MEDIGATE

A Clinical Use-Case Driven Approach to a Comprehensive Cybersecurity Program Development

Solutions to healthcare's IoT asset management and cybersecurity problems require non-traditional, multidisciplinary collaborations. To that end, Medigate continues to organize its platform around a complement of security-enhanced use-cases that leverage a common data foundation. Each Medigate use-case is developed with the following objectives in mind:

- **Cross-Functional Clinical Relevance.** Whether to benefit a traditional stakeholder group (e.g. IT Security, BioMed, Clinical Engineering, Supply Chain, Finance) or the converging practices of cross-functional teams, Medigate's approach ensures clinical relevance. Our philosophy extends to contributing systems (e.g. CMMS, NAC, Firewalls, SIEM, etc.) and the administrative workflows of those systems.
- **Natural Workflow Enhancements.** Medigate concentrates its development efforts on making staff and systems more coordinated and productive at what they already do. Medigate's use-case-centric approach incorporates relevant, naturally adopted security practices into logically connected/converging workflows. The benefits of scale can be achieved with minimal change management.
- **Operational Leverage.** A functionally-integrated approach requires a common data foundation. Medigate manages the capture, enrichment, and orchestration of long-missing data to improve existing workflows and automate outdated routines, as it allows users and use-cases to connect and coordinate in ways that create operational leverage.

Clinical Cyber Hygiene

Clinical Cyber Hygiene encompasses both the identification and remediation of clinical asset vulnerabilities. Although the management challenges are well-known, traditional methods are often disjointed, if not contentious.

Medigate uses Deep Packet Inspection (DPI) to obtain both unique and general identifiers for every device. For perspective, a fully profiled device may include as many as three dozen attributes. Medigate goes well past make, model, MAC and IP address and delivers serial numbers, location history, current status, firmware-level details, Operating System (OS), Application Versions and utilization metrics. Essentially, Medigate maintains a knowledge base of every device signature, including authorized workflows and operating requirements. This also allows us to effectively act as a real-time monitor at the device communication level. By combining all of this intelligence, existing device and network vulnerabilities can be instantly and accurately identified, as can newly published threats. They, too, can be instantly and accurately correlated to the client's environment.

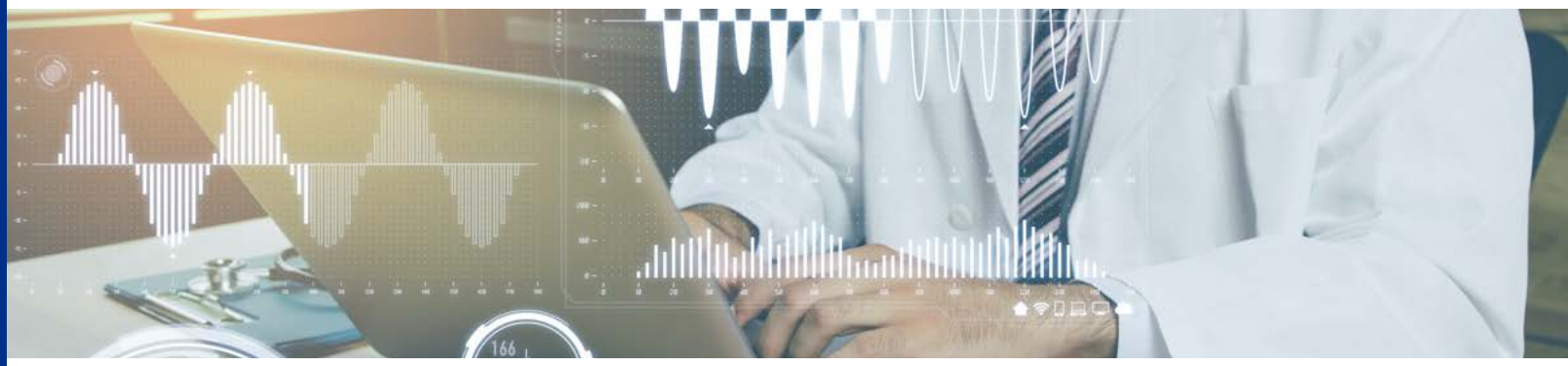
Every connected device receives a dynamic, multifactorial risk score. Beyond incorporating the aforementioned configuration, utilization and workflow intelligence, numerous other factors are taken into account. They include internal/external network connection-types, FDA Class, whether the device stores/transmits PHI/PII, VLAN composition, consequence of failure to patients and operational costs (if the device must be taken out of service). Medigate uses AAMI's Risk Management Technical Information Report along with risk assessment processes and standards prescribed by the FDA, ECRI, ISO and NIST.

