The Segmentation Report

Results from Cisco's 2025 Survey

1. Introduction

Segmentation has long been recognized as core to an organization's network security approach because it creates the boundaries that limit the spread of attacks, safeguards critical assets, and provides the visibility needed to manage complex environments.

To better understand enterprises' experiences with segmentation, Cisco® commissioned independent market research specialist Vanson Bourne to conduct a global survey to understand the drivers, challenges, approaches, and the benefits of segmentation.

The research involved surveying 1000 respondents with knowledge of their organization's network security and segmentation practices across the Americas, EMEA, and Asia Pacific.

Key takeaways:

- Segmentation is a high priority for many, but few have fully executed:
  - 79% say that segmentation is a top priority for their organization.
  - Yet only 33% have fully implemented both macro- and micro-segmentation.
  - And 87% agree that their process of segmentation needs improvement—with the biggest challenges being complex environments (54%), lack of visibility (32%), and difficulty identifying legitimate communication flows between systems (32%).
- Critical asset protection and meeting regulatory compliance are common driving factors for implementing segmentation:
  - 57% report protecting high value/critical assets as a driving factor for pursuing segmentation.
  - 55% want to better meet compliance and regulatory requirements.
  - 52% see breach containment as an additional driver.
- Complete segmentation could deliver measurable gains. Implementing both macro- and micro-segmentation strengthens network security, reduces the impact of breaches, and improves operational alignment. Respondents from organizations that have fully implemented macro- and micro-segmentation report:
  - Faster recovery. Their organizations contain and recover from breaches in an average of 20 days, compared to 29 days for those that have not undergone full implementation.
  - Stronger alignment. 87% of respondents report that their organizations' teams are fully aligned, compared to just 52% of respondents at organizations without full implementation.
  - Smarter scaling. Respondents from organizations that have undergone full implementation are more likely to strongly agree that automation is the key to scaling and maturing segmentation projects: 63% vs 50% without full implementation.

2. The importance of segmentation

Having a robust and secure network security strategy enables organizations to proactively reduce risk and minimize the impact of potential breaches. According to this research, two thirds (67%) of organizations believe they have a proactive approach to their network security, meaning they invest ahead of threats and adapt quickly.

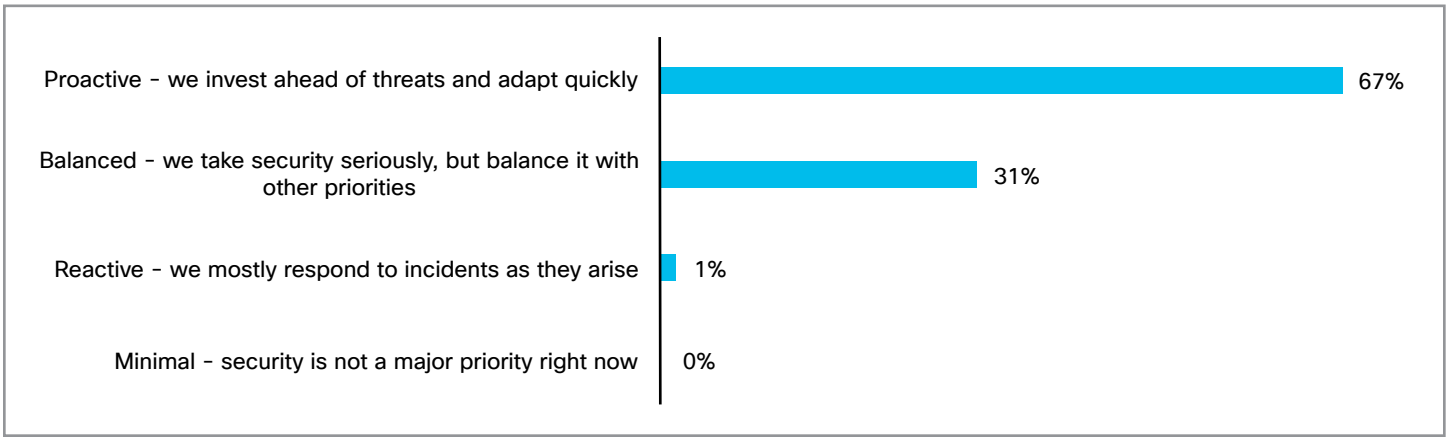


Figure 1. How would you describe your organization's current approach to network security? Base: 1000 respondents.

A cornerstone of this proactivity is segmentation. Segmentation—the practice of dividing networks into smaller, isolated zones—limits the spread of any successful attack and strengthens overall resilience. With this in mind, it's no surprise that 79% of organizations report that segmentation is a top priority within their network security strategy, and an additional 16% say it's important (see Figure 2).

