FROST & SULLIVAN

2024 TECHNOLOGY INNOVATION LEADER

IN THE GLOBAL HEALTHCARE CYBERSECURITY INDUSTRY

ARMIS®

FROST & SULLIVAN

2024 BEST PRACTICES AWARD

Best Practices Criteria for World-Class Performance

Frost & Sullivan applies a rigorous analytical process to evaluate multiple nominees for each award category before determining the final award recipient. The process involves a detailed evaluation of best practices criteria across two dimensions for each nominated company. Armis excels in many of the criteria in the healthcare cybersecurity space.

Security Breaches Challenging the Healthcare Industry

Globally, the healthcare cybersecurity market faces persistent challenges with security breaches that trigger internal and external cyberattacks. These breaches jeopardize essential systems and devices vital for clinical, financial, and operational decisions. The proliferation of the Internet of Things (IoT) and Operational Technology (OT) devices, along with cloud assets and internet-exposed devices, has significantly increased the complexity of securing healthcare environments. Consequently, there is an evident need for relentless, 24/7 surveillance in these intricate and interconnected systems that depend on centralized frameworks.

Enterprise-grade security solutions provide safe access, aggregation, identification, and coordination of health information across the care continuum. Security-management-as-a-service (SMaaS) models represent a transformative shift by blending high-level security with specialized features, offering enhanced flexibility. However, budget constraints and a shortage of cybersecurity expertise present significant challenges, limiting healthcare organizations' ability to address escalating cybersecurity threats.

Healthcare organizations require comprehensive visibility of their assets to manage ransomware and other cybersecurity threats effectively. Challenges such as mergers, acquisitions, third-party vendor integration, evolving regulations, and cyber insurance mandates all complicate this objective. Frost & Sullivan recognizes how Armis, nonetheless, uniquely navigates these challenges with its sophisticated

security solutions. The Armis Centrix™ platform employs artificial intelligence (AI) and machine learning to deliver robust protection across the attack surface, ensuring real-time visibility and risk management. Its exceptional integration capabilities enable seamless coordination of security measures across all connected assets - empowering healthcare organizations to maintain a proactive security posture and manage their cyber risk exposure.

Armis: Driving the Cybersecurity Landscape

Founded in 2016 and headquartered in California, Armis is a premier asset intelligence cybersecurity company that safeguards the entire attack surface and manages cyber risk exposure in real-time. It supports Fortune 100, Fortune 200, and Fortune 500 companies, ensuring continuous protection and management of critical assets in a rapidly evolving, perimeter-less world. Armis serves various sectors: government, state, local, education, healthcare, critical infrastructure providers, retail, manufacturing, smart cities, transport, and energy. Esteemed organizations such as Main Line Health, University Health Network, Nuvance, Colgate-Palmolive, United Airlines, Allegro MicroSystems, Takeda Pharmaceuticals, Mondelēz International, DocuSign, and Booking Holdings all depend on Armis for comprehensive cybersecurity solutions that provide unparalleled visibility, and robust security and manageability.[1]

Armis Centrix: The Most Advanced Cyber Exposure Management Platform

Armis Centrix™ is the most advanced cyber exposure management platform. The suite of products on the Armis Centrix™ platform utilize Armis' AI-driven Asset Intelligence Engine to provide global visibility, security, and management of billions of assets at all times. This cloud-based solution mitigates cyber asset risks, remediates vulnerabilities, and blocks threats. At the same time, Armis Centrix™ helps organizations eliminate security gaps, optimize information technology (IT) network security, and ensure compliance with industry regulations. The platform extends its capabilities across critical areas such as OT/IoT security, medical device security, and actionable threat intelligence. It identifies and secures essential assets while prioritizing vulnerabilities based on business-critical factors, and remediates vulnerabilities and security findings, thereby neutralizing attacks before they impact organizations. The result is an unmatchable transformation of security operations - from reactive to proactive.

