SOLUTION OVERVIEW

THE MEDIGATE PLATFORM

Protecting cyber-physical systems across the modern healthcare network

The Healthcare Cybersecurity Challenge

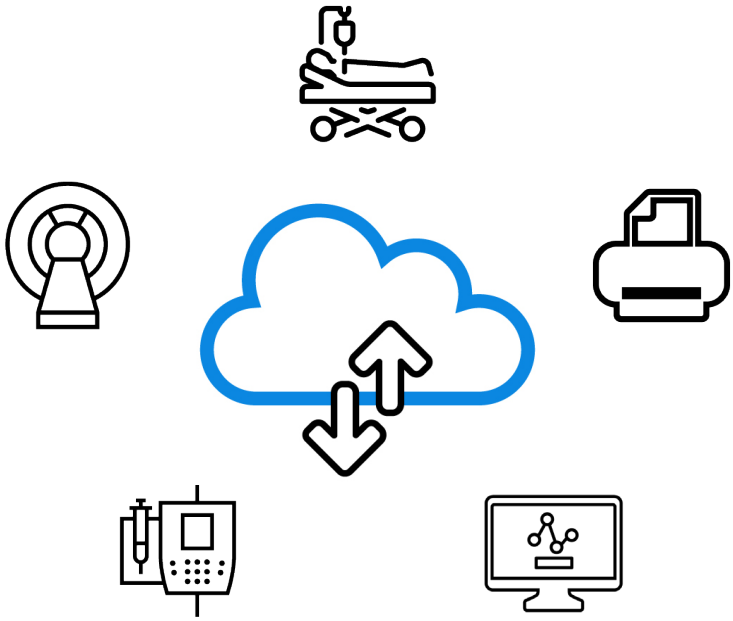
The modern healthcare network has dramatically reshaped patient care delivery. Health systems' infrastructure, staff, and workflows are highly dependent on a wide range of connected devices that make up the Extended Internet of Things (XIoT). This vast cyber-physical web spans everything from medical devices, building management systems such as HVAC systems, and even IoT devices such as printers. Despite its clear business benefits, this growing connectivity is creating new security blindspots and attack surfaces that pose risk to the operational availability, integrity, and safety of healthcare environments.

The Medigate Platform 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. The Medigate Platform spans the entire healthcare cybersecurity journey regardless of the scale or maturity of your environment through:

- Device Discovery
- Vulnerability & Risk Management
- Network Protection
- Threat Detection
- Device & Lifecycle Management
- Operational Intelligence