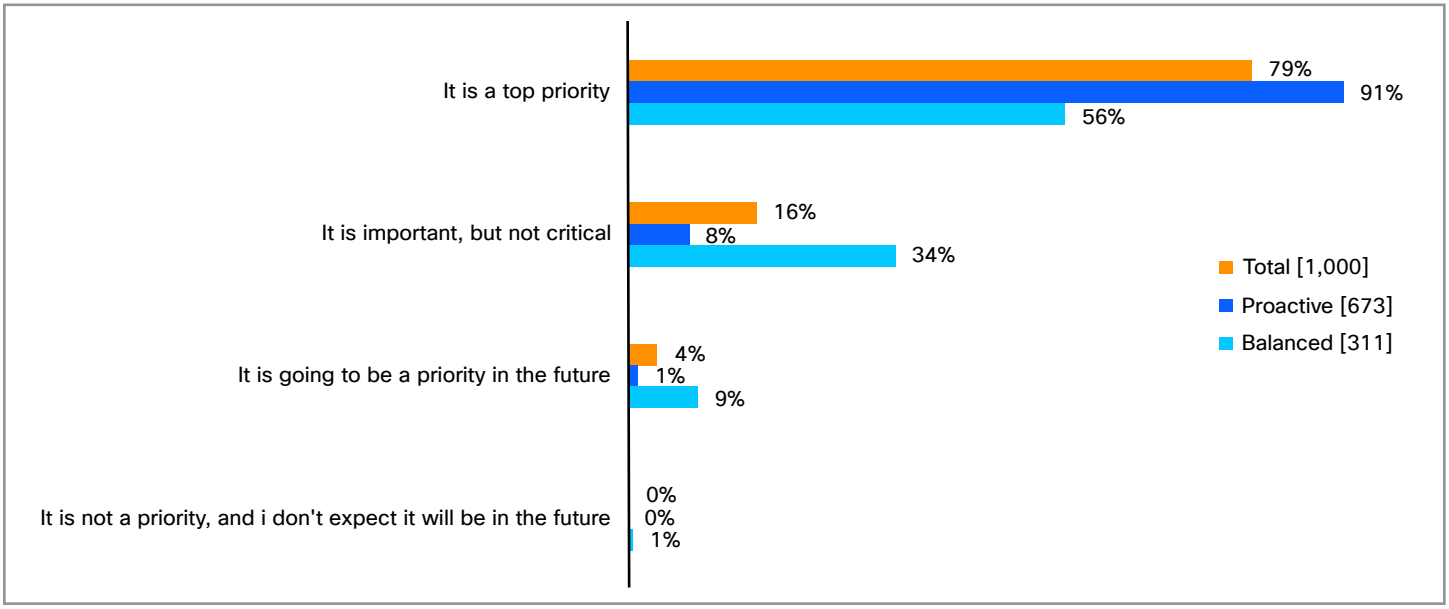


Figure 2. What priority does your organization currently give to segmentation in your network security strategy? Base:1000 respondents. Data split by proactive [673 respondents] or balanced approaches [311 respondents].

Those that take a proactive approach to network security are especially inclined to view segmentation as a critical priority, likely due to their mindset of focusing on prevention and containment through investing in threat mitigation ahead of time. These organizations seem to be thinking ahead and prioritizing segmentation as a way to make their security posture more robust.

Yet here lies a gap: While segmentation is acknowledged as critical by many, it is not always fully implemented in practice.

Current implementation progress

Across organizations, there's a disconnect between perception and reality. While the majority of respondents say that segmentation is a top priority of their organization's network security strategy, only one-third (33%) report that their organizations have fully implemented both macro- and micro-segmentation.

Looking at each in turn, macro-segmentation, the separation into large network zones or environments, has been mostly, or fully implemented by 76% of organizations. A similar proportion, 73%, report the same for micro-segmentation, which was defined in the research as the fine-grained security controls between individual workloads, applications, or services to limit lateral movement and improve visibility.

On the surface, these numbers suggest strong adoption. Yet a closer look reveals the gap: only 33% have fully implemented both approaches in tandem. This highlights how many organizations lag in their segmentation journeys rather than having fully refined deployments.

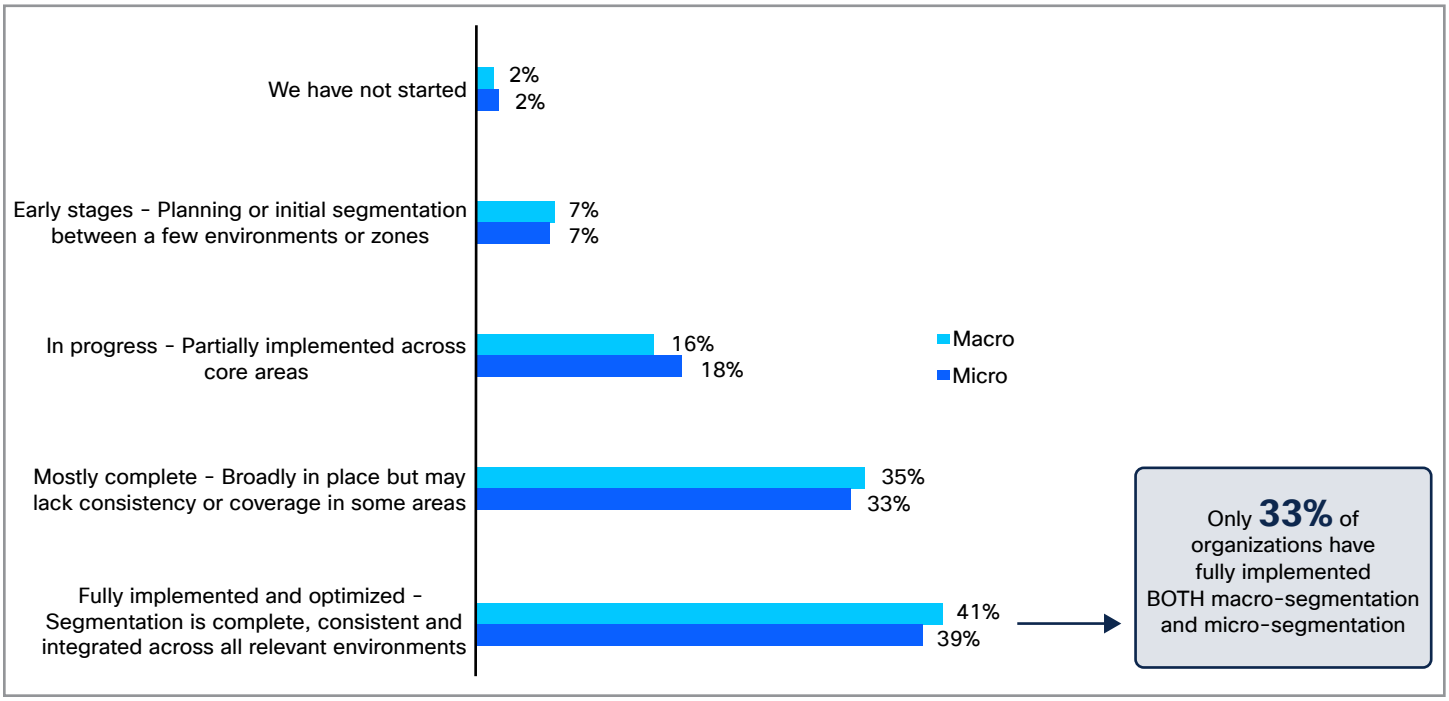


Figure 3. How would you rate your organization's current progress with implementing macro-segmentation? How would you rate your organization's current progress with implementing micro-segmentation? Base:1000 respondents.

