asimily

# Visibility, Inventory and Classification

The best cybersecurity attacks are like sucker punches – you don't see it coming and its happening too fast for you to do anything about it.

An accurate IoT inventory isn't a destination, it's a process. That process has to be fast, automated and comprehensive to bring you success. That success arrives when there are no doubts that you know what IoT exists, what it is doing, and have enough data about each device to protect it throughout its lifecycle. That's hard – here's why:

## Why traditional Inventory taking methods fail for IoT / IoMT

If taking a device inventory were easy for most organizations, there would not be so much innovation solving the following problems for IoT:

### 1. Devices are proliferating faster than older methods can handle

There are millions of IoT devices being added to networks around the world every year. Because users demand it, they are often added to the easiest accessible network, which may not be the place that they should be added.

As a result, savvy security teams plan for the worst. They assume that configurations drift, devices just appear, and the responsibility for secure operation stays exactly where it is – with them.

### 2. Multiple data sources conflict

The typical security team will have a software stack consisting of dozens of products. Many of these will have the responsibility to keep an inventory of what is in their scope. However, they see different IoT with different levels of confidence.

What's needed is a way for all of these information sources to be consolidated and augmented to get a picture of the devices that need to be securely managed.

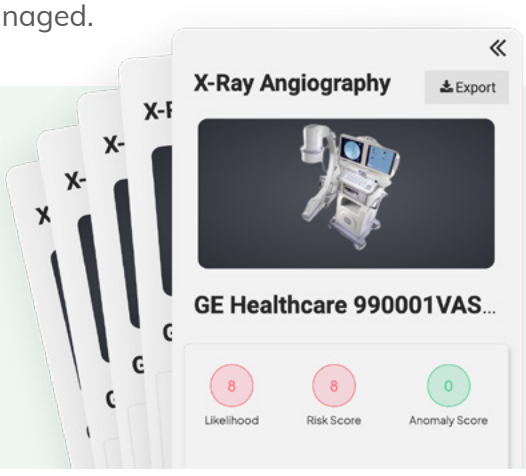
### 3. Devices are hard to identify safely

In the IoT device market, manufacturers juggle functionality, security, and profit. They're typically built to do a few things well, and have adequate security since it's a rare, savvy buyer that can distinguish on that basis.

A passive method to understand device behavior, minimizing active scans, is essential.

### Know It All – End the Era of "Unmanaged" IoT Devices

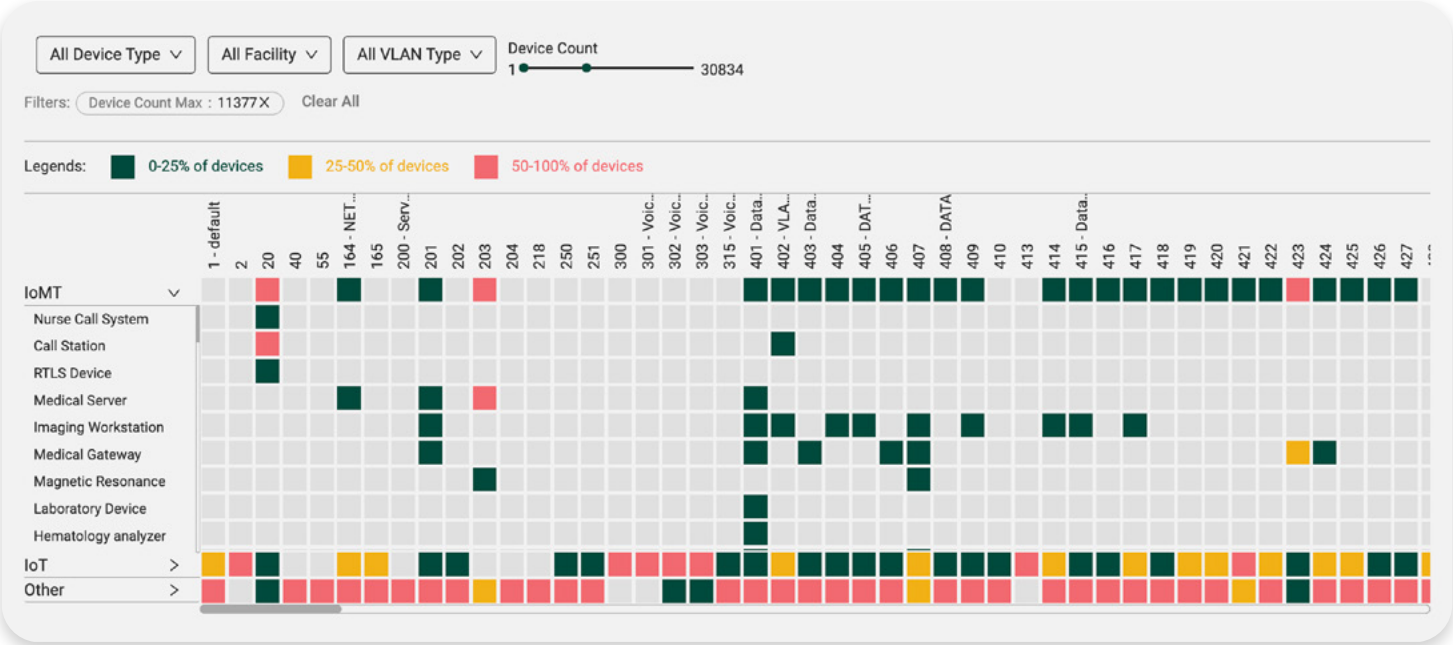
If it is creating network traffic, it's a risk, a target, and a compliance and management liability.



