SOLUTION OVERVIEW

State and Local Transportation

Sustained Cyber-Physical Resilience for Transportation Systems

State and local transportation agencies depend on highly interconnected systems to keep people moving safely and efficiently. Core operational technologies, including signaling systems, rolling stock, power infrastructure, and building management systems, form the foundation of daily transit operations. As these environments modernize, securing them becomes increasingly critical. Connectivity now spans stations, depots, maintenance yards, and traffic management centers, significantly expanding the attack surface. This increased exposure elevates cyber risk, with the potential for operational disruption, impacts to rider safety, and widespread service delays.

Many of these building and facility systems were not designed with cybersecurity in mind. Agencies often manage aging infrastructure, limited budgets, and competing modernization priorities while navigating TSA Security Directives and state mandates, often without deep cybersecurity expertise. This expanding risk surface across digital and physical facility systems creates an urgent need for visibility, risk reduction, and operational resilience. Addressing these challenges requires close coordination across compliance, facilities engineering, transit safety, and cybersecurity teams.

The Claroty Platform supports this mission by unifying visibility, risk management, and control across the systems that support transit operations and the operational technology (OT) and IoT systems that run stations, buildings, and traffic operations. With this foundation, state and local transportation agencies can meet regulatory requirements, reduce operational disruptions, strengthen their security posture, and maintain public confidence in the safety and reliability of their transit facilities and services.

The Claroty Platform

The Claroty Platform supports federal guidelines and directives for transportation cybersecurity, such as those issued by the Transportation Security Administration (TSA), the Department of Homeland Security (DHS), and the National Institute of Standards and Technology Cybersecurity Framework (NIST CSF 2.0). It enables transportation agencies to monitor, govern, and protect their OT within a unified platform—eliminating the need to purchase and integrate multiple point products. Cloud-based or on-premises deployment models provide the flexibility to scale security programs in alignment with budget, modernization priorities, and compliance requirements.

This dynamic approach to OT cybersecurity is how Claroty helps transportation operators reduce IT/OT convergence-based cyber risk with the **quickest time-to-value (TTV)** and a **lower total cost of ownership (TCO)**—regardless of the scale, complexity, or maturity of the agency's cybersecurity program.

- **Document & Assess:** Use Claroty's platform to produce a defensible baseline risk assessment across IT, OT, and connected assets.

- **Implement & Demonstrate:** Apply segmentation, monitoring, and secure remote access controls to close priority gaps and meet TSA Security Directive requirements.
- **Report & Sustain:** Leverage built-in dashboards to continuously demonstrate progress to regulators, transit boards, and the public.

Asset Inventory

Effective OT cybersecurity for transportation agencies begins with a comprehensive, centralized asset inventory. Claroty enables this by delivering a flexible and scalable approach to asset discovery that avoids costly hardware rollouts and rigid deployment paths.

With both active and passive monitoring options, transportation agencies can rapidly profile assets across stations, administrative buildings, depots, maintenance facilities, parking structures, and traffic management centers while capturing the granular data needed for deeper asset insights.

Claroty's multi-method discovery uncovers and profiles the full spectrum of cyber-physical systems found across transit facilities.

This includes:

- BAS and HVAC equipment
- Elevators and escalators
- Fire and life safety systems
- Access control and video surveillance
- Digital signage and passenger information displays
- Fare collection and kiosk technologies
- Onboard Vehicle Networks and Wayside Signaling

This comprehensive asset inventory gives operators, facilities teams, safety leaders, and risk managers the visibility required to meet TSA and NIST-aligned requirements, reduce blind spots, and strengthen resilience against disruption. By providing transportation agencies with a trusted foundation for compliance, continuity, and security, Claroty helps ensure the safe and reliable operation of essential transit facilities and services.