The benefits of total segmentation are clear

Our research finds that organizations that have implemented both macro- and micro-segmentation are more likely to see clear business benefits such as fully aligned teams, quicker recovery times, and smarter scaling.

For example, among respondents at organizations that have fully implemented both macro- and micro-segmentation, 87% report that their teams are fully aligned, compared with just 52% of those at organizations without full implementation.

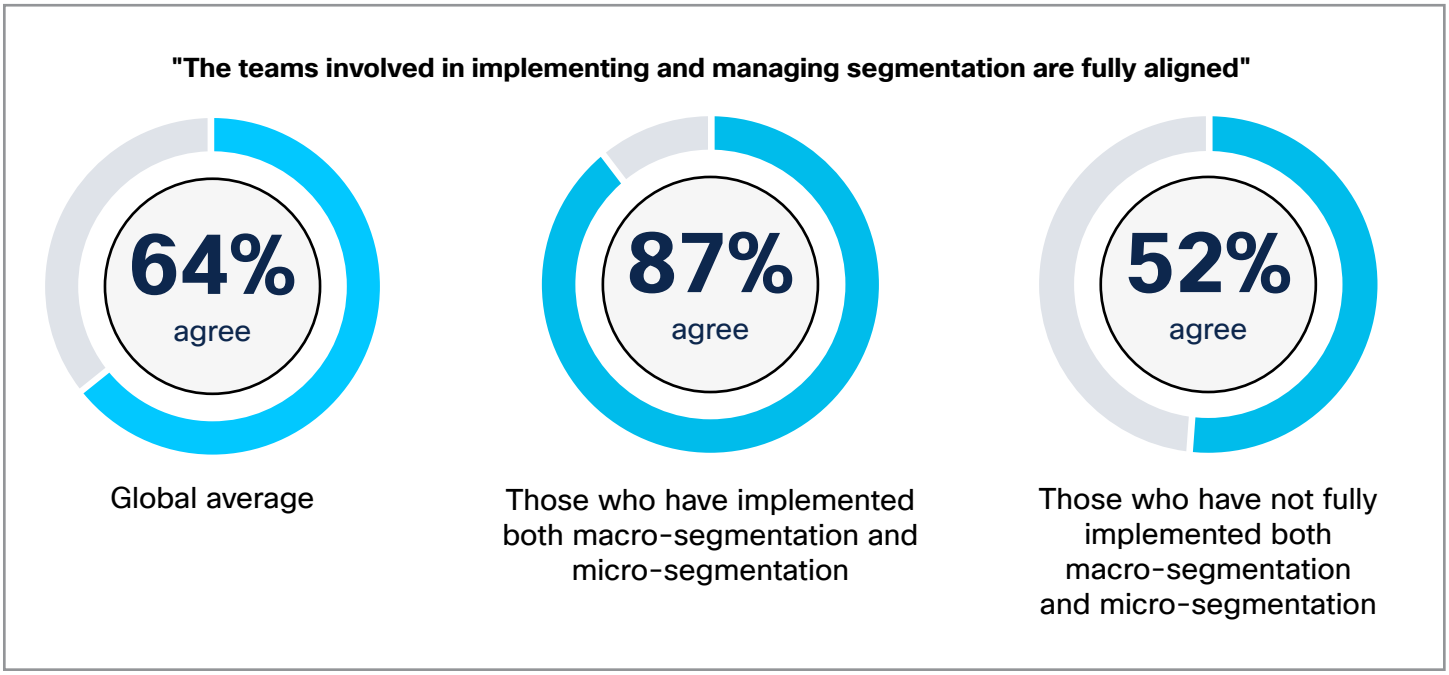


Figure 4. When thinking about the teams involved in implementing or managing segmentation at your organization, how would you rate how aligned they are? Base: if respondent uses two or more teams [994 respondents]. Data split by those who have fully implemented both macro- and micro-segmentation [315] and those who have not fully implemented both [608].

The potential to reduce information silos and better align disparate teams can be highly rewarding for organizations. This better alignment is particularly important given that full implementation of both macro- and micro-segmentation often involves multiple teams. For instance, 43% of respondents at organizations that have implemented both say they use four different teams for managing and implementing segmentation, compared to just 24% who haven't fully implemented both.

Another advantage of implementing full macro- and micro-segmentation is smarter scaling. Around two-thirds (63%) of respondents at organizations with full implementation strongly agree that automation is key to scaling and maturing segmentation projects, versus 50% without full implementation of both, indicating these organizations are better positioned to scale sustainably.

