ELISITY

Gartner COOL VENDOR 2025

BUYER'S GUIDE

Microsegmentation for Healthcare Institutions

Microsegmentation for Healthcare Institutions

Identity-based microsegmentation enables healthcare organizations to rapidly secure complex networks by applying granular, context-aware policies that protect sensitive patient data and medical devices. By automatically controlling access across IT, IoT, and IoMT environments, healthcare providers can prevent lateral movement attacks and maintain patient safety without extensive infrastructure changes.

Executive Summary: The Critical Need for Modern Microsegmentation

In today's healthcare cybersecurity landscape, cybercriminals increasingly leverage lateral movement to amplify attacks after gaining initial access. The expanded attack surface from IoMT devices, electronic health records, and interconnected medical systems creates numerous potential entry points. These connected devices often run legacy software or protocols that can't be properly secured with traditional tools. According to recent data, 60% of successful breaches now involve lateral movement, with attackers potentially compromising patient care systems for an average of 280 days before detection.

Market Context and Infrastructure Challenges

Legacy segmentation approaches rely heavily on complex VLAN architectures, firewall rules, and endpoint agents. This creates significant operational overhead and leaves gaps in coverage where agents can't be deployed, particularly in sensitive healthcare environments. With cybersecurity budgets under pressure and healthcare organizations seeking more efficient solutions, traditional platforms often require specialized expertise and constant maintenance while providing incomplete protection.

Business Drivers and Regulatory Requirements

While EDR platforms excel at endpoint protection, they cannot effectively control east-west network traffic that enables ransomware spread. Key healthcare regulations like HIPAA, HHS 405(d), and emerging cybersecurity standards now specifically mandate comprehensive network segmentation. Healthcare organizations must demonstrate granular access controls and traffic isolation to protect patient data and maintain operational resilience.

Building the Business Case for Microsegmentation

For healthcare organizations, microsegmentation's ability to isolate critical systems provides immense value by preventing costly operational disruptions. Hospitals and health systems report significant potential savings by avoiding system downtime through improved segmentation. The technology's ability to contain breaches and limit lateral movement directly addresses the primary attack vector used in today's most damaging incidents.

When building the business case, healthcare leaders should consider both hard cost savings from operational improvements and risk reduction benefits from enhanced security controls. The comprehensive value proposition spans patient safety, IT operations, incident response, and compliance.

Incident Response & Remediation in Healthcare Cybersecurity

The financial impact of security breaches in healthcare continues to escalate dramatically. The 2024 Cost of a Data Breach Report highlights that healthcare breaches not only incur significant financial costs but also directly impact patient safety and care continuity. With the average breach cost reaching $5.2 million in healthcare settings, organizations face critical challenges in protecting sensitive patient information and maintaining operational resilience.

Regulatory Compliance Drivers

Healthcare-specific regulations like the HIPAA Security Rule and HHS 405(d) are mandating robust network security and incident response capabilities, making network segmentation implementations a critical requirement for protecting patient data and medical systems. These regulatory frameworks specifically require healthcare organizations to demonstrate granular access controls, traffic isolation, and the ability to rapidly contain security incidents - all core capabilities that modern microsegmentation solutions deliver without the complexity of traditional segmentation approaches.

Research demonstrates micro-segmentation delivers substantial value for healthcare cybersecurity

- **reduced incident response costs** (40%–60% decrease in investigation time),
- **improved operational efficiency** (60%–80% reduction in policy management overhead),
- **strengthened compliance posture** (50% less audit preparation time),
- **lower cyber insurance premiums** (15%–25% reduction from major carriers).

The Evolution of Network Segmentation: From Perimeter Defense to Zero Trust Microsegmentation

Network segmentation has evolved dramatically over the past two decades, shifting from simple perimeter-based controls to sophisticated identity-aware microsegmentation. This evolution reflects fundamental changes in healthcare enterprise architecture and the cybersecurity threat landscape.

