ELISITY

Gartner COOL VENDOR 2025

The CISO's Guide to Modern Microsegmentation: Identity-Driven Lateral Movement Prevention for Healthcare Organizations

Transforming Network Security from Static Perimeters to Dynamic, Zero Trust Protection

Executive Summary

Healthcare organizations face an unprecedented convergence of challenges that demand a fundamental rethinking of network security architecture. The rapid proliferation of connected medical devices, expansion of care delivery through telehealth, and sophistication of ransomware attacks have exposed critical limitations in traditional network segmentation approaches.

The statistics are sobering: 67% of healthcare organizations experienced ransomware attacks in 2024, up from 60% the previous year, with healthcare having the second-highest attack rate globally, according to the HIPAA Journal's 2024 report "Healthcare Ransomware Attacks Continue to Increase in Number and Severity." Average breach costs have reached $10.93 million per incident—the highest of any industry—while recovery times extend to 291 days on average, according to IBM's Cost of a Data Breach Report 2024. More troubling, 37% of healthcare organizations now take over a month to recover from attacks, compared to just 22% recovering in less than a week.

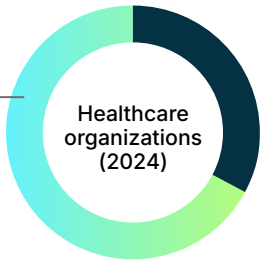
The proposed 2025 HIPAA Security Rule represents the first major overhaul in over a decade, elevating network segmentation from an "addressable" specification to a mandatory requirement. Meanwhile, cyber insurance premiums have increased 200-300% since 2020, with many insurers now requiring specific microsegmentation controls for coverage.

Modern microsegmentation offers a path forward, enabling healthcare organizations to create granular security boundaries that protect patient data and critical systems without impeding clinical workflows. Leading healthcare systems report 76% reduction in total cost of ownership, 95% faster implementation times, and 90% reduction in potential breach impact through identity-based microsegmentation approaches.

The Current Landscape:

67%

of healthcare organizations were hit by ransomware



$10.93 million

the average cost of a breach (per incident)

37%

of organizations breached take over a month to recover from attacks

With Modern Microsegmentation:

90%

reduction in potential breach impact

76%

reduction in total cost of ownership

95%

faster implementation times

The Expanding Attack Surface: Beyond Perimeter Defense

Healthcare networks have evolved into complex ecosystems that bear little resemblance to traditional corporate IT environments. A typical 300-bed hospital now manages between 10,000 and 25,000 network-connected devices, with 50-70% being specialized medical equipment that cannot support traditional security agents.

The Medical Device Explosion

These devices range from infusion pumps delivering critical medications to MRI machines generating diagnostic images. Each represents a potential entry point for attackers, yet many run embedded operating systems that cannot be patched without lengthy FDA recertification processes. Unlike traditional IT systems that might be refreshed every 3-5 years, medical devices often operate for 10-15 years or longer, creating permanent vulnerabilities in the network.

The convergence of Information Technology (IT) and Operational Technology (OT) systems creates additional vulnerabilities. Medical devices communicate using hundreds of different protocols, many proprietary to specific manufacturers. Traditional security tools struggle to understand and protect these communications.

The Human Factor and Resource Constraints

Healthcare's workforce presents unique security challenges. As noted by the CDW Healthcare IT Security Survey 2024, just 14% of healthcare organizations say their IT security teams are fully staffed. Over half need more help, and 30% are understaffed or severely understaffed. Clinical staff, focused primarily on patient care, often lack cybersecurity awareness. The high-stress healthcare environment creates pressure to bypass security controls when they impede patient care.

Lateral Movement: The Critical Threat Vector

With over 70% of successful breaches leveraging lateral movement techniques according to various cybersecurity industry reports, the ability to move sideways through a network after gaining initial access takes on particularly dangerous dimensions in healthcare settings. Consider how lateral movement unfolds in a typical healthcare breach: an attacker might initially compromise a single workstation through phishing, then move laterally to discover an imaging workstation connected to the radiology PACS system, eventually reaching the EMR, pharmacy systems, and life-critical devices.