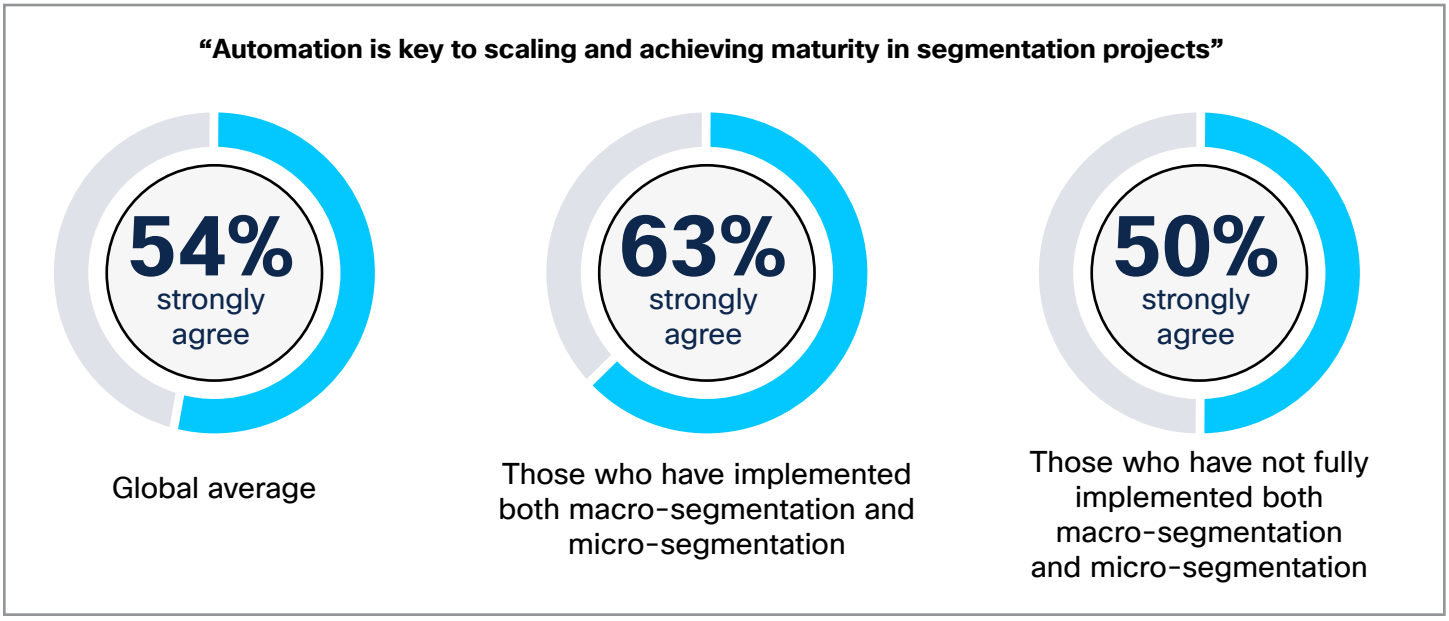


Figure 5. To what extent do you agree with the following statement? "Automation is key to scaling and achieving maturity in segmentation projects." Base: Base:1000 respondents. Data split by those who have fully implemented both macro- and micro-segmentation [315] and those who have not fully implemented both [608].

Taken together, these findings indicate that closing the segmentation maturity gap could translate into stronger alignment and more sustainable scaling. Given the fact that most organizations lag in segmentation maturity, the opportunity ahead is evident: those that fill the gap will be better equipped to thrive in an increasingly complex threat landscape.

"If I could change one thing about my organization segmentation approach, it would definitely be to further automate and integrate our segmentation tools and processes. By leveraging automation and integration, we could enhance the effectiveness and scalability of our segmentation strategy. This change would have significant impact on effectiveness and efficiency."

– UK, IT, telecoms, and technology

3. Deployment experiences with segmentation

Having established the benefits of full segmentation, it's important to understand how organizations are putting it into practice. On average, organizations use three teams for implementing and managing segmentation. Most often, these teams include IT infrastructure or network (87%), Security/SecOps (77%), and DevOps/Cloud Engineering (71%).

The specific responsibilities these teams take on vary. 43% have Layer 2 segmentation, 65% Layer 3 and, most commonly, 70% have Layer 3/4 segmentation (see Figure 6 for a full breakdown).

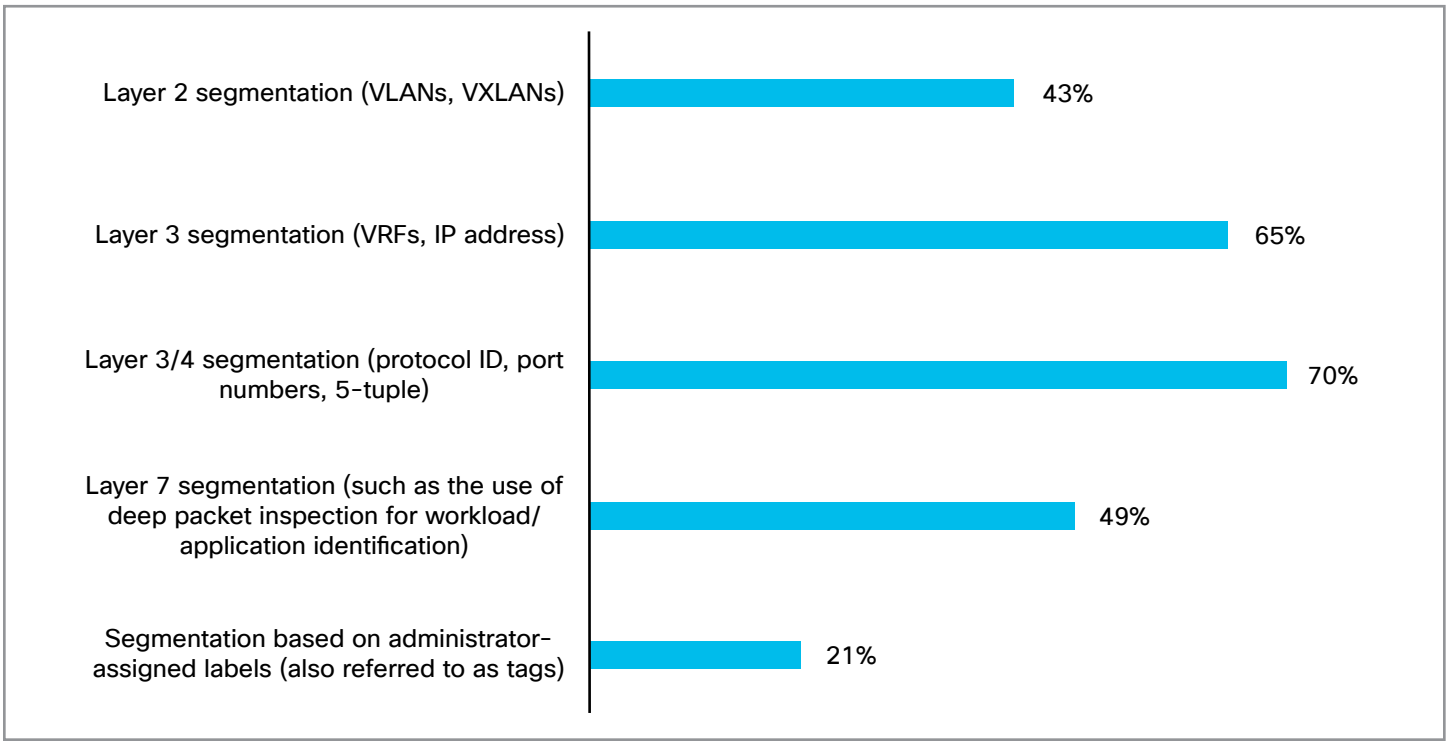


Figure 6. Which of the following approaches is your organization using to segment its environment(s)? Base:1000 respondents.

