

Medigate by Claroty for Healthcare

A modular, SaaS-powered healthcare cybersecurity platform



CONTENTS

Introduction	2
Claroty and Medigate: Securing the XIoT	2
Medigate: Healthcare Cybersecurity	3
Solution Overview	4
The Medigate Platform	4
Module Overview	10
Visibility Insights and Anomaly Threat Detection	10
Vulnerability and Risk Management	14
Network Security Management	16
Clinical Device Efficiency	18
About Cyberworld	20

INTRODUCTION

CLAROTY AND MEDIGATE: SECURING THE XIOT

Medigate is the first company to recognize — and address — the critical need for healthcare IoT security, was purchased by Claroty at the beginning of 2022. Combining Medigate’s leadership in delivering unmatched visibility, protection & threat detection for medical devices with Claroty’s leadership in doing the same for industrial OT devices, will create a powerhouse for security of the Extended internet of Things (XIoT) in healthcare. Organizations can now confidently connect their IoMT, OT, IoT and IT assets with a single, best of breed solution.

About Claroty

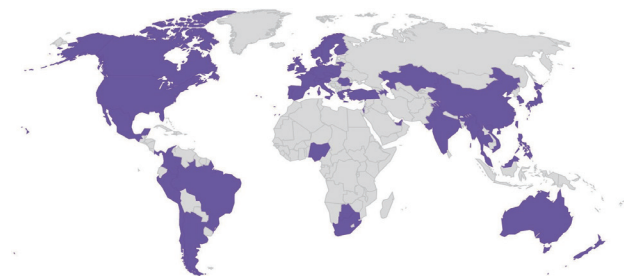


Founded: **2015** HQ: **NYC** Funding: **\$635M** Awards: **50+** Sites Deployed: **10k+** Devices Protected: **20M+**

Claroty empowers industrial, healthcare, commercial, and public sector 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, network protection, threat detection, and secure remote access.



OUR CUSTOMERS: Many of the world’s top brands and respected organizations trust Claroty to protect their most critical cyber physical systems.



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.

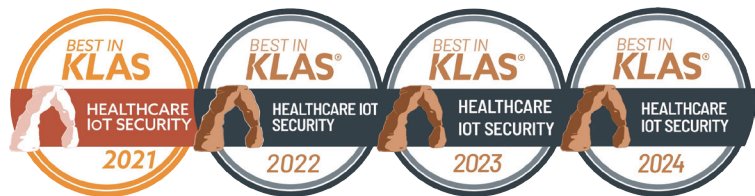
INTRODUCTION

MEDIGATE: HEALTHCARE CYBERSECURITY

Your Partner for Healthcare Device Security

Powered by Medigate's purpose-built technology and deep domain expertise, Claroty empowers healthcare providers to reliably serve patients while safely connecting to the Extended Internet of Things (XIoT).

Medigate by Claroty wins Best in KLAS for Healthcare IoT Security - Four Years in a Row!



30+ Awards

Our platform has earned dozens of accolades in Healthcare Cybersecurity.

100% Healthcare

We evaluate data and protocols to create custom policies for hospitals.

2000+ Healthcare Facilities

We have deployed our solutions in thousands of hospitals worldwide.

13M+ IoT Devices

We protect more than 10 million IoT devices in healthcare environments.

7M+ Medical Devices

We secure and monitor more than seven million IoMT and other medical devices.

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. Clarity 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

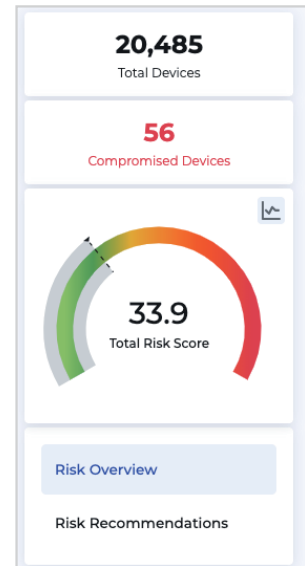
Network Equipment 3 Devices  1 Model 0 High Risk	Network Scanner 8 Devices  2 Models 0 High Risk	Nuclear Medicine 6 Devices  1 Model 0 High Risk	Nurse Call 5 Devices  1 Model 0 High Risk	PACS 5 Devices  1 Model 0 High Risk
PC 782 Devices  4 Models 2 High Risk	PLC 554 Devices  32 Models 38 High Risk	Patient Monitor 1,024 Devices  17 Models 16 High Risk	Point-of-Sale 15 Devices  6 Models 0 High Risk	Printer 116 Devices  61 Models 50 High Risk
RTLS 499 Devices  0 Models 0 High Risk	RTU 95 Devices  0 Models 0 High Risk	Robotic Surgery System 5 Devices  0 Models 0 High Risk	Room Monitor 5 Devices  0 Models 0 High Risk	Router 4 Devices  0 Models 0 High Risk

