State of Segmentation

Strong Implementations Reap Great Security Rewards

Organizations implementing segmentation across four or more critical assets were able to stop attacks 32% faster than those that segmented none or one critical asset.

Guardicore
Now part of Akamai

Table of Contents

Key Takeaways

96%

96% SAY THEY HAVE SEGMENTED THEIR NETWORK
The large majority of respondents say their organizations are currently using segmentation in their IT security approach.

2%

BUT ONLY 2% PROTECT ALL PROTECT ALL MISSION-CRITICAL ASSETS
Just a fraction of respondents protect all mission-critical assets (critical applications, public-facing applications, domain controllers, endpoints, servers, and business critical assets/data) in their networks with segmentation.

32%

THOSE WHO SEGMENT MORE, REDUCE TIME TO STOP ATTACKS BY 32%
Organizations with segmentation across four or more critical assets report a significantly lower time to stop attacks from laterally moving and stopping the attacks entirely.

92%

AND 92% BELIEVE SEGMENTATION HAS PREVENTED SIGNIFICANT DAMAGE
Nearly all respondents attest that segmentation has prevented cyber attacks on their organization from doing significant damage or stealing substantial amounts of data.

A New Status Quo

The perfect storm of digital transformation, accelerated by the global pandemic, a growing population of increasingly sophisticated and business-driven threat actors, and often outdated security concepts, has challenged the status quo in IT security and has prompted security leaders to explore new strategies to better secure digital assets for organizations of any size.

The old premise of keeping the bad guys out and letting the good guys in via bigger walls at the perimeter has proven it is no longer a sustainable strategy for success.

Organizations implementing segmentation across **4 or more critical assets** were able to **stop attacks 32% faster** than those that segmented none or one critical asset.

Segmentation Is Calling... Are Organizations Answering?

Segmentation enables organizations to protect networks from external and internal threats by inspecting and controlling all traffic, east-west and north-south, with process-level details. In other words, segmentation applies “micro perimeters” around sensitive data assets to prevent lateral movement and ultimately reduce the attack surface.

For these reasons, most organizations (96%) are currently implementing segmentation into their network.

They not only recognize the promised benefits, but also the risks, with 96% of respondents to Guardicore’s study stating that leaving networks unsegmented creates significant risk.

However, most organizations claiming to segment their environments are doing so on a limited scale - only 2% protect all six critical assets, including critical applications, public-facing applications, domain controllers, endpoints, servers, and business critical assets/data, with segmentation.

In this report, we examine the current trends of segmentation to understand:

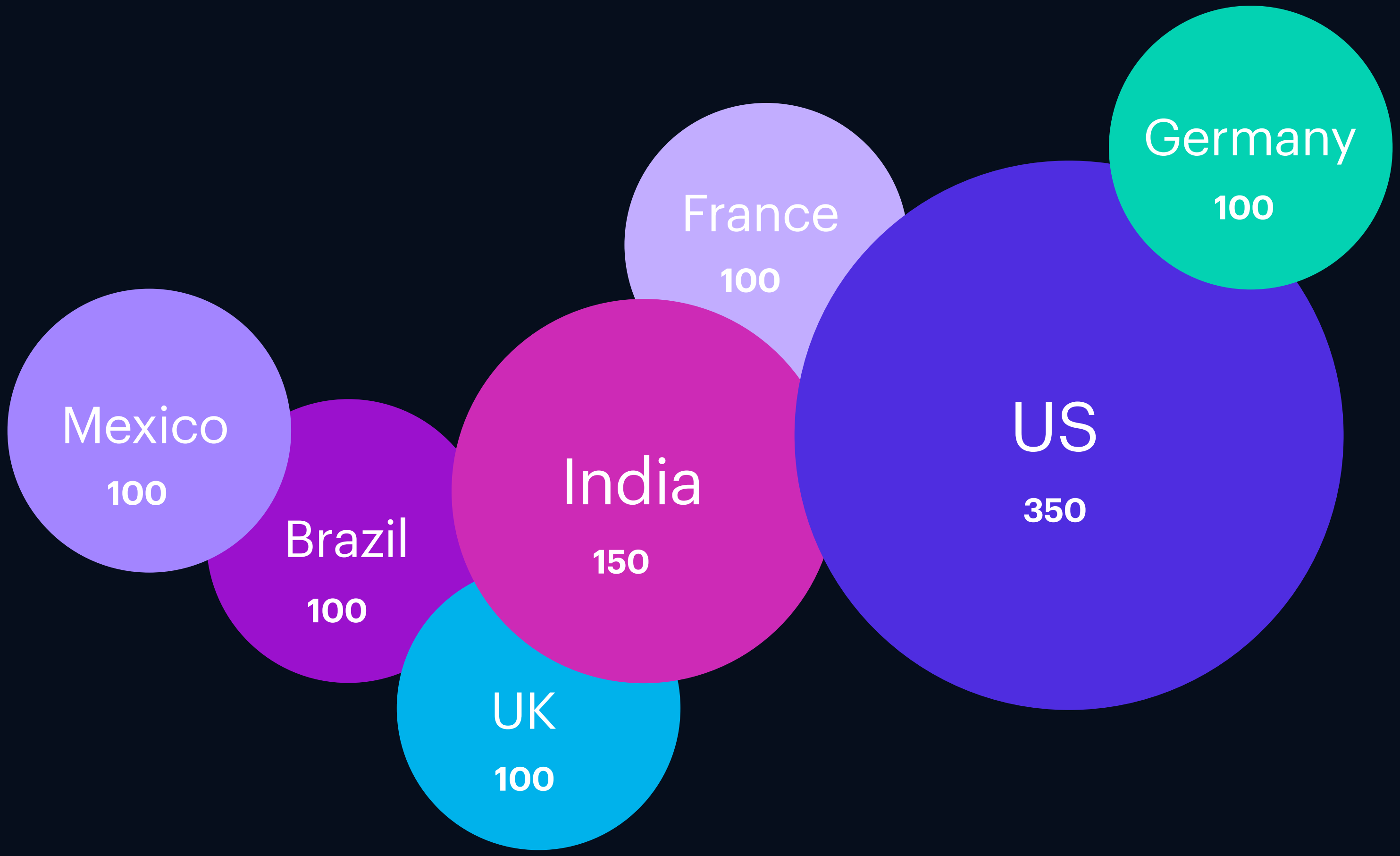
- How does segmentation benefit an organization's security posture?
- What are the risks of leaving networks unsegmented?
- How far are organizations taking segmentation projects?
- Are they proving successful?
- What stands in their way, and what solutions exist to solve those challenges?

Methodology: And The Survey Says...

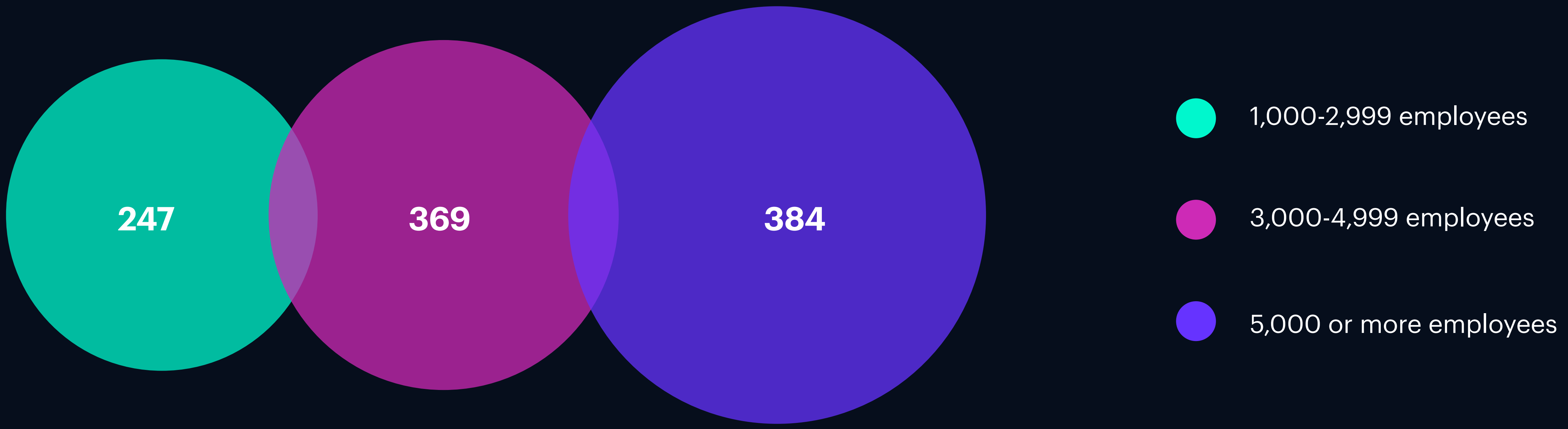
To better understand the state of segmentation within today's enterprises, Guardicore conducted a survey of 1,000 IT security decision-makers in September of 2021.

