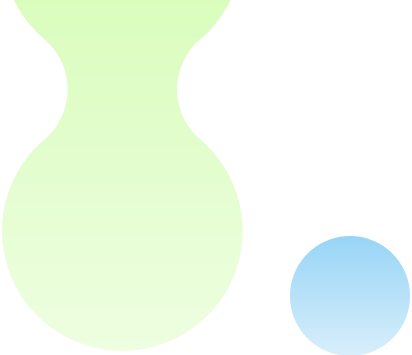


HIMSS MARKET INSIGHTS RESEARCH, COMMISSIONED BY ELISITY AND CARAHSOFT

The implementation paradox.

Healthcare leaders want microsegmentation-level security without disruption.

Findings from a survey of 50 senior leaders at large U.S. health systems.



What the survey says

In December 2025, HIMSS Market Insights asked 50 senior leaders at large U.S. health systems what they want from microsegmentation, what they would pay for, and what stops them. Elisity and Carahsoft commissioned the work; the charts and findings that follow come straight from the report [S1].

58% of Healthcare Leaders Prioritize Avoiding Clinical Downtime When Evaluating Microsegmentation—Yet 40% Say Fear of Disruption Blocks Implementation

HIMSS Market Insights

Survey report, December 2025 [S1]



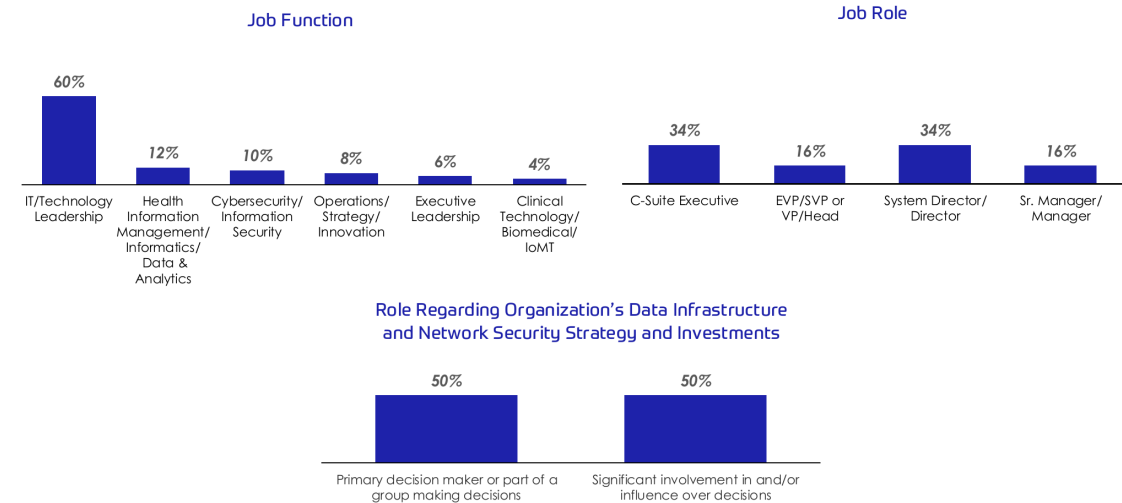
Research by HIMSS Market Insights. Commissioned by Elisity and Carahsoft.

