

## SOLUTION BRIEF

# Elisity Microsegmentation: Accelerate Zero Trust Security in Weeks, Not Years

## A Leap Forward in Network Segmentation Architecture

With cyberattacks and attack surfaces growing rapidly across all users, workloads, and devices, enterprises face mounting challenges in protecting their networks beyond traditional email and endpoint security. With attackers leveraging lateral movement in over 70% of successful breaches, organizations are prioritizing microsegmentation to reduce attack blast radius. In 2025, NIST, CISA, regulators, and cyber insurers are mandating network segmentation as a critical security control.

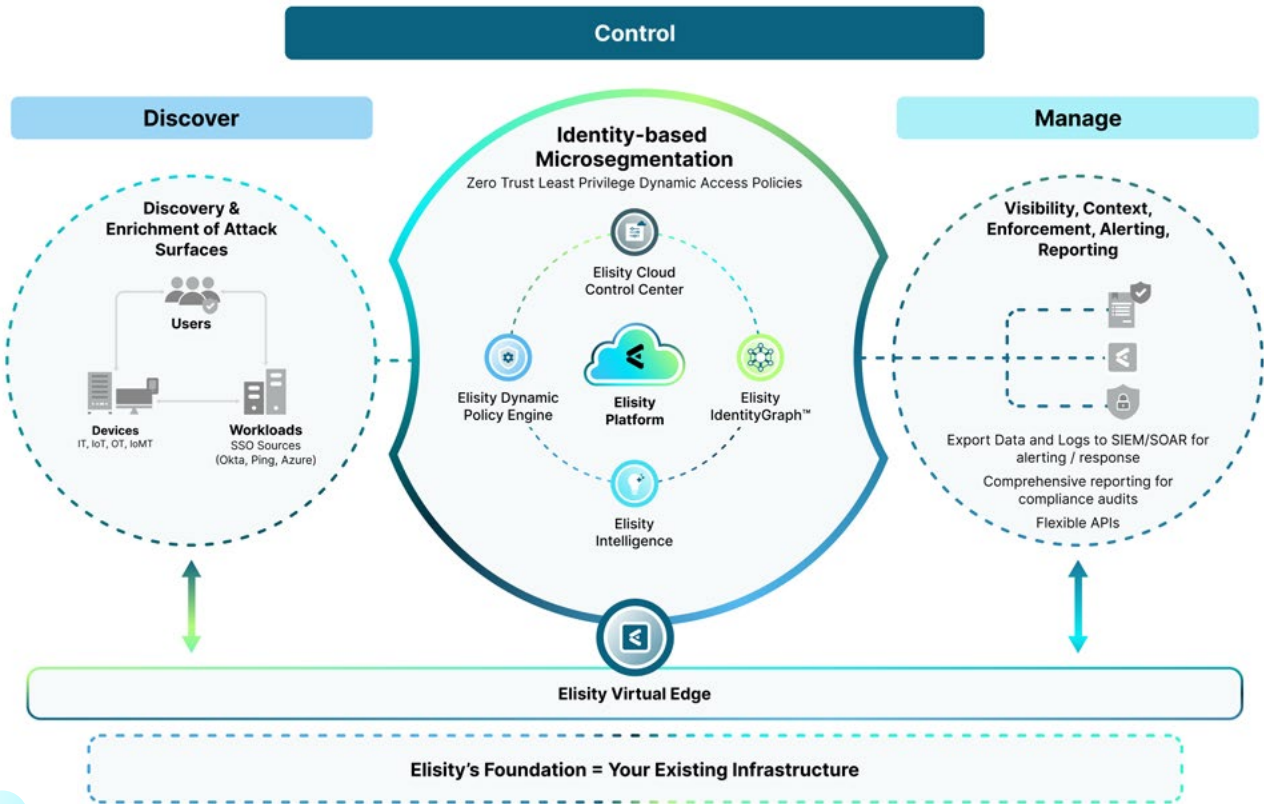
Traditional microsegmentation projects often become complex, never-ending initiatives involving NAC/802.1x, agents, firewalls, and extensive VLAN configurations. The Elisity platform takes a different approach. Trusted by global pharmaceutical, health care, and manufacturing enterprises, our identity-centric architecture decouples access from underlying network infrastructure. The solution can be implemented at scale within weeks using your existing switching infrastructure—eliminating the need for new agents, host firewall configurations, hardware, additional VLANs, firewall rules, or ACLs.

