EBOOK

Overcoming Deployment Obstacles to Protect Critical Healthcare & Life Sciences Systems

Global state of segmentation report

Table of contents

Introduction

Now more than ever, healthcare IT impacts the backroom, boardroom, and the exam room. High-profile data breaches are increasing in terms of severity and frequency, with massive operational and reputational impacts. As threat actors use tactics that are increasingly sophisticated — and in many cases, they join forces — the dangers facing the healthcare ecosystem are more frequent and more serious. Given a large volume of legacy technology, the financial value of patient data, and challenges surrounding rapid digitization and expansion of the Internet of Medical Things (IoMT), this dynamic environment needs to secure its infrastructure, organization, and apps and APIs in ways that no one would have imagined even just five years ago.

As the findings in this report show, cyberattacks are adding to pressure on security leaders to choose the correct solutions in an industry in which continuous uptime is a matter of life or death.

Respondents in healthcare and life sciences organizations across across the United States, Latin America, Europe, the Middle East, Africa, and Asia-Pacific overwhelmingly agree on the effectiveness of segmentation in keeping assets protected. But respondents also report that progress in deploying segmentation around critical business applications and assets is lower than ideal. Respondents (including healthcare providers and healthcare technology specialists, among other organizations specializing in healthcare services or products) say the primary obstacle for healthcare and life sciences organizations has been a lack of expertise to deploy segmentation. The historic complexity of deploying traditional segmentation methods — which don't cover medical devices — is compounded by the fact that teams are still struggling with staffing requirements that began prior to the COVID-19 pandemic.

A survey from the U.S. nonprofit Healthcare Information and Management Systems Society (HIMSS) found that 84% of U.S. healthcare IT experts struggle to attract staff, and 67% report that retaining staff is a problem. The majority of staff don't have up-to-date training on prevailing and emerging threats, HIMSS found.

And just what would that up-to-date training include? Segmentation has proven to have a transformative effect on defense for those who had segmented most of their critical assets, enabling them to mitigate and contain ransomware 11 hours faster than those with only one asset segmented. Imagine the difference those 11 hours make to your team, patients, and reputation.

Segmentation has progressed slowly overall, but those who've persevered have hugely reduced their risk

Segmentation is good. Microsegmentation is better.

Segmentation is an architectural approach that divides a network into smaller segments for the purposes of enhancing performance and security.

Microsegmentation is a security technique that enables you to logically divide a network into distinct security segments down to the individual workload level. Security controls and service delivery can then be defined for each unique segment.

Ransomware attacks continue to rise, as do their impacts

Data from 2021 compared to 2023 shows that the number of ransomware attacks (both successful and unsuccessful) against healthcare organizations in a 12-month span increased 162%. The effects of these attacks can range from operational downtime like cancelled or rescheduled medical procedures, to issues with medication interactions due to lack of access to medical records, and ambulance diversions to other healthcare facilities.

Percentage increase in number of ransomware attacks over the past 12 months by sector (2021 data vs. 2023 data)

