asimily

Vulnerability Mitigation

Because of the volume of vulnerabilities found in modern software, the next CISO who gets their organization's open vulnerability queue to zero will also be the first. That's only a slight exaggeration.

Each year, 25,000-30,000 more vulnerabilities are discovered. That's about one every 20 minutes. So practical security leaders seek a better approach to protect their IT and connected devices (IoT and OT).

Why traditional Vulnerability Management fails for IoT and OT

There are several reasons why the standard vulnerability management approach is a poor fit for the unique challenges of IoT and OT:

1. Vulnerabilities need to be Prioritized, but not by Severity

Vulnerabilities are theoretical, until evaluated in context of each IoT/ OT device's value. That work, with the vulnerability as *one* input, results in showing how much risk the vulnerability has created. Another is how likely the vulnerability is to be in an attack. Likelihood increases if there are known, weaponized attacks.

Asimily customers are more efficient, with prioritized lists of risky devices, to see what to work on first.

2. Attack Prevention Matters, not Vulnerability Prevention

Vulnerabilities appear in too high a number for most organizations to realistically handle them all. Smart organizations work on figuring out which are the basis for a real-world attack and then prioritize those.

Asimily customers get time back by working on fewer problems to reduce the same risk. This results in having only 2% of the devices to fix, using 10% of the time, based on our analysis of our customers.

3. Get Better, Efficient Fixes

What's the vulnerability and its attack? Vector have been identified, there's still needs to be a fix. These can take time.

Asimily customers receive simple fixes to remove risk, not big projects each time such as network reconfiguration. Asimily gives your team the simplest fix for each vulnerability you encounter.

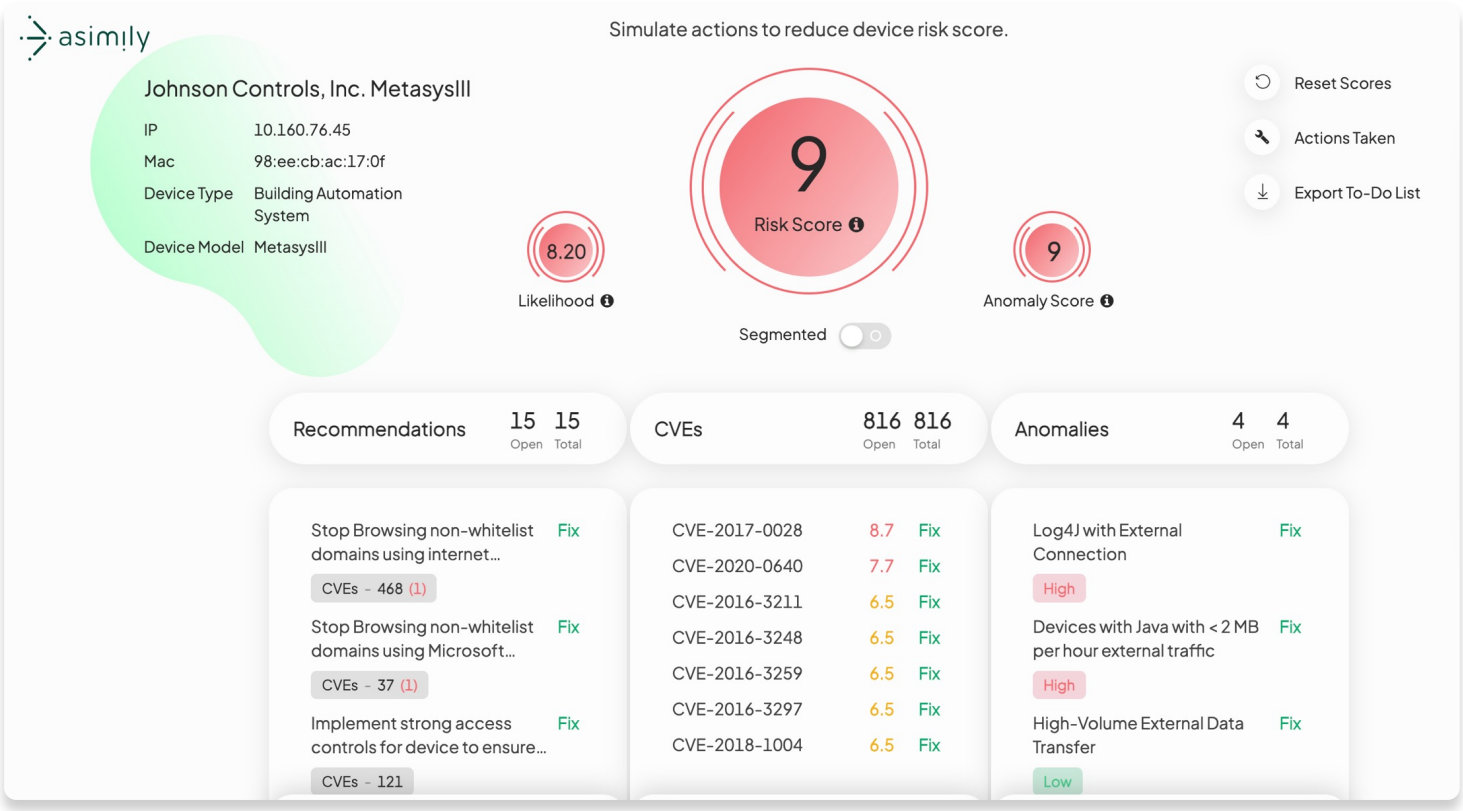
Making Vulnerability Mitigation Manageable – Less Work, Same Risk Reduction

Asimily makes IoT and OT vulnerability handling easier, by offering a ranked order of the riskiest devices with exploitable vulnerabilities, and simple, manageable fixes for each one.

Build Risk Reduction Program

Communicating internally, and being as organized as adversaries, are important for good defense.

On the highest level, get a clear Risk Score from 0-100, allowing you to assess your security against peers and track progress over time. Asimily also provides numerous reports that demonstrate vulnerability mitigation success for every audience are also available in the platform.



With Asimily, vulnerability mitigation programs reduce real risk from IoT/ OT in organizations. The differences are:

- Vulnerabilities are enhanced with information to make intelligent plans. That includes risk level, effort to fix, and risk reduced for each potential fix.
- Theoretical vulnerabilities, which don't affect an IoT or OT device in its current configuration and environment, don't create needless work for busy security teams
- Risk Simulator lets you see your mitigation options for each device, and pick the best one
- Everything is ranked and prioritized
- Results are sharable, reportable, and summarized graphically to advance IoT and OT security program maturity

Asimily Can Help

Securing the Internet of Things is far more complex than securing traditional IT equipment. Poor security practices at IoT and OT 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 Asimily can help companies implement and manage a risk- focused method of securing IoT and OT devices for a more secure future.

Asimily's IoT / OT Risk Management Platform

- Creates a complete IoT and OT 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 and OT 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 or OT 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 provides the only complete IoT and OT Risk Mitigation platform. It has the depth and breadth of capability to keep all devices secure, including visibility, vulnerability prioritization, risk mitigation, threat response, and Governance, Risk and Compliance. Asimily keeps devices safe and operational, driving revenue and cutting capital expenditures.

Connect With Us

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