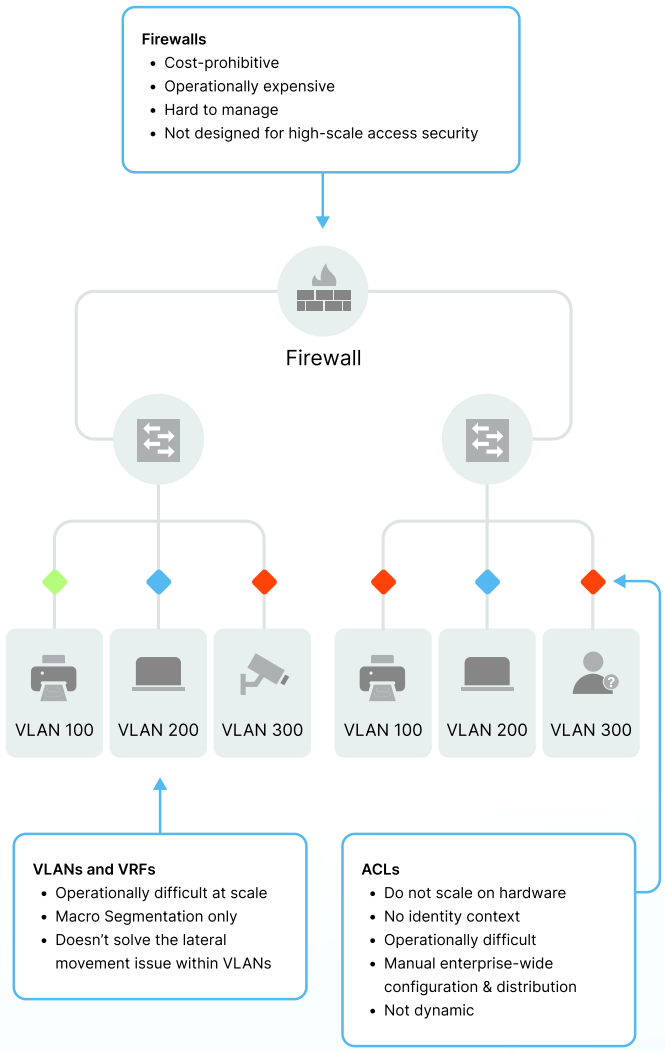
The ransomware attack at a major health system in May 2024, exemplifies this progression. Investigators identified the initial access vector as a malicious file downloaded by an employee, which gave attackers access to the user's device. From there, they moved laterally to compromise 7 of the health system's 25,000 servers, ultimately affecting patient care across 142 hospitals.

Why Traditional Segmentation Falls Short

Most healthcare networks were built on technologies designed for simpler threat landscapes. VLANs, firewalls, and Network Access Control (NAC) systems all serve important purposes, but create fundamental mismatches with how modern healthcare actually functions.

Problems with Traditional Segmentation

Traditional segmentation methods lack identity and context awareness. With no dynamic asset classification or policy enforcement, its configurations are brittle and error-prone. Maintaining a traditional segmentation method is cost-prohibitive, operationally expensive, and requires a complex network architecture.



The VLAN Sprawl Problem

Virtual Local Area Networks became the go-to solution for network segmentation because they offered seemingly straightforward traffic separation. However, healthcare operations quickly complicated clean designs. Each new medical device presents an impossible choice: place it in an existing VLAN where it doesn't quite fit, or create a new VLAN specifically for this device type.

A hospital that started with 10 well-planned VLANs might find itself managing 4,000 or more. Each VLAN requires configuration, documentation, and ongoing maintenance, with complexity growing exponentially. More critically, VLANs are tied to network topology—they care about where a device connects, not what it is or who's using it.

NAC Implementation Realities

Network Access Control systems promised to solve many challenges by making access decisions based on device and user identity. In practice, NAC implementations in healthcare face overwhelming complexity. Many medical devices can't run NAC agents or respond to NAC queries in expected ways. An infusion pump might appear as an unknown device, leading to denied access or assignment to a quarantine network where it can't reach needed systems.