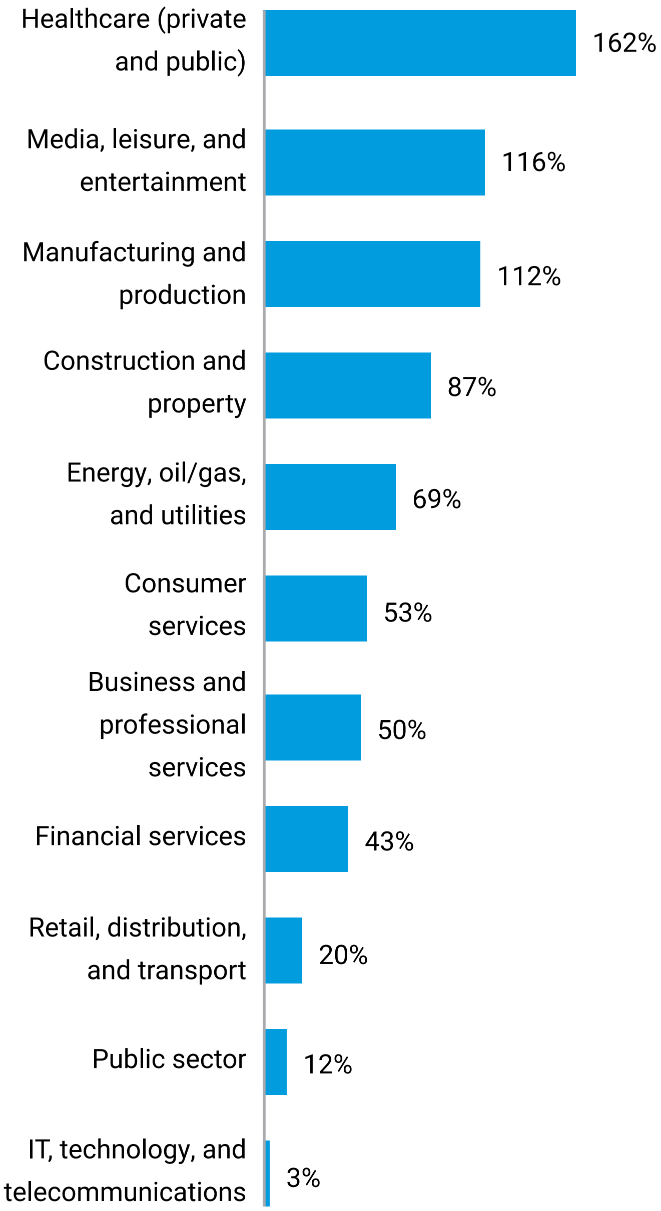

Fig. 1: How many ransomware attacks has your organization been targeted with in the past 12 months (regardless of whether they were successful or not)? Chart reflects base size of 1,200 respondents, only showing the average percentage increase in number of attacks over the past 12 months, split by sector.

On average, the rate of increase for healthcare is the highest across all industries. This could be an indication that healthcare organizations — even including children's hospitals, which also are increasingly victims of attacks — are more unlikely to be seen as "off limits" by hackers.

Ransomware attacks against healthcare organizations are not only more frequent in 2023 vs. 2021, but their impacts are more damaging (figure 2), with respondents indicating increases in reputational damage, loss of customer (patient) loyalty, and network downtime. All of those factors significantly raise the stakes for security teams.

This pressure has also affected agile strategizing. The number of healthcare organizations updating their cybersecurity strategies or policies on at least a weekly basis increased from 17% in 2021 to 25% in 2023, not only in response to ransomware but to a constantly evolving attack surface.

Examining this further, healthcare organizations are among the more likely to suffer financial loss following a cybersecurity attack compared to those in other sectors (43%, compared to 36% overall). Healthcare organizations are also more likely to suffer loss of patient/member loyalty following a cybersecurity attack (48%, compared to 33% overall). This shows that in many respects, healthcare organizations are at greater risk than other types of organizations.