These individuals are responsible for determining an organization's security approach, how an organization responds to a breach, and which tools and solutions will strengthen its security posture. Uncovering their current security approaches, segmentation strategies, and the cybersecurity threats they face offers insight into how integral a strong segmentation strategy furthers an organization's security posture.

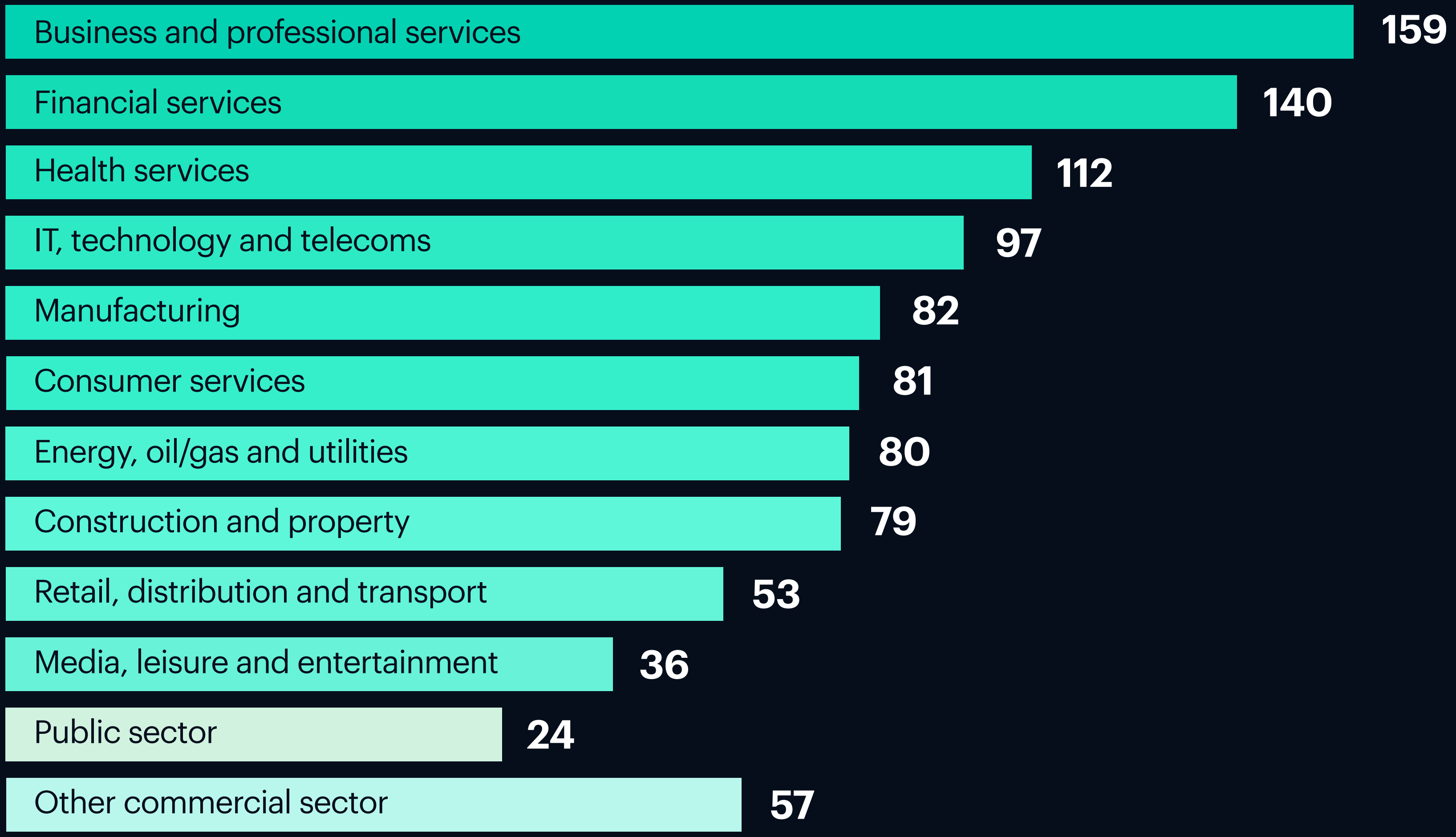
Respondents were predominantly located in the United States; however, given cybersecurity is a global issue, the survey also included respondents from India, Mexico, Brazil, the United Kingdom, France, and Germany.



