Akamai

EBOOK

Overcoming Deployment Obstacles to Protect Critical Banking Systems

Global state of segmentation report

Table of contents

Introduction

Protecting the financial services industry has always posed significant and unique challenges for IT security teams. However, increasingly sophisticated attackers are now combining techniques to launch larger and more frequent threats, putting financial services institution security teams under greater pressure than ever before. Financial services institutions rely on a digital presence to operate, and so one successful breach can cause extensive — if not irreparable — damage to reputation and revenue.

As the findings in this report show, these attacks are also having a greater impact, adding to pressure on security leaders to choose the right solutions and keep the entire environment safe, without compromising overall performance, or risking the exposure of vast amounts of sensitive data.

Respondents in financial services institutions (represented from all regions, including the U.S., LATAM, EMEA, and APAC) agree overwhelmingly on the effectiveness of segmentation in keeping assets protected, but overall progress in deploying it around critical business applications and assets is lower than expected. The number one obstacle for financial services institutions has been increased bottlenecks, which suggests that teams may have been reacting to threats without having the time or support to fully understand and mitigate performance impacts resulting from changes.

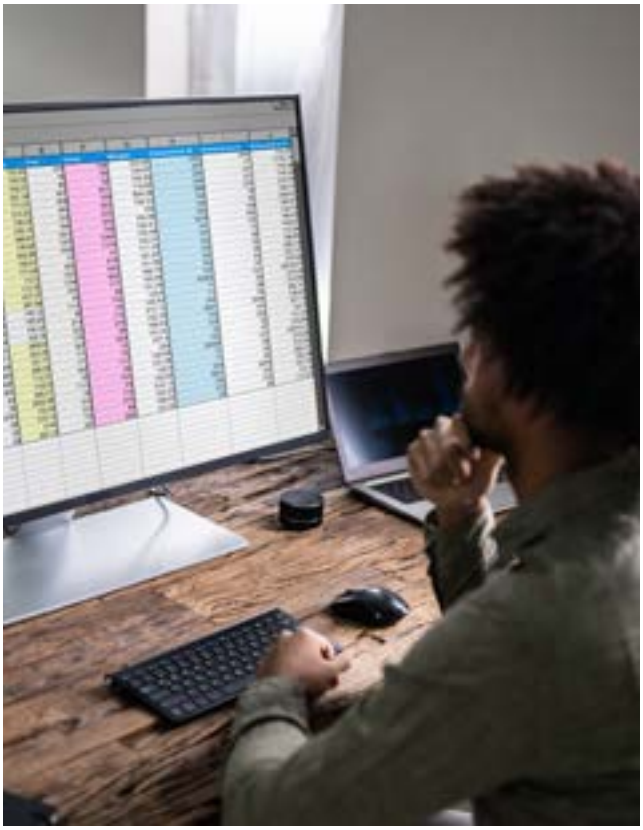
The good news? Perseverance pays off. Segmentation proved to have a transformative effect on defense for those who had segmented most of their critical assets, enabling them to mitigate and contain ransomware 13 hours faster than those with only one asset segmented. Imagine the difference those 13 hours make to your team, customers, and reputation.

The outcome: 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 does their impact

The number of ransomware attacks in financial services institutions (both successful and unsuccessful) has increased by nearly 50% in the past two years, from 43 on average in 2021 to 62 in 2023. Despite the sector's reputation for robust security measures, these numbers underscore a critical vulnerability that cannot be overlooked. It's evident that the financial services sector is not immune to the threat of ransomware, and complacency is not an option.

Financial services institutions in the APAC region have been targeted with the highest number of ransomware attacks on average (73), and LATAM the lowest (48, figure 1).

Average number of ransomware attacks in the financial services sector over the past 12 months by region

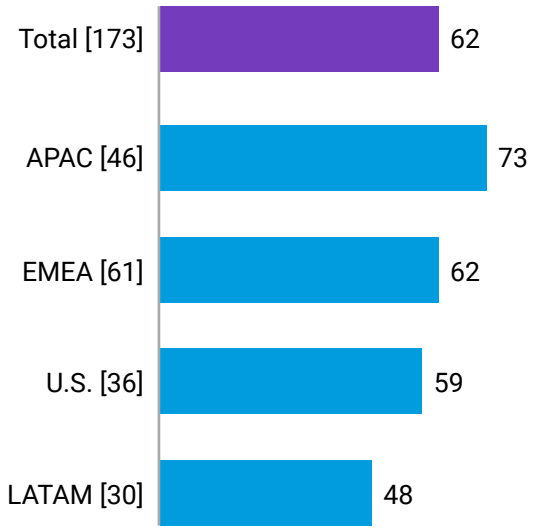


Fig. 1: How many ransomware attacks has your organization been targeted with in the past 12 months (regardless of whether they were successful)? Chart shows the average number of attacks over the past 12 months, split by region (base numbers shown), financial services sector data only.

