PLATFORM OVERVIEW

Claroty xDome

Protecting cyber-physical systems across the modern healthcare network

Protect healthcare organizations from cyber and operational risks to ensure safe and efficient delivery of connected care.

The Healthcare Cybersecurity Challenge

The modern healthcare network has dramatically reshaped patient care delivery. Health systems' infrastructure, stakeholders, and processes are highly dependent on the wide range of network-connected cyber-physical systems (CPS) that span everything from the medical devices, building management systems, and IoT devices that are involved in supporting continuous care delivery. Despite its clear business benefits, growing connectivity in these critical environments creates new security blindspots and an expanding attack surface that pose risks to the operational availability, integrity, and safety of healthcare environments.

Claroty xDome is the industry's leading healthcare cyber-physical systems protection platform–enabling healthcare organizations to safely deliver connected care while enhancing efficiencies across the clinical environment. Claroty xDome spans the entire healthcare cybersecurity journey regardless of the scale or maturity of your environment through:

- Device Discovery
- Exposure Management
- Network Protection
- Threat Detection
- Operational Efficiency

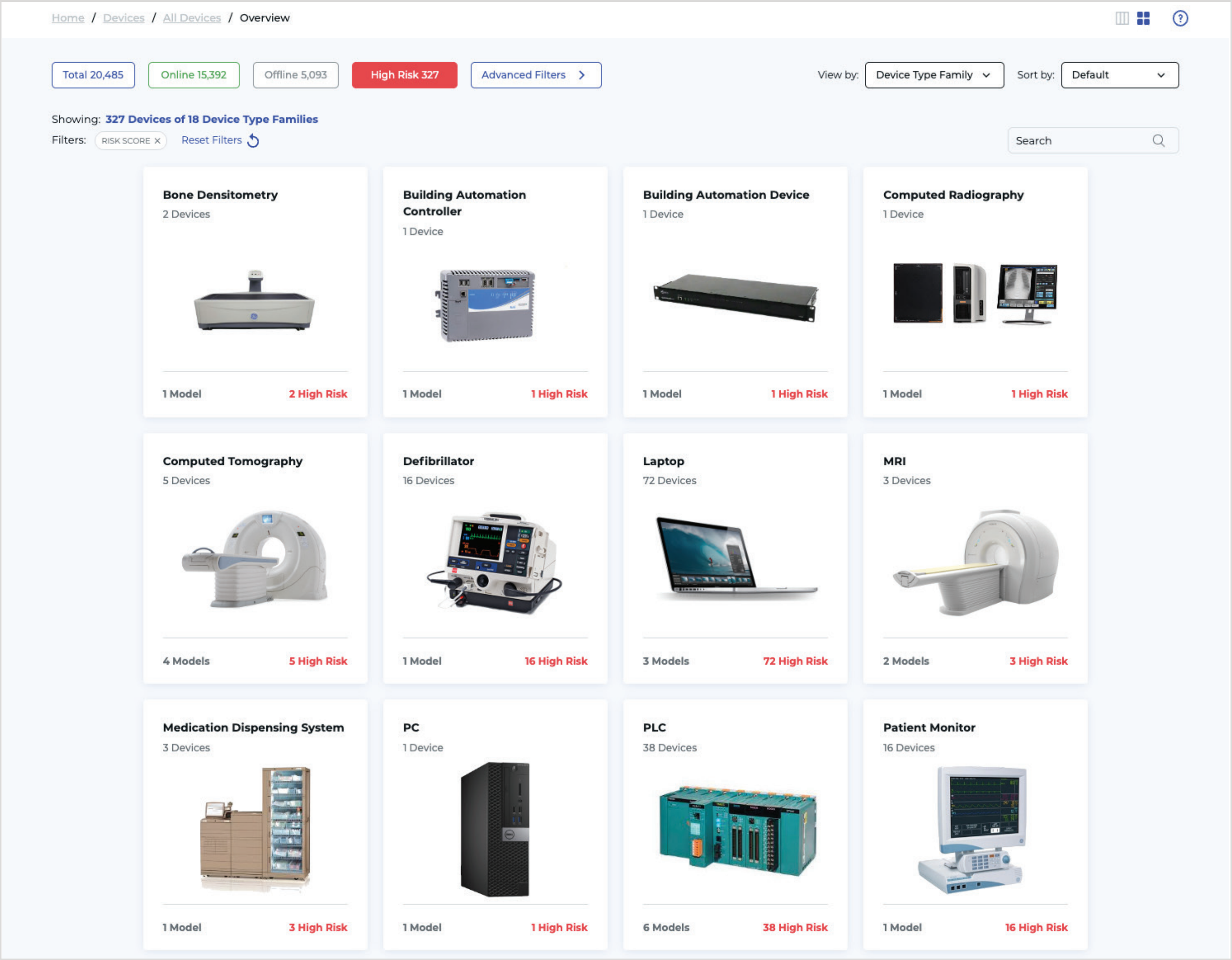
At A Glance

- Eliminate the need to acquire and maintain multiple-point products with a unified, healthcare-specific platform
- Realize value more quickly with tailored device discovery that accounts for unique and complex clinical workflows
- Reduce cyber-risk with actionable insights across exposure management, threat detection, and network protection solutions
- Minimize costs with a flexible deployment that suits your scalability needs, cost considerations, and compliance requirements

Device Discovery

