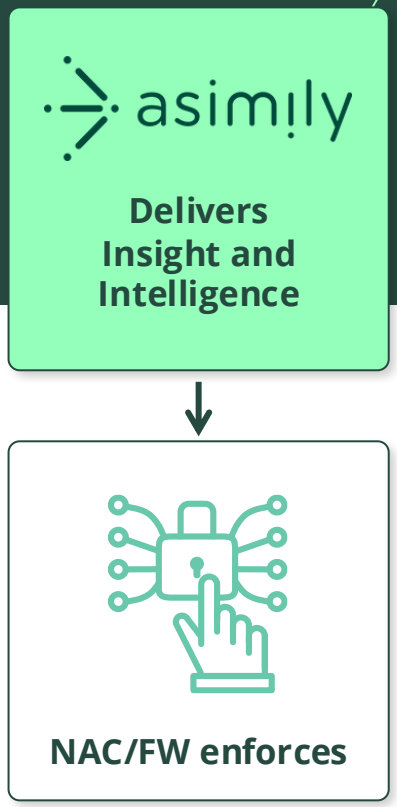
Unlock the Full Potential of Segmentation

With Asimily's Integration



Leverage Asimily's deep integration with Network Access Control (NAC) or Firewall (FW) tools for safe, incremental microsegmentation and targeted segmentation. Operationalize NAC faster with Asimily.

NAC/FW customers are ready for the next step. But implementation challenges prevent most organizations from realizing these benefits. Asimily changes that.

Asimily + NAC/FW: Better Together

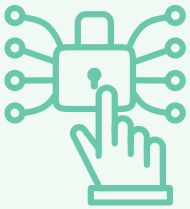
WITHOUT ASIMILY	WITH ASIMILY	
• "We'd rather allow too much than too little" • Broad, generic ACL policies or permissions • Segmentation not well done • High coordination effort with the customer	• ACL policies implemented correctly and with confidence • Communication policies based on observed traffic • Protocols can be selectively allowed or blocked • Segmentation and Microsegmentation becomes predictable and explainable	Asimily helps NAC/FW customers finally implement ACLs correctly, resulting in a direct correlation between safe, incremental segmentation and measurable risk reduction.

Asimily's Value to NAC/FW Users:

- Faster Segmentation projects
- Lower risk during design and implementation
- Less rework after go-live
- Stronger, fact-based arguments informing critical decisions for security teams and business units
- Clear differentiation through added value without deviating from network design

Why Organizations Struggle to Successfully Implement Network Segmentation

Network Access Control requires correct policies – but they do not generate them. Asimily helps by prescribing policies with concrete outcomes, such as ACL scope, enforcement, protocol directionality, east-west vs north-south traffic, and more.



NAC/FW CAN

- Manage identities
- Enforce ACLs
- Enforce policies

CAPABILITIES NEEDED FOR SUCCESSFUL IMPLEMENTATION

- Ability to understand devices such as IoT and OT
- Device prioritization to determine risk mitigation activities
- Device grouping based on function
- Visibility into real communication relationships between devices
- Ability to define minimal, relevant, secure policies

asimily

ASIMILY PROVIDES

Asimily helps NAC/FW customers clearly connect the dots between risk and how strictly a device should be segmented by leveraging policies correctly.

Typical Roadblocks to Operationalizing Network Segmentation

- Organizations struggle to classify devices accurately (especially IoT, OT, MedTech), which limits their ability to prioritize vulnerabilities
- Teams can't determine which policies to apply
- Network administrators don't know how to assign ACLs correctly
- Organizations base communication policies on assumptions rather than data
- Teams fear operational disruption from overly restrictive rules
- Organizations can’t measure whether segmentation is achieving its objectives

Organizations postpone microsegmentation projects and fail to implement even basic segmentation correctly.

Typical Use Cases

Inventory

Asimily can feed device context into NAC/FW

Prioritization

Prioritized devices provide direction on where ACLs or policies should be applied

Block Attack Vectors

Targeted segmentation provides specific policies to minimize attack vectors

Segmentation/ Microsegmentation

Get guided segmentation & microsegmentation policies for prioritized devices based on behavior

Accurate Status

Get the current status of ACLs to understand where you stand

Is Your Customer Segmentation Ready?

Start a discussion about segmentation readiness:

Where are the facts missing today for segmentation and microsegmentation?

Which device types are blocking applied policies?

How can policies be prepared with minimal risk?

About Asimily

Asimily is the next-generation cyber asset and exposure management platform for IT, IoT, OT, and IoMT environments. The platform provides organizations with comprehensive visibility, vulnerability prioritization, risk mitigation, threat detection and response, and Governance, Risk, and Compliance capabilities across their entire cyber asset attack surface. By proactively managing exposure and reducing risk rather than just reporting on it, Asimily enables organizations to keep devices secure and operational, driving business continuity and optimizing capital expenditures. Headquartered in Sunnyvale, California, Asimily is trusted globally by leading organizations across industries, including healthcare, manufacturing, and financial services.

www.asimily.com