Passive Monitorning	**Safe Queries**	**Claroty Edge**	**Project File Analysis**	**Integrations**
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	Enriching visibility with your existing technology investments

Claroty asset discovery methods

Exposure Management

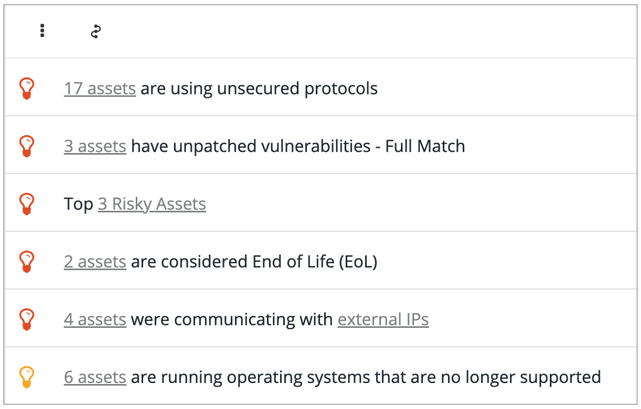
Given the unique complexity and ever-shifting risk landscape of OT environments, transportation agencies cannot rely on traditional, IT-centric vulnerability management workflows. These approaches often overlook the operational realities of transportation and traffic management infrastructure—where downtime can result in safety incidents, cascading delays, and significant economic impact.

What's required is a more dynamic, operationally focused approach that continuously identifies, contextualizes, and prioritizes risks based on their impact to passenger safety, service continuity, and regulatory requirements.

The Claroty Platform delivers exactly this: enabling transportation agencies to map their true OT risk posture, assess vulnerabilities in the context of operational demands, and prioritize mitigation efforts where they matter most. This empowers leaders to make informed decisions that reduce exposure without disrupting essential services, strengthening resilience, safety, and public trust in the reliability of transit systems.

OT Risk Identification: Backed by specialized knowledge of OT, the platform profiles assets to identify their exposure to risk, including vulnerabilities, misconfigurations, weak/default passwords, and more. Additionally, software bill of materials (SBOM) data can be leveraged to provide additional context on the software components within assets, helping security teams assess potential risks tied to third-party or open-source dependencies.

Impact-Centric Risk Assessment: Claroty's customizable risk configurations prioritize exposure remediation based on each asset's business impact, enabling security teams to reduce risk in the most impactful areas and focus efforts on the most critical operational processes.



17 assets are using unsecured protocols

3 assets have unpatched vulnerabilities - Full Match

Top 3 Risky Assets

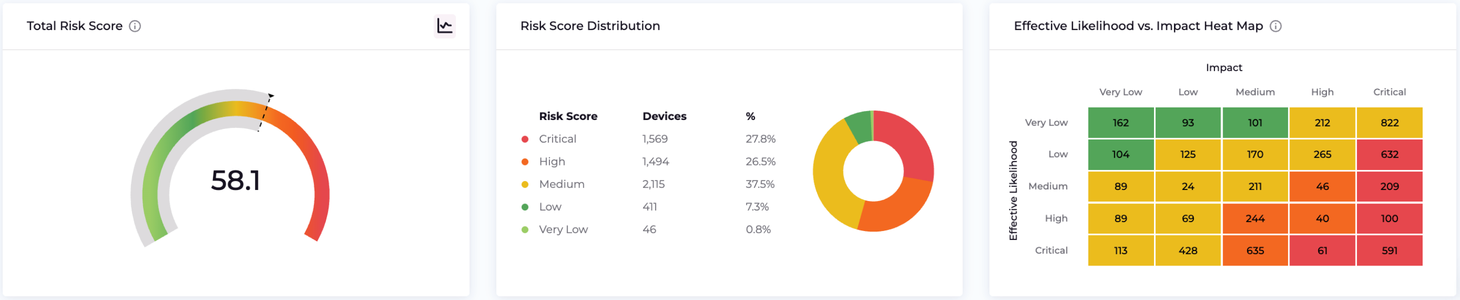
2 assets are considered End of Life (EoL)

4 assets were communicating with external IPs

6 assets are running operating systems that are no longer supported

Claroty CTD Risk Insights

Remediation Prioritization: The Claroty Platform provides actionable recommendations that enable users to prioritize remediation efforts based on quantified outcomes. This simplifies the resource-intensive task of addressing exposures by pinpointing specific attack paths based on their likelihood and impact of exploitation.



