MODULE OVERVIEW

Exposure Management

The Healthcare Exposure 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. Claroty xDome enables HDOs to mitigate risks, vulnerabilities, and exposures before they compromise patient care, PHI, or critical healthcare systems.

An effective continuous threat exposure management program (CTEM) provides visibility into risks within connected devices to streamline workflows for scoping, discovery, prioritization, validation & remediation. Claroty xDome delivers a purpose-built solution for healthcare environments, helping to reduce risk and secure efficient patient care delivery. Highlights include:

| Risk Identification | Risk Assessment | Risk Prioritization |
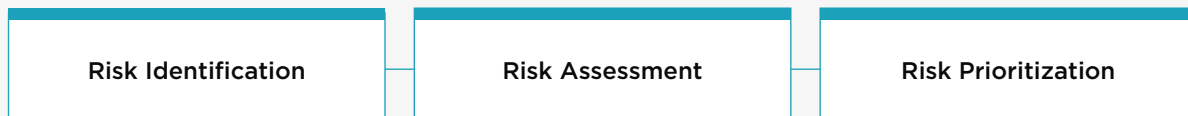
Claroty xDome VRM Module

How It Works

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

Risk Identification

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

Exposure Scenarios: Claroty xDome matches discovered device attributes with known vulnerabilities (CVEs), and other potential risks or risk scenarios from the attacker's POV, 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.

Risk Assessment

The ability to assess the risk of each device and across sites is essential to building a strong foundation for exposure management. Meaningful assessment of risk requires a deep understanding of boththe 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, identifying the right teams and addressing remediation tactics ensure risk-based prioritization across the full lifecycle of a vulnerability.

Vulnerability Prioritization & Auto-Actions: In order to streamline vulnerability remediation, Claroty xDome 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.

*Included in advanced module

About Claroty

Claroty empowers organizations to secure cyber-physical systems across industrial (OT), healthcare (IoMT), and enterprise (IoT) 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, 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.