Effective cybersecurity starts with knowing what needs to be secured, which is why a comprehensive device inventory is the foundation of the healthcare cybersecurity journey. The Claroty xDome leverages the broadest and deepest portfolio of protocol coverage, along with Claroty Team82's, our in-house research team's domain-specific research into CPS specific protocols, to provide a highly detailed, centralized inventory of assets. Claroty is the only vendor capable of providing this caliber of visibility through multiple distinct, highly flexible data collection methods that can be combined or used separately based on the unique needs of both clinical and non-clinical environments:

- **Passive monitoring:** Continuous monitoring of network traffic to identify and enrich device 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 CMMS and device management tools to further enrich device profiles



Home / Devices / All Devices / Overview

Total 20,485 | Online 15,392 | Offline 5,093 | High Risk 327 | Advanced Filters

View by: Device Type Family

Sort by: Default

Showing: 327 Devices of 18 Device Type Families

Filters: RISK SCORE × Reset Filters

Search

Bone Densitometry
2 Devices
1 Model 2 High Risk

Building Automation Controller
1 Device
1 Model 1 High Risk

Building Automation Device
1 Device
1 Model 1 High Risk

Computed Radiography
1 Device
1 Model 1 High Risk

Computed Tomography
5 Devices
4 Models 5 High Risk

Defibrillator
16 Devices
1 Model 16 High Risk

Laptop
72 Devices
3 Models 72 High Risk

MRI
3 Devices
2 Models 3 High Risk

Medication Dispensing System
3 Device
1 Model 3 High Risk

PC
1 Device
1 Model 1 High Risk

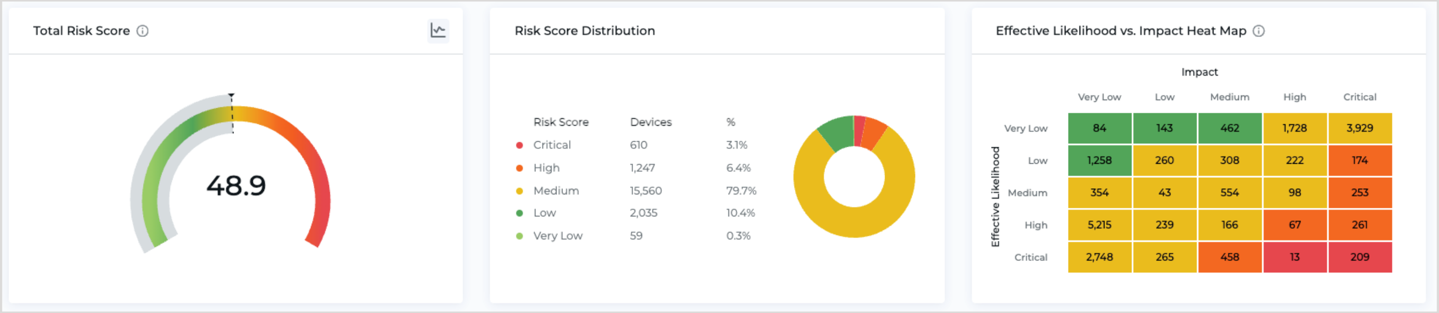
PLC
38 Devices
6 Models 38 High Risk

Patient Monitor
16 Devices
1 Model 16 High Risk

Exposure Management

Due to the nature of clinical workflows, healthcare networks must evolve beyond traditional vulnerability management workflows and create a more dynamic and focused approach to managing their overall exposure to risk. Claroty xDome takes into account the device complexities, unique governance, and operational outcomes of healthcare environments to safely address vulnerabilities and exposures without impacting patient care.

