MEDIGATE

WHITEPAPER

Medigate Aligns with the NIST Cybersecurity Framework

Healthcare Delivery Organizations rely on the continuous operations of their clinical networks to ensure patient care isn't interrupted. The explosion of inherently insecure medical devices being connected and the convergence of once siloed clinical networks is exposing them to an onslaught of cybersecurity threats that put their safety and reliability at risk.

The NIST Cybersecurity Framework was created to provide a set of standards, guidelines, and best practices to promote the protection of critical infrastructure and improve the management of cybersecurity risk. The Framework Core is a set of activities and desired outcomes encompassing the heart of an organization's cybersecurity strategy and risk management. All elements in the Framework Core are built around five concurrent functions, representing the primary pillars of a holistic cybersecurity program: Identify, Protect, Detect, Respond and Recover.

Medigate's IoT and IoMT device security platform directly aligns with three of the Framework Core's functions – Identify, Protect, and Detect. It embodies the security activities and policies the Framework encourages in order to move towards safer networks and improved risk management. Medigate's data, understanding of IoT and IoMT devices communications, and networking and cybersecurity expertise also indirectly contribute to Response and Recovery activities through the establishment of dedicated clinical incident response and recovery workflows.

IDENTIFY

Identify with Medigate

The Identify Function assists in developing an organizational understanding of managing cybersecurity risks associated with assets, data and people. Outcomes within this Function include:

- Identifying physical and software assets
- Identifying asset vulnerabilities
- Identifying internal and external threats
- Implementing a risk assessment methodology
- Establishing an organizational risk management strategy[1]

Medigate shares NIST's notion that security starts with visibility – you can't secure what you can't see. In line with NIST's vision of Cybersecurity Bill of Materials for all connected devices, Medigate uses Deep Packet Inspection (DPI) on passively collected network traffic to discover all connected IoT and IoMT devices and achieve a real-time, accurate asset inventory listing granular technical attributes such as OS, software and hardware versions, and serial numbers for each device.

Medigate also provides valuable risk assessment capabilities for hospitals through our unique device risk score and aggregated risk distribution reports. Our device score is based on risk assessment processes and standards devised by AAMI, NIST, the FDA and others, as well as Medigate's cybersecurity expertise and clinical domain knowledge. We aggregate individual scores into reports that outline the distribution of risk internally (across departments) and externally (across device manufacturers) and translate them into mitigation and remediation activities.

[1] All Functions descriptions are based on NIST's Cyber Framework ***latest publication***

PROTECT

Protect with Medigate

The Protection Function outlines appropriate safeguards to ensure the delivery of the organization's services and support its ability to limit or contain the impact of a potential cybersecurity event. Outcomes within this Function include:

- Deploying protections for systems and devices access control
- Establishing data security protection consistent with the organization's risk strategy
- Incorporating security considerations into system lifecycle management
- Establishing a vulnerability management plan to protect systems and assets

Medigate helps hospitals keep their clinical networks safe via clinically-driven, rule-based policy enforcement. By integrating with existing NAC and firewall solutions Medigate blocks malicious communications in real-time, establishes safer clinical network segmentation, and enforces granular policies tailored for the hospital's connected devices.

Our researchers are always up-to-date with published CVEs (sometimes in the discloser's role), integrating them into device risk scores, as well as inventories and supporting the hospital in prioritizing patching and mitigation activities in collaboration with device manufacturers. Medigate's visibility and risk distribution reports also allow hospitals to incorporate security considerations in procurement processes and introduce safer devices to the clinical network.

Detect with Medigate

The Detect Function defines the appropriate activities to identify the occurrence of a cybersecurity event and enables their timely discovery. Outcomes include:

- Ensuring anomalies and events are detected
- Implementing security continuous monitoring
- Performing vulnerability scans

Medigate has the contextual clinical and networking understanding to accurately detect credible threats. Our platform is based on extensive research of medical devices' communication protocols and manufacturer-intended behavior, allowing us to map all devices' internal and external communications, categorize them by protocol and destination, and detect malicious or out-of-order behavior with minimal false positives.

DETECT

Moreover, on top of our vulnerability intelligence feeds, Medigate's platform also integrates with vulnerability management platforms and scanners. We provide them with the required clinical context, in the form of clinical CVEs and granular device configurations, to properly discover and manage vulnerabilities for IoT and IoMT devices in the clinical setting. Our data enables the configuration of vulnerability scanners to minimize the risk to connected devices and maximize the scan efficiency.

Medigate Corresponds to the Framework Core Subcomponents

While Medigate doesn't directly provide incident response or post-event recovery capabilities, the granular data we obtain and generate on all connected devices, our understanding of their communication protocols and standard workflows, and our extensive cybersecurity expertise in the clinical setting would make valuable contributions to organizations experiencing an incident.

