

F R O S T & S U L L I V A N

# BEST PRACTICES

## AWARDS

F R O S T & S U L L I V A N

2020 BEST PRACTICES AWARD

 **MEDIGATE**

**2020 EUROPEAN MEDICAL DEVICE SECURITY  
ENABLING TECHNOLOGY LEADERSHIP AWARD**

## Contents

Background and Company Performance .....	3
<i>Industry Challenges</i> .....	3
<i>Technology Leverage and Customer Impact</i> .....	4
<i>Conclusion</i> .....	7
Significance of Enabling Technology Leadership .....	8
Understanding Enabling Technology Leadership .....	8
<i>Key Benchmarking Criteria</i> .....	9
Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices .....	10
The Intersection between 360-Degree Research and Best Practices Awards.....	11
<i>Research Methodology</i> .....	11
About Frost & Sullivan .....	11

## Background and Company Performance

### *Industry Challenges*

The momentum of the Internet of Things (IoT) drives various industries to adopt and embrace the advantages of connecting to the Internet. However, the rise in automation and connectivity among devices heightens vulnerability for critical equipment and infrastructure. Furthermore, augmenting connectivity across an organization often results in a lack of clarity and visibility into control systems, which creates an unfavorable scenario for maintaining cybersecurity.<sup>1</sup>

In addition, with the increasing level of malware, cyberattacks, and attack innovation, organizations are under constant threat; every device on a network is a potential attack or reconnaissance point. As such, there is growing adoption of the Zero Trust Network (ZTN) model based on the basic principle of “never trust, always verify.” This is an overarching strategy to prevent unauthorized access, contain breaches, and reduce the risk of an attacker’s lateral movement through a network while securing all access points across an organization’s systems, applications, and environment.

In the sensitive healthcare space, Frost & Sullivan analysts note that medical devices pose a unique challenge for information technology (IT) security. Continuous patchwork is technically challenging and costly, allowing cybercriminals and hackers an easy avenue to break into networks and steal valuable patient data, which can lead to clinical errors (such as incorrect dosage and disease misdiagnosis).<sup>2</sup>

Frost & Sullivan’s own research reveals that the challenge around IoT in the healthcare space lies in several converging factors. On the one hand, the question prevails in the risk related to patient privacy and safety regarding patient data and records on medical devices. Notably, if the medical device is compromised, so is the patient’s treatment. On the other hand, there is a distinct technological challenge. Medical device manufacturers have not properly anticipated connectivity; with further IoT development, when medical devices start to connect to the network, the communication protocols often do not support interoperability. This situation leads to the issue of a lack of management visibility on medical devices. Furthermore, there is a challenge of inefficient processes within clinical engineering departments.

Consequently, healthcare organizations are looking for new security systems that can protect their medical devices from cyberattacks. Therefore, there are growing demands for solutions that ensure complete visibility of medical devices, along with detection and prevention capabilities, to combat potential security risks while also making the healthcare environment more automated and efficient. However, the high complexity of cybersecurity and unpredictable return on investment creates ambiguity among end-users and decision-makers. The lack of cybersecurity awareness and uncertain value-at-risk level constrains investments in cybersecurity solutions within the healthcare space.

Frost & Sullivan points out that it is quite critical to educate customers on the scope of actual cyber threats and demonstrate the effectiveness of cybersecurity solutions while

---

<sup>1</sup> *Innovations in IoT Security, Network Security, and Machine Learning*, (Frost & Sullivan, July 2018)

<sup>2</sup> *Zero Trust—What is it and How to Implement?*, (Frost & Sullivan, May 2020)

demonstrating strong business cases and opportunities to invest.

## *Technology Leverage and Customer Impact*

### **Empowering Medical Device Security**

Founded in 2017 and headquartered in New York, United States, Medigate leverages an innovative mindset to deliver a dedicated security platform for protecting connected medical devices on healthcare provider networks.

