WHITE PAPER

The State of Segmentation 2023

Overcoming deployment obstacles proves to be transformational

Table of contents

Introduction

IT security departments have never had it easy. But now, increasingly sophisticated attackers are combining techniques to pose bigger and more frequent threats, putting security teams under greater pressure than ever before. No business can operate without an online presence, and 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 sacrificing overall performance or innovation.

In updating this report's findings since 2021, we aimed to find out whether segmentation was the solution of choice and whether it was effective. The 1,200 respondents agreed overwhelmingly on the effectiveness of segmentation in keeping assets protected, but their overall progress in deploying it around critical business applications and assets was lower than expected. Across geographies, the number one obstacle has been a lack of expertise to deploy segmentation, which suggests that teams might be hesitant to embark on a project that could disrupt performance — especially given the growing complexity of IT environments.

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 11 hours faster than those with only one asset segmented. Imagine the difference those 11 hours make to your team, customers, brand reputation, and revenue.

Ransomware attacks continue to rise, as does their impact

The number of ransomware attacks (successful and unsuccessful) has doubled over the past two years, from 43 on average in 2021 to 86 in 2023. An even greater rise was measured between Q1 2022 and Q1 2023 by data collected from the leak sites of approximately 90 different ransomware groups. Released in August 2023, Ransomware on the Move: Evolving Exploitation Techniques and the Active Pursuit of Zero-Days cites that the use of zero-day and one-day vulnerabilities has led to a 143% increase in total ransomware victims globally.

Not surprisingly, US companies still face the greatest number of ransomware threats (Figure 1): IT security teams and decision-makers there report an average of 115 ransomware attacks over the past 12 months — the most of any individual country measured.

Average number of ransomware attacks over the past 12 months by country

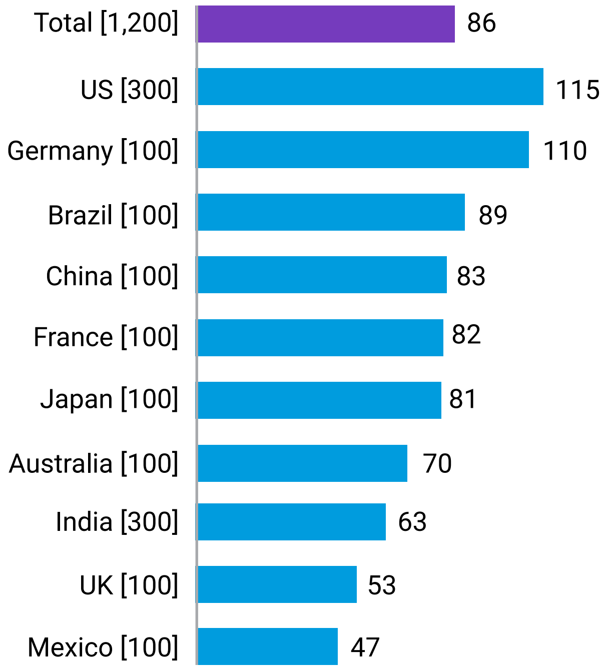


Fig.1: How many ransomware attacks has your organization been targeted with in the last 12 months (regardless of whether they were successful or not)? [1,200], only showing the average number of attacks over the past 12 months, split by country.

Considering that the US is among the two countries least likely to have implemented segmentation across more than two mission-critical business areas (Figure 2), its top ranking in ransomware attacks and its low ranking in deployment of segmentation could be related.

Of course, the high number of ransomware attacks in the US is likely attributable to a range of factors, including the newsworthiness of major breaches like the one a Russian cybercrime group committed against federal agencies in 2023 and the US's proliferation of IoT devices (2 billion more than second-place China). Ransomware for IoT (R4IoT) exploits vulnerable IoT devices, such as IP cameras, to gain an initial foothold then moves laterally in an IT network, taking advantage of poor security practices to hold mission-critical processes hostage.

Ransomware attacks are not only more frequent globally in 2023 vs. 2021 but their impacts are more successful (Figure 3), with our respondents indicating increases in network downtime, data loss, and reputational damage – all of which significantly raise the stakes for security teams. We see the effect of this pressure also in terms of strategy: The number of organizations that are continuously updating cybersecurity strategies or policies has increased from 5% in 2021 to 13% 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.