Fusing these standards with our extensive research into the operating requirements of each device, we have developed a clinically-relevant risk scoring process. And it is practical. Five well-defined grades that characterize risk criticality and prioritize it are provided. And when requested, the risk scoring preferences of our provider-clients can also be factored-in on a custom basis.

Although active scanning solutions can provide insights that lead to the reduction of cyber risks, Medigate understands that they can also introduce operational risks. The potential danger to patients is of genuine concern, which is why many device manufacturers will void their warranties if active scanners or agents are used. And the problems aren't limited to medical devices, or to other clinical devices that may store and/or transmit PHI. The problems manifest across several device classes. Medigate has addressed these problems via meaningful integrations with the industry's leading vulnerability management (VM) solutions.

When relevant clinical device details and vulnerability feeds are married, a symbiotic process can be quickly developed that enables the scanning administrator to understand what kinds of scans are safe for different classes of devices and when those scans should take place. When armed with a device's true fingerprint, meaning all operating and configuration-specifics, approved update/patch availability, device status/readiness, security posture, and even staff availability, VM scans can be appropriately configured and safely targeted. By coordinating all remediation steps/processes, comprehensive audit trails can be recorded, centrally stored and easily referenced.

Medigate's integrations to Computerized Maintenance and Management Systems (CMMS) are also highly meaningful. Essentially, we transform a relatively static inventory capability into a real-time, dynamic system of record, providing yet another relevant point of reference. Whether leveraging existing client infrastructure or enabling effective third party collaborations (e.g. organizations trusted to perform the patching and update functions required), Medigate is well down this path. To be clear, Medigate is not simply "connected" or "interfaced" with the market's leading CMMS solutions. We are not simply "exchanging data via APIs." We have built market-leading partnerships on the back of meaningful integrations engineered to eliminate these business problems, regardless of where the device may be deployed.



For example, remote patient monitoring (RPM) devices transmitting to health system EHRs are covered. Medigate also identifies the telehealth applications being used and determines whether the device/application combinations are authorized and properly detailed in the provider's Mobile Device Management (MDM) system. Because our DPI skill-sets are core and directly applicable, we have been ultra-responsive to client requests and already released our first telehealth use cases. And based on their continued feedback, many more are currently under development. Notably, demand for telehealth support is exposing competitor deficiencies, as their statistical models (e.g. AI/machine-learning) rely on historical data inputs and correlations that don't yet exist.

In summary, Medigate is not introducing new, uncharted goals to already overworked teams. Rather, we are providing a long-missing, common data foundation and responsible levels of automation. Our approach logically connects cross-functional teams and creates leverage by coordinating existing inventory and vulnerability management practices. The result is a continuous process for improving clinical cyber hygiene.

Key Solution Components:

Auto-generated remediation recommendations. Because the security posture of every device is known in extensive detail, Medigate compiles and auto-generates, step-wise, device-specific remediation instructions, complete with all relevant supporting documentation. Implementing these steps automatically updates the device's dynamic risk score, which also feeds into aggregated risk reports that reflect organization-wide progress. For example, knowing which devices pose greater risk, security leadership can now introduce security criteria to procurement for use in supplier selection processes.

Risk Reporting. Medigate reporting clearly outlines the distribution of risk both internally (across departments) and externally (by device manufacturer). To continuously assess device risks, Medigate is constantly correlating such detail to known vulnerabilities (e.g. NIST NVD CVEs) and newly published threats from manufacturers and trusted security advisories (e.g. ICS-CERT). Finally, as Medigate data are fuel to systems throughout the ecosystem, the reporting capabilities of management and enforcement systems (e.g. CMMS, Firewalls, NAC, SIEM) are also dramatically enhanced.

Preventative Maintenance and Procurement Utilization Insights. Detailed utilization-based insights are provided, allowing virtually unlimited, data-driven device/system/operator performance comparisons. Notably, as utilization metrics are provided by device and/or device category, preventative maintenance (PM) scheduling can be based on actual usage, instead of time, and procurement managers can finally coordinate with BioMed to negotiate superior Service Level Agreements (SLAs). As captured utilization intelligence can be analyzed across a category, sub-category, at the device or fleet level, and even cross-category bundles, the potential financial benefits are hard to ignore, especially in an industry where average device utilization hovers around 50% and informed supplier negotiations can deliver double-digit purchase savings.