Risk Score Distribution

Risk Score	Devices	%
● Critical	1,569	27.8%
● High	1,494	26.5%
● Medium	2,115	37.5%
● Low	411	7.3%
● Very Low	46	0.8%

Effective Likelihood vs. Impact Heat Map

Effective Likelihood	Impact: Very Low	Low	Medium	High	Critical
Very Low	162	93	101	212	822
Low	104	125	170	265	632
Medium	89	24	211	46	209
High	89	69	244	40	100
Critical	113	428	635	61	591

Claroty xDome Exposure Management Dashboard

Network Protection

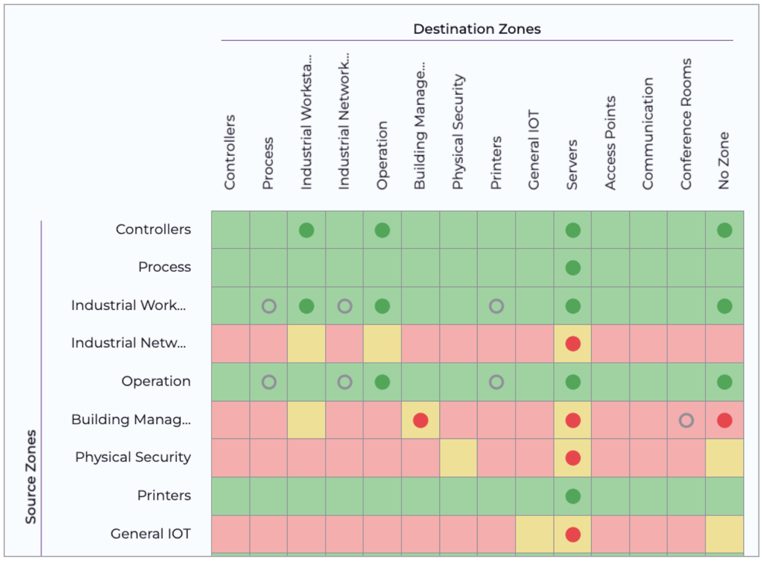
In today’s complex OT environments, transportation agencies need more than outdated, one-size-fits-all segmentation tools. They require a nuanced, risk-informed approach that creates clear separation between high-risk networks, such as passenger Wi-Fi, and safety-critical control systems, ensuring operational continuity and rider safety

Federal guidance, including TSA Security Directives for surface transportation and NIST CSF 2.0, reinforces the necessity of information protection, intrusion detection, operational continuity, and structured risk assessment as foundational components of transportation cybersecurity programs.

Claroty rises to meet this requirement, offering targeted capabilities that extend and operationalize these standards with precision and reliability:

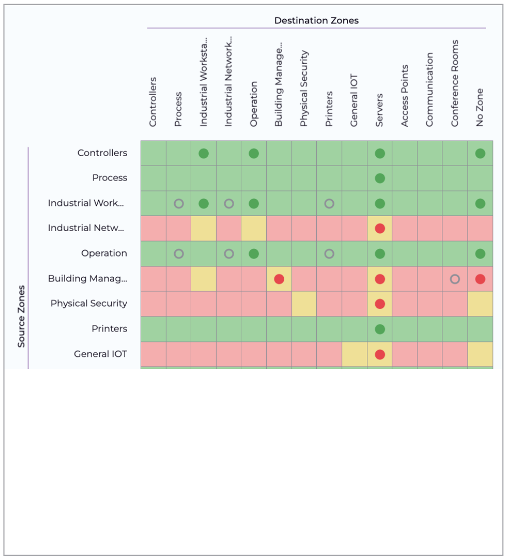
- **Communication Mapping:** Leveraging deep OT domain expertise, Claroty intelligently recommends zoning strategies and identifies deviations from expected communication patterns—even within complex environments like signaling systems, control centers, or traffic management networks.
- **Policy Creation & Simulation:** Agencies can harness automated policy generation and test segmentation strategies virtually, ensuring any changes are both operationally safe and practically enforceable.
- **Alerting & Enforcement:** With real-time anomaly detection and seamless integration into existing enforcement tools—whether firewalls, switches, or NAC—Claroty ensures policy validation and rapid threat response are automatic, reducing risk without adding operational complexity.

