DATA SHEET

Claroty xDome

The Modular XIoT Solution for the Industrial Cybersecurity Journey

The XIoT Security Challenge

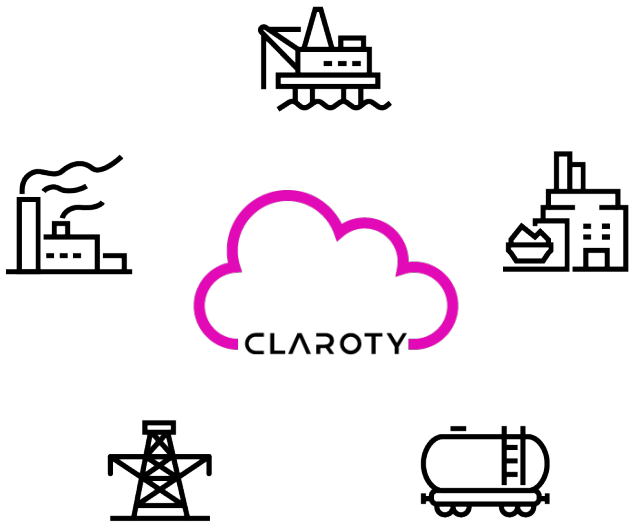
Industrial organizations require cybersecurity to maintain cyber and operational resilience. Both objectives, however, are growing increasingly out-of-reach. The roots of these challenges exist within the growth of the Extended Internet of Things (XIoT). Fueled by digital transformation, this vast cyber-physical web spans everything from traditional OT assets in industrial environments, to the "smart" lighting and HVAC systems and even the internet-connected vending machines within facilities. 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 operational availability, integrity, and safety of operational environments.

Achieving and maintaining cyber and operational 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. Claroty xDome spans the entire cybersecurity journey, from empowering organizations with comprehensive asset visibility, identifying, measuring, and prioritizing risk, to deploying Zero Trust-based protective controls, to optimizing threat detection through a vast network of integrations. xDome is a modular platform, SaaS platform that makes XIoT cybersecurity decision clear through:

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

xDome Benefits At A Glance

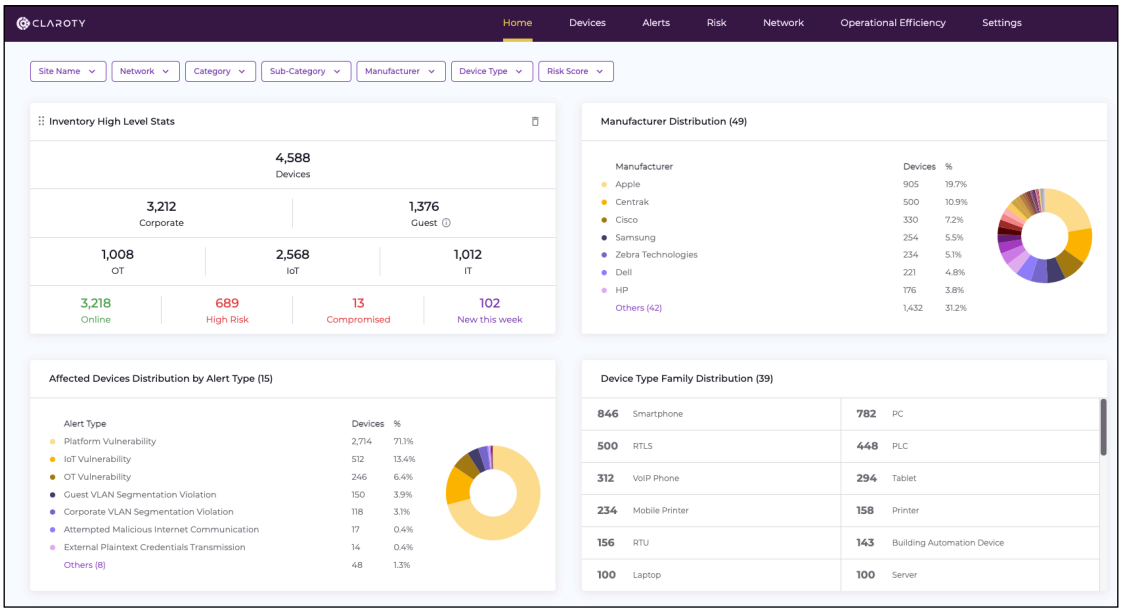
- Extends cybersecurity across the XIoT with a modular, SaaS-powered industrial cybersecurity platform
- Supports the full industrial cybersecurity journey from asset discovery to comprehensive cybersecurity integration and optimization
- Designed for scalability, flexibility, and ease-of-use regardless of network size, architecture, or diversity of end users
- Integrates seamlessly with security solutions to extend existing cybersecurity controls into the industrial environment