Those who have segmented more than two assets/areas by country

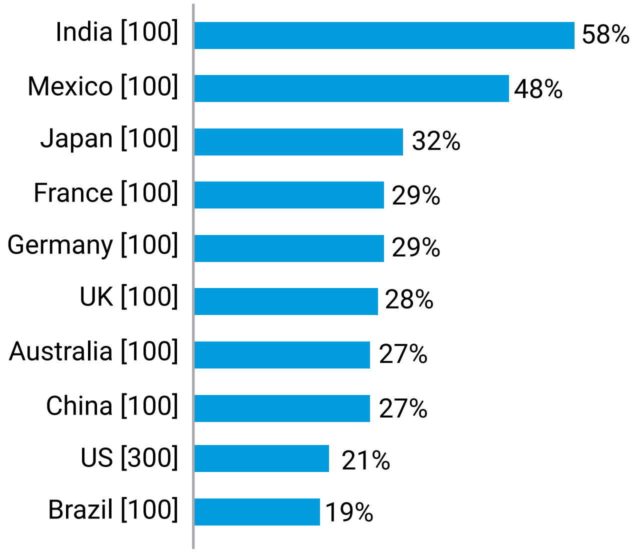


Fig. 2: For each of the following IT security measures, what assets, if any, are they covering? [1,200], showing responses for segmentation security measure only, and percentages that are using segmentation for protecting key assets, split by country.

Impact of ransomware/cyberattacks

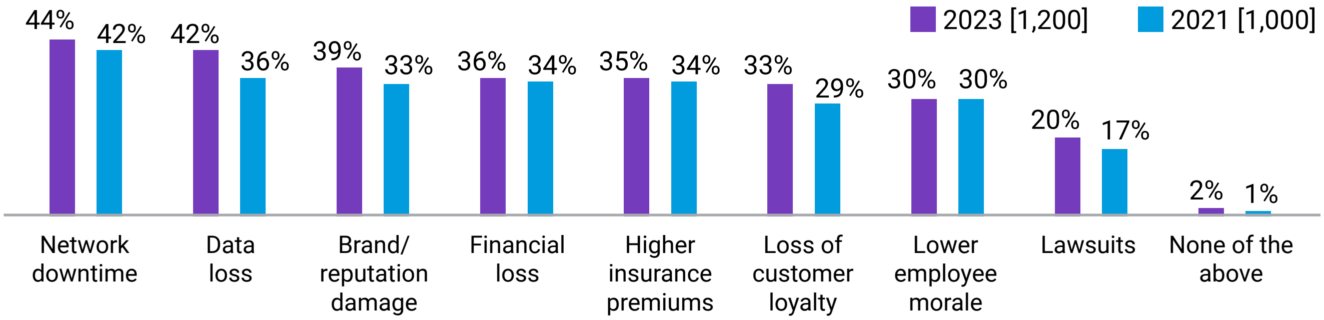


Fig. 3: When your organization has previously detected ransomware or some other cyberattack, which of the following impacts has it had on your organization? [Base sizes in chart], not showing all answer options, split by historical data.

Regional takeaways

Cyberattackers are more likely to target those in the Americas: The total number of ransomware attacks is highest in the Americas, with 96 attacks on average over the last 12 months, compared to 83 in EMEA and 75 in APAC.

Segmentation and microsegmentation are viewed as more important in APAC and Americas than in EMEA: IT security teams and decision-makers in APAC (62%) and the Americas (60%) are more likely to say network segmentation is extremely important to ensuring their organization is secure than those in EMEA (53%).

Those in the Americas are more likely to say microsegmentation is the top priority (41%) than counterparts in APAC (35%) or EMEA (23%).

Those in EMEA are more likely not to have segmented at all: Organizations are far more likely to say no business critical assets have been segmented in EMEA (10%) than in APAC (4%) or the Americas (1%).

The slowest rates of deployment, that is, those with no areas segmented, were seen in the UK (23%), with legacy equipment reported as the main obstacle (46%).