These results highlight how segmentation is rarely owned by a single function. Instead, segmentation projects require coordination across multiple teams with multiple layers of responsibility—necessitating full alignment.

Understanding how segmentation is deployed provides valuable context, but it tells only part of the story. Protecting high value/critical assets (57%), meeting compliance/regulatory requirements (55%), and containing breaches (52%) are the top three most likely drivers for organizations implementing segmentation. Enabling Zero Trust architecture (43%), preventing insider threats (38%), and supporting mergers (37%) are all also part of the push.

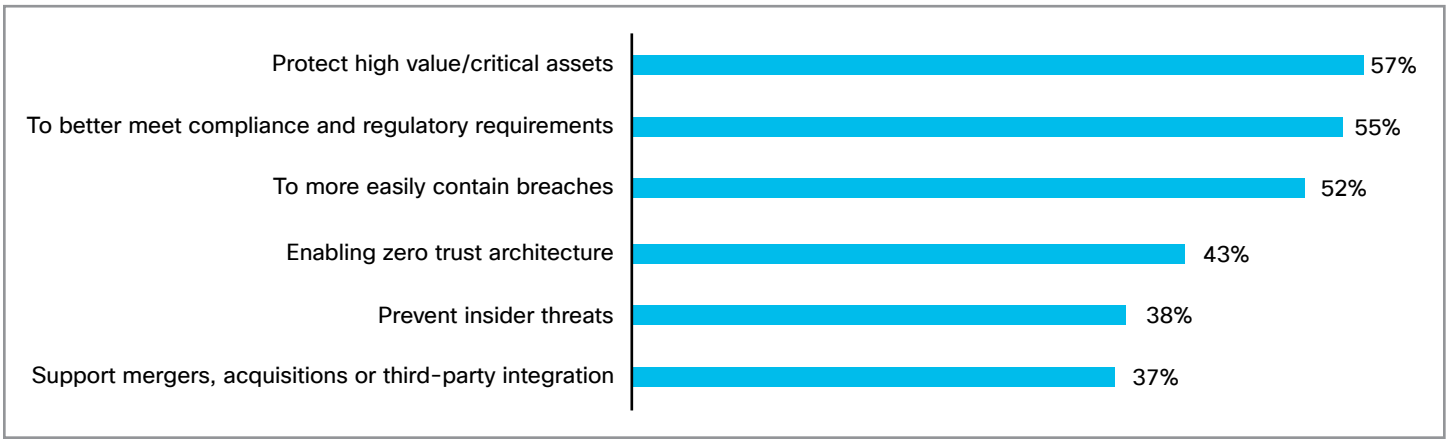


Figure 7. What are, or would be, the main drivers for your organization when pursuing segmentation within its network? Base:1000 respondents.

These varied factors highlight that segmentation is seen as protecting what matters most, meeting mandatory requirements, and strengthening resilience against breaches. In other words, the drivers reflect both business imperatives and security realities, underscoring why segmentation has become a strategic priority for so many.

The final area of consideration is the resource types that organizations are choosing to segment. The research finds that the top priority areas to segment are critical data and assets (74%), compliance zones (58%), and functional/business zones (58%).

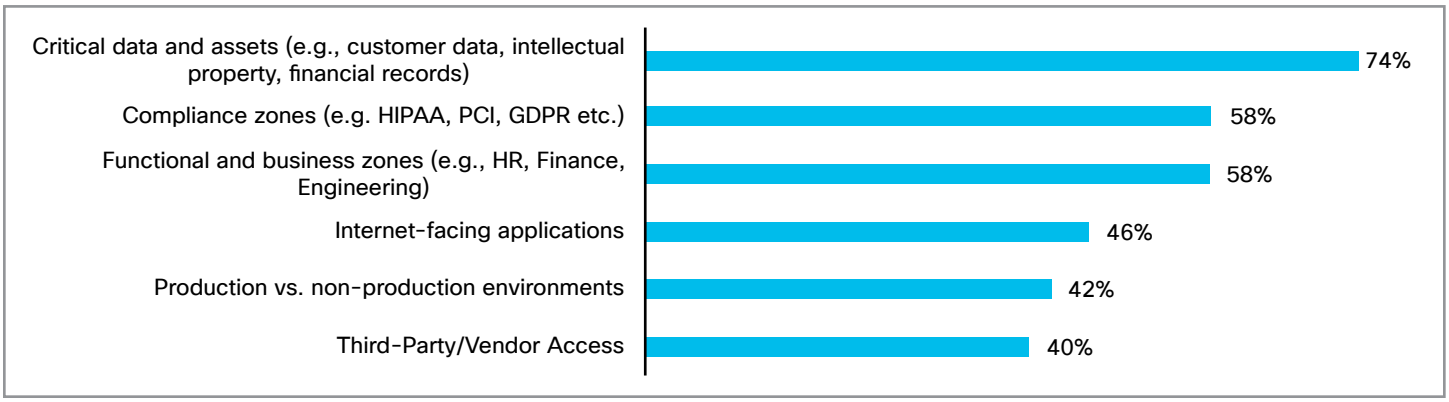


Figure 8. Which of the following business areas are, or would be, your organization's priority when it comes to segmentation? Base:1000 respondents.

This emphasis on critical data and assets highlights how segmentation can be linked to protecting the resources that matter most to organizational resilience. By isolating high-value systems and sensitive information, organizations can reduce the likelihood of a breach spreading to their most important assets while strengthening their ability to meet business continuity and regulatory obligations.