> *"The platform's overarching distinction is that, through a single pane of glass, it provides a real-time, contextual view of the environment and security posture, monitoring and managing all assets affecting patient care, including IT, OT, IoT, medical devices, enterprise assets, and cloud infrastructure. In addition to this robust visibility, Armis offers cutting-edge threat intelligence and forensic monitoring capabilities."*
>
> ***- Manuel Albornoz***
> ***Best Practices Research Analyst***

Armis Centrix™ has established itself as a leading cybersecurity product, achieving the goal of managing over 500 billion events daily and tracking over five billion assets globally.[2] To this end, the company ensures robust coverage and real-time visibility across over 200,000 deployments in 165 countries.[3] The

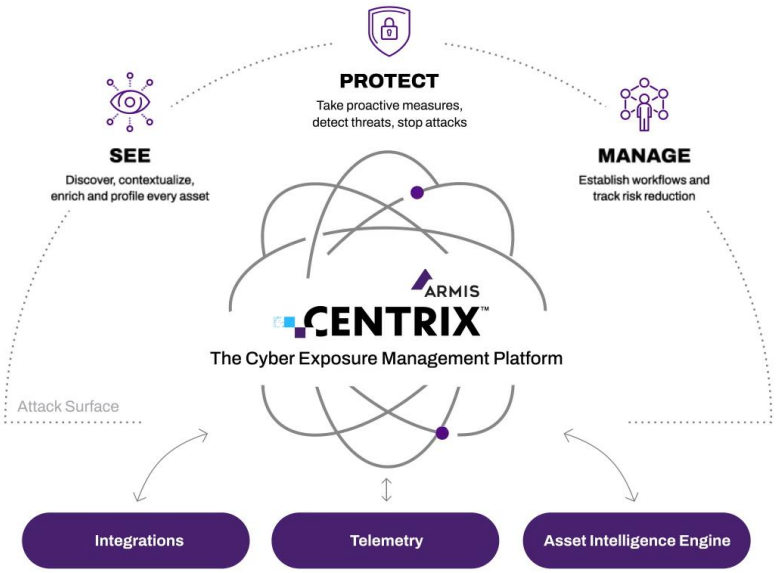
[1] "About Armis" (Armis website: https://www.armis.com/about/about-armis/)

[2] Provided by Armis (Frost & Sullivan, June 2024)

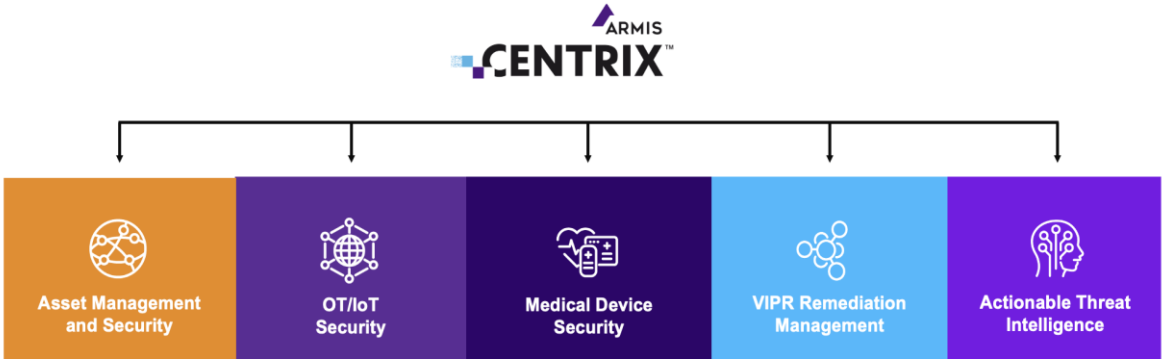
[3] Ibid.

platform's overarching distinction is that, through a single pane of glass, it provides a real-time, contextual view of the environment and security posture, monitoring and managing all assets affecting patient care, including IT, OT, IoT, medical devices, enterprise assets, and cloud infrastructure.

In addition to this robust visibility, Armis offers cutting-edge threat intelligence and forensic monitoring capabilities. Armis Centrix™ scrutinizes network activity, connections, domain name system requests, and application usage to detect anomalies and threats. Frost & Sullivan notes that such comprehensiveness has the milestone of successfully preventing over 500,000 attacks monthly, with Armis Centrix™ for Actionable Threat Intelligence (ATI) further boosting this predictive capability.[4]



A key highlight of the company is its multidimensional asset inventory, which categorizes devices by type, location, role, criticality, and ownership. The in-depth forensics analysis of each asset's behavior augments this detailed inventory - offering unmatched insight into network connections, application usage, unencrypted protected health information transmissions, and threat detection.



