ELISITY

SOLUTION BRIEF

Elisity Microsegmentation: Zero Trust Policies for Users, Workloads, Agents and Devices

Most Segmentation Projects Stall Before Enforcement

Attackers can move laterally in minutes. CrowdStrike's 2026 Global Threat Report puts average eCrime breakout time at 29 minutes. Network segmentation helps contain that movement and reduce the blast radius of a breach. Yet most segmentation programs stall long before they enforce anything, buried in NAC and 802.1X rollouts, agent coverage gaps, firewall rule sprawl, and VLAN redesign.

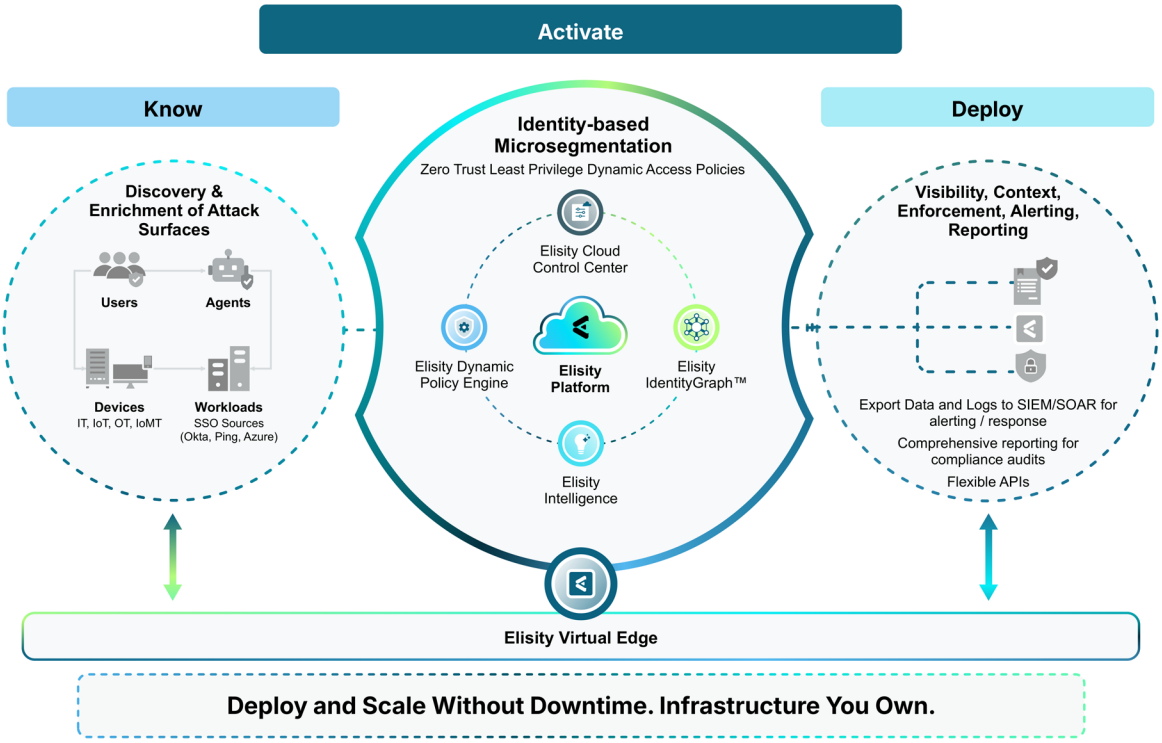
Elisity takes a different approach. Identity-based microsegmentation decouples access from the network, so policy follows users, workloads, agents and devices instead of an IP address or a VLAN. Elisity discovers and classifies connected assets from passive telemetry on supported Cisco, Juniper, Arista, HPE and Hirschmann network infrastructure, including IoT, OT, IoMT and legacy devices that cannot run an agent. Elisity requires no agents, no new hardware, no re-IP and no network redesign. Simulate every policy against real traffic before you enforce it.

> "Elisity's identity-based microsegmentation brings tremendous capabilities to our security stack as a critical control point for containing ransomware, blocking malicious lateral network traffic and minimizing incident blast radius."
>
> Aaron Weismann,
> CISO at Main Line Health

Main Line Health®

Gartner COOL VENDOR 2025

Gartner®, Cool Vendors™ in Cyber-Physical Systems Security 2025, Katell Thielemann, 18 September 2025. GARTNER and COOL VENDORS are trademark of Gartner, Inc. and/or its affiliates. Gartner does not endorse any vendor, product or service depicted in its research publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner research publications consist of the opinions of Gartner's Research & Advisory organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this research, including any warranties of merchantability or fitness for a particular purpose.