Since most financial services institutions operate globally, the increased number of targeted attacks in APAC could stem from hackers' perception that APAC targets offer higher yields. However, this doesn't imply that financial institutions in other regions are safer—just that they may be more likely to suffer lateral attacks that originate elsewhere.

Furthermore, respondents in LATAM are most likely to say that their financial institution has segmented more than two assets, followed by APAC. This shows that financial institutions in APAC may be attempting to increase their segmentation in light of the number of ransomware attacks that they are being targeted with.

Those who have segmented more than two assets/area by region within the financial services sector

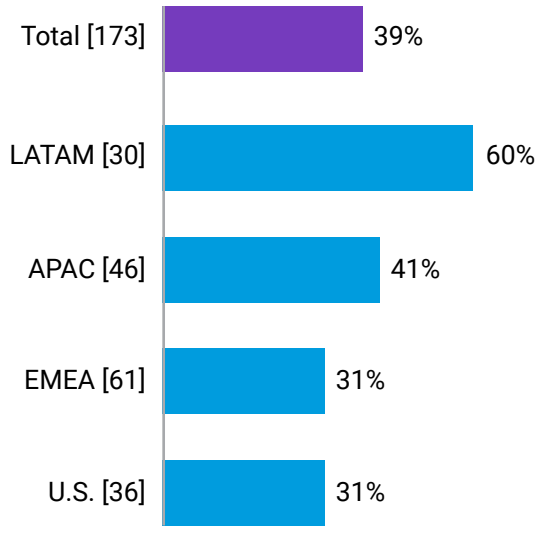


Fig. 2: For each of the following IT security measures, what assets, if any, are they covering? Chart shows responses for segmentation security measure only, and percentages that are using segmentation for protecting key assets, split by region (base numbers shown), financial services sector data only.

Ransomware attacks are not only more frequent in 2023 vs. 2021, but their impacts are more successful (figure 3), with our respondents indicating increases in network downtime and data loss — both of which significantly raise the stakes for security teams. Increases have also been seen in the proportion of respondents reporting higher insurance premiums, driven particularly by U.S. respondents (56%). This demonstrates the level of risk that financial institutions can carry, often holding data not just on individuals but also on businesses.

We see the effect of this pressure also in terms of strategy: The number of financial services institutions that are continuously updating cybersecurity strategies or policies has increased from 3% in 2021 to 18% in 2023, not only in response to ransomware but to a constantly changing attack surface. Distributed workforces and applications, and data migrating to the cloud, are just two factors affecting security strategy on a daily basis.

Impact of ransomware/cyberattacks upon financial services institutions

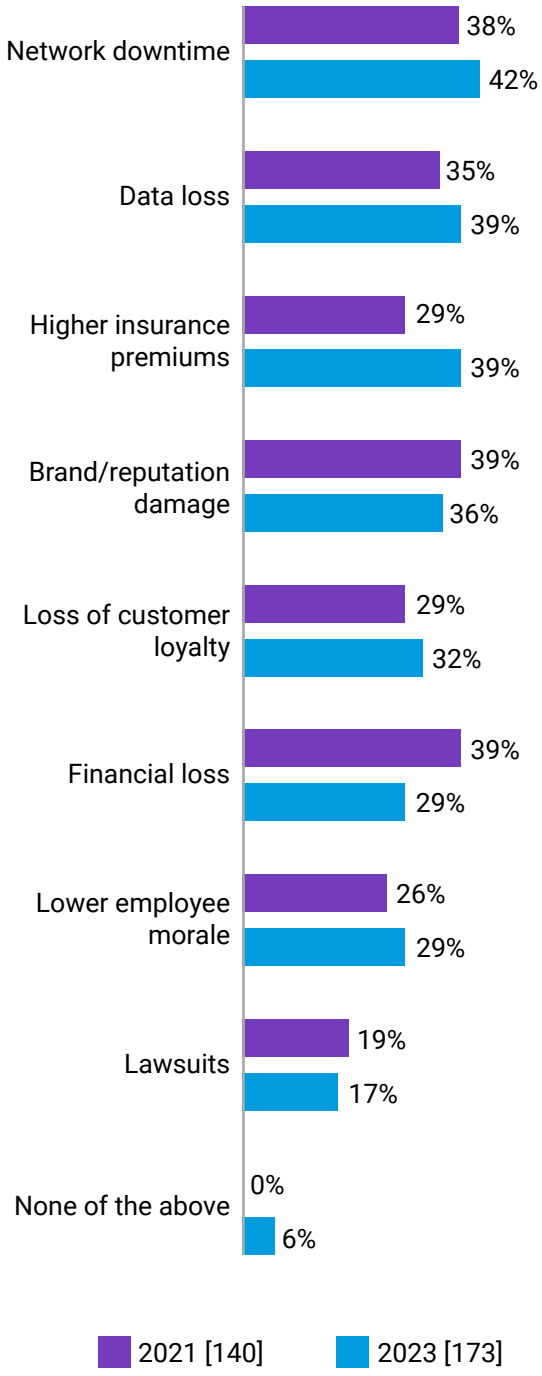


Fig. 3: When your organization has previously detected ransomware or some other cyberattack, which of the following impacts has it had on your organization? Chart shows base sizes by year, split by historical data, financial services sector data only, not all answer options shown.