Unlike conventional IoT solutions, the company built its cybersecurity platform specifically for the unique needs of medical devices and clinical networks. Medigate's medical device security platform addresses healthcare organizations' challenges of protecting their medical devices from cyber-attacks. Combined on-premises and cloud-based architectures secure the medical devices and electronic records connected to the network. Notably, the solution understands over 80 medical device communication protocols, such as Digital Imaging, Communications in Medicine and Health Level-7, to identify and profile devices and to detect malware attacks and intrusion.<sup>3</sup>

The company's unique vision encompasses cybersecurity and clinical engineering. From a value perspective, Frost & Sullivan feels that Medigate properly positions itself as a truly cross-organizational platform for the healthcare system while supporting the IT security and clinical engineering departments as well as the medical staff. It provides a passive network-based solution tailored to the unique and sensitive needs of the healthcare space. Specifically, the company's remarkable performance hinges on its platform's four building blocks.

First, the platform brings complete visibility to the network, including IT, IoT, and medical devices. By leveraging an industry-leading medical device signature database, developed by Medigate Research Labs as well as deep packet inspection (DPI), Medigate uniquely decodes the protocols used by various medical device manufacturers and provides detailed profiles of all connected devices, including their location, status, and security posture. Its deterministic approach accurately and completely identifies all the characteristics of a device, instead of using probabilistic methods that makes for a "best" guess.

The second pillar is detection. In addition to identifying a device and a wide variety of its attributes, Medigate identifies its network behavior and automatically compares it to a baseline, based on its intended usage and workflows, encompassing the approved protocols, ports, and destinations with which the device should be able to communicate. The baseline is based on manufacturer documentation, independent research and communication streams of the same device observed in other clinical networks. Comparing device behaviors across sites and healthcare systems also eliminates port configurations and implementation differences, and prevents the development of a baseline on the basis of a single, possibly misconfigured or compromised environment.

Comparing this treasure trove of information about every device and its communications, Medigate can finally notify its users of anything that is out of the ordinary. To name a few examples: A device that has an outdated software version, a known vulnerability or a functional recall announced for it; A device residing in the wrong segment of the network,

---

<sup>3</sup> *Innovations in Network Security, Container Security, and Cloud Security*, (Frost & Sullivan, March 2018)

based on healthcare IT best practices and user configuration; Or devices that are communicating outside of the defined policy. All of these and more are reported in real time to the users of the system.

The third pillar is policy enforcement. The company introduced a novel approach to the healthcare security space— leveraging the communication profiles described above to enable clinical micro-segmentation, enhancing the value of existing security products the healthcare organization possesses. Its deterministic approach to device identification allows Medigate to generate policies (ACLs) for effective prevention of suspicious communications and attacks and their spread throughout the network. The policies classify traffic as essential (for example, its dedicated medical protocol and DHCP), complimentary (such as DNS and monitoring traffic) and prohibited (all other communication). Medigate's platform flags communication that falls outside the approved patterns, and the policies can be readily implemented via a Network Access Controller, a Firewall and/or an Endpoint-Security solution, from a wide range of industry-leading products, to prevent them from ever taking place. The platform also displays an overarching matrix that maps which device types communicate with one another and which communication types should be approved according to these policies.

The platform leverages data gathered through its visibility and detection capabilities. It minimizes the device attack surface through its clinical micro-segmentation and tailored security policies to make medical devices locked and secured. The solution takes proactive steps regarding security within the hospital setting. The company added a data-driven layer enabling a more efficient security tool—thus, creating clear value for medical facilities as they do not need to replace the existing tools, but only improve their performance. Medigate has taken its extensive visibility and alerting capabilities and integrated with leading firewall, network access control, and security information and event management platforms in deeper ways to allow the user to enforce the most robust contextual security policies. While many companies integrate at an API-for data exchange to support device identification and sharing of device profiles, Medigate goes far beyond that to intelligently sends commands and properly cross-referenced data in a manner that can align workflows and automation. It enables true segmentation, proper risk assessment and informed asset management.

Ongoing collaboration with leading medical device manufacturers and healthcare customers enables Medigate to continue to build its unique knowledge base and expertise to remain up-to-date with the current medical threat landscape. Medigate's framework draws further insights from the Association for the Advancement of Medical Instrumentation's (AAMI's) Risk Management Technical Information Report and the National Institute of Standards and Technology's (NIST's) SP800-30 risk assessment guidance, as well as relevant components of FDA, ECRI, and ISO guidelines. As a result, Medigate has established a comprehensive method to calculate insightful, tangible risk scores for medical and IoT devices in a healthcare organization's network.