Medigate Benefits At A Glance

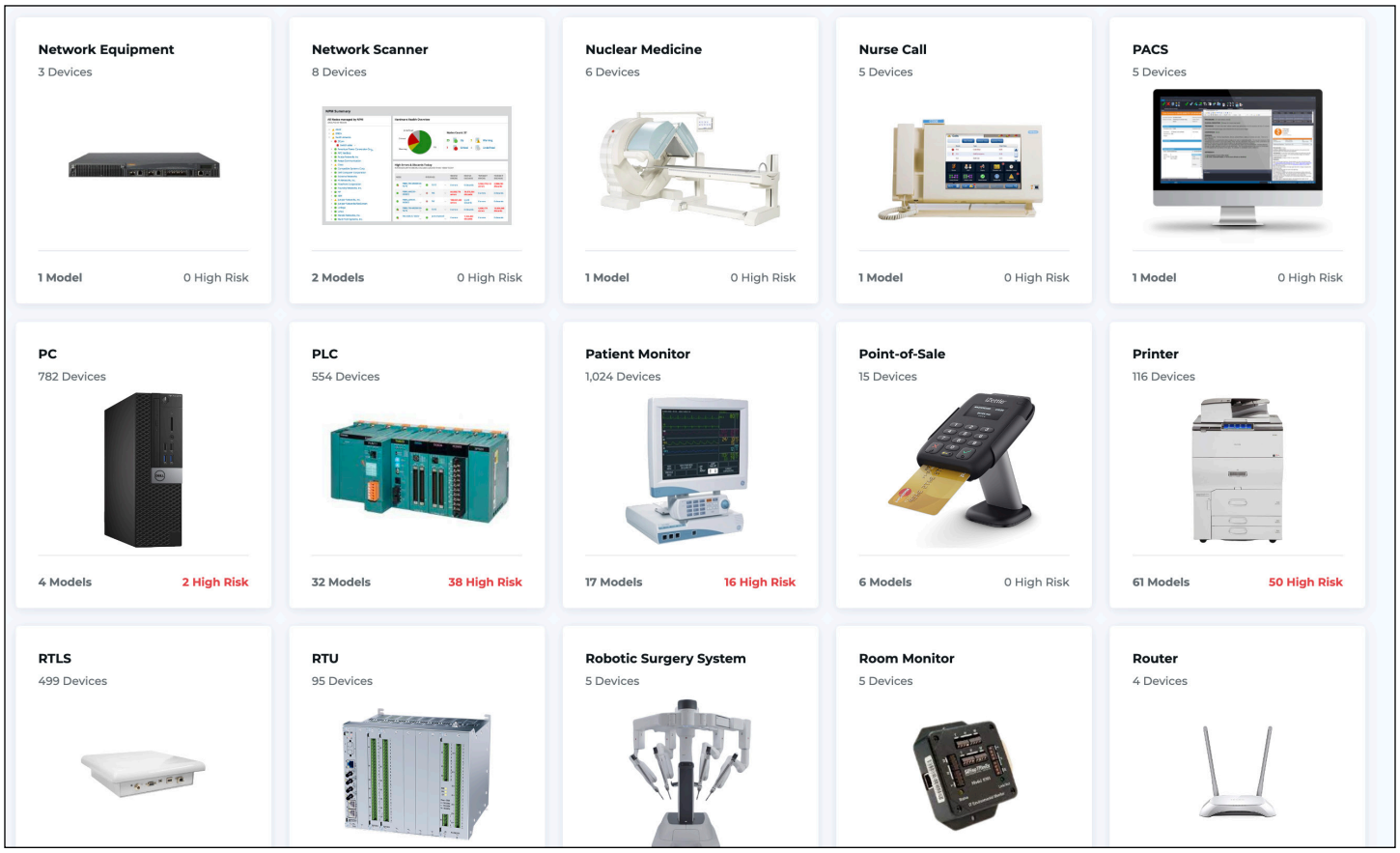
- Extend cybersecurity and operational resilience across the XIoT with a modular, SaaS powered healthcare cybersecurity platform
- Deep and broad device discovery using multiple discovery methods to decode unique and proprietary medical device protocols–achieving unparalleled network visibility
- Integrate seamlessly with existing information security and clinical engineering workflows with Claroty's extensive technical alliance ecosystem
- Achieve increased value and ROI with operational intelligence & device lifecycle insights such as device utilization, location tracking, inventory benchmarking, and more!



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 Medigate Platform leverages the broadest and deepest portfolio of XIoT 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 each environment:

- **Passive monitoring:** Continuous monitoring of network traffic to identify and enrich device details and communication profiles
- **Integration ecosystem:** Seamlessly integrate with common CMMS and device management tools to further enrich device profiles

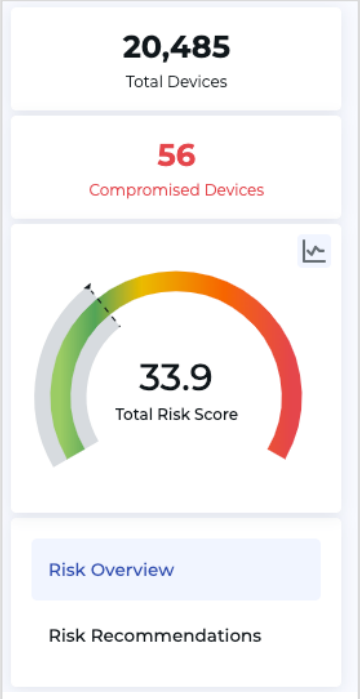


Device overview within the Medigate Platform

Vulnerability & Risk Management

Due to the nature of clinical workflows, safely scanning for and addressing vulnerabilities without potentially impacting patient care can prove to be a challenge. The Medigate Platform streamlines vulnerability and risk management by correlating your assets with multiple sources of vulnerability data, generating a risk score, and automatically prioritizes remediation recommendations based on the potential impact to operations and patient safety.

