MEDIGATE by Claroty

cisco Partner

Protecting Medical Devices and IoT with a Sustainable Clinical Zero Trust Strategy

Solution Overview

Healthcare is Changing, Security Must Change with It

The clinical networks of healthcare delivery organizations are rapidly evolving in order to support new care delivery models, consumer demands, and patient expectations. Security efforts need to evolve as well to ensure all the people, data, and devices within (and connected to) these clinical settings remain private and safe.

As the digital front door that consumers use to enter a health system expands, due in large part to the growth of telehealth, mobile services, and remote patient monitoring, so does the threat landscape that the health system must defend against. As the number and type of devices connecting in clinical settings increases due to the rapid adoption of IoT and IoMT, so does the number and type of threat vectors that the health system must monitor, manage, and secure. Ultimately, to deliver the kind of care communities now require, health systems are going to need to adapt and scale their security efforts to address the potential risks and improve healthcare for patients. Cisco and Medigate can help.

Medigate and Cisco Making Clinical Zero Trust a Reality

Cisco and Medigate are working together to help Health Delivery Organizations (HDOs) transform their cybersecurity posture to support greater productivity, lower risks, and ongoing compliance. It all starts with enabling HDOs to establish and maintain a Clinical Zero Trust (CZT) strategy, which applies the “trust nothing, verify everything” principle to clinical settings.

What is CZT? First, it's a strategy, not a technology; it’s a goal, not a specific feature or capability. No firewall, NAC, end-point security solution, or micro-segmentation product by itself constitutes a

solution. Rather, when deployed properly, they combine to create a CZT environment. The key difference between traditional zero trust and CZT is that CZT shifts the focus from devices and data to protecting the physical workflows involved in delivering connected care. At its core, CZT is about protecting physical processes, not just the specific devices or data involved. It's about protecting the care protocol and all its enabling constituents.

This requires tying the physical world to the cyber one to ensure when security is inserted, it does not disrupt care. Everything associated with administering a procedure or delivering care must be considered, so that controls can be implemented to defend the highest risk “attack surface” possible. These are the devices and processes in the physical world that must be allowed to operate unimpeded and uninterrupted to ensure no negative impact to the delivery of care. It takes deep healthcare expertise to be able to understand what each device is, how it works, what it needs to communicate with, and what workflows it is involved in, so that policies can be appropriately crafted and applied to address and contain any risks to operations or patient care.

Medigate and Cisco have joined efforts to deliver this level of converged operations by integrating Medigate’s healthcare cybersecurity expertise, insights, and services with Cisco’s segmentation strategy for medical device and IOT security. This is accomplished by leveraging Medigate’s Medical Device Security Platform (MDSP) plus Cisco Identity Services Engine (ISE) for policy enforcement. HDOs can further enhance their security posture with the addition of Cisco’s Trustsec and Software Defined Access (SD-Access) solutions. With these combined solutions, healthcare organizations can develop and implement a Zero Trust strategy that can handle the specific requirements of the clinical setting. As a result, health systems can ensure that security is integrated into the fabric and workflows of the environment in a way that protects, not interferes with, the integrity and availability of care. With Cisco and Medigate, healthcare organizations can make decisions and implement mitigation and remediation measures to precisely address the threats they are facing and securely enable the delivery of care.