For a closer understanding of Medigate's alignment with the Framework, the following table describes the platforms contributions to each of the outcome Categories and Subcategories under the Identify, Protect, and Detect functions:

IDENTIFY(ID)		
Category	**Subcategory**	**Medigate Platform**
Asset Management (ID.AM): The data, personnel, devices, systems and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to organizational objectives and the organization's risk strategy.	**ID.AM-1:** Physical devices and systems within the organization are inventoried.	Medigate automatically discovers all IoT and IoMT devices on the network and collects granular information on each device, including OS, software, serial number, maintaining an up-to-date inventory of connected assets.
	ID.AM-2: Software platforms and applications within the organization are inventoried.	
	ID.AM-3: Organizational communication and data flows are mapped.	Medigate presents all existing VLANs and devices within them and maps all internal and external communications of all connected devices, categorized and displayed by protocol and destination.

Category	Subcategory	Medigate Platform
Governance (ID.GV): The policies, procedures, and processes to manage and monitor the organization's regulatory, legal, risk, environmental, and operational requirements are understood and inform the management of cybersecurity risk.	**ID.GV-1:** Organizational information security policy is established.	Medigate's device risk score and aggregated risk report informs and recommends risk management processes and mitigation and remediation activities.
	ID.GV-4: Governance and risk management processes address cybersecurity risks.	
Risk Assessment (ID.RA): The organization understands the cybersecurity risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals.	**ID.RA-1:** Asset vulnerabilities are identified and documented.	Medigate gives each device a multifactorial risk score that incorporates published CVEs and threat intelligence. Medigate also generates aggregated reports that map risk distribution across the organization by device type, manufacturer, and per the hospital's demand.
	ID.RA-3: Threats, both internal and external, are identified and documented.	
	ID.RA-5: Threats, vulnerabilities, likelihoods, and impacts are used to determine risk.	

PROTECT(PR)

Category	Subcategory	Medigate Platform
Identify Management and Access Control (PR.AC): Access to assets and associated facilities is limited to authorized users, processes, devices, activities and transactions.	**PR.AC-1:** Identities and credentials are managed for authorized devices and users.	Medigate's visibility enables the creation of granular profiles for different devices and suits them with the appropriate policies and configuration.
	PR.AC-4: Access permissions are managed, incorporating the principles of least privilege and separation of duties.	Medigate enables clinical policy enforcement by integrating with leading NAC and firewall vendors, establishing segmentation, and accessing control based on device type or functionality.
	PR.AC-5: Network integrity is protected (e.g., network segregation, network segmentation).	
Data Security (PR.DS): Information and records (data) are managed consistently with the organization's risk strategy to protect the confidentiality, integrity, and availability of information.	**PR.DS-1:** Data-at-rest is protected.	Medigate's policy enforcement is driven by a close understanding of IoT and IoMT devices, taking a whitelist-based approach to ensure devices are permitted to communicate only with approved notes using their intended protocols.
	PR.DS-5: Protections against data leaks are implemented.	

Category	Subcategory	Medigate Platform
Information Protection Processes and Procedures (PR.IP): Security policies (that address purpose, scope, roles, responsibilities, management commitment, and coordination among organizational entities), processes, and procedures are maintained and used to manage protection of information systems and assets.	**PR.IP-2:** A System Development Life Cycle to manage systems is implemented.	Medigate's detailed device information and risk assessment enables security considerations to be incorporated into procurement, measure device utilization, as well as conduct effective patching and maintenance cycles.
	PR.IP-12: A vulnerability management plan is developed and implemented.	Medigate's up-to-date clinically relevant CVE data feeds and integrations with vulnerability management platforms support a more robust vulnerability management planning.
Protective Technology (PR.PT): Technical security solutions are managed to ensure the security and resilience of systems and assets, consistent with related policies, procedures, and agreements.	**PR.PT-3:** The principle of least functionality is incorporated by configuring systems to provide only essential capabilities.	Medigate's policy enforcement is driven by a close understanding of IoT and IoMT devices, taking a whitelist-based approach to ensure devices are permitted to communicate only with approved nodes using their intended protocols.
	PR.PT-4: Communications and control networks are protected.	

DETECT(DE)

Category	Subcategory	Medigate Platform
Anomalies and Events (DE.AE): Anomalous activity is detected is a timely manner and the potential impact of events is understood.	**DE.AE-1:** A baseline of network operations and expected data flows for users and systems are established and managed.	Based on extensive research of medical devices' communication protocols and intended device behavior, Medigate maps all device communications and detects malicious or out-of-order behavior. Network data, CMMS entries and integrations with security products are aggregated to create a holistic view of the network and events.
	DE.AE-3: Event data are aggregated and correlated from multiple sources and sensors.	
Security Continuous Monitoring (DE.CM): The information system and assets are monitored at discrete intervals to identify cybersecurity events and verify the effectiveness of protective measures.	**DE.CM-1:** The network is monitored to detect potential cybersecurity events.	Medigate's platform continuously monitors connected devices' communications and alerts in real-time for malicious or out-of-order behavior. Medigate also partners with vulnerability management platforms and scanners to enable safe complementary measures when active scanning is not desired.
	DE.CM-7: Monitoring for unauthorized personnel, connections, devices, and software is performed.	
	DE.CM-8: Vulnerability scans are performed.	

For the full NIST Framework Guidelines, visit:
https://nvlpubs.nist.gov/nistpubs/CSWP/NIST. CSWP.04162018.pdf