DATA SHEET

Asimily + Cisco Integrated Segmentation Solution

INTRODUCTION

Asimily is the Proactive Cyber Asset Defense Platform for IoT, OT, IoMT, and IT environments across every critical infrastructure vertical. Together, Asimily and Cisco provide a comprehensive solution that turns device intelligence into enforced network policy – continuously and without operational disruption.

Asimily discovers and profiles every connected device, feeds rich context to Cisco ISE and uses Segmentation Orchestration to generate, simulate, and push DACLs, Security Groups, and SGACLs across Cisco ISE and Catalyst Center.

CHALLENGE

Organizations across healthcare, manufacturing, energy, utilities, and government operate heterogeneous fleets of IoT, OT, IoMT, and IT devices. As connectivity expands, so does the attack surface. Most security tools cannot see, classify, or act on these devices at scale.

Asimily closes that gap. Its discovery engine profiles every device and applies ATT&CK Analysis to determine which vulnerabilities are actually exploitable in the specific network environment, reducing millions of theoretical CVEs to the handful that carry genuine risk. Segmentation Orchestration then generates conflict-free policies from observed device behavior, simulates their impact before deployment, and enforces them across Cisco ISE, Catalyst Center, and firewall infrastructure.

CAPABILITIES

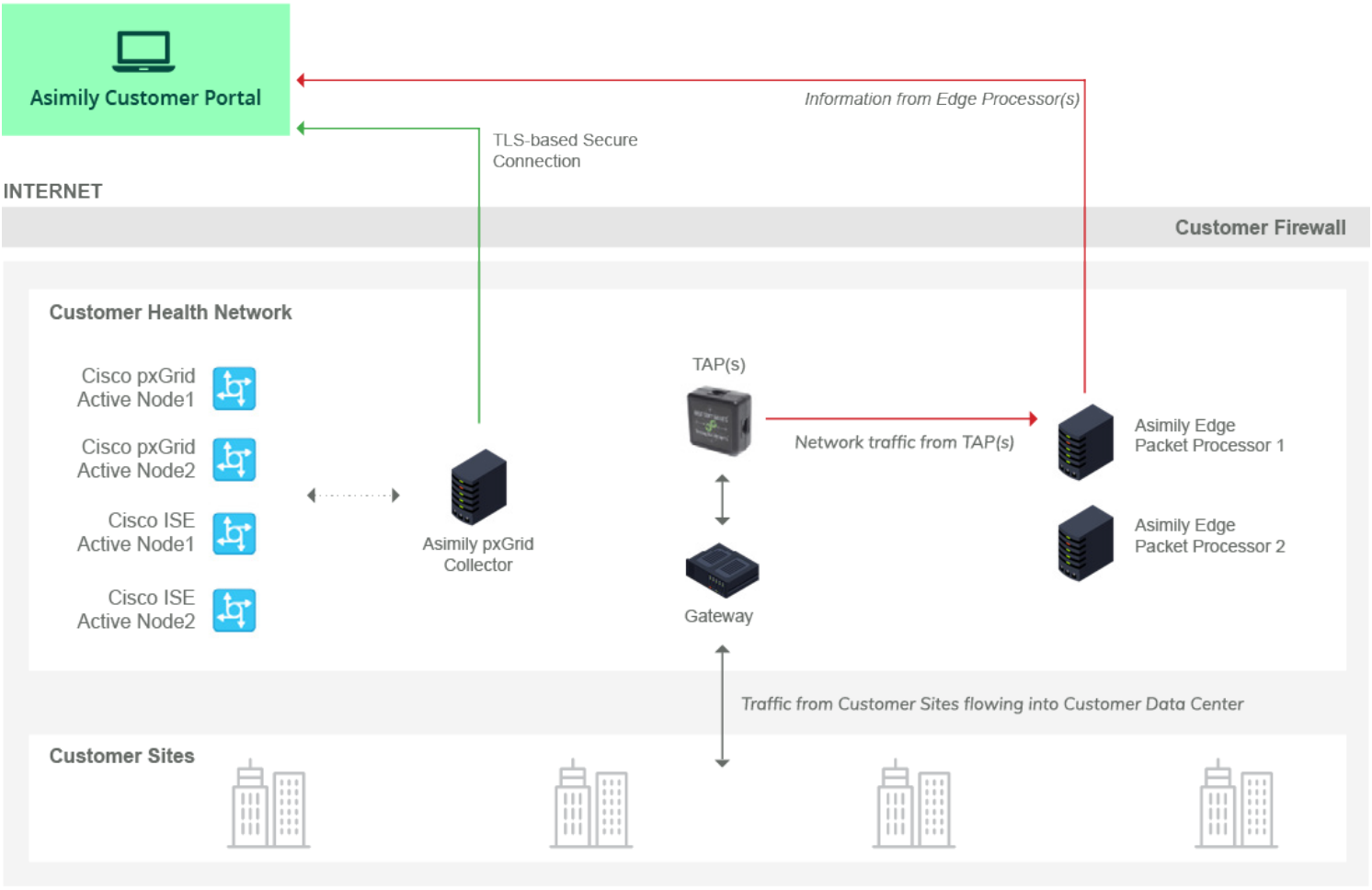
USE CASE	FUNCTIONALITY	BENEFITS
Device Visibility and Profiling	Asimily discovers and profiles every IoT, OT, IoMT, and IT device, capturing manufacturer, type, model, OS, firmware, serial number, and full communication behavior. Device context is fed to Cisco ISE via pxGrid.	Granular classification drives precise, automated segmentation and access policies. Enriching ISE with real device intelligence eliminates manual profile-building.
ATT&CK Analysis and Vulnerability Prioritization	ATT&CK Analysis determines actual exploitability for each vulnerability on each device in the specific network topology, reducing millions of CVEs to the subset carrying real risk.	Security teams act on the 1% that matters. Risk Simulator models expected risk reduction before any action is taken, targeting limited remediation hours to highest-risk devices.
Segmentation Orchestration	Policy Auto-Recommendation generates conflict-free DACLs and SGACLs from observed device behavior. Policy Simulation validates impact before deployment. Policies push directly to Cisco ISE and Catalyst Center.	Segmentation programs stalled by complexity are fully deployed and maintained. Policy Simulation eliminates disruption risk; Continuous Segmentation keeps enforcement current.
Quarantine and Containment	Automated device quarantine and unquarantine via Cisco ISE directly from the platform, with operational-dependency awareness. Service restores automatically upon remediation.	Streamlined incident response reduces mean time to contain. Operational-safety awareness prevents isolating devices whose disruption would carry its own risk.

