Market Guide for Medical Device Risk Management Platforms

15 July 2025 - ID G00826635 - 29 min read

By: Gregg Pessin

Initiatives:Healthcare Provider Technology Insights

Medical device risk management platforms provide cybersecurity risk mitigation and device management capabilities in response to the current healthcare provider threat environment. Healthcare provider CIOs should use this guidance to assess essential platform capabilities and notable vendors.

Overview

Key Findings

- Healthcare providers have become a primary target of cybercrime, motivating IT leaders to increase their cybersecurity budgets, including additional investments for Internet of Medical Things (IoMT) protection and other Internet of Things (IoT) in their enterprises.

- This market has matured, with vendors focusing on developing new, differentiated approaches such as exploitability scoring that build on existing capabilities to enhance healthcare provider IT leaders' ability to manage the risks IoMT poses.

- Healthcare provider IT leaders are taking a more expansive view of IoMT to include the entire operational life cycle rather than focusing on specific aspects or vectors of risk or utilization. They recognize that medical device risk management is one component of a larger whole.

- Healthcare provider leaders now expect their medical device risk management platforms to recognize their specific, local, and unique topology and report on their distinct exploitabilities and vulnerabilities.

Recommendations

- Objectively assess your medical device risk management maturity by reviewing your organization's ability to identify all IoMT assets and detect, analyze and mitigate vulnerabilities.
- Strengthen your organization's cybersecurity risk management by addressing identified IoMT vulnerabilities via vendor solutions and internal process enhancements. Incorporate these device-focused security measures into your current enterprisewide security initiatives.
- Improve operational department efficiencies using vendor-generated metadata, such as device utilization statistics, to inform and augment existing medical device management tools such as a computerized maintenance management system (CMMS) and IT service management (ITSM).

Market Definition

The medical device risk management platform market addresses software, hardware, and network and data protection requirements for the Internet of Medical Things (IoMT). These platforms use knowledge of communication protocols, network packet or traffic metadata, and asset behavior to discover, categorize and map IoMT in the clinical environment. They enable organizations to utilize IoMT securely, ensure IoMT endpoint and data integrity, and verify inventory. They share many technologies and processes used in IT security, such as deep packet inspection and risk identification. These platforms help CIOs foster trust and provide safe, secure and reliable digital care delivery.

In the IoMT-rich healthcare ecosystem, the scale and variety of cybersecurity risks are significant and create a large and complex threat environment. Currently, most IoMT devices in production have minimal internal computing resources, with limited ability to install antivirus, encryption and other forms of protection. However, they commonly connect to healthcare provider back-end computing resources, and they require protection. These factors create the market opportunity for healthcare-provider-specific solutions that help end-user cybersecurity teams protect their patients, data and business processes.

Medical device risk management platforms belong to a larger world of cyber-physical systems (CPS) security. This more extensive market is growing in response to increased threats. Vendors that once focused on passive deep packet inspection now seek differentiation with a variety of additional techniques, including native protocol active queries. They are also rapidly deploying additional functionalities such as vulnerability management, threat intelligence, visualizations, alerts, playbooks and feeds into other IT security and operational management tools. This creates a new asset-centric security discipline for CPS security.

Mandatory Features

The mandatory features for this market include:

Asset Discovery

Asset discovery creates an accurate inventory of all medical devices in the organization. This accounting should include all devices connected to the organization's network. Metadata associated with the inventory entries should identify medical device characteristics that enable analysis for operational and cybersecurity purposes. The resulting database used to store the inventory should be accessible to all other systems in the organization with functional associations with medical devices, such as IT service management (ITSM) or computerized maintenance management software (CMMS).

Risk Analysis

Risk analysis examines all inventory items for cybersecurity vulnerabilities. Typically, these capabilities rely on cyber-industry information repositories of known risks, such as the device, protocols used and embedded operating systems. The result of the risk analysis will be a risk score or a classification of vulnerabilities. This information will help the information security team decide how to best address and mitigate these risks. The results also provide needed input to event detection and response capability.

Common Features

The common features for this market include:

Risk Mitigation

The risk mitigation capability of solutions in this category creates a plan for the organization to follow to eliminate or reduce the risk introduced by medical devices. The plan will include performing firmware updates on devices, updating operating system versions, changing communication protocols, applying vendor-provided patches for known vulnerabilities and suggesting network segmentations.

Event Detection and Response

Event detection and response uses the output from risk analysis to monitor activity within and surrounding medical devices for the identified risks. When a risk manifests into a breach, this function will create an event notification, communicating all known details of the detected breach to support action on the part of the organization. If the tool is configured appropriately, it can also automatically respond to secure the organization in certain situations, although few, if any, healthcare delivery organizations (HDOs) use this feature.

Device Analytics and Management

Device analytics provides operational information about the usage of devices to HDO administration. Early use cases for this information include accurate counts of active devices over a period of time that inform device population levels. This capability helps the organization rightsize device population levels, reducing cost by identifying underutilized equipment. A strong opportunity exists to include GenAI capabilities to augment the ability of users to query and analyze the rich data repository for many operations management use cases. These include device utilization patterns, risk distribution among the device population and mitigation implementation progress.

Market Description

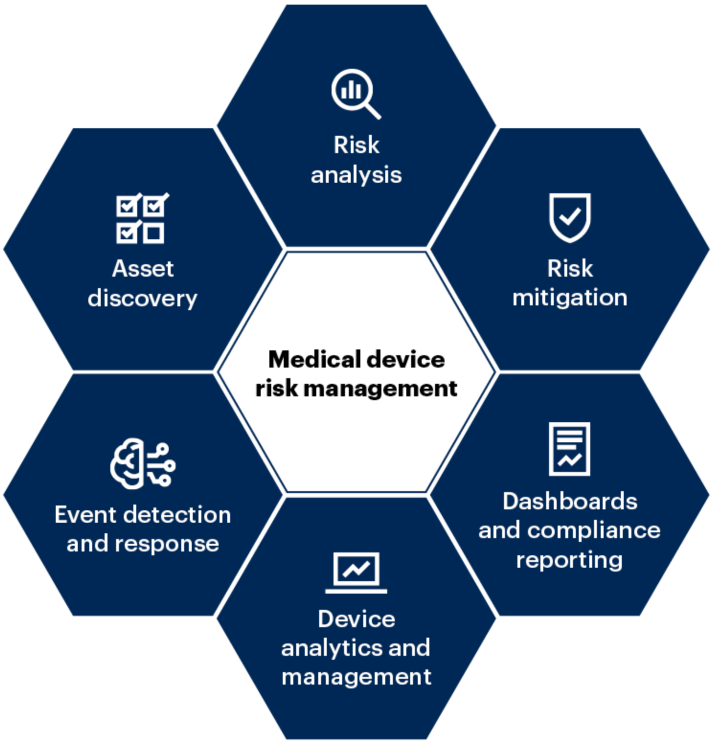
Medical device manufacturers traditionally have not included or embedded cyber protections in their products, resulting in large, vulnerable populations of hospital clinical endpoint devices. The healthcare provider CIO and CISO must minimize the risks exposed by these unprotected devices. Currently, the standard practice is to monitor their environments in real-time in anticipation of an attack. This does not mitigate the risks; it simply accelerates the reaction time of cyber response teams, which in best-case scenarios can lower the amount of damage or data loss.

