

ASIMILY

Competitive Analysis Report

Detailed Analysis of IoT/OT Security Market
Competitive Positioning and Differentiation Strategy

Report Date: February 05, 2026

Version: 1.0 | Classification: Confidential

MARKET OVERVIEW

IoT/OT Security Market Landscape

The Internet of Things (IoT), Internet of Medical Things (IoMT), and Operational Technology (OT) security market has experienced rapid growth driven by digital transformation initiatives, increasing cyber threats targeting connected devices, and regulatory pressure for improved critical infrastructure protection.

Market analysts estimate the IoT security market will reach \$20+ billion by 2027, with healthcare and industrial sectors representing the fastest-growing segments. The convergence of IT and OT networks, combined with the proliferation of connected medical devices, has created significant demand for specialized security solutions that understand the unique requirements of cyber-physical systems.

Key Market Drivers

- Ransomware attacks targeting critical infrastructure and healthcare increased 300% since 2020
- FDA and regulatory mandates requiring medical device cybersecurity (Section 524B)
- NIS2 Directive and critical infrastructure protection regulations in the EU
- Insurance requirements for cyber coverage in healthcare and manufacturing
- Shortage of cybersecurity professionals with OT/IoT expertise

Market Segments

The market can be segmented by deployment type, industry vertical, and solution capability:

- Healthcare IoMT: Medical devices, patient monitoring, imaging systems
- Industrial OT: Manufacturing, energy, utilities, critical infrastructure
- Enterprise IoT: Smart buildings, surveillance, environmental controls
- Smart City: Transportation, public safety, utilities management

COMPETITIVE LANDSCAPE

Primary Competitors

The IoT/OT security market includes several well-funded and established competitors, each with distinct positioning and capabilities. Understanding competitive strengths and weaknesses is critical for effective market positioning.

Claroty

Claroty is widely recognized as the market leader in OT/ICS security, with strong industrial protocol expertise and significant market share in manufacturing and critical infrastructure.

- Strengths: Deep OT protocol knowledge, strong industrial customer base, Medigate acquisition for healthcare
- Weaknesses: Limited remediation capabilities, primarily focused on visibility
- Market Position: Premium pricing, enterprise focus
- Recent Activity: \$635M Series E funding (2022), Rockwell Automation partnership

Armis

Armis provides agentless device visibility across IT and IoT environments, with strong traction in enterprise and healthcare markets.

- Strengths: Agentless architecture, broad device coverage, strong SaaS platform
- Weaknesses: Limited OT protocol support, less mature remediation capabilities
- Market Position: Growth-focused, mid-market to enterprise
- Recent Activity: \$200M Series D (2023), \$2B+ valuation

Nozomi Networks

Nozomi focuses specifically on OT and ICS environments with strong threat intelligence and industrial customer relationships.

- Strengths: OT-specific threat intelligence, industrial focus, European presence
- Weaknesses: Limited healthcare expertise, smaller scale than Claroty
- Market Position: OT specialist, competitive pricing
- Recent Activity: \$100M Series D (2023), acquired by HD Hyundai

Microsoft Defender for IoT

Microsoft's entry into the IoT security market leverages existing enterprise relationships and Azure cloud infrastructure.

- **Strengths:** Microsoft ecosystem integration, attractive pricing, cloud scale
- **Weaknesses:** Less mature OT capabilities, limited healthcare focus
- **Market Position:** Bundled with E5, SMB to mid-market focus
- **Recent Activity:** CyberX acquisition (2020), continuous Azure integration

COMPETITIVE POSITIONING

Asimily Differentiation Strategy

Asimily competes effectively through a differentiated value proposition that emphasizes complete risk mitigation rather than visibility-only approaches, with particular strength in healthcare and remediation capabilities.