Solution Overview

Elisity delivers identity-based microsegmentation on the network infrastructure you already own. Elisity requires no agents, no new hardware, no new VLANs and no re-IP.

The Elisity microsegmentation platform:

- Discovers and classifies users, workloads, agents and devices.
- Correlates identity, behavior, traffic, and risk per entity.
- 25+ native integrations: identity, EDR, CMDB, CPS, ITSM. Many bi-directional.
- Simulates every policy against real traffic before you enforce it.
- Recommends policies for operator review and approval.
- Turns compliance scope into a policy attribute, not a spreadsheet.
- First enforced policy in days to weeks.

Customer-Built AI Agents

Customers can point their own AI agents at Elisity through an open command line interface. The package gives an agent the object model, the platform terminology, and worked examples, so a team can ask its own agent in plain language to verify Zero Trust policies or spot policy drift, and keep that agent under its own control.

Know Who and What's On Your Network

Identity, behavior, traffic, and risk, correlated from 25+ native integrations. Users, workloads, agents and devices classified with business meaning and risk quantification. Elisity Virtual Edge Nodes collect passive telemetry from the network infrastructure you already own; no SPAN, no TAP, no active scanning, nothing on the device. Every attribute carries source attribution and a confidence score, so your team can see which connector asserted what. Retroactive Enrichment back-fills the estate when a new connector comes online, so the graph does not decay the way a CMDB or a spreadsheet does.

Activate Zero Trust Policies

Identity-based least-privilege access policies for users, workloads, agents and devices. Simulate first. See the impact. Then activate. One policy graph covers IT, IoT, OT, and IoMT; including the FDA-regulated and brownfield assets that cannot run an agent. Simulation mode shows blast radius against real traffic before a single packet is blocked. Policies can be static or dynamic: set them to re-evaluate as risk and vulnerability data change, and let Elisity Intelligence recommend new policies and optimizations for your team to approve.

Deploy and Scale Without Downtime

Deploy on the network infrastructure you already own. Scale with the team you already have. No new hardware. No new VLANs. No network redesign. Runs as a VM on a supported hypervisor, a container on supported Cisco switches, or in your cloud. At Virtual Edge onboarding, clear Enable Policy Enforcement for discovery-only operation; plan enforcement for your change window. Site-scoped RBAC supports SOC, network, IT and GRC teams. Microsoft Sentinel, Splunk, Cribl, Syslog, NetFlow, and ServiceNow (inbound by default) connect through native integrations and a REST API.

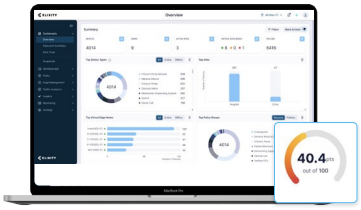
Contain Machine-Speed Attacks

Attackers no longer set the pace alone. In pre-release testing, Anthropic's Claude Mythos Preview found and exploited zero-day vulnerabilities across major operating systems and browsers, including a 27-year-old OpenBSD flaw. Anthropic reported thousands of additional findings undergoing validation and disclosure. As AI accelerates vulnerability discovery and exploitation, patching alone cannot contain a breach. Identity-based microsegmentation limits lateral movement so one compromised asset does not open the rest of the network.

Elisity Microsegmentation Platform

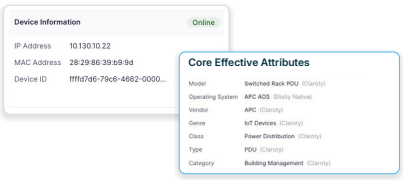
Elisity Cloud Control Center

Cloud-hosted control, visibility and reporting. Manage identity-based policies centrally and track segmentation progress with Zero Trust Posture Score.



Elisity IdentityGraph™

One correlated record for users, workloads, agents and devices: identity, behavior, traffic and risk from 25+ native integrations, each attribute traceable to its connector.

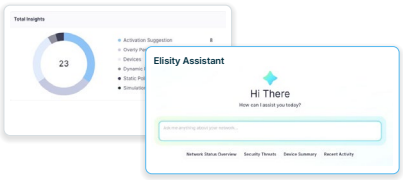


Elisity Dynamic Policy Engine

Creates and enforces dynamic, context-aware policies from IdentityGraph™ identity. Policies follow identity changes, independent of IP addresses.