One major health system reported that implementing Cisco ISE would require 14 additional full-time employees and 300 hours per site to deploy microsegmentation. The project would also require re-IP addressing for significant numbers of IoMT assets, many requiring on-site visits from multiple third-party vendors—making the project cost-prohibitive and operationally disruptive.

The Firewall Bottleneck

Traditional firewalls excel at perimeter defense but struggle with healthcare's real security challenges. They see only traffic crossing their boundaries, missing the vast amount of east-west communication within network segments. When an attacker compromises a workstation and begins exploring connected systems within the same VLAN, perimeter firewalls remain blind to the threat.

Attempts to address this with internal firewalls create operational nightmares. Every new clinical integration requires firewall rule updates. A large hospital might maintain tens of thousands of rules, many obsolete or conflicting, creating both security gaps and operational friction.

The Defense-in-Depth Gap: Why Existing Tools Leave Healthcare Vulnerable

Healthcare organizations typically deploy multiple security technologies, each addressing specific aspects of the threat landscape. While these tools provide valuable protection, they collectively leave a critical gap: unmanaged devices that cannot support traditional security agents.

Network Detection and Response (NDR)
Visibility Without Control

Network Detection and Response systems monitor network traffic patterns, establish baselines of normal behavior, and alert on anomalies that might indicate an attack. In healthcare, NDR might notice unusual data transfers from medical records systems or detect scanning behavior consistent with ransomware reconnaissance. However, NDR alone doesn't prevent attacks—it's a detection system, not a prevention system. By the time NDR alerts on suspicious lateral movement, attackers have already compromised multiple systems. More critically, NDR struggles with the vast ecosystem of medical devices that communicate using proprietary protocols and exhibit irregular behavior patterns that trigger false positives.

Zero Trust Network Access (ZTNA)
Limited to User-Application Scenarios

ZTNA solutions create encrypted connections between users and specific applications, verifying every access request regardless of location. This works well for user-to-application scenarios—doctors accessing patient records from home or administrators reaching billing systems remotely. However, ZTNA fails to address healthcare's core challenge: medical devices don't browse to applications through authentication portals. An MRI scanner can't authenticate through a ZTNA portal before sending images to the PACS system. Patient monitors need constant connectivity to multiple systems, not individually brokered connections. While ZTNA excels at securing remote user access, it doesn't address the fundamental challenge of east-west traffic between systems within healthcare facilities.

Endpoint Detection and Response (EDR)
Agent Dependency Limitations

EDR platforms like CrowdStrike and SentinelOne provide excellent visibility and protection for traditional endpoints—workstations, servers, and laptops that can run security agents. These tools detect malware, monitor process behavior, and enable rapid incident response. The limitation becomes apparent with medical devices. That critical infusion pump delivering medications can't run a CrowdStrike agent. The MRI scanner's embedded system won't support SentinelOne. Building automation systems, surgical robots, and thousands of other IoT/OT devices remain invisible to EDR platforms, creating blind spots that attackers exploit.