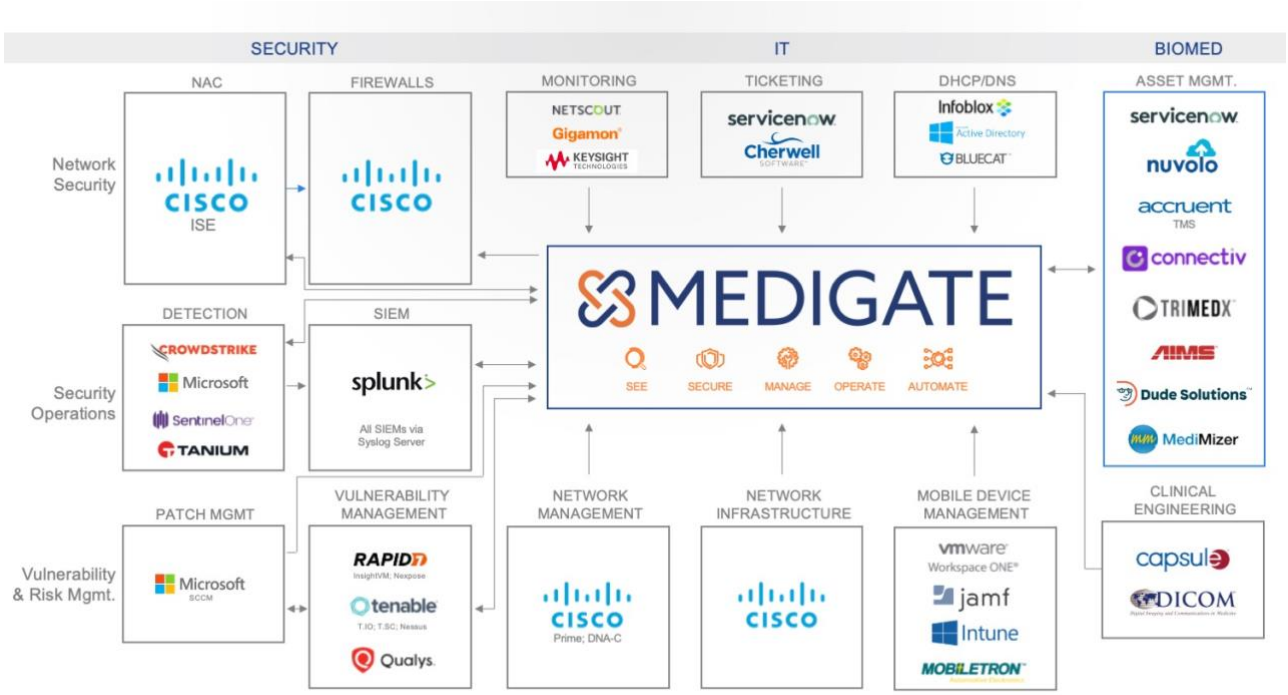
Benefits

- **Optimize the Availability and Delivery of Care** – apply clinical context to keep all connected medical, IoMT, and IoT devices operating as they should. Accurately identify high risk activity and swiftly address it to minimize any impact.

- **Operationalize Clinical Zero Trust Implementations** – automate information sharing and policy recommendations to implement effective segmentation and access control strategies that help mitigate risks and maintain continuity of care.

- **Confidently Adopt New Care Delivery Models** – extend care to meet consumer demands and patient expectations, while securing idelivery across the distributed health system's ecosystem.

How it Works --Convergence



The Converged Operations builds on the innovative network infrastructure that Cisco is known for. It utilizes policy functionality from the Cisco Identity Services Engine (ISE) to help organizations segment their network properly and deploy software-defined access that meets their clinical zero trust objectives. Medigate integrates with Cisco ISE, via APIs, to provide the detailed visibility and context required to make decisions on how best to protect the clinical network.

Medigate feeds Cisco ISE granular profiles that specify the manufacturer, model, device type, operating system, version, embedded software, protocols, etc. of the medical devices connecting to the clinical network. Medigate's sophisticated profiling and behavior analytics also detail the potential risk-level of each device to allow ISE to create and enforce clinically relevant, rule-based policies, as well as detect and take swift action against unsafe devices and activity.

Additionally, orchestration and network management utilizing Cisco's DNA Center simplifies the design, provisioning, policy creation and assurance of the network to help health systems work smarter and faster. In particular, healthcare organizations can use additional Cisco capabilities such as Endpoint Analytics, Trust Analytics, and Policy Analytics applications to apply insights into their endpoints and flows in order to hone their clinical zero trust deployment and implementation.

