Akamai

EBOOK

Overcoming Deployment Obstacles to Protect Energy, Oil, and Gas Systems

Global state of segmentation report

Table of contents

Introduction — 2

Segmentation has progressed slowly overall, but those who've persevered have hugely reduced their risk — 3

Segmentation accepted as cornerstone of Zero Trust — 6

Deployments are slow, but perseverance yields transformative results — 7

How a software-based microsegmentation solution helps solve challenges — 8

Persevere with the right solution and support to transform your security posture — 9

Takeaways — 10

Our survey group — 11

Introduction

IT and OT security departments have historically encountered significant challenges, but in the energy, oil and gas, and utilities sector in general, the pressure becomes even more pronounced due to the critical nature of utilities in relation to populations. Frequently, regional conflicts, political pressures, and ideological disputes exacerbate the difficulties and heighten the dangers faced by this industry. However, as attackers become more sophisticated and combine techniques to present larger and more frequent threats, the security teams of energy organizations are under unprecedented pressure. Without online-connected systems, or systems connected to its private OT networks, it is impossible for an energy organization to operate, and a single successful breach can result in significant harm to the organization's reputation and financial performance.

This report's findings indicate that the repercussions of these attacks are intensifying, thereby increasing the burden on security executives to select appropriate solutions that ensure the security of the entire environment while preserving performance.

In contrast, regulatory agencies and governments across the globe are currently formulating security guidelines and regulations in response to the substantial increase in cybersecurity threats encountered by this sector and the critical nature of the services it provides. Energy corporations are obligated to adhere to regulatory standards and guarantee the upkeep and security of their services.

Respondents in energy sector organizations (representing 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 energy organizations has been increased performance bottlenecks, which suggests that teams might be hesitant to embark on a project that could disrupt performance, without assurances that it won't. It is crucial to bear in mind that, given the vital nature of the services rendered to the public by these organizations, disruptions in the functionality of the solutions may result in harm to customers or jeopardize the safety of their maintenance staff.

Conversely, the energy sector is expected to place a greater emphasis on segmentation than the majority of other industries do, indicating that its value is undoubtedly acknowledged.

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. This granular approach to security allows for more precise control over access and protection of sensitive data. By implementing microsegmentation, organizations can limit the impact of a security breach and better protect their network from advanced cyberthreats. Overall, the combination of segmentation and microsegmentation provides a comprehensive security strategy that is essential for safeguarding critical assets in today's complex and dynamic threat landscape.

Ransomware attacks continue to rise, as does their impact

The number of ransomware attacks (both successful and unsuccessful) in energy organizations has increased notably in the past two years, from 37 on average in 2021 to 62 in 2023, and there is no reason to suspect this growth will not continue in the short term. The impacts can have detrimental effects on the population and economies, including power outages or infrastructure damage leading to lost company credibility, theft of business and personal details, or even risk to people's lives. With the increasing frequency and severity of ransomware attacks, it is crucial for energy organizations to protect their systems and data. Failure to do so not only puts the organization at risk, but also jeopardizes the safety and security of individuals and communities that rely on these services. As ransomware attacks become more sophisticated, it is imperative for organizations to stay vigilant and proactive in their defense strategies to mitigate the potential damage and disruption caused by these malicious threats.