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

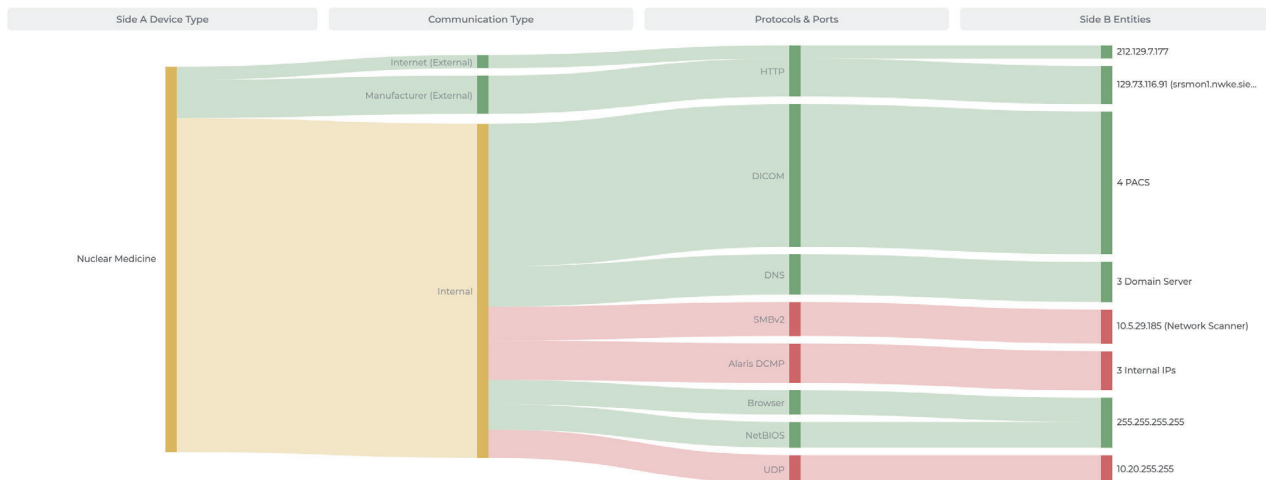


Medigate Platform network risk score indicator

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 alert 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