Different-sized enterprises may face varied cybersecurity risks; therefore, the IT security decision-makers surveyed currently work for enterprises with 1,000-2,999 employees, 3,000-4,999 employees, and 5,000 or more employees.



Finally, respondents represented a range of company industries, including business and professional services, financial services, healthcare, and technology.



4 Key Findings

Based on the data, we've created four key findings on the state of segmentation, to help illustrate how organizations are segmenting their networks, how it benefits an organization's security posture and more.

01

MOST ORGANIZATIONS SEGMENT THEIR NETWORKS TO SOME DEGREE

According to the data, 96% of respondents say their organizations are currently using segmentation in their IT security approach – and for a good reason.

Segmentation is recognized as a critical driver of a Zero Trust architecture.

Security professionals use microsegmentation technologies to limit the ability of malicious attackers to move across data centers and cloud deployments by creating secure zones in hybrid environments down to the workload level without requiring a hardware appliance.

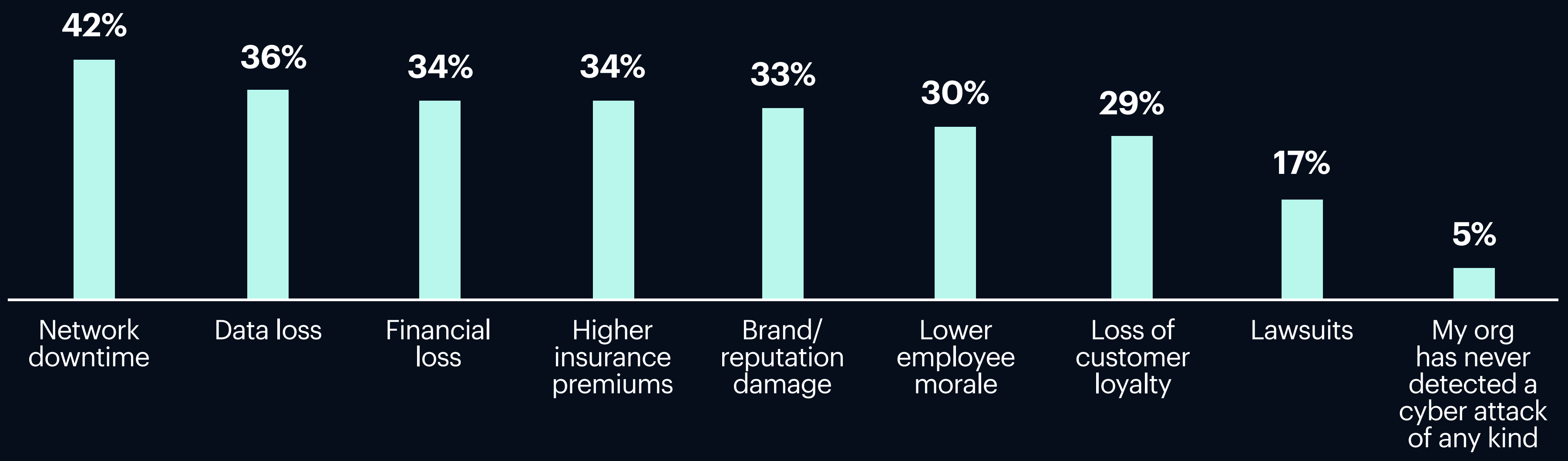
Organizations not only recognize the benefits of segmentation, but they understand the risks as well. 96% of respondents believe that leaving networks unsegmented will lead to more risk.

