ELISITY

SOLUTION BRIEF · MANUFACTURING & OT

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

> "Now we can plug any device into the network, it gets profiled along with the identity behind that device, and no matter where that device plugs into the network, the policy follows."
>
> Mike Elmore,
> CISO at GSK

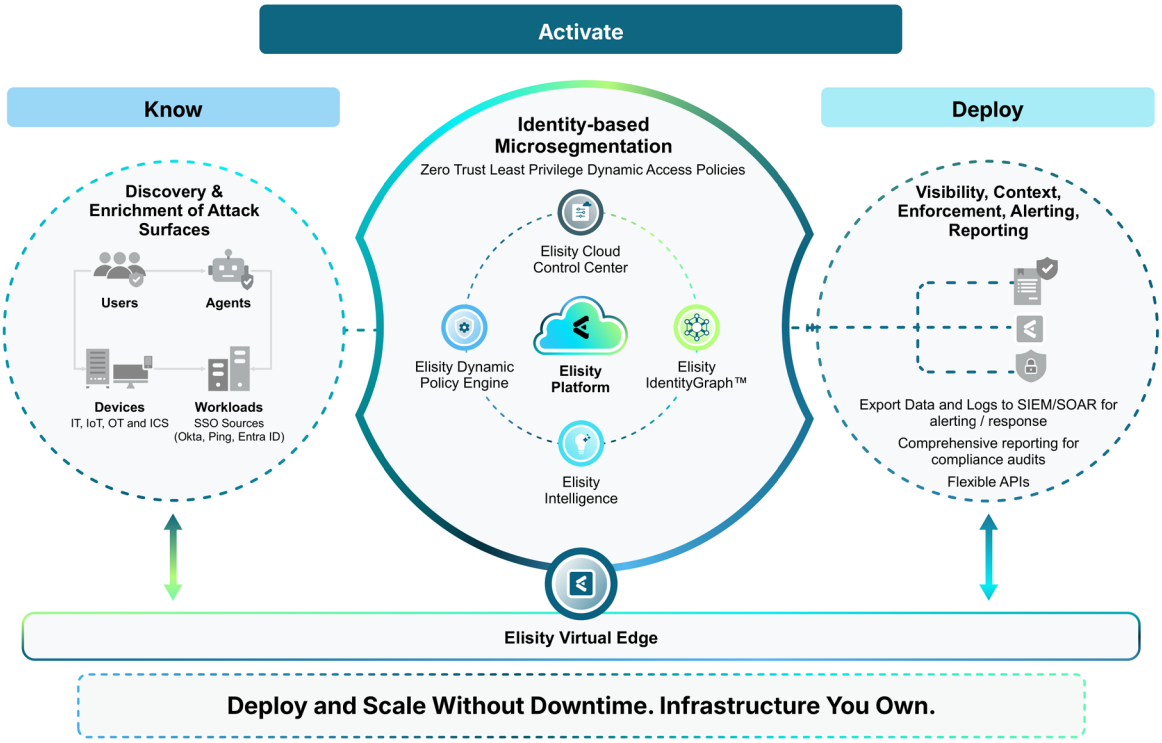
Most OT Segmentation Projects Stall Before Enforcement

IEC 62443 calls for zones and controlled conduits on plant networks. NIST CSF 2.0 supports network segregation; defense suppliers may carry NIST SP 800-171 obligations, and NIS2 covers specified manufacturing sectors. The challenge is applying these controls without stopping production. NAC and 802.1X rollouts, controller limitations, per-cell firewalls and re-IP can stall enforcement. 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 lets policy follow users, workloads, agents and devices instead of IP addresses or VLANs. Passive telemetry discovers connected assets on supported Cisco, Juniper, Arista, HPE and Hirschmann infrastructure, including controllers 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 enforcing them during plant maintenance windows.

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 plant and enterprise network infrastructure you already own. Elisity requires no agents, no new hardware, no new VLANs and no re-IP.

Our 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.

Customer-Built AI Agents

Customers can connect their own AI agents to Elisity through an open command line interface. Its object model and examples help teams ask agents in plain language to verify Zero Trust policies or spot drift across plant networks, while keeping those agents under their own control.

Know Who and What's On Your Network

Identity, behavior, traffic and risk, correlated from whichever of 25+ integrations you run. Every user, workload, agent and device the network sees, classified with business meaning. 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 device, so nothing touches a validated controller. The Custom Connector ingests the plant spreadsheet too, enriching devices already found; Retroactive Enrichment back-fills the estate when a connector comes online.