Early Segmentation
(2000–2010)

Initially, healthcare organizations relied primarily on firewalls and VLANs to create broad network segments, focusing on north-south traffic. Network Access Control (NAC) and 802.1x added endpoint authentication but operated at a relatively coarse network level. This approach worked when medical applications were monolithic and hosted in on-premises data centers behind clear perimeters.

The Cloud Transition
(2010–2015)

As healthcare began adopting cloud services and virtualization, traditional perimeter-based segmentation proved inadequate. The rise of east-west traffic within data centers and cloud environments created new security challenges. Early Software-Defined Networking (SDN) solutions attempted to address this but often required complex network redesigns.

Modern Microsegmentation
(2015–Present)

Today's microsegmentation solutions reflect the Zero Trust principle that no traffic should be trusted by default. Modern approaches focus on user identity rather than network location, enabling fine-grained control of communication between individual users, workloads, and devices in healthcare environments.

Microsegmentation provides healthcare organizations with a critical tool set to

- rapidly isolate compromised systems,
- prevent lateral movement of potential threats,
- maintain continuous patient care during security incidents,
- provide detailed forensic tracking and investigation capabilities.

By implementing advanced microsegmentation strategies, healthcare security teams can transform incident response from a reactive to a proactive approach, ultimately protecting patient data and maintaining the critical mission of healthcare delivery.

Key technological advances include

- identity-based policies that follow workloads across environments,
- automated device discovery and classification,
- dependency mapping and automated policy recommendations,
- integration with existing security stacks and metadata providers.

Current Market Landscape

The microsegmentation market has evolved to support multiple deployment models:

- **Host-based:** Uses software agents on workloads.
- **Network-based:** Leverages existing network infrastructure.
- **Software-based:** Through SDN or overlay networks.
- **Cloud-native:** Utilizes built-in cloud provider controls.
- **API-based:** Orchestrates policies across multiple enforcement points.

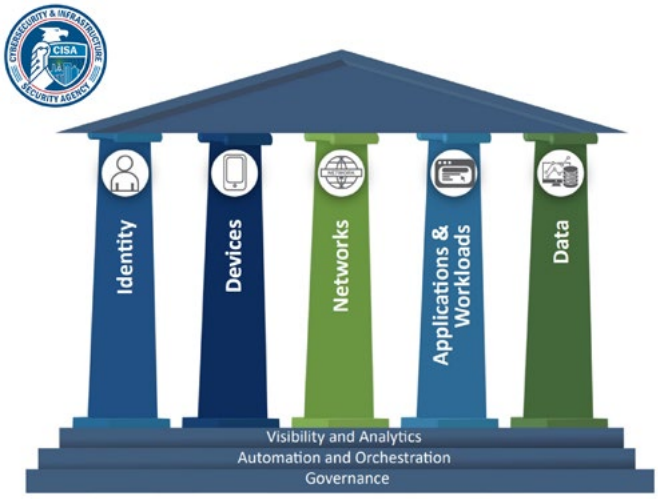
Healthcare-specific microsegmentation needs:

- Protecting sensitive patient data and IoMT medical devices.
- Maintaining high availability of critical care systems.
- Securing electronic health records.
- Ensuring compliance with HIPAA and other healthcare regulations.
- Preventing unauthorized access to patient information.
- Supporting complex, interconnected healthcare ecosystems.

Current Trends in Healthcare Microsegmentation

The market is being shaped by several factors:

- Zero Trust initiatives driving healthcare cybersecurity adoption.
- Ransomware threats highlighting the need to limit lateral movement.
- Hybrid cloud architectures requiring consistent security across complex healthcare environments.
- Increasing complexity of medical device connectivity and IoMT ecosystems.



Zero Trust Model Maturity Pillars

Critical Capabilities for Healthcare Organizations:

- Close attack surface gaps in medical networks.
- Provide unified visibility across hybrid healthcare environments.
- Automate policy creation and management for sensitive patient data.
- Integrate with existing healthcare IT security tools.
- Support both traditional and cloud-native medical workloads.
- Meet HIPAA, HHS 405(d), and other healthcare compliance requirements.
- Lower cyber insurance premiums.