92% attest that network segmentation has prevented cyber attacks on their organization from doing significant damage or stealing substantial amounts of data.

Further, respondents identified external “attacks spreading more quickly” (49%) and “internal attack ease” (44%) as the most likely risks stemming from unsegmented networks.

A common concern for security organizations today is the risk of ransomware.

As noted by respondents, unsegmented environments are likely much more vulnerable, due to the lack of limitations on lateral movement. Respondents highlight “network downtime” (42%), “data loss” (36%), “financial loss,” and “higher insurance premiums” (both 34%) as significant consequences to a ransomware attack.



02

CURRENT SEGMENTATION STRATEGIES ARE LIMITED IN BREADTH AND DEPTH

Although the data shows that organizations understand the benefits of segmentation, most organizations are not implementing the approach across enough business-critical areas.

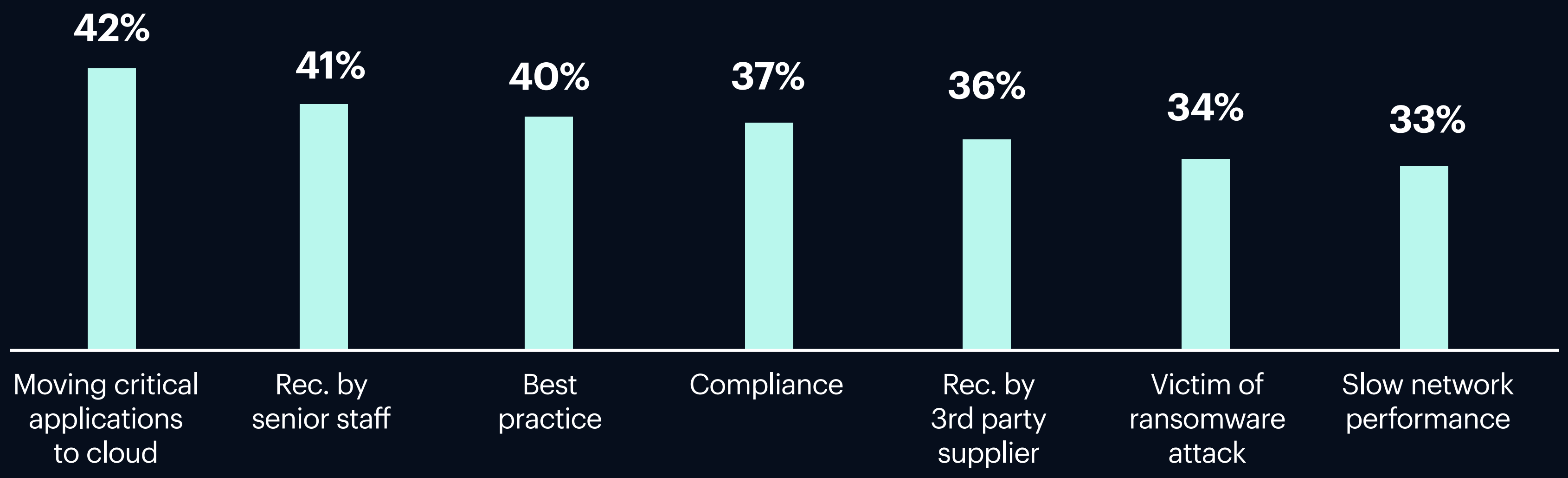
Just 25% of respondents say their organization uses segmentation across more than two critical areas that businesses need to protect.