Clinical SOC

When cybersecurity incidents affecting medical devices occur today, SOC analysts are tasked with investigating the incident without adequate information. In most cases, the analyst lacks specific knowledge about device configuration parameters, whether the device is in patient-use, and what actions can be safely taken. In short, incident response playbooks are nearly impossible to develop because SOC analysts don't know what they're up against. Known-to-be-vulnerable devices cannot be protected with existing EPS (events-per-second) tools. Clinically-specialized visibility tools are required.

Medigate pinpoints a device's location, analyzes its current utilization, and both alerts and arms staff/systems with all the data required to efficiently remediate threats. By integrating this data with security incident and event management (SIEM) systems, SOC analysts can correlate IT alerts, medical security alerts and locally stored device logs in an intuitive, operative context, resulting in the ability to develop clinically-aware remediation playbooks.

Because the concepts are often confused, the acronyms SIEM and SOAR (security orchestration automation and response) tend to be used interchangeably. In fact, they are different. SIEM and SOAR have highly complementary capabilities that Medigate's "clinical SOC" is designed to optimize.

- SIEM attempts to make sense of event-related data generated by firewalls, intrusion detection systems and various network appliances. The problem is, SIEM solutions tend to produce more alerts than SecOps teams can manage. That's why machine learning, specialized analytics software and dedicated sensors are often used to try and make sense of it. But, for SIEM tools to work effectively, they require continuous tuning, generally obliging security analysts to spend more time on the tool itself, rather than triaging the data.
- SOAR addresses the problem. Consider it an integration "platform" for security automation. At its core, it establishes integration as a means to accommodate highly automated, complex incident response workflows. Put simply, it brings speed and scale to the equation, resulting in a far more practical and adaptive defense capability. An essential benefit to SOC is that it automates outdated routines like opening a trouble ticket, thereby freeing up resources to actually work on the problem. For example, in terms of managing device posture, Medigate automatically provisions CMDB and CMMS with trouble tickets and assigns them.

The Clinical SOC supports the following automated detection and response process frameworks:

Device Posture Alerts

- **Alert:** e.g. Outdated Firmware Vulnerability
- **Verify:** Determine if the device is in use
- **Scan:** Scan device with custom/appropriate lightweight scanner
- **Profile:** Update risk and populate device profile including vulnerabilities in CMMS
- **Ticket:** Create a work order in CMMS and a ticket or, record outreach if the patch is unavailable
- **Patch:** Automatically patch where possible (workstations, dispensing systems)

Network Posture Alerts

- **Alert:** Medigate suspicious/malicious traffic alert
- **Correlate:** Correlate with Medigate's clinical vulnerability alert
- **Collect 1:** Collect logs from endpoints, network equipment, firewalls
- **Collect 2:** Collect logs from medical devices
- **Record:** Record network data captures of the compromised device
- **Verify:** check to see if the device is in-use
- **Act:** Push ACL / Block / Isolate if applicable

In summary, unlike generic SOCs, a clinical SOC ensures relevance throughout the incident response (IR) process. Stakeholders of varied expertise can be presented with findings that make sense to them and justify their involvement. We facilitate effective vulnerability scanning by informing administrators when it is safe to scan and alert based on confirmed, suspicious activity. At the network level, Medigate enables correlations between IT/IS and clinical alerts. And because we automatically capture logs and traffic from medical devices exhibiting anomalous behavior, playbooks for medical devices can be confidently created and applied. Importantly, the automation Medigate provides also extends to relevant notifications from manufacturers, including patching for clinical endpoints, if/when appropriate. And because we automatically propagate CMMS and CMDB with detailed profiles of all connected assets, Medigate is able to generate a detailed ticket for every alert, assign it, provide device-specific remediation instructions and verify case-closure.

Key Solution Components:

Comprehensive IoT risk assessments on a continuous basis. Medigate has given new meaning to clinical network visibility. Our device profiles are comprehensive. Using deep packet inspection (DPI) to discover, fingerprint and maintain a dynamic inventory of all connected assets, Medigate research further enriches this foundation with authorized workflow details and clinical context. Based on our precise understanding of the device, its intended behavior and utilization, Medigate is able to provide the generic SOC with a clinical context, enabling far superior detection and response processes. Beyond providing comprehensive device-specific attribution, additional identifiers such as VLAN assignment, utilization metrics and authorized workflow requisites are presented in the appropriate context.

