Akamai

EBOOK

The State of Segmentation

Overcoming deployment obstacles proves to be transformational

Ecommerce sector

Table of contents

Introduction

IT security teams — especially those defending ecommerce organizations — have never had it easy. Traditionally tighter budgets and limited security resources have meant enterprise defenders having to do more with less. But now, highly motivated and sophisticated attackers, combined with managing an increasingly complex infrastructure, are putting security teams under greater pressure to mitigate risk than ever before. Ecommerce organizations rely on a performant online presence to operate, so one successful breach — like a ransomware attack — could cause extensive, if not irreparable, harm to brand reputation and revenue. Imagine the damaging impact if online operations, order fulfillment, or production lines came to a halt as critical servers and systems became unavailable due to a mass encryption — and possible double extortion via data exfiltration — event.

As the findings in this State of Segmentation for ecommerce report show, these attacks are also having a greater impact, raising the stakes for leaders to choose the right tools and solutions that help keep critical data safe, without sacrificing performance or adding operational overhead. According to the report, ecommerce is the most targeted industry sector of all survey respondents, highlighting the urgency to prevent, detect, and respond as quickly as possible to a ransomware attack in order to contain the fallout.

Respondents in ecommerce sector organizations (representing all regions, including the U.S., LATAM, EMEA, and APAC) agree overwhelmingly on the effectiveness of segmentation in keeping IT assets protected, but overall progress in deploying it around critical business applications, servers, and systems is lower than expected. The main obstacles for ecommerce organizations have been a lack of expertise to deploy segmentation effectively, coupled with burdensome data compliance requirements. This shows that not only are teams struggling to recruit or retain the necessary talent to their industry, they may also find that precious time is being spent trying to ensure compliance with legislation, further consuming already-strained resources.

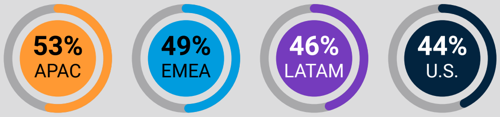
The good news? Perseverance — and choosing the right solution — pays off. For those who had successfully segmented most of their critical assets across six key areas, segmentation proved to have a transformative effect on defensive capabilities, enabling them to mitigate and contain ransomware 11 hours faster than those with only one asset segmented. Imagine the difference those 11 hours can make not only for your incident responders, but also your customers and brand reputation.

Segmentation has progressed slowly overall, but those who persevere 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 improving security and to reduce risk associated with flat networks. It has also been used to help reduce the scope, cost, and difficulty of achieving and maintaining PCI compliance for ecommerce-driven organizations.

Microsegmentation is a software-defined security technique that logically divides a network into distinct security segments down to the individual workload or process level (Layer 7). Security controls and service delivery can then be defined for each unique segment at a more granular level when compared to traditional segmentation methods such as VLANs, ACLs, and internal firewalls that only offer Layer 4 control. That's why 94% of ecommerce respondents prefer software-based segmentation solutions over traditional methods.



Security decision-makers in APAC are more likely to say network segmentation is extremely important to ensuring their organization is secure than those in EMEA, LATAM, or the U.S. Those in LATAM are more likely to say microsegmentation is the top priority (42%) than counterparts in APAC (35%), the U.S. (34%), and EMEA (26%).

Ecommerce is the most targeted industry, and ransomware attacks continue to rise

The number of ransomware attacks in ecommerce organizations (both successful and unsuccessful) is, on average, 167 in the previous 12 months. Not only does this put ecommerce at the top of the list for the number of average ransomware attacks, it is about double that of the sector closest behind (construction — average of 89 attacks).

Cyberattackers are more likely to target ecommerce organizations in the U.S.: The number of ransomware attacks in the U.S. is the highest amongst all regions, with 312 attacks on average over the past 12 months, compared to 119 in APAC, 91 in EMEA, and 68 in LATAM (figure 1).

Average number of ransomware attacks in ecommerce organizations over the past 12 months by region

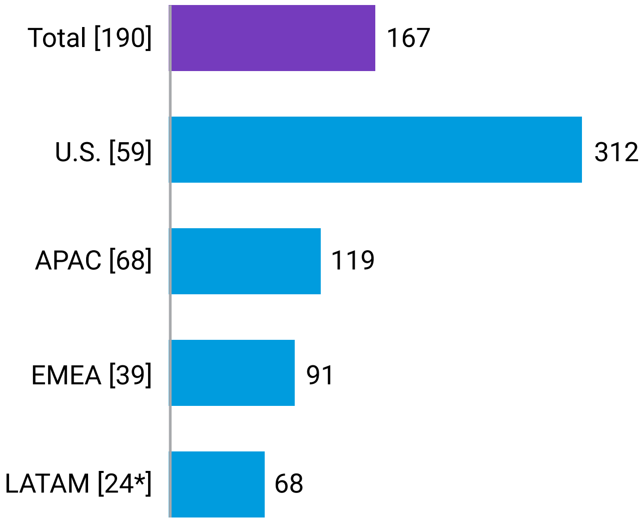


Fig. 1: How many ransomware attacks has your organization been targeted with in the past 12 months (regardless of whether they were successful)? Chart shows the average number of attacks over the past 12 months, split by region, ecommerce sector data only.