## Be Ready for Anything – By Knowing Every Active Device

The easiest target is one that can't be defended because nobody else knows about it.

With a constantly updated and accurate inventory of IOT devices alongside your regular IT assets, you can be ready for everything. That can include a security incident, which may be trying to find its way through your organization, an audit, or a new regulation that's facing your industry.




With Asimily, inventory and visibility of IoT devices becomes the starting point for real risk reduction

- Asimily identifies devices safely based on their network traffic. With the industry's best protocol analyzer, deep packet inspection (DPI), and AI/ML-based traffic analysis, Asimily finds and classifies each device into a family, along with all apps, services, and connections.
- Devices are displayed rapidly based on any network traffic or other record, avoiding shadow IT issues.
- To get the best possible inventory, Asimily augments its own passively gathered information across a variety of integrations including CMDB, CMMS, Vulnerability Scanners, and NACs to get to a simple, accurate inventory of devices and importantly – their topologic risk.

# Asimily Can Help

Securing the Internet of Things is far more complex than securing traditional IT equipment. Poor security practices at IoT device manufacturers paired with minimal visibility by IT and security teams make connected equipment a major security risk. The distributed and broadly installed nature of these devices means that a risk-based approach is required. This can be done, and thankfully Asimily can help companies implement and manage a risk-focused method of securing IoT devices for a more secure future.


## Asimily's IoT Risk Management Platform

- Creates a complete IoT inventory, collecting 100+ attributes for each device;
- Identifies and prioritizes the riskiest vulnerabilities;
- Recommends simple, validated mitigation actions;
- Conducts a full flow analysis for each device, recording all communication patterns across the network;
- Calculates risk for every connected device based on device attributes, dataflows, vulnerabilities, anomalies, configuration, and overall criticality of the device on operations;
- Generates ACLs for targeted segmentation for use by a NAC;
- Flags anomalous device behavior based on profiling data from millions of IoT devices;
- Makes it easy to set policies to monitor accepted risks and identify suspicious activity proactively;
- Automates packet capture for forensic analysis of any IoT device to support root cause analysis;
- Documents when the device is being used so users can understand utilization and operational efficiency;
- Allows device configuration snapshots to be taken, to thwart ransomware and simply recovery; and
- Risk simulator helps determine the benefit of work before it is performed, increasing team efficiency.

Asimily can help enterprise organizations drastically reduce cyber risk while minimizing resource and time costs.

To see how Asimily can help your organization, **arrange a demo today.**

## About Asimily

Asimily is an industry-leading risk management platform that secures IoT devices for medical, diagnostic, life sciences, pharmaceutical, and enterprise companies.

## Connect With Us

info@asimily.com
440 N Wolfe Road
Sunnyvale, CA 94085
(833) 274-6459
(833) ASI-MILY