INTEGRATION BRIEF

MEDIGATE COLLECTOR APP FOR CISCO CATALYST 9000 SERIES SWITCHES

Certified, rapid, cost-effective implementation for clinical environments

The Healthcare Cybersecurity Challenge

The multiplying number of devices within clinical networks coupled with increasing threats has created an urgency for healthcare delivery organizations to ensure they have visibility into device risk and protective measures to mitigate potential disruptions to patient care. According to the HIPAA Journal more than 80% of healthcare organizations experienced a cybersecurity attack targeting IoT devices over a 12-month period and the attacks jeopardize patient data, compromise safety, and put the health systems reputation at risk.

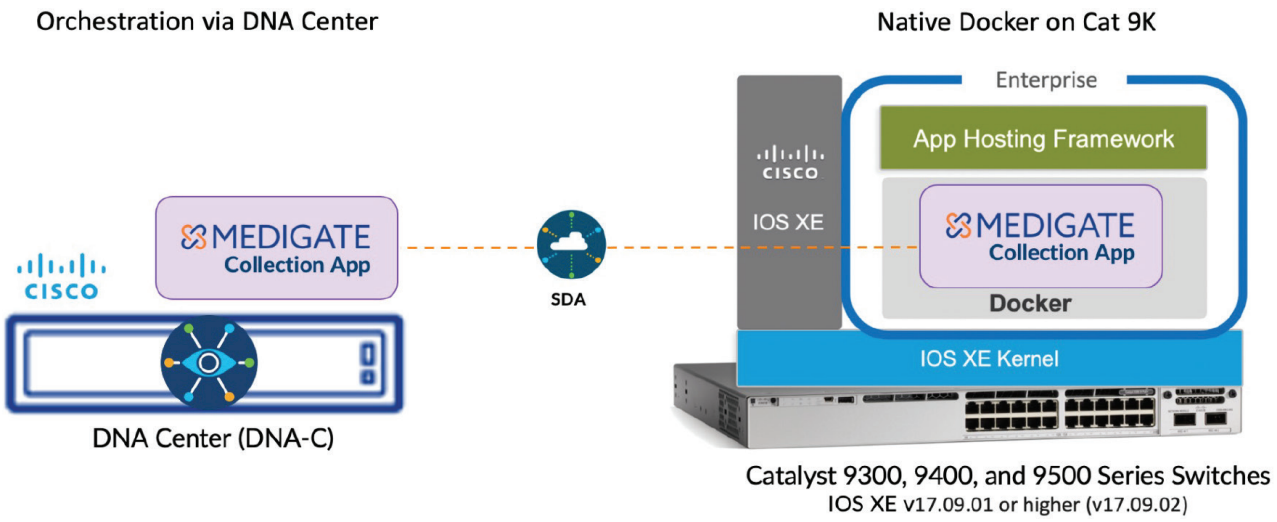
To protect themselves from cybersecurity threats, healthcare organizations need to accurately identify all the connected devices and effectively mitigate the threats. However, medical devices are not like general IT and gaining comprehensive, real-time visibility into these networked medical devices can be extremely challenging and has left many HDOs largely blind to potential security risks. Without enterprise-wide visibility and contextual insight, organizations are unable to protect their environments from cyber attacks and avoid disruptions. Medigate by Claroty and Cisco have teamed up to offer enterprise discovery, visibility, and network protection solutions for medical devices to address the challenges facing healthcare providers across the globe.

Highlights

- **Medical Device Discovery** and visibility into associated cybersecurity risks for all of your networked assets
- **Enterprise Scalability** via centrally managed deployment of Medigate's Collector Apps to Cisco Catalyst 9300-9500
- **Easy to Deploy Solution** with a small physical footprint, built to deploy on pre-existing hardware investments
- **Speed to Value Realization** from visibility into your device assets and cybersecurity risks enables faster progression to asset protection phase

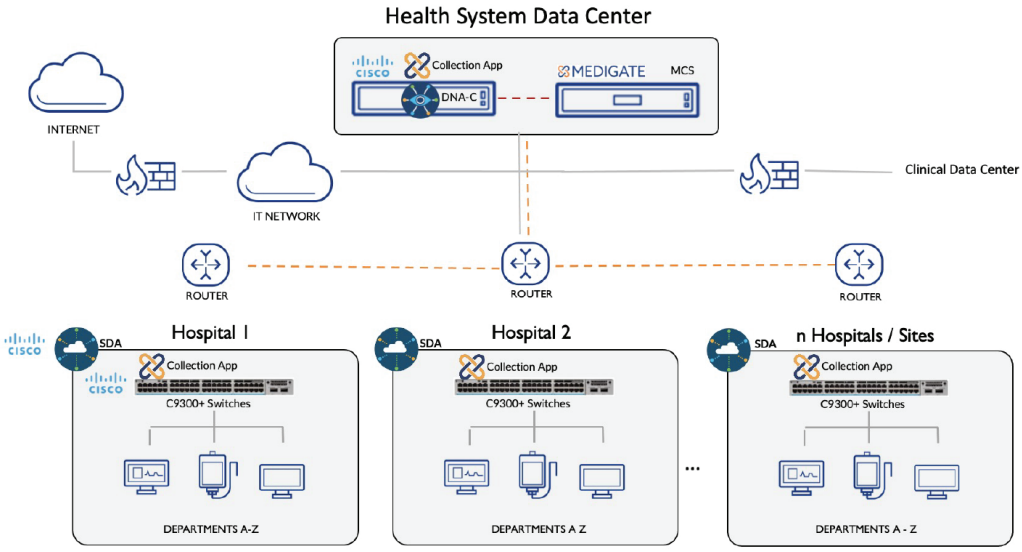
Integrated End-to-End Security

Medigate by Claroty utilizes the application hosting capabilities Cisco DNA-C alongside Catalyst 9000* series switches to host a Medigate Collection App instance - a lightweight Docker container app. Powered by an x86 CPU, the application hosting solution of Cisco Catalyst 9000 series switches provides the intelligence required at the edge. Administrators now have a platform for deploying Medigate Collector Apps leveraging their investment in Cisco Catalyst 9000 series switches as well as deploying their own tools and utilities, such as security agents, Internet of Things (IoT) sensors, and traffic monitoring agents on the same platform.



Cisco DNA-C managed deployment of Medigate Collector App on a Cisco Catalyst 9000Series switch

With the Medigate Collector Apps deployed on Catalyst 9000 series switches, a collection server captures, filters, and parses a healthcare provider's raw network traffic to provide asset visibility and monitor for vulnerabilities and risks. Wherever Cisco switches are already installed, Medigate can extend its sensors and broaden the HDOs cybersecurity coverage. This innovation provides a much quicker, easier deployment with less effort, saving time and reducing costs. In remote locations where deploying a separate sensor was not possible, Medigate by Claroty customers can now vastly improve visibility. No matter the location, the Cisco Catalyst 9000 series and Medigate by Claroty solution provides the necessary context for network segmentation, powerful coverage of "East-West" traffic, and monitoring of "North-South" communications across boundaries.



Cisco DNA-C managed multi-site deployment of Medigate Collector App for speed to value-realization

To learn more, visit claroty.com/healthcare-cybersecurity/medigate