Quadrant Knowledge Solutions

Security and Risk Management

SPARK Matrix™: Connected Medical Device Security Solutions, Q4 2023

Market Insights, Competitive Evaluation, and Vendor Rankings

November, 2023

TABLE OF CONTENTS

Executive Overview

This research service includes a detailed analysis of the global Connected Medical Device Security Solution market dynamic, vendor landscape, and competitive positioning analysis. The study provides a competitive analysis of leading vendors. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors' capabilities and competitive differentiation.

Market Dynamics and Overview

Quadrant Knowledge Solutions defines a Connected Medical Device Security (CMDS) solution as "a software suit that identifies, tracks, and secures all the medical devices deployed in Healthcare Delivery Organization (HDO) from any vulnerabilities and breaches." These solutions are designed to monitor, manage, and protect IoMT devices, networks, building management systems, and all other connected devices in a health delivery organization." These solutions provide asset visibility, risk management, and device analytics to secure the IoMT devices from security risks.

Healthcare delivery entities (HDOs), like hospitals and clinics, must manage very complex networks consisting of different devices, including the Internet of Medical Things (IoMT), Operational Technology (OT), and Internet of Things (IoT) devices. The use of the Internet of Medical Things (IoMT) is also becoming a critical part of the field of Medical Technology (MedTech). However, IoMT and the devices using it are susceptible to threats such as ransomware. These have the potential to cause human fatalities, as these devices form a critical part of modern healthcare systems.

However, securing interconnected medical devices presents a unique challenge due to their proprietary protocols. Furthermore, the management of inventory also poses a challenge for HDOs due to the huge number of IoMT devices in use. These factors underline the need to deploy CMDS solutions.

CMDS solutions provide security from attacks, threats, and data exfiltration attempts to the IoT, OT, IT, and edge assets within the Health Delivery Organization's (HDO) ecosystem. These solutions streamline automated asset management, offering a comprehensive approach to locating, identifying, tracking, and monitoring all connected assets, whether managed or unmanaged, in the HDO network. This streamlined process reduces expenses and ultimately enhances the financial performance of HDOs. Connected medical device security solutions provide extensive visibility into the organization's network, enabling administrators to supervise equipment, enhance the security posture of the environment, optimize inventory and staffing, and ensure adherence to regulatory requirements.

The following is a detailed description of the key capabilities of a connected medical device security solution:

- **Asset Inventory Management:** A CMDS solution provides a device discovery and inventory tracking capability that accurately maps and categorizes devices linked to the HDO network. This mapping and categorizing enables the HDO to recognize and monitor both managed and unmanaged clinical as well as non-clinical devices across its wide and varied network ecosystem. The capability provides real-time, comprehensive insight into the HDO network, including links to unauthorized or unmanaged networks. It also updates inventory levels and streamlines inventory management, resulting in significant cost reductions. The capability helps to take data from FDA database to identify FDA recalls and manufacturer databases to obtain other information such as classification, version, and device risk.

- **Risk Management:** Risk management is a key capability provided by a CMDS solution. The capability considers the clinical hazards connected to the device, including metrics like PHI transmission volume and ongoing FDA recalls, identifies these risks or irregularities, and initiates protective protocols to minimize potential hazards. It also evaluates all items within the inventory, assessing each for vulnerabilities related to cybersecurity. The risk analysis provides a score indicating the level of risk associated with the device, which helps the information security team plan their strategy for minimizing potential issues. The capability also helps to formulate the plan for eliminating or reducing the risks posed by medical devices. The plan will include tasks like implementing firmware upgrades for devices, updating operating systems, altering communication protocols, employing patches provided by vendors to address recognized vulnerabilities, and proposing the segmentation of networks.

- **Vulnerability Management:** Most medical devices rely on firmware for functioning, and healthcare delivery organizations (HDOs) continue to use older devices until they meet clinical standards. However, as these devices get older, their firmware becomes outdated, and they serve as potential access points for attackers into the HDO network. A CMDS solution provides a vulnerability management module, which ensures comprehensive patching of all devices. This capability also

identifies and resolves vulnerabilities within devices that cannot be patched due to regulatory constraints or specific model versions.