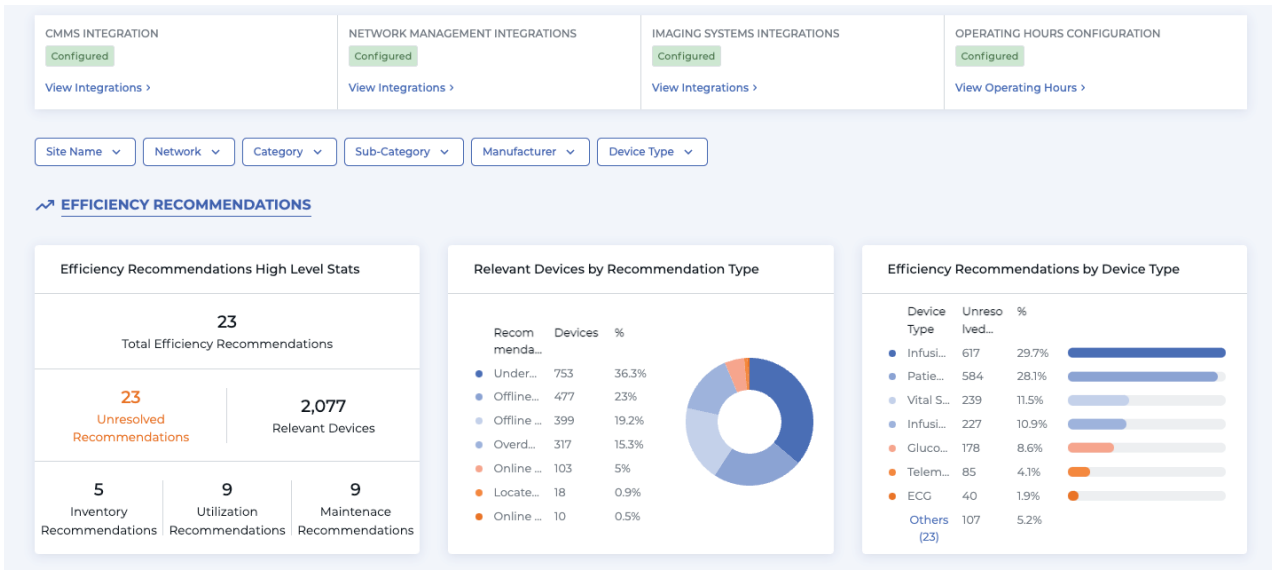
INITIAL ACCESS	EXECUTION	PERSISTENCE	PRIVILEGE ESCALATION	EVASION	DISCOVERY	LATERAL MOVEMENT	COLLECTION	COMMAND AND CONTROL	INHIBIT RESPONSE FUNCTION	IMPAIR PROCESS CONTROL	IMPACT
12 Techniques	9 Techniques	6 Techniques	2 Techniques	6 Techniques	5 Techniques	7 Techniques	11 Techniques	3 Techniques	14 Techniques	5 Techniques	12 Techniques
Drive-by Compromise	Change Operating Mode	Hardcoded Credentials	Exploitation for Privilege Escalation	Change Operating Mode	Network Connection...	Default Credentials	Adversary-in-the-Middle	Commonly Used Port	Activate Firmware Update Mode	Brute Force I/O	Damage to Property
Exploit Public-Facing...	Command-Line Interface	Modify Program	Hooking	Exploitation for Evasion	Network Sniffing	Exploitation of Remote...	Automated Collection	Connection Proxy	Alarm Suppression	Modify Parameter	Denial of Control
Exploitation of Remote...	Execution through API	Module Firmware		Indicator Removal on Host	Remote System Discovery	Hardcoded Credentials	Data from Information Repositories	Standard Application...	Block Command Message	Module Firmware	Denial of View
External Remote...	Graphical User Interface	Project File Infection		Masquerading	Remote System Information...	Lateral Tool Transfer	Detect Operating Mode		Block Reporting Message	Spoof Reporting Message	Loss of Availability
Internet	Hooking	System		Rootkit	Wireless	Program	I/O Image		Block Serial	Unauthorized	Loss of Control