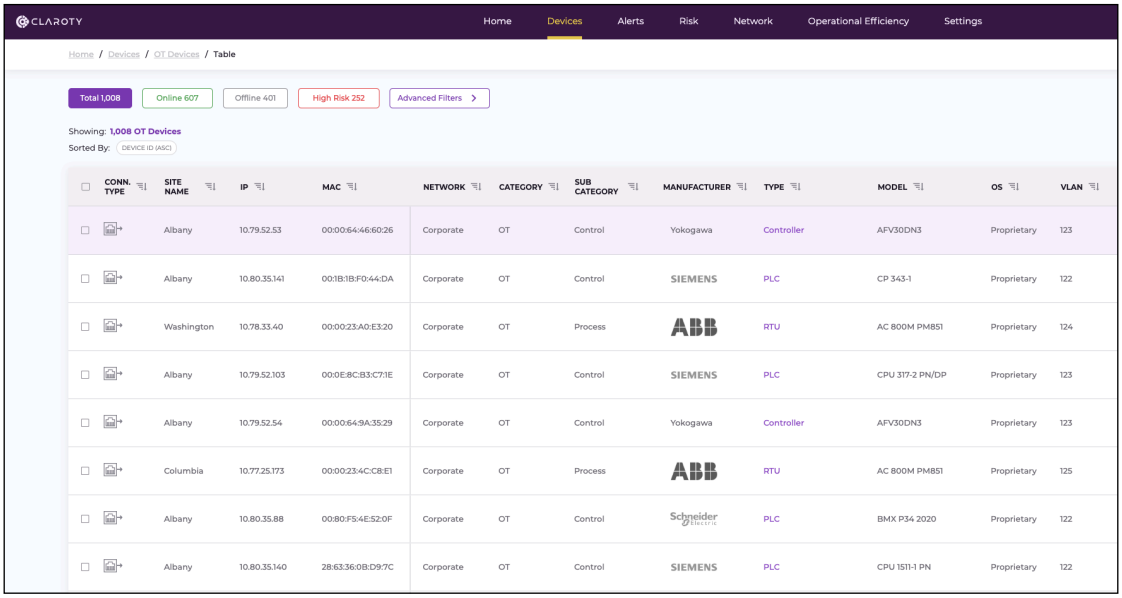
Asset Discovery

Effective industrial cybersecurity starts with knowing what needs to be secured, which is why a comprehensive XIoT asset inventory is the foundation of the industrial cybersecurity journey. Claroty xDome leverages the broadest and deepest portfolio of XIoT protocol coverage, along with Claroty Team82's domain-specific research into these protocols, to provide a highly detailed, centralized inventory of XIoT assets. Claroty is the only vendor capable of providing this caliber of visibility through three distinct, highly flexible methods that can be combined or used separately based on the unique needs of each environment:

- **Passive Monitoring**: Continuous monitoring of network traffic to identify and enrich asset details and communication profiles
- **Claroty Edge**: Strategically placed, quick, and safe querying of difficult or otherwise unreachable parts of the network
- **Integration Ecosystem**: Seamlessly integrate with common CMDB and asset management tools to further enrich asset details and optimize enterprise asset management



Claroty xDome Home Dashboard



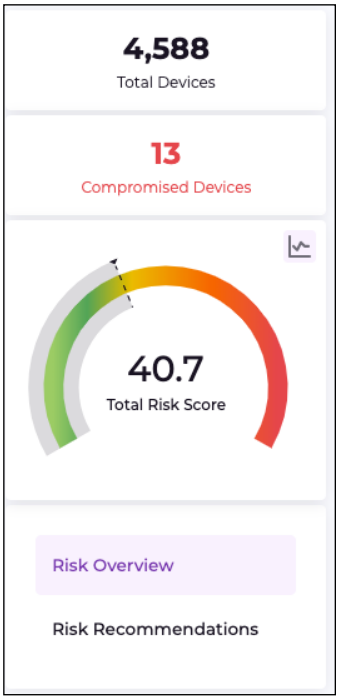
Claroty xDome OT Asset List

Vulnerability & Risk Management

xDome automatically correlates every XIoT asset with the latest vulnerability findings from our award-winning Team82 researchers, as well as our vast database of CVEs and other weaknesses. With the ability to completely customize an organization's risk tolerances, xDome provides tailored risk scores and recommendations for network-wide risk reduction actions. Highlights include the ability to:

- Streamline vulnerability identification and manage remediation planning and execution
- Safely employ vulnerability scanners and orchestration tools to identify IT risk in the industrial environment
- Prioritize risk mitigation based on real and simulated impact results

This translates to a holistic, organization-specific view of risk, the potential impact of vulnerabilities, and indicators of areas most likely to be exploited. As a result, users can identify, prioritize, and remediate vulnerabilities in industrial environments more effectively.



