Segmentation Impact Study

Healthcare and Life Sciences

Segmentation is emerging as a powerful defense in the cybersecurity world. Learn how healthcare and life sciences companies are reducing ransomware impact, increasing visibility, preventing zero-day attacks, and achieving compliance.

Healthcare and life sciences organizations operate in some of the world's most targeted and regulated environments. In this landscape, a cybersecurity failure isn't just an IT issue. It affects your patients' safety, privacy, your compliance with HIPAA (a U.S. law) or other country-specific regulations, and your organization's reputation.

The threat is real. In Akamai's **2025 Segmentation Impact Study**, conducted by Phronesis Partners, 76% of healthcare (payer, provider, and health tech) and life sciences (pharma, medical equipment, and devices) organizations faced at least one attack in the past two years. Twenty-seven percent of healthcare and 24% of life sciences organizations reported breaches at least once a quarter.

Akamai's study includes results from 232 healthcare and life sciences leaders across the United States; Europe, the Middle East, and Africa (EMEA); Latin America (LATAM); and Asia-Pacific (APAC). Across the board, the results are clear: Cyberthreats are evolving quickly.

To stay resilient, many organizations are turning to segmentation as a core part of their security strategy — and many more plan to follow.

Segmentation and ransomware containment: A clear connection

In the quest to minimize lateral movement and strengthen Zero Trust security, segmentation plays a major role, and adoption trends reflect that urgency. Forty-five percent of healthcare and life sciences organizations have adopted identity-based segmentation, while **microsegmentation** adoption stands at 36% in healthcare and 31% in life sciences.

This shift is driven by the limits of traditional perimeter defenses in the face of ransomware, third-party access risks, and hybrid environments. Attackers can move freely once inside. By tying access controls to identities and workloads instead of static networks, segmentation helps contain breaches, reduce attack surfaces, and better protect sensitive data like patient records and research IP — delivering operational resilience in highly regulated settings.

Most organizations deploy segmentation to isolate high-risk assets (72% in both sectors) and **contain ransomware** (61% in healthcare and 65% in life sciences), reflecting a shift from mere prevention to limiting blast radius when breaches occur. With ransomware increasingly targeting sensitive systems like patient records, clinical applications, and research environments, organizations are prioritizing controls that keep critical assets segmented from the broader network. The result is faster containment of attacks, reduced operational disruption, and a stronger ability to maintain continuity of care and research, even in the face of active threats.

Key insights

45% of healthcare and life sciences organizations use identity-based segmentation

31% faster ransomware containment in life sciences with microsegmentation

33% of healthcare professionals say segmentation reduces the cost of attesting and ensuring compliance

Top three challenges of implementation:

1. Network complexity
2. Cost
3. Organizational resistance

Akamai

Segmentation most often protects:

- Endpoints (91% in healthcare and 89% in life sciences)
- Business-critical applications (81% in healthcare and 82% in life sciences)
- Servers (75% in healthcare and 61% in life sciences)
- Domain controllers and identity infrastructure (64% in healthcare and 58% in life sciences)

Segmentation brings a measurable impact. In life sciences, organizations report a 31% reduction in the time it takes to stop a ransomware attack. Healthcare organizations report a more than 4% reduction. While the amount of time varies, the takeaway is clear: **Segmentation** helps you contain threats faster.

How organizations are implementing segmentation

Segmentation isn't replacing existing security programs. It's becoming a critical layer within them. Nearly all healthcare and life sciences organizations already rely on firewalls and VPNs, but those tools alone can't stop lateral movement once a threat gets in. That gap is driving growing interest in segmentation, even as complexity, cost, and organizational resistance remain barriers.

The momentum behind segmentation approaches is building. Nearly half of healthcare organizations (47%) and more than half in life sciences (53%) plan to implement microsegmentation within two years, and among current users, a strong majority are increasing budgets.

Clearly, organizations are recognizing that without segmentation, breaches are harder to contain and more costly to recover from. The impact is a shift from reactive security to resilience: Segmentation limits the blast radius of attacks, protects critical systems, and reduces downtime, making it an investment not just in security, but in business continuity.

Cyber insurance and compliance: Boosting your bottom line

Segmentation is also influencing insurance and compliance costs — areas that directly impact your bottom line. For 35% of healthcare and 28% of life sciences organizations, segmentation is now mandatory to renew cyber insurance.

Even when it's not required, 57% of healthcare and 63% of life sciences respondents say insurers view it favorably. Seventy-five percent of healthcare and 77% of life sciences respondents believe segmentation improves the likelihood of claim approval.

There are compliance benefits, too. It even brings cost benefits: 33% of healthcare and 35% of life sciences organizations report lower compliance costs with segmentation.

Ease the road to segmentation

As ransomware evolves and regulatory scrutiny increases, more organizations in your industry are adopting segmentation to:

- Reduce containment time
- Strengthen compliance cost control
- Improve cyber insurance outcomes

But **implementation can feel overwhelming**, especially when you're balancing cost, complexity, and internal resistance.

Partnering with the right provider can help you simplify deployment, avoid operational disruption, and accelerate results — without spreading your internal team too thin.

Research methodology

This report is informed by proprietary research that was conducted by Phronesis Partners for Akamai in 2025. It captures insights from 232 security and technology leaders who represent the healthcare and life sciences industries, offering a rare window into how organizations are approaching segmentation and evolving toward microsegmentation maturity. The sample spans regions and organizational sizes, providing a high-resolution view of current practices, challenges, and emerging priorities.

To read the full report and learn about best practices for segmentation, download the 2025 Segmentation Impact Study.

Ready for a conversation about your segmentation challenges and how Akamai can help? **Request a demo** of Akamai Guardicore Segmentation.

To learn more about how to eliminate risk in your network with industry-leading segmentation, visit **akamai.com/guardicore**.

Akamai is the cybersecurity and cloud computing company that powers and protects business online. Our market-leading security solutions, superior threat intelligence, and global operations team provide defense in depth to safeguard enterprise data and applications everywhere. Akamai's full-stack cloud computing solutions deliver performance and affordability on the world's most distributed platform. Global enterprises trust Akamai to provide the industry-leading reliability, scale, and expertise they need to grow their business with confidence. Learn more at **akamai.com** and **akamai.com/blog**, or follow Akamai Technologies on **X** and **LinkedIn**. Published 04/26.