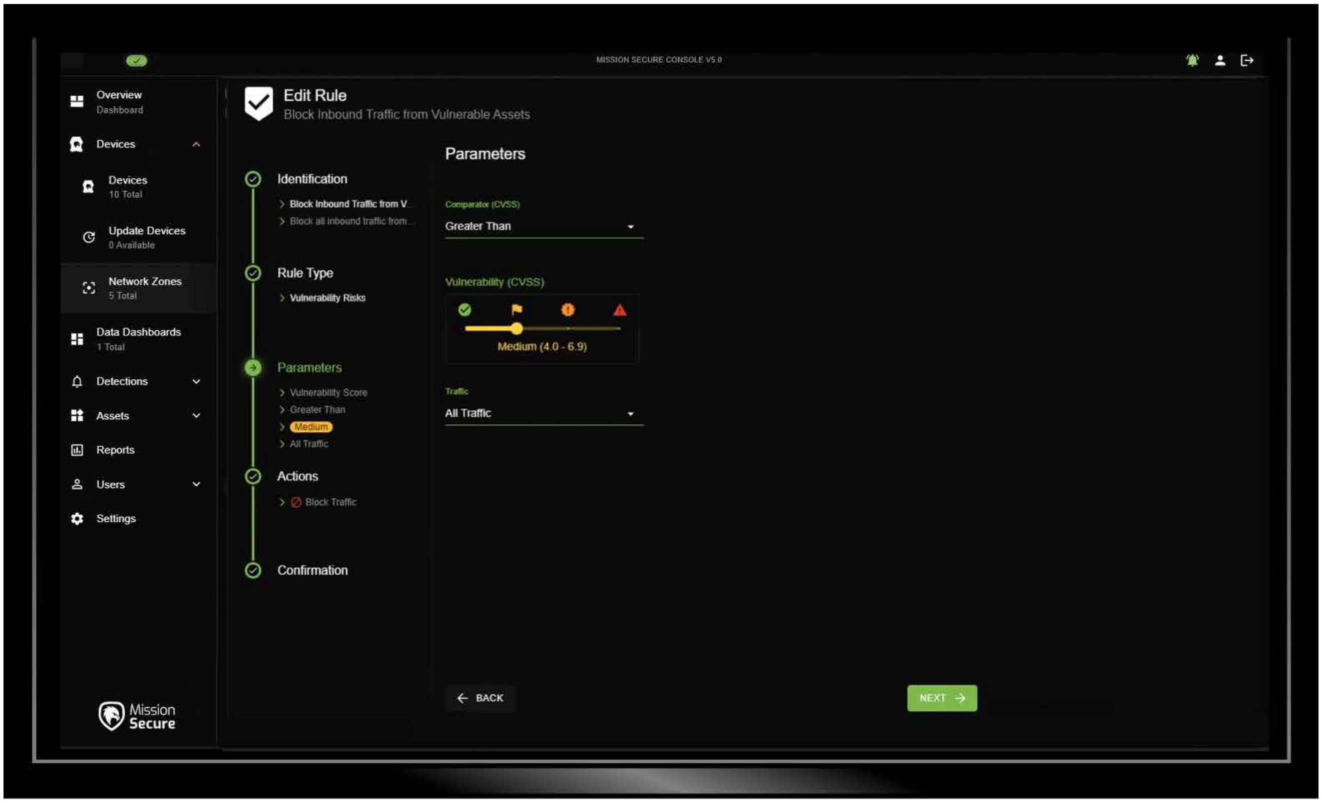
- Physical location or network segment
- Calendar date, day of the week, or time of day
- Risk scores of the source and/or destination devices
- Firmware version, patch status, or other device attributes
- Custom variables defined by the organization

In addition, Mission Secure's Level 0 signal monitoring and validation technology enables enhanced threat detection and policy enforcement at the lowest and most critical levels of the OT network.

How it Works

1. Device profiles created and maintained by Claroty, which include attributes such as OS, firmware versions, risk score, and site, are passed to Mission Secure.
2. Claroty xDome policy recommendations provide the basis for tailored OT security policies, which are configured and deployed using Mission Secure's policy engine.
3. Detections of anomalous behaviors are aggregated and reported to improve overall mitigation and remediation response effectiveness.

With the rapid growth in XIoT devices—and the risks they pose when connecting to your networks—the pairing of Mission Secure and Claroty represents a uniquely powerful security solution, providing state-of-the-art visibility and network controls.



Edit Rule
Block Inbound Traffic from Vulnerable Assets

Identification
- Block Inbound Traffic from V...
- Block all inbound traffic from...

Rule Type
- Vulnerability Risks

Parameters
- Vulnerability Score
- Greater Than
- Medium
- All Traffic

Actions
- Block Traffic

Confirmation

Parameters

Comparator (CVSS): Greater Than

Vulnerability (CVSS): Medium (4.0 - 6.9)

Traffic: All Traffic

Using asset and vulnerability inputs from Claroty, Mission Secure allows administrators to define and deploy tailored OT security policies.

About Mission Secure

Mission Secure is a leader in cybersecurity for operational technology and industrial control systems, helping organizations gain visibility and control over their critical assets. With unique, built-for-OT threat detection and policy enforcement capabilities, Mission Secure enables effective Zero Trust cybersecurity architectures from signal to cloud.

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide a full range of controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the world's largest investment firms and industrial automation vendors, Claroty is deployed by hundreds of organizations at thousands of sites globally.

For more information, visit claroty.com or email contact@claroty.com.