- **Compliance with Medical Regulations:** A CMDS solution ensures compliance with medical regulations. Medical devices are required to follow both medical device regulations and other directives related to data transmission and security of personal information. The security solutions for interconnected medical devices help healthcare delivery organizations (HDOs) simplify their audit mechanisms by ensuring compliance with regulations such as HIPAA, PII, or PCI-DSS. Furthermore, the capability provides compliance reports to fulfill both government regulations and internal policy audit requirements.

- **Policy Management:** The policy management features enable administrators to define and monitor policies for automatically mitigating risks or addressing security incidents. This capability enables healthcare delivery organizations (HDOs) to create custom protocols for addressing policy breaches. Moreover, administrators can define exemptions, run network segmentation policies, or adjust sensitivity levels in alignment with device characteristics and risk evaluations.

- **Device Analytics & Dashboard Reporting:** The connected medical device security solution provides an integrated analytics and reporting feature, which monitors all device actions, constructs dashboards, and produces reports. Device analytics provides operational insights regarding device usage to HDO administration. This feature assists the organization in optimizing device quantities, leading to cost reduction by highlighting underutilized equipment. While reports offer valuable information regarding security status, identified risks, vulnerabilities and irregularities, inventory quantities, device usage, and maintenance notifications. The reports are integrated into security or network operation centers as well as biomedical engineering workplaces and can be presented through a centralized dashboard for real-time operational details regarding the status of medical devices.

- **Event Detection and Response:** The event detection and response capability uses the results of risk analysis to monitor operations within and around medical devices to manage the identified risks. Upon

detecting a risk, the capability generates an event alert, conveying comprehensive information about the identified risk to create an organizational response.

- **Network Monitoring:** The network monitoring feature monitors all devices and entry points within the healthcare delivery organization's (HDO) network. It identifies vulnerable points, compromised devices, data leakage, anomalies, breaches, or any behavior that poses a risk to device security or violates medical regulations such as HIPAA or PII. This includes activities like data extraction attempts, phishing attempts, malware and ransomware incidents, direct manipulation of medical device controls, or unauthorized access to sensitive medical records. The capability is equipped with packet sniffing and packet capture capabilities, facilitating in-depth analysis of packets in case of an attack.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of the major connected medical device security solution vendors by evaluating their products, market presence, and value proposition. The evaluation is based on primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall connected medical device security solutions market. This study includes an analysis of key vendors, including AirEye, Armis, Asimily, Claroty, CloudWave, Cybeats, Cylera, Cynerio, Forescout, Gurucul, LOCH Technologies, MedSec, Ordr, Palo Alto Networks, and Sepio.

AirEye, Armis, Claroty, Cylera, Cynerio, Forescout, Gurucul, and Ordr are the top performers and technology leaders in the global Connected Medical Device Security solutions market. These companies provide a sophisticated and comprehensive technology platform to provide visibility, location, usage, and risk score of all the devices present in the network ecosystem. The platform categorizes devices based on their type, criticality, and risk associated with them. The platform records real-time updates of device inventory. It also secures all the devices from threats by performing a risk analysis of devices and providing remediation according to the criticality of their use and the risk associated with them. The platform provides efficiency by determining the underused devices present in the network ecosystem.

The AirEye solution provides various features, including the monitoring of wireless channels, identification and classification of assets, categorization of devices and networks, breach detection, quick termination of attacks, and forensic insights. This solution offers two deployment options. The first involves the use of an Overlay Architecture, where strategically placed software-based sensors known as "Halo" eliminate the need for an endpoint agent. The second option integrates the AirEye solution with the cloud, which is achieved by connecting the AirEye server to the Cisco Meraki cloud network using an API key. This deployment helps the organization to increase the solution's scalability.

The Armis offers Armis Centrix™ platform that provides different capabilities, including real-time comprehensive visibility into the inventory of medical devices, insights into device usage to optimize efficiency, assessment of device risks based on vulnerabilities, detection of breaches involving Protected Health Information (PHI), identification of threats and their remediation, and the automation of medical device security.

Claroty offers Medigate, a SaaS-powered healthcare cybersecurity platform strategically developed to secure organizational device ecosystems and meet business objectives. Medigate enables enterprises to effectively supervise and mitigate risks in their healthcare Extended Internet of Things (XIoT) landscape.

Cylera offers Cylera Platform, which takes a proactive approach to managing connected medical devices within the organization's network ecosystem. This comprehensive platform incorporates features like Executive Management, Procurement & Vendor Management, Information Security, Risk Management & Compliance, and Information Technology. These functions allow the platform to possess enhanced control over devices, leading to improved operational efficiency and security measures. The platform also helps the IT team to monitor and manage network devices, enabling them with in-depth insights that help optimize device maintenance and management practices.