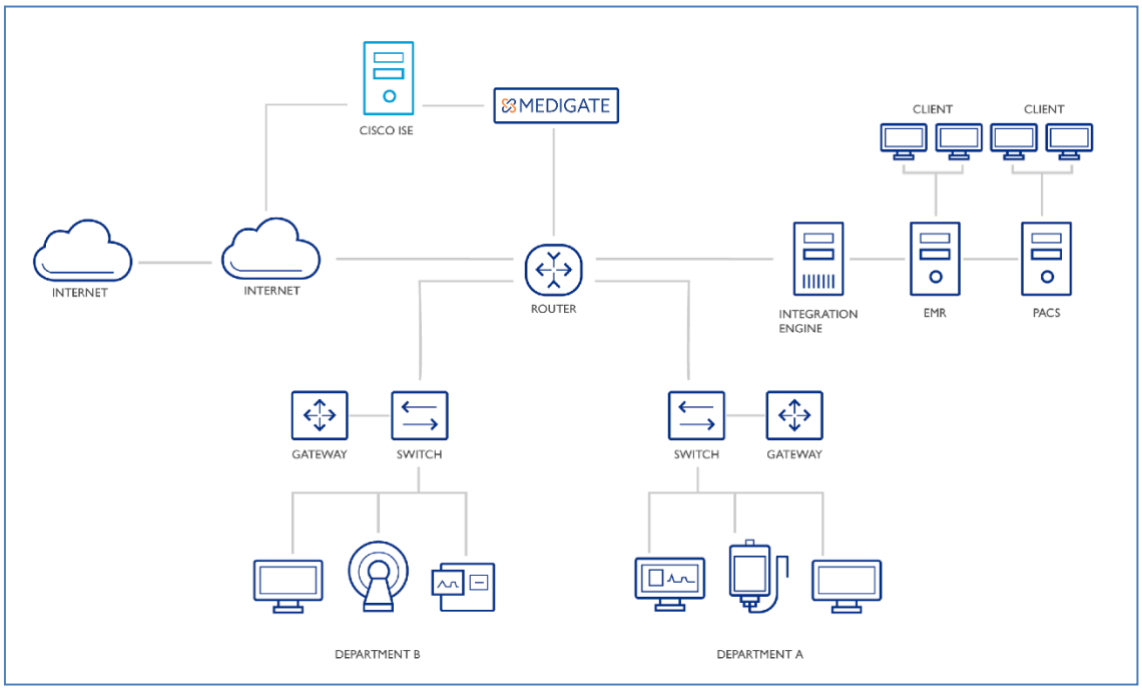
Information from the Cisco DNA Center flows back to Medigate to help refine device profiles and policy recommendations going forward. This ensures Cisco ISE can apply an intimate understanding of current clinical workflows to create the granular access control policies that know exactly when and why an action should be taken to protect the healthcare network.

Deployment

- A customer will deploy the Medigate Device Security Platform (MDSP) in their network.

- The Medigate platform will connect via pxGrid/ERS 2.2 APIs to the Cisco ISE platform to enable the sharing of contextual device attributes and relevant authorization policies between Medigate, Cisco ISE, and Cisco Security Technical Alliance solutions.

- Through the pxGrid/ERS APIs, Medigate will retrieve relevant session information to enrich its database and set optimized criteria for on-going data collection.



Use Cases

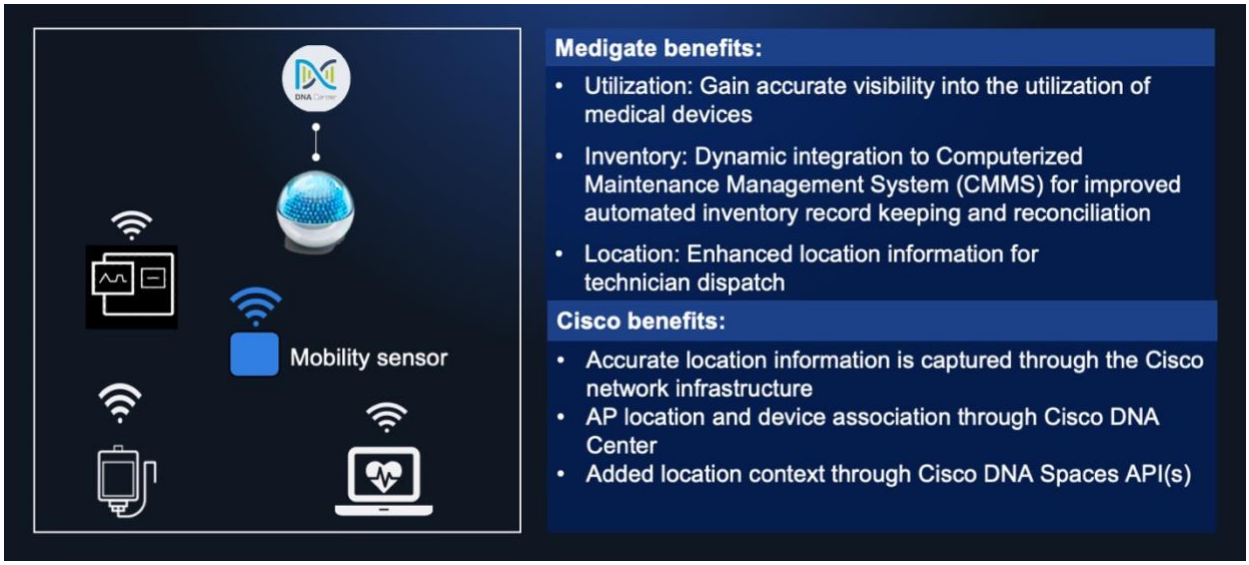
Medical Device and Healthcare Cybersecurity