[4] Ibid.

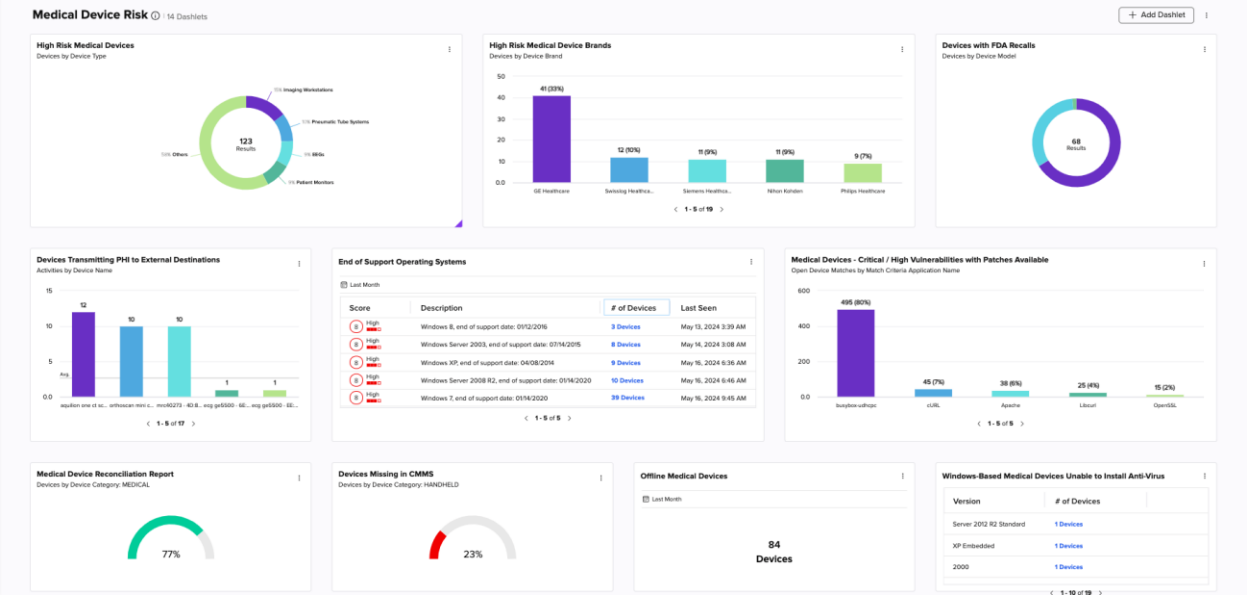
Armis Centrix™ for Actionable Threat Intelligence

In February 2024, Armis acquired Cyber Threat Cognitive Intelligence (CTCI). Using the CTCI technology, Armis launched a new product called Armis Centrix™ for Actionable Threat Intelligence (ATI) and positioned itself to develop the world's most advanced early warning cyber intelligence system. ATI delivers early warnings to detect active attacks, exploits, and at-risk assets. The company leverages Armis' Asset Intelligence Engine, incorporating CTCI's proprietary intelligence to utilize early warning indicators from the dark web, AI-based honeypots, and known adversaries. This AI-driven pre-attack threat-hunting technology enriches the platform with critical intelligence, boosting the effectiveness of security operations teams in preventing breaches, detecting attacks, and assessing organizational compromises.

Armis Centrix™ for Medical Device Security

Armis Centrix™ for Medical Device Security is engineered to protect healthcare institutions from the expanding array of connected devices, from specialized medical devices and clinical devices to everyday infrastructure, without disruption to patient care. It stands out by offering agentless profiling, deep packet inspection, and non-disruptive active discovery features. These tools enable it to deliver a detailed and contextual analysis of an organization's cybersecurity posture with minimal disruption to patient care.

The platform offers unmatched visibility and security across an expanding array of connected devices, from specialized medical equipment to everyday infrastructure. It provides real-time monitoring of asset behavior against global standards to ensure compliance and detailed insights into device utilization to aid clinical, cybersecurity, and IT teams in resource allocation and maintenance planning. Finally, Armis Centrix™ simplifies managing Food and Drug Administration recalls and security advisories by automatically linking new guidelines to specific devices.