Cynerio offers the Cynerio Platform that enables hospitals to detect and address threats associated with medical within the network, including IoMT, IoT, OT, unmanaged IT, and mobile devices. Cynerio's solution for Healthcare IoT Attack Detection and Response enables hospitals to identify and mitigate threats originating from devices. Additionally, Cynerio offers Cynerio's Preventative Risk Management, which provides insights into the interconnected medical devices, IoT, and OT infrastructure.

Forescout offers the Forescout Platform that continuously operates to identify, enhance security, and ensure compliance across a range of cyber assets, including IT, IoT, IoMT, and OT, while minimizing disruptions to business operations. Forescout eyeSight provides comprehensive visibility of all the devices across the extended enterprise, securing critical business operations from disruption. It detects all IP-connected devices, automatically categorizes them, and promptly assesses their compliance status and associated risks. Forescout Risk and Exposure Management serves as an asset intelligence solution that helps organizations to understand their security posture of the potential targets. Meanwhile, Forescout eyeSegment simplifies the procedure of creating, strategizing, and implementing non-intrusive, adaptable segmentation for all cyber assets (IT, OT, IoT, IoMT).

Gurucul's security solution for connected medical devices offers key functions, such as device recognition, continuous monitoring, inventory management, risk evaluation, vulnerability control, compliance monitoring, and robust analytics with reporting options. Gurucul enhances its offering by introducing a managed

security analytics service. Gurucul UEBA can identify when a device is no longer in its regular operational cycle and when it's safe to perform maintenance, like patching.

Ordr offers Ordr Clinical Defender, a solution incorporating essential features found in security solutions for connected medical devices. These include functions such as asset discovery and monitoring, vulnerability and risk management, threat detection and mitigation, compliance adherence, micro-segmentation implementation, and the provision of intelligent reporting tools. Ordr also offers a Connected Device Security platform that identifies and secures connected devices, spanning traditional IT devices to potentially more vulnerable IoT, IoMT, and OT devices. Its key differentiators include full visibility of medical devices, insights into potential risks, automated policy implementation, and seamless integrations.

CloudWave, MedSec, Palo Alto Networks, and Sepio have been positioned as Strong Contenders. CloudWave offers the SensatoMD solution. This single-suite solution for medical devices provides features like medical device vulnerability assessment, implementing a breach detection system through the Sensato Cybersecurity-as-a-Service platform, and providing guidance for incident response related to medical devices.

MedSec offers governance structures and models that help manage cybersecurity threats to medical devices. MedSec provides HDOs with the remediation for the security of medical devices from vulnerabilities.

Palo Alto offers a Medical IoT Security solution that enables enterprises to identify and evaluate all linked devices within their network. The solution enables the segregation of devices, enforcing the principle of least privilege access. This proactive approach guarantees the continual protection of medical devices against cyber threats.

Sepio offers the Asset Risk Management platform for providing device security features to HDOs. Asset Risk Management provides complete asset visibility regardless of their location, type, and usage. The platform helps to provide compliance with global regulations such as HIPAA and GDPR. It also provides integration with third-party vendors.

Asimily, Cybeats and LOCH Technologies have been placed as aspirants in the Connected Medical Device Security market. Asimily provides Asimily Risk Remediation Platform, which offers features like identifying and documenting devices, keeping inventory records, monitoring network activity, identifying and reducing risks, addressing threats and vulnerabilities, managing policies, and utilizing analysis and reporting tools.

Cybeats offers the RDSP IoT Security Platform that provides a dashboard that integrates into the SIEM systems and helps the Security Operation Centers to respond quickly to attacks. The dashboard offers visibility of devices present in the ecosystem. Cybeats provides threat intelligence to identify emerging threats.

LOCH Technologies offers AirShield Solution that offers comprehensive functionalities, including Asset Visibility and Classification, Asset Configuration Management, and Security Posture Monitoring. It also provides Remote Wireless Performance and Reliability Troubleshooting with alerting capabilities. In addition, it aids in Risk Management and Compliance adherence to standards like PCI, HIPAA, and NIST.

