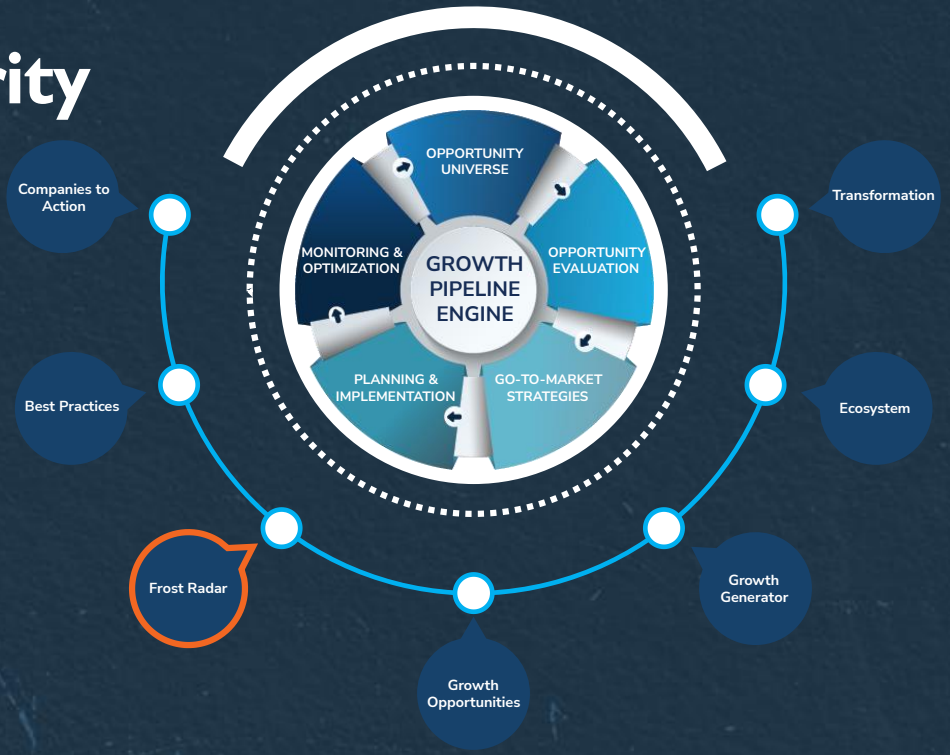
FROST & SULLIVAN

Frost Radar™: Healthcare Infrastructure Cybersecurity in North America, 2025

A Benchmarking System to Spark Companies to Action - Innovation that Fuels New Deal Flow and Growth Pipelines



Global Transformational Health Research Team at Frost & Sullivan

KB4A-48
April 2025

FROST & SULLIVAN

Strategic Imperative and Growth Environment

Strategic Imperative

- The healthcare cybersecurity market encompasses all systems, applications, and IT-enabled services that protect digital infrastructure, sensitive patient information, connected medical devices, and healthcare systems from cyberattacks. The increased adoption medical and non-medical devices, the interconnected nature of the ecosystem, the growing volume and complexity of data, evolving cyber threats, and regulatory compliance requirements are increasing security risks and patient safety concerns. In this context, there is a need for healthcare cybersecurity solutions with comprehensive technological capabilities, particularly in the United States as increasingly large cyberattacks affect patient care and cause financial, legal, and trust headaches for healthcare organizations.
- Healthcare infrastructure cybersecurity that allows data exchange between different systems from hospitals, clinics, and other healthcare providers is complex and includes modern and legacy systems that can create vulnerabilities. It safeguards the foundational systems and network architecture supporting operations, including data centers, servers, and communication layers. It protects against unauthorized access, data breaches, and cyber threats, ensuring secure and reliable healthcare delivery.
- The solutions must include technologies such as network segmentation and microsegmentation, zero trust network access, next-generation firewalls, intrusion detection and prevention systems, and security information and event management. The companies that are leading this market are adding more features to their products—usually all-in-one platforms, with more technological developments, continuous R&D, and partnerships and acquisitions. The success of healthcare infrastructure cybersecurity lies in comprehensive solutions at the device level, intelligence, and inventory of assets.
- Top companies are prioritizing critical system securitization, working on updates and patching regularly, and aligning their solutions for regulatory compliance while addressing challenges such as legacy systems, interoperability, scalability, and user experience.