- **Discover vulnerabilities & exposures:** Backed by specialized knowledge of the healthcare environment, xDome identifies exposures like vulnerabilities, misconfigurations, weak/default passwords, and more– leveraging manufacturer insights like SBOMs or MDS2 files to obtain more granular visibility into devices.
- **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 clinical engineering, security, and facilities management to understand your cyber risk posture, inform decisions, and track progress.


Total Risk Score

48.9

Risk Score Distribution

	Risk Score	Devices	%
●	Critical	610	3.1%
●	High	1,247	6.4%
●	Medium	15,560	79.7%
●	Low	2,035	10.4%
●	Very Low	59	0.3%

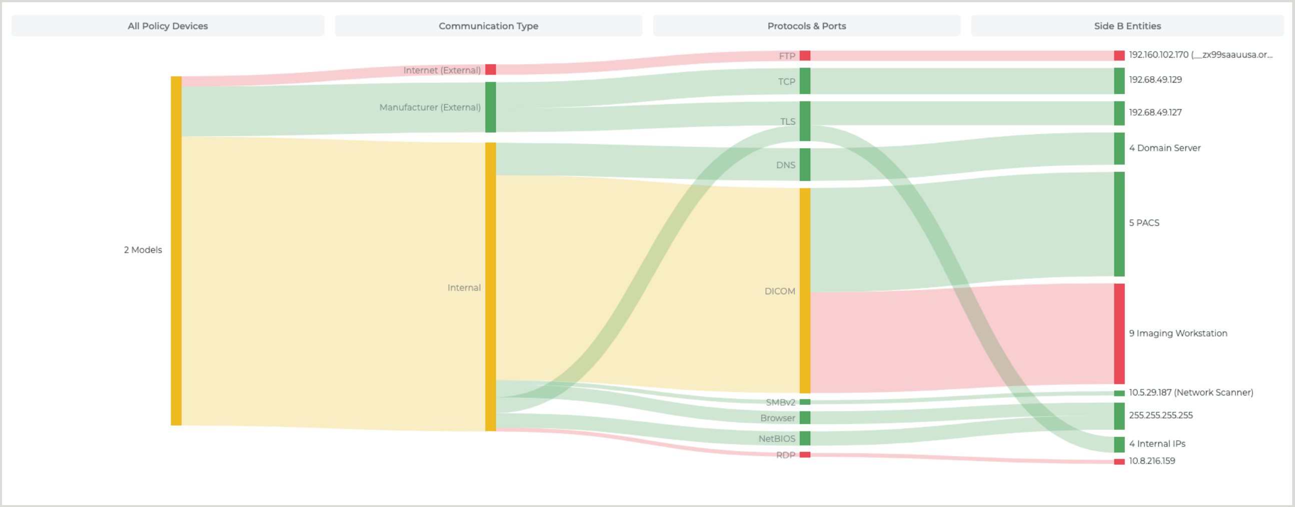
Effective Likelihood vs. Impact Heat Map

Effective Likelihood	Impact: Very Low	Low	Medium	High	Critical
Very Low	84	143	462	1,728	3,929
Low	1,258	260	308	222	174
Medium	354	43	554	98	253
High	5,215	239	166	67	261
Critical	2,748	265	458	13	209

Network Protection

Due to the specialized nature of device communications and the need to move freely through the healthcare setting, implementing proper network protection through communication policy controls can be both cost-prohibitive and difficult. An effective network protection strategy requires visibility into device communications in order to properly segment devices and enforce policies. Fueled by specialized expertise in healthcare devices and clinical workflows, the Claroty xDome helps protect clinical environments through advanced communication controls. Highlights include:

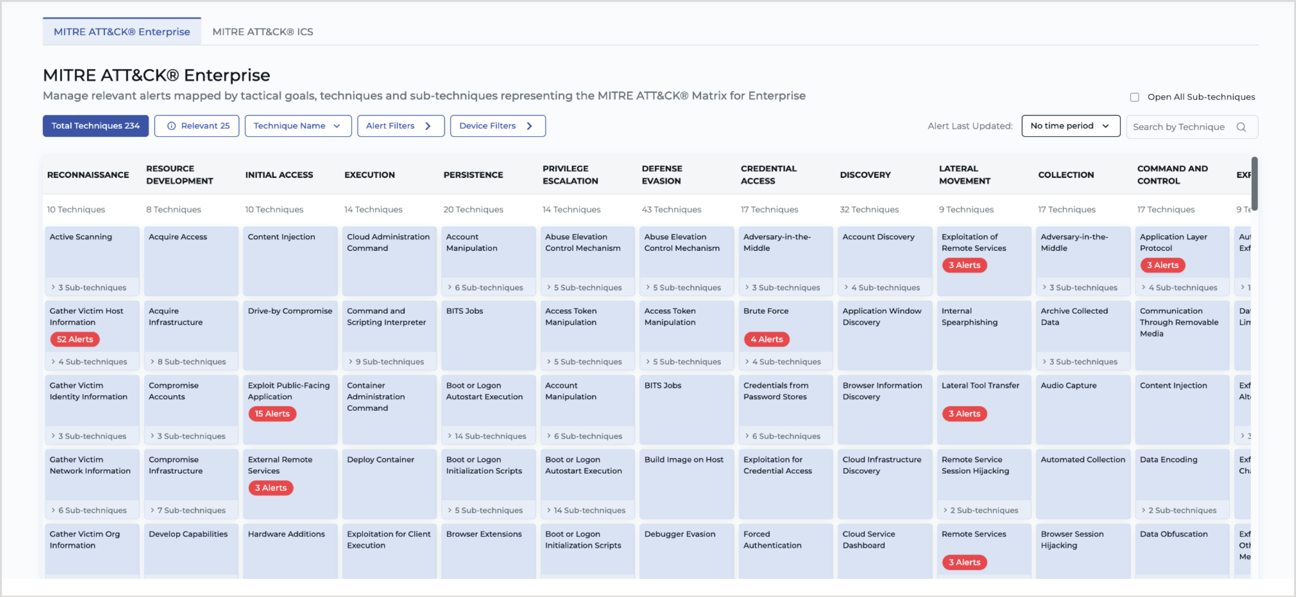
- **Network communication mapping:** Claroty xDome profiles all device communication on the network in order to understand how and with what each device communicates.
- **Jumpstarting network segmentation:** The solution automatically creates, and enables the testing of, recommended communication policies based on network context and industry best practices
- **Policy enforcement:** Secure communication within a clinical context by tailoring recommended communication policies and seamlessly integrating with existing network tools like NACs and Firewalls.



Threat Detection

No HDO is immune to threats, so effective detection and response is critical. The Claroty xDome's unified insights and alert system provides automated methods to monitor, prioritize, and respond to affected devices through an unmatched depth of device visibility and remediation workflow capabilities. Our cyber-resilient detection model gives you the ability to monitor, prioritize, and respond to alerts. Highlights include:

- **Known threat identification:** Threat, compliance, and operational alerting to detect known threats such as ransomware, malware, and signature based detection methods.
- **Unknown threat identification:** Threat, compliance, and operational alerting to detect unknown threats such as anomalous behavior, zero-day attacks, and significant device status changes
- **Custom communication alerts:** Create alerts based on specific device communication methods like type, protocol, or category for greater visibility and a more contextual threat detection strategy.
- **Broad integration opportunities:** Integrate with existing SIEM and EDR tools to extend existing SOC capabilities to your healthcare environment