All the vendors captured in the 2023 SPARK Matrix™ of Connected Medical Device Security vendors are focusing on improving their capabilities to identify all the devices present in the network ecosystem, analyzing devices for their risk assessment and proving accurate risk score to them, increasing the operational efficiency of devices. Additionally, they are working to ease the process of compliance of devices with global regulations. Organizations are consistently looking at enhancing their Connected Medical Device Security products and expanding support for multiple deployment options.

Key Competitive Factors and Technology Differentiators

Many connected medical device security solution vendors provide comprehensive functionalities that support different use cases. However, their technology and customer value proposition may differ depending on customer size, industry vertical, geographic location, and organization-specific needs. Some of the key competitive technology differentiators for an integrated connected medical device security solution are:

Network Segmentation: When selecting a vendor, healthcare delivery organizations should consider the adoption of network segmentation as a strategic approach to address various challenges in IT and IoMT (Internet of Medical Things) environments. This method offers multiple key advantages, including enhancing security practices by halting the spread of threat across the network, exerting control over access to crucial patient data to mitigate data exfiltration risks, and reducing the attack surface for essential functions performed by susceptible medical systems.

Knowledge Database: Users should look for vendors providing proprietary knowledge repositories containing comprehensive data regarding medical devices, including their attack history and attack patterns. These repositories enable the solution to identify, categorize, and seamlessly integrate a wide range of medical devices from various manufacturers and versions. Moreover, they facilitate the detection of attacks and vulnerabilities by these solutions, enabling the identification of best remedial actions through analysis of historical data, consequently leading to reduced Mean Time to Remediation (MTTR) metrics.

Use of AI/ML: Organizations should consider vendors who use artificial intelligence (AI) and machine learning (ML) in their tools to manage vulnerabilities and reporting. Some vendors offer the capability to detect vulnerabilities through an analysis of a device's Software Bill-of-Material (SBOM). This integration enables Healthcare Delivery Organizations (HDOs) to proactively establish measures for vulnerability mitigation even before any potential incidents arise.

Service Delivery models: Organizations should look for vendors that provide agentless passive real-time monitoring as it will save the time and effort needed for maintenance and updates. Most medical devices are not compatible with agent-based solutions for installation, and the utilization of active monitoring tools

could potentially disrupt the essential functions of these devices. The vendors must offer a range of deployment alternatives. Depending on the specific needs of Healthcare Delivery Organizations (HDOs), They can opt for vendors that can provide their preferred deployment model, either on-prem or on the cloud.