The fourth and final pillar revolves around the clinical engineering and Biomed insights space—Medigate aims to make the data about device utilization visible and actionable to healthcare personnel and decision making.

Using the device identification data, Medigate compiles an online, dynamic inventory that is automatically generated, always up-to-date and highly reliable. While using the same clinically-based DPI method, Medigate extracts the device's utilization data, differentiating between online/offline times and hours when the device is actually in use, and presents tailored reports that deliver optimization insights. Medigate then automatically exports inventory and location data into the existing CMMS platform, making it easily accessible to support decisions such as managing patient flow, planning preventative maintenance that's based on actual device utilization, informed procurement that's based on PAR levels and device utilization management as well as security aspects, and more.

Through the powerful combination of these pillars, Medigate's platform enables healthcare providers to operationalize their data while ensuring the uninterrupted delivery of critical treatment and the reliable protection of patient information. Frost & Sullivan recognizes that Medigate's platform cloud-based architecture, automated detection of potential threats, and the visibility provided of all the connected devices truly differentiate it from other solutions.

### **Professionalism, Innovation, and Passion for Delivering the Greatest Value**

Medigate's outstanding performance aligns with its remarkable capabilities and resources to optimize system performance continuously. The company's market efficiency is the result of product quality and its commitment to working with its customers and partners to meet and exceed expectations. Medigate focuses on the constant improvement of its customer service alongside its ongoing development. It devotes a significant focus on product quality, especially precision, as it cannot misidentify mission-critical medical device behavior. The company also relies on the trust of its customers, which depends on an exceptional level of reliability and top-notch precision.

While understanding the exacting and sensitive needs of the healthcare space, the company offers not only a single product; it provides a clever solution for the issues the industry faces. In addition to imparting value in day-to-day operations, Medigate provides technological consultancy that drives the product's usability within the enterprise. The company receives positive testimonials from Biomed and security staff, which recognize that its performance directly impacts the organization and ensures exceptional cost savings. In addition, customers leverage the ZTN concept enabled by Medigate.

With a focus on continuous development, the company combines qualified employees, the latest technologies, and sustained product excellence to ensure the most significant value and most reliable solution for its customers. A prominent example of its value is Medigate Research Labs, which helps manufacturers deliver more secure products. The company studies numerous device vendors and proprietary device protocols and behaviors to develop the leading signature database and clinical alert mechanism. As a result, Medigate leverages its expertise and versatility to provide security architectures and risk assessment services to manufacturers. Notably, Philips and Medigate partnered to disclose and mitigate three vulnerabilities, potentially putting Philips' IntelliVue Patient Monitors and Avalon Fetal/Maternal Monitors at risk of improper authentication, information exposure, and stack-based buffer overflow. As recognition for remarkable performance,



the company entered Philips' Hall of Honors.<sup>4</sup>

Medigate continues its vital growth stemming from its branding strategy and product quality, which made it the partner-of-choice for industry-leading collaborators. Recently, Forescout Technologies, a leader within the device visibility and control space, announced a strategic partnership with Medigate. This remarkable partnership aims to help healthcare organizations achieve wide contextual visibility into their IT and clinical networks, as well as sophisticated network analysis to detect threats and implement clinically driven policies.<sup>5</sup>

Another example of powerful synergy comes from the partnership with Cisco, integrating its platform to provide superior cybersecurity for clinical networks. The joint solution combines Cisco ISE's strengths and Medigate's platform to provide industry-leading access control capabilities. These include granting network visibility of IT devices, enforcing highly customizable access policies, and facilitating swift action against unsafe devices.<sup>6</sup>

While continuing its solid performance, the company focuses on continuous development to maintain the leading position in the medical device security market. Medigate seeks to provide the highest value level and leverage its unique focus on healthcare and the expanding security and data needs in the space, all while creating a powerful product portfolio.

As cybersecurity yields long-term savings, the company comes to customers and investors as a reliable and trustworthy partner that shares responsibility for investments. Medigate's successful history of operation further strengthens its credibility and demonstrates its wealth of experience.

## Conclusion

The sensitive healthcare space is under constant threat with the increasing intensity of malware, cyberattacks, and attack innovation. Healthcare organizations must properly protect the patient privacy and safety in the data and patient records contained on and collected by connected medical devices. Therefore, there is a growing demand for reliable security systems that can protect medical devices from cyberattacks.