MITRE ATT&CK® Enterprise

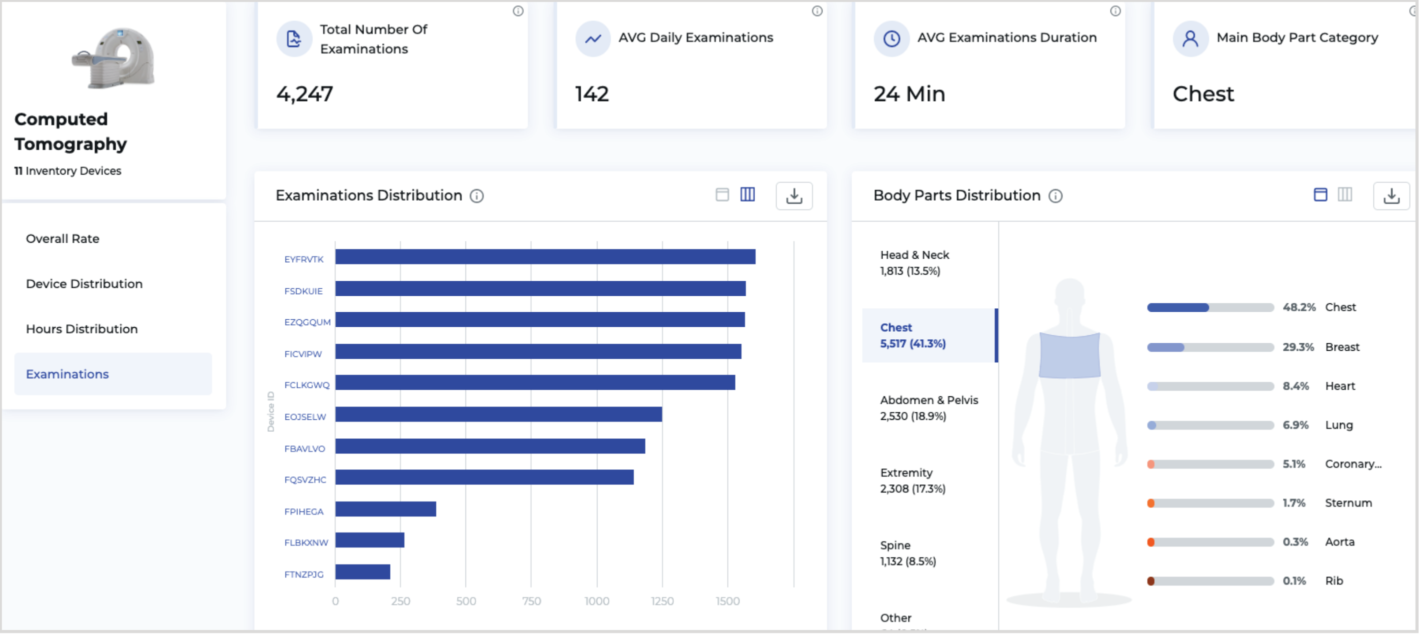
Manage relevant alerts mapped by tactical goals, techniques and sub-techniques representing the MITRE ATT&CK® Matrix for Enterprise

RECONNAISSANCE	RESOURCE DEVELOPMENT	INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	DEFENSE EVASION	CREDENTIAL ACCESS	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	EXF
10 Techniques	8 Techniques	10 Techniques	14 Techniques	20 Techniques	14 Techniques	43 Techniques	17 Techniques	32 Techniques	9 Techniques	17 Techniques	17 Techniques	9 Te
Active Scanning › 3 Sub-techniques	Acquire Access	Content Injection	Cloud Administration Command	Account Manipulation › 6 Sub-techniques	Abuse Elevation Control Mechanism › 5 Sub-techniques	Abuse Elevation Control Mechanism › 5 Sub-techniques	Adversary-in-the-Middle › 3 Sub-techniques	Account Discovery › 4 Sub-techniques	Exploitation of Remote Services 3 Alerts	Adversary-in-the-Middle › 3 Sub-techniques	Application Layer Protocol 3 Alerts › 4 Sub-techniques	Au Exf › 1
Gather Victim Host Information 52 Alerts › 4 Sub-techniques	Acquire Infrastructure › 8 Sub-techniques	Drive-by Compromise	Command and Scripting Interpreter › 9 Sub-techniques	BITS Jobs	Access Token Manipulation › 5 Sub-techniques	Access Token Manipulation › 5 Sub-techniques	Brute Force 4 Alerts › 4 Sub-techniques	Application Window Discovery	Internal Spearphishing	Archive Collected Data › 3 Sub-techniques	Communication Through Removable Media	Da Lin
Gather Victim Identity Information › 3 Sub-techniques	Compromise Accounts › 3 Sub-techniques	Exploit Public-Facing Application 15 Alerts	Container Administration Command	Boot or Logon Autostart Execution › 14 Sub-techniques	Account Manipulation › 6 Sub-techniques	BITS Jobs	Credentials from Password Stores › 6 Sub-techniques	Browser Information Discovery	Lateral Tool Transfer 3 Alerts	Audio Capture	Content Injection	Exf Alt › 3
Gather Victim Network Information › 6 Sub-techniques	Compromise Infrastructure › 7 Sub-techniques	External Remote Services 3 Alerts	Deploy Container	Boot or Logon Initialization Scripts › 5 Sub-techniques	Boot or Logon Autostart Execution › 14 Sub-techniques	Build Image on Host	Exploitation for Credential Access	Cloud Infrastructure Discovery	Remote Service Session Hijacking › 2 Sub-techniques	Automated Collection	Data Encoding › 2 Sub-techniques	Exf Ch
Gather Victim Org Information	Develop Capabilities	Hardware Additions	Exploitation for Client Execution	Browser Extensions	Boot or Logon Initialization Scripts	Debugger Evasion	Forced Authentication	Cloud Service Dashboard	Remote Services 3 Alerts	Browser Session Hijacking	Data Obfuscation	Exf Ot Me