"Armis is an integral part of Main Line Health's cybersecurity program, providing unparalleled visibility into every asset and device within our environment. As a hospital system dedicated to delivering safe, high-quality, equitable, and affordable care to treat and cure disease, Armis allows us to focus on what truly matters"

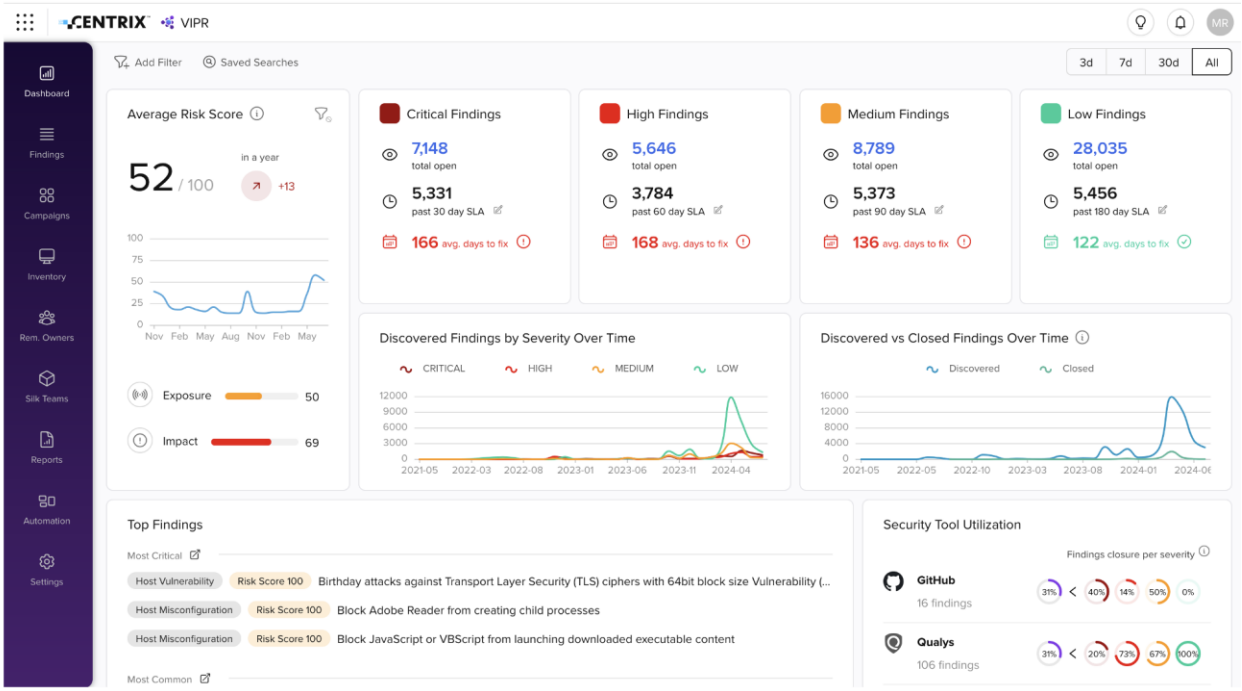
- Aaron Weismann, Chief Information Security Officer at Main Line Health[5]

Armis Centrix™ Vulnerability Prioritization and Remediation (VIPR)

Armis provides vulnerability prioritization and remediation in a revolutionary way, improving legacy vulnerability management systems. Traditional approaches focus on asset-based common vulnerabilities and exposures, overlooking security findings such as misconfigurations, end-of-life issues, and application defenselessness. Thus, VIPR fills this void by aggregating and contextualizing security data from diverse sources, including on-premises devices, cloud services, code, and application security tools. Leveraging AI to deduplicate and correlate this data, the platform reduces clutter and delivers a clear, actionable overview of an organization's security posture.

In April 2024, Armis acquired Silk Security. With the integration of Silk Security capabilities, VIPR Pro automates remediation processes and shortens the mean time to resolution, streamlining ticket management through bidirectional workflow capabilities. Armis Centrix™ now captures and analyzes a comprehensive array of data sources, from on-premises devices to cloud computing, code, and application security tools. It streamlines the entire remediation lifecycle, from identifying owners to operationalizing fixes, providing a unified platform for prioritization and efficient risk resolution management. This strategic enhancement empowers teams to stay ahead of evolving threats, mitigate high-risk findings, ensuring robust cybersecurity management across the organization.

