ELISITY

SOLUTION BRIEF · HEALTHCARE

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

Most Clinical Segmentation Stalls Before Enforcement

HHS's proposed HIPAA Security Rule update would require network segmentation to limit access to electronic protected health information. The proposal is not a final rule; the current Security Rule remains in effect. Yet clinical segmentation programs stall before enforcement, buried in NAC and 802.1X rollouts, medical-device agent gaps and VLAN redesign. In Omdia research commissioned by Elisity, only 9% of organizations implementing microsegmentation have 81% or more of critical systems covered.

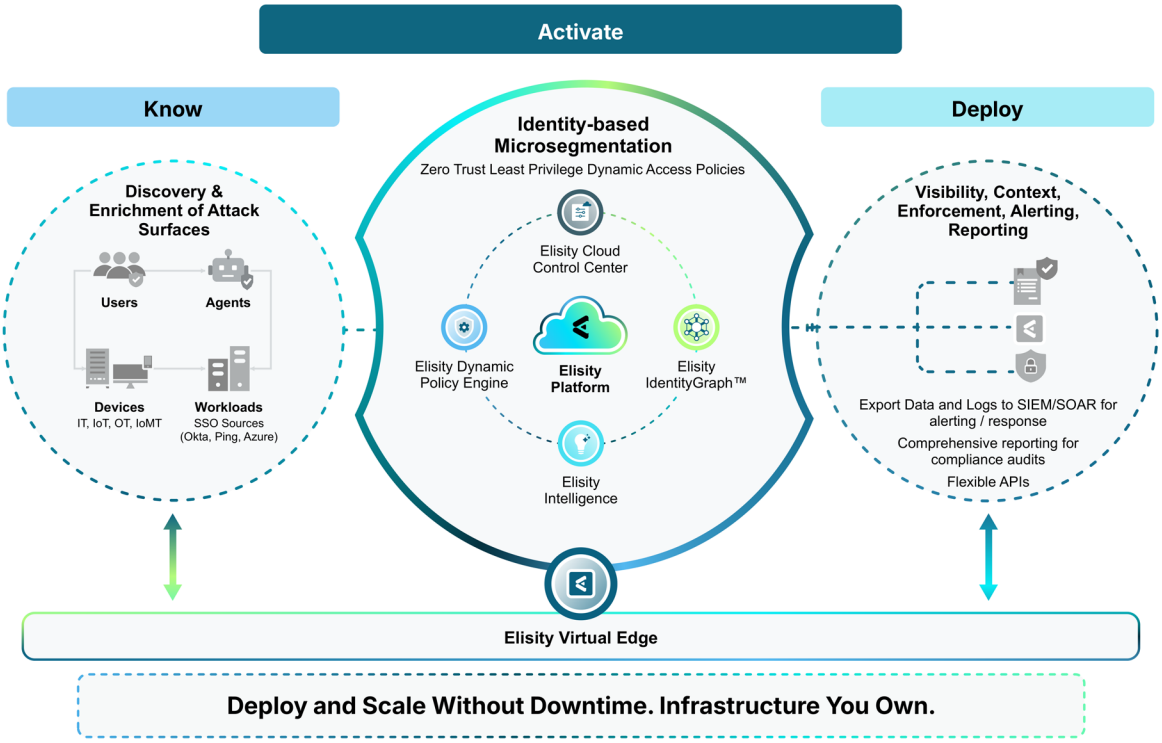
Elisity takes a different approach. Identity-based microsegmentation decouples access from the network, so policy follows users, workloads, agents and devices instead of an IP address or a VLAN. Elisity discovers connected assets from passive telemetry on supported Cisco, Juniper, Arista, HPE and Hirschmann infrastructure, including medical devices that cannot run an agent. Elisity requires no agents, no new hardware, no re-IP and no network redesign. Simulate policies against real traffic before enforcement to protect care continuity.

> "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 healthcare 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, SIEM. 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 connect their own AI agents to Elisity through an open command line interface. Its object model, platform terminology and examples help teams ask an agent in plain language to verify Zero Trust policies or spot drift across clinical networks, while keeping that agent under their 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, and nothing installed on the medical 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, enriching discovered medical assets with the latest available context.

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 clinical IT, IoT, OT and IoMT, including medical devices 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 clinical change windows. Site-scoped RBAC supports SOC, network, IT and GRC teams. Microsoft Sentinel, Splunk, Cribl, Syslog and NetFlow connect through native integrations and a REST API.