Who answered

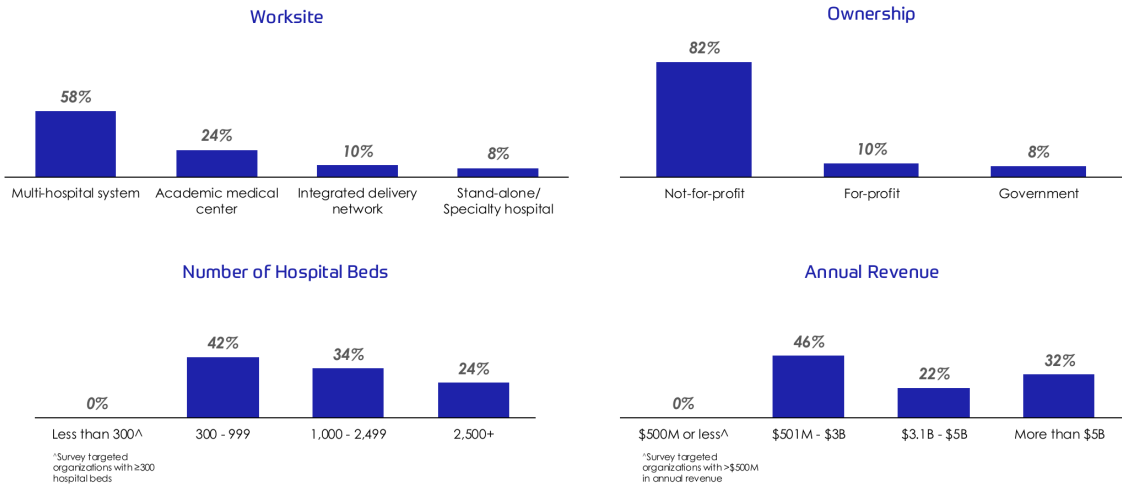
HIMSS Market Insights conducted this research in December 2025 among leaders in healthcare, to understand their perspectives on data infrastructure and network security. Topics included gaps or limitations in organizations' current IoMT, medical device security, and protection strategies; actions taken by cyber insurance carriers in the last two years; the most important ROI outcomes when considering microsegmentation investments; decision drivers when evaluating microsegmentation solutions; and barriers to implementing microsegmentation strategies [S1].

The report describes the fieldwork in its own words: "This research was conducted online amongst Executives and IT/Technology, Cybersecurity/Information Security, Clinical Technology/Biomedical/IoMT, Health Information Management/Informatics/Data & Analytics, and Operations/Strategy/Innovation leaders (managers and above) in healthcare in the United States." Respondents were screened for working in organizations with 300 or more hospital beds and annual revenues exceeding \$500 million, and for having a role in their organizations' strategy and investments related to data infrastructure and network security. A total of 50 qualified respondents participated. This was a blind data collection effort; Elisity was not identified as a sponsor of the research [S1].

Respondent Profile



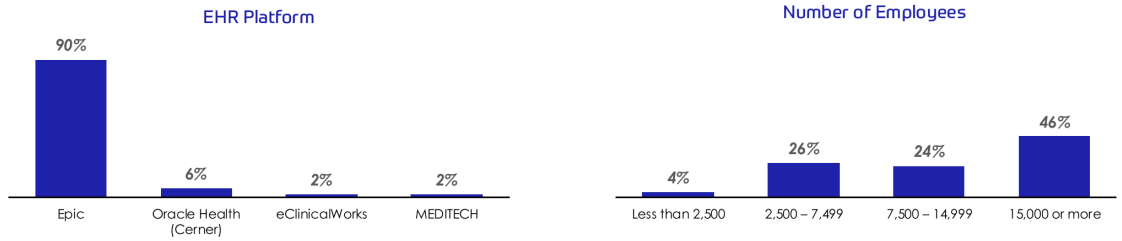
Respondent Organizational Profile



S1. Which of the following best describes your worksite?
S8. Which of the following best describes your health system / hospital ownership?
S2. Please tell us the total number of hospital beds in your organization.
S3. What is your organization's annual net revenue?
Base: Total Respondents; n = 50

HIMSS Market Insights survey report [S1]

Respondent Organizational Profile (cont.)