The Coverage Gap Reality

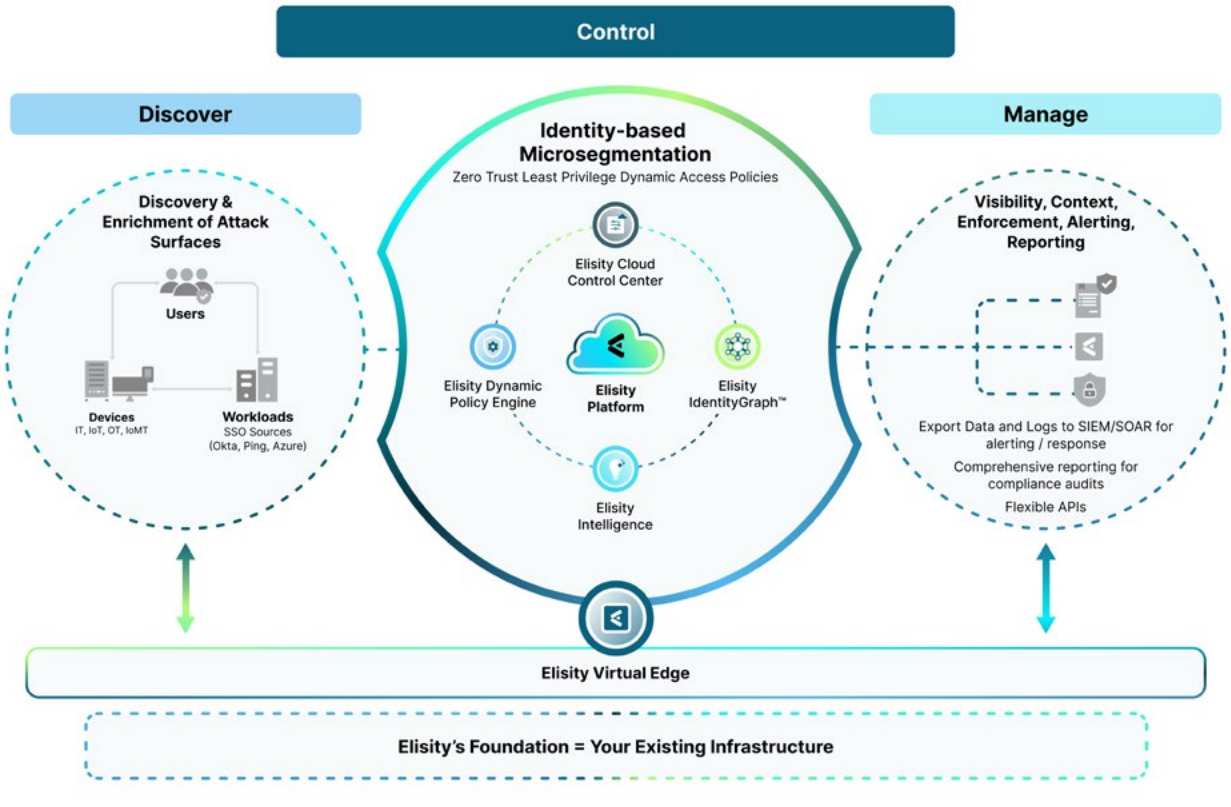
A typical healthcare organization might achieve 90% visibility and control over traditional IT assets through their layered security stack. Firewalls protect perimeters, EDR monitors managed endpoints, ZTNA secures remote access, and NDR provides network visibility. This seems comprehensive until you realize that the remaining 10%—those unmanaged medical devices, building systems, and IoT sensors—often represents 50-70% of connected devices in healthcare environments. This coverage gap isn't theoretical. The Change Healthcare attack that affected 100 million records began with the compromise of poorly segmented systems. Healthcare-specific breaches consistently involve lateral movement through networks where traditional security tools lack visibility and control over the very devices that make modern healthcare possible.

Modern vs. Legacy Microsegmentation

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

The Modern Microsegmentation Solution

Identity-based microsegmentation represents a fundamental shift from infrastructure-centric to identity-driven security. Instead of caring about which VLAN a device joins or which firewall rules apply to an IP address, modern solutions focus on what a device is, who's using it, and what it needs to do.



The Elisity Approach
Discover, Control, Manage

Elisity is a leap forward in network segmentation architecture, designed to be implemented in days without downtime. The platform rapidly discovers every user, workload, and device on an enterprise network and correlates comprehensive insights into the Elisity IdentityGraph™. This empowers teams with the context needed to automate classification and apply dynamic security policies to any device wherever and whenever it appears on the network.

The solution operates through three core functions:

Discover: Elisity provides continuous visibility into every user, workload, and device, identifying and mapping risks in real-time. By ingesting metadata from existing network infrastructure and integrating with existing tech stacks, Elisity correlates identity, configuration, risk scores, and detailed device data. Teams gain actionable context and deep visibility of all assets in real-time, even unmanaged and ephemeral IT/IoT/OT/IoMT devices.

