CLAROTY

Healthcare

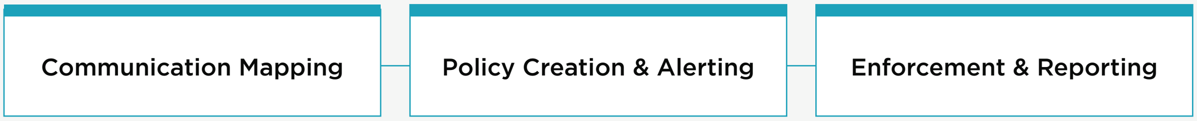
MODULE OVERVIEW

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. Claroty xDome'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.



Claroty xDome NSM Module

How It Works

Claroty xDome leverages passive DPI (deep packet inspection) technology and the industry's broadest portfolio of CPS 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 Claroty xDome 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. Claroty xDome 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. Claroty xDome helps to build these controls through recommended and customizable policies that can be integrated into existing infrastructure:

Policy Recommendations*: Claroty xDome 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. Claroty xDome's integrations with NAC & firewall solutions accelerate network security management.

NAC and Firewall Policy Enforcement*: Extend Claroty xDome'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.

About Claroty

Claroty has redefined cyber-physical systems (CPS) protection with an unrivaled industry-centric platform built to secure mission-critical infrastructure. The Claroty Platform provides the deepest asset visibility and the broadest, built-for-CPS solution set in the market comprising exposure management, network protection, secure access, and threat detection – whether in the cloud with Claroty xDome or on-premise with Claroty Continuous Threat Detection (CTD). Backed by award-winning threat research and a breadth of technology alliances, The Claroty Platform enables organizations to effectively reduce CPS risk, with the fastest time-to-value and lower total cost of ownership. 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