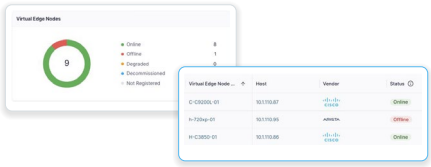
Elisity Intelligence

Cloud Control Center's AI classifies unknown devices, suggests policy groups and allow/deny rules from traffic, flags permissive rules with no traffic, and answers questions via Elisity Assistant. Models are private and single-tenant; customer data is not used for training. Proposed policies start in simulation; changes require human approval.



Elisity Virtual Edge

Translates identity and policy into controls your network infrastructure enforces in hardware. Normalizes policy across multiple vendors and sites.



Your Environment

Your Network Infrastructure

Elisity enforces least-privilege policy on supported Cisco, Juniper, Arista, HPE and Hirschmann network infrastructure. Elisity requires no agents, no new hardware, VLANs or re-IP.

Your Existing Tech Stack

Elisity enriches device records with Claroty, Armis, Asimily, Nozomi, CrowdStrike, SentinelOne, Tenable and ServiceNow (inbound by default). Many integrations are bi-directional, so context flows back into your systems of record.

25+ Native Integrations

CLAROTY · asimily · ARMIS · NOZOMI NETWORKS · CROWDSTRIKE · SentinelOne · tenable · servicenow · Microsoft Entra ID · splunk>

From Site Activation to Enforced Policy

First enforced policy in days to weeks, not quarters

Measure Containment with Zero Trust Posture Score

Containment is now measurable. The Zero Trust Posture Score rates segmentation posture from 0 to 100, refreshed daily and averaged from active factors: Policy Deployment, Least Privilege and Malware Lateral Movement. Higher scores reflect tighter restrictions on possible communication paths. Paths marked as Independent Control receive full restriction credit, including those enforced by non-Elisity firewalls.

> "We deployed [Elisity] at two of our sites in less than an hour, and by the next day we were confidently implementing policies. This made Elisity an indispensable part of our network security strategy across our manufacturing sites."

Max Everett,
CISO at Shaw Industries

Elisity vs Legacy Microsegmentation Implementations

Elisity delivers identity-based microsegmentation for healthcare, manufacturing, pharmaceutical, financial services and public sector enterprises. Compliance scope, including HIPAA, IEC 62443, PCI DSS, NIS2 and NIST, can become an IdentityGraph™ attribute that informs policy.

	Firewalls, VLANs/ACLs	Host Firewalls or Agent-based Solutions	ELISITY	Proxy Cloud Based
Coverage across IT, IoT, OT and IoMT	×	×	✓	×
Native discovery of users and devices	×	×	✓	–
Visibility and context enrichment	–	–	✓	–
Dynamic policy automation	×	–	✓	–
Downtime-free rollout and updates	×	–	✓	–
Application and process control (Layer 7)	✓*	✓	–	–

✓ Supported – Partial / varies × Not native *Next-generation firewalls

Elisity Microsegmentation Use Cases

Network Asset Discovery	Discover IT, IoT, OT, IoMT and legacy devices that cannot run an agent. A Top 10 US health system: 99% discovery in 4 hours; 213K endpoints across 354 sites.
Network Visibility	Flow evidence for investigations and audits, with Flow Context and Confidence Scores on Layer 4 flows. Natural-language investigation through Elisity Intelligence.
IoT and IoMT Segmentation	Cameras, printers, badge readers, infusion pumps and imaging modalities. Identity-based policy with no device modification.
OT Segmentation	PLCs, sensors and brownfield production cells. Apply network policy without PLC re-engineering or changing the device.
Ransomware and Lateral Movement Containment	East-west containment with Ransomware Isolation Policy Sets. A consumer-health manufacturer: no downtime or incidents during deployment or as policies were applied. MultiCare: 13 hospitals and 350+ clinics, after 4 prior failed segmentation attempts.
Segmentation Compliance	HIPAA, IEC 62443, PCI DSS, NIS2 and NIST: scope becomes a policy attribute. Main Line Health: CSO50 2024 and CIO 100 2025 recognition.

"For over 10 years we were looking at what was in the market, whether it be putting firewalls in place, isolating through different VLANs. Nothing really would work for us."

Nathan Phoenix, Information Security Officer
Southern Illinois Healthcare

"We've been able to get [Elisity] up within two months in an organization that has 15 hospitals ... 23,000 active users, 1,800 vendors, and 85,000 devices across a majorly complex environment."

David Finkelstein, CISO
St. Luke's University Health Network

Let's Discuss Your Microsegmentation Plan

elisity.com/demo

BOOK A DEMO