[5] Provided by Armis (Armis, July 2024)



Artificial Intelligence Integration

As part of its outstanding growth strategy, Armis has integrated AI across various levels, significantly boosting its threat intelligence and detection capabilities. Armis Centrix ™allows the company to generate and update protocol analyzers, detect new protocols, and broaden real-time visibility, drastically reducing response times from days to seconds.

Additionally, AI has enhanced Armis's context and anomaly detection capabilities, enabling the analysis of petabytes of data to spot trends, assess risks, and provide actionable intelligence tailored to healthcare environments. By aligning this data with industry standards and advisories from major manufacturers like Siemens, GE, and Philips, Armis can offer precise, AI-driven recommendations.[6] These improvements enhance the efficiency and effectiveness of threat detection and response and render the data more accessible and useful for security and clinical engineering teams.

Fostering Innovation, Security, and Compliance

Compliance optimization is another aspect in which Armis excels, as the company seamlessly combines various compliance and security frameworks into Armis Centrix™. Armis Centrix™ adheres to stringent standards set by frameworks such as the Center of Internet Security Critical Security Controls and the NIST CyberSecurity Framework.[7] The platform offers in-depth device insights essential for compliance, reporting, and asset management, including confirming the appropriateness of network segments and identifying banned devices from manufacturers like Hikvision, Huawei, Dahua, or ZTE.[8]

[6] Frost & Sullivan Interview with Armis (Frost & Sullivan, June 2024)

[7] "Internal and External Compliance Reporting" (Armis website: https://www.armis.com/solutions/internal-and-external-compliance-reporting/)

[8] Ibid.

Armis Centrix™ platform supports essential compliance and security frameworks like the NIST 800-53 cybersecurity framework for baseline assessments and integrates technical mappings to security frameworks such as MITRE ATT&CK and HICP.[9] The company also aligns with US government regulatory guidelines, including Health and Human Services performance goals, ensuring comprehensive regulatory compliance. With over 200 ready-to-use integrations, the platform connects with existing healthcare infrastructures, including Active Directory, SCCM, security platforms, firewalls, network access control solutions, and clinical management systems.[10]

Regarding the innovation process, Frost & Sullivan appreciates how the company regularly interacts with partners to gather insights and monitor progress. Armis uses customer advisory boards, executive business reviews, discovery activities with customers, and design partners to stay informed of market shifts. Further insights from user groups and interviews, particularly involving the 5 billion devices under Armis's protection, inform the development of new initiatives.[11]

Leveraging extensive market knowledge, Armis employs an agile development methodology that fosters internal innovation and encourages broad team participation. The company invests heavily in thought leadership and musters a robust customer advisory board to align its product direction and long-term goals. Operating on two-week development sprints, Armis ensures swift responses to customer feedback and the rapid deployment of new features.[12] Once it develops a new technology or capability, the company prepares a comprehensive go-to-market package with supporting materials and new processes, securing a smooth transition from development to deployment.

Exceptional Customer Success Strategy Driving Sustainable Growth

Cementing its leadership in the space, Armis maintains strong executive alignment through a team of experts and senior security leaders who direct the company's security controls and frameworks strategy. This group collaborates closely with dedicated teams for each product line, including customer success, healthcare security programs, network research, and systems engineering. It emphasizes client engagement and support, resulting in a comprehensive offering that ranges from standard customer success management to 24/7 dedicated technical account management and on-site resident engineering.

The company delivers tailored support packages, including round-the-clock technical assistance, private training, and strategic advisory services, fostering a supportive environment that has helped build an impressive clientele of 1,106 global customers.[13] Additionally, Armis provides a wealth of resources like training programs, webinars, whitepapers, and thought leadership content to educate and empower its customers.