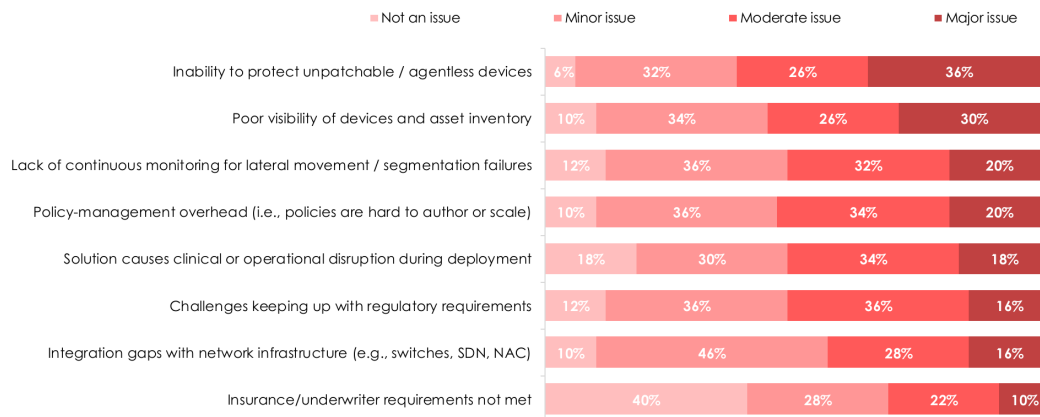
S7. What is your organization's primary EHR (electronic health records) platform?
S9. Please tell us the total number of employees in your organization.
Base: Total Respondents; n = 50

HIMSS Market Insights survey report [S1]

The findings

Healthcare organizations' biggest infrastructure security limitations are their inability to protect unpatchable/agentless devices and poor visibility of devices and asset inventory

To what extent are each of the following gaps or limitations in your organization's current IoMT / medical device security / protection strategy?



Not displayed: 'Something else' (n=4)

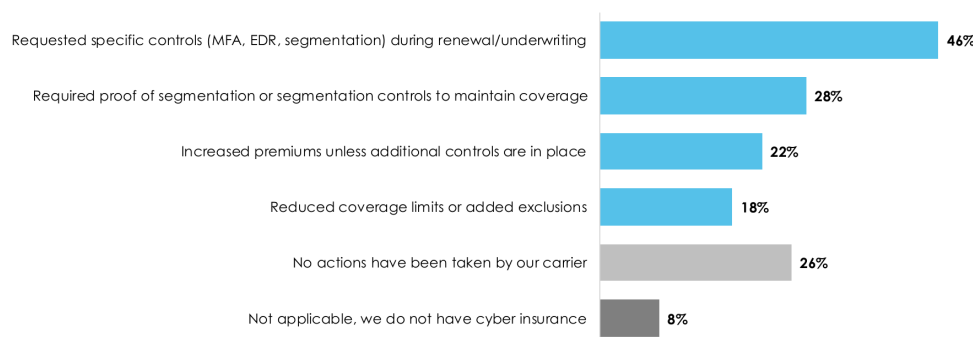
Q1. To what extent are each of the following gaps or limitations in your organization's current IoMT / medical device security / protection strategy?
Base: Total Respondents; n = 50

8

HIMSS Market Insights survey report [S1]

Nearly half of health organizations report their cyber insurance carriers requesting specific controls during renewal or underwriting in the last two years

Has your cyber insurance carrier taken any of the following actions in the last 24 months?



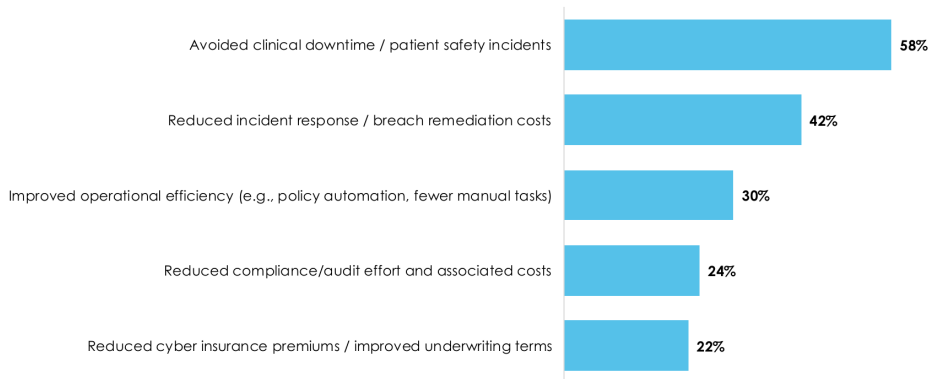
Q2. Has your cyber insurance carrier taken any of the following actions in the last 24 months?
Base: Total Respondents; n = 50

