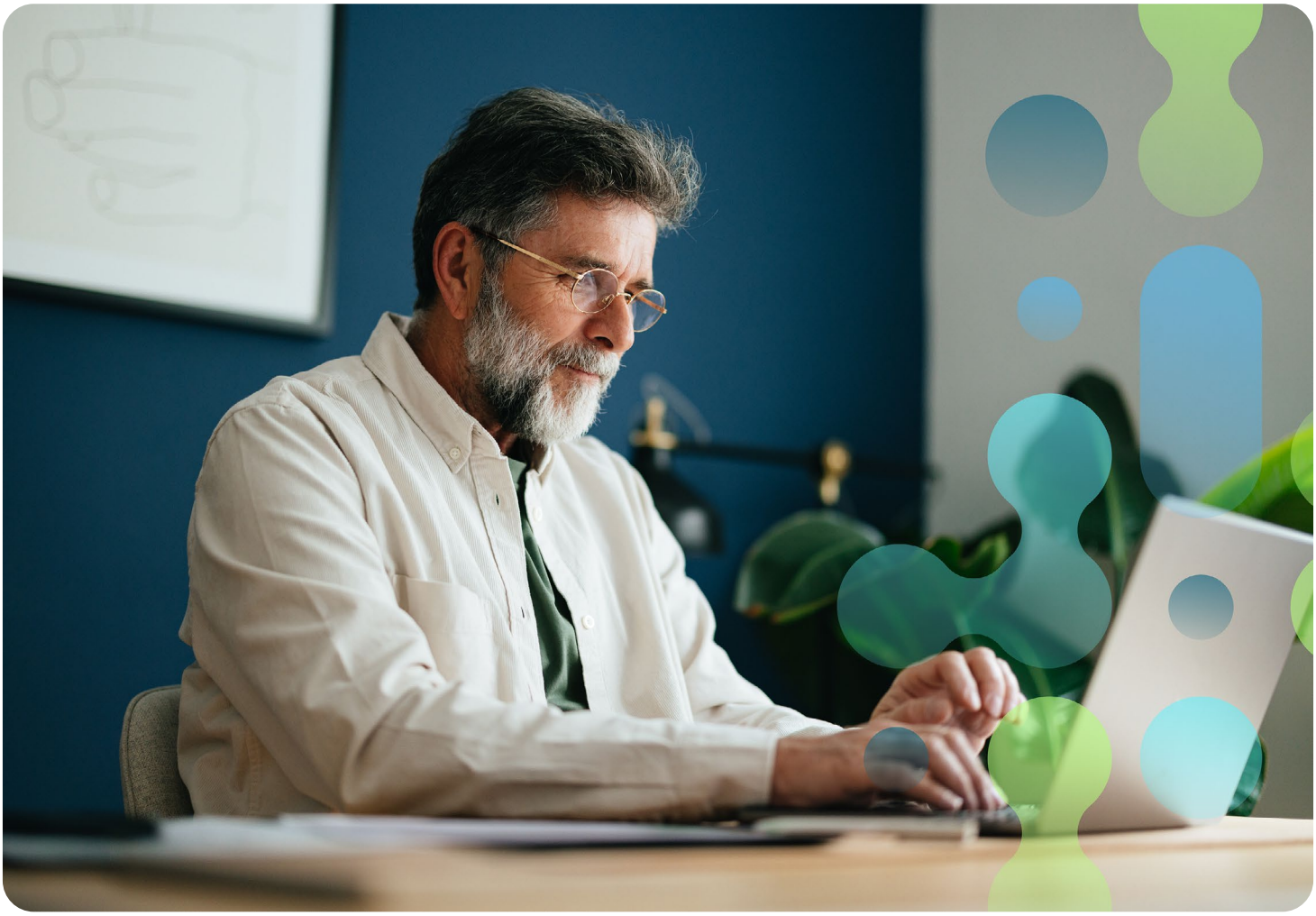
ELISITY

BUYER'S GUIDE

Microsegmentation Buyer's Guide 2025



Definition of Microsegmentation

Identity-based microsegmentation enables organizations to rapidly secure their networks by applying granular, context-aware least-privilege access policies that automatically protect users, workloads, and devices wherever they appear on the network — preventing lateral movement attacks while eliminating the need for new hardware, agents, or complex network reconfigurations.

