ASIMILY

Comprehensive Intelligence Report

Next-Generation Cyber Asset and Exposure Management Platform

Complete Analysis of Products, Market Position, and Strategic Direction

Report Date: February 05, 2026

Classification: Confidential

EXECUTIVE SUMMARY

Asimily is a leading cybersecurity company specializing in IoT (Internet of Things), IoMT (Internet of Medical Things), and OT (Operational Technology) security. Founded in Silicon Valley, the company has rapidly established itself as a market leader through innovative technology, strong customer focus, and consistent recognition by industry analysts.

The company provides the only complete risk mitigation solution that goes beyond simple vulnerability scanning to deliver actionable intelligence, automated remediation, and comprehensive governance capabilities. Asimily customers typically eliminate more than 10,000 high-risk vulnerabilities within their first three months of deployment.

KEY ACHIEVEMENTS

Best in KLAS 2026 - Healthcare IoT Security Leader | Ranked #11 on Deloitte Technology Fast 500 (North America) | 50+ Industry Awards in the last 24 months | 98% NIST compliance achieved by customers (vs. 71% industry average)

COMPANY OVERVIEW

Corporate Profile

Asimily Inc. is headquartered in the United States with a mission to secure the connected devices that power critical infrastructure, healthcare, manufacturing, and government operations. The company was founded by cybersecurity veterans who recognized that traditional security tools were inadequate for the unique challenges posed by IoT, medical devices, and industrial control systems.

Unlike conventional security platforms that focus primarily on IT assets, Asimily has developed specialized capabilities for cyber-physical systems that cannot tolerate traditional security scanning methods. The platform uses passive, protocol-based, and API-driven discovery methods that maintain device stability while providing comprehensive visibility.

Market Position

Asimily operates in the rapidly growing Cyber Asset Attack Surface Management (CAASM) and IoT security markets. The company has carved out a leadership position in healthcare IoMT security, as evidenced by the Best in KLAS 2026 recognition. This healthcare expertise translates effectively to other regulated industries including manufacturing, life sciences, and government sectors.

PRODUCT PORTFOLIO

1. Inventory & Visibility

The foundation of the Asimily platform is comprehensive device discovery and inventory management. The system automatically identifies and catalogs all connected devices across IT, IoT, OT, and IoMT categories without disrupting operations. Key capabilities include:

- Passive network monitoring that observes traffic without generating probe traffic
- Protocol-based discovery using native device communications (SNMP, Modbus, DICOM, HL7)
- API integrations with existing network infrastructure and management tools
- Automated device classification with detailed hardware and software inventories
- Continuous monitoring to detect new devices and configuration changes

2. Vulnerability Prioritization

Asimily addresses the challenge of vulnerability overload by focusing security teams on the riskiest 2% of devices. The platform goes beyond CVE scores to calculate actual exploitability using the MITRE ATT&CK framework and proprietary Asimily Labs research:

- Risk scoring based on device context, network exposure, and exploit availability
- Automated correlation of vulnerabilities with device-specific compensating controls
- Risk Simulator tool for modeling ROI of remediation actions before deployment
- Prioritization queues that focus teams on highest-impact remediation activities

3. Risk Mitigation & Remediation

Unlike platforms that only identify risks, Asimily provides multiple active remediation capabilities that reduce exposure without requiring vendor patches or maintenance windows:

- Targeted Attack Prevention: 180+ attack vector mitigations without device changes
- Network Segmentation: Microsegmentation recommendations and policy enforcement
- IoT Patching: Safe firmware updates for supported devices with rollback capabilities
- Configuration Control: Baseline establishment, drift detection, and automated recovery
- Password Management: Secure credential rotation for IoT and embedded devices

4. Threat Detection & Response

The platform provides continuous monitoring for anomalous behavior and indicators of compromise specific to IoT/OT environments:

- Behavioral analytics establishing normal device communication patterns
- Anomaly detection with customizable rules and automated response actions
- Integrated packet capture for forensic investigation and incident response
- SIEM and SOAR integrations for enterprise security operations