[9] Ibid.
[10] Provided by Armis (Frost & Sullivan, June 2024)
[11] Ibid.
[12] Frost & Sullivan Interview with Armis (Frost & Sullivan, June 2024)
[13] Provided by Armis (Frost & Sullivan, June 2024)

This commitment to customer impact extends through Armis's active engagement in the Product Advisory Council and various community initiatives such as the "Connect" events, where customers, partners, and industry professionals exchange best practices and insights. Ultimately, Armis Centrix™ exhibits a customer attrition rate of less than 2%.[14]

Some examples of Armis Centrix's impressive performance include one customer saving over $600,000 by optimizing its medical device maintenance contracts.[15] In another standout case, Armis uniquely detected ransomware activity in a client's environment, identifying 26 to 28 times the number of incidents that traditional security tools missed. While other solutions detected roughly 50 events, Armis discovered over 2,200, providing essential insights for board reports and tracking remediation efforts.[16]

> *"The company exceeded its 2023 North American targets in the healthcare sector by 200%, bolstered by a substantial contract with a leading healthcare and insurance provider and multiple multimillion-dollar deals with US Federal entities. This triumph underscores the effectiveness of a well-executed go-to-market strategy, reinforced by strong partnerships with leading firms such as Fortified Health Security, Cyber Salus, KPMG, and PwC."*
>
> ***- Dr. Rishi Pathak***
> ***Research Director***

Flexible and scalable subscription plans allow Armis customers to pay only for what they use and scale without vendor lock-in. Likewise, free trials and demos enable potential customers to explore Armis Centrix's capabilities. These strategies contributed to the company's acquisition of over 200 new large enterprise customers in 2023.[17] In 2024, approximately 25-30% of Armis's revenue derives from IoT, OT, and medical device security products.[18] Platform users also benefit from managing medical devices, building management systems, and IT infrastructure. The versatility of Armis has led to impressive adoption rates, with 55% of the company's customers purchasing three or more products, and 35% integrating the two newest offerings.[19]

Impressive Business Performance and Future Outlook

Armis's exceptional business performance impresses Frost & Sullivan. In February 2023, Armis reached a significant milestone by surpassing $100 million in annual recurring revenue, achieving this target faster than any other asset visibility and security vendor.[20] The company exceeded its 2023 North American targets in the healthcare sector by 200%, bolstered by a substantial contract with a leading healthcare and insurance provider and multiple multimillion-dollar deals with US Federal entities.[21] This triumph underscores the effectiveness of a well-executed go-to-market strategy, reinforced by strong partnerships with leading firms such as Fortified Health Security, Cyber Salus, KPMG, and PwC.[22]

---

[14] Ibid.
[15] Frost & Sullivan Interview with Armis (Frost & Sullivan, June 2024)
[16] Ibid.
[17] Ibid.
[18] Provided by Armis (Frost & Sullivan, June 2024)
[19] Ibid.
[20] "Armis Surpasses 100m USD ARR in Less Than 5 Years" (Armis press release, February 2023)
[21] Provided by Armis (Frost & Sullivan, June 2024)
[22] Ibid.

Armis has the potential to expand significantly, driven by its asset visibility and management capabilities across IT, OT, IoT, IoMT, and cloud infrastructures. The escalating frequency of large-scale healthcare cyberattacks underscores the necessity for Armis's solutions, driving increased market adoption. At the same time, the company is broadening its collaborations with Original Equipment Manufacturers, Medical Device Manufacturers, Healthcare Delivery Organizations, Managed Service Providers, and technical alliances. This strategy, coupled with a substantial investment in research and development accounting for approximately 70% of the company's budget, positions Armis for sustained growth.[23]

Finally, Armis continues its heavy R&D investments and evaluation of additional potential acquisitions as it continues to innovate and expand its product suites. The company plans to stay ahead of the global regulatory and compliance curve, deepening its integration with international bodies. This approach will enable Armis to deliver comprehensive security recommendations across the entire medical device lifecycle, from procurement to disposal. With a clear vision and a well-defined execution plan, the company will lead the cybersecurity market and achieve significant growth in the coming years.

Conclusion

In the healthcare sector, stakeholders must select top-tier technology-based solutions to maximize their market impact. Frost & Sullivan recognizes Armis Centrix™ for providing unmatched cybersecurity protection within this framework. This advanced platform ensures global visibility, security, and management of an extensive range of assets, effectively mitigating risks, remediating vulnerabilities, and thwarting threats. It excels in critical areas such as OT/IoT security, medical device security, and actionable threat intelligence, empowering organizations to neutralize threats before they disrupt operations.