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

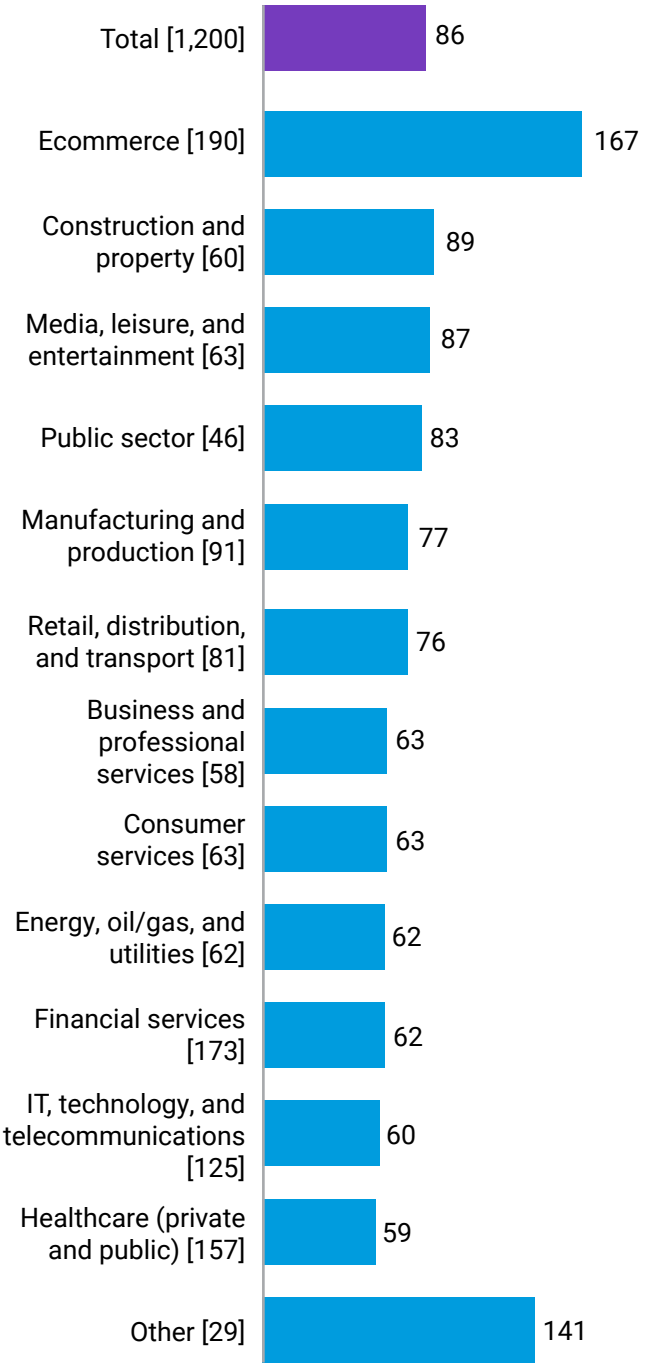

Fig. 1: How many ransomware attacks has your organization been targeted with in the past 12 months (regardless of whether they were successful or not)? Chart shows the average number of attacks over the past 12 months, base numbers split by sector.

One reason for this relatively low number of attacks is that an energy organization's main asset tends to be physical (oil, gas, etc.) rather than digital (money or customer data). They are also not known as being "soft/easy" targets, as some other organizations with relatively few regulations governing them may be, such as media or retail. This means that attacks may be more likely to be driven by political objectives rather than financial objectives. This is potentially supported by the fact that, while only 5% of respondents across all industries overall said that their organization has never detected a cyberattack, this increases to 24% of respondents in the energy sector.

Ransomware attacks within the energy sector were more frequent in 2023 vs. 2021, but the severity of their impacts tell a more mixed story (figure 2), with our respondents indicating a notable increase in data loss, but declines in all other issues. This broad trend may be driven by the increasing awareness of the value of data (which is therefore prioritized as a target by hackers), but may also be due to improvements in approach within the energy sector. The number of energy organizations that are updating cybersecurity strategies or policies on at least a weekly basis increased from just 2% in 2021 to 23% in 2023. With global events (principally related to conflict or climate change) making countries look more closely at their energy security, it's no surprise to see energy organizations increasing their focus on their cybersecurity strategies.