The future of microsegmentation in healthcare points toward greater automation and AI-driven policy optimization. As healthcare organizations continue digital transformation, microsegmentation has become a critical component of modern patient safety and data protection strategies.

Key Success Factors for Selecting the Right Solution

1. **Deployment Model Alignment**
   Choose between agent-based and agentless approaches specifically designed for healthcare environments. Consider long-term maintenance costs and coverage requirements for medical devices, IoMT systems, and complex clinical networks that cannot support traditional agents.

2. **Integration Capabilities**
   Ensure seamless integration with healthcare-specific security infrastructure, including Identity and Access Management (IAM), SIEM, SOAR, and medical device security platforms. API support for automation is crucial for operational efficiency and patient safety.

3. **Total Cost of Ownership**
   Evaluate costs over a 3–5 year period, including implementation, ongoing operations, and staffing requirements. Modern solutions may have higher upfront costs but deliver better long-term value by reducing operational complexity and enhancing patient data protection.

4. **Vendor Expertise**
   Select vendors with proven experience in your industry vertical and a strong track record of supporting similar deployments. Validate through customer references and proof-of-concept testing.

When you are ready to enhance your healthcare cybersecurity with state-of-the-art microsegmentation, schedule a call or demo with Elisity to learn how our solutions enable healthcare organizations to ensure patient data protection and maintain operational excellence.

Key Features and Capabilities for Healthcare Microsegmentation Solutions

Understanding the essential features and capabilities is crucial for selecting a microsegmentation solution that will effectively reduce attack surfaces and prevent lateral movement in complex healthcare environments. These requirements ensure the solution can scale across hybrid networks while maintaining patient data security and operational efficiency.

When evaluating these requirements, organizations should consider their current environment, future growth plans, and operational capabilities. The chosen solution must balance security needs with operational efficiency while providing the flexibility to adapt to changing infrastructure and threats. Attention should be given to the solution's ability to handle specialized environments like IoT, OT, IoMT networks, which often require unique protocols and security considerations.

Success with microsegmentation depends heavily on choosing a solution that not only meets these technical requirements but also aligns with your organization's security maturity and operational capabilities. Consider starting with critical applications and expanding coverage as your team gains experience with the chosen solution.

Success depends on choosing a solution that:

- Meets technical requirements
- Aligns with healthcare security maturity
- Protects patient data
- Maintains high system availability
- Supports complex clinical workflows

Recommended Approach

Start with critical systems like patient records and specialized medical devices, then expand coverage systematically.

☑ Core Functionality Requirements:

- **Comprehensive Visibility and Discovery**
  - Map all medical devices, IoMT systems, and network assets
  - Identify communication flows across clinical environments
- **Granular Policy Creation and Management**
  - Define precise access controls for sensitive patient information
  - Automated policy recommendations based on clinical workflows
- **Robust Policy Enforcement**
  - Validate security policies across healthcare networks
  - Ensure compliance with HIPAA and HHS 405(d) guidelines

☑ Technical Requirements:

- **Network-Based Controls**
  - Leverage existing healthcare IT infrastructure
  - Extend beyond traditional IP-based segmentation
- **Identity and Metadata-Driven Segmentation**
  - Integrate with healthcare-specific identity providers
  - Support complex user roles (physicians, nurses, contractors)

☑ Must-Have Capabilities:

- **Automatic Asset Discovery and Classification**
  - Identify medical devices, IoMT systems, IoT devices, HVAC devices clinical workstations
- **Policy Simulation**
  - Test policy changes without disrupting patient care
- **Real-Time Flow Monitoring**
  - Track east-west traffic in clinical networks
- **Risk-Based Automated Segmentation**
  - Dynamically adjust policies based on device risk scores

☑ Integration Requirements:

Seamless connections with:

- Electronic Health Record (EHR) systems
- Identity and Access Management platforms
- Security monitoring tools
- Medical device management systems

☑ Deployment Options:

- **Agentless deployment** (preferred for medical environments)
- **Support for legacy medical systems**
- **Minimal operational disruption**
- **Compatibility with diverse medical device protocols**

Vendor Selection Process

"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®

"Elisity provides technical distancing between devices to stop cyberattack progression while preserving safe and effective technology-supported care continuity."