●	**2%**	All 6 areas segmented
●	**2%**	5 areas segmented
●	**7%**	4 areas segmented
●	**14%**	3 areas segmented
●	**21%**	2 areas segmented
●	**50%**	1 areas segmented
●	**4%**	No areas segmented

MISSION-CRITICAL AREAS

- critical applications
- public-facing applications
- domain controllers
- endpoints
- servers
- business critical assets/data

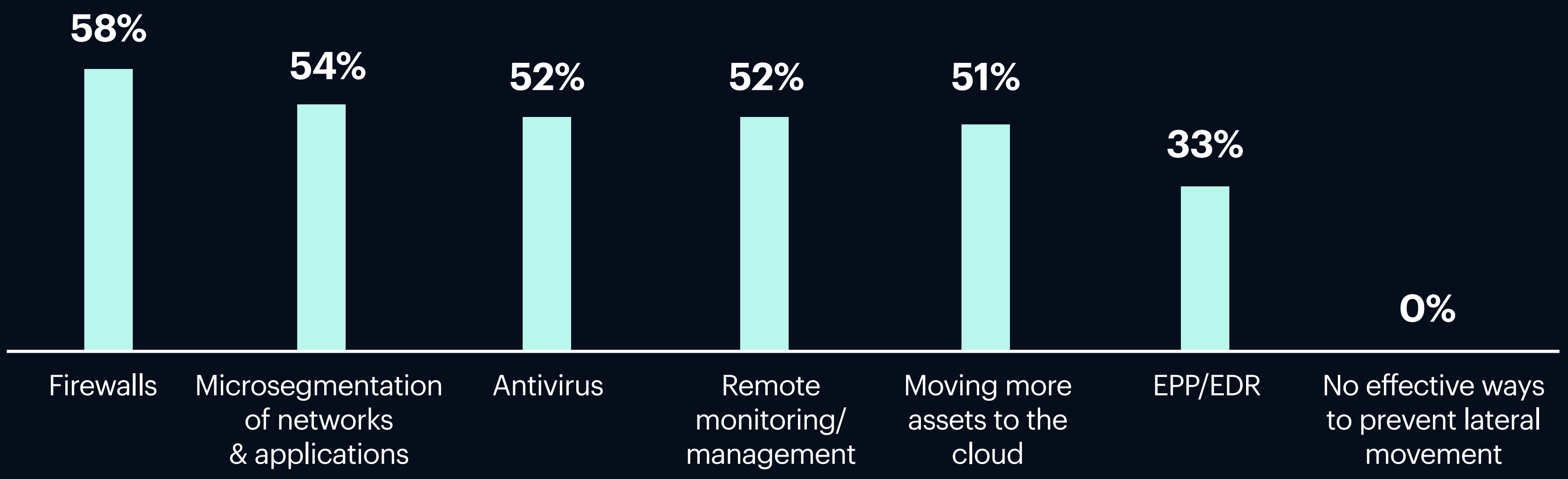
According to the survey, moving critical applications to the cloud (42%) was most likely to be highlighted as a driver for network segmentation overall, followed by recommendations by senior staff (41%). However, 43% also say that network segmentation has not occurred in their organization for at least two years or has never been implemented.



These statistics are meaningful, given the significant and global shift to hybrid cloud environments made by enterprises to adapt to remote working conditions due to COVID-19. Based on the data, it's likely that critical assets added to the IT infrastructure during the pandemic – or any time after the network was initially segmented – may not have been incorporated into any segmentation projects in most organizations.