Segmentation is the cornerstone of Zero Trust

Our respondents in the financial services sector agree that segmentation is important to ensuring their organization is secure, and particularly in addressing malware: 66% state it's extremely important, and 92% believe it is critical to help thwart damaging attacks.

Segmentation also contributes majorly to a Zero Trust framework. When citing why their organization began a segmentation project, the most common answer was to advance Zero Trust: Almost all those who have segmented at all are deploying or have already deployed a Zero Trust security framework (99%), although less than half (47%) report their Zero Trust framework as being fully complete and defined, and therefore mature.

A majority of respondents in financial services institutions aspire to go further and implement microsegmentation, which protects application workloads at a granular level: 88% say microsegmentation is at least a high priority, with 39% naming it as their top priority. Respondents in LATAM are most likely to regard it as a top priority (50%), with those in EMEA the least likely (31%). The fact that LATAM respondents are more likely to report this being a top priority is reflected in their performance (figure 1), showing that organizations which prioritize microsegmentation can expect to reap the benefits.

Furthermore, 99% of IT decision-makers in this sector report that microsegmentation has been adopted by at least a minority of their industry, emphasizing that it is a solution that nearly all have broad awareness around.

Perseverance yields transformative results

The harsh reality is that even with such broad agreement that segmentation is the key to stopping attacks, segmentation deployment has been slow — slower than perhaps expected. Only 39% of financial services institutions have segmented across more than two critical business areas in 2023 (compared to 26% in 2021), and 45% last started a network segmentation project two or more years ago, suggesting efforts have stalled.

Slow deployments are most clearly explained by the top obstacles encountered by respondents: increased performance bottlenecks (41%), lack of skills/expertise for segmentation (39%), and compliance requirements (35%). It's worth noting that while a lack of resource or expertise is a key reason behind delay in segmentation projects, a talent shortage is present across cybersecurity, and with changes in this space happening so quickly, skill gaps are bound to be present.

However, when broken down by region (see figure 4), there is variation in the obstacles most likely to be encountered. This shows that certain issues may be driven as much, if not more so, by local conditions (e.g., lack of skills in the U.S., compliance concerns in APAC) than they are by global issues.

Despite slow progress, rates of segmentation are gradually increasing overall. The percentage of organizations with segmented business-critical applications/data rose 17%, and segmented servers also rose 17% from 2021 to 2023. These increases outstrip the overall average increases seen across all sectors (12% and 8%, respectively), showing that IT departments in financial services institutions are somewhat more able than most to address obstacles that are encountered. This may be because the generally strict compliance requirements noted above require an increasingly stronger level of security. It could also be linked with the higher insurance premiums that financial services institutions have been facing — insurers may be placing requirements upon their customers to be able to address certain issues as quickly as possible.

Obstacles encountered when segmenting the network in the financial services sector — top three by region