Watch the Case Study Interview Here →

Or visit:
elisity.com/resources/videos/main-line-health

Setting a Strategic Foundation

When selecting a microsegmentation solution, organizations should begin by establishing clear business objectives and technical requirements specific to their healthcare, manufacturing, or other industry environments. The complexity of these environments, particularly with medical devices, industrial systems, and legacy equipment, demands thorough proof-of-concept testing using actual devices and protocols. Success hinges on choosing vendors with demonstrated expertise in your vertical industry and a proven track record of supporting similar deployments.

Evaluating Vendor Strength and Capability

Vendor evaluation should focus on both technical capabilities and business viability. Look for vendors offering flexible deployment options (on-premises, cloud, hybrid) and seamless integration with existing security software and infrastructure.
The vendor's financial stability and long-term market presence are crucial, as implementing microsegmentation is a strategic investment. Evaluate their support structure, ensuring 24/7 availability and comprehensive professional services that align with your operational needs. Speak with analysts or read and understand what Gartner or Forrester are saying about the category and vendors.

Technical Differentiators

Key technical differentiators between vendors may include the breadth of supported industrial protocols, the accuracy of asset discovery, and sophistication of policy management capabilities. Superior solutions offer robust visualization tools, automated policy recommendations, and integration with broader security platforms. Industry-specific threat intelligence and domain expertise should inform the solution's approach to protecting critical assets.

Risk Indicators and Warning Signs

Several red flags warrant careful consideration during evaluation. Be wary of vendors with limited experience in your industry, unclear product roadmaps, dependencies with legacy systems, or heavy reliance on professional services for basic functionality. Complex pricing models or poor technical support responsiveness often indicate potential implementation challenges. Limited integration capabilities may hinder long-term value realization.

Reference Validation Process

Reference customer validation is essential for understanding real-world implementation experiences. Focus on organizations of similar size and complexity in your industry, particularly those with comparable regulatory requirements and operational constraints. Through reference discussions, assess the total cost of ownership, including hidden costs, ongoing support quality, and operational impact. Pay special attention to the vendor's incident response capabilities and their ability to support business continuity requirements in crisis situations.

Business Value and Benefits Evaluation Criteria for Healthcare Organizations Financial impact

Modern microsegmentation solutions deliver substantial ROI specifically tailored to healthcare environments. Healthcare organizations see cyber insurance premium reductions of 15%–30% due to improved breach containment capabilities and documented security controls for sensitive patient data. Automated policy management typically reduces operational costs by 60%–80%, while incident response times in clinical settings drop by 40%–60%. Organizations generally achieve positive ROI within 12–18 months through direct cost savings and enhanced patient safety.

15%–30%
reduction in cyber insurance premiums

40%–60%
decrease in incident response times

60%–80%
reduction in operational costs

70%–90%
reduction in vulnerable attack paths

This comprehensive approach makes microsegmentation a core security investment for modern healthcare, supporting patient safety, operational efficiency, and compliance.

Risk Reduction in Healthcare

The primary business value of microsegmentation comes from dramatically reduced breach impact in critical healthcare systems. By limiting lateral movement, healthcare organizations can significantly protect electronic Protected Health Information (ePHI) and prevent ransomware spread across medical networks. This approach reduces potential breach costs by 45% and minimizes risks to patient care delivery. The technology effectively reduces vulnerable attack paths by 70%–90%, creating a robust defense mechanism that prevents unauthorized access to medical devices and patient records.

Operational Efficiency in Clinical Environments

Microsegmentation transforms healthcare security operations by fundamentally changing how medical networks are managed and secured. It dramatically reduces change management cycles from weeks to hours, enabling real-time visibility into medical device communications. Healthcare IT teams can now focus more on supporting patient care technology rather than managing complex security configurations. The solution simplifies compliance with HIPAA and HHS security requirements while providing unprecedented control over network access and device interactions.