Key Solution Benefits

- Device classification and profiling across IoT, OT, IoMT, and IT that drives precise, automated network policy
- ATT&CK Analysis that identifies truly exploitable vulnerabilities in your specific environment, not just high CVSS scores
- Policy Simulation that validates segmentation impact against live traffic before any rule goes live
- Direct policy enforcement across Cisco ISE and Catalyst Center with no manual rule writing
- Rapid containment of compromised devices with operational-safety awareness and automatic service restoration

Technical Solution

Asimily integrates with Cisco ISE within the enterprise through the pxGrid controller node (px-Grid API) and the ISE admin node (ERS API). A dedicated Asimily edge appliance or a virtual machine acting as Collector helps Asimily cloud-based portal to connect Cisco ISE and any other third-party vendor platforms deployed within a customer's private network. The Collector must have outbound connectivity with the customer's dedicated portal server in the cloud. The Collector must also have internal connectivity with the required platform such as Cisco ISE.



About Asimily

Asimily is the Proactive Cyber Defense Platform across your entire cyber asset attack surface: IoT, OT, IoMT, and IT. It empowers teams to reduce risk efficiently by identifying the riskiest devices, prioritizing what matters, and continuously orchestrating the segmentation and mitigation actions that close exposures without disrupting operations.

www.asimily.com

About Cisco Networks

Cisco (NASDAQ: CSCO) is the worldwide leader in technology that powers the Internet. Cisco inspires new possibilities by reimagining your applications, securing your data, transforming your infrastructure, and empowering your teams for a global and inclusive future.

www.cisco.com