- **Uncover risk blindspots:** Incorporate various sources of risk intelligence such as a vulnerability databases, MDS2 forms, and manufacturer patches and recalls to safely and accurately uncover risk in your environment
- **Remediation prioritization:** Immediately identify risks of high severity & criticality and efficiently address the most critical vulnerabilities first
- **Measure security program progress:** Granular KPIs and flexible reporting help understand your cyber risk posture, inform decisions, and track progress

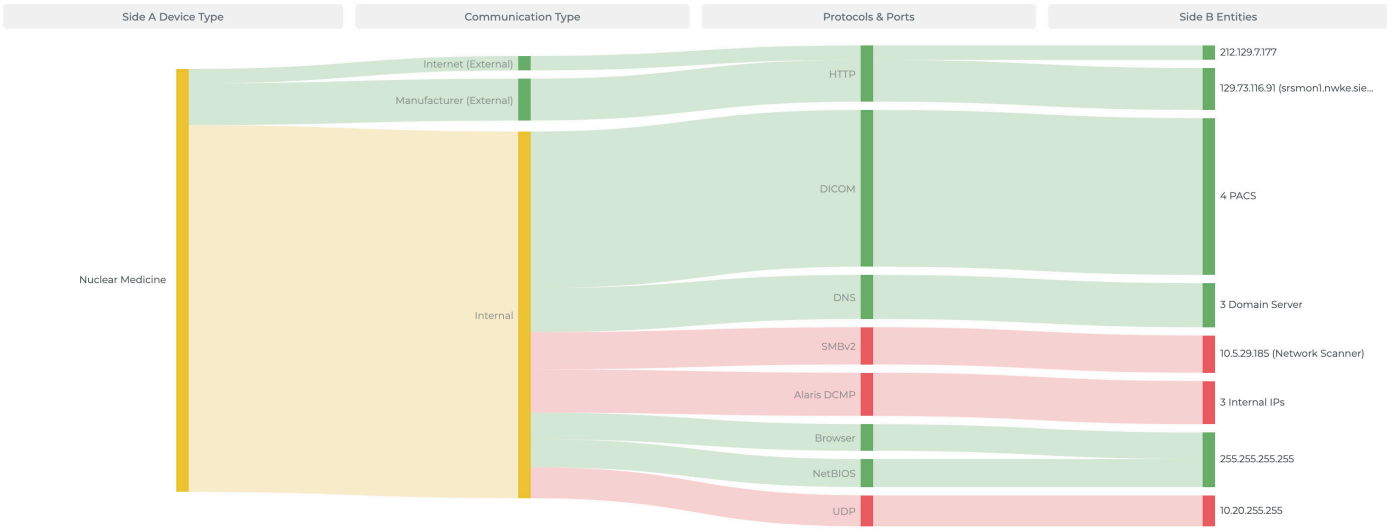


Medigate Platform network risk score indicator

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 Medigate Platform helps protect clinical environments through advanced communication controls. Highlights include:

- **Network communication mapping:** The Medigate Platform 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.