Control: Elisity's policy-creation engine dynamically manages and enforces security and access policies quickly and without risk. The Elisity Cloud Control Center enables teams to create, simulate, and apply smart, automated dynamic security policies that persist for every device, wherever and whenever a device appears on networks. This makes it easy to apply least privilege access for users, workloads, and devices.

Manage: Elisity's cloud-delivered policy management control plane quickly connects to existing networks. Having this capability abstracted from network infrastructure means no additional firewalls, VLANs, ACLs, or agents to install, configure, and update. Unlike legacy solutions, policies aren't tied to IP addresses or brittle network constructs.

Modern Microsegmentation Facts

Ideal Timeline

Most organizations[1] follow a phased implementation of Modern Microsegmentation

Phase 1 — **Setup**
A few days

Phase 2 — **Discovery & Planning**
2–6 weeks

Phase 3 — **Initial Deployment & Policy Development**
4–25 weeks
Depending on the vendor and architecture selected

Phase 4 — **Production Rollout**
Weeks-months
The goal should be to get a few simple policies active in the first two weeks

Phase 5 — **Optimization & Expansion**
On-going

Consider starting with critical applications or specific segments to demonstrate value and refine processes before broader deployment. Cloud-based solutions typically enable faster implementation through automated discovery and policy recommendation engines.

1: Example based on the average Elisity customer.

Real-World Implementation Success

At Main Line Health, the contrast with traditional approaches proved stark. Their previous plan using a legacy platform would have required 14 employees and 300 hours per site. With Elisity, they achieved comprehensive microsegmentation across their entire health system—5 hospitals, 6 health centers, and over 40 offices—with just two full-time employees. Implementation time dropped from months to days, with most sites coming online within 2-8 hours. **The results were transformational:**

99%

of devices discovered and classified within 4 hours without network disruption

76% TCO reduction

Total forecasted spending decreased from $38 million to $9 million

Compliance ensured

Automated policies ensured compliance with NIST, HIPAA, and HHS 405(d) requirements

---

"Elisity's identity-based micro-segmentation 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."

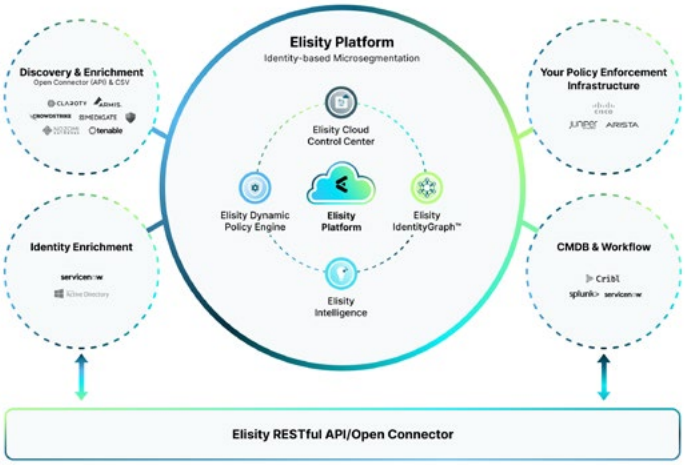
Aaron Weismann, CISO, Main Line Health

Main Line Health®

Key Capabilities Transforming Healthcare Security

Comprehensive Asset Discovery

Modern microsegmentation platforms approach discovery from multiple angles simultaneously. Rather than relying on a single mechanism, they combine passive observation of network traffic, active integration with CPS (Cyber-physical systems), existing CMDB systems, and specialized connectors for healthcare-specific platforms.



The platform observes network communications to identify devices based on behavior patterns. An infusion pump has distinctive communication patterns—periodic status updates to medication management systems, regular heartbeats to monitoring stations, and specific protocols for drug library updates. By understanding these patterns, the platform can identify device types even when traditional discovery methods fail.