Source: Frost & Sullivan

Growth Environment

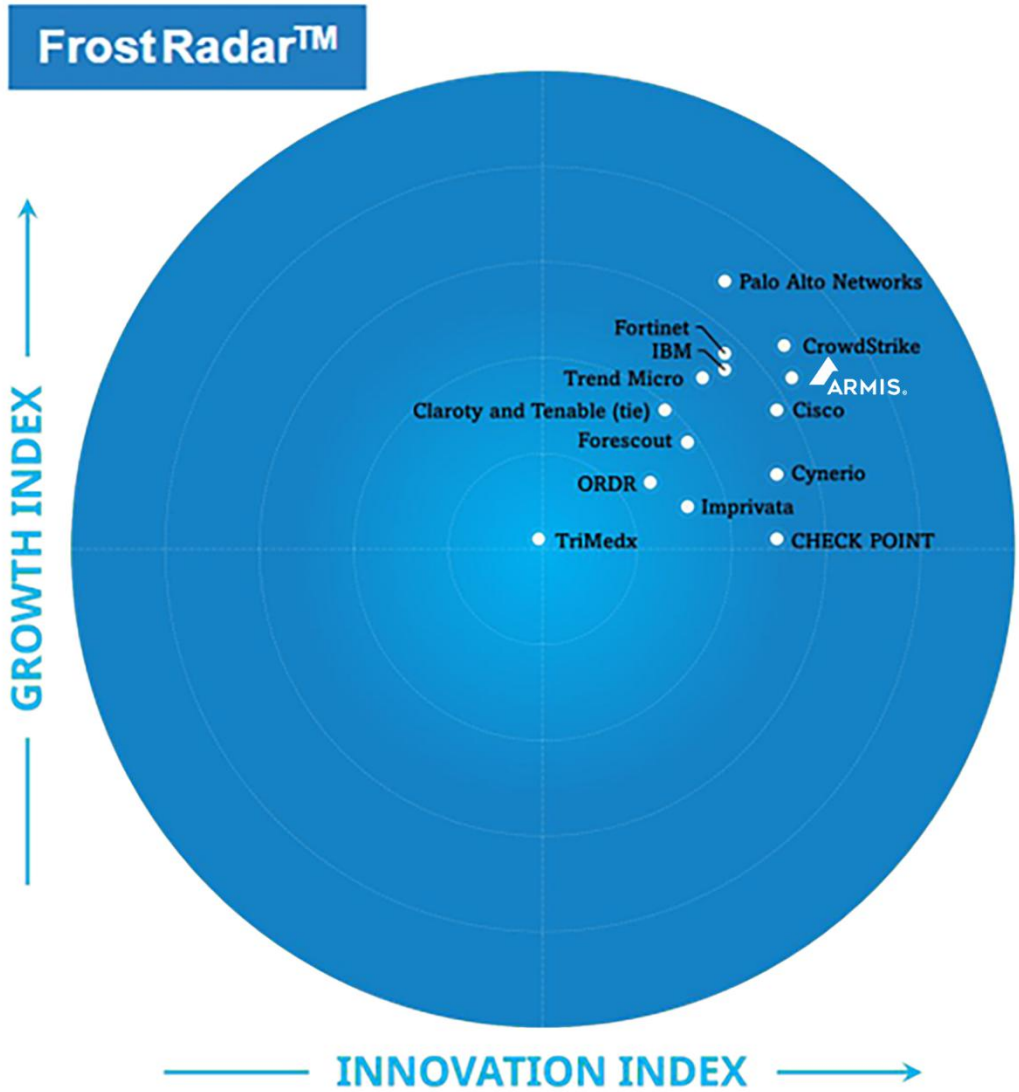
- The cybersecurity healthcare market in North America in 2024 was valued at $15.34 billion and is expected to be worth $37.84 billion by 2030 at a compound annual growth rate of 16.2%. The United States represents approximately 75% of the market.
- This market includes two kinds of vendors: large corporations operating in healthcare among multiple verticals and specialist SMEs. Both are leveraging increased global interest in healthcare cybersecurity, with a strong focus in the United States. In 2023, 57% of healthcare organizations in the United States planned a budget increase in 2024, demonstrating a need to take action to face increasing cyberattacks and their costs.
- Healthcare is a target for cyber attackers because the industry is highly vulnerable, putting patient safety at risk. The average cyberattack breach cost for healthcare in 2024 was $9.77 million.
- Healthcare organizations have some security guidance, but most is voluntary and does not guarantee patient safety. Various guidelines and best practices exist for enhancing security, yet the lack of standardized requirements leaves internal security teams overwhelmed, with no clear way to prioritize actions and limited resources for implementation. Until a minimum security standard is established and enforced, the regulatory landscape for healthcare security will remain uncertain.
- Other key initiatives shaping the regulatory landscape post-HIPAA include the Protecting and Transforming Cyber Healthcare (PATCH) Act (2023), the US Department of Health and Human Services' Healthcare and Public Health Cybersecurity Performance Goals (2024), and the National Institute of Standards and Technology's (NIST) Cybersecurity Framework.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Healthcare Infrastructure Cybersecurity in North America