Compliance Benefits

Healthcare-specific microsegmentation solutions streamline compliance through automated policy enforcement and comprehensive reporting mechanisms. These solutions provide built-in reporting capabilities specifically designed for HIPAA Security Rule requirements, generating detailed activity logs that meet HHS 405(d) compliance standards. By reducing audit preparation time and costs, and ensuring consistent security controls across clinical environments, microsegmentation becomes an essential tool for healthcare organizations navigating complex regulatory landscapes.

Long-Term Strategic Value for Healthcare

Beyond immediate financial and operational benefits, microsegmentation provides lasting strategic advantages for healthcare delivery organizations. It supports improved medical technology deployment, enhances protection of patient data, and simplifies cloud migration for healthcare systems. By reducing technical debt in legacy medical IT infrastructure, the solution directly supports digital transformation efforts in healthcare delivery. The comprehensive protection of sensitive medical information becomes a strategic asset, enabling organizations to innovate while maintaining the highest standards of data security.

Implementation Considerations for Microsegmentation

Integration Architecture for Healthcare Cybersecurity

Modern microsegmentation in healthcare requires seamless integration with complex IT systems that protect patient data and medical workflows. Identity management integration with healthcare-specific IAM solutions provides robust user and workload authentication across clinical environments. Integration with security platforms like SIEM, SOAR, and EDR enables coordinated threat detection and response that maintains patient safety and data integrity. Specialized integration with CAASM and CPS platforms offers comprehensive asset visibility and risk management across IT and medical device networks. RESTful APIs enable automation through CI/CD pipelines and DevOps workflows tailored to healthcare ecosystems. CMDB and ITSM integration ensures accurate tracking of medical devices, electronic health records, and critical healthcare infrastructure..

Deployment Approach for Medical Environment

Selecting the right deployment strategy is crucial in healthcare, where device diversity and patient care continuity are paramount. The choice between agent-based and agentless deployment significantly impacts implementation complexity and ongoing operations. While agent-based solutions provide granular control, they often struggle with the unique challenges of medical devices like IoMT systems, which cannot support traditional security agents. Modern agentless solutions leverage existing network infrastructure for enforcement, reducing operational overhead while maintaining effective segmentation across complex medical networks. Healthcare organizations must carefully consider the long-term costs of agent management, particularly in environments with high device turnover and diverse medical technology ecosystems.

OT/IoT Considerations in Healthcare

Healthcare environments demand specialized integration with medical device security platforms. Modern microsegmentation solutions support agentless monitoring of sensitive medical devices through network-based controls, eliminating the risks associated with traditional agent deployment on critical clinical systems. By integrating with specialized healthcare OT security platforms, organizations can ensure comprehensive visibility and protection without disrupting patient care operations or medical device functionality.

Resource Requirements Vary by Platform

Implementation typically requires a mix of security, networking, infrastructure and IT teams. A typical enterprise[1] deployment needs the following:

Ideal Resource Allocation

- **Project Manager**
  Full-time, 3–6 months
- **Security Architect**
  Part-time, ongoing
- **Network Engineer**
  Part-time, initial setup
- **Security Teams**
  Consultation during policy development

Ideal Timeline

Most organizations[2] follow a phased implementation:

- 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 & 2: Examples based on the average Elisity customer.

Case Study: Main Line Health — Accelerating Zero Trust with Identity-Based Microsegmentation

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

PREVIOUS PLAN

Implement traditional NAC/802.1x and firewall-based segmentation requiring additional staff, hardware, and 300+ hours per site with significant network disruption.

