asimily

CONFIGURATION CONTROL

Protect your device from Risk Flare-Ups

Detect Configuration Drift and Restore Safe States Faster

IoMT, IoT and OT Cyber-Physical Systems (CPS) are notoriously difficult and expensive to keep configured properly compared to standard IT. Configuration drift happens when software, people and manufacturers legitimately access devices. Each touch – whether made locally or remotely over the network - can accidentally change or reset settings. These Configuration Drifts are a core cyber-security problem.

Asimily fights this drift problem with complete IoMT/IoT/OT configuration snapshots for any device, enabling monitoring, reversion to known good states, audit readiness and enhanced threat detection. Here’s how.

Enhanced Inventory with Known Good State Snapshots for Devices

- **Create Rules for when a Snapshot is taken:** Use different settings (e.g. Low Risk) for devices so that a snapshot is taken only when those conditions are met.
- **Save a Known Good State for each Device**: Easily preserve a good configuration for recovery, audit, and compliance purposes.
- **See Settings for Any Device**: See the Settings grouped by different areas which includes information gathered from the entire network to make it easier to see most important aspects of a device
- **Efficiently Protect Device Fleets**: Protect all your IoT/ IoMT configurations from one place.

Detect Drift and Return to Safe Device States Faster

- **Set Alerts**: Let configuration variances trigger alerts, to help see exactly when and how a configuration changed.
- **Avoid Alert Fatigue**: Configurations are classified into four categories, which can be set to High, Medium, Low or None to trigger or suppress alerts.
- **Highlight Differences**: Any device can be compared to its known good state with changes clearly highlighted.
- **Roll back using Timelines**: Check how configurations have changed over time to understand how a deviation occurred, based on correlation with external events.

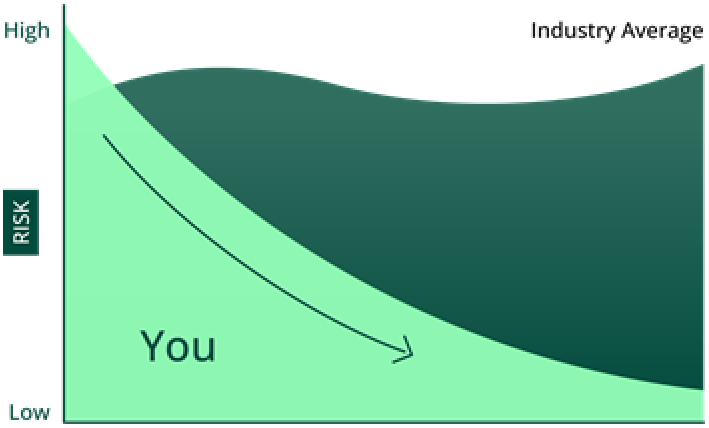
Asimily’s IoT Risk Management

- Creates a complete IoT/OT inventory, collecting 100+ attributes for each device
- Identifies and prioritizes the riskiest vulnerabilities
- Recommends simple, validated mitigation actions based on MITRE ATT&CK Framework
- 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, segmentation or micro-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
- Fights configuration drift by taking snapshots of known good states to aid restoration and detect deviations with comparison to good state
- Risk Simulator helps determine the benefit of work before it is performed, increasing team efficiency.
- Track utilization of all devices for procurement and planning
- Centralized information makes IT/OT convergence easier, while finding “unmanaged” devices

MemorialCare

Customer MemorialCare scored 98% on compliance with NIST best practices, 27% better than the industry average.

Device Risk Score



Inc. 5000	**170th** fastest growing company	**3rd** fastest growing in cybersecurity
500 Technology Fast 500	**187th** Deloitte Fast 500 growth company	**13th** fastest growing in cybersecurity

Connect With Us

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