DATA SHEET

Comprehensive Cyber Security Managment Platform for IoT and Medical Devices

Who?

Healthcare and Lifesciences
Asimily Insight is built to meet the complex risk management needs of HDOs and life science companies.

When?

Real-time
Alert when devices will likely have a problem, show anomalous behavior, protect and respond in real-time.

Why?

Reduce Operational Inefficiencies & Device Downtime
Asimily Insight provides continuous, data-driven results with clear actionable recommendations to discover and protect assets and respond to vulnerabilities and anomalies across devices, departments, and vendors.

Provider-Specific Solutions
Every healthcare provider is different, with unique data needs and tools. Asimily Insight leverages healthcare -specific data sources to provide dynamic insights to each unique provider and stakeholder.

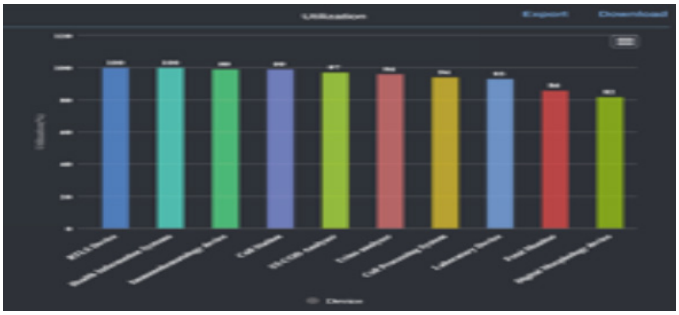
Traditional Security Approaches Do Not Work for IoMT
Patches are often not available or able to be applied, and traditional scanning tools can cause IoMT devices to malfunction and often cannot properly identify them. Network segmentation is not always realistic due to the heterogeneity, complexity, and number of devices.

What?

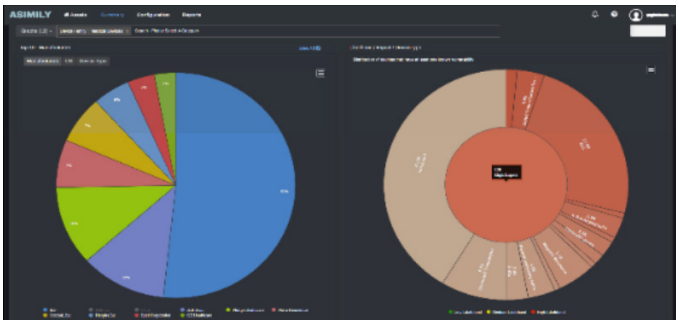
Predict
Know which connected devices are most critical, have the highest risk, and are most likely to cause a problem.

Where?

Anywhere
Easy-to-deploy, secure browser-based web application permits broad access with role-based access controls, virtually accessible from anywhere.



Single Pane of Glass
Asimily Insight solves for a variety of use cases across asset inventory, cybersecurity, and operational dimensions to provide comprehensive understanding of an organization's connected devices with unique views for each stakeholder in the organization.



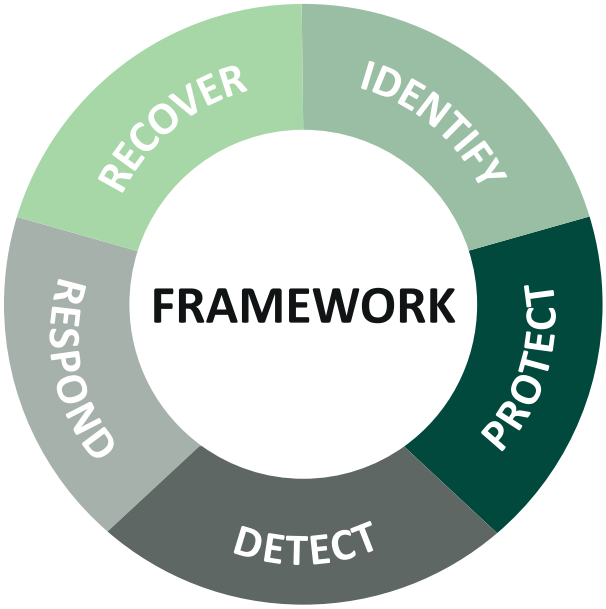
Passive Technology
Asimily Insight doesn't require HDOs to install any software agents, ideal for medical devices where this is often not possible.

Asimily + NIST Cybersecurity Framework

Asimily Insight adopts the National Institute of Standards and Technology's Cybersecurity Framework (CSF).

The Framework is voluntary guidance, based on existing standards, guidelines, and practices for organizations to better manage and reduce cybersecurity risk. In addition to helping organizations manage and reduce risks, it was designed to foster risk and cybersecurity management communications among both internal and external organizational stakeholders.

[Ref: https://www.nist.gov/cyberframework/newframework]



Asimily Insight enables you to ...

IDENTIFY — Identify device parameters, applications, and network parameters. Perform deep packet inspection of customer's data, and understand asset utilization and usage.

PROTECT — Protect the resources by applying network controls and organizational policies to block, segment, and isolate suspect devices.

DETECT — Detect vulnerabilities and anomalies (against the baseline). Prioritize high likelihood, high impact devices for vulnerability management and provide workarounds to mitigate the risks.

RESPOND — Respond to specific threats and take actions based on findings. Perform forensic analysis to investigate the root cause of identified problems; assess data flows, protocols used, and data Tx/Rx. Capture network traffic from devices behaving abnormally and save it for offline analysis.

RECOVER — Recover through plans created via device profiling: unique device characteristics are captured and defined; utilizing data analytics to profile unique behaviors, configurations, and controls.

Support and Success

- 24/7 support for critical items
- Customer success managers to enable organization's IoMT management plan
- North American based support
- Cloud and on-prem deployment options available

Contact Info

Want to watch a demo?
Contact us now...
info@asimily.com
440 N Wolfe Road
Sunnyvale, CA 94085

asimily