CHALLENGE

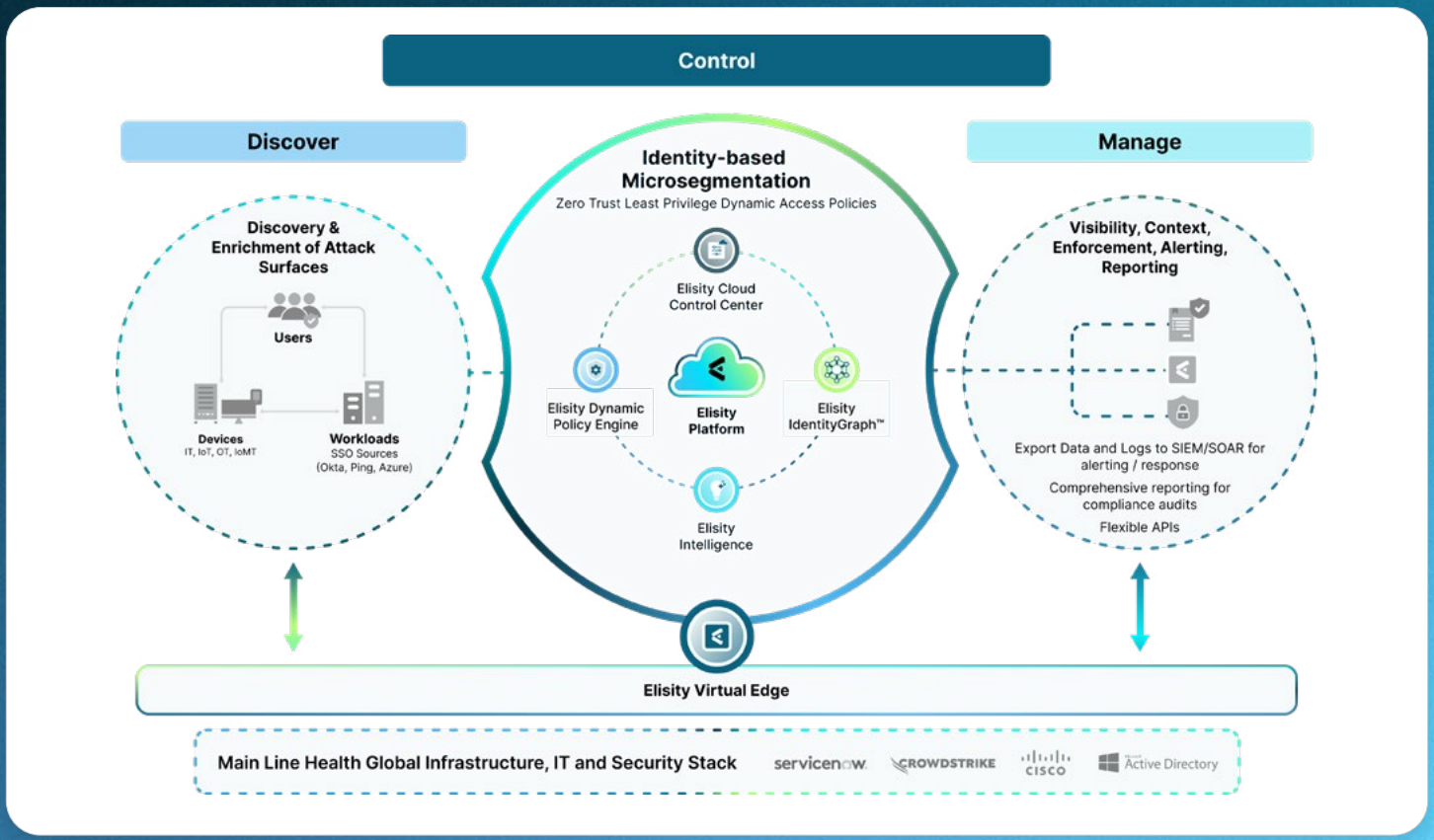
Main Line Health, serving Philadelphia with 4 hospitals, 145 health centers, and 13,000+ employees, faced critical security challenges. They needed HITRUST certification while securing FDA-regulated biomedical devices that couldn't be patched. Their board mandated network microsegmentation amid rising ransomware threats. Traditional solutions faced internal resistance and would take one year per location.