It's also worth noting that segmentation maturity appears to shape segmentation priorities. According to respondents in the survey, organizations that have fully implemented both macro- and micro-segmentation are more likely to segment compliance zones (67%) than those without full implementation of both (54%). This suggests that once fundamentals of asset protection are in place, mature organizations extend segmentation into compliance-driven areas—reflecting both evolving regulatory demands and the pursuit of more comprehensive control.

Segmentation challenges

Organizations are having difficulty closing the maturity gap, but understanding the challenges they face will ease the transition from partial to comprehensive segmentation.

Globally, 94% of organizations are experiencing segmentation challenges, ranging from technical to non-technical challenges. This is a huge proportion of organizations and suggests that while segmentation is widely prioritized, it remains difficult to execute in practice.

Complex environments resulting from hybrid IT, cloud, containers, and legacy systems make segmentation harder to manage or implement (54%). A lack of visibility into what resources to segment (32%) is also a common challenge.

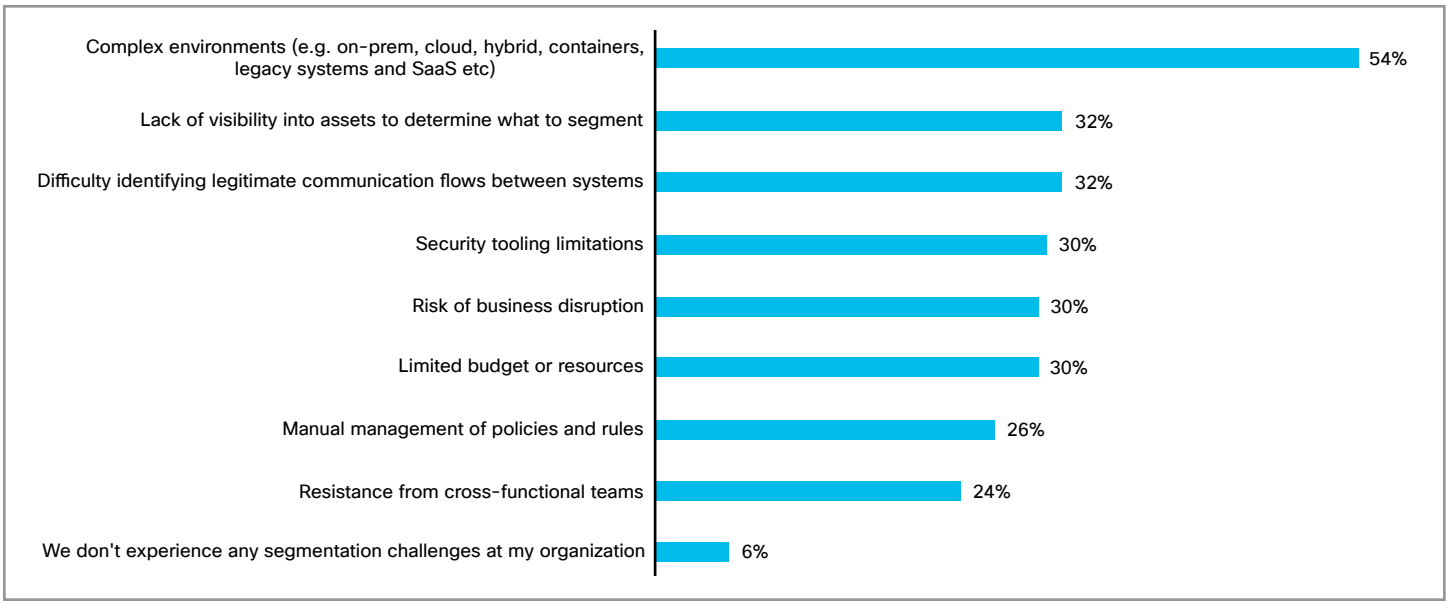


Figure 9. Currently, what are/ could be the biggest segmentation challenges you are/ could be experiencing at your organization? Base:1000 respondents.

In addition, challenges intensify when organizations attempt to manage multiple segmentation approaches in parallel. This is especially important to call out as achieving segmentation maturity requires multiple approaches. Yet doing so introduces greater complexity, highlighting a critical customer pain point that makes full segmentation harder to achieve.

For instance, organizations that employ five segmentation approaches struggle with technical challenges resulting from complex environments (58%), lack of visibility (36%), or difficulty identifying legitimate communication flows between systems (40%), when compared to those with just one segmentation approach (41%, 22%, and 26% respectively).