Executive Summary: The Critical Need for Modern Microsegmentation

In today's threat landscape, cybercriminals increasingly leverage lateral movement (east-west traffic) to amplify attacks after gaining initial access. The expanded attack surface from IoT, OT, and IoMT devices 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 dwelling in networks 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. With cybersecurity budgets under pressure and 75% of organizations pursuing vendor consolidation, businesses need 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 regulations now specifically mandate network segmentation, including IEC 62443 for industrial systems, HIPAA Security Rule, HHS 405(d) for healthcare, and NIST 800-207 Zero Trust architecture guidelines. Organizations must demonstrate granular access controls and traffic isolation to meet compliance requirements.

The Growing Cost of Security Breaches

The financial impact of breaches continues to escalate dramatically. IBM's 2024 **Cost of a Data Breach Report** shows the global average has reached $4.88 million, up from $4.45 million in 2023 — the largest year-over-year increase since 2020. For financial services firms, costs typically exceed $5.9 million per incident.

Building the Business Case for Microsegmentation

For industrial organizations, microsegmentation's ability to isolate critical systems provides additional value by preventing costly operational disruptions. Manufacturing firms report $2 million–$3 million in annual savings by avoiding production 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, organizations should consider both hard cost savings from operational improvements and risk reduction benefits from enhanced security controls. The comprehensive value proposition spans IT operations, incident response, compliance, and cyber insurance — making microsegmentation a foundational security investment for modern enterprises.

Research demonstrates micro-segmentation delivers $3.50 in value for every dollar invested through

- **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 enterprise architecture and the threat landscape.

Early Segmentation (2000–2010)

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

The Cloud Transition (2010–2015)

As organizations began adopting cloud services and virtualization, traditional perimeter-based segmentation proved inadequate. The rise of east-west traffic (lateral movement between workloads) 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, regardless of its location. Modern approaches focus on user identity rather than network location, enabling fine-grained control of communication between individual users, workloads, and devices.

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 to enforce policies.
- **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.

Leading vendors like Illumio pioneered host-based approaches, while newer entrants like Elisity focus on network-based enforcement without requiring agents. Cloud providers offer native capabilities, though these typically work best within their own environments.

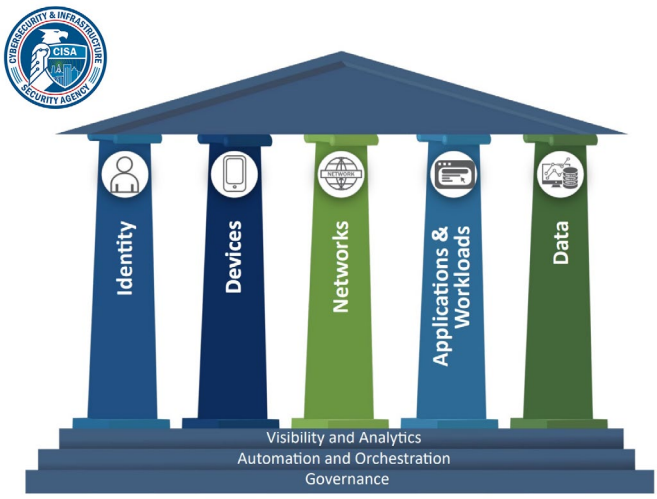
Industry-specific requirements in different sectors have unique microsegmentation needs:

- **Healthcare:** Must protect sensitive patient data and (IoMT) medical devices while maintaining high availability.
- **Manufacturing:** Requires OT/IT convergence security and protection for industrial control systems.
- **Financial Services:** Needs granular segmentation for compliance and protection of critical trading systems.

Current Trends

The market is being shaped by several factors:

- Zero Trust initiatives driving adoption.
- Ransomware threats highlighting the need to limit lateral movement and limit the blast radius.
- Hybrid cloud architectures requiring consistent security across environments.
- Container adoption demanding new approaches to workload-level security.