Network Risk Score

Network Protection

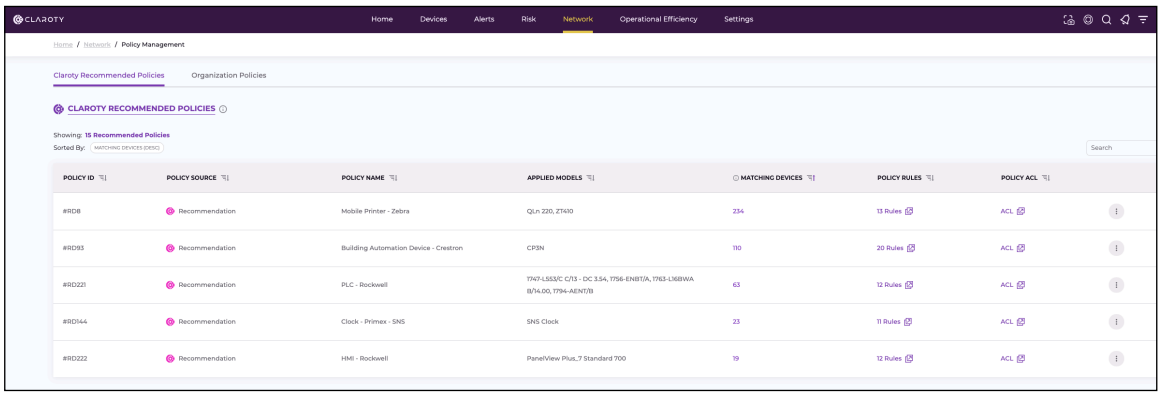
Backed by Claroty's deep domain expertise, xDome leverages the visibility it provides into XIoT assets and their behavioral patterns to automatically define and recommend network communication policies. This automated solution makes it easier to monitor, refine, and enforce these policies through existing security infrastructure without impacting operations. These policies are also dynamic and can be simulated to demonstrate network impact before implementation, helping organizations keep up with the changing conditions within complex environments.

As a method of network segmentation, Claroty xDome's network protection capabilities help lay the foundation for Zero Trust practices that are core to improving an organization's industrial cybersecurity posture by:

Enhancing the visibility of assets within the network architecture

Providing a baseline view of normal network communications

Reducing risk through policy monitoring and enforcement



Claroty xDome Recommended Policies View

Threat Detection

Recognizing the rising frequency and impact of threats targeting industrial environments, xDome embraces a resilient detection model to continuously monitor your environment for the earliest indicators of both known and emerging threats. Claroty xDome profiles all XIoT assets and their communication patterns in order to generate a baseline for normal network behavior, providing automated methods to monitor, prioritize, and respond to alerts. Highlights include:

- **Detect Known and Unknown Threats**: Characterize legitimate traffic to detect anomalous communications, identify threat signatures, weed out false positives, and alert users in real-time to known, unknown, and emerging threats.
- **Domain-specific Threat Intelligence**: Claroty xDome receives automatic detection updates for new signatures, vulnerabilities, malicious IP's, threats, and other data so organizations are always operating on the most up-to-date threat intelligence.
- **Broad Integration Opportunities**: Claroty xDome extends existing SOC capabilities into the operational environment with ready-made integrations with SIEM, EDR, and other security solutions.
- **MITRE ATT&CK Alert Mapping**: Incoming alerts are mapped to the MITRE ATT&CK for ICS Framework to help increase the context surrounding the event and assist in identifying known remediation measures.

Asset & Change Management

After discovering, enriching, and profiling all XIoT assets across the industrial environment, Claroty xDome empowers organizations to streamline asset and change management. Through robust role-based access controls organizations can automate asset management workflows by specific users and groups, saving administration time and reducing maintenance windows for operations personnel.

xDome equips users with the tools needed to manage a broad range of asset needs:

- **Monitor for asset updates**: xDome continuously monitors for vulnerabilities, outdated software, EoL indicators, and other changes requiring updates to help preserve asset availability
- **Streamline SLA compliance**: xDome makes it easy to identify and report on the SLA compliance status of specific assets through availability,location data, and custom-defined attributes
- **Identify asset changes**: Additions to the network, configuration changes, and anomalies are some of the many variables monitors by xDome to support MoC programs
- **Support audit requests**: Advanced reporting capabilities and integrations with version control and backup tools enhance stakeholder communication through xDome.

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.