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

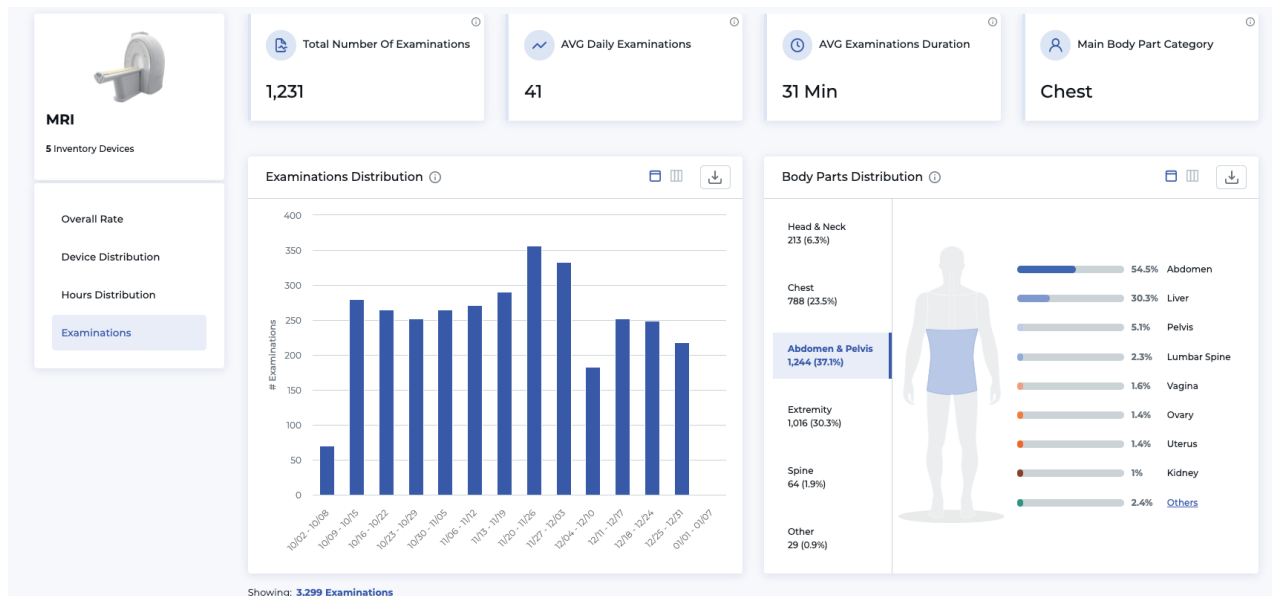


Medigate Platform operational efficiency overview dashboard

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

MODULE OVERVIEW

VISIBILITY & INSIGHTS AND ANOMALY & THREAT DETECTION

Understand, Manage, and Protect Connected Devices

SHINING A LIGHT ON YOUR CONNECTED MEDICAL DEVICES

There's a surge of connected medical devices and the Internet of Medical Things (IoMT), and it's a massive challenge for healthcare IT, BioMed, and security teams. Unlike those found on other IT networks, managing and securing these Extended Internet of Things (XIoT) devices cannot be done the same way. They use different operating systems and protocols, and most importantly, they're involved in life-critical situations.

Your healthcare delivery organization (HDO) must ensure that every device decision – whether it's about procurement, operations, or security – considers the clinical setting at large. It takes accurate visibility into each device's inner workings and behaviors. Still, this level of device detail and clinical context is hard to come by, and manual data collection can't keep up with the pace of growth. At the same time, out-of-date processes and general-purpose discovery tools miss critical device details and threats.

To close the gaps and increase the effectiveness of your IT, BioMed, and security programs, you need high fidelity, detailed device data that produces complete, up-to-date inventories, accurate risk assessments, and improved lifecycle management and security strategies. Medigate's Visibility, Insights, and Anomaly Detection delivers all of this and is the #1 device security solution designed specifically for healthcare.

MEDIGATE'S VISIBILITY, INSIGHTS, AND ANOMALY DETECTION

The essential Visibility, Insights, and Anomaly Detection function of the Medigate Device Security Platform (MDSP) discovers and profiles every connected device on your network, analyzing the inner workings and risks, so you can make decisions to operate safely and efficiently. With unparalleled accuracy, you have the medical device profiles and contextual risk identification you need to make data-driven management and security decisions that help you better protect and optimize your extended, connected medicine operations.

HOW IT WORKS

Within hours of deployment, through either a network tap or SPAN port, Medigate passively discovers the IoT and IoMT devices connecting to your network and begins providing accurate, granular details on every connected device. The platform uses unique Deep Packet Inspection (DPI) techniques to offer data-rich profiles and contextualized risk assessments that give you the most accurate inventories and threat detection available. With Visibility, Insights, and Anomaly Detection, you receive:

- **Detailed device profiles:** Over 100 unique device attributes that often go undocumented, such as device IDs, version information, physical location, serially attached devices, vulnerability assessments, network connectivity, and more.

Device IDs	Device ID	Model	Manufacturer	Category	Sub-Category
BOIS-PC-Unit	BOIS-PC-Unit	BOIS-PC-Unit	Amibios (Joss-Tandy)	Medical	Patient Device
Alerts	Infusion Pump	BOIS-PC-Unit		Physical	Portable
Versions & Names	Proprietary Erase OS	Proprietary	Erase OS	9.10.2	
Network	Corporate	WIFI	WIFI_902	WIFI_902	Wireless
Network Security	CHCP	WPA2	WPA2	WPA2_128_Phd	WPA2_128_Phd
Location	Canada	WPA2	BOIS-PC-Unit_Wireless_Access	BOIS-PC-Unit_Wireless_Access	
Chassis & Chassis ID	CL8020603	In Service	Hospital - Ontario	WPA2_128_Phd	
Custom Attributes	ADD Values	ADD Values	ADD Values	ADD Values	2023-12-05 16:53:12.81939-0000

- **Network communications maps:** Get documented inter-device communication relationships with a world map, connection matrix, and VLAN visibility. With these tools, you can weigh the impact of potential segmentation decisions on the broader environment.