Risk-Adaptive Security Posture

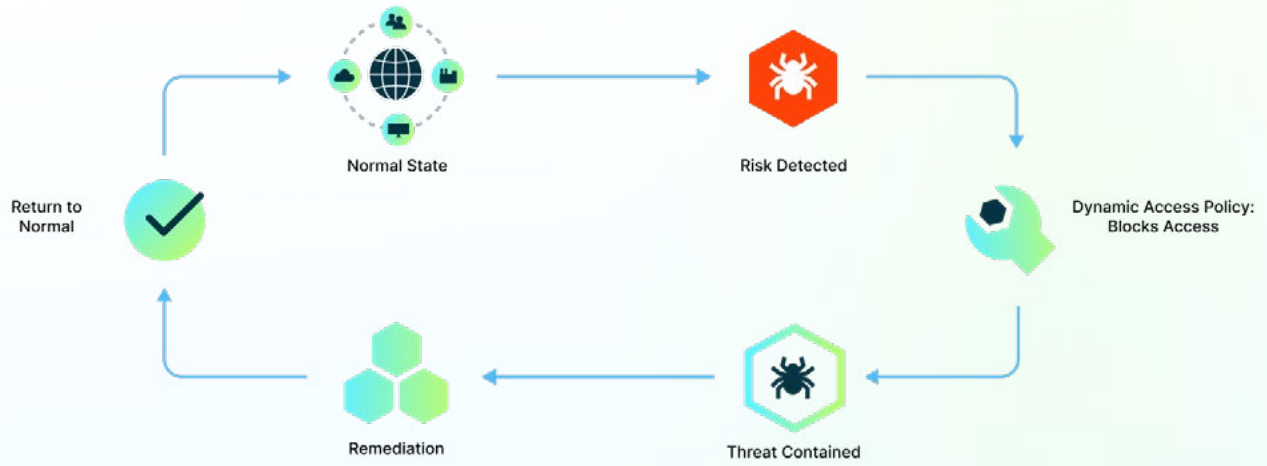
Traditional security operates on a binary model—access is either permitted or denied based on predefined rules. Modern microsegmentation implements continuous risk assessment that evaluates every device, user, and communication pattern in real-time. By integrating with endpoint detection and response (EDR) platforms, and CPS platforms like Armis and Claroty, the platform maintains current risk scores for every entity on the network.

When CrowdStrike detects suspicious activity on a workstation, traditional approaches require manual intervention to isolate the device. With risk-adaptive microsegmentation, policies automatically tighten the moment the risk score increases, containing threats in seconds rather than hours.

Automated Compliance and Continuous Validation

Healthcare organizations face an increasingly complex regulatory landscape. A modern platform automatically maps every policy, change, and access decision is logged with full context—who requested it, why it was needed, when it was implemented, and what controls ensure security. Auditors receive comprehensive reports showing not just current state but historical compliance over any time period.

Risk Adaptation Flowchart



The Business Case for Modern Microsegmentation

"Elisity has changed how we look at microsegmentation solutions overall and we have now experienced how Elisity is the easiest to implement and easiest to manage."

Aaron Weismann, CISO

Main Line Health®

6000+
Actively enforced policies

+100k
IoT, OT, and IoMT devices protected

150
Hospitals, health centers and physicians' practices

3
Days to deploy

Financial Impact

The most immediate financial impact comes from infrastructure and operational efficiency. Some sample ROI data points from customers include a 76% total cost reduction compared to traditional approaches. These savings stem from:

- **Reduced infrastructure requirements**
  (no new hardware, firewall sprawl, or VLAN redesign)
- **Lower staffing needs**
  (2 FTEs versus 14 FTEs required for legacy approaches)
- **Faster deployment**
  (weeks instead of years means faster risk reduction and lower project costs)
- **Simplified operations**
  (automated policy management reduces ongoing burden)

Risk Reduction Quantification

With healthcare organizations experiencing 181 confirmed ransomware attacks in 2024 involving 25.6 million healthcare records, and average ransom demands of $5.7 million according to the HIPAA Journal's report "2024 Was Another Bad Year for Healthcare Ransomware Attacks," risk reduction becomes tangible rather than theoretical. Modern microsegmentation reduces risk through:

- **Blast radius reduction**
  (GSK a large pharmaceutical company, another Elisity customer, achieved 95% reduction in potential attack spread)
- **Faster containment**
  (Main Line Health reduced mean-time-to-contain from 4-6 hours to under 10 minutes)
- **Attack surface minimization**
  (eliminating unnecessary communications reduces entry points by 70-90%)

Insurance and Compliance Benefits

Cyber insurance has become both more expensive and more difficult to obtain for healthcare organizations. Insurers now require specific security controls, with microsegmentation increasingly appearing as mandatory requirements. Organizations implementing comprehensive microsegmentation report 15-30% premium reductions and higher coverage limits.

