Guardicore

SOLUTION BRIEF
Guardicore + Medigate

Zero Trust Enabled Ransomware Mitigation for Healthcare Environments

Healthcare Security Landscape

The networks that healthcare organizations depend on are an increasingly complex maze of applications, sensitive data, and sensors. Interconnectivity through sensor-rich devices improves the patient experience and facilitates the collection of valuable data for healthcare providers. Chasing these benefits has produced enormous numbers of devices that need to be secured, with nearly 16 billion IoT devices expected to be in service worldwide by 2025. But many of these sensors are not currently visible to network administrators, making it more challenging to visualize communication flows and minimize the attack surface.

IoT devices are often used as an attack vector much like traditional endpoints. However, even next-gen endpoint security cannot properly see and secure an IoT device. This results in expansive blind spots and vulnerabilities. Medigate solves this problem with an IoT-focused solution that discovers and fingerprints all connected assets, including unmanaged medical devices (IoMT). The solution creates and maintains a data-rich, dynamically risk-scored inventory in near real time. Missing patches and other vulnerabilities are continuously detected and highlighted for action.

> ***Medigate's comprehensive IoMT security capabilities paired with Guardicore's microsegmentation platform create a robust Clinical Zero Trust solution.***

MEDIGATE by Claroty

KEY BENEFITS

Enhanced Device Discovery
Medigate accurately identifies and discovers all IoT/IoMT devices to generate a centralized, dynamic and mapped asset inventory.

Deep Device Security Insights
Effective vulnerability management and threat processing requires a deep understanding of the connected landscape. Detailed device attribution and knowledge of authorized device behavior is essential to detect unauthorized, anomalous behavior.

Limit Lateral Movement
Leveraging comprehensive device information and risk scores from Medigate, Guardicore can segment your environment and reduce unnecessary connections. Intelligent ransomware detection combined with comprehensive microsegmentation capabilities produce a combined solution that is highly effective at blocking lateral movement and scaling defenses.

Real-Time and Historical Views
Simplify your view of complex connected environments by having access to the right data, delivered in full context to the right workflows at the right time. Historical analytics are, therefore, made meaningful.

Visualize and Control your Connected Device Landscape with Guardicore and Medigate

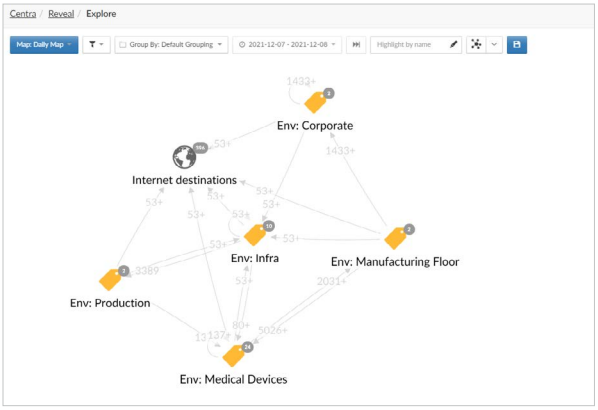
Creating segmentation policies that make sense, are agile, and can enable the security requirements of your unique environment requires hyper-detailed visibility to the assets that connect to your networks. With this in place, effective segmentation strategies can be created, and implementation projects can be accurately scoped and executed. Using the Guardicore platform, which draws device classification, and risk score information from Medigate, you'll be able to significantly reduce your attack surface by eliminating unnecessary communication flows.

KEY FEATURES

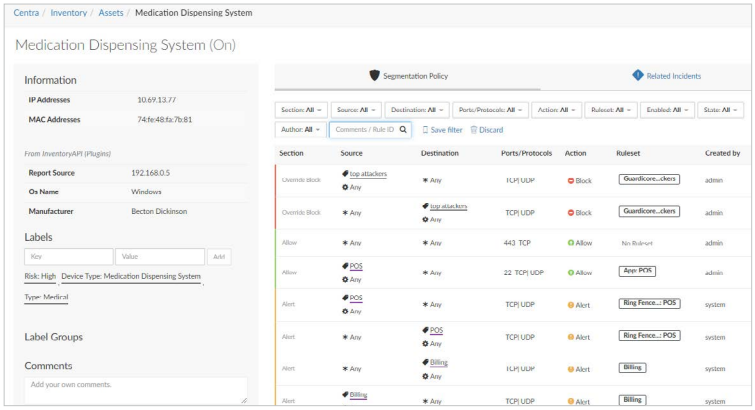
- Medigate-created and maintained device profiles, including attributes such as OS, App versions, risk score and location, are passed and mapped to Guardicore's asset database.
- Medigate detections of anomalous behavior are aggregated and reported to improve overall mitigation and remediation response effectiveness.
- Medigate-created security policy recommendations are used for testing and enforcement.
- Using Guardicore's policy orchestration engine, segmentation policies can be modified and/or adapted, as required, to meet the needs of operations and the various IT infrastructures of the Health System.

With fewer possible attack vectors in your network, it becomes much easier to see potential breaches as they occur and respond effectively. Questions related to healthcare data privacy compliance can be answered with all the underlying details in hand. For example, additional security measures can be taken by ring-fencing critical applications that traffic sensitive patient data.

Despite the rapid growth in IoT devices --and the risks they pose when connecting to your networks-- the pairing of Guardicore and Medigate is powerful. Our combined solution provides state-of-the-art visibility and network controls.



IoT devices, traffic patterns, and connections are clearly illustrated in Guardicore's Reveal map.



Manage your entire segmentation policy, view important IoT asset details, and review security alerts in Guardicore.

Protection across any complex environment.

Guardicore.com

About Guardicore
Guardicore delivers easy-to-use Zero Trust network segmentation to security practitioners across the globe. Our mission is to minimize the effects of high-impact breaches, like ransomware, while protecting the critical assets at the heart of your network. We shut down adversarial lateral movement, fast. From bare metal to virtual machines and containers, Guardicore has you covered across your endpoints, data centers and the cloud. Our software-based platform helps you become more secure to enable your organization's digital transformation.