Vendors have responded to this monitoring need and have created various products to assist health systems in understanding the cyber risks their medical devices pose to their enterprises. This market is maturing with the dominant players providing well-developed risk management solutions that can discover devices, assess device population risk levels, monitor for those risks and provide contextualized risk mitigation advice (see Figure 1). End users have become more sophisticated and are expressing interest in proactive mitigation. They are looking for device-embedded protections. They are also looking critically at the networks where the devices attach — looking for novel ways to prevent cyber criminals from locating and targeting their devices.

Several governments have implemented national regulations emphasizing the proactive protection of IT systems vital to critical infrastructure, including hospitals. These regulations will drive changes in device manufacturing and network defense strategies, helping organizations shift from a largely reactive security posture to a proactive one.

Figure 1: Key Capabilities of Medical Device Risk Management Platforms

Medical Device Risk Management Key Functional Requirements


Risk analysis
Asset discovery
Risk mitigation
Medical device risk management
Event detection and response
Dashboards and compliance reporting
Device analytics and management

Source: Gartner
791902_C

Market Direction

Over the last several years, healthcare provider organizations have acquired risk identification and mitigation tools for medical devices and other forms of IoMT. After building their experience and understanding of their IoMT populations and behaviors from a cybersecurity perspective, they have expanded their view of what is necessary today to protect their environments. In the early days of this market, vendors responded to a narrower set of discovery and risk measurement requirements and use cases, creating product capability blind spots.

Today, the understanding of cybersecurity needs in this industry is much broader. The current need is to bring into focus IoMT's participation in large, complex workflows that include people, software and other devices, including other IoMT. This new perspective continues to drive interest in this market space, bolstered by market drivers including:

- **Growing threats —** Medical devices play a vital role in diagnosing and treating patients. The more connected they become, the more they expand the attack surface. This increasingly makes them attractive targets for ransomware and the development of targeted malware. The number of disclosed attacks continues to rise. [1] From the recent RunSafe's 2025 Medical Device Cybersecurity Index Report, [2] of the healthcare providers that experienced a medical device compromise:
    - 43% experienced one to four hours of downtime
    - 31% faced five to 12 hours without critical systems
    - 19% dealt with downtime exceeding 13 hours
    - 7% experienced more than three days of device unavailability
- **Increasing vulnerabilities —** Year over year, the number of disclosed vulnerabilities grows. In many ways, the increasing number of vulnerabilities is linked to security researchers and vendors focusing on medical devices as they become increasingly connected. But it is also because, traditionally, medical device manufacturers regarded the problem of cyber vulnerabilities as something to take care of in the postmarket.

- **Infosec skills shortages —** Skills shortages, in areas such as security engineering, security assessments and clinical security operations, have made it clear that developing an effective security strategy that spans IT and clinical environments is challenging for healthcare provider organizations. This creates increasing demand for software tools to enhance a healthcare provider organization's risk management capability without increasing required staff levels.

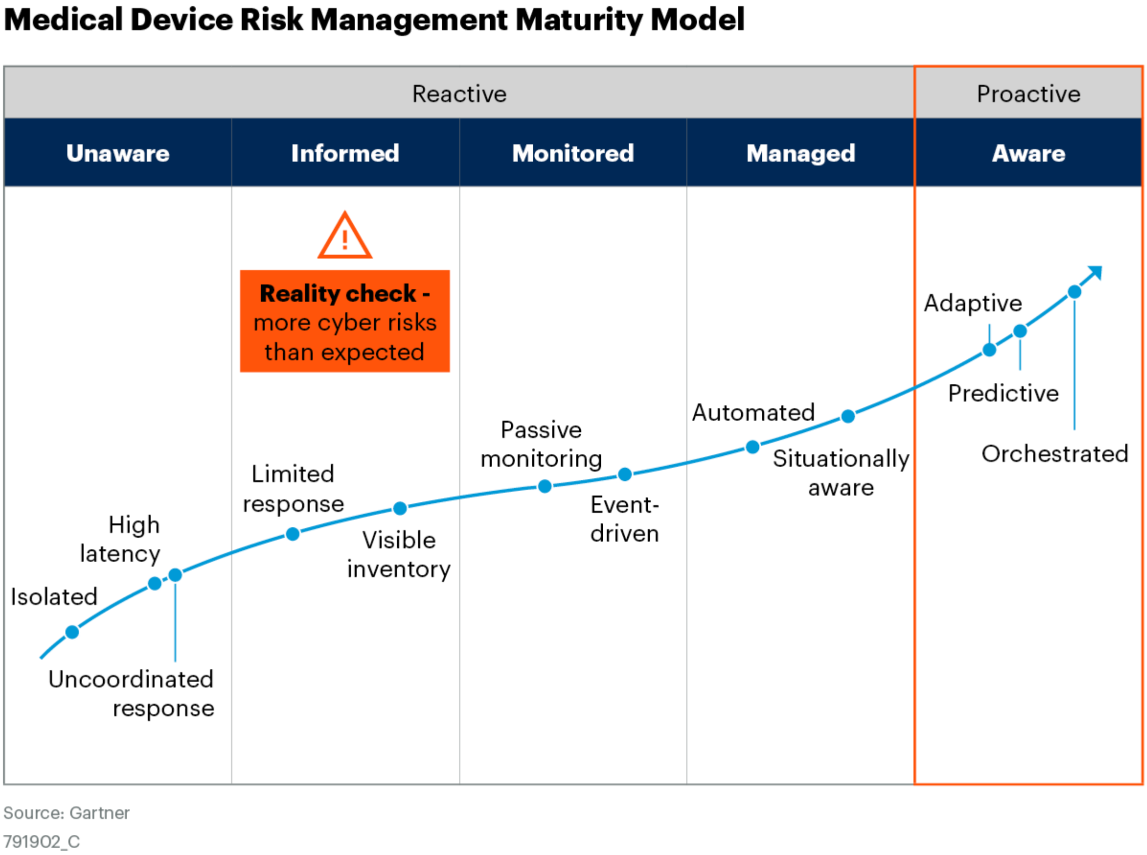
- **Government involvement —** Due to increased threats to critical infrastructure-related organizations, governments recognize that the ubiquitous IoMT technology landscape supporting them is key to national security. As a result, new regulations, directives and frameworks are emerging:

  - In the U.S., the Consolidated Appropriations Act of 2023 granted the U.S. Food and Drug Administration (FDA) the authority to require medical device manufacturers to submit cybersecurity risk management details as part of the premarket device submission process. Starting in October 2023, [3] the FDA can refuse submissions lacking sufficient cybersecurity risk management information.

  - In the EU, the Medical Device Coordination Group (MDCG) 2019-16 Rev.1 Guidance on Cybersecurity for medical devices provides "essential safety requirements for all medical devices that incorporate electronic programmable systems and software that are medical devices in themselves. [4] They require manufacturers to develop and manufacture their products by the state of the art, taking into account the principles of risk management, including information security, as well as to set out minimum requirements concerning IT security measures, including protection against unauthorized access." This guidance follows the same path the FDA took in the U.S. to introduce cybersecurity best practices to the medical device manufacturing industry before the passing of the regulation.