Operational Efficiency

Healthcare environments make up a complex web of devices, workflows, and personnel–all working together to deliver high-quality patient care in a safe and efficient manner. Claroty xDome is uniquely suited to help HDOs optimize clinical workflows, utilization, and device lifecycles in order to decrease costs, increase revenue, and mitigate risk. By discovering these insights, the Medigate Platform enables:

- **Track and maintain device utilization and lifecycle:** Understand overall device utilization, location, and life cycles of devices with customized report and dashboard creation directly in Claroty xDome
- **Optimize device procurement:** Industry benchmarks for inventory and utilization help to right-size fleets of medical devices, load-balance across sites, or renegotiate lease and maintenance agreements.
- **Improve device efficiency:** Automate time intensive tasks such as CMMS auditing and device recovery so that healthcare delivery teams can focus on higher value objectives.
- **Extend device usage:** Identify, assess, and create compensating controls around end-of-life or other high risk devices that are still able to perform their clinical function.



Computed Tomography
11 Inventory Devices

Total Number Of Examinations: 4,247
AVG Daily Examinations: 142
AVG Examinations Duration: 24 Min
Main Body Part Category: Chest

The modular platform for your healthcare cybersecurity journey

As a modular solution, Claroty xDome is suited for organizations at any stage in their healthcare cybersecurity journey, regardless of their scale, staffing, or program maturity. The solution consists of platform essentials, offering foundational capabilities across all core areas mentioned above, as well as advanced modules that provide increased value and enhanced programmatic capabilities.

	xDome Essentials	xDome Advanced Modules
Visibility & Insights	As the foundation of Claroty xDome, this functionality provides complete visibility into your device inventory with multiple, distinct discovery methods–backed by the broadest and deepest library of medical device and IoT protocols in the industry. The result is unparalleled accuracy with granular device profiles including information like serial numbers, firmware versions, OS, nested devices, and more.	
Anomaly & Threat Detection	Robust, customizable threat detection engine based on behavioral baselining and anomaly detection with MITRE ATT&CK for Enterprise alerts mapping.	Enhanced threat detection capabilities that include signature-based detection for known threats, custom communication alerts to further monitor and alert on unique device behavior, and additional uses for the MITRE ATT&CK for Enterprise matrix.
Vulnerability & Risk Management	Comprehensive vulnerability & risk identification and assessment capabilities based on multiple sources of intelligence, proprietary risk profiling, individual MDS2 forms, and endpoint management integrations.	End-to-end vulnerability & risk management including network-wide recommendation and prioritization features, risk simulation, complete MDS^2 directory, and vulnerability scanning integrations. This module enables HDOs to take more impactful and efficient risk reduction measures at the site-level.
Network Security Management	Device communication mapping and visualization through a communication matrix and world map view of external connections, setting the foundation for network segmentation and integrations with networking infrastructure.	Provides recommended communication policies that can be customized, monitored, optimized, and enforced through Firewall and NAC integrations. This module is essential for environments looking for a programmatic approach to network security who wish to adhere to Clinical Zero-Trust practices.
Clinical Device Efficiency	Operational intelligence on devices including utilization activity, device location and mapping through integrations, and end-of-life information.	This module provides users with the ability to monitor, benchmark, and optimize device usage across their healthcare network in order to maximize operational value and achieve increased ROI.

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

ValuTrack
TECHNOLOGY SOLUTIONS

ValuTrack Corporation
Email: sales@valutrack.com
Phone: 866-825-8382