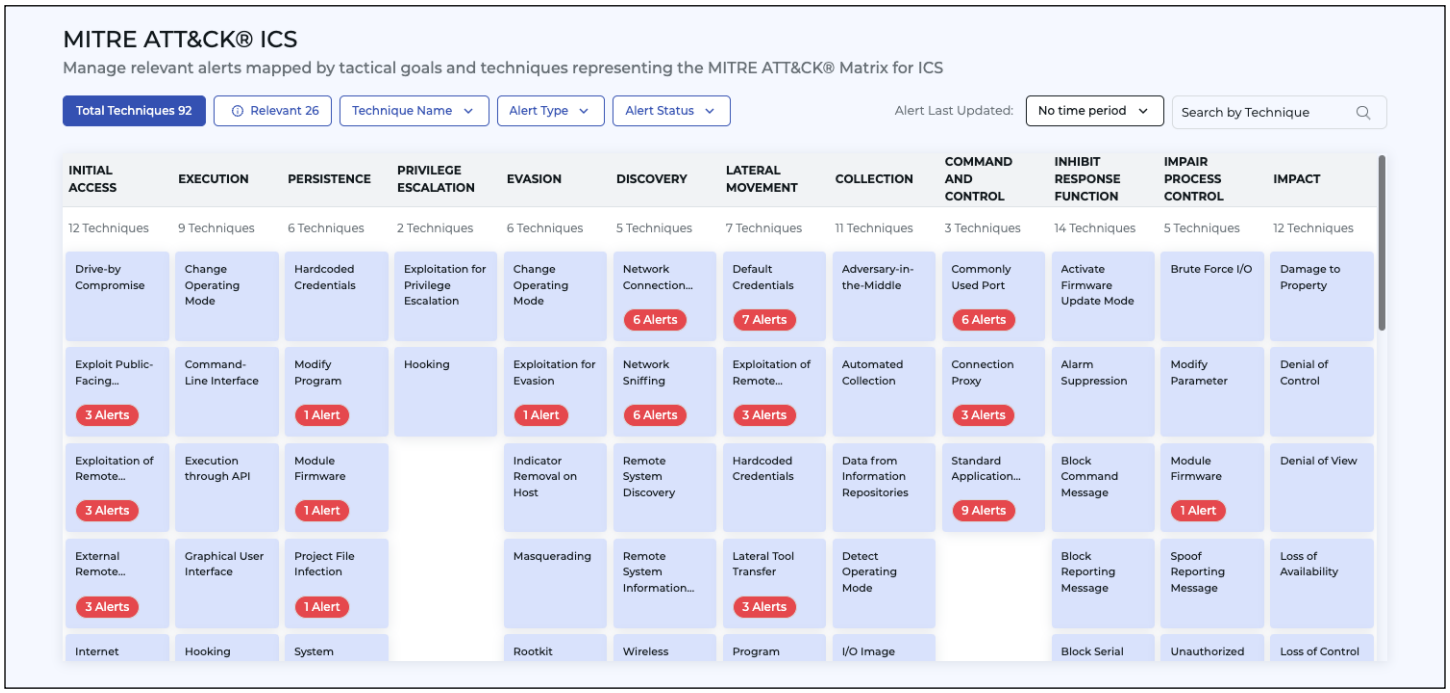


Device communication policy enforcement map

Threat Detection

No HDO is immune to threats, so effective detection and response is critical. The Medigate Platform'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 other signature based events.
- **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

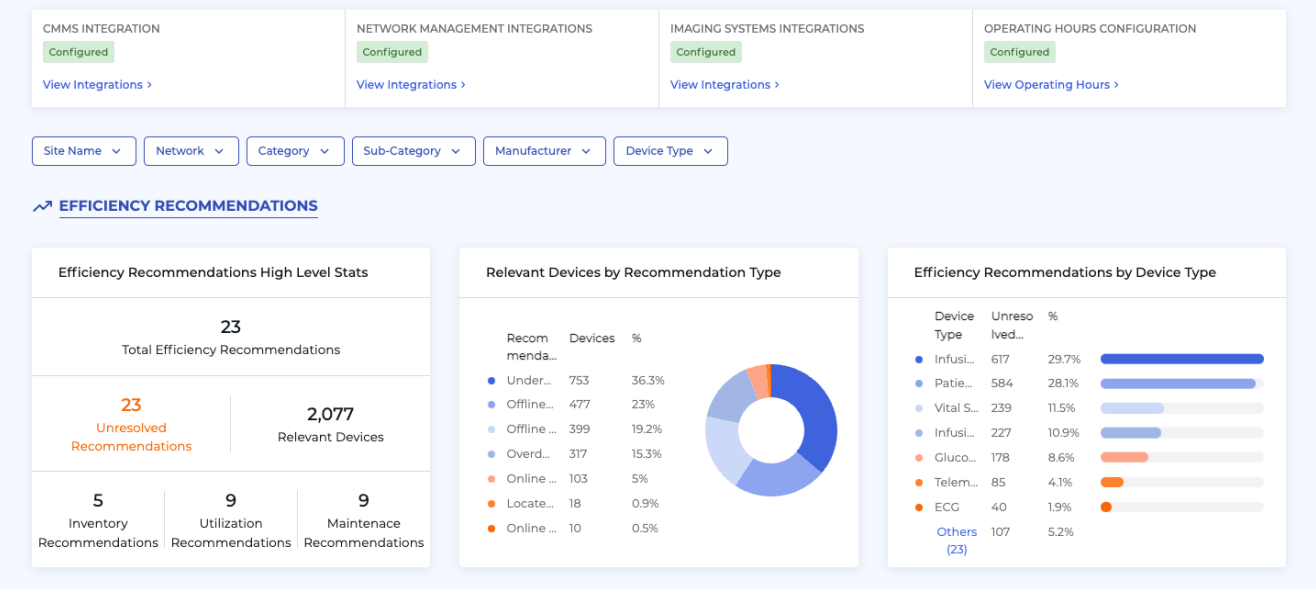


Medigate Platform alert mapping to the MITRE ATT&CK Framework

Device & Lifecycle Management

Maintaining a complete and accurate inventory while continuously monitoring the full lifecycle of each device across an HDO is a challenging endeavor. The Medigate Platform eliminates inaccurate and manual tracking of device attributes by automating the discovery and monitoring process in order to get a complete understanding of device status, changes, and usage–resulting in more efficient and effective management across your healthcare environment.

