SOLUTION OVERVIEW

ACHIEVING CYBER RESILIENCE

XIoT Cybersecurity Requirements in the Modern Industrial Network

The XIoT Security Challenge

Cyber-resilient organizations not only survive adverse cyber conditions — they thrive in spite of them. Unfortunately, cyber resilience is growing increasingly out-of-reach across industrial sectors.

The roots of these challenges exist within the growth of the Extended Internet of Things (XIoT). Fueled by digital transformation, this vast cyber-physical web spans everything from traditional OT assets in your industrial environment to the "smart" systems like lightbulbs, HVAC systems, and even the internet-connected vending machines within them. Despite its clear business benefits, this cyber-physical connectivity is also creating new security blindspots and a growing attack surface that pose considerable risks to the availability, integrity, and safety of industrial environments.

Achieving and maintaining cyber resilience amid the XIoT's challenging security and risk conditions is far from impossible — but it does entail a robust set of requirements that simply cannot be satisfied by traditional solutions or generalized approaches. Having built and optimized industrial cybersecurity solutions around the globe, Claroty views the journey towards cyber resilience through a few core use cases:

- Asset Discovery
- Vulnerability & Risk Management
- Network Protection
- Threat Detection

Key Requirements

Ongoing security and compliance management

A comprehensive, always up-to-date inventory of assets is essential for managing an environment's exposure to cyber risk and reporting compliance metrics to organization stakeholders and auditors

A Zero Trust security architecture

Successfully implementing Zero Trust policies across the organization creates a solid foundation for security practices that minimize cyber risk by driving everything from network segmentation to secure remote access

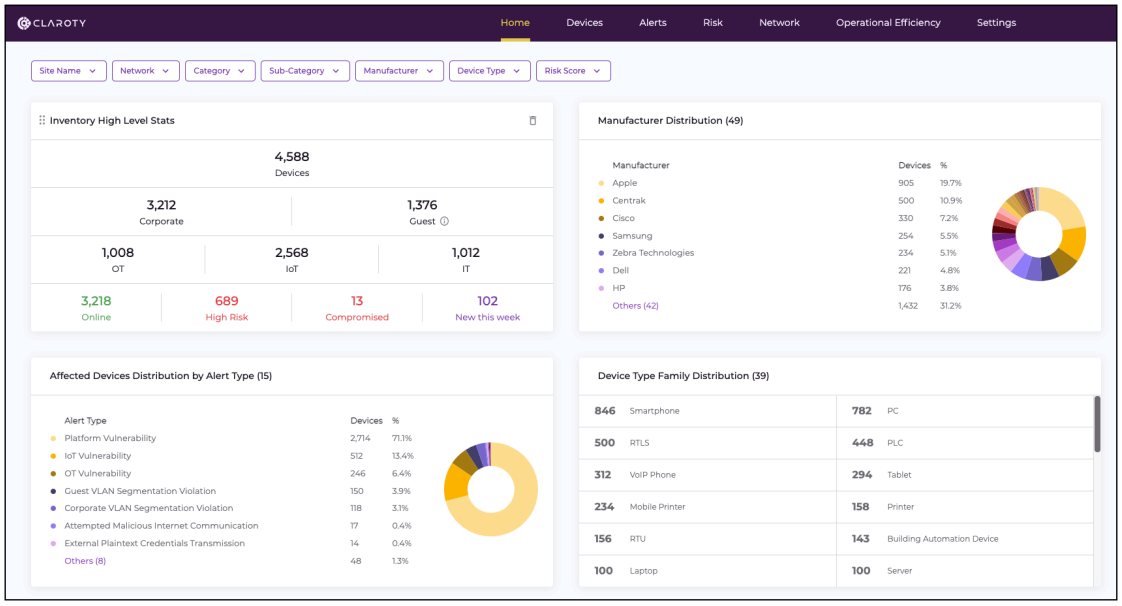
The ability to detect and mitigate threats

Continuous monitoring for indicators of both known and emerging threats and a deep understanding of attack vectors are essential to being prepared for, able to respond to, and able to withstand malicious cyber activity.