By grounding network segmentation in sector-specific best practices and offering flexible, tool-agnostic deployment options, Claroty empowers transportation agencies to enhance visibility, reduce operational risk, and maintain the continuity and safety of critical transit services for the communities they serve.



	Destination Zones													
Source Zones	Controllers	Process	Industrial Worksta...	Industrial Network...	Operation	Building Manage...	Physical Security	Printers	General IOT	Servers	Access Points	Communication	Conference Rooms	No Zone
Controllers	🟩	🟩	🟩 🟢	🟩	🟩 🟢	🟩	🟩	🟩	🟩	🟩 🟢	🟩	🟩	🟩	🟩 🟢
Process	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩 🟢	🟩	🟩	🟩	🟩
Industrial Work...	🟩	🟩 ○	🟩 🟢	🟩 ○	🟩 🟢	🟩	🟩	🟩 ○	🟩	🟩 🟢	🟩	🟩	🟩	🟩 🟢
Industrial Netw...	🟥	🟥	🟨	🟥	🟨	🟥	🟥	🟥	🟥	🟨 🔴	🟥	🟥	🟥	🟥
Operation	🟩	🟩 ○	🟩	🟩 ○	🟩 🟢	🟩	🟩	🟩 ○	🟩	🟩 🟢	🟩	🟩	🟩	🟩 🟢
Building Manag...	🟥	🟥	🟨	🟥	🟥	🟨 🔴	🟥	🟥	🟥	🟨 🔴	🟥	🟥	🟥 ○	🟥 🔴
Physical Security	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟥	🟥	🟨 🔴	🟥	🟥	🟥	🟨
Printers	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩 🟢	🟩	🟩	🟩	🟩
General IOT	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨 🔴	🟥	🟥	🟥	🟨

Claroty xDome Network Zones Matrix



	Destination Zones													
Source Zones	Controllers	Process	Industrial Worksta...	Industrial Network...	Operation	Building Manage...	Physical Security	Printers	General IOT	Servers	Access Points	Communication	Conference Rooms	No Zone
Controllers	🟩	🟩	🟩 🟢	🟩	🟩 🟢	🟩	🟩	🟩	🟩	🟩 🟢	🟩	🟩	🟩	🟩 🟢
Process	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩 🟢	🟩	🟩	🟩	🟩
Industrial Work...	🟩	🟩 ○	🟩 🟢	🟩 ○	🟩 🟢	🟩	🟩	🟩 ○	🟩	🟩 🟢	🟩	🟩	🟩	🟩 🟢
Industrial Netw...	🟥	🟥	🟨	🟥	🟨	🟥	🟥	🟥	🟥	🟨 🔴	🟥	🟥	🟥	🟥
Operation	🟩	🟩 ○	🟩	🟩 ○	🟩 🟢	🟩	🟩	🟩 ○	🟩	🟩 🟢	🟩	🟩	🟩	🟩 🟢
Building Manag...	🟥	🟥	🟨	🟥	🟥	🟨 🔴	🟥	🟥	🟥	🟨 🔴	🟥	🟥	🟥 ○	🟥 🔴
Physical Security	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟥	🟥	🟨 🔴	🟥	🟥	🟥	🟨
Printers	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩	🟩 🟢	🟩	🟩	🟩	🟩
General IOT	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟥	🟨	🟨 🔴	🟥	🟥	🟥	🟨

Claroty CTD Virtual Zone Mapping

Secure Access

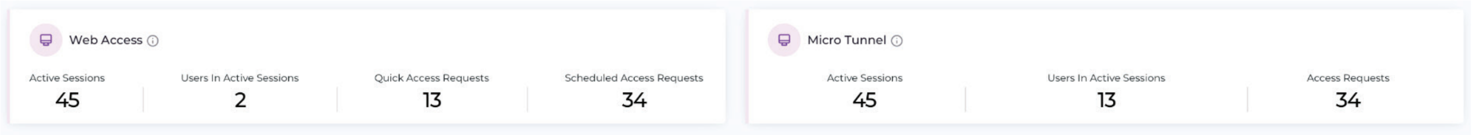
Transportation agencies have increasingly been targeted through insecure remote access and weak access control governance—exposing a critical vulnerability that attackers exploit to bypass defenses and disrupt essential services.