9

HIMSS Market Insights survey report [S1]

Avoiding clinical downtime and patient safety incidents is the most often cited ROI outcome leaders look for when considering microsegmentation investments

As you consider investing in microsegmentation, which of the following ROI outcomes are most important to your organization?



Not displayed: "Other" (n=2)

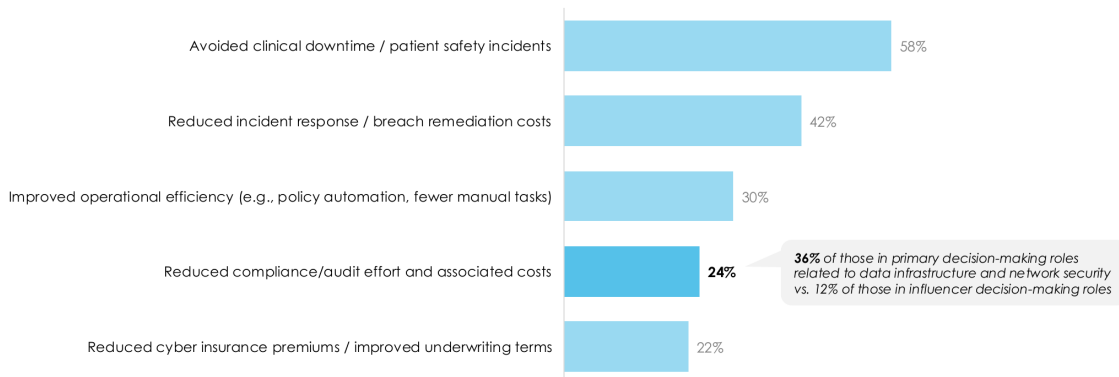
Q3. As you consider investing in microsegmentation, which of the following ROI outcomes are most important to your organization? Please select up to two items.
Base: Total Respondents; n = 50

10

HIMSS Market Insights survey report [S1]

Leaders playing a primary role in decision-making about their organizations' infrastructure and network security more often say reduced compliance/audit effort and the associated costs is a key ROI outcome they consider

As you consider investing in microsegmentation, which of the following ROI outcomes are most important to your organization?



Not displayed: "Other" (n=2)

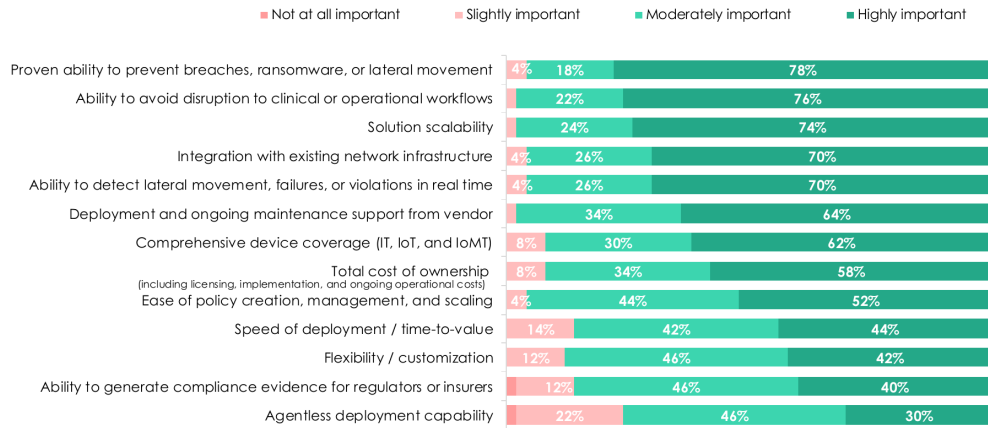
Q3. As you consider investing in microsegmentation, which of the following ROI outcomes are most important to your organization? Please select up to two items.
Base: Total Respondents; n = 50