Activate Zero Trust Policies

Identity-based least-privilege policies for every user, workload, agent and device. Simulate first. See the impact. Then activate. One policy graph covers plant IT, IoT and OT — including the controllers that cannot run an agent. Policy is written per relationship on port and protocol, never a blanket allow. Simulation mode shows the blast radius against real traffic before a single packet is blocked. Engineers can lock controllers to a Policy Group so identity changes do not move them to another group.

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 plant maintenance 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.

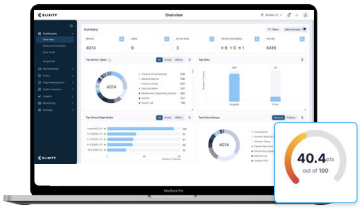
Contain Machine-Speed Attacks

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 OT devices. Identity-based microsegmentation limits lateral movement between enterprise IT and plant systems, helping contain a breach and protect production.

Elisity Microsegmentation Platform

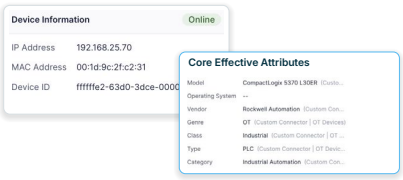
Elisity Cloud Control Center

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.

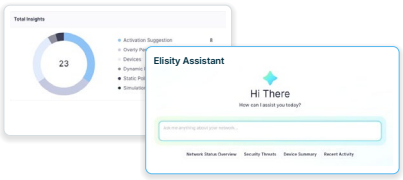


Elisity Dynamic Policy Engine

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

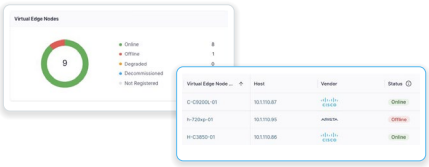
Elisity Intelligence

Cloud Control Center's AI classifies devices, suggests industrial 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 Manufacturing Environment

Your Plant Network

Elisity enforces policy on supported Cisco, Juniper, Arista, HPE and Hirschmann infrastructure, at the access or aggregation layer. No agents, no new hardware, VLANs or re-IP.

Your Industrial Tech Stack

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

25+ Native Integrations

CLAROTY · DRAGOS · ARMIS · NOZOMI NETWORKS · CROWDSTRIKE · SentinelOne · ORDR · 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

Plant 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.

"It's always a challenge when you have a paradigm shift. There are going to be those who initially have some doubts, and the proverbial question: why is it going to be different this time?"

Jeff Binkley,
Security Architect
GSK

Elisity vs Legacy OT Microsegmentation

Elisity delivers identity-based microsegmentation for manufacturers and industrial operators. Map compliance scope to IdentityGraph™ attributes that inform policy, including IEC 62443 zones and conduits, NIST CSF 2.0 and NIS2.

	Firewalls, VLANs/ACLs	Host Firewalls or Agent-based Solutions	ELISITY	Proxy Cloud Based
Coverage across IT, IoT, OT and ICS	×	×	✓	×
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

Manufacturing Microsegmentation Use Cases

Plant-Floor and OT Asset Discovery	PLCs, HMIs, VFDs, robotics, safety systems and engineering workstations. Passive network telemetry: no TAP, no SPAN and no active scanning.
Enforcement Through a Cloud Outage	The last configuration stays in place on the network infrastructure if the plant loses its connection to the cloud.
IT/OT Isolation and Ransomware Containment	Contain lateral movement between enterprise IT, plant networks and the OT estate. Write policy per relationship on port and protocol, rather than a blanket allow.
IEC 62443 Zones and Conduits	Organize assets into zones with Policy Groups and control the conduits between them. Apply identity-based policies across the existing network infrastructure.
Third-Party and Integrator Access	Scope OEM, integrator and contractor access to the assets they support. Update group membership and policy as access requirements change.
Retiring Legacy Segmentation Cost	Reduce firewall-and-VLAN build-out with the network infrastructure and team you already have. A global industrial electronics manufacturer: $18.5M+ capital avoided.

"We were able to go in and quickly test it, get value and visibility without any disruption. ... Whatever the variety of attacks coming in, we can limit the damage, we can control it, we can manage it."

Max Everett, CISO
Shaw Industries

"Our ability to scale policy deployment across the business enables the business to expand and scale at speed."

Edmond Mack, former CISO
Haleon

Segment the Plant Floor Without Stopping It

elisity.com/solutions/industrial

BOOK A DEMO