- **Accurate alerts:** With highlighted risks – including the use of plain text credentials and your exposure to the risks generated by unencrypted health information (PHI), vulnerabilities, and outdated versions – you can start taking the appropriate steps to protect your operations.
- **Threat intelligence:** Tailored, healthcare-specific Indicators of Compromise (IoCs) help you understand and address the risks in your environment.
- **Vulnerability assessments:** Medigate passively assesses your XIoT devices to known vulnerabilities to ascertain current device risk levels without login credentials. This correlation enables you to prioritize your patch management workflows to strengthen your environment's security posture.

THE CORE MEDIGATE DIFFERENCE

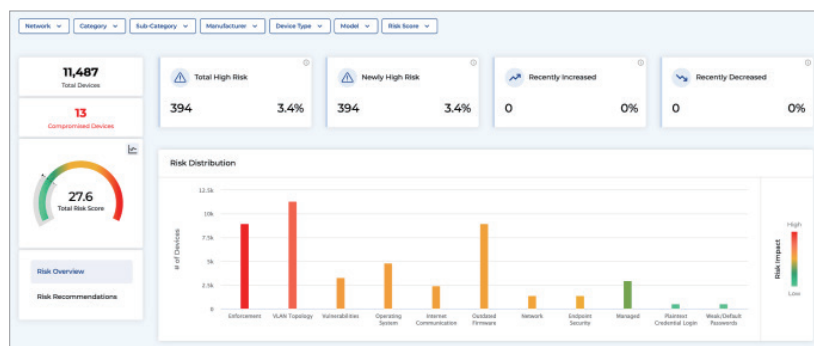
Achieve Complete, Up-to-Date, Detailed Inventories

You can't manage what you don't know. With Medigate, you know everything with up-to-date, detailed inventories of the XIoT devices connecting in your environment. Medigate Research Labs has built out the industry's largest database of medical and IoMT devices, which our platform leverages to identify the devices in any clinical setting accurately.

Using several unique DPI techniques, Medigate extracts a variety of hard-to-get technical attributes to generate highly granular device identification. Through passive traffic collection, Medigate can determine network traffic, characteristics such as OS, app version, firmware version, serial numbers, and unique device identifiers for each device. Better lifecycle management decisions around procurement, operations, maintenance, and security will save you time and money with accurate data.

Action with Accurate Alerts

If a device behaves anomalously, you need to know about it and address it ASAP. You need to be able to trust an alert to avoid wasting valuable resources dealing with false alarms.



It takes a solution that understands the unique nature of medical and IoMT devices and can discern between normal and abnormal activity.

If Medigate's research team has parsed device protocol specifications, manufacturer instructions, and architecture documentation to get the most profound understanding of the communications and operations of medical and IoMT devices under normal conditions as intended. This depth allows Medigate to quickly and accurately identify anomalous activity risks to your organization.

When you see a Medigate alert, it means a device is doing something it wasn't engineered or configured to do by the manufacturer. Medigate gives you the early warnings and accurate risk assessments to take action, so you can address and minimize the impact of malicious activity in your environment.

Improve Your Security Stance

Attackers are looking to exploit any weakness to get into your network. Make sure your medical and IoMT devices aren't leaving you exposed. Medigate passively discovers and profiles your devices, assessing and correlating device attributes to known vulnerabilities to identify current device risk levels – all without needing login credentials.

For instance, Medigate can pinpoint the use of plain text credentials or devices that have unencrypted PHI on them, as well as known vulnerabilities and outdated versions that can put your organization at risk. This information allows you to appropriately plan and prioritize configuration updates, patches, and other actions that will help you protect your data and strengthen your security posture.

DELIVER IT ALL WITH SERVICES

To help quickly reduce cyber risks and ensure your security investments pay off, Medigate has developed a healthcare cyber-physical security services program called Partner Ready Operational Services (PROS). Designed to secure your Extended Internet of Things (XIoT), PROS applies a proven maturity roadmap to speed the journey to your ideal state. Certified “PROS” deliver a standards-driven, trusted services path based on best practices that we’ve developed partnering with more than 1,000 hospitals. From prioritized investment strategies to properly sequenced integrations, they can support you wherever you need.