11

HIMSS Market Insights survey report [S1]

When evaluating microsegmentation solutions, leaders are most likely to say a proven ability to prevent threats, avoid disruption, and scale with their business are important factors in their decision-making

When evaluating microsegmentation solutions, how important are each of the following factors in your organization's decision-making?



Data labels <3% not shown

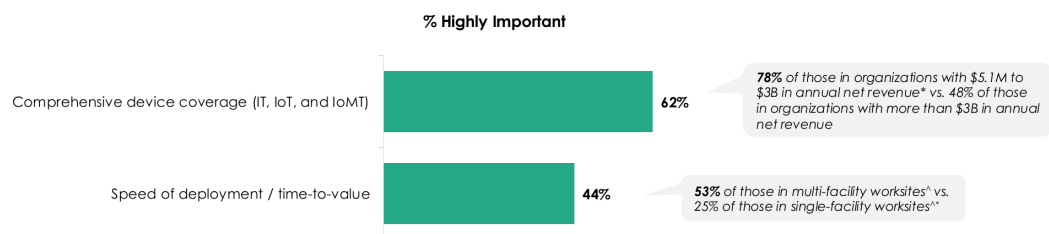
Q5. When evaluating microsegmentation solutions, how important are each of the following factors in your organization's decision-making?
Base: Total Respondents; n = 50

12

HIMSS Market Insights survey report [S1]

Comprehensive device coverage is more often considered highly important by leaders in organizations with \$5.1M-\$3B in annual net revenue, while speed of deployment / time-to-value is more often considered highly important for those in multi-facility worksites

When evaluating microsegmentation solutions, how important are each of the following factors in your organization's decision-making?



*Low base size, insights for directional use only
**Single Facility = Academic Medical Centers, Stand-Alone / Specialty Hospitals, and Clinic / practice settings; Multi-Facility = Integrated Delivery Networks and Multi-Hospital Systems

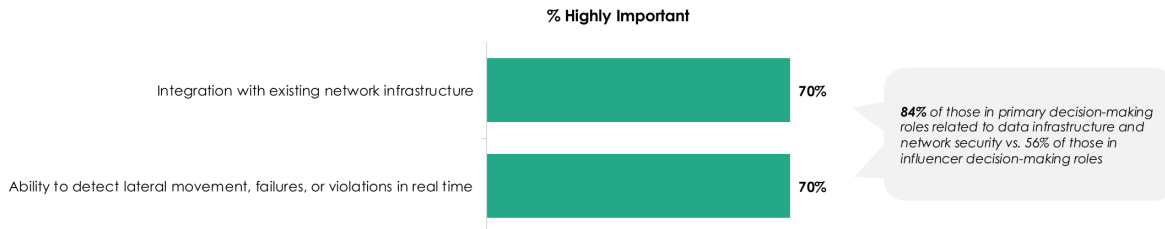
Q5. When evaluating microsegmentation solutions, how important are each of the following factors in your organization's decision-making?
Base: Total Respondents; n = 50

13

HIMSS Market Insights survey report [S1]

Primary decision makers for data infrastructure and network security are more likely to consider integration with existing infrastructure and the ability to detect threats in real time highly important when evaluating microsegmentation solutions

When evaluating microsegmentation solutions, how important are each of the following factors in your organization's decision-making?