* Caution – low base size under 30

Although the averages in the regions outside the U.S. could not be described as low, they are dwarfed by the number of attacks that focus on the U.S. Having the world's largest economy, the U.S. is the most targeted country by ransomware gangs, and attackers frequently set their sights on other English-speaking and western countries. Geopolitical motivations also play a role in which countries and sectors are hardest hit. Ecommerce organizations are often caught in the crosshairs as they traditionally have less security maturity when compared to other industries like financial services, making them a softer target. Adding to the pressure, a successful ransomware attack can be highly public, especially if organizations are hit during critical revenue-generating periods such as holidays, festivals, sporting events, back to school, or other peak shopping events, making a payout more likely — in the attacker's mind — if operations are disrupted.

Despite the high number of ransomware attacks that ecommerce organizations are being targeted with, there is a disappointing level of segmentation being implemented. Only 11% of these organizations have segmented more than two areas, a figure broadly consistent across all regions. This indicates that many of these organizations may have limited resources beyond what is required to deal with problems and attacks as they arise.

Ransomware attacks in the ecommerce sector can have huge and immediate impacts upon the business (figure 2), with our respondents indicating financial loss and reputational damage — both of which significantly raise the stakes for security teams in ecommerce organizations. Increases have also been seen in the proportion of respondents reporting higher insurance premiums. This demonstrates the level of risk that ecommerce organizations can carry, often holding personal data on individuals and their shopping habits, in addition to the risks related to logistical issues with stock or warehousing.

Impacts can vary by region: APAC respondents are particularly likely to highlight financial loss, with more than half (51%) doing so, compared to the overall average of 42%. U.S. respondents, however, are most likely to report network downtime, with nearly half (49%) doing so, compared to the overall average of 39%. EU respondents are more likely to report lower employee morale as an impact (41%, compared to the overall 36%).

We also see the effect of this pressure in terms of strategy: The number of ecommerce organizations that are continuously updating cybersecurity strategies or policies has increased from 3% in 2021 to 13% in 2023, not only in response to ransomware but to a constantly changing attack surface. Increasing complexity of infrastructure as workloads migrate to the cloud are just some of the risk factors affecting security strategies — and security teams — on a daily basis.

Impact of ransomware/cyberattacks upon ecommerce organizations

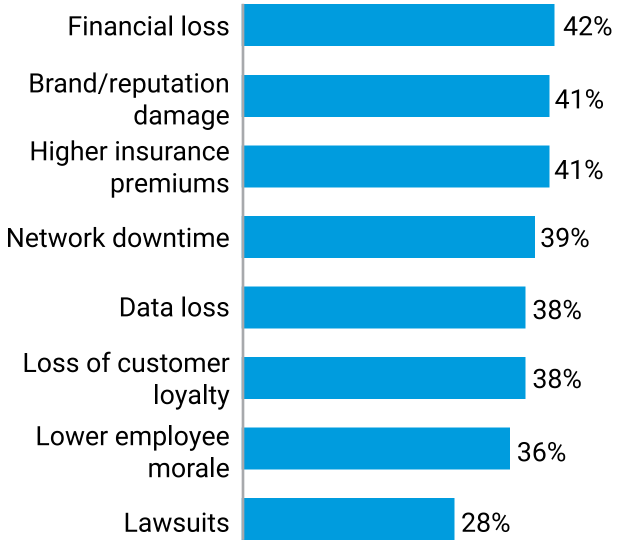


Fig. 2: When your organization has previously detected ransomware or some other cyberattack, which of the following impacts has it had on your organization? Chart does not show all answer options, ecommerce sector data only.

Segmentation broadly recognized as important part of Zero Trust

Our respondents agree that segmentation is important to ensuring their organization is secure, and particularly in addressing malware.

Nearly half (48%) state that segmentation is extremely important, and 89% believe it is critical to help thwart damaging attacks.

Segmentation is also acknowledged as a cornerstone of a Zero Trust security framework, and the good news for ecommerce organizations is that progress has already been made in this area. All are deploying or have already deployed a Zero Trust security framework (100%), although only just over two in five (42%) report their Zero Trust framework as being fully complete and defined, and considered mature. This, therefore, is an area where segmentation can help ecommerce organizations advance their journey to Zero Trust. Based on the data, organizations in the U.S. are far more mature when it comes to their Zero Trust security framework deployment: They are far more likely to say their Zero Trust deployment is fully complete and defined (63%), vs. LATAM (46%), APAC (32%), and EMEA (23%).