Impact of ransomware/cyberattacks within the energy sector

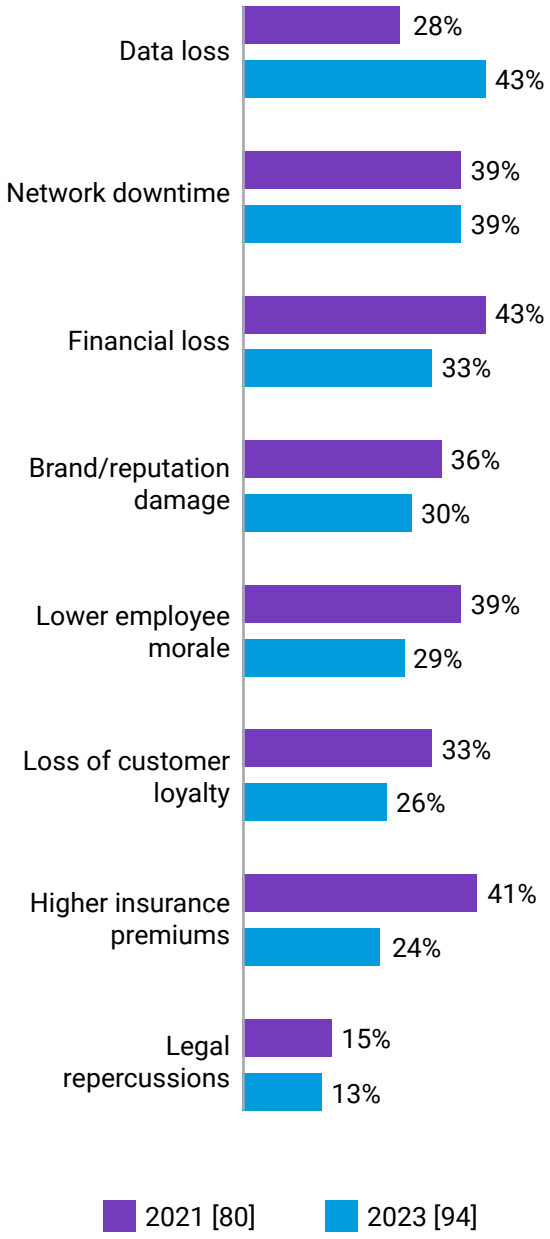

Fig. 2: When your organization has previously detected ransomware or some other cyberattack, which of the following impacts has it had on your organization? Chart shows base sizes by year, not showing all answer options, split by historical data, energy sector data only.

Segmentation broadly recognized as important part of Zero Trust

Our respondents within the energy sector agree that segmentation is important to ensuring their organization is secure, and particularly in addressing malware. Sixty-six percent (among the highest of all sectors) state it's extremely important, and 95% believe it is critical to help thwart damaging attacks.

Segmentation also contributes significantly to a Zero Trust framework, and the good news for energy organizations is that progress has already been made in this area. All (100%) are deploying or have already deployed a Zero Trust security framework, although fewer than half (46%) report their Zero Trust framework as being fully complete and defined, and therefore mature. This therefore is an area where segmentation can help energy organizations on their journey to Zero Trust. This is the result of the survey for organizations' IT environments, although the OT environment may be different due to the technologies used.

A majority of respondents in energy organizations 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 47% naming it as their top priority. Across all sectors, only 34% report microsegmentation as their top priority, demonstrating that energy sector organizations are more likely, on average, to be pushing for this to be rolled out as soon as possible. Furthermore, nearly all (98%) 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 has broad awareness.

Deployments are slow, but perseverance yields transformative results

The harsh reality: Even with such broad agreement that segmentation is the key to stopping attacks, segmentation deployment has been slower than expected. Only 38% of energy sector organizations have segmented across more than two critical business areas in 2023 (compared to 30% in 2021), and 33% 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 (49%), compliance requirements (43%), and proprietary equipment (41%, figure 3).