SOLUTION

Main Line Health implemented Elisity's identity-based microsegmentation platform across all facilities. Within hours of deployment, they achieved comprehensive visibility of their entire network. By integrating with their existing Armis deployment, Elisity's IdentityGraph™ correlated device metadata to create context-aware policies. The agentless solution leveraged their existing Cisco infrastructure, eliminating the need for network redesigns. The team cleverly used deployment downtime for tabletop exercises, training clinicians on paper-based processes—earning them CSO50 and CIO100 awards for innovation.

ROI

- Reduced deployment time from 300 hours to 2-8 hours per site.
- Achieved 99% device discovery within 4 hours without downtime.
- Created blocking rules within 24 hours of deployment.
- Eliminated need for 14 additional FTEs originally required.
- Accelerated HITRUST compliance with automated reporting.
- Strengthened disaster preparedness through integrated training.
- Board confidence in microsegmentation implementation achieved in months vs years.



Solution: Elisity Microsegmentation Platform

Pricing Models and Total Cost of Ownership for Microsegmentation

When evaluating microsegmentation solutions, organizations must look beyond initial licensing costs to understand the total cost of ownership across their security infrastructure. Traditional segmentation approaches using VLANs and firewalls may appear cost-effective at first glance, but they often mask significant operational expenses. These legacy solutions require specialized networking expertise, complex change management processes, and regular hardware refresh cycles. The manual effort required to maintain and update policies across multiple tools can quickly escalate staffing costs and increase the risk of costly misconfigurations. Legacy solutions require specialized networking expertise, complex change management processes, and regular hardware refresh cycles.

Legacy solutions require specialized networking expertise, complex change management processes, and regular hardware refresh cycles.

Modern cloud-based microsegmentation platforms typically follow a subscription pricing model that may seem more expensive initially. However, these solutions often deliver better long-term value through automated operations and reduced complexity. Their integrated approach combines visibility, policy discovery, and enforcement in a single platform, eliminating the need for multiple-point solutions. Agentless solutions require far less disruption for implementation and ongoing maintenance. Automated policy recommendations and simplified management interfaces reduce the reliance on specialized expertise, allowing organizations to operate effectively with smaller teams.

Staffing considerations play a crucial role in the total cost equation. Traditional approaches require multiple specialists, including network engineers, firewall administrators, and dedicated IoT, OT, IoMT security experts. Modern solutions reduce this burden through automation and intuitive interfaces that require less specialized training. This is particularly important for organizations managing industrial or healthcare environments, where security expertise is often scarce and expensive.

Implementation costs vary significantly between approaches. Traditional solutions often require substantial professional services for deployment, integration, and policy development. Cloud-based platforms typically offer faster deployment with built-in integration capabilities, though some professional services may still be needed for complex environments. Ongoing operational costs must also be considered, including agent updates, policy maintenance, compliance reporting, and incident response capabilities.

Organizations should evaluate TCO over a 3-5 year period, considering factors like cloud migration costs, multi-cloud management overhead, and compliance requirements. While modern solutions may require higher upfront investment, they often prove more cost-effective by reducing operational complexity, automating routine tasks, and providing enhanced security capabilities. The ability to start with critical workloads and expand gradually also allows organizations to manage costs while demonstrating value, making modern microsegmentation solutions an increasingly attractive option for organizations focused on long-term security and operational efficiency.

Selecting the Right Micro-segmentation Solution for Your Organization

Forrester Research recently stated in the Forrester Wave™: Microsegmentation Solutions, Q3 2024, "We're Living In The Golden Age Of Microsegmentation." This technology stands out as a crucial strategy for preventing lateral movement and minimizing the impact of east-west attacks, particularly in manufacturing and industrial environments.

The business case for micro-segmentation is compelling, with research showing $3.50 in value for every dollar invested. Organizations implementing comprehensive microsegmentation solutions report:

15%–30%
reduction in cyber insurance premiums

40%–60%
decrease in incident response times

60%–80%
reduction in policy management overhead

70%–90%
reduction in vulnerable attack paths

Key Questions to Ask Vendors

Visibility & Discovery in Healthcare Environments

Notes:

Why it matters: Complete visibility into medical devices, clinical users, and network assets is critical for protecting patient data and maintaining care continuity.