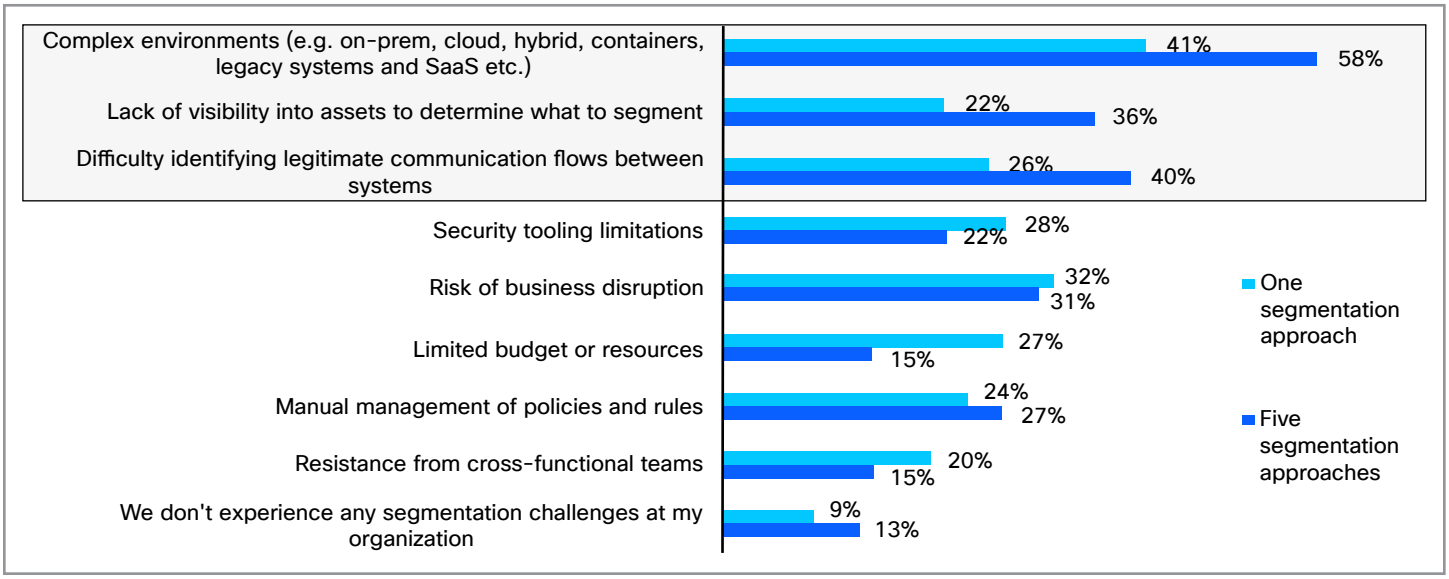


Figure 10. Currently, what are/could be the biggest segmentation challenges you are/ could be experiencing at your organization? Base:1000 respondents. Data split by the number of segmentation approaches. One approach [188 respondents], five approaches [55 respondents].

Additional segmentation approaches may promise stronger protection, but the added complexity can make management harder or amplify technical barriers if organizations don't have the right tools and knowledge in place.

Ultimately, the data underscores that while segmentation is a priority for most, turning that priority into reality requires addressing deep-rooted technical and organizational challenges.

"I'd streamline our segmentation so it's less manual and more consistent across cloud, on prem, and containers. Too much effort goes into patching gaps lately."

– U.S., financial services

Beyond technical hurdles, policy-related issues create compounding difficulties with more than half of organizations (53%) struggling to keep up with ever-changing networks and application behaviors.

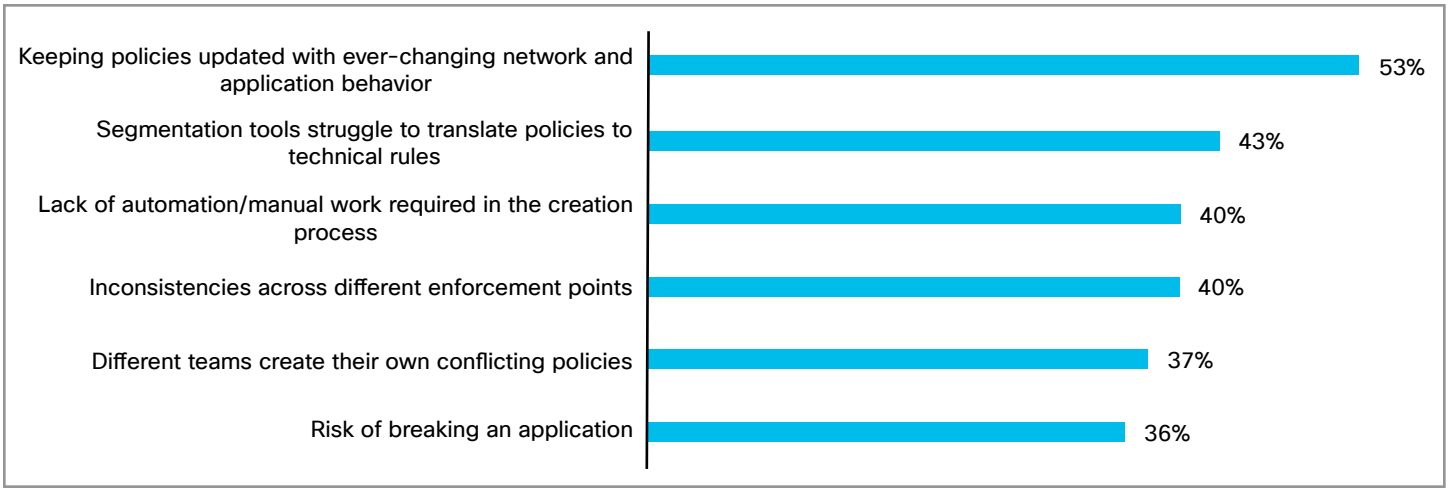


Figure 11. When creating segmentation policies, what are your biggest pain points? Base:1000 respondents.

Automation could be the solution to mitigating these challenges. In fact, 65% of respondents said that policy automation would be in their top three capabilities in a segmentation tool, and 95% of respondents say that the ability to test policies and procedures within their environment prior to deployment will be game changing.

"I'd streamline policy management by moving to a more unified platform, so teams spend less time coordinating across different tools and enforcement points."

– UK, IT, telecoms and technology

"I would propose implementing an advanced automation solution for creating, testing, and continuously updating segmentation policies, integrating orchestration tools..."

– Brazil, IT, telecoms and technology

"Automating security policy creation and maintenance with real-time application visibility is crucial to prevent service disruption and reduce risk in ever-changing environments."

– India, Financial services

Agent-based tools

Agent-based tools installed on endpoints such as servers or containers can enforce segmentation policies. With enforcing segmentation policies being a consistent hurdle for organizations, it makes sense to see that two-thirds (64%) have already deployed them for micro-segmentation.