Frost Radar™: Healthcare Infrastructure Cybersecurity in North America



FROST & SULLIVAN

Source: Frost & Sullivan

Frost Radar™ Competitive Environment

- From a field of active healthcare infrastructure cybersecurity competitors, Frost & Sullivan analyzed 50 vendors to better understand their solutions and ability to be agents of change in this rapidly evolving industry.
- From this list, Frost & Sullivan independently plotted 15 healthcare infrastructure cybersecurity providers on this Frost Radar™: Armis, Checkpoint Software Technologies, Cisco Systems, Claroty, CrowdStrike, Cynerio, Forescout Technologies, Fortinet, IBM, Imprivata, ORDR, Palo Alto Networks, Tenable, Trend Micro Incorporated, and TriMedx. They stand out for their sophisticated offerings, technologies, scalability, and capabilities.
- Companies on the Frost Radar™ adopt a robust vision focused on growth and rigorous innovation that promotes seamless integration of new technologies, identifies the critical needs of each area, and offers distinctive features for each use of their solutions. These players pursue a strong, collaborative strategy and investments to leverage industry trends and integrate new technologies and features into their solutions to stay at the forefront. Personalized, configurable offerings for each client distinguish these players in the market and bolster adoption.
- Palo Alto Networks leads on the Growth Index due to its strong market performance.
- CrowdStrike, Armis, Cisco, Cynerio, and CHECK POINT stand out on the Innovation Index thanks to their technological advancements.
- Fortinet, IBM, Trend Micro, Claroty, Tenable, and Forescout form a tight cluster just behind the leaders on each index.
- ORDR, Imprivata, and TriMedx show promise in specific areas, positioning them for potentially higher Innovation and Growth Index scores in the future.

Source: Frost & Sullivan

Frost Radar™ Competitive Environment (continued)

- Frost Radar™ Innovation and Growth leaders dominate innovation in the healthcare infrastructure cybersecurity space with more features, technological developments, and comprehensive solutions. R&D, partnerships, and acquisitions are also catalysts for growth.
- An early version of the Radar, published in 2023, included companies focused on IoT. The latest version focuses on infrastructure and network security, breaking it down into segments to account for this space's increasing complexity. More Frost Radar™ analyses for other segments in the space (e.g., cloud and application security) are expected to be published in the future.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™: Companies to Action

Armis

INNOVATION

- Armis Centrix™ has revolutionized healthcare cybersecurity by providing an end-to-end platform that delivers real-time visibility, automated asset discovery, and advanced risk assessment across medical devices, IT, and OT assets. Armis provides proactive risk insights and early indicators of threats including ransomware attacks that allow healthcare organizations to take action before an attack hits, easily mitigate vulnerabilities, and maintain operational continuity, This enables clinical engineering and IT security teams to rapidly identify vulnerabilities, streamline FDA recall management, and ensure compliance within a single platform—all while reducing operational errors and lowering costs. The platform's integrated approach improves patient safety, optimizes clinical workflows, and facilitates better collaboration between IT security and clinical teams to effectively reduce patient care risk.
- Continuous innovation is at the core of Armis's strategy, rated at 4.70 on the Innovation Index. The company has consistently enhanced its solution through in-house R&D and strategic acquisitions, such as Silk Security, CTCI, and OTORIO, which have enriched its AI-powered analytics, early warning, and on-premises OT security capabilities. These enhancements have elevated the platform's performance, enabling it to deliver contextual risk insights and prioritize vulnerabilities more effectively.
- The Armis platform's scalable architecture and vast integration ecosystem contribute to improved sensor accuracy, expanded medical device telemetry, and seamless integration with healthcare systems and electronic health records. Armis's AI-powered Asset Intelligence Engine leverages massive device behavior baselines across billions of assets, making threat detection and risk management more precise.