- How does your solution discover and map medical devices, clinical users, and IoMT systems across hybrid healthcare environments?
- What methods are used to identify and classify medical assets?
- What percentage of the healthcare attack surface can be comprehensively covered?
- How are ephemeral medical devices handled across hospitals, clinics, and patient home care settings?
- Can the solution identify unauthorized medical applications and shadow IT in clinical networks?
- What integrations exist with healthcare organization CMDBs and medical asset management systems?

Policy Management & Enforcement for Patient Safety

Notes:

Why it matters: Granular policy creation directly impacts patient data protection and clinical system security.

- How are policies created and validated specifically for healthcare compliance (HIPAA, HHS 405(d))?
- What granularity of control is available for medical device access?
- How flexible is policy creation across different clinical environments?
- How are policies maintained in the face of evolving medical technology landscapes?
- What AI capabilities exist for automated policy management that respond to risk changes?
- Do policies persist for mobile medical devices and IoMT systems?
- How are exceptions for critical patient care scenarios documented and managed?

Architecture & Deployment in Clinical Settings

Notes:

Why it matters: Microsegmentation must align with complex healthcare IT infrastructures without disrupting patient care.

- What deployment options support the diversity of medical devices?
- How is enforcement handled in sensitive clinical networks?
- How does the solution scale across multiple hospital systems, locations, and networks?
- What ensures high availability for critical healthcare systems?
- How are remote clinics and telehealth networks supported?
- How are wireless medical networks and devices securely segmented?
- What performance impacts exist for clinical applications or networks?

Operational Technology Support for Medical Devices

Notes:

Why it matters: Medical devices require specialized security handling due to unique protocols.

- How are medical device protocols discovered and classified?
- What methods can be used to enforce segmentation without disrupting the functionality of medical devices?
- How are IT, IoT, and medical device security policies unified?
- What integrations exist with medical device security platforms?
- How are air-gapped medical networks supported?

Incident Response in Healthcare

Notes:

Rapid incident containment is critical to maintaining patient safety.

- What capabilities exist for quarantining compromised medical systems or devices?
- How quickly can policies be updated during a security incident?
- What forensic tools support medical network investigations?
- How are policy changes tracked for compliance?
- What automated response capabilities protect patient data?

Management & Reporting for Compliance

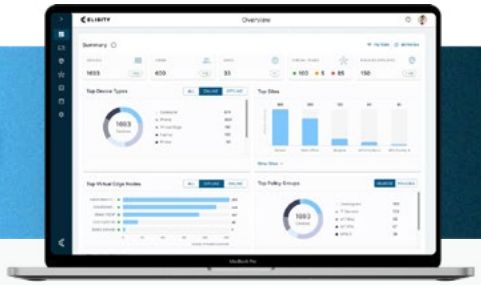
Notes:

Why it matters: Ongoing operations require comprehensive visibility and regulatory adherence.

- What dashboards support HIPAA and HHS reporting requirements?
- How are policy violations in medical networks monitored?
- What SIEM integrations are supported?
- How is compliance documentation generated?
- What APIs enable healthcare security automation?
- Are all actions tracked for audit purposes?
- What role-based access controls protect patient information?

Let's Discuss Your Healthcare Microsegmentation Strategy

BOOK A DEMO



ELISITY

After reviewing this comprehensive Buyer's Guide and Checklist, it's clear that identity-based microsegmentation is essential for protecting patient data and preventing lateral movement attacks in complex healthcare environments. Elisity delivers rapid implementation specifically designed for medical networks - using existing infrastructure without agents, hardware, or complex reconfigurations. Schedule a consultation today to see how your healthcare organization can achieve Zero Trust maturity and enhanced patient data protection in weeks, not years. Protect your clinical systems, secure medical devices, and maintain compliance with a modern microsegmentation approach. **Schedule Your Healthcare Security Demo →**