Impact of ransomware/cyberattacks in healthcare & life sciences

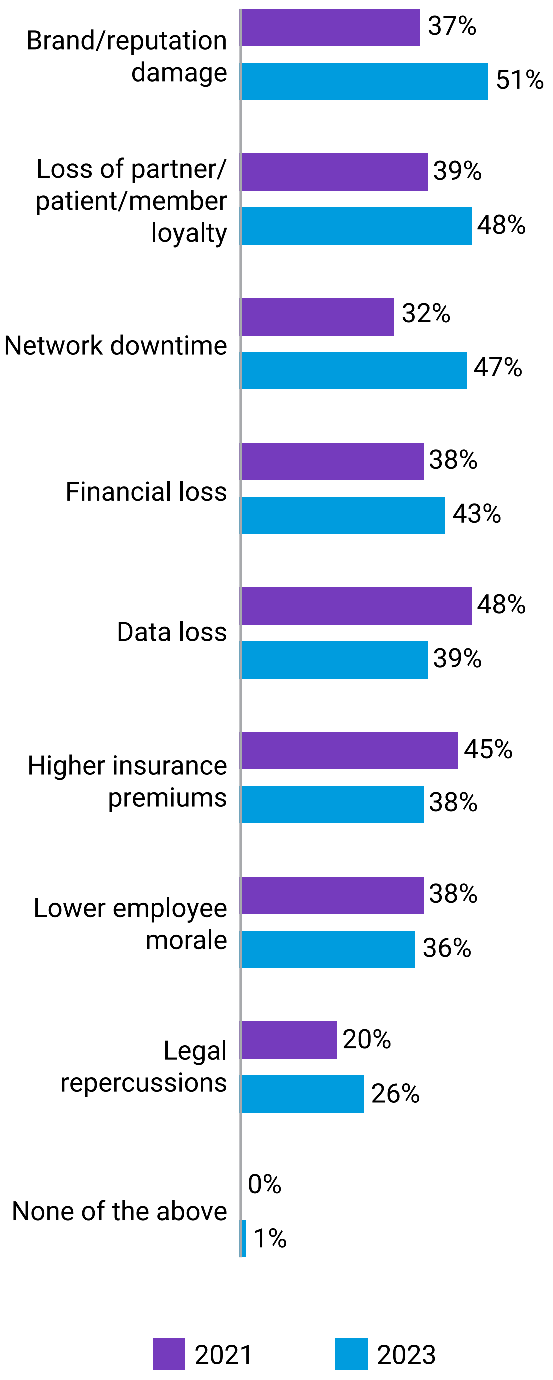

Fig. 2: When your organization has previously detected ransomware or some other cyberattack, which of the following impacts has it had on your organization? Chart shows base sizes by year, not showing all answer options, split by historical data (2021=112, 2023=157), healthcare sector data only.

Segmentation accepted as cornerstone of Zero Trust

Respondents in healthcare and life sciences agree that segmentation is important to ensuring their organizations are secure, particularly in addressing malware.

Zero Trust is a network security strategy based on the philosophy that no person or device inside or outside of an organization's network should be granted access to connect to IT systems or workloads unless it is explicitly deemed necessary. In short, it means zero implicit trust.

Sixty-four percent of survey respondents state that segmentation is extremely important, and 94% believe it is critical to thwart damaging attacks.

Zero Trust adoption is often driven by circumstances beyond healthcare IT leaders' control. When citing why their organization began a segmentation project, a third (33%) of healthcare respondents say it was because of their government's focus on cybersecurity, and nearly as many (29%) say that it was due to them already having fallen victim to a ransomware attack.

But only about one in three (34%) healthcare respondents report that their Zero Trust framework is fully complete and defined, and therefore mature. This is among the lowest across all industries, with some sectors (such as construction and financial services) being notably more likely to have a mature Zero Trust framework in place (53% and 47%, respectively). Zero Trust maturity is likely to be driven by healthcare organizations in the U.S. (where 50% say they have a fully complete and defined framework), compared to the other regions (just 23% of other countries and regions say their Zero Trust framework is fully complete and defined). This reflects the overall trend, where U.S. organizations across all industries report being victims of cyberattacks compared to other regions (115 in the past 12 months, compared to the overall average of 86).

Healthcare organizations therefore have challenges when it comes to Zero Trust. Respondents from this industry are more likely to have encountered issues around proprietary technology when segmenting their network (41%, compared to 32% overall), and are also more likely to be experiencing budget challenges while implementing Zero Trust (47%, compared to an average of 37% across all industries). Support from an experienced partner can help overcome some challenges: Among the most difficult aspects of a Zero Trust framework to implement for healthcare organizations is application workload (68%, compared to 60% overall); a partner can supplement skills gaps, which were reported by 45% of healthcare organizations.

A majority of respondents in healthcare organizations aspire to go further and implement microsegmentation, which protects application workloads at a granular level:

92% of healthcare respondents say microsegmentation is at least a high priority, with 43% naming it as their top priority. Across all industries surveyed, only 34% report microsegmentation as their top priority, demonstrating that healthcare sector organizations are more likely, on average, to value — and advocate for — Zero Trust frameworks.