Organizations in APAC have segmented the most: Organizations in APAC are more likely to have segmented more than two business-critical assets (36%) than those in EMEA (29%) or the Americas (26%).

Organizations, in all regions, experience challenges: 97% of those in the Americas say they encounter issues when segmenting their network. A similar amount said the same in EMEA (94%) and APAC (97%).

Those in EMEA and APAC both cite lack of skills/expertise (38% and 43%) as their greatest segmentation obstacle. For those in the Americas, the greatest obstacle is increased performance bottlenecks (41%).

More organizations in the Americas view their Zero Trust security frameworks as mature: Those in the Americas are more likely to say their Zero Trust deployment is fully complete and defined (49%) than APAC (35%) or EMEA (33%).

Segmentation broadly recognized as important part of Zero Trust

Our respondents agree that segmentation is important to ensuring their organization is secure, particularly in addressing malware. Across industries, 93% believe it is critical to help thwart damaging attacks, a number that rises to 99% for those in manufacturing and production. This could be due to the fact that those industries rely heavily on a number of third parties in their supply chain, so a disruption can have massive cascading effects on the business.

Segmentation also contributes majorly to a Zero-Trust framework. When citing why their organization began a segmentation project, the third-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 only two in five (40%) report their Zero Trust framework as being fully defined and complete.

Globally, a majority of respondents aspire to go further and implement microsegmentation, which protects application workloads at a granular level: 89% say microsegmentation is at least a high priority, with 34% naming it as their top priority. Furthermore, 97% of IT security teams and decision-makers report that it has been adopted by at least a minority of their industry. This number drops to 80% for those in the public sector (excluding healthcare) — a difference that may be attributable to tighter budgets and legacy infrastructure posing greater obstacles to deploying microsegmentation's workload-level protection.

Microsegmentation

of IT security teams and decision-makers report microsegmentation has been adopted by at least a minority of their industry

But the public sector stands to benefit greatly from implementing advanced security techniques like microsegmentation. Because systems in this sector are not necessarily designed to interact with one another, they lack interoperability, which increases both the likelihood of human error and likelihood of a successful cyberattack.

At the segmentation level, 15% of public sector respondents report having no segmentation — even though 93% recognize its importance. This represents the lowest deployment level by sector, with the greatest obstacle being compliance requirements (52%).

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 divides a network into segments at the individual workload level so that security controls and service delivery can then be defined for each unique segment.

Deployments are slow, but persevering 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 30% of organizations have segmented across more than two critical business areas in 2023 (compared to 25% in 2021), and 44% started a network segmentation project two or more years ago, suggesting efforts have stalled.

Critical business areas

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

Slow deployments are most clearly explained by the top obstacles encountered by respondents: lack of skills/expertise for segmentation (39%), increased performance bottlenecks (39%), and compliance requirements (38%; Figure 4). Almost all of those surveyed, no matter the sector, industry, or country, reported the same obstacles to slightly different extents. It's worth noting that while a lack of skills/expertise is the number one cause of 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.

Despite slow progress, rates of segmentation are gradually increasing overall. The percentage of organizations with segmented business-critical applications/data rose 12% and segmented servers rose 8% from 2021 to 2023.