CONCLUSION

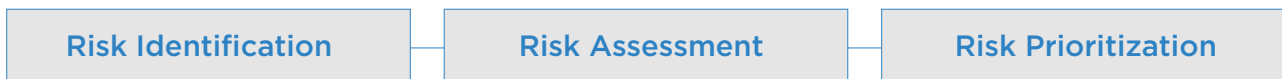
You need complete visibility into the makeup and potential risks of the devices operating in your environment. The only way to attain this level of detail and insight is with a purpose-built solution for healthcare. Medigate understands the unique languages of clinical devices and does not guess what they’re saying through AI or Machine Learning. Instead, the platform uses specialized techniques to deliver advanced insights from device data. With Medigate, the data available in all of your connected devices are unlocked and validated, so you can connect with confidence and accelerate your real-time healthcare initiatives.

VULNERABILITY & RISK MANAGEMENT

The Healthcare Vulnerability & Risk Management Challenge

The modern healthcare network has reshaped patient care delivery. Health system workflows now depend highly on connected devices. With increasing reliance on this connectivity, healthcare delivery organizations (HDOs) face new risks when assessing their security posture. The Medigate Platform enables HDOs to mitigate risks & vulnerabilities before they compromise patient care, PHI, or critical healthcare workflows.

An effective vulnerability management & risk management program provides visibility into risks within connected devices to streamline workflows for prioritization & remediation. The Medigate Platform delivers a purpose-built solution for healthcare environments, helping to reduce risk and secure efficient patient care delivery. Highlights include:



Medigate Platform VRM Module

How It Works

The Medigate Platform leverages passive deep packet inspection technology and the industry's broadest portfolio of XIoT protocol coverage to provide a detailed view of devices in the healthcare environment. This caliber of visibility is made possible through a flexible deployment based on the unique needs of each environment. This level of device detail enables the Medigate Platform to assess overall risk based on technical device attributes, external vulnerability intelligence, and proprietary in-house research.

Risk Identification

Understanding all the potential risks and vulnerabilities that impact devices across hospital environments can be challenging due to their unique attributes and applications. The Medigate platform lays the foundation for comprehensive vulnerability & risk management with complete visibility into the devices and network blind spots most prone to risk. Highlights include:

- **Enriched Device Profiles:** The Medigate Platform matches discovered device attributes with known vulnerabilities, manufacturer patch information, recalls, MDS2 forms, and more, creating the foundation for network risk assessment and prioritization.
- **Threat Intelligence Feed:** A curated list of threat intelligence from third parties and Claroty's in-house research group, Team82. This feed provides news and information about common vulnerabilities likely to impact CPS devices.
- **Vulnerability Management (VM) Integrations*:** Integrating with VM solutions enables HDOs to leverage existing solutions in order to provide further depth of visibility into their clinical environment while eliminating the risk of incorrectly scanning medical devices with the ability to create exclusion lists.

* Included in advanced module

Risk Assessment

The ability to assess the risk of each device and across sites is essential to building a strong foundation for vulnerability and risk management. Meaningful assessment of risk requires a deep understanding of both the devices and the environment in which they operate.


- **Proprietary Device Risk Scores:** Claroty's risk framework provides risk scoring based on three core metrics: likelihood, compensating controls, and impact. This ensures that an HDOs risk posture is reflective of their unique environment and risk reduction priorities.
- **Risk Simulator*:** To support device procurement, deployment, or management, the risk simulator illustrates the possible risk a device poses to the network—even if the device is not yet acquired by the HDO—by pulling data from across Claroty's install base.
- **MDS2 Directory*:** The MDS2 Directory contains valuable information to better understand supported security controls on medical devices, helping users drive better informed procurement and risk management decisions.

Risk Prioritization

Once vulnerabilities and potentially impacted devices are identified, addressing remediation tactics ensure risk-based prioritization across the full lifecycle of a vulnerability.

- **Vulnerability Prioritization & Auto-Actions:** In order to streamline vulnerability remediation, the Medigate Platform enables priority group assignments and workflow automations for impacted devices.
- **Risk Overview & Recommendations*:** Enables users to focus on the most impactful risk remediation efforts with visualized risk metrics across the network and tailored risk recommendations based on their quantitative impact on the overall network risk score.

Medigate Platform Vulnerability & Risk Management Module

Medigate Platform Essentials	Medigate Platform Advanced Modules
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 site-level.