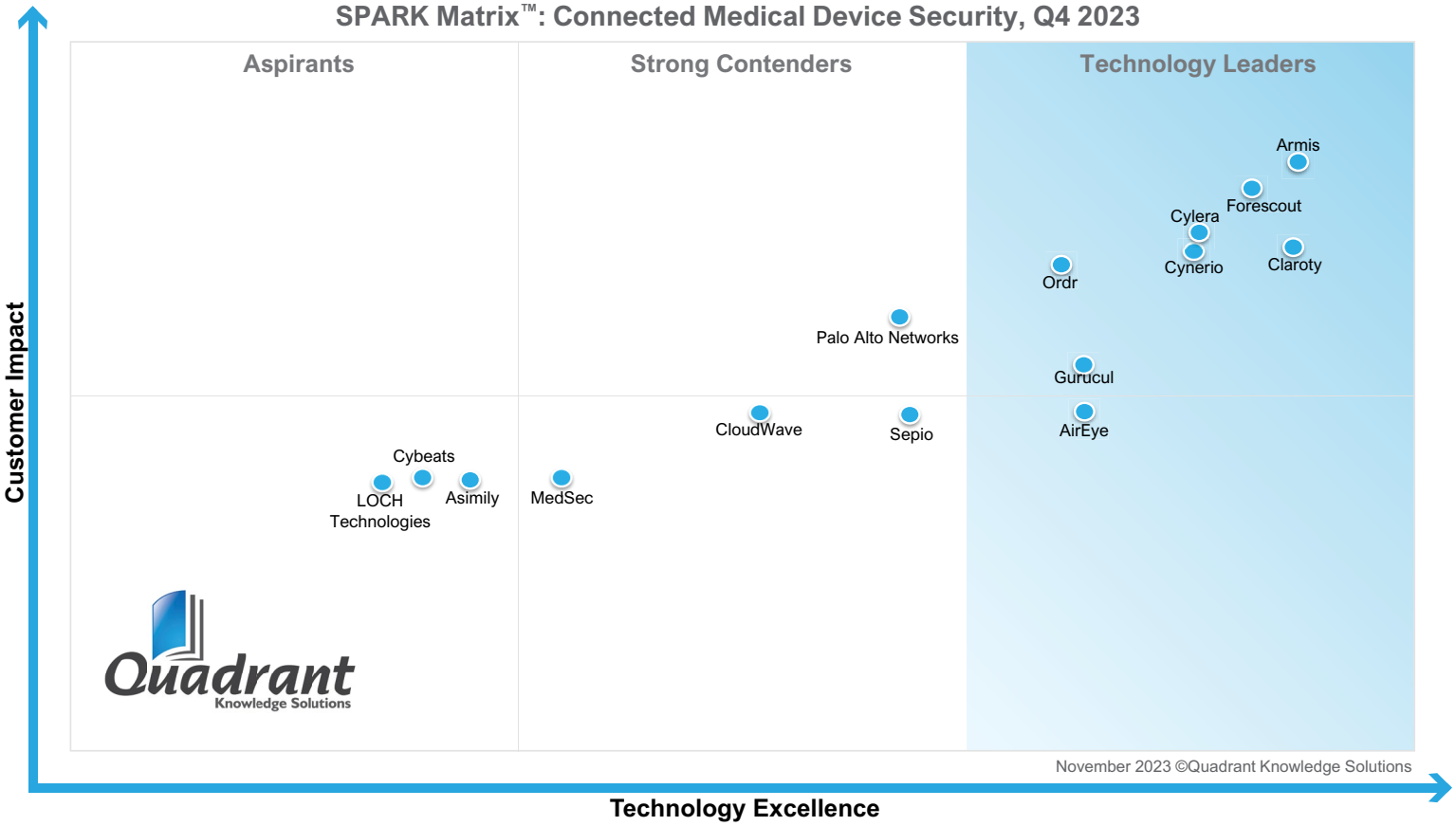
Integration, Interoperability, and Ease of Use: Healthcare Delivery Organizations (HDOs) should look for vendors with established technological collaborations with other security providers or those offering comprehensive integrations that helps in smooth incorporation of the solution into the HDO's existing security framework. These integrations could include systems such as Security Information and Event Management (SIEM) or Network Access Control (NAC), as well as network infrastructure solutions, third-party risk management databases, and analytical tools. These integrations help organizations understand their device ecosystem and security level.

Managed Security Services: Major healthcare delivery organizations (HDOs) may also explore the option of considering vendors that offers Managed Security Services as part of their portfolio when they lack the capacity to monitor their operations or seek to implement the solution across their network of facilities.

SPARK Matrix™: Connected Medical Device Security

Strategic Performance Assessment and Ranking

Figure: 2023 SPARK Matrix™
Strategic Performance Assessment and Ranking)
Connected Medical Device Security, Q4 2023



Vendor Profile

Following are the profiles of the leading Connected Medical Device Security solution vendors with a global impact. The following vendor profiles are written based on the information provided by the vendor's executives as part of the research process. Quadrant research team has also referred to the company's website, whitepapers, blogs, and other sources for writing the profile. A detailed vendor profile and analysis of all the vendors, along with various competitive scenarios, are available as a custom research deliverable to our clients. Users are advised to directly speak to respective vendors for a more comprehensive understanding of their technology capabilities. Users are advised to consult Quadrant Knowledge Solutions before making any purchase decisions regarding connected medical device security solution and vendor selection based on research findings included in this research service.

Armis

URL: https://www.armis.com/

Company Introduction:

Founded in 2015 and headquartered in San Francisco, CA, Armis offers a cyber exposure management platform powered by its AI-driven Asset Intelligence Engine. The platform, Armis Centrix™, sees, protects, and manages critical assets in real-time for IT, cloud, IoT devices, medical devices (IoMT), operational technology (OT), industrial control systems (ICS), and 5G environments. For healthcare, Armis Centrix™ provides complete visibility, continuous security, and optimized utilization of IoMT, unmanaged medical/non-medical devices.

Product Introduction:

Armis Centrix™ for Medical Device Security offers features like real-time complete visibility into medical device inventory, information regarding device usage for increasing utilization efficiency, medical device risk assessment based on vulnerabilities, identifying Protected Health Information (PHI) breaches, identifying and remediating threats, and automating security of medical devices. The product is also equipped with an Asset Intelligence Engine with over 20 million device profiles, and the AI-powered Armis Standard Query.