Armis Centrix™ clearly stands out by shifting security operations from reactive to proactive. It features a comprehensive multidimensional asset inventory that categorizes devices by type, location, role, criticality, and ownership. Deep forensic analysis enhances this inventory and provides real-time insights into network connections, application usage, and threat detection. The platform's robust capacity to manage and monitor massive events and assets daily emphasizes its extensive coverage and real-time visibility across global deployments.

Frost & Sullivan analysts observe how Armis has achieved significant commercial success, drawing numerous new large enterprise customers over the past year and generating substantial revenue through its versatile platform. The company's relentless pursuit of innovation, strategic acquisitions, and expansion into new markets ensures its continued growth and leadership in the cybersecurity landscape.

With its strong overall performance, Armis earns the 2024 Frost & Sullivan Global Technology Innovation Leadership Award.

[23] Frost & Sullivan Interview with Armis (Frost & Sullivan, June 2024)

What You Need to Know about the Technology Innovation Leadership Recognition

Frost & Sullivan's Technology Innovation Leadership Award recognizes the company that has introduced the best underlying technology for achieving remarkable product and customer success while driving future business value.

Best Practices Award Analysis

For the Technology Innovation Leadership Award, Frost & Sullivan analysts independently evaluated the criteria listed below.

Technology Leverage

Commitment to Innovation: Continuous emerging technology adoption and creation enables new product development and enhances product performance

Commitment to Creativity: Company leverages technology advancements to push the limits of form and function in the pursuit of white space innovation

Stage Gate Efficiency: Technology adoption enhances the stage gate process for launching new products and solutions

Commercialization Success: Company displays a proven track record of taking new technologies to market with a high success rate

Application Diversity: Company develops and/or integrates technology that serves multiple applications and multiple environments

Business Impact

Financial Performance: Strong overall financial performance is achieved in terms of revenues, revenue growth, operating margin, and other key financial metrics

Customer Acquisition: Customer-facing processes support efficient and consistent new customer acquisition while enhancing customer retention

Operational Efficiency: Company staff performs assigned tasks productively, quickly, and to a high-quality standard

Growth Potential: Growth is fostered by a strong customer focus that strengthens the brand and reinforces customer loyalty

Human Capital: Commitment to quality and to customers characterize the company culture, which in turn enhances employee morale and retention

About Frost & Sullivan

Frost & Sullivan is the Growth Pipeline Company™. We power our clients to a future shaped by growth. Our Growth Pipeline as a Service™ provides the CEO and the CEO's growth team with a continuous and rigorous platform of growth opportunities, ensuring long-term success. To achieve positive outcomes, our team leverages over 60 years of experience, coaching organizations of all types and sizes across 6 continents with our proven best practices. To power your Growth Pipeline future, visit Frost & Sullivan at http://www.frost.com.

The Growth Pipeline Engine™

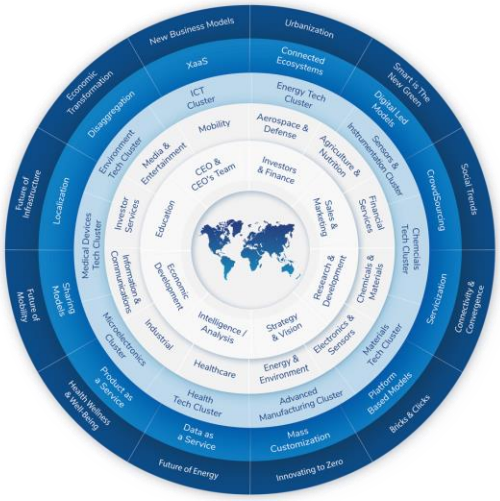
Frost & Sullivan's proprietary model to systematically create ongoing growth opportunities and strategies for our clients is fuelled by the Innovation Generator™.
Learn more.

Key Impacts:

- **Growth Pipeline:** *Continuous Flow of Growth Opportunities*
- **Growth Strategies:** *Proven Best Practices*
- **Innovation Culture:** *Optimized Customer Experience*
- **ROI & Margin:** *Implementation Excellence*
- **Transformational Growth:** *Industry Leadership*

The Innovation Generator™

Our 6 analytical perspectives are crucial in capturing the broadest range of innovative growth opportunities, most of which occur at the points of these perspectives.



Analytical Perspectives:

- Mega Trend (MT)
- Business Model (BM)
- Technology (TE)
- Industries (IN)
- Customer (CU)
- Geographies (GE)