With several years of end-user experience and vendor process improvements in IoMT risk management, Gartner has identified an emerging maturity model. The ultimate objective of this model is comprehensive situational awareness of the medical device landscape, offering complete end-to-end visibility. This encompasses the proactive monitoring of all operational facets of every device, spanning data, network, physical, mechanical and patient safety. Consequently, vendors are adapting to this demand, shifting their focus from reactive to proactive approaches in medical device risk management (see Figure 2).

Figure 2: Medical Device Risk Management Maturity Model



Source: Gartner
791902_C

The maturity model has five stages, from “unaware” to “aware.” The first four stages are considered “reactive” in that the organization can only respond to a cyber event after the event has already occurred in its environment. The fifth and final stage represents “proactive” capabilities, where the healthcare provider organization’s CISOs can prevent attacks before they impact the enterprise. As the cyberthreats continue to increase, healthcare provider organization CISOs are pushing their teams to become more proactive. They recognize that the current managed response approach does not provide complete protection, and network microsegmentation (the most common of these risk mitigation approaches) has its limits.

The current market space has developed sophisticated capabilities to address the first four maturation stages. Over time, the playing field has evened out from a key functional requirement perspective — all vendors in the market fulfill the requirements for the “reactive” stages of the maturity model (see Note 1 for a full listing of capabilities and integrations).

Reactive:

- **Unaware** — This is the nascent maturity stage, the starting point for the risk management journey. Typical risk response behaviors are uncoordinated, with each event handled in isolation and a very long elapsed period between detection and response.

- **Informed** — This stage represents an organization with an accurate inventory of its IoMT populations that has begun classifying and prioritizing its risks. It is hallmarked by a reality check moment when the organization realizes that it has many more IoMT-based connected devices and associated cyber risks than expected. Healthcare provider organizations in this stage have begun to balance their risk tolerance level with the financial realities of mitigation costs.

- **Monitored** — Represents the growth in monitoring capability and the transformation of the organization's attack response abilities. Unlike the earlier maturity stages, the responses begin to be coordinated across IT, clinical and operational departments. Healthcare provider organizations at this stage begin to view IoMT populations from an ecosystem perspective rather than as isolated devices.

- **Managed** — With the situational awareness and automation capabilities provided by software-based risk management solutions, healthcare provider organizations can begin to take an enterprise-level, managed approach to IoMT risks. Fluid data integrations between the various software applications and operational and security management platforms enable automated, cross-departmental responses to active cyberattack events.

Proactive:

- **Aware** — The next era for this market space will be differentiated by vendors' ability to develop capabilities that allow their healthcare provider organization customers to get ahead of cyberthreats, proactively protecting their environments and patients. We expect a more proactive methodology to emerge, including a device-centric approach. This approach would stop malicious activity before it enters the healthcare provider organization's network.

Market Analysis

The medical device risk management landscape has shifted significantly. Organizations are moving away from reactive cybersecurity measures driven by fear toward a more proactive, engineered information security framework. Medical devices are no longer viewed in isolation, but rather as a component within the broader IoT ecosystem. This allows for centralized governance similar to IT endpoints. Consequently, risk management platforms have adapted, offering capabilities extending beyond medical devices to encompass most IoT devices within healthcare environments.

Healthcare providers today have a clearer understanding of their cyber risks. Many have well-established risk management programs with supporting protective technologies. Healthcare provider leaders now expect their medical device risk management platforms to recognize their specific, local and unique topology, and report on their distinct exploitability and vulnerabilities. It is no longer viable for these platforms to simply discover and report on known industry risks; they must contextualize that risk to the local environment, providing direct and precise medical device risk reporting and advice.

Evolving Threat Surface

As the IoMT market matures, the threat surface expands with additional threat vectors, such as embedded wireless access points within medical devices. Some medical device manufacturers supply access points built into devices that allow wireless communication between system components. Medical imaging systems are an example. In addition, many simple devices have built-in wireless capability, creating direct vulnerabilities. If not adequately protected and monitored, these independent access points and directly accessible devices can bridge the outside world and the provider organization’s network. Solutions like those sold by Aireye, Bastille and LOCH Technologies address this emerging wireless airspace threat surface (see Table 2).

Device Management Opportunity

Additionally, in the U.S., with the passing of the Consolidated Appropriations Act, provider organization customers of medical device risk management solutions will have another set of options to address the cyber risks inherent in their device populations, from the medical device manufacturers themselves. Similar to methods used to manage IT endpoint cyber protection, medical devices will soon require the same operational attention. Rather than viewing this as a threat, the medical device risk management solution market should use this milestone event as an opportunity to evolve its solutions. The advent of regulated, device-embedded, cyber-risk protections opens the door for existing risk-monitoring platforms to help end users proactively respond to the dynamic risk environment by creating a life cycle management feature, including visibility of software bills of materials (SBOMs).

Dashboards and Compliance Reporting Requirements

Dashboards and compliance reporting fulfill healthcare provider organization requirements to display and disseminate information collected and analyzed by these solutions. Dashboard displays can be added to security or network operation centers and biomedical engineering workplaces to communicate real-time operational information about medical device status. These solutions can also provide medical device compliance reporting for government regulatory requirements and internal policy audit needs.

Privacy compliance is becoming an increasingly important component of these tools. Deep packet inspection reveals protected health information (PHI) data flows, and some representative vendors offer their compliance consultant practice or partner with companies to meet these needs. As this market evolves, we expect more privacy compliance monitoring and response capabilities to be built into these software platforms.

Alternate Approach

Today, most solutions in this space take a reactive approach to medical device risk management because they are built to detect cybersecurity issues and then take action in response. Typically, the response will align with suggestions for network segmentation changes. One emerging approach is transport access control (TAC). Invisinet’s product offering represents this technique (see its entry in Vendor Profiles). This approach would stop malicious activity before it enters the healthcare provider organization’s network.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

Gartner has included a range of vendors in this research to ensure coverage from a geographical and capabilities perspective. Gartner estimates that more than 30 vendors in this market claim to offer medical device risk management solutions (see Note 2). Those included in this Market Guide:

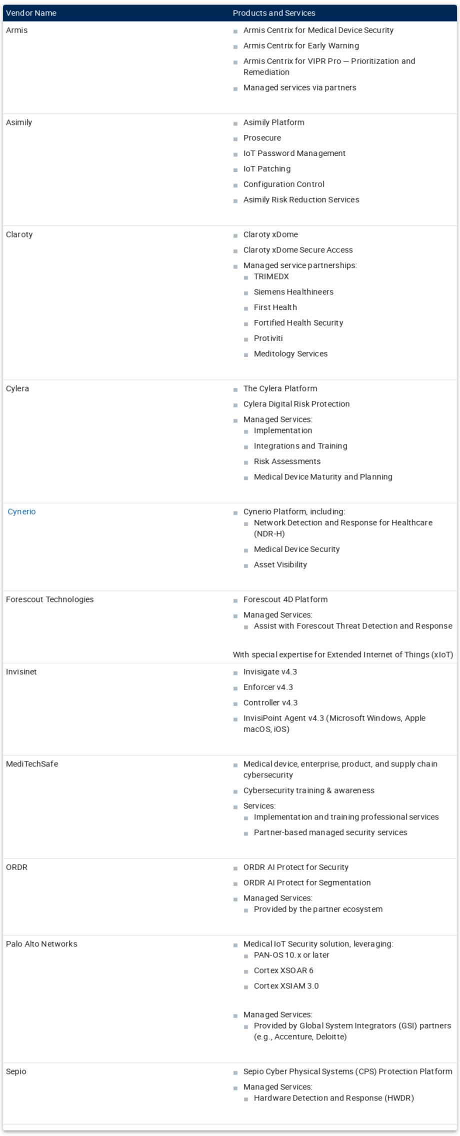
- Are visible to Gartner clients (based on inquiries)
- They are variable in size and distribution to reflect the buying population
- Have a clear end-user and outcome-focused offering, distinct from pure technology-driven offerings

A list of representative vendors for medical device risk management solutions is provided in Table 1. Table 2 highlights representative vendors in wireless airspace defense for healthcare providers.