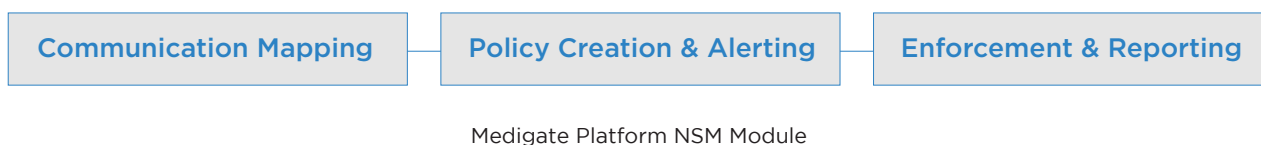
* Included in advanced module

NETWORK SECURITY MANAGEMENT

The Healthcare Network Security Challenge

Connectivity in the modern healthcare network has dramatically reshaped patient care delivery. While this connectivity has many benefits, there tends to be a lack of governance outside of traditional IT devices. At a time where health systems are increasingly targeted for ransomware and other cyber attacks, this can result in ever-expanding attack surfaces. Blind spots of unidentified risk can have costly implications for health systems across clinical & non-clinical workflows.

Securing a healthcare environment's network requires specialized knowledge and nuanced considerations for clinical workflows. The Medigate Platform's Network Security Management Module (NSM) enables healthcare-focused network-centric communication policy creation and enforcement to help HDOs strengthen their security posture without impacting care delivery.



How It Works

The Medigate Platform leverages passive deep packet inspection technology and the industry's broadest portfolio of XIoT protocol coverage to provide a detailed view of devices in the healthcare environment. This caliber of visibility is made possible through a flexible deployment based on the unique needs of each environment. This level of device detail enables the Medigate Platform to profile device communications and provide users a visualized look into network communication patterns.

Communication Mapping

The first step towards network protection is to gain complete visibility into all devices on the network, however, this can be challenging due to the unique nature of clinical devices and the networks in which they operate. The Medigate Platform provides deep insights into device communication across the HDO environment, highlights include:

- **Visualized Device Communications:** Complete profile of device communications, including protocol usage, communication type, and a list of all devices communicating with an individual asset.
- **NAC Discoverability & Visibility:** Integrate with existing NAC solutions to further enrich the device profile with authentication information, logic profiles, identity groups, ACL type, and more.
- **Communication Matrix*:** The purpose of the matrix is to enhance visibility about device communication within your network, aimed to drive clinical-aware network segmentation policies by delivering an in-depth visibility into how devices are communicating on the network vs. how they should communicate.

Policy Creation & Alerting

Once visibility into devices and their communications are achieved, the next step is to begin implementing controls that will help protect the network in a way that does not interrupt care delivery. The Medigate Platform helps to build these controls through recommended and customizable policies that can be integrated into existing infrastructure:

- **Policy Recommendations*:** The Medigate Platform automatically creates recommended communication policies based on discovered device behaviors and known best practices in healthcare environments that can be customized for specific needs.
- **Policy Monitoring & Alerting*:** Monitor policies and generate real-time alerts when policy deviations occur for enforcement testing, investigation, and remediation.
- **VLAN Segmentation*:** Enforce security, improve performance, and streamline operations by reviewing VLAN hygiene, creating rules to prevent network congestion, and tracking VLAN violations.

Enforcement & Reporting

Existing NAC solutions may need more visibility into unmanaged devices or more ability to fine-tune policies critical to healthcare environments. The Medigate platform's integrations with NAC & firewall solutions accelerate network security management.

- **NAC and Firewall Policy Enforcement*:** Extend Medigate's recommended policies by dynamically refining them and automatically enforcing them to optimize protection.
- **Network Security Overview*:** Provide visibility over organizations' enforcement and segmentation projects. Leverage insights to support metrics, network policy planning, and drive overall program support.
- **Network Protection Reporting*:** Build user-specific dashboards, customize metrics tracking, and schedule routine reports to inform stakeholders and support end-user progress.

Network Security Management

Medigate Platform Essentials	Medigate Platform Advanced Modules
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 the 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

The Healthcare Network Security Challenge

The connectivity of the modern healthcare network has dramatically reshaped patient care delivery. With clinical workflows increasingly dependent on this connectivity, proper governance of these devices is a critical component of operational efficiency across healthcare environments. The Medigate Platform enables healthcare delivery organizations (HDOs) to improve the management of connected devices from medical devices to building management systems. The Medigate Platform's Clinical Device Efficiency (CDE) module enables users to leverage the network data of connected devices to solve standard device and lifecycle management challenges while maximizing ROI with operational excellence.