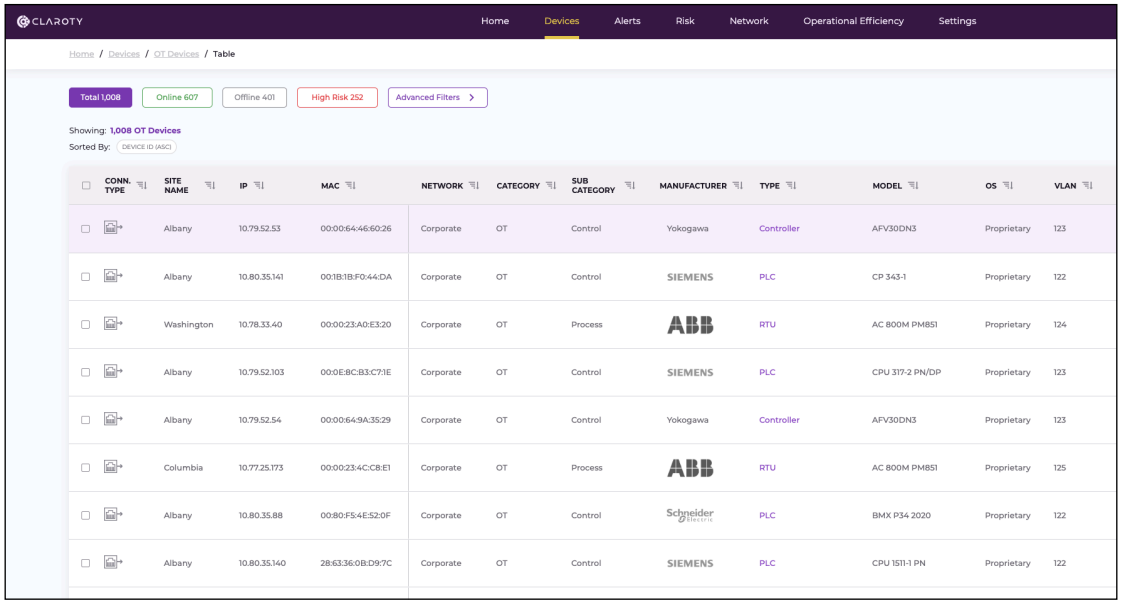
Asset Discovery

As the backbone of cyber resilience, nearly all industrial cybersecurity use cases would be practically impossible without comprehensive visibility into all XIoT assets and their communications. Given this, organizations should stand for no less than a complete, always up-to-date inventory of assets across the XIoT–including each asset's full scope of identifiers and behavioral details. Claroty supports these goals through:

- **Discovery Methods**: A variety of asset discovery methodologies supported by the largest, most in-depth library of XIoT protocol coverage in the industry.
- **Implementation**: Flexible SaaS-based and on-premise deployment options to suit industrial environments regardless of their scale, architecture, or geographic span.
- **Integrations**: Claroty works seamlessly with common CMDB tools and other asset management solutions to help optimize enterprise-wide asset workflows.



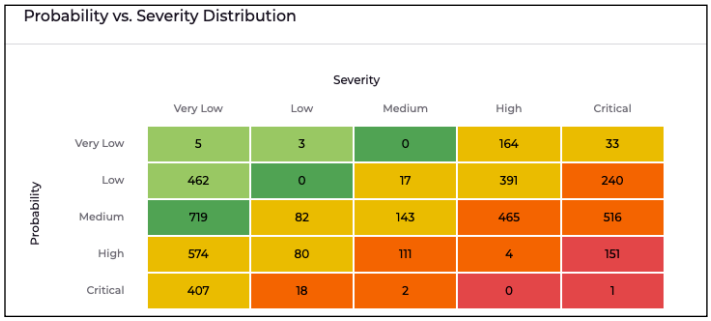
Claroty xDome Home Dashboard



Claroty xDome OT Assets List

Vulnerability & Risk Management

Vulnerabilities are inherent in industrial environments due to their legacy systems, diverse asset base, and limited maintenance windows. By correlating network and asset details with our vulnerability and risk knowledge base, Claroty uncovers risk blindspots that take the form of unpatched CVEs, misconfigurations, poor security practices, and unsecured protocol usage to:



