MEDIGATE

Medigate Integration Overview

Medigate has taken clinical visibility to entirely new levels. Having transformed the state-of-the-art in Deep Packet Inspection (DPI), the company's ability to passively extract device-specific configuration parameters, as well as posture and utilization details, is unmatched. Demand for how Medigate orchestrates the resulting data has not only driven relationships with the nation's largest health systems but also integration partnerships that span the entire cybersecurity ecosystem.

Medigate understands that effective cybersecurity program development requires a layered, multidisciplinary approach. Therefore, a common data-foundation is needed. Medigate is delivering that reference architecture through meaningful integrations that enhance the productivity of established, cross-functional workflows. In doing so, it provides health systems an organic, non-disruptive way to address the problem.

By capturing and orchestrating long-missing information to the people and systems that directly benefit; and by incorporating certain aspects of good cybersecurity practice into their enhanced workflows, Medigate and its partners help health systems of all sizes streamline their development of future-proof defenses.

Firewalls

Medigate compiles the configuration details of every connected device and creates an "enriched tag" that is then matched to each device IP address. In concert with its library of clinical device functional profiles, including the internal/external connections that each device requires to perform its respective mission, Medigate has created a "security policy engine" and integrated its capabilities to the market's leading firewall systems.

To be clear, Medigate has developed and maintains a comprehensive library of firewall rules. Think of them as baseline rule-sets fully informed by the manufacturer's operating dictates for each device, inclusive of functional requirements and recommended workflows. These rule-sets can be applied as is, edited and/or appended based on the requirements of the health system.

As Medigate is able to track device IP addresses and match them to the enriched identification tags in the firewall, accurate firewall/device matching is ensured. Through that same integration, Medigate delivers administrators a way to access this information in the firewall dashboard within the constructs of their existing workflows. In other words, Medigate is not introducing a new learning curve. Rather, it is enabling the firewall to perform as intended, which is why Medigate is partnered with all of the market's leading vendors.

Medigate's ability to alert in real-time on device- and communication-specific anomalies reduces false positives, enabling the adaptive security controls long sought by firewall administrators. Furthermore, Medigate's tagging mechanism opens up a new world of security policy management possibilities, including tag-to-tag traffic controls, controls by network zones, port and protocol segmentation, and a wide range of naturally derived zero-trust policy options, based on a level of visibility that powers safe, contextualized management of device connections/communication flows.

Network Access Control (NAC)

Most Network Access Control (NAC) problems are directly traceable to the lack of clinical visibility described in this paper. And it's not necessarily the fault of NAC, as many IoT and IoMT devices were not designed to be network-managed in the first place. Especially with medical equipment, where active scanning is often not a viable option, NACs have not been able to capture device information at the level of detail required to satisfy their mission.

The objective here is to facilitate policy-driven network segmentation and policy enforcement via far more intelligent and adaptable implementations of NAC. So, in much the same way that Medigate supports firewalls, its policy engine generates Dynamic Access Control Lists (dACLs) for every device. Again, these dACLs are presented to administrators in the NAC dashboard, allowing ready approval, editing, application, etc., from existing workflows.

As Medigate tracks all device communications, it is able to detect any unauthorized internal or external access/connection attempts and close the loop by delivering detailed alerts that trigger appropriate NAC action/response. With Medigate, the power of NAC is delivered to all devices connected to clinical networks. In addition, it provides far more granular control of authentication processes, superior segmentation designs, and the ability to manage network resources based on device-type and changing risk levels.

Medigate and its NAC partners have exercised this integration model in support of some of the largest, most successful NAC implementations in healthcare. In other words, the company's experience is real-world, ongoing, and highly referencable.

Vulnerability Management (VM)

When full clinical device details and vulnerability feeds are married, a process can be quickly developed to tell the scanning administrator what kinds of scans are safe for different classes of devices and when they should take place. But that is only the beginning.

Medigate combines vulnerabilities detected by the VM solution(s), live threat intelligence feeds, and CVEs released by the device manufacturers. And because Medigate automatically provides a high level, rationalized device categorization (e.g. medical IoT, clinical IoT, general IoT and facilities-based IoT), healthcare providers can then execute sub-category-based remediation and mitigation programs knowing that when a threat is discovered, it will be instantly correlated to the potentially affected devices in their environments.

As Healthcare Technology Management (HTM) professionals play a significant role in vulnerability management, Medigate is also integrated with computerized maintenance and management systems (CMMS) platforms. These integrations cover commercial systems that are used by health systems directly and/or used by the maintenance organizations often hired to perform patching and update functions.

Medigate and its VM partners delivers health systems an intelligent and safe process that is based on real time, asset management capability. When factoring in all applicable risk data and correlating a score for every connected device, patching and maintenance prioritization is finally taken to a new, practicable level.

SIEM

Medigate integrates with security incident and event management (SIEM) platforms to provide health systems a way to implement custom, clinically-relevant detection and incident response strategies. Medigate-detected deviations from the functional behaviors and clinical workflows defined by the device manufacturer, and/or authorized by the health system, are fed by Medigate into the SIEM. The SIEM isn't just alerted, but provided the details its administrators require to target their investigations and remediation activities.

"What if" scenario-based analyses are supported and often used to enable playbook development. Medigate regularly hosts client workshops for this specific purpose. Because we see it as a best practice, we are working with our SIEM partners to ensure that device-specific incident response playbooks can be developed and integrated programmatically.

Ticketing

Once again, Medigate's integration to the market's leading trouble-ticketing systems delivers the intelligence that's been missing to traditional ticketing workflows. Naturally, the integration allows each system and/or respective system user(s) to create tickets. However, as Medigate is continuously monitoring both network communications and device performance, alerts can now be configured to "trigger" the auto-creation and routing of a ticket. Furthermore, as Medigate has eliminated the blind spots, including device utilization posture, remediation workflows can be safely executed and rationally coordinated.

Bottom line, when software updates are announced, or security risks become known, or suspicious communications are detected, trouble tickets are now created that contain all the previously missing context. And finally, as remediation steps are taken and/or trouble tickets are eventually closed, the records-database in both systems are updated/synchronized accordingly.

Takeaway

"Turning the lights on" is one popular way of expressing the value of clinical visibility. However, as this paper describes, unless that visibility is of high definition, the ability to effectively secure clinical networks remains severely hamstrung. Simply put, the ripple effects of data quality cannot be overstated. Up or down, data quality determines the value of system integrations and the resulting synergies that ultimately drive the ecosystem.

Cybersecurity is a team sport. Therefore, a common data foundation, or reference architecture, is required. Medigate supports the team-based collaborations required by orchestrating the on-time delivery of the right data to the right, existing workflows via integrations across the entire ecosystem. By doing so in ways that enhance staff expertise and improves cross-operational performance in ways that address clinical hygiene, Medigate and its partners deliver health systems layered, sustainable pathways to secure clinical networks.

Author's Note: *The list of integrations described in this paper is by no means exhaustive. For example, integrations to Computerized Maintenance Management Systems (CMMS) were mentioned in passing, and Wireless Management Systems (WMS) come to mind. With respect to WMS, Medigate extracts data that helps pinpoint the location of wireless connected devices. For CMMS, Medigate transforms an otherwise static database into a dynamic system of record. Both integrations are among Medigate's most popular, as they have been implemented by the vast majority of its health system clients. Additional information on these and other integrations are available under "Resources" @ www.medigate.io.*