Medigate applies its deep medical expertise to discover, fingerprint and analyze all medical and IoT devices and feeds this information to Cisco ISE for a much more complete and detailed inventory of all health system's assets. This includes devices behind a medical-device-terminal-server, which could have a number of devices (e.g., Ventilators) connected to it.

During the endpoint onboarding process, Cisco ISE is configured to pull in Medigate's device attribute detail so that it can automatically build and deploy prevention policies. Medical devices that are currently marked as generic or lack clinical context in ISE will automatically be enriched with Medigate's device details and clinically-aware policies.

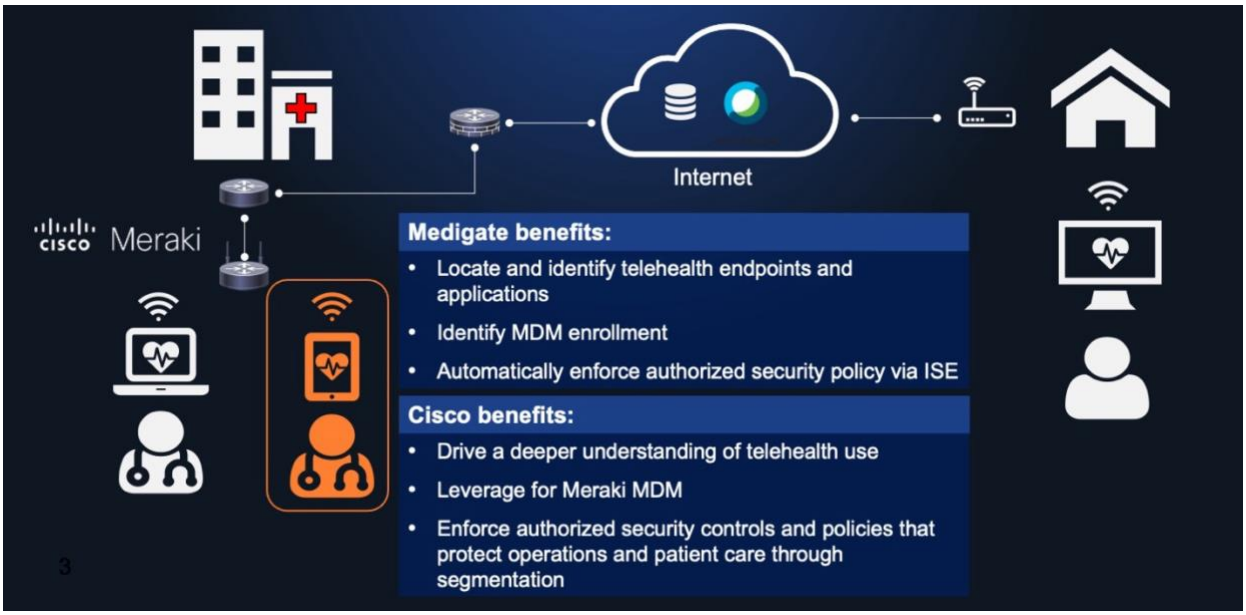
Location Services for Clinical Environments and Smart Hospitals

From a single dashboard, healthcare organizations can access detailed device information that will help them make better decisions around their assets. They can identify exactly what they have and where it is located to improve procurement, deployment, redeployment, maintenance, and end of life planning. For example, Cisco location data can be tied to Medigate's utilization data to illustrate device utilization per location within the healthcare system. This helps organizations improve their asset management and planning, allowing them to shift maintenance interventions from elapsed time to actual utilization and supporting more dynamic periodic automatic replenishment (PAR)-level management.