“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



The GARTNER COOL VENDOR badge is a trademark and service mark of Gartner, Inc., and/or its affiliates, and is used herein with permission. All rights reserved. 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 empowers security and IT teams to achieve robust microsegmentation using their existing infrastructure, and does not require new hardware, agents, VLANs, or complex ACLs.

### The Elisity microsegmentation platform:

- Rapidly discovers every user, workload, and device.
- Correlates metadata and adds context in the Elisity IdentityGraph™.
- Integrates with your: identity systems, EDR, CMDB, and asset tracking platforms.
- Centralizes granular policy creation and simulation capabilities.
- Automates dynamic policies that can be configured to change as risk changes—all via machine-learning algorithms.
- Enables faster compliance reporting and full API extensibility.
- Implements in a few weeks and requires no downtime.

### Discover

Elisity empowers your teams with comprehensive discovery and visibility of every user, workload and device, everywhere on your network, both managed and unmanaged. By ingesting metadata from your existing network infrastructure and by integrating with your existing tech stack, Elisity correlates those identity, configuration, risk scores, and detailed data about the device and adds them to your unique and dynamic Elisity IdentityGraph™. Your teams get actionable context and deep visibility of all users, workloads and devices on your networks in real-time, even unmanaged and ephemeral IT/IoT/OT/IoMT devices.

### Control

Elisity's "no-fear" policy-creation engine dynamically manages and enforces security and access policies quickly and without risk. Elisity's Cloud Control Center enables your team to create, simulate and apply smart, automated dynamic security policies that persist for every device, wherever and whenever a device appears on your networks. Elisity makes it easy to apply least privilege access for your users, workloads and devices to protect your organization from east-west attacks. Your unmanaged device chaos will disappear.

### Manage

Elisity's cloud-delivered policy management control plane quickly connects to your existing network. Having this capability abstracted from our network infrastructure means there are no additional firewalls, VLANs, ACLs, and agents to install, configure, and update, making it easy to deploy at every location in hours and without downtime. Unlike legacy solutions, policies are not tied to IP addresses or brittle network constructs. Elisity translates security policies into efficient controls that your network infrastructure enforces, making Elisity, the high-performance and simplest-to-integrate microsegmentation platform available.

# Elisity Microsegmentation Platform

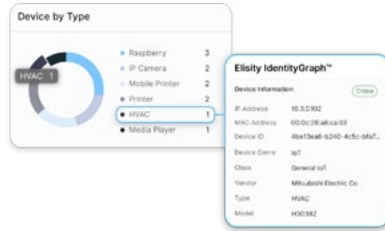
## Elisity Cloud Control Center

Centralized management console providing visibility, policy configuration, and analytics. Utilizes AI and machine learning to adapt to network changes.



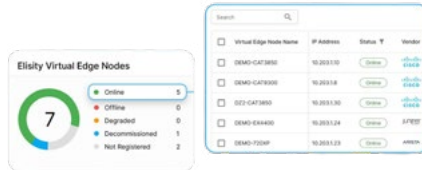
## Elisity IdentityGraph™

Creates a real-time, correlated visibility of user, workflow, and device metadata and relationships across the network, enabling teams with the confidence needed to create policies.



## Elisity Virtual Edge

Translates identity mappings and policies to your network infrastructure. Supports normalization of policies across multiple vendors, multiple sites.



## Elisity Dynamic Policy Engine

Enables the creation and enforcement of dynamic, context-aware policies based on the rich identity information provided by IdentityGraph™. Ensures granular control over network access.



## Your Environment

### Your Network Infrastructure

Elisity enforces least privilege access policies with your Cisco, Juniper or Arista switches. No agents. No new hardware, ACLS, additional VLANs or Re-IPing projects required.