Deployments are slow, but perseverance yields transformative results

Even with broad recognition that segmentation is pivotal to preventing cyberattacks, segmentation deployment is slow.

Only 36% of healthcare sector organizations have segmented across more than two critical business areas in 2023, and 43% last started a network segmentation project two or more years ago — suggesting efforts have stalled.

The mission-critical areas

- Critical applications
- Public-facing applications
- Domain controllers
- Endpoints
- Servers
- Business-critical assets/data

Slow deployments can be attributed to many of the top obstacles encountered by respondents in the healthcare industry: lack of skills/expertise to implement segmentation (45%), increased performance bottlenecks (such as those caused by the need to manually troubleshoot errors, 44%), and the use of proprietary technology (41%, figure 3). Lack of skills/expertise in particular is a problem for organizations in the healthcare industry, more so than organizations in any other industry (all lower than healthcare's 45%, with the cross-vertical average being 39%). Those results align with recent findings from Ponemon Institute, a top IT security research organization, around prevailing threats for the healthcare industry, which primarily include ransomware and business email compromise (BEC) schemes. While competitive pay for healthcare IT professionals is one challenge, the growing volume of complex regulatory needs is another.

Healthcare organizations around the world continue to feel the aftereffects of the COVID-19 pandemic and the strain it placed upon human and fiduciary capital, and this compounds such challenges.

Obstacles encountered when segmenting the network in healthcare & life sciences

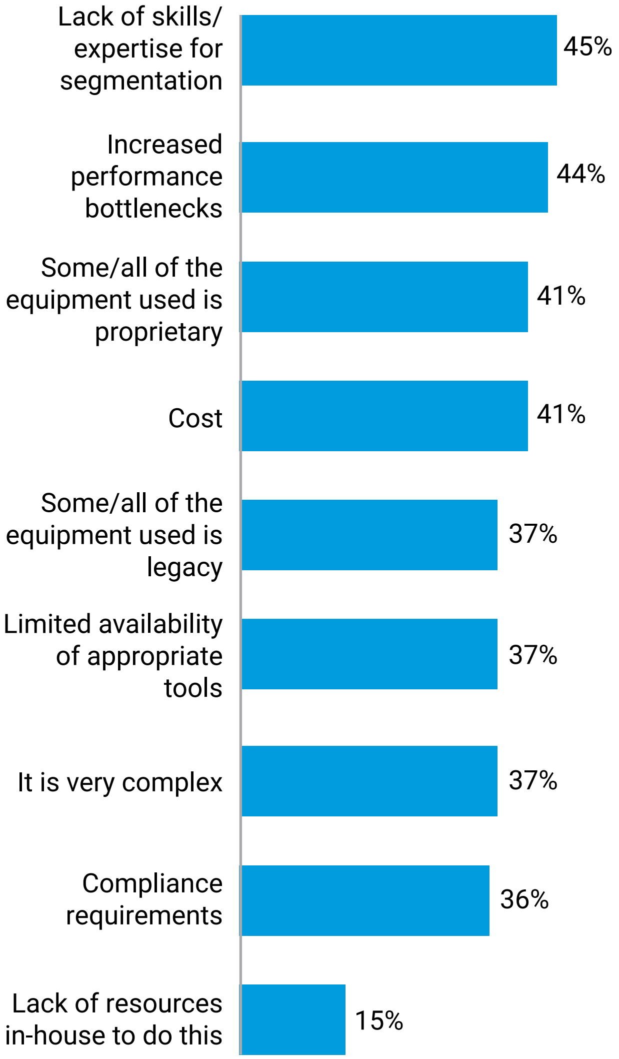

Fig. 3: What problems, if any, did your organization encounter/does your organization foresee when segmenting the network? Chart shows 2023 base size of 157, not showing all answer options. This question was only shown to respondents in organizations that have segmented their network at some point, healthcare sector data only.

