CDI, Medigate, Cisco and Rapid7 Raise the Bar on Remote Asset Management & Cybersecurity

Executive Summary

Center for Diagnostic Imaging (CDI) is one of the nation's leading providers of high-quality diagnostic imaging and interventional radiology services. With more than 130 outpatient imaging clinics and more than 150 mobile MRI, CT and PET/CT units, CDI has been creating thriving partnerships with radiologists, specialty groups, hospitals, and health care systems to deliver best-in-class imaging solutions.

CDI is also an advanced user of connected asset management and cybersecurity technologies. Its ecosystem includes Rapid7 for Vulnerability Management (VM) and Cisco ISE for Network Access Control (NAC). CDI selected Medigate to scale its medical device management capabilities, improve its returns on assets and, via integrations to the aforementioned, unify its security ecosystem. Through a synchronized, common data foundation, those objectives were achieved ahead of schedule. New, value-adding use-cases continue to be implemented, further distinguishing CDI's leadership.

Challenge

Organizing remote asset and security management processes across a geographically diverse, mobile, and dynamic environment presented numerous challenges including:

CDI
DIAGNOSTIC IMAGING®

Company:

Center for Diagnostic Imaging

Industry:

Healthcare-Imaging

Number of Locations:

>280

Website:

https://www.mycdi.com/

- Establishing and maintaining an accurate inventory of assets;
- Scaling effective maintenance and remediation processes;
- Improving collaborations with biomed and finance partners;
- Standardizing asset performance reporting.

Solution

Medigate secured access to traffic flows across the CDI network. As a result, an accurate, dynamic, and fully attributed inventory of all CDI connected assets was quickly established. In addition:

- All CDI connected assets are now dynamically risk scored.
- An integrated maintenance and security program enabling instant identification of vulnerabilities and correlations of new threats was created.
- Device utilization data detailing asset performance are now being used to improve capital planning and validate performance to clients. The data are also being used to improve allocations of company-owned and client-side resources.

Results

As stated, CDI's asset management and cybersecurity capabilities are well-developed. For example, CDI's Cisco ISE design is sophisticated and for vulnerability scanning, CDI is an expert user of Rapid7. That said, as CDI leadership became aware of Medigate's meaningful integrations with these solutions, powerful enhancements were identified, and project scope increased:

- Because Medigate's integration to Rapid7 is bi-directional, CDI is now able to orchestrate identity-based scanning in a richer, clinically relevant context. Scanning operations are now safer, maintenance coordination has been improved, and asset uptime/availability has been increased.

- Medigate sends device profiles to Cisco ISE and updates them dynamically. It also automatically creates and delivers device-specific and group-defined security policies. To close the security enforcement loop, Medigate combines device profiles, device group communication requirements and security policies to apply Security Group Tags (SGTs).

MEDIGATE

Get in touch

Email: contact@medigate.io
Visit: medigate.io