Technology Perspective:

Following is the analysis of Armis's capabilities in the global Connected Medical Device Security (CMDS) solution market:

- Armis Centrix™ for Medical Device Security provides specialized visibility into all assets across all departments along with device context, for example, tablets used for medical care. The platform provides real-time, uninterrupted visibility to all connected devices. Armis Centrix™ for Medical Device security provides holistic visibility into the user's overall risk and attack surface. The platform also provides the business context of business-critical assets based on their roles.

- Armis Centrix™ for Medical Device Security provides insights into the utilization of different devices, such as CT scanners, machines for MRIs, X-rays, as well as ultrasound, patient monitors, infusion pumps, and lab equipment. The platform compares the utilization of different devices across the organization to identify which assets are being utilized and identifies the least utilized devices to optimize maximum efficiency of device usage. Armis Centrix™ integrates this information into business intelligence platforms that help organizations achieve operational efficiencies.

- Armis Centrix™ for Medical Device Security provides contextualized risk assessment based on vulnerabilities and PHI. It also provides information regarding all threat detection, anomalous behavior, and additional behavioral-based risks such as network perimeter evasion, insecure protocol usage, invalid certificate detection, IP conflicts and clinical risks such as FDA recalls. Furthermore, Armis Centrix™ Asset Vulnerability Prioritization and Remediation helps the organization reduce their attack surface by analyzing attributes of devices and overlay threat intel as part of the analysis.

- Armis Centrix™ for Medical Device Security can detect and identify PHI breaches, such as the transmission of unencrypted PHI as well as unencrypted credentials with PHI access and secures streaming cameras and recording devices from breaches. The solution also detects Manufacturer Disclosure Statement for Medical Device Security (MDS2) information, which outlines whether devices are storing, transmitting, or exporting PHI. This is all integrated into the risk engine which assesses the device risk based on configuration profile (ie. MDS2), EOL / EOS status, vulnerabilities, behaviors, and policy violations.

- Armis Centrix™ for Medical Device Security provides visibility into which vulnerability is being exploited, as well as access to PCAPs for security team incident response as required. The product also provides complete threat context to all vulnerabilities, including the detection of capabilities, active exploits, attack groups, and associated ransomware activities.

- Armis Centrix™ integration capabilities enable organizations to share and get information with IT systems, security solutions, and clinical platforms. The pull integrations provide contextualized risk assessment by understanding which medical devices have security solutions installed and are protected. The enforcement integrations provide real-time policy assessment and actions.

These integrations enable automated security enforcement, automated workflow generation, and compliance reporting across the entire organization.

- The product also offers an asset inventory management and tracking feature. The feature is backed by the Armis Asset Intelligence Engine, which contains over 20 million device profiles and information about the 3B+ assets maintained by Armis.

- Armis AI Search Query is the proprietary filter-based query search feature that helps organizations manage queries, reports, policies, and dashboards. The product's key differentiator is the ability to completely customize reports and dashboards, the Asset Intelligence Engine, and its AI-powered Armis Standard Query.

- One of the technological differentiators of the platform is Armis Centrix™ for Vulnerability Prioritization and Remediation. This solution is used to prioritize vulnerabilities and enable organizations to focus on remediation based on business needs.

- Other technological differentiators of Armis Centrix™ include a threat detection engine that helps to detect threats in real-time, a 360-degree view of the network environment, including users, cloud assets, business applications, operating systems, devices, services, and traffic.

- Armis Centrix™ offers various deployment models, including hardware or virtual collectors (appliances), as well as direct cloud-to-cloud integrations such as Meraki, CrowdStrike, Azure, Nuvolo, etc. In addition, its cloud-native approach ensures all updates are taken care of, and no maintenance is required from the client's side.

Market Perspective:

- Regarding geographical presence, Armis has a major presence in North America, Canada, UK/I, Germany, Italy, Spain, Middle East, with its largest customer base in the USA and numerous healthcare customers internationally. Regarding industry verticals, the company's primary verticals include energy & utilities, healthcare, manufacturing, retail, finance, education, and the public sector.

- The top use cases for Armis Centrix™ for Medical Device Security include providing medical device asset inventory, medical device asset assessment, network/device threat detection & response, device utilization/operational analytics, network segmentation, and compliance support.