Alerts on deviations from manufacturer-intended device behaviors and client-approved clinical workflows. All connected asset profiles, including authorized device-specific communication mappings, are fed into the client's SIEM. The SIEM becomes an aggregator/integrator of correlated threats from all available, trusted sources. Now armed with the missing device and workflow data, security analysts gain a system capable of instant, targeted investigations and finally, reliable baselines against which incident response (IR) programs can be developed.

Massive reduction in false negatives and positives. Unlike generic SOCs, the clinical SOC ensures clinically-relevant context throughout the entire IR process. Finally, healthcare organizations can know exactly what various findings mean to the security of their operations. Combining device profile data with a precise understanding of each device's authorized behavior not only means anomalies can be accurately correlated and prioritized for remediation, but also, it allows analysts to trace the potential attack vector from end-to-end. And finally, by enabling the creation of IR playbooks directly on the SIEM platform, Medigate has made it easy for healthcare organizations to proactively assign, track and justify work orders.

Clinical Policy Enforcement

Clinical policy enforcement inevitably leads to discussions around network segmentation and how best to virtually map strategically-considered segments onto existing networks. Although the security rationale for pursuing segmentation is widely accepted and well understood, projects aimed at achieving dynamic segmentation continue to flounder. Put simply, if knowing what's on your network remains a challenge, then the ability to create and enforce security policies can't even be considered.

Because many IoT and IoMT devices were not designed to be network-managed in the first place, many go undiscovered when attempts to establish/update inventories are made. Network Access Control systems (NACs) do not store all the required device signatures and they aren't designed to capture changing configurations at the required levels of detail.

Meeting this challenge requires deep knowledge and continuous monitoring of every device, meaning dynamic profiling capability combined with a detailed understanding of what each device needs to perform its respective mission. Updated views of device risk that are based on profile, clinical relevance, workflow and networking requirements are also required. In other words, the entire clinical context of a connected endpoint should be available when defining its security policy.

As said, the data required to accomplish this haven't been available and that's why segmentation projects continue to stall. Although high level and known considerations (e.g. geography, existing networking tiers) are still used to rationalize how network segments are initially defined, health systems now know that more comprehensive segmentation criteria are what's needed. Provider IT security professionals not only know this but, they now realize that trade-offs resulting in the implementation of more blunt, generic access controls can make matters worse.

The implementation of network segmentation can be achieved through a security-focused redesign that may not require significant further investment in infrastructure. By grouping device types and users in a clinical context and only permitting access to the networked resources each requires to perform their respective mission(s), intelligent, agile zoning via network segmentation can finally happen.

Medigate's breakthroughs in clinical network visibility are finally providing health systems the confidence they need to effectively pursue all the benefits of segmentation. Because we continuously maintain the data, clinically-vetted security policies can be safely auto-generated for each device and provided in an intuitive matrix that not only shows authorized communications per device but authorized connections relative to other devices, systems and segments. Through meaningful integrations, this policy information can be mapped directly to NAC enforcement mechanisms.

In short, clinical networking professionals are learning that a more informed, adaptable approach has benefits that include:

- fewer policies to create
- policies that can be centrally managed
- policies that are clinically relevant
- policies that can adapt regardless of changes to infrastructure
- higher-performing networks

Our innovations have reduced segmentation project cycles by 10X. To be clear, the completeness of the visibility we provide is a game-changer. Medigate enablement of NAC is so profound that it begs questions around how segmentation practice ever happened without it.

Key Solution Components:

Automated device security policy creation. Through the industry's first "security policy engine," Medigate automatically provides clinically-vetted, device-specific dACLs directly to the NAC administrator's dashboard (we also auto-generate rules-sets for firewalls). Our library of dACLs is continuously improved via our dedicated research and community intelligence gained through partnerships with provider-clients and manufacturers.

Network-wide communication matrix. In addition to auto-generating device-specific dACLs, we have evolved our capabilities to also present them in a network-wide communication matrix. In this view, all device policies relative to each other are displayed. The matrix maps directly to the simulation and enforcement mechanisms used by all of the market's leading NAC vendors, providing a coordinated and comprehensive "picture" of both policy recommendations and enforcement. Medigate has several operationalized implementations under our belt and always encourages solution evaluators to investigate them, as IoT cybersecurity vendors are highly differentiated on this count.