Legacy VPNs, shared credentials, jump boxes, and ad hoc third-party connections leave operators exposed, creating blind spots in environments where downtime can trigger service disruptions, safety risks, and cascading delays across entire networks. To close this gap, agencies need a solution designed specifically for OT—one that balances operational continuity with uncompromising control.

Claroty xDome Secure Access delivers exactly that:

- **Enhance Productivity:** Authorized staff and contractors connect quickly and securely to the assets they need, with streamlined workflows that keep signaling systems, traffic control, and passenger services uninterrupted.
- **Minimize Risk:** Request management, granular access controls, multi-factor authentication, full audit trails, and session recording eliminate the blind spots that have historically enabled breaches in transit and traffic environments.
- **Reduce Administrative Complexity:** Centralized management replaces scattered VPNs and manual approvals, simplifying provisioning, monitoring, and auditing of all OT remote sessions.

With xDome Secure Access, utilities can finally shut the door on one of their most persistent vulnerabilities, ensuring resilient operations and protecting the trust of the communities they serve. With xDome Secure Access, transportation agencies can finally shut the door on one of their most persistent vulnerabilities hereby ensuring resilient operations, protecting passenger safety, and preserving the public's trust in the continuity of critical transit services.



Web Access

Active Sessions	Users In Active Sessions	Quick Access Requests	Scheduled Access Requests
45	2	13	34

Micro Tunnel

Active Sessions	Users In Active Sessions	Access Requests
45	13	34

Claroty xDome Secure Access Admin View

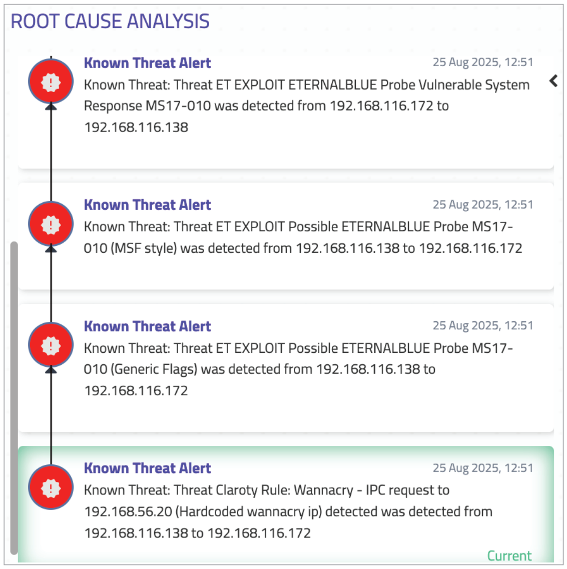
Threat Detection

Recognizing the rising frequency and impact of threats targeting critical infrastructure environments, the Claroty Platform employs a resilient detection model to continuously monitor for operational anomalies that may indicate unauthorized changes or emerging threats within safety-critical environments. The platform profiles OT assets and their communication patterns, enabling automated detection, prioritization, and response to operational anomalies that could impact system integrity, availability, and safety.

Key capabilities include:

- **Industry-Specific Detection:** The Claroty Platform identifies both unknown operational anomalies through behavioral baselining and deep packet inspection (DPI), and known threats through integrated threat intelligence and IOCs, ensuring broad visibility into malicious activity. Tools like **CTD Root Cause Analysis, xDome MITRE ATT&CK™ alert mapping** provide organizations with clear, actionable visibility into threats across OT environments.

- **Curated Threat Intelligence:** Continuous updates from Claroty's Team82 research team deliver the latest signatures, vulnerabilities, and indicators, contextualized to each OT environment so teams can focus on the threats that matter most.
- **Threat Response:** Consolidated "attack stories," MITRE ATT&CK™ for ICS mapping, and seamless integrations with SOC tools enable faster investigation, triage, and remediation across IT and OT systems.