Reasons for beginning a network segmentation project varied significantly by region, with a government focus on cybersecurity rising to the top at 41%. LATAM and countries within the EU both listed high-profile zero-day vulnerabilities as the top drivers for pursuing a segmentation initiative (by 44% and 42%, respectively). But respondents in the EU are far more likely to also report that projects started because it is best practice (41%, compared to the overall 22%). The U.S. and APJ respondents, however, are more likely to say that they started because of their government's focus on cybersecurity (41% and 39% respectively, compared to the overall 35%). APJ respondents are also more likely to say that moving critical applications to the cloud was what made them begin a project (39%, compared to the overall 32%).

A majority of respondents in ecommerce organizations aspire to go further and implement microsegmentation, which protects application workloads at a granular level: 92% say microsegmentation is at least a high priority, with 34% naming it as their top priority. Furthermore, all (100%) IT and security decision-makers in this sector report that it has been adopted by at least a minority of their industry, emphasizing that it is a solution that all at least have broad awareness around, even if progress has been limited to date.

Respondents also note that gaining more visibility across the organizations' IT environment was needed. Those in LATAM state they need "a lot more" visibility (63%) — followed by APAC (56%), the U.S. (46%), and EMEA (44%) — into network communications, asset locations, etc., to reduce risk.

Deployments are slow, but perseverance yields transformative results

The harsh reality is that even with such broad agreement that segmentation is the key to stopping attacks by protecting IT assets, segmentation deployment has been slow — perhaps slower than expected.

Only 11% of ecommerce organizations have segmented across more than two critical business areas, and 48% 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 are most clearly explained by the top obstacles encountered by respondents: lack of skills/expertise for segmentation (40%), compliance requirements (40%), and increased performance bottlenecks (38%) — all associated with traditional segmentation methods. It's worth noting that while a lack of resource or 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.

Ecommerce organizations, in all regions, experience challenges: 100% of those in the U.S. and in LATAM say they encounter issues when segmenting their network. Nearly as many say the same in APAC (99%) and in EMEA (97%).

However, when broken down by region (figure 3), there is variation in the obstacles most likely to be encountered. This shows that certain issues (e.g., lack of skills, compliance) may be driven as much or more so by local issues than they are by global issues.

Those in EMEA and LATAM both cite lack of skills/expertise (both 54%) as their greatest segmentation challenge. For those in the U.S., the greatest challenge is increased performance bottlenecks (44%), and in APAC, it's compliance requirements (43%) that are most likely to be the problem.

	Most likely experienced problem	Second and third most likely experienced problem	
U.S. [59]	Increased performance bottlenecks (44%)	Compliance requirements / Limited availability of appropriate tools (both 41%)	
LATAM [24*]	Lack of skills/expertise for segmentation (54%)	It is very complex (46%)	Some/all of the equipment used is proprietary / Some/all of the equipment used is legacy (both 38%)
EMEA [39]	Lack of skills/expertise for segmentation (54%)	Limited availability of appropriate tools (41%)	Compliance requirements / Some/all of the equipment used is legacy / It is very expensive (all 36%)
APAC [67]	Compliance requirements (43%)	Limited availability of appropriate tools / Some/all of the equipment used is proprietary / Increased performance bottlenecks (all 37%)	

Fig. 3: What problems, if any, did your organization encounter/does your organization foresee when segmenting the network? Chart shows those who have segmented their network at some point, showing top three selected answers by region, ecommerce sector data only.

* Caution – low base size under 30

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

Protecting and segmenting more assets across the ecommerce environment immediately makes organizations more secure. With the right solution, security teams are able to identify attacks faster, thereby improving the mean time to detect (MTTD) and the mean time to respond (MTTR) to an incident. However, under-segmentation of assets — typically a result of using legacy segmentation technologies — can create security gaps and blind spots, leaving the organization in a more vulnerable or reactive position. But when done right, segmentation via a software-defined approach can help organizations better manage their attack surfaces to keep critical assets protected in a more efficient, cost-effective manner.

Our findings show that after a breach, recovery happens 11 hours faster with segmentation.
Doing the math: For those ecommerce organizations 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 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 cost 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 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 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 multicloud deployments, from legacy tech like Windows Server 2003 and Windows XP to the latest POS systems, IoT/OT devices, and even 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 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. The time and effort spent having to manually segment business areas then manually troubleshoot 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 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 segmentation streamlines compliance

Many of our customers deploy our solution to ensure and attest compliance with a number of country-specific 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 — like the cardholder data environment (CDE) for PCI DSS — is separated and protected 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 compliance mandates by physically showing that in-scope data is not being accessed by unauthorized users, systems, 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 lateral movement and allows incident responders to react faster during an active attack. And after a breach, recovery efforts are secured and take less time to complete.

Choosing a software-defined solution that's designed to overcome the common challenges associated with a traditional 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.

Our survey group

For the purposes of this report, we analyzed 190 respondents working in the ecommerce sector (59 in the U.S., 39 in EMEA, 68 in APAC, and 24 in LATAM).

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 from a 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, workforce, 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, 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 cloud computing, security, and content delivery solutions at akamai.com 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.