Asimily

Leading IoT, OT, and IoMT cybersecurity and risk mitigation platform, providing complete visibility, vulnerability prioritization, and automated threat response for connected devices.

https://asimily.com/

Overview

Asimily is an industry-leading, all-in-one Risk Mitigation Platform designed to secure the complex and growing networks of connected devices, including IoT (Internet of Things), OT (Operational Technology), and IoMT (Internet of Medical Things). The platform is purpose-built to address the unique security challenges of devices in healthcare, manufacturing, and public sector environments.

Key Benefits and Capabilities

1. Inventory and Visibility: Asimily provides automated, accurate discovery and inventory of all connected devices (medical, lab, IoT, OT, and IT) using passive monitoring, deep packet inspection (DPI), machine learning, and protocol-based/API-based techniques. This provides a comprehensive, continuously updated view of all assets, their configurations, and their behavior.

2. Vulnerability Prioritization: The platform uses patented AI/ML and a detailed, MITRE ATT&CK-based analysis to move beyond basic vulnerability categorization. It identifies the top 2% of riskiest devices with the highest likelihood and impact on clinical safety, business operations, and data security, allowing security teams to focus their limited resources efficiently.

3. Threat Detection and Response: Asimily offers real-time network anomaly detection, policy management, and automated threat response. Capabilities include targeted attack prevention, micro-segmentation guidance, and automated packet capture for forensic analysis to support root cause analysis and incident response.

4. Governance, Risk, and Compliance (GRC): The platform helps organizations maintain compliance with major industry regulations. It provides detailed reporting, record-keeping, device timelines, and configuration control (snapshots of hardened states) to support standards like HIPAA, SOC 2, ISO 27001, and FDA medical device security requirements. It also offers risk modeling to prevent risk before purchasing new devices.

Target Users and Use Cases

Asimily is best suited for **hospitals and healthcare organizations** (HDOs) managing large fleets of IoMT devices, as well as **enterprises** and **government entities** with diverse IoT and OT environments. Primary use cases include IoMT security, vulnerability management, risk-based security compliance, and third-party vendor management.

Key Features

- IoT/IoMT Device Discovery and Inventory (Passive, DPI, ML-based)
- Vulnerability Prioritization (AI/ML, Context-aware, Risk-based)
- Threat Detection and Network Anomaly Management
- Risk Mitigation (Segmentation/Micro-segmentation, Targeted Attack Prevention)
- IoT Patching and Password Management
- Governance, Risk, and Compliance (GRC) Reporting
- Forensics and Incident Response (Automated Packet Capture)

Pricing

Model: enterprise

Customized, enterprise-level pricing based on the organization's cybersecurity needs and connected device fleet size. Pricing information is not publicly disclosed. Contact the vendor for a tailored quote.

Target Company Size: medium, enterprise

Integrations

ServiceNow, Splunk Enterprise, Cisco, Palo Alto Networks, Check Point, IBM Security QRadar, Tenable Vulnerability Management, CMMS, CMDB, NAC

Compliance & Certifications

HIPAA, SOC 2, GDPR, ISO 27001, FDA Medical Device Security Standards, NIST

This document was generated by IntuitionLabs.ai with the assistance of AI. While we strive for accuracy, please verify critical information independently.