ROOT CAUSE ANALYSIS

Known Threat Alert 25 Aug 2025, 12:51
Known Threat: Threat ET EXPLOIT ETERNALBLUE Probe Vulnerable System Response MS17-010 was detected from 192.168.116.172 to 192.168.116.138

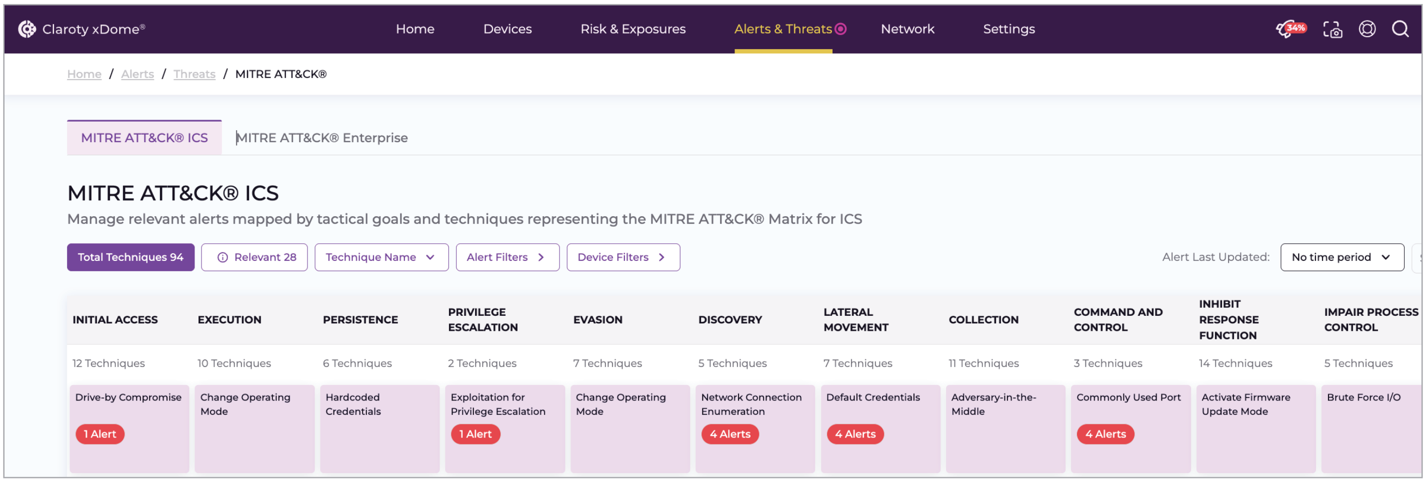
Known Threat Alert 25 Aug 2025, 12:51
Known Threat: Threat ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (MSF style) was detected from 192.168.116.138 to 192.168.116.172

Known Threat Alert 25 Aug 2025, 12:51
Known Threat: Threat ET EXPLOIT Possible ETERNALBLUE Probe MS17-010 (Generic Flags) was detected from 192.168.116.138 to 192.168.116.172

Known Threat Alert 25 Aug 2025, 12:51
Known Threat: Threat Claroty Rule: Wannacry - IPC request to 192.168.56.20 (Hardcoded wannacry ip) detected was detected from 192.168.116.138 to 192.168.116.172

Current

Claroty CTD Threat Root Cause Analysis



MITRE ATT&CK® ICS

Manage relevant alerts mapped by tactical goals and techniques representing the MITRE ATT&CK® Matrix for ICS

Total Techniques 94 | Relevant 28 | Technique Name | Alert Filters | Device Filters | Alert Last Updated: No time period

INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL
12 Techniques	10 Techniques	6 Techniques	2 Techniques	7 Techniques	5 Techniques	7 Techniques	11 Techniques	3 Techniques	14 Techniques	5 Techniques
Drive-by Compromise 1 Alert	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation 1 Alert	Change Operating Mode	Network Connection Enumeration 4 Alerts	Default Credentials 4 Alerts	Adversary-in-the-Middle	Commonly Used Port 4 Alerts	Activate Firmware Update Mode	Brute Force I/O

Claroty xDome MITRE ATT&CK Alert Mapping

Enabling Safer, More Reliable Transportation

Claroty empowers transportation organizations to protect the cyber-physical systems that underpin safe, reliable movement of people and goods. By enabling teams to understand risk in operational context, prioritize what matters most, and take action without disrupting service, the Claroty platform supports safer operations, reduced downtime, and resilient modernization across complex, distributed transportation infrastructure.

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. 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