Brought to you by Informa TechTarget

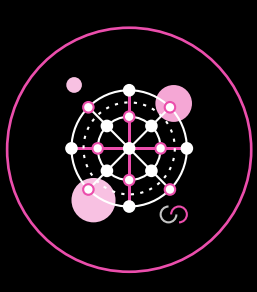
Microsegmentation has matured—is your security architecture keeping up?

Why over 90% of organizations are falling behind, and what to do about it

REALITY CHECK:

Your microsegmentation program is likely falling behind

99% of organizations are implementing or planning microsegmentation. Nearly two-thirds (62%) say today's tools are easier than those from five years ago.

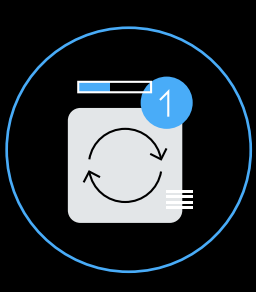


90%

of organizations are falling behind on modern segmentation.

9%

of organizations report that 80% or more of their critical systems are microsegmented.



Most teams are **still relying on outdated methods**, even though they recognize their flaws.

How teams fell behind

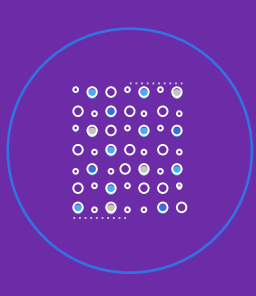
This gap occurred due to continued reliance on legacy approaches, clunky operational processes, and the inability to quickly integrate.

Legacy approaches (VLANs, ACLs, firewalls) **demand constant rework and leave lateral-movement gaps.**

Nearly 50%

experienced incidents involving lateral movement in the past year, even though 57% are prioritizing microsegmentation to stop lateral movement.

Previous microsegmentation approaches created operational drag. **These agent-based and firewall-centric designs couldn't uniformly cover IT, IoT, OT, or IoMT.**



These approaches had outdated or unsupported software (56%), high maintenance costs and hardware limitations (50%), and frequent failures or performance issues (43%).

56%

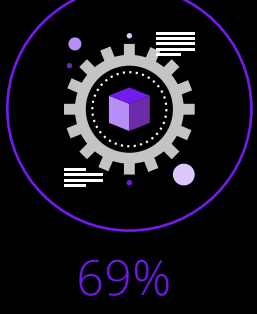
Both healthcare and manufacturing organizations **struggled with integration with SIEM/EDR/SOAR.**

1# **Healthcare** organizations rank this as #1 challenge

2# **Manufacturing** organizations rank this as a #2 challenge

Why the modern approach is different

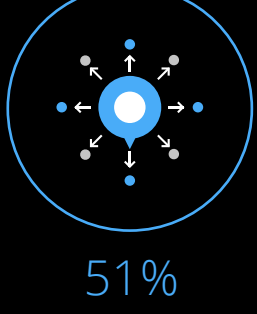
Security leaders in our study demand that their modern solution includes:



69%

Identity-based controls

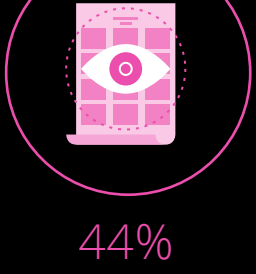
Identity-centric policy + agentless, switch-enforced control means broader coverage with less friction and implementations in weeks – without downtime.



51%

Fast deployments

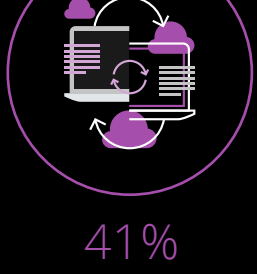
No more multi-year segmentation projects.



44%

Comprehensive visibility

It's critical to be able to see every user, device, and workload



41%

Seamless integration

Microsegmentation must fit into SIEM, EDR, IAM, and cloud stacks you already run.

Applications in critical industries

Modern, identity-first microsegmentation adapts to who, what, and where – not just IPs and VLANs. Certain users and devices require special consideration in different environments, most commonly:

HEALTHCARE

Users

74% Visiting clinicians

72% Clinical staff

Devices

Hard-to-segment patient monitoring/IoMT

Shared terminals

MANUFACTURING

Users

70% Remote engineers

58% Operators

Devices

BMS/ICS

Shared/ remote terminals

What now? Make modern microsegmentation solutions work for you

Microsegmentation is now the #1 initiative to stop lateral movement. Modern, identity-driven, agentless solutions can be deployed in days, not years, with no downtime. **The message is clear: evolve your security architecture now — or stay exposed. But where do you start?**

1

Identify the right platform:

Demand unified user and device discovery, policy creation, simulation, and enforcement on existing infrastructure, with audit-ready reporting.

2

Demo & POV:

Run a POV on real segments, include remote/third-party access, and measure time-to-visibility, time-to-policy, and lateral-movement containment

3

Implement in weeks:

Discover → simulate → enforce at the switch. Tackle high-impact zones first, then expand and report coverage, accuracy, and blocked east-west.

Read the full survey analysis, get a buyer's guide and checklist, or **schedule a demo today** →

https://www.elisity.com

OMDIA

Omdia.com

Omdia OmdiaHQ

ELISITY

elisity.com

elisity elisity