CLAROTY MEDIGATE by Claroty

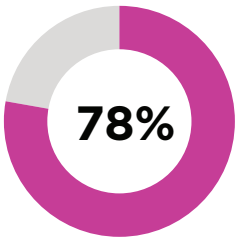
HEALTHCARE

SOLUTION OVERVIEW

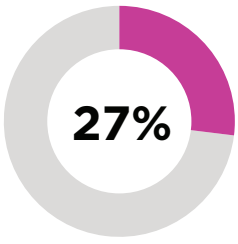
WHY HEALTHCARE NEEDS CLINICALLY-AWARE THREAT DETECTION

Managing Blind Spots Amidst a Growing Threat Landscape

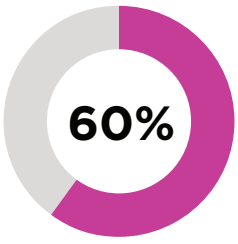
Cyber attacks against the healthcare industry continue to increase year over year — the most common of which include ransomware, insider threats, and attacks on the supply chain. As connectivity in healthcare environments expands, so does the potential for these cyber incidents to impact medical devices, as well as the building management systems that keep hospital operations running. According to the 2023 Global Healthcare Cybersecurity Study[1], 78% of respondents experienced at least one cybersecurity incident in the last year. When clinical workflows and patient care are involved, there is no room for blindspots.



Experienced a cybersecurity incident



Affected building management systems



Reported an impact on care delivery

[1]The Global Healthcare Cybersecurity Study, 2023

Going Beyond Traditional IT Solutions

While most organizations have some level of protection against cyber threats in their healthcare network, these solutions lack the specialized knowledge of clinical environments and the devices within them that are required to protect them. Without the full context required to identify, assess, and prioritize threats across medical devices, IoT, and building management systems, your healthcare network is susceptible to risk. Healthcare organizations can help to protect against cyber threats against their clinical networks by employing a threat detection solution that boasts:

Agentless threat monitoring within the clinical network, not only at its boundary, provides increased visibility and operational context into managed and unmanaged devices.

Clinically aware alerts that provide in-depth details about affected devices, creating a strong foundation for investigation and response and helps to avoid care disruption.

Compliance and hardening validation with custom monitoring capabilities that help healthcare organizations meet and maintain compliance with security standards.

Comprehensive insights and coverage of all cyber-physical systems (CPS) in the healthcare environment, including medical devices, IoT systems, and building management systems (BMS).

Navigating Growing Regulatory Pressure

Cybersecurity is patient safety is a recurring theme across organizations and regulatory bodies. Governments around the globe are urging, and often requiring, action to be taken to increase cyber protections of healthcare environments in light of growing threat activities. This has become more evident in recent years as regulatory activity is shifting away from a purely data-centric approach to healthcare cybersecurity to one that includes specific measures for network-connected medical devices. Examples of such regulatory frameworks include:

HICP Section 405(d)	HHS Cybersecurity Performance Goals (CPG)	The 2022 PATCH Act

The challenge for healthcare providers and medical device manufacturers lies in effectively and efficiently adhering to these regulations and guidelines while remaining flexible in the face of a changing threat landscape. This requires adopting a holistic cybersecurity strategy that includes continuous monitoring of the entire clinical network, regular risk assessment, and network protection controls that uphold clinical workflows.

Threat Detection with the Medigate Platform

The Medigate Platform helps healthcare organizations protect their most critical devices by continuously monitoring for known threats and the earliest indicators of compromise, helping users detect, prioritize, and respond to threats before they can impact patient care. Leveraging multiple device discovery methods backed by the most comprehensive library of CPS protocols, the Medigate Platform reveals potential risks across all CPS in the healthcare environment while aiding response efforts within existing security tools and workflows. Highlights include:

Threat Identification

Detect and respond to known and emerging threats across the healthcare environment signature and anomaly-based detections that map to the MITRE ATT&CK framework

Customized Alerting

No two healthcare environments are identical. Create alerts that fit unique threat detection needs and/or goals that cover specific communication or device condition scenarios

Enhanced SOC Workflows

Integrate with SOC workflows like security appliances, automation, and orchestration tools to unify alerts and security processes into a centralized workflow.

Cybersecurity IS patient safety. To learn more about the Medigate Platform's Anomaly and Threat Detection Capabilities visit www.claroty.com

About Claroty

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.

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.

For more information, visit claroty.com or email contact@claroty.com.

CLAROTY MEDIGATE by Claroty