Key Differentiators

- Complete Remediation: Unlike visibility-only tools, Asimily provides active risk reduction through patching, segmentation, and attack prevention
- Healthcare Leadership: Best in KLAS recognition validates healthcare market leadership and clinical workflow integration
- Safe Discovery: Passive and protocol-based methods avoid the network disruption risks of active scanning in critical environments
- Risk Prioritization: Focus on exploitable vulnerabilities rather than raw CVE counts reduces alert fatigue
- IoT Patching: Automated firmware updates for supported devices reduce exposure without vendor involvement

Competitive Matrix

Feature Comparison (Asimily vs. Key Competitors):

- Device Visibility: Asimily = Claroty = Armis (all provide comprehensive discovery)
- OT Protocol Support: Claroty > Asimily > Armis (Claroty has deepest OT expertise)
- Healthcare Focus: Asimily > Claroty > Armis (Asimily Best in KLAS)
- Active Remediation: Asimily > Claroty > Armis (Asimily patching advantage)
- Threat Intelligence: Claroty = Nozomi > Asimily (dedicated threat research teams)
- Pricing: Armis < Asimily < Claroty (Claroty premium positioning)

Win/Loss Analysis

Analysis of competitive engagements reveals patterns in customer decision-making:

- Asimily wins when: Healthcare environment, remediation prioritized, 90-day ROI required
- Claroty wins when: Heavy OT/ICS focus, existing Rockwell relationship, unlimited budget
- Armis wins when: Cloud-first strategy, agentless requirement, Microsoft ecosystem
- Nozomi wins when: European requirements, specific OT threat intelligence needs

MARKET OPPORTUNITIES

Addressable Market Expansion

Several market trends create opportunities for Asimily to expand its addressable market and competitive position.

- Government Sector: Carahsoft partnership opens federal, state, and local opportunities
- International Expansion: European NIS2 compliance requirements create demand
- Mid-Market: Product packaging for smaller healthcare systems and manufacturers
- Managed Services: MSSP partnerships for organizations lacking security expertise

Technology Trends

Emerging technology trends will shape competitive dynamics over the next 3-5 years:

- AI/ML Advancement: Automated threat detection and response becoming table stakes
- Zero Trust Architecture: Network segmentation alignment with zero trust initiatives
- 5G and Edge Computing: New attack surfaces requiring specialized protection
- Quantum Computing: Cryptographic agility for long-lived IoT devices

Strategic Recommendations

To strengthen competitive position, Asimily should consider the following strategic initiatives:

- Invest in OT protocol expansion to compete more effectively in manufacturing
- Develop threat intelligence offerings to match Claroty/Nozomi capabilities
- Expand international presence, particularly in Europe for NIS2 compliance
- Create mid-market product tier to compete with Armis on price-sensitive deals
- Strengthen Microsoft ecosystem integration to defend against Defender for IoT

SWOT ANALYSIS

Strengths

- Best in KLAS 2026 recognition validates healthcare market leadership
- Complete remediation capabilities differentiate from visibility-only competitors
- Strong customer reference base with quantified ROI metrics
- Rapid growth trajectory (#11 Deloitte Fast 500) demonstrates market traction
- Safe discovery methods suitable for critical healthcare and OT environments
- Proven 10,000+ vulnerability remediation in first 90 days

Weaknesses

- Smaller brand recognition compared to Claroty in OT/industrial markets
- Less mature threat intelligence capabilities vs. dedicated research teams
- Limited international presence compared to global competitors
- Mid-market pricing may limit addressable market vs. lower-cost alternatives

Opportunities

- Government sector expansion through Carahsoft partnership
- European market growth driven by NIS2 compliance requirements
- Ransomware defense demand creating urgency for IoT/OT security
- Insurance market requirements driving security investment
- Channel partner expansion to increase market reach

Threats

- Microsoft Defender for IoT bundled pricing pressure
- Consolidation among competitors creating stronger integrated offerings
- Economic downturn reducing security budgets
- Shortage of qualified sales and technical talent limiting growth
- Increasing sophistication of IoT/OT threats requiring continued R&D investment

CONCLUSION

Asimily occupies a strong competitive position in the IoT/OT security market, with particular strength in healthcare and remediation capabilities that differentiate from visibility-focused competitors. The Best in KLAS 2026 recognition and rapid growth trajectory validate the company's market approach and technology differentiation.

The competitive landscape will continue to evolve with increasing consolidation, technology advancement, and market expansion. Asimily's focus on active risk reduction, healthcare expertise, and proven customer outcomes positions the company well for continued growth despite competitive pressure from well-funded rivals.

Success in the coming years will require continued investment in OT protocol support, threat intelligence capabilities, international expansion, and mid-market product offerings to address the full spectrum of competitive threats and market opportunities.

This analysis is based on publicly available information and market research.

Competitive intelligence should be updated quarterly for accuracy.