5. Governance, Risk & Compliance

Asimily streamlines compliance with healthcare, industrial, and government security frameworks:

- Pre-configured reporting for NIST, HIPAA, FDA, ISO 27001, and SOC 2
- Device timeline tracking for audit trails and forensic analysis
- Configuration snapshots for disaster recovery and ransomware resilience
- Crowdsourced device hardening guidance from Asimily community

INDUSTRY SOLUTIONS

Healthcare (IoMT)

Asimily's healthcare solution addresses the unique challenges of medical device security, where patient safety cannot be compromised for security updates. The platform is deployed at leading healthcare systems including MemorialCare, Methodist Le Bonheur Healthcare, Tufts Medicine, and St. Lawrence Health. Key healthcare capabilities include:

- Integration with biomedical engineering workflows and CMMS systems
- Support for medical device protocols including DICOM and HL7
- FDA medical device guidance alignment and recall management
- Clinical context integration for risk prioritization
- Achieved 98% NIST compliance at MemorialCare (vs. 71% average for 60 similar HDOs)

Manufacturing (OT)

For manufacturing environments, Asimily secures industrial control systems and operational technology without disrupting production processes. The platform supports industrial protocols including Modbus, Ethernet/IP, and Profinet while maintaining the availability requirements critical to manufacturing operations.

Government & Public Sector

The February 2025 Carahsoft partnership expanded Asimily's reach into federal, state, and local government markets. The platform supports critical infrastructure protection requirements and integrates with government-specific security frameworks and procurement vehicles.

CUSTOMER SUCCESS

MemorialCare

MemorialCare, a leading healthcare system in Southern California, deployed Asimily to address the growing challenge of IoMT device visibility and vulnerability management. Under the leadership of Kevin Torres, VP of IT and CISO, the organization achieved remarkable results:

RESULT

Using the Asimily Risk Management Platform, MemorialCare gained full visibility into connected IoT and IoMT devices and their associated vulnerabilities. Our security program achieved 98% NIST compliance while the average of 60 similar HDOs is 71%.

Source: Kevin Torres, VP of IT/CISO, MemorialCare

Methodist Le Bonheur Healthcare

Paul Moore, Clinical Technology Services System Engineer, describes the operational impact:

RESULT

Asimily is our single pane of glass for connected devices. Instead of physically driving to six locations looking for devices not in use, Asimily provides full visibility enterprise-wide with accurate reporting.

Source: Paul Moore, Clinical Technology Services, Methodist Le Bonheur Healthcare

Tufts Medicine

Brian Cayer, Chief Information Security Officer at Tufts Medicine, emphasizes the partnership aspect:

RESULT

Asimily is not just a technology vendor. They are a true security partner. The team is quick to respond to inquiries and feature requests as we build out and mature our Cybersecurity program.

Source: Brian Cayer, CISO, Tufts Medicine

St. Lawrence Health

Richard Ingersoll, Director of Information Systems, quantifies the resource savings:

RESULT

Asimily gives us visibility and insights into our environment we didn't have before. It notifies us of issues and prioritizes vulnerabilities efficiently - time savings equivalent to at least one full-time employee.

Source: Richard Ingersoll, Director of IS, St. Lawrence Health

MARKET RECOGNITION

Awards & Accolades

Asimily has received significant industry recognition, validating both its technology leadership and market impact:

- Best in KLAS 2026 - Healthcare IoT Security: Named category leader in the annual KLAS Research report
- Deloitte Technology Fast 500 2024: Ranked #11 fastest growing cybersecurity company in North America
- 50+ Industry Awards: Recognition spanning healthcare, cybersecurity, and technology categories over 24 months
- Gartner Peer Insights: Positive customer reviews validating platform effectiveness

Strategic Partnerships

The February 2025 Carahsoft partnership represents a significant expansion of Asimily's market reach. Carahsoft, as a leading government IT solutions provider, enables Asimily to access federal, state, and local government markets through established procurement channels and a extensive reseller network.

This partnership aligns with growing government focus on critical infrastructure cybersecurity and follows successful deployments at healthcare and manufacturing organizations that serve as models for government sector implementations.