Zero Trust Model Maturity Pillars

Organizations increasingly seek solutions that include these critical capabilities:

- Close attack surface gaps.
- Provide unified visibility across hybrid environments.
- Automate policy creation and management.
- Integrate with existing security tools and cloud platforms.
- Support both traditional and cloud-native workloads.
- Meet compliance, regulatory or Zero Trust framework goals for segmentation.
- Lower cyber insurance premiums.

The future of microsegmentation points toward greater automation and expanded use of AI/ML for policy optimization. As organizations continue their digital transformation journeys, microsegmentation has become a critical component of modern security architectures.

Key Success Factors for Selecting the Right Solution

1. **Deployment Model Alignment**
   Choose between agent-based and agentless approaches based on your environment. Consider long-term maintenance costs and coverage requirements, especially for IT, IoT, OT, IoMT devices that cannot support agents.

2. **Integration Capabilities**
   Ensure seamless integration with existing security infrastructure, including IAM, SIEM, SOAR, and EDR platforms. API support for automation and orchestration is crucial for operational efficiency.

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 through automation and reduced complexity.

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 cybersecurity with state-of-the-art microsegmentation, schedule a call or demo with Elisity at elisity.com/demo-request and learn how our solutions enable manufacturers and industrial companies and their critical infrastructure leaders to ensure compliance and maintain operational excellence in the face of evolving cyber threats.

Key Features and Capabilities for Microsegmentation Solutions

Understanding the essential features and capabilities is crucial for selecting a microsegmentation solution that will effectively reduce your attack surface and prevent lateral movement. These requirements ensure the solution can scale across hybrid environments while maintaining 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.

☑ Core Functionality Requirements:

- **Visibility and Discovery** (provides comprehensive mapping of all assets and communication flows)
- **Policy Creation and Management** (enables granular policy definition and automated recommendations)
- **Policy Enforcement** (implements and validates security policies across environments)
- **Security Monitoring** (continuous monitoring of policy violations and suspicious behavior)
- **Incident Response** (ability to quickly isolate compromised users, workloads devices)

☑ Must-Have Capabilities:

- **Asset Discovery and Classification** (automatically identifies and categorizes workloads)
- **Policy Simulation** (tests policy changes before enforcement)
- **Real-Time Flow Monitoring** (tracks east-west traffic patterns)
- **Configurable Static and Dynamic Automated Policy Recommendations** (suggests policies based on observed behavior)
- **Automated Risk Score-based segmentation** (automatically changes or suggests policies based on metadata from trusted sources)
- **Comprehensive reporting and audit logs**

☑ Technical Requirements:

- **Network-based Controls** (leverages existing infrastructure for enforcement)
- **Extends beyond IP address or ports** (leverages identity and metadata for segmentation)

☑ Integration Requirements:

- **Identity Providers** (synchronizes with existing IAM solutions)
- **Security Tools** (integrates with CPS [cyber physical systems] or Cyber Asset Attack Surface Management [CAASM], SIEM, SOAR, and EDR platforms)
- **Configuration Management** (connects with CMDB, ITSM, and asset management)
- **RESTful API** (to support CI/CD pipeline integration)
- **IoT, OT, IoMT Security** (interfaces with specialized security platforms)

☑ Deployment Options:

- **Agentless Deployment** (Best-in-class)
- **Agent Based**
- **Host-Based Firewalls**
- **Fabric Overlay**
- **Uses existing infrastructure for enforcement and lower operational overhead**

Vendor Selection Process

"Elisity's deployment at GSK is nothing short of revolutionary, making every other solution pale in comparison."

Michael Elmore, CISO

GSK

"No other vendor can provide the network visibility, telemetry, intelligence, and microsegmentation required to effectively accelerate the time to reduce risk in both greenfield and brownfield environments."

Watch the Case Study Interview Here →

Or visit: **hubs.ly/Q039vCKc0**

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

Change management cycles that once took weeks are now completed in hours — or, in some cases, are not even necessary.