Table 3 highlights representative vendors supporting medical device manufacturing risk management.

Table 1: Representative Vendors in Medical Device Risk Management Solutions

(Enlarged table in Appendix)



Vendor Name	Products and Services
Armis	■ Armis Centrix for Medical Device Security ■ Armis Centrix for Early Warning ■ Armis Centrix for VIPR Pro — Prioritization and Remediation ■ Managed services via partners
Asimily	■ Asimily Platform ■ Prosecure ■ IoT Password Management ■ IoT Patching ■ Configuration Control ■ Asimily Risk Reduction Services
Claroty	■ Claroty xDome ■ Claroty xDome Secure Access ■ Managed service partnerships: ■ TRIMEDX ■ Siemens Healthineers ■ First Health ■ Fortified Health Security ■ Protiviti ■ Meditology Services
Cylera	■ The Cylera Platform ■ Cylera Digital Risk Protection ■ Managed Services: ■ Implementation ■ Integrations and Training ■ Risk Assessments ■ Medical Device Maturity and Planning
Cynerio	■ Cynerio Platform, including: ■ Network Detection and Response for Healthcare (NDR-H) ■ Medical Device Security ■ Asset Visibility
Forescout Technologies	■ Forescout 4D Platform ■ Managed Services: ■ Assist with Forescout Threat Detection and Response With special expertise for Extended Internet of Things (xIoT)
Invisinet	■ Invisigate v4.3 ■ Enforcer v4.3 ■ Controller v4.3 ■ InvisiPoint Agent v4.3 (Microsoft Windows, Apple macOS, iOS)
MediTechSafe	■ Medical device, enterprise, product, and supply chain cybersecurity ■ Cybersecurity training & awareness ■ Services: ■ Implementation and training professional services ■ Partner-based managed security services
ORDR	■ ORDR AI Protect for Security ■ ORDR AI Protect for Segmentation ■ Managed Services: ■ Provided by the partner ecosystem
Palo Alto Networks	■ Medical IoT Security solution, leveraging: ■ PAN-OS 10.x or later ■ Cortex XSOAR 6 ■ Cortex XSIAM 3.0 ■ Managed Services: ■ Provided by Global System Integrators (GSI) partners (e.g., Accenture, Deloitte)
Sepio	■ Sepio Cyber Physical Systems (CPS) Protection Platform ■ Managed Services: ■ Hardware Detection and Response (HWDR)

Source: Gartner (July 2025)

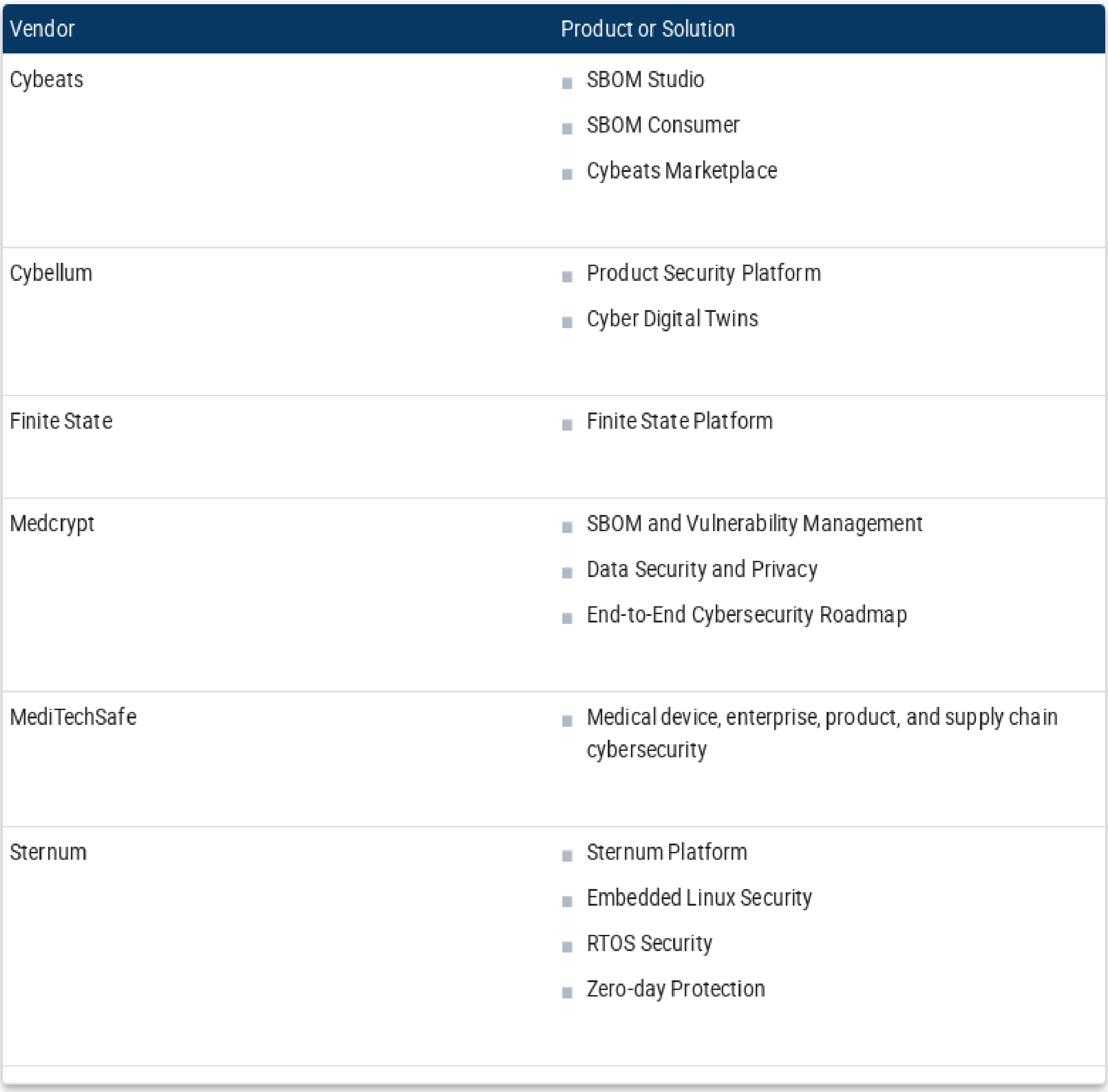
Table 2: Representative Vendors in Wireless Airspace Defense