TECHNOLOGY ARCHITECTURE

Deployment Options

Asimily supports flexible deployment models to accommodate diverse customer environments:

- On-Premises: Full platform deployment within customer data centers
- Cloud: SaaS deployment with customer data isolation
- Hybrid: Mixed deployment with cloud management and on-premises collectors
- Air-Gapped: Secure deployment for isolated networks without internet connectivity

Integration Ecosystem

The platform integrates with existing security and IT infrastructure to maximize value and minimize operational disruption:

- SIEM Integration: Splunk, QRadar, Sentinel, and others for centralized logging
- SOAR Integration: Automated response workflows with major SOAR platforms
- CMDB Integration: ServiceNow and BMC for asset management synchronization
- Network Infrastructure: Direct integration with switches, firewalls, and wireless controllers
- Vulnerability Scanners: Tenable, Rapid7, and Qualys data correlation
- Ticketing Systems: ServiceNow, Jira, and Remedy for workflow integration

Compliance Frameworks

Asimily supports compliance with major security frameworks and regulations:

- NIST Cybersecurity Framework: Comprehensive coverage of Identify, Protect, Detect, Respond
- HIPAA: Healthcare-specific controls and reporting for protected health information
- FDA Guidance: Alignment with medical device cybersecurity guidance documents
- ISO 27001: Information security management system requirements
- SOC 2: Service organization control reporting
- GDPR: Data protection for European operations

COMPETITIVE LANDSCAPE

Market Differentiation

Asimily differentiates from competitors through several key capabilities:

- Complete Remediation: Unlike vulnerability-only tools, Asimily provides active risk reduction
- IoT-Specific Expertise: Deep knowledge of IoT, IoMT, and OT protocols vs. IT-focused competitors
- Safe Discovery: Passive and protocol-based methods that don't disrupt critical devices
- Prioritization: Focus on exploitable vulnerabilities rather than raw CVE counts
- Healthcare Leadership: Proven healthcare deployments with clinical workflow integration

Key Competitors

The IoT/OT security market includes several notable competitors:

- Claroty: Strong OT/ICS focus with industrial protocol expertise
- Armis: Agentless device visibility with broad IT/IoT coverage
- Forescout: Network access control with device visibility capabilities
- Nozomi Networks: OT-specific security with strong industrial focus
- Dragos: ICS/OT threat intelligence and incident response specialization

Asimily's differentiation lies in its combination of healthcare expertise, complete remediation capabilities, and focus on risk reduction rather than mere visibility.

STRATEGIC OUTLOOK

Growth Trajectory

Asimily is well-positioned for continued growth based on several market trends:

- Expanding IoT Attack Surface: Continued proliferation of connected devices increases addressable market
- Regulatory Pressure: Increasing compliance requirements drive demand for governance capabilities
- Healthcare Digitization: Medical device connectivity growth sustains core market demand
- OT Security Awareness: Growing recognition of industrial cybersecurity risks expands market
- Government Investment: Critical infrastructure protection initiatives create new opportunities

Product Roadmap Indicators

Recent product announcements and partnerships suggest continued innovation focus:

- Enhanced Risk Simulator capabilities for pre-deployment ROI modeling
- Expanded IoT patching support for additional device categories
- AI/ML advancement for improved vulnerability prediction and prioritization
- Government sector expansion through Carahsoft partnership
- Continued healthcare workflow integration and clinical context development

CONCLUSION

Asimily represents a compelling solution in the growing IoT/OT security market. The company's combination of deep technical expertise, proven healthcare deployments, and focus on actual risk reduction (rather than just visibility) positions it strongly against competitors.

The Best in KLAS 2026 recognition and Deloitte Fast 500 ranking validate both product quality and business momentum. The Carahsoft partnership opens significant new market opportunities in government and public sector segments.

For organizations struggling with IoT, IoMT, and OT security challenges, Asimily offers a mature platform with documented customer success and clear differentiation through its complete remediation capabilities and healthcare expertise.

This report was generated for informational purposes based on publicly available data.

All trademarks are property of their respective owners.