### Your Existing Tech Stack

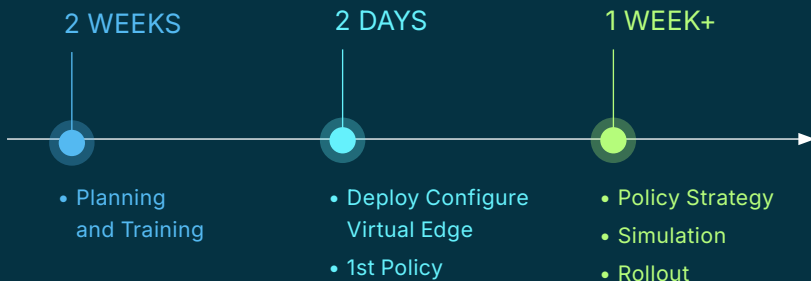
In addition to Elisity’s powerful platform, Elisity gains deeper insights to your users, workloads, and devices by integrating with your stack via APIs. It aggregates user, workload and device data from all available sources and integrations, becoming a valuable dataset for flexible dynamic policies.

## 50+ Integrations



## Average Elisity Implementation Time

Designed to be implemented in weeks, without downtime




“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 is a powerful micro-segmentation platform that delivers comprehensive security benefits for manufacturing, healthcare, and other enterprises with critical assets to protect. The platform enables organizations to rapidly implement identity-based security policies across their entire network infrastructure.

	Firewalls, VLANs/ACLs	Host Firewalls or Agent-based Solutions	 ELISITY	Proxy Cloud Based
<b>Gapless coverage</b> (Endpoints, Servers/ VMs, IoT/OT/IoMT)	✗	✗	✓	✗
<b>Native discovery of users and devices</b>	✗	✗	✓	—
<b>Visibility and context enrichment</b>	✗	—	✓	—
<b>Dynamic policy automation</b>	✗	—	✓	—

### Elisity Benefits and Use Cases

<b>99% discovery and visibility of all users, workloads and devices</b>	<ul style="list-style-type: none"> <li>• <b>Attack Surface Coverage</b> (Cover all of your IT, IoT, OT, IoMT)</li> <li>• <b>Comprehensive Visibility</b> (See enriched content for all users, workloads, devices)</li> <li>• <b>Faster Incident Response</b> (Real-time breach containment through dynamic policy enforcement)</li> </ul>
<b>Limit the blast radius, contain breaches Stop insider threats</b>	<ul style="list-style-type: none"> <li>• <b>Lateral Movement Prevention</b> (Block the tactic used in 70% of successful breaches)</li> <li>• <b>Ransomware Protection</b> (Stop the spread of ransomware)</li> <li>• <b>Cyber Insurance Premium Reduction</b> (Lower cyber insurance premiums by 20% or more)</li> <li>• <b>Prevent Credential Escalation Attacks</b> (Insulate from sub-par access policies)</li> </ul>
<b>Protect Intellectual Property</b>	<ul style="list-style-type: none"> <li>• <b>Prevent Data Exfiltration</b> (Block insider threats and protect data)</li> </ul>
<b>Prevent Downtime</b>	<ul style="list-style-type: none"> <li>• <b>Stronger Resilience</b> (Prevent widespread disruption to critical systems)</li> </ul>
<b>Continuous Policy Hygiene</b>	<ul style="list-style-type: none"> <li>• <b>Centralized Policy Management</b> (Comprehensive view of all policies, both manual and automated)</li> <li>• <b>Dynamic Automated Policies That Respond to Risks</b> (Intelligent policies that adapt to risk reports and anomalies)</li> </ul>
<b>Compliance and Regulations</b>	<ul style="list-style-type: none"> <li>• <b>Faster Audits</b> (Push-button reports per user, workload and device, compliance policy groups)</li> <li>• <b>Accelerated Zero Trust Maturity</b> (Centralize least privilege access policies for identity, devices, networks, workloads and data)</li> </ul>



**Let's Discuss Your Microsegmentation Plan**  
 — Learn More and [BOOK A DEMO](#)