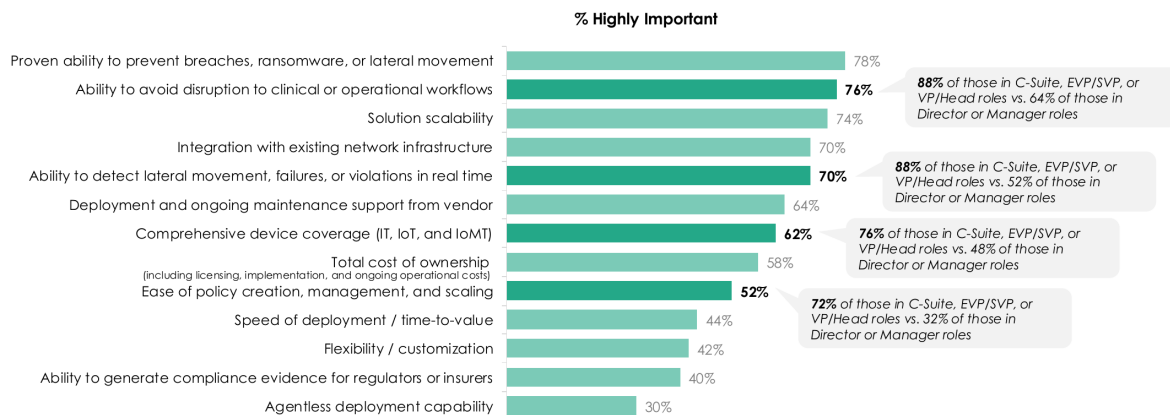
Q5. When evaluating microsegmentation solutions, how important are each of the following factors in your organization's decision-making?
Base: Total Respondents; n = 50

14

HIMSS Market Insights survey report [S1]

Senior leaders more often say a solution's ability to avoid disruptions, detect lateral movement or threats in real time, provide comprehensive device coverage, and offer ease of policy creation, management, and scaling are highly important factors when evaluating microsegmentation solutions

When evaluating microsegmentation solutions, how important are each of the following factors in your organization's decision-making?



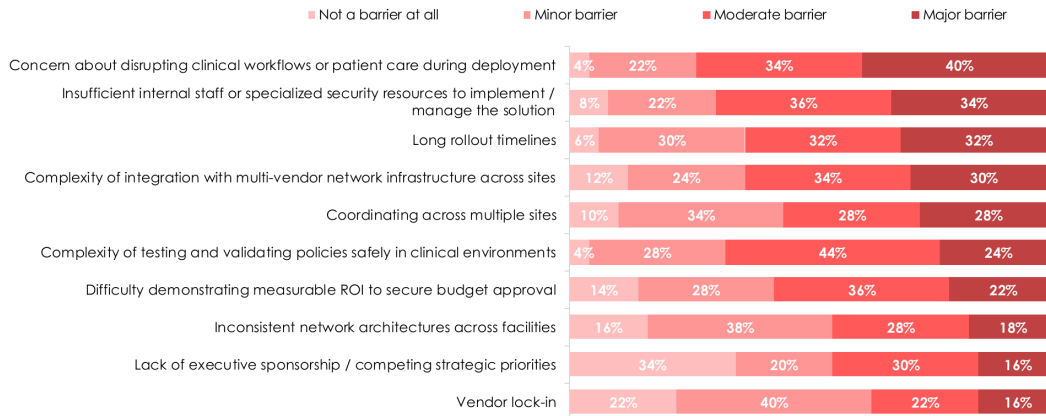
Q5. When evaluating microsegmentation solutions, how important are each of the following factors in your organization's decision-making?
Base: Total Respondents; n = 50

15

HIMSS Market Insights survey report [S1]

More than one-third of healthcare leaders say concerns about disrupting clinical workflows or patient care and insufficient internal staff or resources to manage microsegmentation are key barriers to implementation in their environments

To what extent have each of the following been barriers to implementing microsegmentation in your environment?



