PLATFORM OVERVIEW

# Claroty xDome

The CPS Protection Platform for the Industrial Cybersecurity Journey

## The CPS Cybersecurity Challenge

The pace of automation and connectivity within manufacturing and other critical infrastructure sectors is accelerating. As organizations continue to embrace digital transformation they face growing complexity in protecting their cyber-physical systems (CPS) amid expanding threat activity by malicious cyber actors. Due to their unique architectures, proprietary protocol usage, and environmental and operational constraints, existing IT solutions fall short when protecting CPS. Additionally, deploying and integrating various point products for CPS increases both cost and complexity. Industrial organizations require a comprehensive platform that delivers critical business outcomes including the reduction of CPS risk, faster time to value, and a lower total cost of ownership — this is where Claroty xDome comes in.

Claroty's xDome allows users to manage, monitor, and control their CPS security solutions within a unified platform–making it easier for organizations to streamline risk management, apply network-based security controls, respond to threats, and manage their overall security posture with a comprehensive view of their CPS environment in real-time. xDome is a modular, SaaS platform supporting the following CPS cybersecurity solutions:

- Asset Discovery & Asset Management
- Exposure Management
- Network Protection
- Threat Detection

## At A Glance

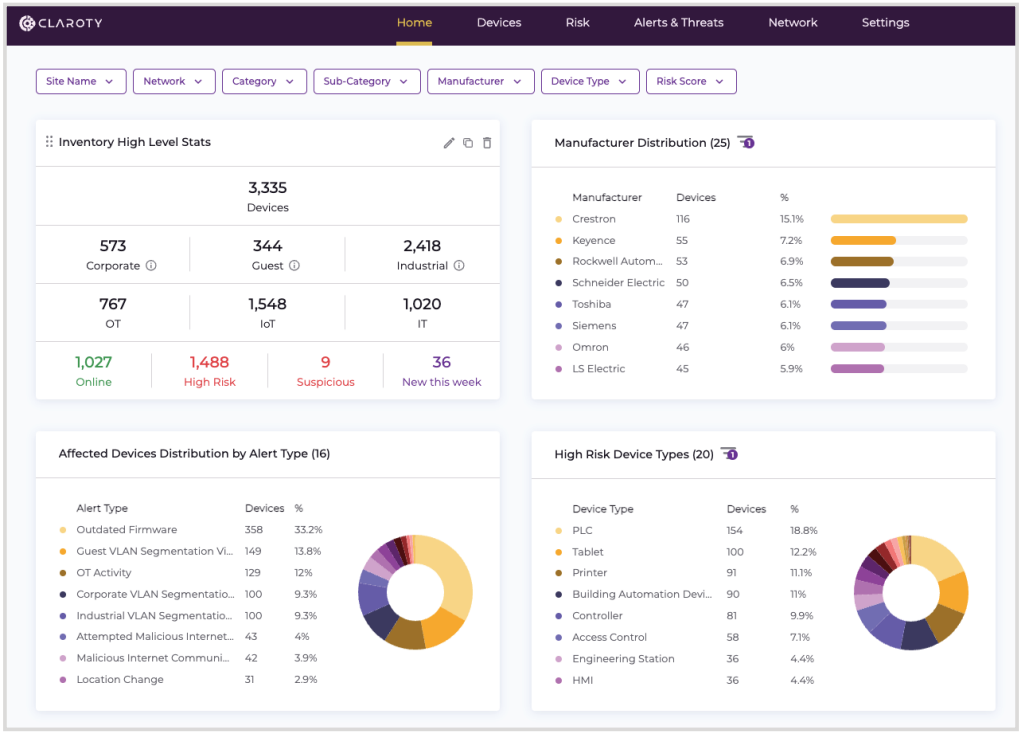
- Eliminate the need to acquire and maintain multiple-point products with a unified, CPS-specific platform
- Realize value more quickly with tailored device discovery that accounts for unique and complex operational needs
- Reduce cyber-risk with actionable insights across exposure management, threat detection, and network protection solutions
- Minimize cost with a flexible deployment that suits your scalability needs, cost considerations, and compliance requirements.
- Designed for scalability, flexibility, and ease-of-use regardless of network size, architecture, or diversity of end users

## Asset Discovery & Asset Management

Effective CPS cybersecurity starts with knowing what needs to be secured, which is why a comprehensive asset inventory is the foundation of the industrial cybersecurity journey. Claroty xDome leverages the broadest and deepest portfolio of CPS protocol coverage to provide a highly detailed, centralized inventory of all assets. Backed by award-winning CPS research and alliances with leading automation vendors, Claroty is the only vendor capable of providing this caliber of visibility through:

- **Breadth of Discovery:** Employ distinct, highly flexible methods that can be combined or used separately to create comprehensive asset profiles
- **Tailored Visibility:** Account for the unique architectural complexities of an organization like geography, environmental factors, and network topology.
- **Identify Asset Changes:** Additions to the network, configuration changes, and anomalies are some of the many variables monitors by xDome to support MoC programs

| Passive Monitorning | Safe Queries | Claroty Edge | Project File Analysis |
|---|---|---|---|
| Continuous monitoring of network traffic to identify asset profiles | Targeted discovery of assets in their native protocol | Speedy, host-based asset profiling through localized queries | Regular ingestion of offline configuration files for asset enrichment |

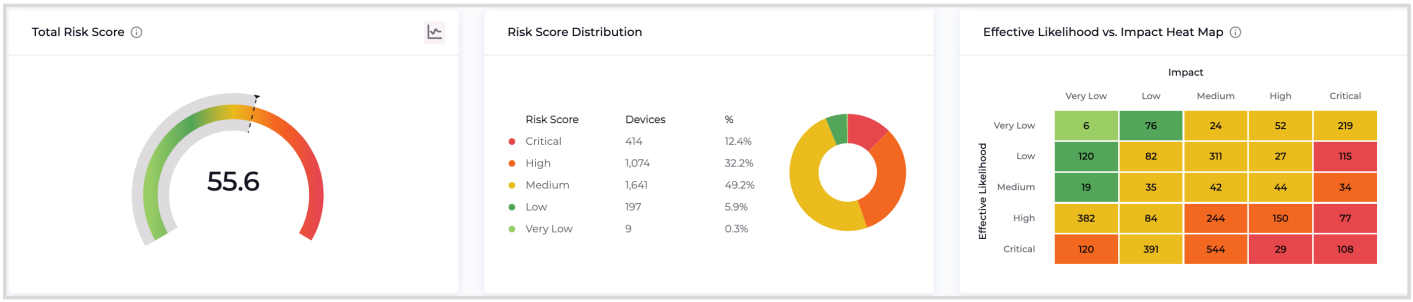



Claroty xDome Home Dashboard

## Exposure Management

Due to the unique nature of and changing risk landscape within industrial environments, organizations must evolve beyond traditional vulnerability management workflows and create a more dynamic and focused approach to managing their overall exposure to risk. Focusing on the operational needs and complex challenges of these environments, Claroty xDome empowers organizations to identify, assess, and prioritize their exposure to risk across their CPS.

- **Discover vulnerabilities & exposures:** Backed by specialized knowledge of CPS, xDome profiles assets to identify their exposure to risk, including vulnerabilities, misconfigurations, weak/default passwords, and more.
- **Remediation prioritization:** Simplify the resource-intensive task of addressing exposures by pinpointing specific attack paths based on their likelihood and impact of exploitation. xDome provides actionable recommendations that enable users to prioritize remediation efforts based on quantified outcomes.
- **Validate and mobilize program efforts:** Granular KPIs and flexible reporting help mobilize workflows across all asset owners such as engineering, security, and facilities management to understand your cyber risk posture, inform decisions, and track progress.




Claroty xDome Exposure Management Dashboard

## Network Protection

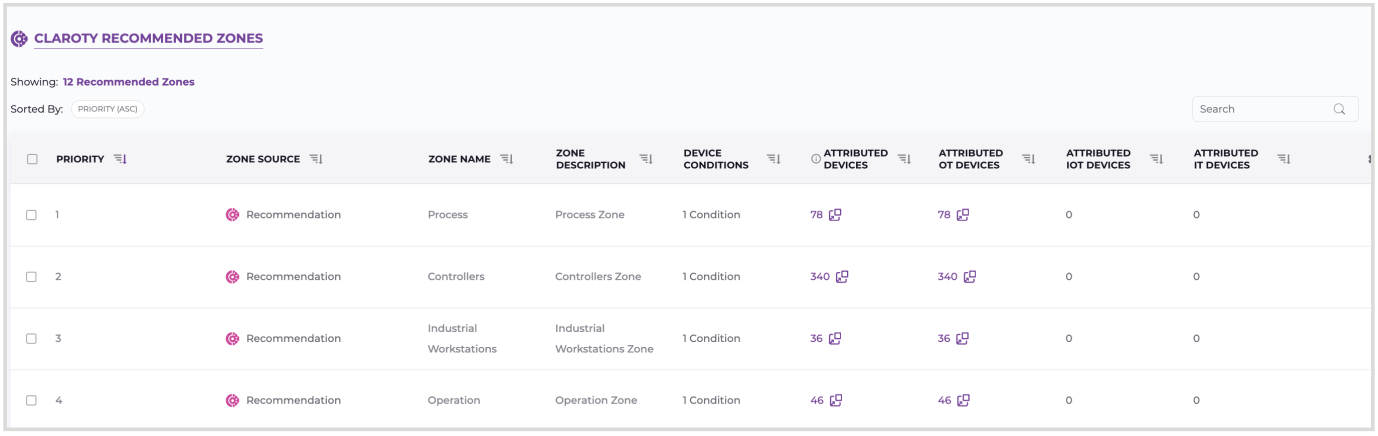
Backed by Claroty's deep domain expertise, xDome leverages its asset visibility to automatically define and recommend network zones for communication policies. This zone-based approach simplifies the process of monitoring, refining, and enforcing communication policies through existing security infrastructure. These dynamic policies 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**