Obstacles encountered when segmenting the network in the energy sector

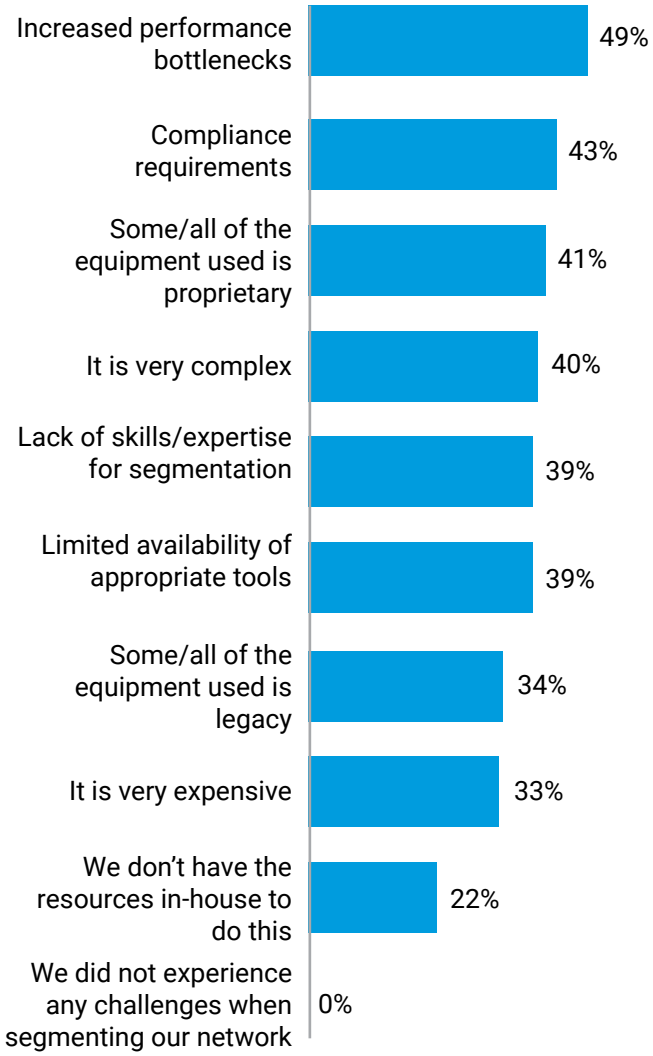

Fig. 3: What problems, if any, did your organization encounter/does your organization foresee when segmenting the network? Chart shows base size of 94, only shown to those who have segmented their network at some point, not showing all answer options, energy sector data only.

An encouraging fact for the energy sector, however, is that 42% report that their network segmentation project began as a result of a recommendation by leadership/a board of directors. This is the highest of all sectors (overall average is 28%) and demonstrates that segmentation is clearly recognized as important in this sector.

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 implies that you are only managing one solution with a single interface to view and manage connections made by various operating systems and devices throughout your entire environment, regardless of their physical location.

It is important to note that the Akamai Guardicore Segmentation solution can also be used in OT environments, allowing microsegmentation to be applied to private control networks, legacy operational systems, and agentless IoT devices.

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 or OT 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 domestic and international compliance mandates, such as PCI DSS, SWIFT, Sarbanes-Oxley, HIPAA, GDPR, LGPD, 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. In the case of a breach happening, recovery efforts are safe and take less time to complete, since the impact should be limited to the affected segment only.

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

Segmentation and microsegmentation is more important in the energy sector than many other sectors: IT, IT security, and OT decision-makers in energy sector organizations (66%) are more likely to say network segmentation is extremely important to ensuring their organization is secure than those in consumer services (36%), but less likely than those in IT and technology (73%).

Those in the energy sector are much more likely to say microsegmentation is the top priority (47%) than counterparts in consumer services (12%), and only slightly less likely than those in the public sector (48%).

Those in the energy sector are among the least likely to have not segmented at all: Energy sector organization respondents are unlikely to say no business-critical assets have been segmented (4%), albeit still more likely than those in the construction, consumer services, and media sectors (all 0%), but less likely than those in the public sector (15%).

Those in the energy sector are among the most likely to have made the most progress with segmentation: Organizations in the energy industry are only slightly less likely to have segmented more than two business-critical assets (38%) than those in the retail sector (43%) and far more so than those in the consumer services sector (3%).

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 UK, France, Germany, China, Japan, and Australia. They were from organizations with 1,000+ employees, as well as 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.

For the purposes of this report, we analyzed 94 (2023) and 80 (2021) respondents working in the energy 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 at akamai.com 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.