Visibility 3.0. Although segmentation projects are challenging and will remain so, when attacked on a step-wise, category-focused basis, they can be accomplished in a fraction of the time traditionally allocated. Of course, the key to effective segmentation is the right kind of visibility. Not an incremental perspective that may eliminate certain tradeoffs, but comprehensive intelligence capable of powering a direct, no-regrets approach. Put simply, Medigate has redefined clinical network visibility. By eliminating visibility constraints, we have opened minds to entirely new practice possibilities.

Clinical Asset Management

Given exploding numbers of connected assets, coupled with utilization rates hovering between 40-60 percent, not only is current asset management practice more challenging than ever, but a purchasing mess has emerged. Without knowledge of asset status, location and utilization, preventative maintenance is more reactive than ever, and purchase requests cannot be objectively justified. And given the advent of telehealth, further complexities are being created.

To address the challenge, BioMed and Clinical Engineering teams tend to rely on Computerized Maintenance Management Systems (CMMS) as their main source of data. But current generation CMMS are largely static systems mostly driven by manual entries. These systems are not up to the task, especially when considering the following:

- increasing numbers of devices
- the dynamic nature of clinical networks
- confounding actions of manufacturers
- telehealth
- legacy equipment matters
- the nature of replenishment contracts
- the disparate maturity levels of the operators themselves

CMMS relies on manually generated snapshots of the connected landscape. Therefore, CMMS records tend to be error-prone and are almost never up to date. What's required is a continuously updated "movie," as manufacturer updates, including security patches, software revisions, etc., cannot be appropriately sequenced if there is little knowledge of the current status of the endpoint. While experienced BioMed and Clinical Engineering professionals can make positive strides based on disciplined onboarding processes, the improvements are short-lived, because clinical networks are far too dynamic. Among other reasons, that's why their workflows remain interrupt-driven, forcing tradeoffs that are far from ideal. Furthermore, as preventive maintenance scheduling is time-, rather than utilization-based, Service Level Agreements (SLAs) have little meaning when negotiated by procurement, as they cannot be enforced.

Based on such challenges, clinical asset management is often outsourced to third parties. Although these organizations bring staff and often use their own asset management tools (e.g. CMMS), their efforts and systems are not integrated with network security or the newly introduced complexities associated with telehealth. Rather, the promise here is about relieving the health system of its traditional, internal asset management headache. The goal is to make certain that in-house device availability and related maintenance problems don't negatively impact patient care. Despite not addressing any network security dimension, it's obviously important work. But, it's a service focused on managing problems versus a solution focused on eliminating them, which is why market-leading vendors are partnering with Medigate. Otherwise, problems resulting from the lack of a common data foundation persist. They are not addressed, but circumvented, with efficiencies gained accruing to the benefit of the service provider.

An integrated, leveraged approach based on a common data foundation is what's necessary. Regardless of where a device is located and who is performing the work, at a minimum, IT Security still needs MAC and IP address data, clinical engineering still needs serial numbers and configuration parameters, networking engineers must monitor communication behaviors/workflows and procurement wants to understand utilization. If the device is communicating to an EHR, where it is deployed cannot matter. If these and other evolving data needs are not continuously satisfied, the opportunity to drive operational improvements meant to fully safeguard patients and improve the care provider's bottomline cannot be achieved.

Key Solution Components:

A real-time, location-specified, comprehensive inventory. Medigate passively fingerprints and creates a real-time inventory of everything connected to hospital networks. As part of each device profile, definitive data from RTLS and other sources are combined to create a dynamic, location history. At the device- and network-level, when any configuration, status, or security posture change is detected, we update integrated systems accordingly (e.g. CMMS, MDM and SIEM). Through integration with CMMS and MDM, Medigate not only creates new records based on what it discovers but enriches existing entries with all the missing data it captures. We create a common, dynamic system of record that enables natural collaborations.

Detailed utilization intelligence. Medigate captures detailed utilization data to improve preventative maintenance (PM) and procurement effectiveness. The device utilization metrics captured by Medigate can be monetized in a variety of ways. Consider just the following opportunities resulting from the capture of this data:

- **Preventative Maintenance/Proactive Asset Management:** In addition to providing MDS2 documentation and allowing PM to be scheduled based on actual usage vs. time, Medigate is integrating with maintenance systems to provide rule-based automation and trigger periodic automatic replenishment (PAR). For example, Medigate is capturing:
  - Number of suppliers per device category
  - Device volume per supplier
  - Total procedural capacity is broken down by supplier/device type
  - Average utilization by supplier/device type, model, configuration
  - Risk profile by device type, model, configuration