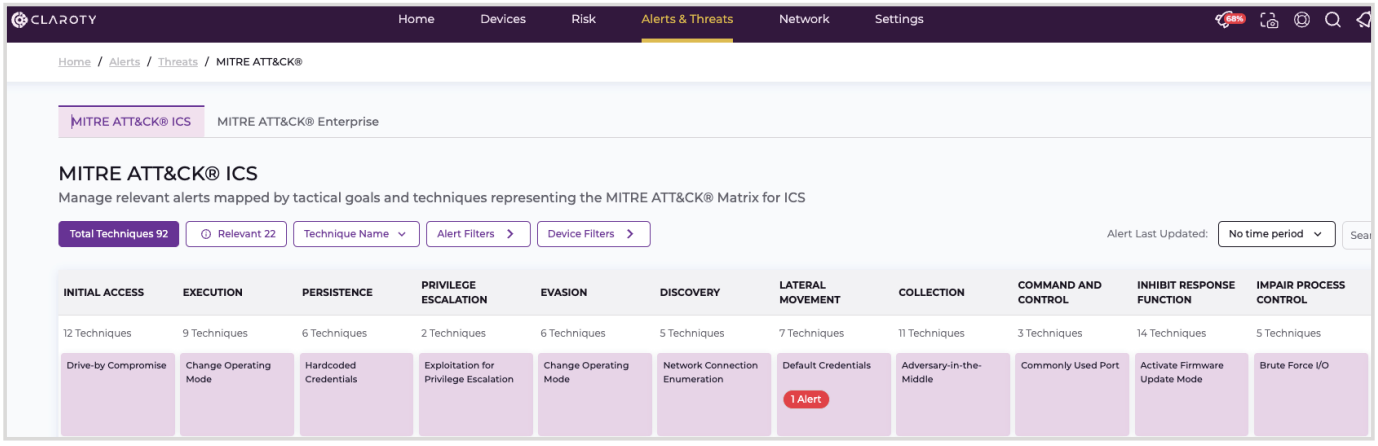



Claroty xDome Recommended Zones View

## 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 CPS 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. Key capabilities include:

- **Detects Known and Unknown Threats:** Characterize legitimate traffic to detect anomalous communications, identify threat signatures, weed out false positives, and alert in real-time to known, unknown, and emerging threats.
- **Domain-specific Threat Intelligence:** Claroty xDome receives automatic detection updates from our award-winning Team82 research team 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.




Claroty xDome MITRE ATT&CK Alert Mapping

## Platform Scalability for the CPS Cybersecurity Journey

Claroty xDome is a comprehensive and modular platform specifically designed to address all CPS cybersecurity use cases. The foundation of the platform, **xDome Essentials**, encompasses a broad array of fundamental capabilities that begin with asset visibility and span exposure management, network protection, and threat detection capabilities. xDome is designed with scalability in mind, offering **advanced modules** as your organization progresses along its CPS security journey.

| | xDome Essentials | xDome Advanced Modules |
|---|---|---|
| **Visibility & Insights** | As the foundation of xDome, this module provides full visibility into your asset inventory with multiple discovery methods, supported by the industry's most comprehensive library of CPS communication protocols. This ensures unparalleled accuracy with detailed asset profiles and in-depth insights. | |
| **Anomaly & Threat Detection** | Robust, customizable threat detection engine based on behavioral baselining and anomaly detection with MITRE ATT&CK for ICS alerts mapping. | Enhanced capabilities that include signature-based detection, custom communication alerts, and OT change alerts to further monitor and alert on unique asset behavior. |
| **Vulnerability & Risk Management** | Comprehensive exposure management and risk-factor identification and assessment capabilities based on proprietary risk profiling that includes exploitability and potential impact, SBOMs, and integrations. | End-to-end exposure management including network-wide recommendation and prioritization features, risk simulation, and vulnerability scanning integrations. |
| **Network Security Management** | Asset communication mapping and visualization that sets the foundation for network segmentation and policy management. Includes integrations with networking infrastructure. | Provides recommended communication policies that can be customized, monitored, optimized, and enforced through Firewall and NAC integrations–helping to build a programmatic approach to network security and implement Zero-Trust principles. |

**About Claroty**

Claroty empowers organizations to secure cyber-physical systems across industrial, healthcare, commercial, and public sector 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, exposure management, network protection, threat detection, and secure 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. To learn more, visit claroty.com.

CLAROTY