Vendor Name	Product or Solution
Aireye	- AirEye Dome
Bastille	- Bastille Enterprise - Bastille FlyAway Kits
LOCH Technologies	- AirShield

Source: Gartner (July 2025)

Table 3: Representative Vendors in Medical Device Manufacturer Risk Management

(Enlarged table in Appendix)



Vendor	Product or Solution
Cybeats	- SBOM Studio - SBOM Consumer - Cybeats Marketplace
Cybellum	- Product Security Platform - Cyber Digital Twins
Finite State	- Finite State Platform
Medcrypt	- SBOM and Vulnerability Management - Data Security and Privacy - End-to-End Cybersecurity Roadmap
MediTechSafe	- Medical device, enterprise, product, and supply chain cybersecurity
Sternum	- Sternum Platform - Embedded Linux Security - RTOS Security - Zero-day Protection

Source: Gartner (July 2025)

Vendor Profiles

Details are provided for medical device risk management solution vendors only. Visit the vendors' websites for wireless airspace defense and medical device manufacturer risk management solutions.

Armis

- **Location:** San Francisco, California
- **Ownership:** Private
- **Coverage:** Global
- **Healthcare Focus:** Multivertical, including providing services to hospitals, medical manufacturing, R&D and biomedical companies

Armis provides real-time exposure management insights across medical devices, IT, operational technology (OT) and IoT, powered by its Asset Intelligence Engine, currently profiling over 6 billion assets. Armis issues early warning threat intelligence alerts to find and stop attacks before they launch. Its vulnerability database powers AI insights on emerging risks. The company believes that balancing security with the need for consistent uptime requires proactive protection tailored for healthcare. Armis' view is that medical device risk management must move beyond visibility and shift to predictive threat intelligence, detection, patient-centric prioritization and remediation.

Armis' AI-driven vulnerability management deduplicates, contextualizes, prioritizes and assigns mitigations based on a clinical risk score to directly improve patient safety and operational uptime. Its AI-driven risk prioritization differentiates Armis through clinical impact risk scoring, automated workflows, specialized threat intelligence and detection, anomalous behavior alerts and clinical usage/location data.

Asimily

- **Location:** Sunnyvale, California
- **Ownership:** Private
- **Coverage:** Global
- **Healthcare Focus:** Healthcare first

Asimily's platform provides real-time visibility into IoMT populations. It goes beyond reporting publicly available data by analyzing each issue to quantitatively prioritize the cost of risk and remediation along with the risk reduction benefit. Asimily's platform incorporates impact and likelihood analyses, allowing end users to prioritize patient care impact risks first. The company offers analytics that let end users allocate resources intelligently, which improves overall operational efficiencies.

Its vulnerability analysis offers targeted remediations, segmentation, microsegmentation and patching where possible, not just segmentation or patching. Asimily offers unique features such as configuration control (capturing benchmark snapshots of device metadata and comparing against the current state), packet capture and procurement risk analysis. Asimily understands the need for 24/7 vigilance in healthcare IT. Its platform sends configurable rule-based alerts when it detects suspicious activity from monitored devices. It offers integrated packet capture for any device. Asimily believes the medical device risk management space should provide full life cycle cybersecurity enhancements for IoMT (and other cyber-physical systems). This includes prepurchase risk analyses, gathering inventory, vulnerability mitigation — including configuration control for easy recovery — and automated patching.

Claroty

- **Location:** New York, New York
- **Ownership:** Private
- **Coverage:** Global
- **Healthcare Focus:** Multivertical, including services to the healthcare industry with dedicated leadership, product, delivery and marketing teams

Claroty's platform is backed by domain expertise in medical devices and clinical workflows inherited from its Medigate acquisition. It continues to innovate in this market, including assessing risk based on a device's purpose in the environment, advancing the use of nonpassive discovery in clinical networks, providing automated exposure remediation and including AI methodologies with its xDome Model Context Protocol (MCP) server. Claroty differentiates by providing insights for risk reduction with segmentation via codeless policy creation, impact-centric exposure management, healthcare-specific threat detection and device efficiency capabilities.

Claroty's platform is supported by internal healthcare experience, including dedicated business leaders and functions serving the healthcare sector. These include a center of excellence, evangelists, product line teams and customer care teams. The platform spans the entire medical device cybersecurity life cycle and is supported by a wide array of alliances with medical device manufacturers.

Cylera

- **Location:** New York, New York
- **Ownership:** Private
- **Coverage:** Global
- **Healthcare Focus:** Healthcare first

Cylera's platform provides a medical device asset intelligence and cybersecurity solution that fortifies care delivery and protects connected healthcare environments. The platform advances healthcare cyber maturity programs with intelligent attack surface management, improved service availability, and optimized productivity of teams that manage IoT and connected medical device security. Cylera differentiates from the market through its patented network traffic emulation and adaptive datatype analysis technology, which delivers high-fidelity asset intelligence, monitoring and risk profiling. Its team includes expert healthcare customer success managers.

Cylera is focused on ensuring that healthcare IoT and connected medical devices are safe and secure throughout their entire life cycle. Its platform identifies, evaluates, analyzes, assesses and mitigates potential risks associated with healthcare. It also ensures connected medical devices meet regulatory requirements in major markets for medical devices.

Cynerio

- **Location:** New York, New York
- **Ownership:** Private
- **Coverage:** Global
- **Healthcare Focus:** Healthcare first

Cynerio differentiates its medical device security platform with purpose-built network detection and response for healthcare (NDR-H), providing an active defense that identifies and contains threats in real time. In addition to sending alerts, NDR-H can remediate live attacks. It treats risk reduction as a strategy, combining proactive preparation and reactive controls, recognizing that cyberattacks on healthcare organizations are inevitable and can evade any single layer of defense. The platform is also designed to drive compliance with international regulatory standards for healthcare security.

The Cynerio platform delivers real-time control and response in clinical environments, going beyond the base capabilities of asset visibility, alerts and risk scores. It enables information security, biomedical engineering and network teams to collaborate around shared, actionable defense strategies. Cynerio leverages techniques adapted from other high-risk industries to strengthen operational security in healthcare environments. Success, to Cynerio, means containing unavoidable attacks quickly, safely and without impacting clinical workflows.

Forescout

- **Location:** San Jose, California
- **Ownership:** Private
- **Coverage:** Global
- **Healthcare Focus:** Multivertical, including providing services to healthcare, with a dedicated leader

The Forescout 4D platform includes real-time and continuous agentless discovery and classification of managed and unmanaged assets; traditional IT, IoT, IoMT, and OT/industrial control systems (ICS). Its healthcare-specific capabilities were acquired from CyberMDX and enhanced with OT capabilities through its SecurityMatters acquisition. These combined solutions provide persona-based, contextual visualization dashboards that deliver insights into risks, threats, behaviors and the compliance state.

Its platform enables systems to share policy-based decisions to automate proactive and reactive security controls. This reduces exposure and minimizes incident response time through a coordinated response. It provides integrations to more than 100 third-party IT and security products. This allows workflow automation and orchestration across disparate tools, and improves systemwide response to mitigate risks and respond to threats.