Source: Frost & Sullivan

Armis (continued)

INNOVATION

- Innovative features—from enhanced protocol analyzers and utilization integrations (including deeper analytics via DICOM PACS) to specialized dashboards (e.g., the FDA Recall and NHS Cyber Alerts Dashboards) reduce downtime, improve operational resilience, and empower healthcare organizations to make data-driven decisions that safeguard patient care. Armis Centrix ™ can secure every asset in the modern healthcare environment, ensuring patient-centric innovations and cementing Armis's leadership in cybersecurity technology for healthcare.
- Recent successes highlight Armis Centrix ™'s impact on healthcare, benefiting institutions such as Burke Rehabilitation Hospital in New York. The platform swiftly identifies previously unseen medical devices, reducing remediation times and enhancing patient safety. Burke Rehabilitation Hospital, facing vulnerabilities from its diverse medical devices, gained automated visibility, allowing it to address security risks and improve compliance and operational efficiency without disrupting care.

Source: Frost & Sullivan

Armis (continued)

GROWTH

- With a 4.0 score on the Growth Index, Armis has built a robust global presence by winning business across North America, Europe, and high-growth markets in Asia. The company's customer base spans Fortune 100 organizations and numerous healthcare providers with deployments in more than 165 countries and a broad portfolio of healthcare customers. This widespread market penetration reflects a deliberate strategy to address the cybersecurity challenges of digital transformation across diverse industries.
- The company's success is driven by a multifaceted growth strategy that integrates innovative sales and marketing initiatives, superior customer experience, and a strong partner ecosystem. Armis has leveraged targeted digital campaigns, thought leadership, and strategic alliances with cloud marketplaces and system integrators to boost market penetration and customer retention.
- A recent $200 million Series D investment has fueled organic growth, expansion into new verticals and regions, and strategic acquisitions. Armis acquired Silk Security and CTCI in 2024, enabling the launch of flagship solutions Armis Centrix™ VIPR Pro – Prioritization and Remediation and Armis Centrix™ for Early Warning. The recent OTORIO acquisition creates a hybrid and on-premises expansion of its OT and cyber-physical environments.
- The company's growth pipeline and market strategies include the development of a dedicated healthcare cybersecurity team with extensive industry expertise and the integration of a channel-first approach. These strategies have accelerated revenue growth and driven significant expansion in headcount and market share. The comprehensive product capabilities and customer success stories underscore its dynamic and evolving growth trajectory.

Source: Frost & Sullivan

Armis (continued)

FROST PERSPECTIVE

- Armis Centrix™ has established a robust cybersecurity platform that provides real-time visibility, automated asset discovery, and advanced risk assessment across IT, OT, and medical devices. To advance further, the company should expand for AI for predictive risk and modeling. This module should be tailored to clinical data streams and integrate with dashboards such as FDA Recall and NHS Cyber Alerts, offering proactive, context-aware risk mitigation recommendations.
- Armis stands out with its scalable architecture and integration capabilities, supporting deep analytics and early warning systems. Armis should work on extending and deepening integrations by enabling real-time data exchange between cybersecurity and clinical workflows. This would allow IT and clinical teams to act on risk insights immediately, optimizing workflows and reinforcing Armis's role in healthcare cybersecurity.
- Armis integrates with platforms such as ServiceNow and Palo Alto XSOAR for response automation in diverse healthcare environments. However, it could further enhance its orchestration capabilities. While Armis is already recognized by several manufacturers and regulators and works with many others, the company should continue partnering with additional sensor and medical device manufacturers to integrate cybersecurity protocols directly into next-generation devices, creating a secure ecosystem from the point of manufacture. Such collaborations would set Armis apart in a critical market, reinforcing its leadership.

Source: Frost & Sullivan

FROST & SULLIVAN

Best Practices & Growth Opportunities

Best Practices

1. Comprehensive solutions with more features require interoperability and scalability under a unified hospital system, with cybersecurity present at all levels of hospital infrastructure.

2. Healthcare organizations and cybersecurity companies must work together to overcome challenges such as legacy devices and systems, digital illiteracy, lack of expertise, and regulatory compliance.

3. Technological solutions that integrate consultancy practices and support regulatory compliance are required to ensure that healthcare infrastructure has adequate levels of cybersecurity.

Source: Frost & Sullivan

Growth Opportunities

1. Generative AI tools enhance cybersecurity by proactively identifying, defending, and mitigating threats, while automating tasks, such as threat hunting, anomaly detection, and incident response, through advanced data analysis. Healthcare organizations are adopting AI and generative AI to strengthen security measures, reduce administrative burdens, and address the shortage of expertise needed to handle fast-evolving security threats.