Roadmap:

- As a part of the technological roadmap, Armis is focusing on medical device lifecycle management, complete micro-segmented workflow, visibility, and alerting. Armis is also focusing on healthcare XDR offerings, segmentation gap analysis and clinical workflow integration. The company is also increasing its presence in NHS hospitals in the UK, EMEA, Asia Pacific, and the Middle East. Armis will also continue to expand the platform capabilities for ensuring the entire attack surface is both defended and managed in real-time.

SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix™ provides a snapshot of the market positioning of the key market participants. SPARK Matrix™ provides a visual representation of market participants and provides strategic insights on how each supplier ranks related to their competitors concerning various performance parameters based on the category of technology excellence and customer impact. Quadrant's Competitive Landscape Analysis is a useful planning guide for strategic decision-making, such as finding M&A prospects, partnerships, geographical expansion, portfolio expansion, and similar others.

Each market participant is analyzed against several parameters of Technology Excellence and Customer Impact. In each of the parameters (see charts), an index is assigned to each supplier from 1 (lowest) to 10 (highest). These ratings are designated to each market participant based on the research findings. Based on the individual participant ratings, X and Y coordinate values are calculated. These coordinates are finally used to make SPARK Matrix™.

Technology Excellence	Weightage
Device Discovery and management	15%
Risk Analytics and Management	15%
Analytics	10%
Technology Differentiators	5%
Vulnerability management	7%
Threat Response and Management	10%
Dashboarding, Reporting, and Compliance	7%
Vision & Roadmap	7%

Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Customer Service Excellence	15%
Unique Value Proposition	15%
Ease of deployment	15%

Evaluation Criteria: Technology Excellence

- **Device Discovery and management:** The ability to map and classify devices and identify the real-time location and accurate number of inventories of all medical devices present in the organization.
- **Risk Analytics and Management:** The ability to analyze all devices for risk vulnerabilities and provide a risk score so that organizations can make mitigation plans accordingly.
- **Analytics:** The ability to track usage of devices to optimize the use of underutilized medical devices.
- **Technology Differentiators:** Technical USPs and their competitive advantage.
- **Vulnerability management:** The ability to identify and rectify vulnerabilities associated with medical devices.
- **Threat Response and Management:** The ability to notify threats and communicate information to an organization.
- **Dashboarding, Reporting, and Compliance:** The ability to display the information collected and provide compliance reports for Government regulations.
- **Vision & Roadmap:** Key Planned enhancement to offer superior products/technology.

Evaluation Criteria: Customer Impact

- **Product Strategy & Performance:** Evaluation of multiple aspects of product strategy and performance in terms of product availability, price-to-performance ratio, excellence in GTM strategy, and other product-specific parameters.
- **Market Presence:** The ability to demonstrate revenue, client base, and market growth along with a presence in various geographical regions and industry verticals.

- **Proven Record:** Evaluation of the existing client base from SMB, mid-market, and large enterprise segments, growth rate, and analysis of the customer case studies.

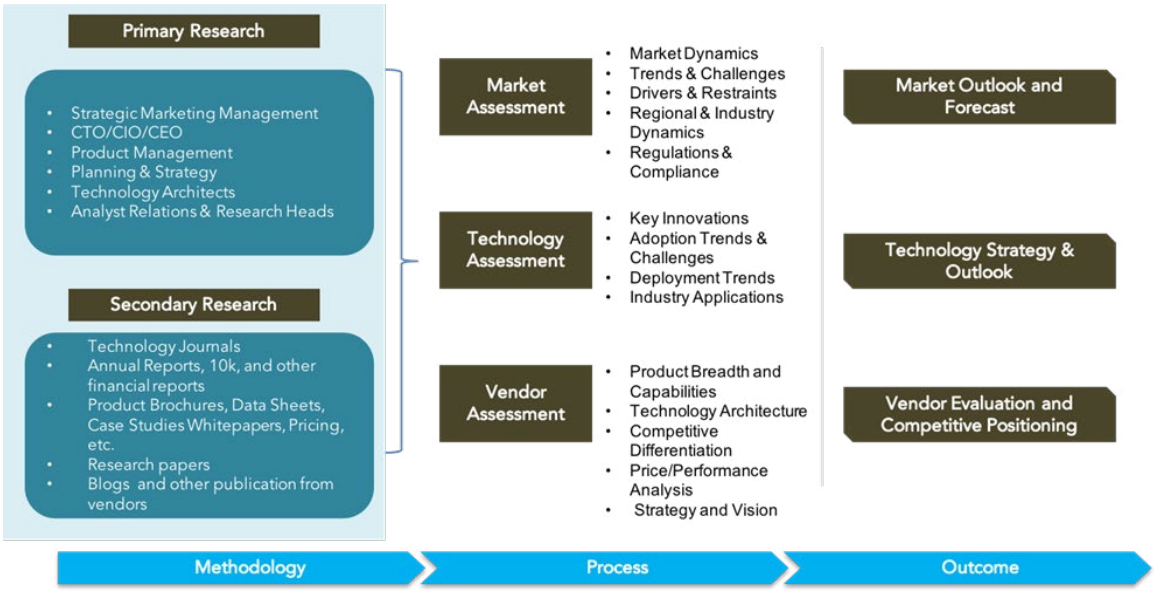
- **Ease of Deployment & Use:** The ability to provide superior deployment experience to clients supporting flexible deployment or demonstrate superior purchase, implementation, and usage experience. Additionally, vendors' products are analyzed to offer a user-friendly UI and ownership experience.