Not displayed: 'Something else' (n=3)

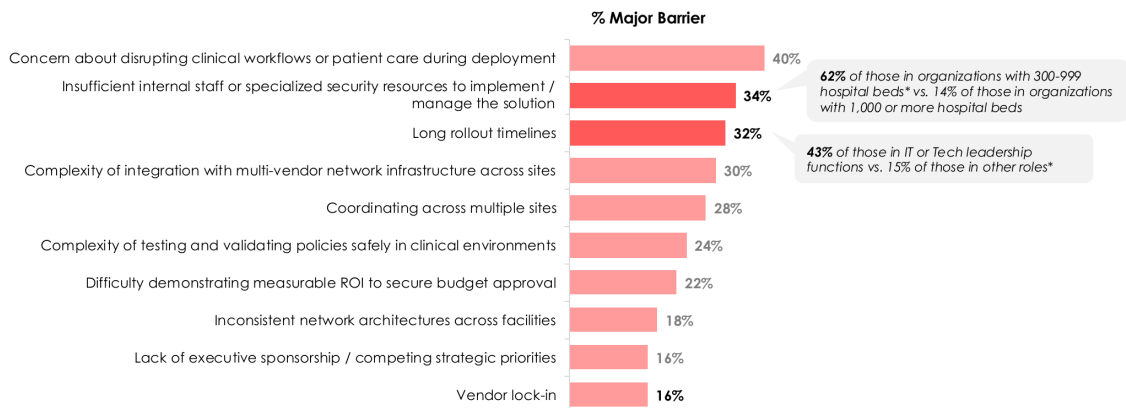
Q4. To what extent have each of the following been barriers to implementing microsegmentation in your environment?
Base: Total Respondents; n = 50

16

HIMSS Market Insights survey report [S1]

Insufficient internal resources to manage microsegmentation and vendor lock-in are more often barriers for those in mid-sized organizations; IT and Tech leaders more often say long rollout timelines is a barrier to their organization implementing microsegmentation compared to leaders in other roles

To what extent have each of the following been barriers to implementing microsegmentation in your environment?



Not displayed: 'Something else' (n=3)
*Low base size, insights for directional use only

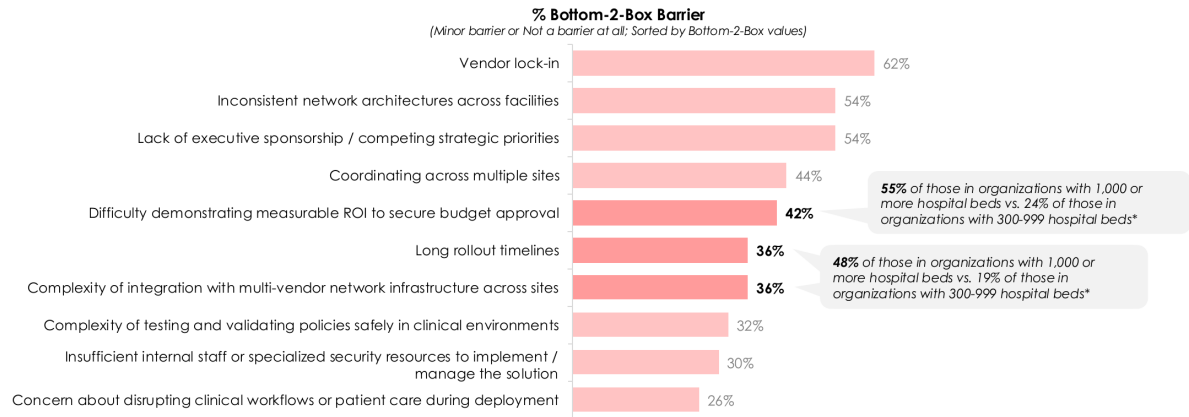
Q4. To what extent have each of the following been barriers to implementing microsegmentation in your environment?
Base: Total Respondents; n = 50

17

HIMSS Market Insights survey report [S1]

Leaders in large organizations (1,000+ hospital beds) are significantly less likely to say difficulty demonstrating measurable ROI to secure budget, long rollout timelines, or the complexity of integration across sites are meaningful barriers to implementing microsegmentation

To what extent have each of the following been barriers to implementing microsegmentation in your environment?