Despite slow progress, rates of segmentation are gradually increasing across all industries. Within the healthcare sector, the percentage of organizations with segmented business-critical applications/data rose 20% and segmented servers rose 18% from 2021 to 2023. But while these increases outstrip the overall average increases seen across all industries (12% and 8%, respectively), key vulnerabilities mean segmentation rates must accelerate. The healthcare industry is most likely to have had an office-based employee/user be the reason/source of attacker gaining network access (47%, compared to 26% overall), and this is more than double other such compliance-critical industries such as financial services and energy (both 19%). The impact of such attacks can be minimized with segmentation, and given how critical so many systems can be within healthcare organizations — with lives at stake — it demonstrates the value of segmenting as quickly as possible.

Learnings from segmenting six critical business areas

Enhancing visibility reduces risk, which is pivotal in a risk-averse industry. Protecting and segmenting more assets makes healthcare organizations more secure, allowing security teams to more quickly identify threats and respond far more effectively.

Vanson Bourne's findings show that after a breach, recovery happens 11 hours faster with segmentation. The math: For healthcare organizations that have implemented segmentation across all six mission-critical areas, it takes an average of three hours to completely stop a ransomware attack, for those with segmentation against only one asset, it's 14 hours.

Similarly, segmentation shaves 11 hours off containing lateral movement. For those who have implemented segmentation across all six mission-critical areas, it takes an average of three hours to significantly limit lateral movement of a ransomware attack. For those with segmentation against only one asset, it takes an average of 14 hours.

Consider the difference to your team, the brand damage, and costs incurred during those 11 hours in either scenario.

To stop an attack
3 hours

The time it takes, on average, to completely stop a ransomware attack — for those who have segmented all six business assets. For those who have only segmented one asset: **14 hours**

To limit movement
3 hours

The time it takes, on average, to significantly limit the lateral movement of a ransomware attack — for those who have segmented all six business assets. For those who have only segmented one asset: **14 hours**

How a software-based microsegmentation solution helps solve challenges

Microsegmentation not only enables a more advanced, granular kind of segmentation, but it has become easier to implement as well.

Software-based solutions, like Akamai Guardicore Segmentation, can be quickly deployed without having to make physical changes to the network. There is no need to re-IP new segments or worry about where servers and devices might be physically located. This makes the solution much quicker and easier to deploy than infrastructure-based approaches like firewalls and VLANs. And because the solution does not rely on the underlying operating system for policy enforcement, it works seamlessly across machines and operating systems: from bare-metal servers to multi-cloud deployments, from legacy technology like Windows Server 2003 to the latest Internet of Medical Things (IoMT) devices and containerized technology. This means you're only managing a single solution with one interface to visualize and control connections being made by different operating systems and devices throughout your entire environment, regardless of their physical location.

How it eases deployment

Akamai Guardicore Segmentation first generates an interactive visual of all the connections being made in your environment, which is a critical component to overcoming the primary obstacles to deployment. Moreover, Akamai has built into its solution active ways to address performance bottlenecks and compliance requirements.

Performance bottlenecks don't necessarily arise from any technical strain on a system caused by a segmentation solution but from workforce bottlenecks. The time and effort spent having to manually segment business areas then manually troubleshooting those areas when things break can be tremendous. Akamai works to solve this problem — and the number one obstacle to deployment, lack of expertise — by reducing the time spent manually segmenting, along with top-tier technical support and professional services. Our segmentation experts partner with you throughout the deployment process to ensure you achieve your segmentation goals in your unique IT environment.

Support for deployment also comes from the solution itself: Its AI-powered labeling and policy recommendations and out-of-the-box policy templates for common use cases save time and clicks, simplify workflow, reduce the overall time to policy, and prevent misconfigurations due to human error. For one customer, Akamai delivered a granular segmentation project estimated to take two years and more than US$1 million in total costs in just six weeks with a single engineer, reducing the overall cost of the project by 85% — proving that granular segmentation can be quickly and easily deployed, without suffering from bottlenecks.

How microsegmentation eases compliance

Many healthcare and life sciences organizations deploy Akamai Guardicore Segmentation to ensure compliance with a number of domestic and international compliance mandates, such as HIPAA, GDPR, PCI DSS, and many more. These regulatory mandates usually require that in-scope data is separated from other systems in your environment.