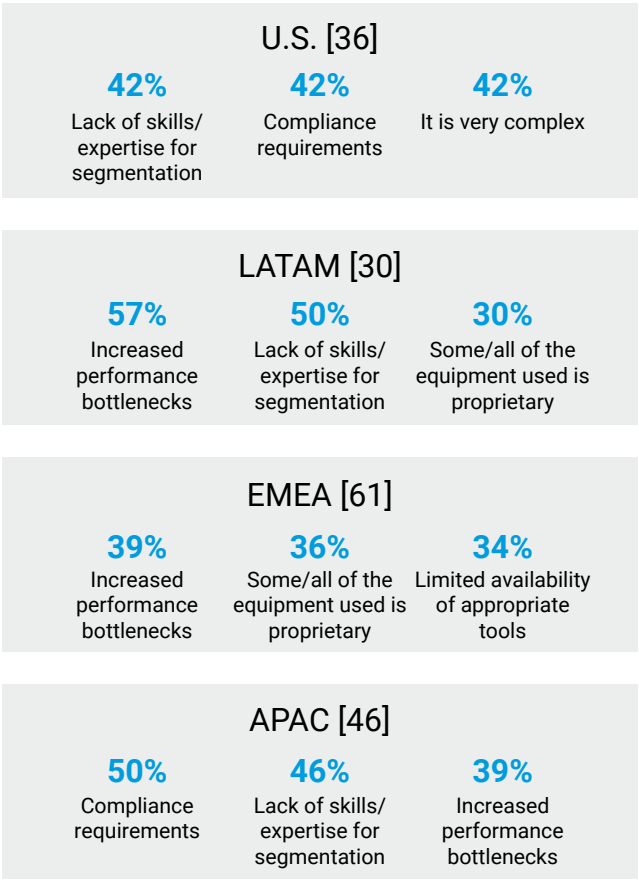


Fig. 4: What problems, if any, did your organization encounter/does your organization foresee when segmenting the network? Chart shows base sizes by region, question only shown to those who have segmented their network at some point, only showing top three selected answers by region, financial services sector data only.

Those who've segmented six critical business areas have greatly reduced risk

Protecting and segmenting more assets immediately makes financial institutions more secure. Security teams are more able to identify attacks and can respond far more effectively. The implementation of immature or ill-defined segmentation strategies only increases vulnerability — but when done right, segmentation improves cyber resilience and prevents cyberattacks from causing major business failures by stopping ransomware and breaches from spreading to critical systems and data.

Our findings show that after a breach, recovery happens 13 hours faster with segmentation.
Doing the math: For those financial services institutions that have implemented segmentation across six mission-critical areas, it takes an average three hours to completely stop a ransomware attack. For those with segmentation against only one asset, it's 16 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 cost incurred during those 11–13 hours, depending upon the 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: **16 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

Financial institutions are seeking to enhance scalability, leverage existing investments, optimize costs, and improve agility and flexibility by migrating workloads to the cloud, often integrating on-premises data centers with private or public clouds. Software-defined segmentation solutions, such as Akamai Guardicore Segmentation, have emerged as a flexible, streamlined, and cost-effective approach to application-level security, dramatically accelerating implementation, simplifying maintenance, and effectively mitigating threats. Because it is quicker and easier to deploy than infrastructure-based approaches like firewalls and VLANs, it allows financial institutions to achieve security at scale while meeting the accelerating demands of their business and providing innovative customer experiences with cutting-edge technologies. Additionally, it seamlessly operates across diverse systems and environments, providing centralized management and control, from bare-metal servers to multicloud deployments and legacy systems. Thus, it offers a unified solution for visualizing and controlling connections across the entire environment, regardless of physical location.

How it eases deployment

Microsegmentation 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 our 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 caused by having to manually segment business areas and then manually troubleshoot those areas when things break. Akamai works to solve this problem — and the number one obstacle to deployment, lack of expertise — by reducing the need to manually segment and by offering 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 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 of our customers, we were able to deliver a granular segmentation project estimated to take two years and over 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 of our customers deploy our solution to ensure and attest compliance with a number of compliance mandates, such as PCI DSS, SWIFT, Sarbanes-Oxley, GDPR, DORA, 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 complex. But as this report shows, those who manage to implement it effectively see improved network security, better network performance, compliance, and simplified network management. 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.

Regional takeaways

Segmentation and microsegmentation is more important in EMEA and the U.S. than it is in LATAM: IT security decision-makers in EMEA (70%) and the U.S. (60%) are more likely to say network segmentation is extremely important to ensuring their organization is secure than those in LATAM (57%).

Those in LATAM are more likely to say microsegmentation is the top priority: (50%) than counterparts in the U.S. (42%), APAC (41%), and EMEA (31%).

Those in EMEA are more likely to have not segmented at all: Those in EMEA are more likely to say no business-critical assets have been segmented (7%) — all other regions had segmented to some extent.

Those in LATAM are most likely to have made most progress with segmentation: Financial services organizations in LATAM are more likely to have segmented more than two business-critical assets (60%) than APAC (41%), EMEA (31%), and the U.S. (31%).

Organizations in all regions experience challenges: 98% of those in APAC say they encounter issues when segmenting their network, and a similar amount said the same in the U.S. (97%), although slightly fewer said this in EMEA (89%) and LATAM (87%).

Financial services institutions in LATAM are far more mature when it comes to their Zero Trust security framework deployment: Those in LATAM are far more likely to say their Zero Trust deployment is fully complete and defined (57%) vs. EMEA (48%), the U.S. (47%), and APAC (41%).

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 faced 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 from all over the world, including those from the U.S., India, Mexico, Brazil, the U.K., France, Germany, China, Japan, and Australia. They were from organizations with 1,000+ employees, as well as a range of industries and sectors.

For the purposes of this report, we analyzed 173 (2023) and 140 (2021) respondents working in the financial services sector.

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 financial institutions at akamai.com/finserv and akamai.com/blog, or follow Akamai Technologies on X, formerly known as Twitter, and LinkedIn. Published 05/24.

VansonBourne

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.