

Elisity Microsegmentation for Financial Services: Contain Machine-Speed Attacks

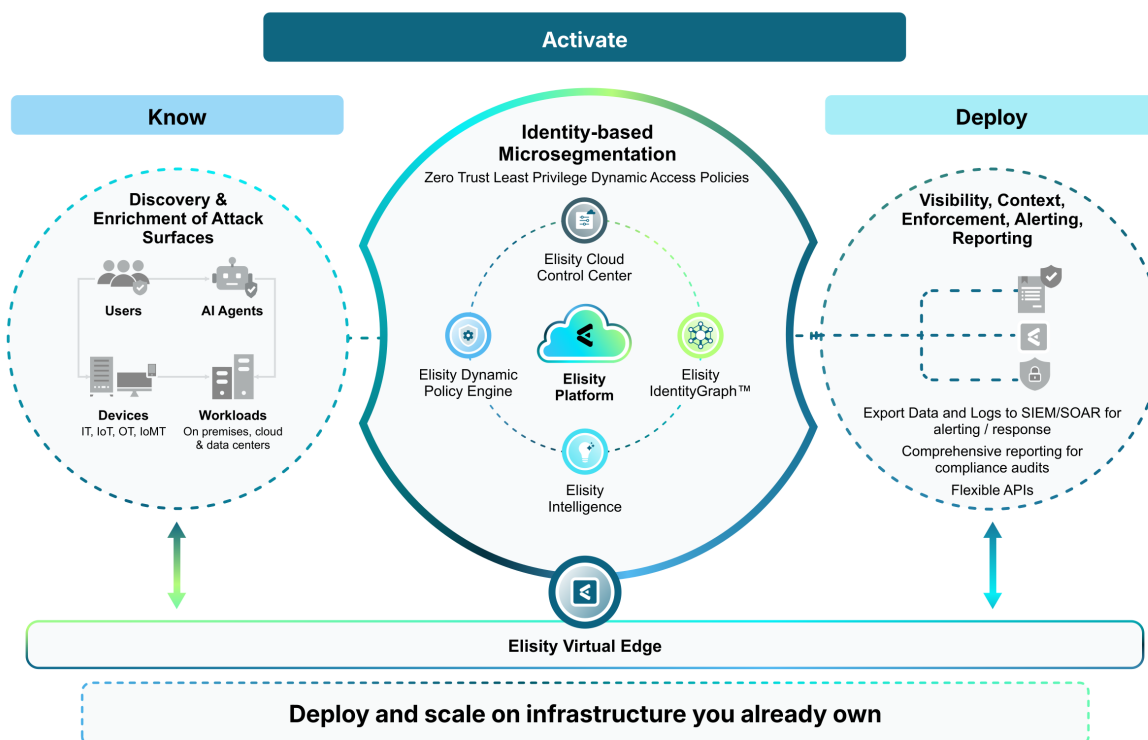
When Attackers Move Faster Than Defenders Can Patch

Acquisitions compress integration timelines. Frontier AI compresses attack timelines. Financial institutions need to connect acquired environments, protect branch services and satisfy examiners without turning every change into a network redesign. Inherited devices, legacy systems and IoT assets can remain exposed while teams wait for agents, firewall rules and VLAN changes. The priority is practical containment: integrate what the business needs, isolate what remains uncertain, and retire complexity as the environment becomes understood.

Elisity makes identity the basis for network access. Policies follow users, workloads, agents and devices across branches and corporate sites. Passive telemetry discovers connected assets on supported infrastructure, including devices that cannot run an agent. Existing identity, EDR and CMDB tools enrich each record. Simulate policies against real traffic, then enforce least privilege on the network you already own. Elisity requires no endpoint agents, no new hardware, no re-IP and no network redesign.

"We can't assume we'll patch every vulnerability before an attacker finds it. When attackers move at machine speed, we need to limit their access to critical systems. Our priority is to contain a compromise before it spreads and keep banking services running."

Chief Information Security Officer
U.S. financial services institution



Solution Overview

Elisity delivers identity-based microsegmentation through the branch and corporate network infrastructure you already run. Limit each asset to the communication it needs, without installing software agents on protected devices.

The Elisity microsegmentation platform:

- Discover connected devices and cloud workloads.
- Correlate identity and security context.
- Build policy around users, devices and workloads.
- Simulate changes against observed traffic.
- Review AI proposals before enforcement.
- Connect policy to business and compliance scope.
- Roll out in phases with your team.

AI Agents and Workloads

AI agents run on laptops, servers and cloud workloads. Apply access policy to the device or workload hosting the agent, outside its runtime. Additional non-human identities, including service accounts and machine credentials, are in development.

Know Who and What's On Your Network

Bring users, devices and workloads into one policy context. Combine passive network observations with identity, endpoint, CMDB, IoT and cloud context. Use that evidence to organize branch devices, payment systems and critical business services around business requirements. AWS and Azure connectors add workload tags and instance details to IdentityGraph.

Activate Zero Trust Policies

Build identity-based policy around the communication each asset needs. Protect branch IT, IoT and legacy systems, including devices that cannot run a software agent. Simulate changes against observed traffic, review the results, then choose what moves to enforcement. Elisity Intelligence proposes classifications, Policy Groups and policies for administrator review.