- **Customer Service Excellence:** The ability to demonstrate vendors' capability to provide a range of professional services from consulting, training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.

- **Unique Value Proposition:** The ability to demonstrate unique differentiators driven by ongoing industry trends, industry convergence, technology innovation, and such others.

Research Methodologies

Quadrant Knowledge Solutions uses a comprehensive approach to conduct global market outlook research for various technologies. Quadrant's research approach provides our analysts with the most effective framework to identify market and technology trends and helps in formulating meaningful growth strategies for our clients. All the sections of our research report are prepared with a considerable amount of time and thought process before moving on to the next step. Following is the brief description of the major sections of our research methodologies.



Secondary Research

Following are the major sources of information for conducting secondary research:

Quadrant's Internal Database

Quadrant Knowledge Solutions maintains a proprietary database in several technology marketplaces. This database provides our analyst with an adequate foundation to kick-start the research project. This database includes information from the following sources:

- Annual reports and other financial reports
- Industry participant lists
- Published secondary data on companies and their products
- Major market and technology trends

Literature Research

Quadrant Knowledge Solutions leverages on several magazine subscriptions and other publications that cover a wide range of subjects related to technology research. We also use the extensive library of directories and Journals on various technology domains. Our analysts use blog posts, whitepapers, case studies, and other literature published by major technology vendors, online experts, and industry news publications.

Inputs from Industry Participants

Quadrant analysts collect relevant documents such as whitepaper, brochures, case studies, price lists, datasheet, and other reports from all major industry participants.

Primary Research

Quadrant analysts use a two-step process for conducting primary research that helps us in capturing meaningful and most accurate market information. Below is the two-step process of our primary research:

Market Estimation: Based on the top-down and bottom-up approach, our analyst analyses all industry participants to estimate their business in the technology market for various market segments. We also seek information and verification of client business performance as part of our primary research interviews or through a detailed market questionnaire. The Quadrant research team conducts a detailed analysis of the comments and inputs provided by the industry participants.

Client Interview: Quadrant analyst team conducts a detailed telephonic interview of all major industry participants to get their perspectives of the current and future market dynamics. Our analyst also gets their first-hand experience with the vendor's product demo to understand their technology capabilities, user experience, product features, and other aspects. Based on the requirements, Quadrant analysts interview with more than one person from each of the market participants to verify the accuracy of the information provided. We typically engage with client personnel in one of the following functions:

- Strategic Marketing Management
- Product Management
- Product Planning
- Planning & Strategy

Feedback from Channel Partners and End Users

Quadrant research team researches with various sales channel partners, including distributors, system integrators, and consultants to understand the detailed perspective of the market. Our analysts also get feedback from end-users from multiple industries and geographical regions to understand key issues, technology trends, and supplier capabilities in the technology market.

SPARK Matrix: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix representation provides a visual representation of market participants and provides strategic insights on how each supplier ranks in comparison to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact.

Final Report Preparation

After finalization of market analysis our analyst prepares necessary graphs, charts, and table to get further insights and preparation of the final research report. Our final research report includes information including competitive analysis; major market & technology trends; market drivers; vendor profiles, and such others.

Client Support

For information on hard-copy or electronic reprints, please contact Client Support at

ajinkya@quadrant-solutions.com | www.quadrant-solutions.com