Many of these organizations have been feeling the repercussions of not correctly segmenting critical assets. According to the survey, organizations faced an average of 43 ransomware attacks in the last 12 months. Further, 14 of those attacks reached the stage of lateral movement, demonstrating that the segmentation protections organizations have in place are not as strong as they could be.

While the effectiveness of segmentation is acknowledged by a significant number of respondents (54%), antiquated security approaches such as firewalls (58%) and antivirus (52%) were ranked similarly. Security leaders view segmentation as one of many approaches, rather than being a 'must-have,' illustrating why organizations have not more widely adopted it.



03

MANY HAVE EXPERIENCED, OR EXPECT TO EXPERIENCE, SIGNIFICANT CHALLENGES IN SEGMENTATION PROJECTS

Most organizations have implemented segmentation using traditional network security tools such as internal firewalls, VLANs, and ACLs. However, with today's dynamic and hybrid data center environments, these conventional approaches are no longer practical as they are slow to adapt to the pace of change, and policy management is increasingly more expensive and complex.

Therefore, it makes sense that 82% of respondents agree that segmenting their organization's network is a huge task.

Nearly all respondents say that their organization experienced at least one problem in the most recent network segmentation project – listing compliance requirements (44%), limited availability of appropriate tools (42%), and complexity (38%) as the most significant barriers to adopting segmentation.

Many turn to software-based segmentation as a key solution to these challenges, as it may reduce complexity and enable more granular control and visibility than what is offered by traditional hardware firewalls.