Telehealth Application and Mobile Device Management

Integrations and visibility into telehealth applications means healthcare organizations can better manage and enable their service delivery wherever it may be. Together, Medigate and Cisco can help health systems locate all the devices that are being used for telehealth and assess their security posture. For example, devices that are not currently being managed by the organization's mobile device management (MDM) solution can be identified, so that measures can be taken to address and prevent any possible exposure of health records or personally identifiable information (PII). Using Cisco Endpoint Analytics, healthcare organizations can dive deeper into the potential risks different devices pose and move quickly to apply controls and mitigating policies to protect their operations and care.



Protecting Patient Data

Cisco and Medigate have developed services designed to enable organizations to more efficiently protect their operations and patient data. Leveraging the combined power of Medigate and Cisco's ecosystem of security products (RTLS, Prime, MDM, ISE, Umbrella, etc.), the services enable accurate risk assessments of clinical networks, remediation based on clinically-aware, granular network policies (enforced via ISE), and ongoing monitoring and improvements to the health system's security stance via best practice playbook definitions.

The Value of Cisco Services

Healthcare organizations are under pressure to deliver value at a faster pace and scale, with fewer resources, increased complexity, and higher risk. Together with partners, Cisco Customer Experience (CX) delivers services to help you:

- **Optimize for today's healthcare challenges** with data-driven, actionable insights coupled with expert guidance to drive better access, engagement, and experience across the care continuum, without compromising security.

- **Prepare for tomorrow's healthcare changes** with resiliency and agility so you can adapt to the next normal, transform at the speed of change, and empower your teams to respond faster and more effectively.

- **Innovate for a healthcare future redefined** by reimagining the future of healthcare, using human and digital intelligence to create connected care facilities and ubiquitous digital experiences for patients and providers.

Cisco's Healthcare Security Segmentation Service for Medical Devices

- Provides advisory services for healthcare customers on how to minimize risk and liability caused by cyberattacks, protect critical business and patient operations, and prevent IoT device breaches.

Cisco and Medigate Assessment Tools: Improving Clinical and Operational Outcomes

Cisco INFRAM Maturity Readiness Services:

The **HIMSS Analytics Infrastructure Adoption Model (INFRAM)** helps healthcare leaders assess and map the technology infrastructure capabilities required to reach their facility's infrastructure goals—and meet international benchmarks and standards. The Infrastructure Adoption Model is an international eight stage (0-7) model for technology infrastructure adoption and maturity.

Cisco's INFRAM Maturity Readiness Services help healthcare providers to assess infrastructure adoption and capabilities maturity. By utilizing the INFRAM, providers can help improve care delivery, reduce cyber and infrastructure risk, and create a pathway for infrastructure development tied to business and clinical outcomes.

Medigate Real-Time Healthcare Convergence Assessment:

Medigate Real-Time Healthcare Convergence Assessment delivers an innovative customer self-assessment opportunity. It is an online survey that combines NIST security compliance questions with questions that reveal operational maturity/competency as detailed in Gartner's Real Time Health System (RTHS). The reporting exposes and prioritizes top areas of concern in the form of a security-operations gap analysis. It is already being used as a product and services roadmap that is relevant to Healthcare Information Technology (HIT) or Healthcare IT Management (HTM) and financial leadership.

For more information or to schedule a demo, email us at ContactCisco-Medigate@medigate.io.

About Medigate

Medigate provides award-winning cybersecurity for connected devices in hospitals. The platform combines a deep understanding of manufacturers' protocols and clinical workflows with cybersecurity expertise to deliver comprehensive and accurate identification, contextual anomaly detection, and clinical policy enforcement. The resulting automated, rule-based clinically-driven security policies keep patients, networks, and PHI safe.

MEDIGATE by Claroty

cisco Partner

Email: **contact@medigate.io**

Visit: **medigate.io**