Innovatively responding to these demands, Medigate continues its solid performance while offering its proven, market-leading technology and expertise. The company provides the industry's only truly dedicated medical device security platform. It ensures full visibility of all of the medical and Internet of Things devices connecting to the network while detecting and preventing potential threats, automating device inventories, and simplifying clinical-based policy enforcement and micro-segmentation. With a breadth of expertise in medical device protection, Frost & Sullivan appreciates how Medigate's platform enables providers to ensure the uninterrupted delivery of critical treatment and the reliable protection of patient information.

With its deep healthcare expertise, innovative mindset, and passion-driven performance, Medigate earns the 2020 Frost & Sullivan Enabling Technology Leadership Award.

---

<sup>4</sup> <https://www.medigate.io/platform/manufacturers-2/>, accessed June 2020

<sup>5</sup> <https://medigate.pathfactory.com/c/forescout-announces-?x=FTkYaI&lx=hO1BMA>, accessed June 2020

<sup>6</sup> <https://medigate.pathfactory.com/c/medigate-and-cisco-ise-joint-security-solution?x=PzKYM0&lx=eZUePY>, accessed June 2020

## Significance of Enabling Technology Leadership

Ultimately, growth in any organization depends on customers purchasing from a company and then making the decision to return time and again. In a sense, then, everything is truly about the customer. Making customers happy is the cornerstone of any successful, long-term growth strategy. To achieve these goals through enabling technology leadership, an organization must be best in class in three key areas: understanding demand, nurturing the brand, and differentiating from the competition.



## Understanding Enabling Technology Leadership

Product quality (driven by innovative technology) is the foundation of delivering customer value. When complemented by an equally rigorous focus on the customer, companies can begin to differentiate themselves from the competition. From awareness, to consideration, to purchase, to follow-up support, organizations that demonstrate best practices deliver a unique and enjoyable experience that gives customers confidence in the company, its products, and its integrity.



## *Key Benchmarking Criteria*

For the Enabling Technology Leadership Award, Frost & Sullivan analysts independently evaluated Technology Leverage and Customer Impact according to the criteria identified below.

### *Technology Leverage*

#### **Criterion 1: Commitment to Innovation**

Requirement: Conscious, ongoing adoption of emerging technologies that enable new product development and enhance product performance.

#### **Criterion 2: Commitment to Creativity**

Requirement: Technology leveraged to push the limits of form and function in the pursuit of white space innovation.

#### **Criterion 3: Stage Gate Efficiency**

Requirement: Adoption of technology to enhance the stage gate process for launching new products and solutions.

#### **Criterion 4: Commercialization Success**

Requirement: A proven track record of taking new technologies to market with a high rate of success.

#### **Criterion 5: Application Diversity**

Requirement: The development and/or integration of technologies that serve multiple applications and can be embraced in multiple environments.

### *Customer Impact*

#### **Criterion 1: Price/Performance Value**

Requirement: Products or services offer the best value for the price, compared to similar offerings in the market.

#### **Criterion 2: Customer Purchase Experience**

Requirement: Customers feel they are buying the optimal solution that addresses both their unique needs and their unique constraints.

#### **Criterion 3: Customer Ownership Experience**

Requirement: Customers are proud to own the company's product or service and have a positive experience throughout the life of the product or service.

#### **Criterion 4: Customer Service Experience**

Requirement: Customer service is accessible, fast, stress-free, and of high quality.

#### **Criterion 5: Brand Equity**

Requirement: Customers have a positive view of the brand and exhibit high brand loyalty.

## Best Practices Recognition: 10 Steps to Researching, Identifying, and Recognizing Best Practices

Frost & Sullivan analysts follow a 10-step process to evaluate Award candidates and assess their fit with select best practice criteria. The reputation and integrity of the Awards are based on close adherence to this process.