Medigate Platform CDE Module

How It Works

Identifying all connected devices can add measurable business value to decrease costs, increase revenues, and mitigate risks across HDOs. The first step is understanding the devices involved across clinical and non-clinical workflows. Once you achieve visibility, properly leveraging these insights to implement process improvements or enhance existing workflows that correlate directly to organizational outcomes can help add immediate business value.

By profiling devices to monitor their utilization, location information, and operational status, the Medigate Platform can help users drive more efficient workflows and use data to inform operational planning and capital expenditures.

Device Intelligence

The unique nature of devices in a healthcare setting makes it challenging to get a complete picture of a device's activity and status on the network. With complete visibility into connected devices, the Medigate Platform helps HDOs better manage devices to achieve operational excellence. Consider the following:

- **Device Utilization:** Knowing how and when a device is being used helps HDOs improve operations through various means, such as identifying patch windows, load-balancing device usage across sites to increase throughput and efficiency, making data-driven inventory-level decisions, and more.
- **EoL Information:** The Medigate Platform identifies devices considered end-of-life by their manufacturer so that device managers can enable compensating controls around them, extending their useful lifetime to defer replacement costs and reducing network risk.
- **FDA Recall Information*:** Identify which devices may be impacted by an FDA recall to determine if any action should be taken on the current usage or maintenance of the device to ensure patient safety.

Operational Management

Clinical workflows require a clinical context. With deep visibility into the usage of connected devices within the hospital environment, the Medigate Platform provides actionable insights that enable HDOs to enhance operational efficiency with the following:

- **Device Location:** Locate devices in the hospital with a high degree of precision by leveraging enriched device profiles and integrations with network management tools, saving time and improving labor efficiencies when devices require maintenance, patching, or removal.
- **Industry Benchmarking*:** The Medigate Platform benchmarks device counts against observed industry standards in similar-sized health systems to aid users in driving better inventory planning decisions and utilization metrics, reducing costs and increasing operational efficiency.
- **Efficiency Recommendations*:** The Medigate Platform recommends ways to improve operational efficiencies. Categories include overdue preventative maintenance, underutilized rented devices, located lost devices, and more, showing which devices are affected and resolution status.

Optimization and Integration

The Medigate Platform eliminates inaccurate and manual device inventory records across the HDO by automating the discovery and monitoring of network devices and integrating their profiles into existing solutions. Add immediate business value by optimizing workflows with existing inventory and processes.

- **Operational Efficiency Dashboard*:** The Medigate Platform provides key metrics across the overall picture of inventory, location, and utilization through customizable dashboards and in-depth analytics.
- **CMMS/CMDB Integrations*:** Integrating with your asset management platform helps enrich data collection and analysis to drive more granular device profiling and risk scoring, helping to streamline device and lifecycle management workflows.
- **CMMS/CMDB Reconciliation*:** Match inventory records between the Medigate Platform and an existing CMMS/CMDB to create a stronger, centralized device inventory across the hospital environment while eliminating tedious manual inventory collection work.

Clinical Device Efficiency

Medigate Platform Essentials	Medigate Platform Advanced Modules
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 to maximize operational value and achieve increased ROI



*Advanced Offering Only**

ABOUT CYBERWORLD

OT Security · Data Management · Cybersecurity

Founded in 1991, Cyberworld (Asia) Ltd. has steadily established itself as a reputable IT products distributor in Hong Kong and Macau. With a foresight to open Chinese mainland market strategy, in 2011, we established Guangzhou Cyberworld Technology Company Limited. Now we have offices in Guangzhou, Shanghai and Beijing.

We explore the current excellent IT products and solutions according to local conditions, and cooperate with well-known foreign vendors such as Claroty, Cohesity, Qualys, SecurityScorecard, Skybox Security, Sophos, SSH, Trellix and Varonis to form a unique solutions of OT Security, Data Management, and Cybersecurity.

Products We Distributed



COHESITY



SOPHOS



Trellix



Contact Us

Hong Kong

13/F, Yau Lee Centre, 45 Hoi Yuen Road, Kwun Tong, Kowloon, Hong Kong

info@cyberworldchina.com

Learn more at cyberworld.com.cn

CLAROTY HEALTHCARE

We envision a future where cyber and physical worlds
safely connect to sustain our lives.