While this can be prohibitive to do using firewalls and VLANs, our software-based solution allows you to create segments specifically for in-scope data and enforce communication rules on what can and cannot access that data. Using our visual map with near real-time and historical views, you can attest to your compliance with these mandates by physically showing that in-scope data is not being accessed by unauthorized users and machines.

Persevere with the right solution and support to transform your security posture

Segmentation can be prohibitively difficult to implement. But as this report shows, those who manage to implement it effectively see massive reductions in their cyber risk. Having proper segmentation in place limits the lateral movement of threats and allows you to react faster during an active breach. And after a breach, recovery efforts are secured and take less time to complete.

Choosing a solution that's designed to overcome the common challenges to segmentation deployment — and partnering with provided experts as you navigate that journey — puts you in the best possible position to transform your security posture. Plus, the more business areas you segment, the more you also advance your Zero Trust architecture, by reducing your present-day risk and ensuring a first line defense against future threat vectors.

Takeaways

Cyberattackers are targeting healthcare sector organizations at an increasing rate: Ransomware attacks against healthcare organizations grew 162% from 2021 to 2023. Comparatively, the energy sector grew 69% in that time frame, and financial services grew 43%.

Healthcare respondents are likely to say that their organization suffered financial loss following a cybersecurity attack: 43% report this, compared to 36% of respondents across all industries.

Segmentation and microsegmentation is more important in the healthcare sector than many other industries: IT security decision-makers at healthcare organizations (64%) are more likely to say network segmentation is extremely important to ensuring that their organization is secure than those in many other sectors, such as construction (58%), manufacturing (53%), and ecommerce (48%). Healthcare IT security decision-makers' sentiments track with the figures from respondents in financial services and energy (both 66%).

Healthcare organizations are unlikely to be more mature when it comes to their Zero Trust security framework deployment: Those in the healthcare sector are unlikely to say their Zero Trust deployment is fully complete and defined (34%), as opposed to those in the financial services sector (47%), energy sector (46%), and ecommerce sector (42%).

Our survey group

For the full research study, we interviewed 1,200 IT and security decision-makers in 10 countries, to measure the progress organizations have made in securing their environments, with a focus on the role of segmentation.

They were asked questions related to their IT security approaches, segmentation strategies, and the threats their organization faces in 2023. These insights and findings give us detail into how security strategies have changed since 2021, and where progress still needs to be made.

Respondents were surveyed globally, including the United States, India, Mexico, Brazil, the United Kingdom, France, Germany, China, Japan, and Australia. They were from organizations with 1,000+ employees, as well as a range of industries and sub-verticals.

Note: This sample differed slightly from 2021. Sample sizes: 2023: 1,200 completes; 2021: 1,000 completes. In 2023, respondents from Australia, Japan, and China were also interviewed. The sectors differed slightly from 2021. In 2023, we focused specifically on digital commerce as its own sector.

For the purposes of this healthcare and life sciences report, we analyzed 157 (2023) and 112 (2021) respondents working in the sector. These respondents represent the same countries as the main report (U.S., India, Mexico, Brazil, the U.K., France, Germany, China, Japan, and Australia).

The full research study included the following additional industries: Ecommerce (190), Financial services (173), IT, technology and telecoms (125), Energy, oil/ gas and utilities (94), Manufacturing and production (91), Retail, distribution and transport (81), Media, leisure and entertainment (63), Construction and property (60), Business and professional services (58), Public sector (46), Consumer services (33), Other industries (29).

Learn more about Akamai Guardicore Segmentation

Akamai powers and protects life online. Leading companies worldwide choose Akamai to build, deliver, and secure their digital experiences — helping billions of people live, work, and play every day. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, stop ransomware, secure apps and APIs, or fight off DDoS attacks — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's solutions for healthcare and life sciences at akamai.com/healthcare and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn. Published 05/24.

Vanson Bourne is an independent specialist in market research for the technology sector. Their reputation for robust and credible research-based analysis is founded upon rigorous research principles and their ability to seek the opinions of senior decision-makers across technical and business functions, in all business sectors and all major markets. For more information, visit www.vansonbourne.com.