STEP	OBJECTIVE	KEY ACTIVITIES	OUTPUT
1 <b>Monitor, target, and screen</b>	Identify Award recipient candidates from around the globe	<ul style="list-style-type: none"> <li>Conduct in-depth industry research</li> <li>Identify emerging sectors</li> <li>Scan multiple geographies</li> </ul>	Pipeline of candidates who potentially meet all best-practice criteria
2 <b>Perform 360-degree research</b>	Perform comprehensive, 360-degree research on all candidates in the pipeline	<ul style="list-style-type: none"> <li>Interview thought leaders and industry practitioners</li> <li>Assess candidates' fit with best-practice criteria</li> <li>Rank all candidates</li> </ul>	Matrix positioning of all candidates' performance relative to one another
3 <b>Invite thought leadership in best practices</b>	Perform in-depth examination of all candidates	<ul style="list-style-type: none"> <li>Confirm best-practice criteria</li> <li>Examine eligibility of all candidates</li> <li>Identify any information gaps</li> </ul>	Detailed profiles of all ranked candidates
4 <b>Initiate research director review</b>	Conduct an unbiased evaluation of all candidate profiles	<ul style="list-style-type: none"> <li>Brainstorm ranking options</li> <li>Invite multiple perspectives on candidates' performance</li> <li>Update candidate profiles</li> </ul>	Final prioritization of all eligible candidates and companion best-practice positioning paper
5 <b>Assemble panel of industry experts</b>	Present findings to an expert panel of industry thought leaders	<ul style="list-style-type: none"> <li>Share findings</li> <li>Strengthen cases for candidate eligibility</li> <li>Prioritize candidates</li> </ul>	Refined list of prioritized Award candidates
6 <b>Conduct global industry review</b>	Build consensus on Award candidates' eligibility	<ul style="list-style-type: none"> <li>Hold global team meeting to review all candidates</li> <li>Pressure-test fit with criteria</li> <li>Confirm inclusion of all eligible candidates</li> </ul>	Final list of eligible Award candidates, representing success stories worldwide
7 <b>Perform quality check</b>	Develop official Award consideration materials	<ul style="list-style-type: none"> <li>Perform final performance benchmarking activities</li> <li>Write nominations</li> <li>Perform quality review</li> </ul>	High-quality, accurate, and creative presentation of nominees' successes
8 <b>Reconnect with panel of industry experts</b>	Finalize the selection of the best-practice Award recipient	<ul style="list-style-type: none"> <li>Review analysis with panel</li> <li>Build consensus</li> <li>Select recipient</li> </ul>	Decision on which company performs best against all best-practice criteria
9 <b>Communicate recognition</b>	Inform Award recipient of Award recognition	<ul style="list-style-type: none"> <li>Announce Award to the CEO</li> <li>Inspire the organization for continued success</li> <li>Celebrate the recipient's performance</li> </ul>	Announcement of Award and plan for how recipient can use the Award to enhance the brand
10 <b>Take strategic action</b>	Upon licensing, company is able to share Award news with stakeholders and customers	<ul style="list-style-type: none"> <li>Coordinate media outreach</li> <li>Design a marketing plan</li> <li>Assess Award's role in future strategic planning</li> </ul>	Widespread awareness of recipient's Award status among investors, media personnel, and employees

## The Intersection between 360-Degree Research and Best Practices Awards

### *Research Methodology*

Frost & Sullivan's 360-degree research methodology represents the analytical rigor of our research process. It offers a 360-degree-view of industry challenges, trends, and issues by integrating all 7 of Frost & Sullivan's research methodologies. Too often companies make important growth decisions based on a narrow understanding of their environment, leading to errors of both omission and commission. Successful growth strategies are founded on a thorough understanding of market, technical, economic, financial, customer, best practices, and demographic analyses. The integration of these research disciplines into the 360-degree research methodology provides an evaluation platform for benchmarking industry participants and for identifying those performing at best-in-class levels.

### 360-DEGREE RESEARCH: SEEING ORDER IN THE CHAOS



## About Frost & Sullivan

Frost & Sullivan, the Growth Partnership Company, enables clients to accelerate growth and achieve best-in-class positions in growth, innovation and leadership. The company's Growth Partnership Service provides the CEO and the CEO's Growth Team with disciplined research and best practice models to drive the generation, evaluation and implementation of powerful growth strategies. Frost & Sullivan leverages more than 50 years of experience in partnering with Global 1000 companies, emerging businesses, and the investment community from 45 offices on six continents. To join our Growth Partnership, please visit <http://www.frost.com>.