Deploy and Scale with Your Team

Enforce through supported network infrastructure, without installing agents on protected assets or redesigning the network. Start with discovery and stage enforcement around branch operational requirements. Connect existing security and operations tools to enrich context and share policy events. Cloud discovery supplies context; confirm the enforcement path for each environment.

Contain Machine-Speed Attacks

Patching addresses the vulnerabilities you know about. Identity-based microsegmentation helps contain what you cannot patch or predict by limiting unnecessary communication between branch devices, payment systems and critical business services. Apply policy to the devices and workloads running your business—including those hosting AI agents—so a compromised asset has fewer paths to other systems.

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 per asset, combining network observations with identity, endpoint, CMDB, IoT and cloud context. Service-account and machine-credential support is in development.

Elisity Dynamic Policy Engine

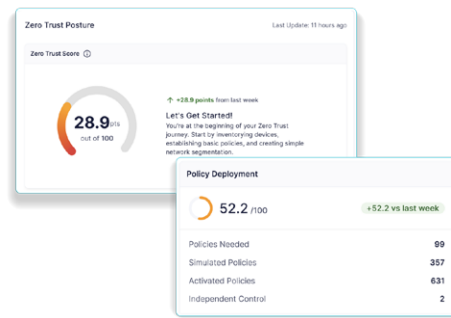
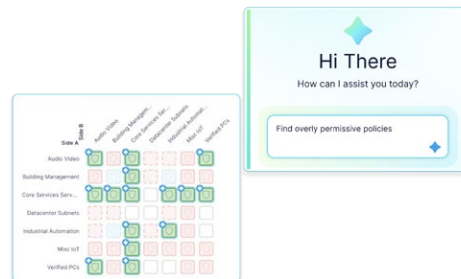
Creates and enforces dynamic, context-aware policies from IdentityGraph™ identity. Policies follow identity changes, independent of IP addresses.

Elisity Intelligence

Proposes device classifications, Policy Groups and policies, flags unused Allow rules, and answers questions through Elisity Assistant. Suggested policies start in simulation; administrators approve enforcement.

Elisity Virtual Edge

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



Your Financial Environment

Your Branch Network

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

Your Security and IT Stack

Active Directory, Entra ID, ServiceNow and EDR sources enrich identity and risk. Splunk connects policy events to the SOC. Add branch and PCI-scope attributes through the Custom Connector.

Connected Security Context

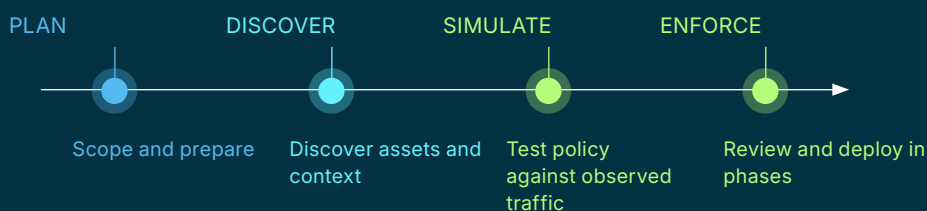


From Site Activation to Enforced Policy

A phased path from discovery to enforcement

Track Progress with Zero Trust Posture Score

Track segmentation posture and see where policy needs attention. The Zero Trust Posture Score brings policy deployment and access restrictions into a daily view. Use it alongside observed traffic and branch requirements to prioritize the next policy changes.



"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

Segmentation and Audit Evidence

Apply identity-based policy across branches, corporate sites and supporting workloads. Organize assets around business services and regulatory scope, then use policy and traffic evidence to support reviews. Segmentation is one part of a broader compliance program.

	Network firewalls, VLANs / ACLs	Host-based segmentation		Cloud proxy access
Network coverage on supported infrastructure	Varies	Varies	✓	Varies
User and device discovery	Varies	Varies	✓	Varies
Visibility and context enrichment	Varies	Varies	✓	Varies
Dynamic policy automation	Varies	Varies	✓	Varies
Simulate policy before enforcement	Varies	Varies	✓	Varies
Application and process control (Layer 7)	Varies	Varies	—	Varies

Capabilities vary by product and deployment. Elisity checks refer to supported infrastructure.

Financial Services Microsegmentation Use Cases

Branch Threat Containment	Limit lateral movement between branch devices and critical business services. Enforce identity-based policy through supported infrastructure.
Workload, IT, IoT and OT Discovery	Discover employee endpoints, application/cloud workloads, HVAC, badge readers and other IoT/OT. Enrich their records with identity and security context.
Cardholder Data Environment Isolation	Use Policy Groups and access restrictions to separate in-scope systems. Include segmentation validation in the broader compliance program.
M&A and Transitional Environments	Connect required services while isolating systems still under review. Learn traffic relationships and simulate policy before enforcement.
AI Workload Isolation	Apply network access policy to devices and workloads hosting AI agents. Allow required connections and limit unnecessary paths to sensitive services.
Identity-Based Policy Across the Estate	Build policy around users, devices and workloads across branches and corporate sites. Scale through supported infrastructure with existing teams.

“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 at the Speed of Your Business
elisity.com/demo

BOOK A DEMO