Obstacles encountered when segmenting the network

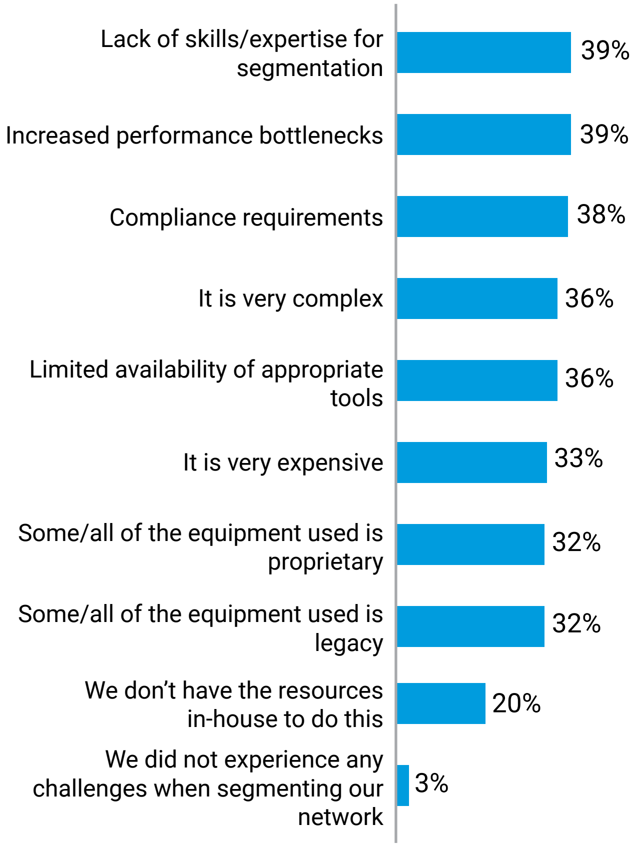


Fig. 4: What problems, if any, did your organization encounter/ does your organization foresee when segmenting the network? [1,187], only shown to those who have segmented their network at some point, not showing all answer options.

The takeaway: Segmenting six critical business areas hugely reduces risk

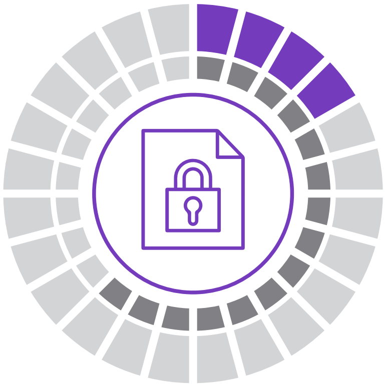
Protecting and segmenting more assets immediately makes organizations more secure. Security teams are more able to identify attacks and can respond far more effectively. The implementation of immature or ill-defined segmentation strategies only likely increases an organizations risk — but when done right, segmentation is clearly worth all it takes to overcome obstacles and implement.

Our findings show that after a breach, recovery happens 11 hours faster with segmentation. Doing the math: For those who have implemented segmentation across six mission-critical areas, it takes an average of four hours to completely stop a ransomware attack; for those with segmentation against only one asset, it's 15 hours.

Similarly, segmentation shaves off 11 hours when limiting 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 11 hours makes to your team and to containing costs and brand damage in either scenario.

To stop an attack

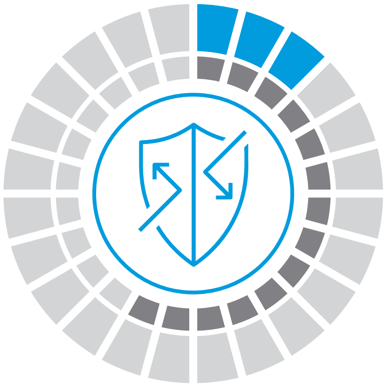


4 hours

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: **15 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 makes it 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 your new segments or worry about where your 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 since the solution uses its own proprietary driver for policy enforcement, it works seamlessly across machines and operating systems: from bare-metal servers to multicloud deployments, from legacy tech like Windows Server 2003 to the latest IoT/OT devices and containerized technology. This means you're only managing one 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

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 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 it eases compliance

Many of our customers deploy our solution to ensure and attest compliance with a number of domestic and international compliance mandates, such as PCI-DSS, SWIFT, Sarbanes-Oxley, HIPAA, GDPR, and many more. These compliance 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.

Our survey group

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 during 2023. These findings give us insight into how security strategies have changed since 2021, and where progress still needs to be made.

We surveyed security personnel and decision-makers from the US, Mexico, Brazil, the UK, France, Germany, China, India, Japan, and Australia. All worked for organizations with more than 1,000 employees, and they represented a balanced range of industries and sectors.

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.

Learn more about Akamai Guardicore Segmentation

Akamai protects your customer experience, systems, and data by helping to embed security into everything you create — anywhere you build it and everywhere you deliver it. Our platform's visibility into global threats helps us adapt and evolve your security posture — to enable Zero Trust, protect apps and APIs, and secure your infrastructure — giving you the confidence to continually innovate, expand, and transform what's possible. Learn more about Akamai's security, compute, and delivery solutions at akamai.com and akamai.com/blog, or follow Akamai Technologies on Twitter and LinkedIn. Published 10/23.

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.