Invisinet

- **Location:** Houston, Texas
- **Ownership:** Private
- **Coverage:** North America (NA), EMEA
- **Healthcare Focus:** Multivertical, including providing solutions to healthcare

Invisinet can eliminate hackers' ability to surveil or perform reconnaissance of protected networks, disrupting attackers' ability to search for, find and exploit vulnerabilities. Unauthorized connection attempts elicit no response, making protected assets invisible to unauthorized access. Patented technology cloaks networks from unsolicited access. InvisiPoint agents provide identity-centric protection at the network layer to medical device networks. Its zero-trust authentication solution works entirely through the TCP/IP protocol, reducing overhead and maximizing performance. Its transport access control (TAC) approach supports both TCP and UDP protocols.

TAC authenticates users and client applications on the first packet receipt in a TCP/IP session. First Packet Authentication (FPA) [5] protects data and network applications by concealing network applications from port scans, network reconnaissance and intrusion, while allowing authenticated users to use network applications normally. A second feature of TAC, bidirectional authentication, ensures that it is protected against impostor servers and phishing attacks. [6]

MediTechSafe

- **Location:** Cincinnati, Ohio
- **Ownership:** Private
- **Coverage:** Global
- **Healthcare Focus:** Healthcare first

MediTechSafe's patented solution provides assurance-based asset discovery, risk/incident identification and management for various provider settings. It accounts for the vast diversity of devices, manufacturers, life cycles, configurations and clinical protocols. The platform enables risk management in a clinically and privacy-compliant manner.

The solution provides auditing, reporting and governance capabilities. It also considers human factors in cybersecurity, in addition to technical vulnerabilities. MediTechSafe provides its solution across various healthcare venues, including home health, imaging centers, surgery centers, labs, hospitals and enterprise-level integrated delivery networks (IDNs). Its solution incorporates a detailed understanding of clinical protocols to ensure patient safety. For MediTechSafe, the scope of medical device risk management involves devices and networks that are both secured by design and managed over their respective life cycles. Solutions can include technology tools, a platform and services.

ORDR

- **Location:** Santa Clara, California
- **Ownership:** Private
- **Coverage:** NA, Asia/Pacific (APAC), EMEA
- **Healthcare Focus:** Multivertical, including providing solutions to healthcare

The ORDR platform discovers, deduplicates, classifies and provides context on all connected devices using artificial intelligence/machine learning (AI/ML) educated from the millions of devices it has analyzed in addition to legacy flow data. The platform prioritizes risk based on business criticality, behavior and other device insights. It turns real-time network traffic into segmentation policies using collected intelligence such as classification, context and location. It also leverages large language models (LLMs) to simplify data search for end users.

ORDR believes that medical device risk management ensures resilient patient care by addressing risks across all connected assets. It defines the space as supporting the full medical device life cycle, including: an accurate contextual inventory, configuration management database/computerized maintenance management system (CMDB/CMMS) reconciliation, status monitoring, clinical impact assessment, and prioritizing actions like patching and segmentation, especially for legacy systems. The company believes it is not just about device protection, but securing all assets critical to care continuity.

Palo Alto Networks

- **Location:** Santa Clara, California
- **Ownership:** Public
- **Coverage:** Global
- **Healthcare Focus:** Multivertical, including a dedicated IoMT product

Palo Alto Networks views medical device risk management as integral to a healthcare organization's overall network security rather than a separately managed space. In that light, its platform provides broad visibility into all connected devices (IoMT, IoT, OT), highlighting risks such as vulnerabilities, recalls, weak passwords and insecure protocols. It can also detect poor security postures, such as unsanctioned apps and internet exposure. Mitigations include enablement for granular segmentation and policy enforcement. In addition, it offers virtual patching to reduce attack surface, prevent threats and support compliance.

Palo Alto Networks Medical IoT Security (acquired from Zingbox) is a portfolio-based, cloud-delivered, AI/ML-powered security subscription that is integrated within its Strata Network Security Platform and Cortex platforms. Through Strata, it provides comprehensive visibility, risk assessment, zero-trust security policy enforcement and AI-powered threat prevention for all connected (medical and nonmedical) devices. Its Cortex platform provides automation, including XSOAR. In addition, Palo Alto Networks provides visibility and security for 5G connected IoMT devices and secure access service edge (SASE), including internal IoMT traffic and intersite/WAN IoMT communications.

Sepio

- **Location:** Rockville, Maryland
- **Ownership:** Private
- **Coverage:** Global
- **Healthcare Focus:** Provides services to financial institutions and healthcare

Sepio's platform provides Layer 1 visibility to detect unmanaged, spoofed and legacy medical devices invisible to network or agent-based tools; this is a differentiator in the market. This approach allows its platform to provide close to 100% device identification and visibility within an extremely short period. The solution's trafficless, nonintrusive approach supports hybrid, air-gapped and offline environments without impacting clinical operations.

Sepio's CPS Protection Platform enforces device trust, provides real-time asset inventory, and integrates with CMDB, security information and event management (SIEM), and network access control (NAC) systems — enhancing patient safety, regulatory compliance and zero-trust adoption. The platform provides visibility into the medical device ecosystem, enabling healthcare organizations to inventory assets, detect vulnerabilities, establish device trust, enforce security policies and ensure compliance with industry standards.

Market Recommendations

As healthcare provider organizations continue to evolve their medical device risk management strategy, CIOs should add a medical device risk management solution to assist with the following:

- **In the near term:**
    - Inventory all IoMT assets, such as minor sensors, clinical facility controls and medical devices to create visibility into IoMT networks and topologies.
    - Assess the risk and regulatory exposure from IoMT-related initiatives and the healthcare provider organization's security posture.
    - Provision for IoMT risk management as a vital capability in digital transformation projects.

- **In the longer term:**
    - Incorporate regulatory compliance requirements for IoMT technologies within existing IT, CPS and physical security regulation tracking and management.
    - Align governance and oversight of IT and OT projects with digital risk reduction requirements introduced by IoMT.
    - Assign enterprise ownership for IoMT technologies, including those claimed by a business or clinical unit and clinical or biomedical engineering.
    - Enhance cyber response by including clinical engineering/biomedical engineering and clinical care team departments when updating policy and procedure.
    - Assess ecosystem integration points for IoMT implementations and determine design gaps in capabilities, skills and infrastructure (see Note 1 for integration opportunity list).
    - Develop deeper in-house IoMT security expertise.
    - Restructure skill sets and support resources (for example, organizational accountability and responsibility) to support the deployment and operation of secure IoMT systems.
    - Make medical device risk management a critical component of total medical device life cycle management.

Evidence

[1] 2025 Data Breach Investigations Report, Verizon.

[2] RunSafe Security's 2025 Medical Device Cybersecurity Index, RunSafe Security.

[3] Cybersecurity in Medical Devices: Quality System Considerations and Content of Premarket Submissions, U.S. Food and Drug Administration.

[4] MDCG 2019-16 Rev.1 Guidance on Cybersecurity for Medical Devices, European Union.