04

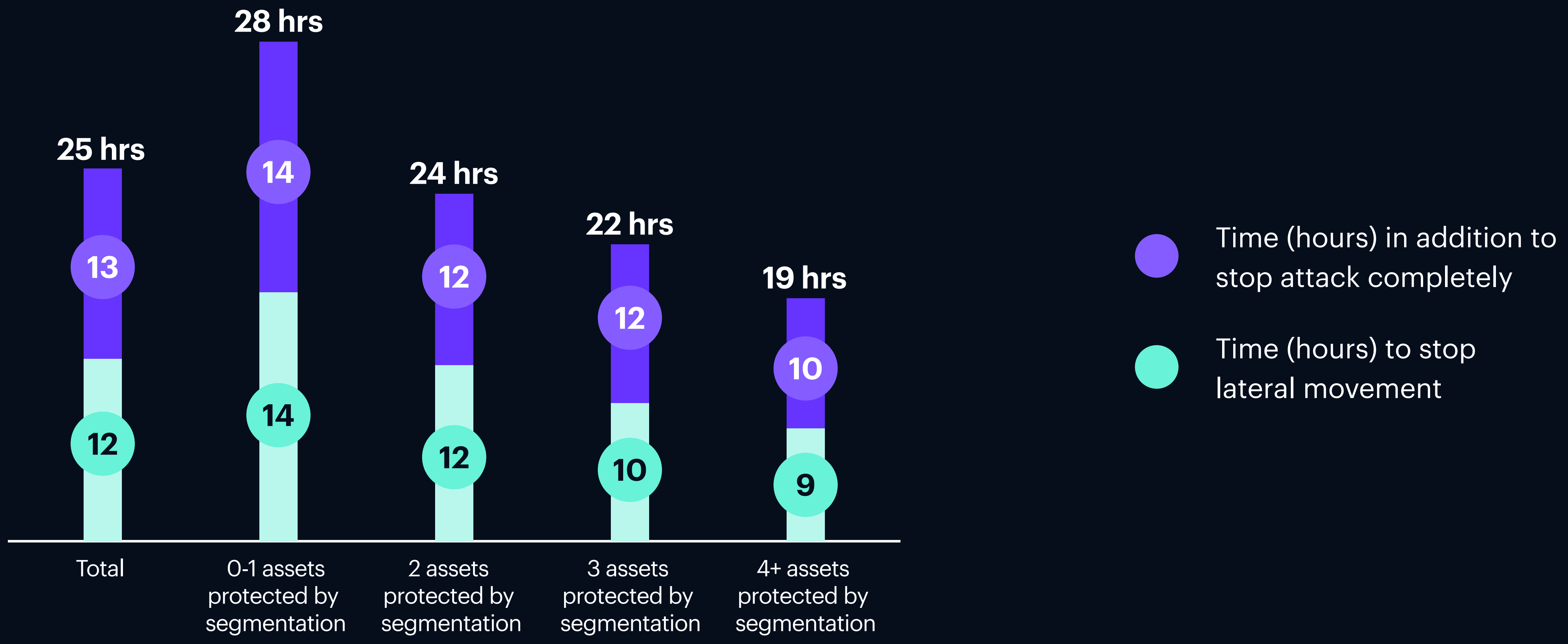
SEGMENTATION, WHEN CARRIED OUT MORE EXTENSIVELY, BRINGS REWARDS

When done right, segmentation (particularly software-based segmentation) allows companies to apply workload and process-level security controls to on-premises and cloud assets that have an explicit business purpose for communicating with each other. It is highly effective at detecting and blocking lateral movement in on-premises, cloud, and hybrid-cloud environments. It ultimately helps organizations move rapidly towards Zero Trust architecture.

Finding #2 highlights that 25% of respondents said their organization uses segmentation across more than two of the critical areas that businesses need to protect – but what about those organizations that used segmentation across all six?

Organizations implementing segmentation across four or more critical assets were able to stop attacks 32% faster than those that segmented none or one critical asset.

The survey shows that increased segmentation across critical assets leads to a reduced average time to stop the attacks. The average time required to limit lateral movement and prevent ransomware attacks entirely is lower on average for organizations with greater use of segmentation to protect their key assets.



New technologies in the field of segmentation allow for micro-segmentation of environments. Unlike regular segmentation, micro-segmentation aims to segment the environment into smaller parts, by using software-based segmentation tools. Solutions that offer this capability often use software-based agents rather than hardware firewalls to allow for more granular network traffic visibility and easy policy configuration, and potentially, a more highly segmented environment.

The Bottom Line

Although widely known and adopted in some form, organizations have a greater opportunity to adopt segmentation more strategically as a vital security practice in their Zero Trust architecture.

Organizations using segmentation extensively experience significant rewards.

Guardicore's data shows that organizations that leverage segmentation increase visibility into their IT environment to prevent more attacks and improve their mean-time-to-remediation (MTTR) compared to the rest of the market. However, despite the benefits, organizations' use of segmentation can be limited and only used in isolated cases and areas. Organizations report that they believe they will face or have faced significant challenges when adopting segmentation. But many of these expected challenges are based upon outdated misconceptions or poorly executed projects.

Guardicore's software based micro-segmentation offers organizations a more agile process to isolate and segment networks and applications that is faster and easier to manage than internal firewalls and VLANs. It is more flexible across on-premises and hybrid cloud environments and enables more rapid implementation of a Zero Trust Security model to protect your most critical applications and data.

Guardicore enables rapid deployment and easy ongoing management of segmentation and micro-segmentation policies in any environment. This allows security teams to move more rapidly to a Zero Trust security posture while also reducing the cost and complexity of ongoing policy management. It also gives your team the ability to consistently enforce segmentation policy across any environment, whether your critical applications and workload are running on legacy systems, bare metal, hypervisors, or public cloud/IaaS.

For more information on how to improve your organization's segmentatuon practices and further your Zero Trust architecture, visit: www.guardicore.com

Learn More →

Guardicore
Now part of Akamai

About Guardicore
Guardicore delivers easy-to-use Zero Trust network segmentation to security practitioners across the globe. Our mission is to minimize the effects of high-impact breaches, like ransomware, while protecting the critical assets at the heart of your network. We shut down adversarial lateral movement, fast. From bare metal to virtual machines and containers, Guardicore has you covered across your endpoints, data centers and the cloud. Our software-based platform helps you become more secure to enable your organization's digital transformation. **Guardicore.com**