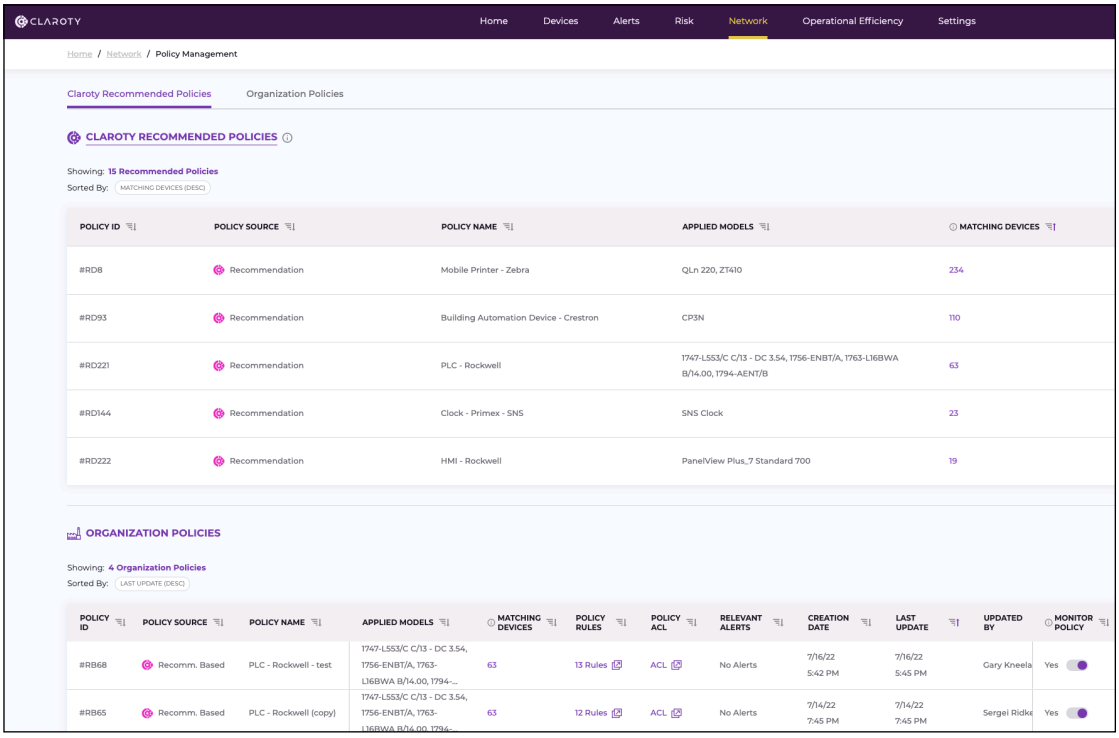
Claroty xDome Risk Prioritization

- **Provide Multi-Factor Risk Scores** that reveal the true risk of an asset as it relates to an organization's unique environment
- **Enable and Measure Comprehensive Risk Reduction** by helping organizations prioritize remediation of vulnerabilities most likely to be exploited

Network Protection

Network segmentation and secure remote access are zero trust controls deemed highly effective at improving industrial cybersecurity posture. Distinguishing legitimate communication across business processes and applications requires a clear picture of how and why these assets are communicating and frequently, ineffective or completely nonexistent segmentation between assets is the root cause of many aspects of network risk.

Claroty jumpstarts network segmentation programs by automatically creating and deploying communication policies that can be enforced through existing infrastructure. Additionally, Claroty streamlines remote access through an OT-specific solution offering RBAC, an industrial-aware secure architecture, and simple administration.

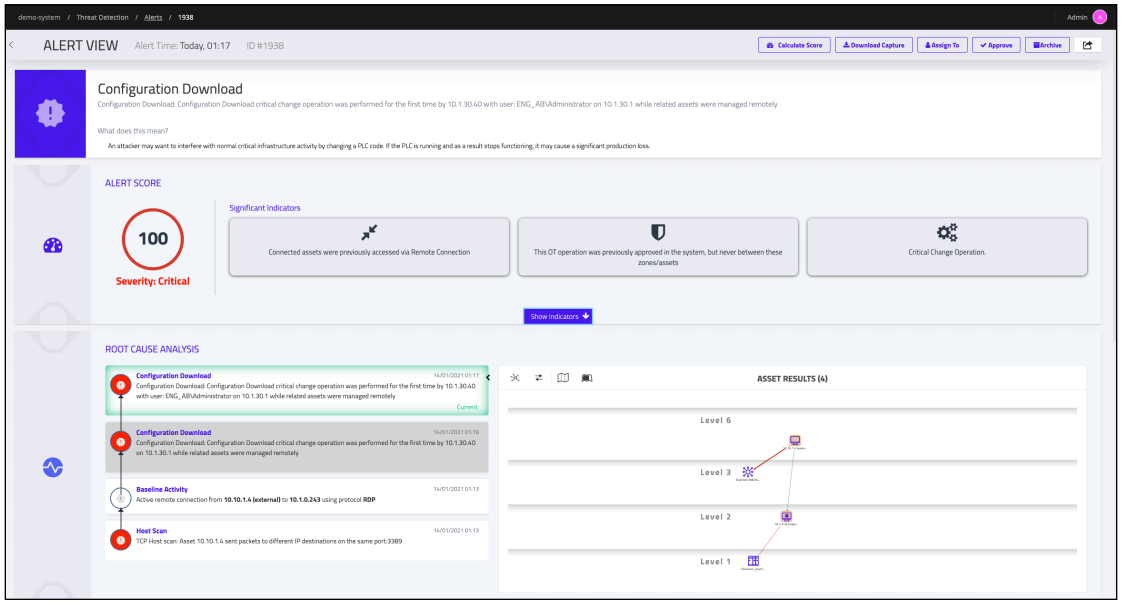


Claroty xDome Policy Management

Threat Detection

No industrial environment is immune to threats and the ability to detect and respond when they surface is a necessary requirement in a mature cybersecurity program. The difficulty behind this is two-sided: 1) Industrial environments are unique in their operational goals and architectures and 2) the threat landscape is rapidly evolving as a result of growing interconnectivity. Claroty's cyber-resilient threat detection model tackles these challenges by:

- **Monitoring and alerting on anomalous network communications** resulting from potentially malicious communication policy violations
- **Detecting threats through indicators of compromise** backed by known threat signatures and proprietary signatures from Claroty's Team82
- **Extending existing SOC capabilities into the operational environment** with ready-made integrations with SIEM, SOAR, and EDR solutions



Claroty CTD Alert View

About Claroty

Claroty empowers industrial, healthcare, and commercial organizations to secure all cyber-physical systems in their 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. The company is headquartered in New York City and has a presence in Europe, Asia-Pacific, and Latin America.

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