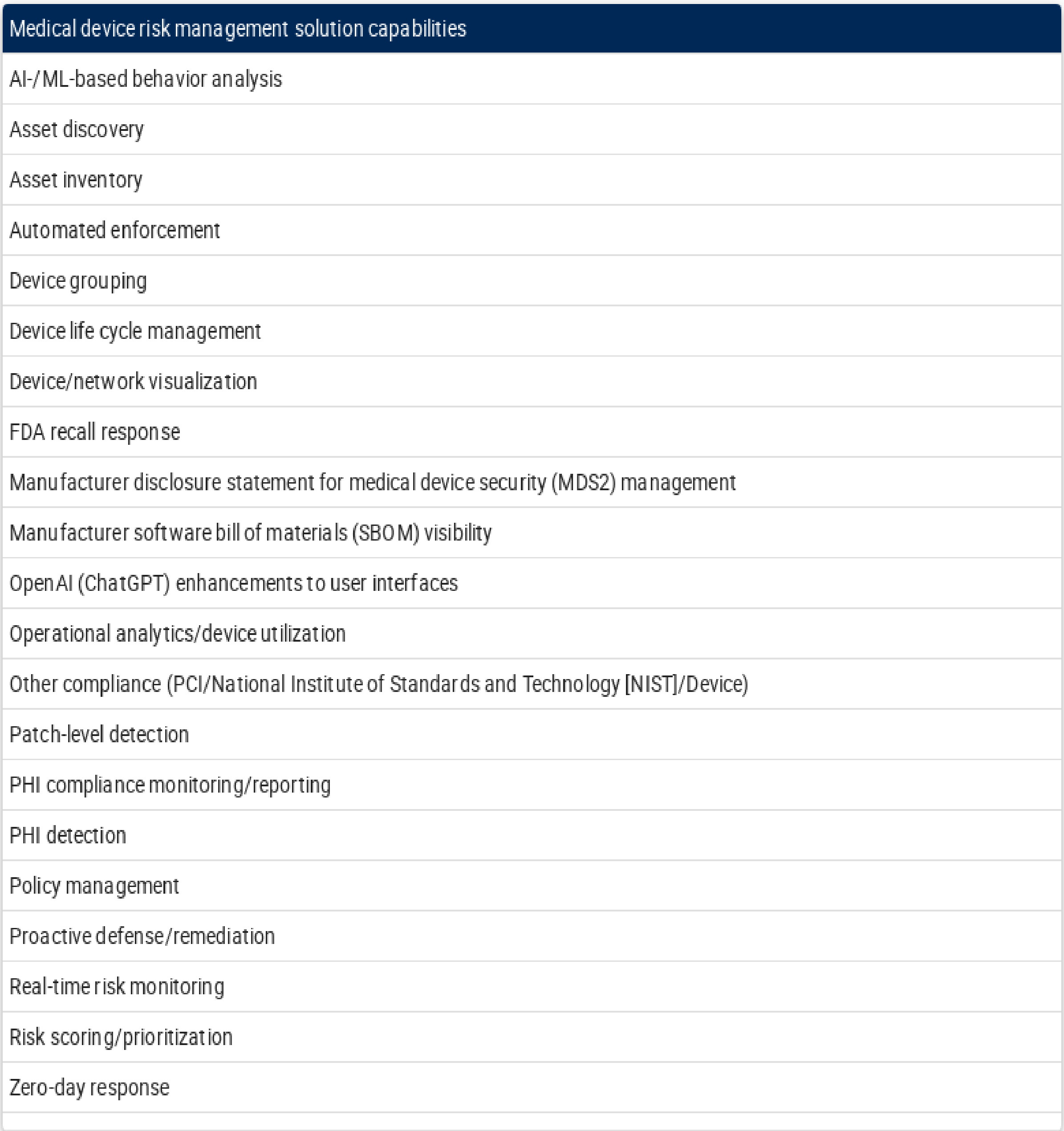
[5] Method for First Packet Authentication, John W. Hayes, Current Assignee: Invisinet.

[6] Implementing Zero Trust Cloud Networks With Transport Access Control and First Packet Authentication, IEEE Xplore.

Note 1: Market Solution Capabilities and Integrations

Table 4: Important Solution Capabilities

(Enlarged table in Appendix)

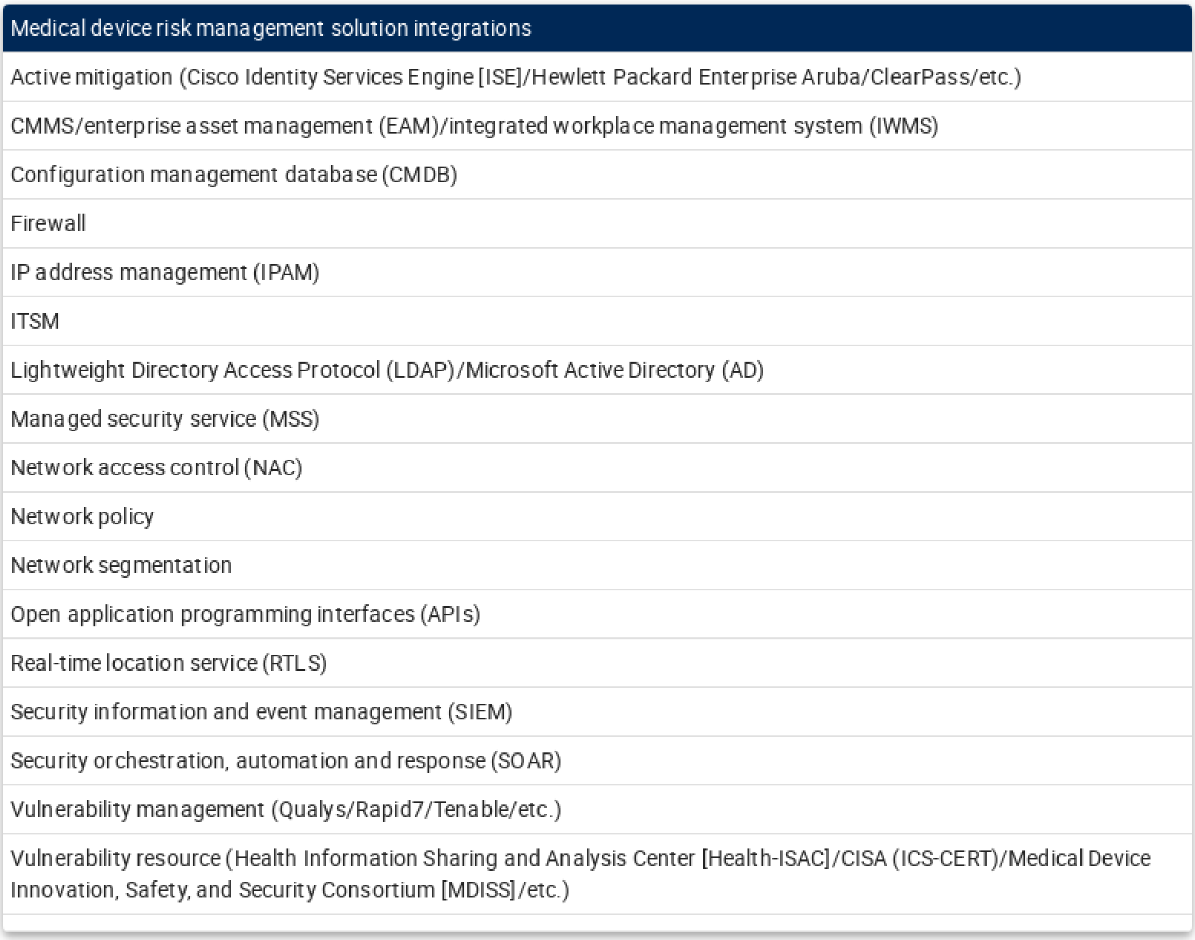


Medical device risk management solution capabilities
AI-/ML-based behavior analysis
Asset discovery
Asset inventory
Automated enforcement
Device grouping
Device life cycle management
Device/network visualization
FDA recall response
Manufacturer disclosure statement for medical device security (MDS2) management
Manufacturer software bill of materials (SBOM) visibility
OpenAI (ChatGPT) enhancements to user interfaces
Operational analytics/device utilization
Other compliance (PCI/National Institute of Standards and Technology [NIST]/Device)
Patch-level detection
PHI compliance monitoring/reporting
PHI detection
Policy management
Proactive defense/remediation
Real-time risk monitoring
Risk scoring/prioritization
Zero-day response