60%–80%
reduction in operational costs

40%–60%
decrease in incident response times

70%–90%
reduction in vulnerable attack paths

Financial Impact

Modern microsegmentation solutions deliver substantial ROI through multiple financial channels. Most organizations see cyber insurance premium reductions of 15%–30% due to improved breach containment capabilities and documented security controls. Automated policy management typically reduces operational costs by 60%–80%, while incident response times and associated costs drop by 40%–60%. Organizations generally achieve positive ROI within 12–18 months through direct cost savings from tool consolidation and operational efficiency gains.

Risk Reduction

The primary business value of microsegmentation comes from dramatically reduced breach impact. By limiting lateral movement, organizations typically see 45% lower breach costs when incidents occur. The technology reduces vulnerable attack paths by 70%–90% through granular segmentation and effectively prevents widespread ransomware encryption across networks. This enhanced protection of critical applications and sensitive data translates directly to reduced business risk.

Operational Efficiency

Microsegmentation transforms security operations by automating previously manual processes. Change management cycles that once took weeks are now completed in hours — or, in some cases, are not even necessary. Real-time visibility into application dependencies enables faster troubleshooting and more efficient application deployments. The technology also simplifies cloud migration by providing consistent security controls across hybrid environments. These operational improvements allow IT teams to focus on strategic initiatives rather than routine policy management.

Compliance Benefits

Modern solutions streamline compliance through automated policy enforcement and documentation. Built-in reporting capabilities generate required compliance evidence for standards like IEC 62443, HHS 405(d), HIPAA, PCI DSS, NIST-207, and other regulatory frameworks. Detailed activity logs and automated reports significantly reduce audit preparation time and costs. The consistent application of security controls across environments ensures ongoing compliance between audits.

Long-Term Strategic Value

Beyond immediate cost savings and efficiency gains, microsegmentation provides lasting strategic value. Organizations gain improved business agility through faster application deployment and simplified cloud adoption. Technical debt decreases as legacy security tools are consolidated. The enhanced security posture supports digital transformation initiatives while reducing overall cybersecurity risk. This combination of operational efficiency, risk reduction, and strategic enablement makes microsegmentation a foundational security investment.

Implementation Considerations for Microsegmentation

Integration Architecture

Modern microsegmentation requires seamless integration with existing security and IT systems. Identity management integration with IAM solutions provides the foundation for user and workload authentication. Integration with security platforms like SIEM, SOAR, and EDR enables coordinated threat detection and response. CAASM and CPS integration offers comprehensive asset visibility and risk management across IT and OT environments. RESTful APIs enable automation through CI/CD pipelines and DevOps workflows, while CMDB and ITSM integration ensures accurate asset tracking and change management.

Deployment Approach

The choice between agent-based and agentless deployment significantly impacts implementation complexity and ongoing operations. Agent-based solutions provide granular control but require ongoing maintenance and updates, and agents only run on endpoints — they do not run on IoT, OT, IoMT devices, for example. Some modern agentless solutions leverage existing network infrastructure for enforcement, reducing operational overhead while maintaining effective segmentation. Consider the long-term costs of agent management, especially in environments with high workload turnover or diverse operating systems.

OT/IoT Considerations

Industrial and healthcare environments require specialized integration with OT/IoT security platforms. Modern solutions support agentless monitoring of these sensitive devices through network-based controls, eliminating the risks of agent deployment on critical systems. Integration with specialized OT security platforms ensures comprehensive visibility and protection without disrupting operations.