- **Recall Management:** Recalls occur when a medical device is defective and/or when it could be a risk to patient health. But a recall doesn't always mean that the product cannot be used or must be returned to the manufacturer. Sometimes it means that the medical device needs to be checked, adjusted, or fixed. A manufacturer may be aware of a problem with a group of products but may be unable to predict which devices will be affected. To appropriately address this concern, the company may recall an entire lot, model, or product line. By managing recall information in much the same way that we manage an existing vulnerability or newly published threat, Medigate can add significant value to the current process. For example, Medigate can:
  - Identify the number of affected devices on the client's network
  - Determine the location of all affected devices
  - Determine the status of the device (in-use, online, offline)
  - Correlate any/all additional risks and problems
  - Send alert information to contract management systems tracking SLA terms and conditions
  - Send alert information in the form of pre-configured reports to identified systems (e.g. CMMS, trouble-ticket, ERP, requisitioning systems, inventory, fulfillment, etc.)
  - Provide an audit trail mechanism (i.e. evidence of action taken, close the loop)
  - Identify the location and posture of substantially equivalent devices that can be put into service until alternative devices can be accessed

- **Category-based Procurement Support:** While non-strategic areas of spend (i.e. "tail spend") may remain under the management of GPOs, many health systems now manage the more expensive, higher physician preference and strategic areas of their spend locally/directly. Medigate identifies the high volume, more expensive connected device types/categories on the health system's network. Medigate captures the following supporting data:
  - Volume of devices by manufacturer
  - Procedural capacity by manufacturer
  - Average utilization by manufacturer and/or across a fleet, broken down by model variants, configuration differences and risk profile differences, by groups (if any)

- **"Deep Utilization" Metrics for Imaging Devices:** Beyond providing online-time and usage metrics for all connected devices, Medigate's analysis of image device utilization goes several steps further. Medigate leverages its DPI techniques to extract specific details from each scan, including identification of the operator, the part of the body scanned, number of scans per procedure and the duration of each scan. Such detail provides an added layer of analysis enabling benefits ranging from smarter patient scheduling to reducing variance at the workflow/procedural-level.

Medigate is transforming clinical asset management. The starting point is a real-time, dynamic and fully profiled inventory of all connected assets. Through integration, Medigate essentially turns static CMMS and MDM into real-time systems of record. By providing a common data foundation, Medigate is leveraging existing systems and workflows and breaking down barriers to valuable collaborations between biomed, clinical engineering, network engineering and procurement.

Takeaway

To enable operational improvements that benefit both patients and health system bottomlines, siloed thinking at both staff and system-levels is being systematically eliminated. The transformational benefits are widely accepted as highly available. In light of increasing risks and expenses, a more leveraged approach to asset management and cybersecurity practice has become an overnight priority. To make it happen, key workflow components of professionals across information technology, networking, security, HTM and procurement must become more functionally-integrated.

Medigate creates and continuously maintains the requisite, common data foundation. It has centered its platform on use cases that connect the right complement of asset management and cybersecurity workflows. Because the insights orchestrated by Medigate are made relevant to the respective interests of professionals whose practices are already converging, the underlying use cases are powerful and naturally adopted, allowing for the scaled delivery of best practices. The resulting operational improvements are quickly realized.

By operationalizing data flows to a more inclusive ecosystem, Medigate continues to embed clinically-relevant cybersecurity enhancements into multidisciplinary workflows. If the workflows don't exist, Medigate helps its clients implement them. When human resources are not available, or the client's technology constraints cannot be overcome, various managed service approaches are explored, even if only as stop-gaps. Medigate is committed to foundation-building and works with its partners to deliver effective hybrid approaches, as required.

When considering the variety of use-cases explored in this document, a fair question to ask is what additional data might Medigate be able to capture and utilize in the future? We will continue to answer this question in the form of use cases that we vigorously continue to develop, as we are dedicated to healthcare, we understand clinical networks and have no competing development or service agendas. And, we have meaningful partnerships with a provider-base spanning all sizes and specialties. Easily the largest, most reputable and fastest-growing healthcare footprint in this solution market.

Medigate is raising the organizational profile of its users by strengthening their respective ROI missions to the enterprise. The operational improvements they are driving are quantifiable and dramatic. Their success has fueled our success. Investment in the Medigate platform and the clinical network subject matter expertise we provide have been objectively justified. Based on what our clients say, the value of our partnership has been validated many times over.

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. Learn more.