Not displayed: 'Something else' (n=3)
*Low base size, insights for directional use only

Q4. To what extent have each of the following been barriers to implementing microsegmentation in your environment?
Base: Total Respondents; n = 50

Key takeaways

Key Takeaways

1 **More than three-in-five healthcare organizations report gaps in their ability to protect unpatchable or agentless devices**

Organizations' biggest network security limitations are their inability to protect unpatchable or agentless devices (36% rate this as a critical or significant issue), poor visibility of devices and asset inventory (30%), lack of continuous monitoring for lateral movement and segmentation failures (20%), and policy-management overhead (20%).

2 **Nearly half of healthcare leaders surveyed say their cyber insurance carrier has requested specific controls during renewal or underwriting in the last two years**

More than one-fifth of leaders have also reported their cyber insurance carrier required proof of segmentation or segmentation controls to maintain coverage (28%) or increased their premiums unless additional controls were put in place (22%) in the last 24 months. Larger organizations (those with more than \$3B in annual revenue or 15,000+ employees) are more likely to report not currently having cyber insurance.

3 **Avoiding clinical downtime and patient safety incidents is the primary ROI outcome leaders are looking for when considering microsegmentation investments**

Reducing incident response and breach remediation costs is also often cited as one of the most important ROI outcomes when considering microsegmentation investments (42%). Reducing compliance/audit effort and the associated costs are more often cited as important for leaders with primary decision-making roles in their organizations' data infrastructure and network security strategies and investments (36% vs. 12% of those in influencer positions).



HIMSS Market Insights survey report [S1]

Key Takeaways

4 **When evaluating microsegmentation solutions, leaders place a great deal of emphasis on the ability to avoid workflow disruptions**

More than two-in-five (44%) say it is extremely important that a microsegmentation solution is able to avoid disruption to clinical or operational workflows. Overall, leaders are most likely to say a solution's proven ability to prevent breaches, ransomware, or lateral movement (78%), ability to avoid disruption to clinical or operational workflows (76%), scalability (74%), integration with existing network infrastructure (70%), and ability to detect lateral movement, failures, or violations in real time (70%) are highly important.

5 **Concerns about workflow disruptions is the primary barrier to implementing microsegmentation in healthcare environments**

Two-in-five (40%) healthcare leaders say concerns about disrupting clinical workflows or patient care during deployment has been a barrier to implementing microsegmentation in their environments. Additional barriers include insufficient internal staff or specialized security resources to implement and manage the solution (34%), long rollout timelines (32%), and the complexity of integration with multi-vendor network infrastructure across sites (30%). Insufficient resources is more often a challenge for organizations with 300-999 hospital beds (62% vs. 14% of those with 1,000+ beds), while rollout timelines are more often cited by IT and Tech leaders (43% vs. 15% of those in other roles).



HIMSS Market Insights survey report [S1]

Speak to us

Thoughts or questions on the research? Scan the code to connect with the Elisity team and schedule a demo, or visit elisity.com/demo-request.



elisity.com/demo-request

Sources

1. HIMSS Market Insights. Healthcare microsegmentation survey, commissioned by Elisity and Carahsoft. Conducted online in December 2025 among 50 qualified leaders (managers and above) at U.S. hospitals and health systems with 300 or more beds and annual revenues exceeding \$500 million. Research copyright 2025–2026 Healthcare Information and Management Systems Society, Inc. (HIMSS). The views and opinions expressed are solely those of the author/presenter and do not necessarily represent any policy or position of HIMSS or Informa. Research contact: Jill Brewer, Market Insights Lead, HIMSS.
elisity.com



Security for
what's next.

Elisity provides identity-based microsegmentation that deploys on existing network infrastructure, giving health systems device visibility, policy simulation, and enforcement without agents or new hardware. Learn more at elisity.com.

elisity.com

© 2026 Elisity, Inc.