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: GSK — Global Biopharma Company

GSK

x4
Implemented 3-4 sites per week

240
IT and OT locations

70k
Employees with managed assets

510k
Unmanaged IoT and OT assets

PREVIOUS PLAN

Implement legacy firewall vendor with hundreds of VLANs and ACLs

CHALLENGE

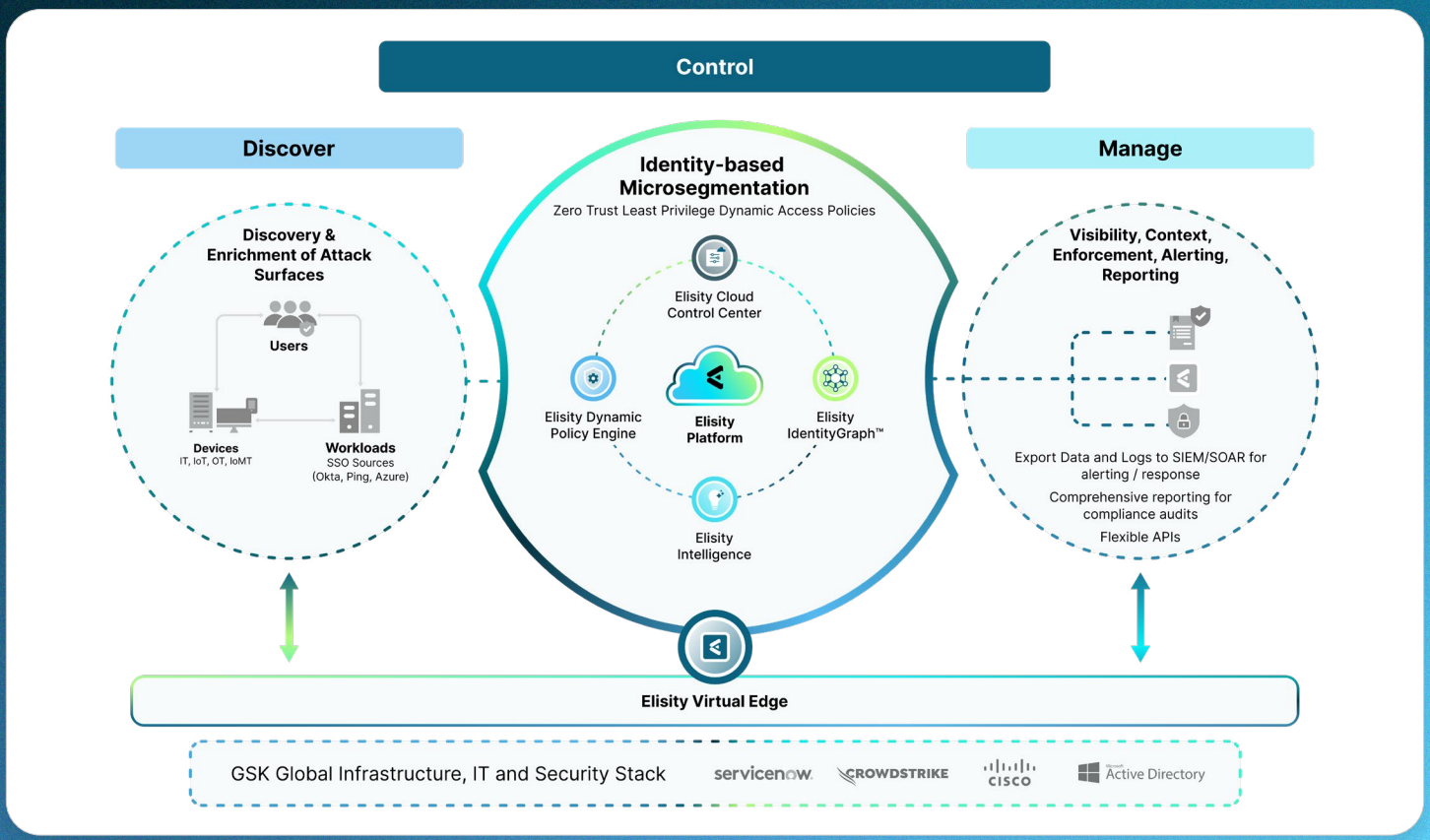
The CISO needed to transition from an approved plan to train and expand the security, network, and IT teams, with the goal of scoping, planning, and implementing segmentation across 275 global sites using legacy firewall technologies. However, the plan failed because it required manually discovering and classifying tens of thousands of devices across these sites while staying within budget. With a deployment timeline of one year per location under the current plan, the project would never meet the required deadlines or be completed within the approved budget.

