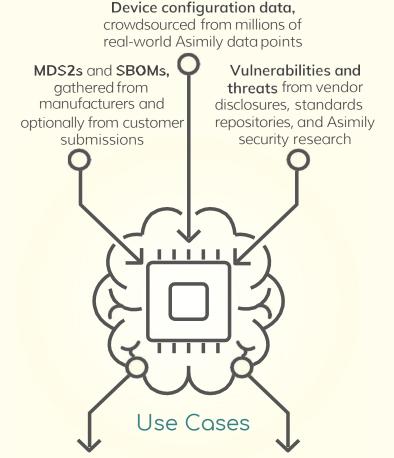# Asimily ProActive

A proactive approach to medical device security

Evaluating cybersecurity concerns during the procurement process for IoMT devices can sometimes feel like putting together a puzzle with half the pieces missing.

Asimily ProActive gives you the missing pieces back. Using ProActive, you can accurately model the risk of any device model, whether you already own it or not. Asimily draws upon real-world data from hundreds of thousands of medical devices deployed in the customer base.

With ProActive, you can view a comprehensive report about the device in question, its capabilities, connections, and possible configurations, including the highest and lowest risk configurations that have been seen in the wild. What's more, you can test out a configuration change by simulating it in the platform and seeing how it impacts overall risk.

Unsecured medical devices can result in patient or clinician safety events, data breaches, and even render the medical devices unavailable, all of which are devastating and can negatively impact the ability to deliver patient care. Rather than reactively fixing problems after they've been created, try out ProActive and discover a proactive approach to solving the medical device security puzzle.

Device configuration data, crowdsourced from millions of real-world Asimily data points

MDS2s and **SBOMs,** gathered from manufacturers and optionally from customer submissions

Vulnerabilities and threats from vendor disclosures, standards repositories, and Asimily security research

Use Cases

Pre-Procurement Risk Assessments

- Model the risk of any device model and version with the largest repository of device capability information
- Evaluates vulnerabilities by likelihood of exploitation using real-world configurations
- Quantifies risk on a 1-10 scale based on the CVSS standard
- Compare similar models to identify which would be most secure

Device Hardening & Configuration Guidance

- Create guides for any device, including standalone devices that have not yet been connected
- Discover which configuration changes would have the highest impact to cybersecurity risk
- See the highest and lowest risk configurations observed in the patient care environment
- Model planned configuration changes for a customized risk assessment