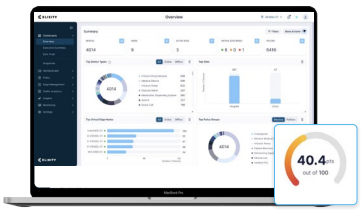
Contain Machine-Speed Attacks

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 protect legacy medical devices. Identity-based microsegmentation limits lateral movement between clinical systems, helping contain a breach and protect care continuity.

Elisity Microsegmentation Platform

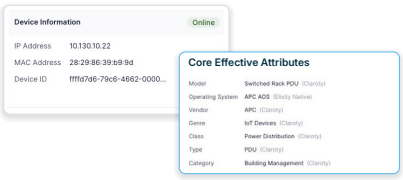
Elisity Cloud Control Center

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.

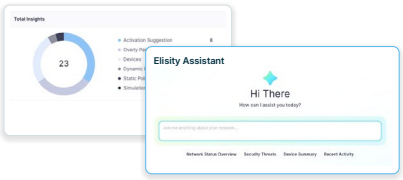


Elisity Dynamic Policy Engine

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

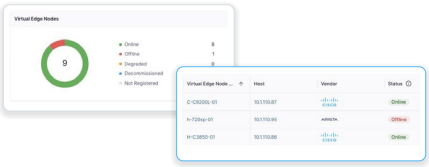
Elisity Intelligence

Cloud Control Center's AI classifies devices, suggests healthcare policy groups and allow/deny rules, flags unused permissive rules, 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 Healthcare Environment

Your Clinical Network

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 Clinical Tech Stack

Integrations enrich device identity, behavior and risk. The Custom Connector uses biomed spreadsheets to add asset tags and service lines as policy criteria for devices already discovered.

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

Clinical and security teams can track containment on a daily 0–100 scale. Zero Trust Posture Score averages active factors: Policy Deployment, Least Privilege and Malware Lateral Movement. Higher means more restricted paths. Independent Control paths, including non-Elisity firewalls, receive full restriction credit.

2 WEEKS	HOURS TO DAYS	DAYS TO WEEKS	WEEKS TO MONTHS
Planning and Academy training	Virtual Edge install and discovery	Policy strategy, simulation, first policy	Site-by-site rollout; clinical change windows

"I kept waiting for the moment where something's got to break, something's got to give. And it just didn't. ... Since it's [Elisity] been deployed, it's almost hands-off. I'm in it maybe five to ten hours a week."

Taylor Calloni,
Cybersecurity Engineer III
Southern Illinois Healthcare

Elisity vs Legacy Healthcare Microsegmentation

Elisity delivers identity-based microsegmentation for hospitals, health systems and clinics. Map healthcare compliance scope to IdentityGraph™ attributes that inform policy, including HIPAA, HHS 405(d) HICP, HITRUST and NIST CSF 2.0.

	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

Healthcare Microsegmentation Use Cases

Clinical and Biomedical Device Discovery	Infusion pumps, telemetry, EKGs, imaging systems, beds and nurse call. A Top 10 US health system: 99% discovery in 4 hours; 213K+ endpoints across 354 sites.
IoMT Segmentation Without Device Changes	Identity-based policy with no re-IP, no NIC swap and nothing installed on the device. St. Luke's University Health Network: 15 hospitals and 85,000 devices in 46 days.
Ransomware Containment and Care Continuity	Contain lateral movement between clinical workstations, EHR servers and medical devices. MultiCare: 13 hospitals and 350+ clinics, after 4 prior failed segmentation attempts.
Clinical OT and Building Systems	Segment HVAC, nurse call, pneumatic tube systems and physical security from clinical networks. Southern Illinois Healthcare found undocumented Windows 7 machines supporting tube systems.
Segmentation Compliance and Audit Evidence	HIPAA, HHS 405(d) HICP, HITRUST and NIST CSF 2.0: scope becomes a policy attribute. Main Line Health: CSO50 2024 and CIO 100 2025 recognition.
Retiring Legacy Segmentation Cost	Reduce firewall-and-VLAN build-out with the network infrastructure and team you already have. A Top 10 US health system: 76% lower segmentation TCO, from $38M to $9M.

"Elisity gives us the ability to microsegment in a way that's operationally sustainable and doesn't add a ton of overhead — and in healthcare, where you simply can't afford downtime, that's critical."

Jason Elrod, CISO
MultiCare Health System

"You have to do it smart and swift, but in a way that the business really doesn't even see it. They just go, 'oh, I get to use that still.'"

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

Build Your HIPAA Segmentation Roadmap

elisity.com/microsegmentation-healthcare

BOOK A DEMO