SOLUTION

With Elisity's capabilities, GSK sought to be able to natively discover all managed/unmanaged, wired/wireless IT/IOT/OT endpoint devices on IT Networks, OT Networks and hybrid IT/OTN Networks and then be able to apply segmentation or quarantine for all unauthorized devices. Another capability GSK gained with Elisity was the ability to expand the capabilities of OT segmentation from strictly network (subnet) based policies, to a hybrid of network and local zone-based device policy groupings.

ROI

- Elisity's platform cut microsegmentation implementation for each site from one year for a single location to one week for three to four locations per week.
- Elisity dramatically reduced the operational overhead of managing and configuring firewall-based segmentation for existing and new devices joining the network.
- Elisity did not require an investment in new firewalls or licenses for existing firewalls.
- Elisity enables GSK to correlate and reconcile all of the discovered endpoint devices with multiple "Systems of Record" (ServiceNow, CrowdStrike and AD), and Regional/Local Spreadsheets of IT/OT Assets. This enables them to quickly determine which devices at each location are "Authorized" vs. "Unauthorized."
- These benefits resulted in this customer reducing their total investment to complete this project from $200 million to $50 million, lowering TCO by 75%.



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.**

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

FORRESTER®
WAVE STRONG PERFORMER 2024
Microsegmentation Solutions

Key Questions to Ask Vendors

Visibility & Discovery

Notes:

Why it matters: Complete visibility into all users, workloads, devices, network assets, traffic flows, and dependencies is foundational for implementing effective microsegmentation policies.

- How does your solution discover and map users, workloads and devices and their dependencies across hybrid environments?
- What methods are used to identify assets and classify them (agents, agentless, APIs)?
- What percentage of the attack surface coverage are your customers achieving?
- How do you maintain visibility when applications move between on-premises and cloud?
- How are ephemeral devices handled — for example, IoMT devices that move between hospitals, patient homes and healthcare clinics?
- Can the solution identify shadow IT and unauthorized applications?
- What integrations exist with CMDBs and asset management tools?

Policy Management & Enforcement

Notes:

Why it matters: The ability to create, test, and enforce granular policies determines the effectiveness of microsegmentation in reducing the attack surface.

- How are policies created, tested, and validated before enforcement?
- What granularity of control is available (host, process, user identity level)?
- How flexible and easy is the policy creation process for global, local, static, and dynamic policies?
- How are policies maintained and updated as environments change?
- What AI/ML automation capabilities exist for policy management?
- Do policies persist for ephemeral devices?
- How are exceptions handled and documented?

Architecture & Deployment

Notes:

Why it matters: The microsegmentation architecture must align with existing infrastructure and scale across hybrid environments.

- What deployment options are available (software agents, agentless, network-based)?
- How and where is enforcement handled?
- How does the solution scale across multiple data centers and clouds?
- What is required for high availability and disaster recovery?
- How are remote and branch locations supported?
- How are wireless networks and devices configured to be segmented?
- What are the performance impacts on applications and network traffic?

Operational Technology Support

Notes:

Why it matters: OT and IoT devices require specialized handling due to their unique protocols and inability to host agents.

- How are OT protocols and devices discovered and classified?
- What methods are used to enforce segmentation without agents?
- How are IT and OT security policies unified?
- What integrations exist with OT security tools?
- How are air-gapped networks supported?

Incident Response & Remediation

Notes:

Why it matters: Microsegmentation must support rapid containment and response during security incidents.

- What capabilities exist for quarantine and isolation?
- How quickly can policies be updated during an incident?
- What forensics and investigation tools are provided?
- How are policy changes tracked and audited?
- What automated response capabilities are available?

Management & Reporting

Notes:

Why it matters: Ongoing operations require comprehensive visibility, reporting and integration with security tools.

- What dashboards and reporting capabilities are included?
- How are policy violations monitored and alerted?
- What SIEM and SOAR integrations are available?
- How is compliance reporting handled?
- What APIs exist for automation and integration?
- Are all user actions and automated policies tracked in audit reports?
- What permission authorization limits for RBAC can be configured?