- **Device utilization metrics:** Full visibility into XIoT devices and understanding of their overall device utilization, location, and efficiency
- **Comprehensive inventory device management:** Identify, track, and automatically assign management of change (MoC) workflow items to specific team members based on group or device ownership
- **Track and maintain device lifecycles:** Advanced report creation, scheduling, and automatic run-and-send capabilities enable stakeholder communication through the Medigate Platform

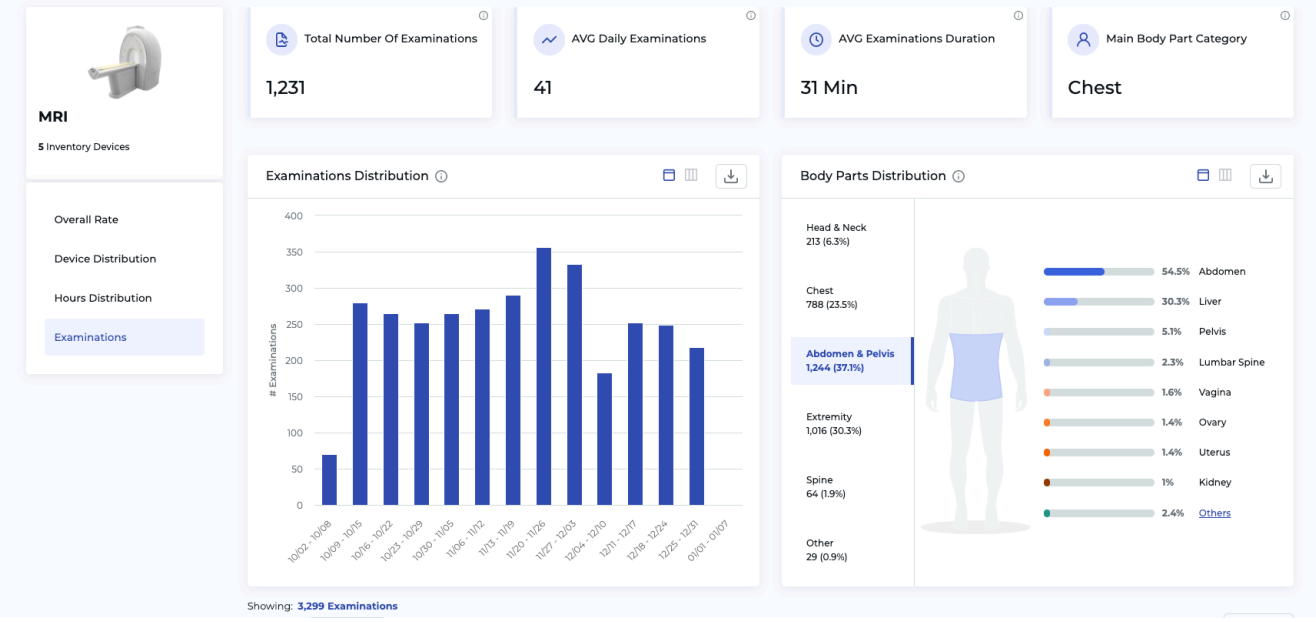


Medigate Platform operational efficiency overview dashboard

Operational Intelligence

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. The Medigate Platform is uniquely suited to help HDOs optimize clinical workflows and device utilization in order to decrease costs, increase revenue, and mitigate risk. By discovering insights about the quantity, utilization, and throughput of devices across your environment the Medigate Platform enables you to:

- **Improve efficiency:** Automate time intensive tasks such as CMMS auditing and device recovery so that healthcare delivery teams can focus on higher value objectives
- **Optimize device procurement:** Industry benchmarks for inventory and utilization, help HDOs right-size their fleet or medical devices, load-balance across sites, or renegotiate lease and maintenance agreements.
- **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.



Multi-site MRI utilization and operations overview page

The modular platform for your healthcare cybersecurity journey

As a modular solution the Medigate Platform 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.

	Medigate Platform Essentials	Medigate Platform Advanced Modules
Visibility & Insights	As the foundation of the Medigate Platform, 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 ICS 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 ICS matrix.
Vulnerability & Risk Management	Comprehensive vulnerability & risk identification and assessment capabilities based on multiple sources of intelligence, proprietary risk profiling, individual MDS^2 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 network-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, and commercial environments: the Extended Internet of Things (XIoT). The company's unified platform integrates with customers' existing infrastructure to provide comprehensive controls for visibility, risk and vulnerability management, threat detection, and secure remote access. Backed by the leading investment firms and industrial automation vendors, Claroty is deployed 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.

CLAROTY MEDIGATE by Claroty