2. Managed security solutions can address escalating cyber threats, ensure regulatory compliance, and safeguard patient data across complex, interconnected systems. By leveraging advanced threat detection, real-time monitoring, and proactive incident response, these solutions empower healthcare organizations to strengthen cybersecurity, mitigate risks, and focus on delivering high-quality patient care without compromise.

3. A holistic cybersecurity approach integrates technologies, processes, people, and policies, focusing on risk evaluation, staff training, automated threat detection, recovery policies, compliance, and best practices. Key elements include risk and vulnerability evaluation, staff training, threat detection automation, recovery policy development, compliance, and the implementation of best practices.

Source: Frost & Sullivan

FROST & SULLIVAN

Frost Radar™ Analytics

Frost Radar™: Benchmarking Future Growth Potential 2 Major Indices, 10 Analytical Ingredients, 1 Platform

Growth Index

Growth Index (GI) is a measure of a company's growth performance and track record, along with its ability to develop and execute a fully aligned growth strategy and vision; a robust growth pipeline system; and effective market, competitor, and end-user focused sales and marketing strategies.

GI1

MARKET SHARE (PREVIOUS 3 YEARS)
This is a comparison of a company's market share relative to its competitors in a given market space for the previous 3 years.

GI2

REVENUE GROWTH (PREVIOUS 3 YEARS)
This is a look at a company's revenue growth rate for the previous 3 years in the market/industry/category that forms the context for the given Frost Radar™.

GI3

GROWTH PIPELINE
This is an evaluation of the strength and leverage of a company's growth pipeline system to continuously capture, analyze, and prioritize its universe of growth opportunities.

GI4

VISION AND STRATEGY
This is an assessment of how well a company's growth strategy is aligned with its vision. Are the investments that a company is making in new products and markets consistent with the stated vision?

GI5

SALES AND MARKETING
This is a measure of the effectiveness of a company's sales and marketing efforts in helping it drive demand and achieve its growth objectives.

Source: Frost & Sullivan

Frost Radar™: Benchmarking Future Growth Potential 2 Major Indices, 10 Analytical Ingredients, 1 Platform (continued)

Innovation Index

Innovation Index (II) is a measure of a company's ability to develop products/ services/ solutions (with a clear understanding of disruptive megatrends) that are globally applicable, are able to evolve and expand to serve multiple markets and are aligned to customers' changing needs.

II1

INNOVATION SCALABILITY
This determines whether an organization's innovations are globally scalable and applicable in both developing and mature markets, and also in adjacent and non-adjacent industry verticals.

II2

RESEARCH AND DEVELOPMENT
This is a measure of the efficacy of a company's R&D strategy, as determined by the size of its R&D investment and how it feeds the innovation pipeline.

II3

PRODUCT PORTFOLIO
This is a measure of a company's product portfolio, focusing on the relative contribution of new products to its annual revenue.

II4

MEGATRENDS LEVERAGE
This is an assessment of a company's proactive leverage of evolving, long-term opportunities and new business models, as the foundation of its innovation pipeline. An explanation of megatrends can be found here.

II5

CUSTOMER ALIGNMENT
This evaluates the applicability of a company's products/services/solutions to current and potential customers, as well as how its innovation strategy is influenced by evolving customer needs.

Source: Frost & Sullivan

Next Steps

JOIN:
Growth Council

APPLY:
Companies to Action

ENGAGE:
Growth Dialog

PARTICIPATE:
Growth Council Think Tank

Does your current system support rapid adaptation to emerging opportunities?

Source: Frost & Sullivan

Legal Disclaimer

Frost & Sullivan is not responsible for any incorrect information supplied by companies or users. Quantitative market information is based primarily on interviews and therefore is subject to fluctuation. Frost & Sullivan research services are limited publications containing valuable market information provided to a select group of customers. Customers acknowledge, when ordering or downloading, that Frost & Sullivan research services are for internal use and not for general publication or disclosure to third parties. No part of this research service may be given, lent, resold, or disclosed to noncustomers without written permission. Furthermore, no part may be reproduced, stored in a retrieval system, or transmitted in any form or by any means—electronic, mechanical, photocopying, recording, or otherwise—without the permission of the publisher.

For information regarding permission, write to: permission@frost.com