Source: Gartner (July 2025)

Table 5: Important Solution Integration Opportunities

(Enlarged table in Appendix)



Medical device risk management solution integrations
Active mitigation (Cisco Identity Services Engine [ISE]/Hewlett Packard Enterprise Aruba/ClearPass/etc.)
CMMS/enterprise asset management (EAM)/integrated workplace management system (IWMS)
Configuration management database (CMDB)
Firewall
IP address management (IPAM)
ITSM
Lightweight Directory Access Protocol (LDAP)/Microsoft Active Directory (AD)
Managed security service (MSS)
Network access control (NAC)
Network policy
Network segmentation
Open application programming interfaces (APIs)
Real-time location service (RTLS)
Security information and event management (SIEM)
Security orchestration, automation and response (SOAR)
Vulnerability management (Qualys/Rapid7/Tenable/etc.)
Vulnerability resource (Health Information Sharing and Analysis Center [Health-ISAC]/CISA (ICS-CERT)/Medical Device Innovation, Safety, and Security Consortium [MDISS]/etc.)

Source: Gartner (July 2025)

Recommended by the Author

Some documents may not be available as part of your current Gartner subscription.

2025 Cybersecurity Primer: Build and Optimize Cybersecurity Programs

How Healthcare and Life Science CIOs Can Assess and Mitigate the Most Critical Cyberthreats

Magic Quadrant for CPS Protection Platforms

Table 1: Representative Vendors in Medical Device Risk Management Solutions

Vendor Name	Products and Services
Armis	■ Armis Centrix for Medical Device Security ■ Armis Centrix for Early Warning ■ Armis Centrix for VIPR Pro — Prioritization and Remediation ■ Managed services via partners
Asimily	■ Asimily Platform ■ Prosecure ■ IoT Password Management ■ IoT Patching ■ Configuration Control ■ Asimily Risk Reduction Services
Claroty	■ Claroty xDome ■ Claroty xDome Secure Access ■ Managed service partnerships: ■ TRIMEDX Siemens Healthineers

	■ First Health ■ Fortified Health Security ■ Protiviti ■ Meditology Services
Cylera	■ The Cylera Platform ■ Cylera Digital Risk Protection ■ Managed Services: ■ Implementation ■ Integrations and Training ■ Risk Assessments ■ Medical Device Maturity and Planning
Cynerio	■ Cynerio Platform, including: ■ Network Detection and Response for Healthcare (NDR-H) ■ Medical Device Security ■ Asset Visibility
Forescout Technologies	■ Forescout 4D Platform ■ Managed Services:

	Assist with Forescout Threat Detection and Response With special expertise for Extended Internet of Things (xIoT)
Invisinet	Invisigate v4.3 Enforcer v4.3 Controller v4.3 InvisiPoint Agent v4.3 (Microsoft Windows, Apple macOS, iOS)
MediTechSafe	Medical device, enterprise, product, and supply chain cybersecurity Cybersecurity training & awareness Services: Implementation and training professional services Partner-based managed security services
ORDR	ORDR AI Protect for Security ORDR AI Protect for Segmentation Managed Services: Provided by the partner ecosystem
Palo Alto Networks	Medical IoT Security solution, leveraging:

	PAN-OS 10.x or later Cortex XSOAR 6 Cortex XSIAM 3.0 Managed Services: Provided by Global System Integrators (GSI) partners (e.g., Accenture, Deloitte)
Sepio	Sepio Cyber Physical Systems (CPS) Protection Platform Managed Services: Hardware Detection and Response (HWDR)

Source: Gartner (July 2025)

Table 2: Representative Vendors in Wireless Airspace Defense

Vendor Name	Product or Solution
Aireye	- AirEye Dome
Bastille	- Bastille Enterprise - Bastille FlyAway Kits
LOCH Technologies	- AirShield

Source: Gartner (July 2025)

Table 3: Representative Vendors in Medical Device Manufacturer Risk Management

Vendor	Product or Solution
Cybeats	- SBOM Studio - SBOM Consumer - Cybeats Marketplace
Cybellum	- Product Security Platform - Cyber Digital Twins
Finite State	- Finite State Platform
Medcrypt	- SBOM and Vulnerability Management - Data Security and Privacy - End-to-End Cybersecurity Roadmap
MediTechSafe	- Medical device, enterprise, product, and supply chain cybersecurity
Sternum	Sternum Platform

- Embedded Linux Security
- RTOS Security
- Zero-day Protection

Source: Gartner (July 2025)

Table 4: Important Solution Capabilities

Medical device risk management solution capabilities
AI-/ML-based behavior analysis
Asset discovery
Asset inventory
Automated enforcement
Device grouping
Device life cycle management
Device/network visualization
FDA recall response
Manufacturer disclosure statement for medical device security (MDS2) management
Manufacturer software bill of materials (SBOM) visibility
OpenAI (ChatGPT) enhancements to user interfaces
Operational analytics/device utilization
Other compliance (PCI/National Institute of Standards and Technology [NIST]/Device)
Patch-level detection
PHI compliance monitoring/reporting

PHI detection
Policy management
Proactive defense/remediation
Real-time risk monitoring
Risk scoring/prioritization
Zero-day response

Source: Gartner (July 2025)

Table 5: Important Solution Integration Opportunities

Medical device risk management solution integrations
Active mitigation (Cisco Identity Services Engine [ISE]/Hewlett Packard Enterprise Aruba/ClearPass/etc.)
CMMS/enterprise asset management (EAM)/integrated workplace management system (IWMS)
Configuration management database (CMDB)
Firewall
IP address management (IPAM)
ITSM
Lightweight Directory Access Protocol (LDAP)/Microsoft Active Directory (AD)
Managed security service (MSS)
Network access control (NAC)
Network policy
Network segmentation
Open application programming interfaces (APIs)
Real-time location service (RTLS)
Security information and event management (SIEM)
Security orchestration, automation and response (SOAR)

Vulnerability management (Qualys/Rapid7/Tenable/etc.)
Vulnerability resource (Health Information Sharing and Analysis Center [Health-ISAC]/CISA (ICS-CERT)/Medical Device Innovation, Safety, and Security Consortium [MDISS]/etc.)

Source: Gartner (July 2025)