For the proposed 2025 HIPAA Security Rule requirements, organizations with modern microsegmentation find themselves already compliant. The mandate for network segmentation, asset inventory, and network mapping represents current state rather than a future project.

Taking Action: Your Path Forward

The window for proactive security transformation is narrowing. With 67% of healthcare organizations experiencing ransomware attacks according to the HIPAA Journal and regulatory requirements tightening, the question isn't whether microsegmentation is necessary—it's whether you'll lead transformation or react to crisis.

Immediate Steps

1

Assess

Assess Your Current State: Document existing segmentation approaches, costs, and gaps. Include current security spending, compliance costs, operational inefficiencies, and risk exposure.

2

Engage

Engage with Proven Solutions: Schedule demonstrations with healthcare-focused micro-segmentation vendors. Demand to see real healthcare deployments, not generic demos. Request proof-of-concept in your environment with your actual devices and workflows.

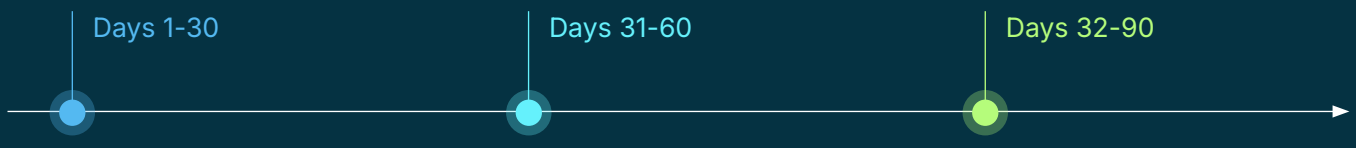
3

Build

Build Your Coalition: Form a micro-segmentation steering committee including IT, security, clinical, and finance leaders. Secure executive sponsorship and communicate the vision across the organization.

The 90-Day Transformation Timeline

Modern microsegmentation can be implemented in weeks with platforms like Elisity following a proven path:



Foundation & Discovery
Deploy infrastructure, integrate systems, begin comprehensive device discovery

Learning & Policy Development
Analyze communication patterns, create policies, run simulations

Enforcement & Expansion
Activate policies progressively, scale to additional sites, establish operational procedures

Conclusion: Security as a Strategic Enabler

Healthcare security professionals carry a unique responsibility. Unlike other industries where breaches mean financial loss, healthcare breaches can disrupt patient care and endanger lives. Modern microsegmentation enables you to fulfill this responsibility by implementing comprehensive, identity-based security that adapts to healthcare's unique requirements.

76%
cost reduction
(over legacy architectures)

95%
faster
implementations

90%
smaller blast radius
for attacks

The technology exists. The path is proven. Leading healthcare organizations have benefited from modern platforms like Elisity with a 76% cost reduction (over legacy architectures), 95% faster implementations, and 90% smaller blast radius for attacks. Most importantly, they've transformed security from a source of friction between users, IT, and security into an enabler of clinical excellence.

> **Leading healthcare organizations have benefited from modern platforms like Elisity**

The choice is clear: continue accepting the limitations of traditional security, or join the healthcare leaders who've transformed their security posture, protected their patients, and positioned their organizations for the future. In healthcare, security isn't just about protecting data—it's about protecting lives.

Ready to Transform Your Healthcare Network Security?

BOOK A DEMO

ELISITY

Schedule your personalized microsegmentation assessment with Elisity today. See how identity-based microsegmentation can transform your security posture in weeks, not years. Visit **elisity.com/demo-request** to begin your journey. Because in healthcare, security isn't just about protecting data—it's about protecting lives.