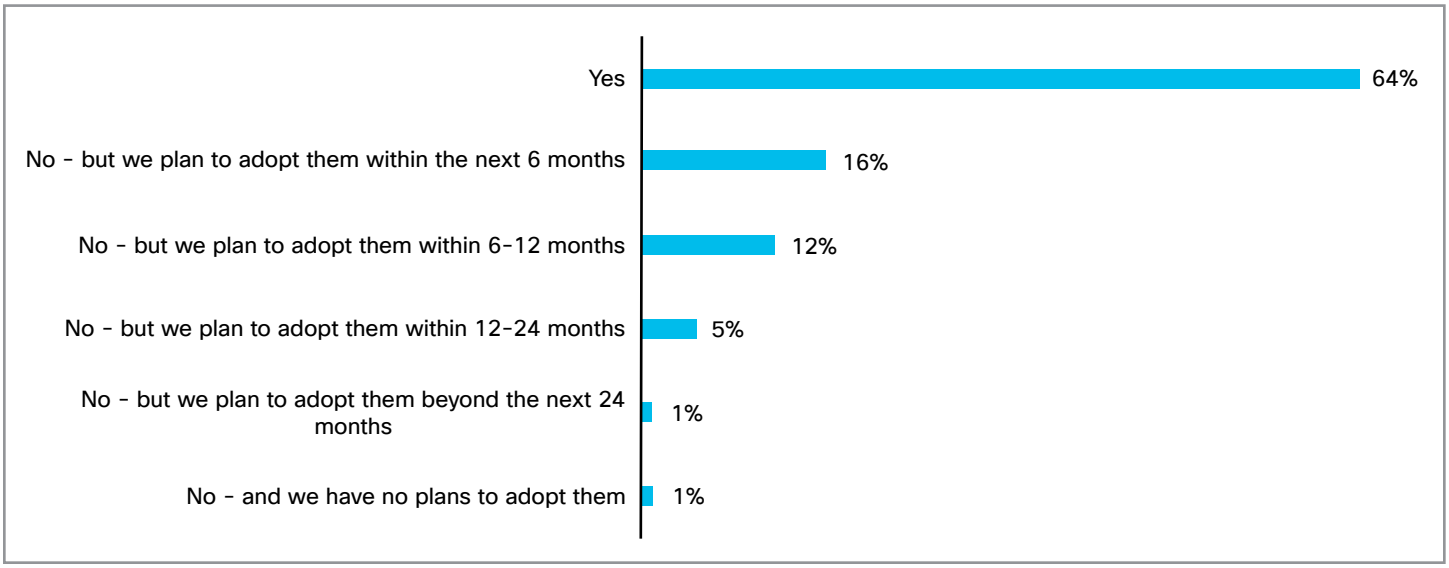


Figure 12. Does your organization use or plan to use agent-based tools to implement micro-segmentation? Base:1000 respondents.

It's widely recognized that agent-based tools can cause operational overhead and increase management complexity by adding additional software layers that require ongoing management. However, the high level of adoption suggests that the lack of viable alternatives to agents in many deployment situations outweigh the challenges. Respondents from organizations that have implemented agent-based tools are more likely to report challenges—such as security tooling limitations or a need for more teams—when implementing and managing segmentation (see Figure 13).

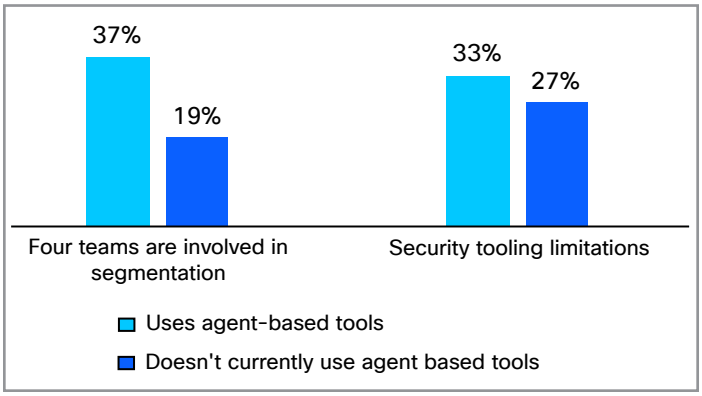


Figure 13. Which of the following teams, if any, are involved in implementing or managing segmentation at your organization? Currently, what are/could be the biggest segmentation challenges you are/could be experiencing at your organization? Base: 1000 respondents; Data split by organizations who use agent-based tools [637 respondents], and those who do not but plan to [342 respondents].

In other words, while agent-based tools are a popular choice, they can introduce added complexity that organizations must be prepared to address.

4. The impact of a breach

A successful breach can be devastating for an organization. It can cause financial losses, reputational damage, and an erosion of customer trust. Considering the consequences, it's shocking to see that more than eight out of ten (84%) organizations have experienced a successful breach within the last 12 months. A similar proportion (82%) have experienced at least two types of breaches within the same time period.

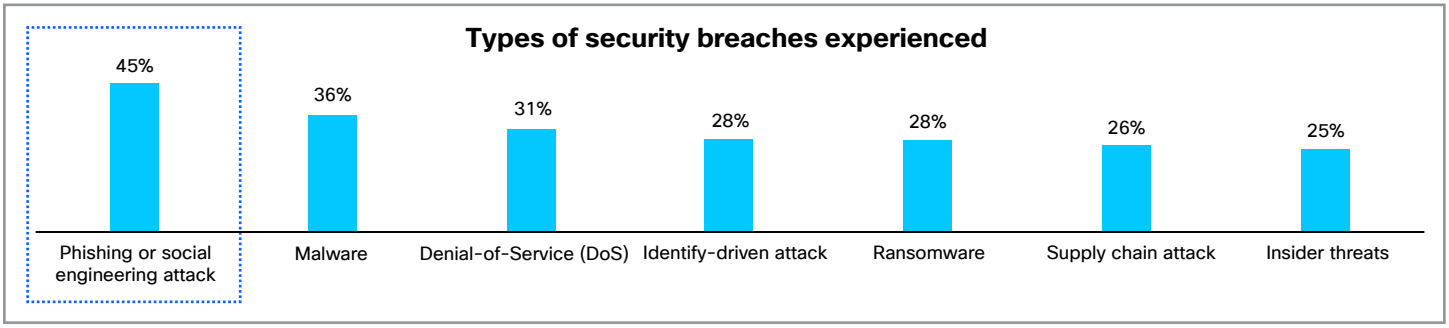


Figure 14. Which of the following has resulted in a security breach at your organization in the last 12 months? Base:1000 respondents.

Segmentation plays a key role in speeding up recovery from breaches. Respondents from organizations that have full implemented macro- and micro-segmentation report that breach containment and recovery time takes up to 20 days on average, compared with the reported 29 days for organizations without full implementation of both.

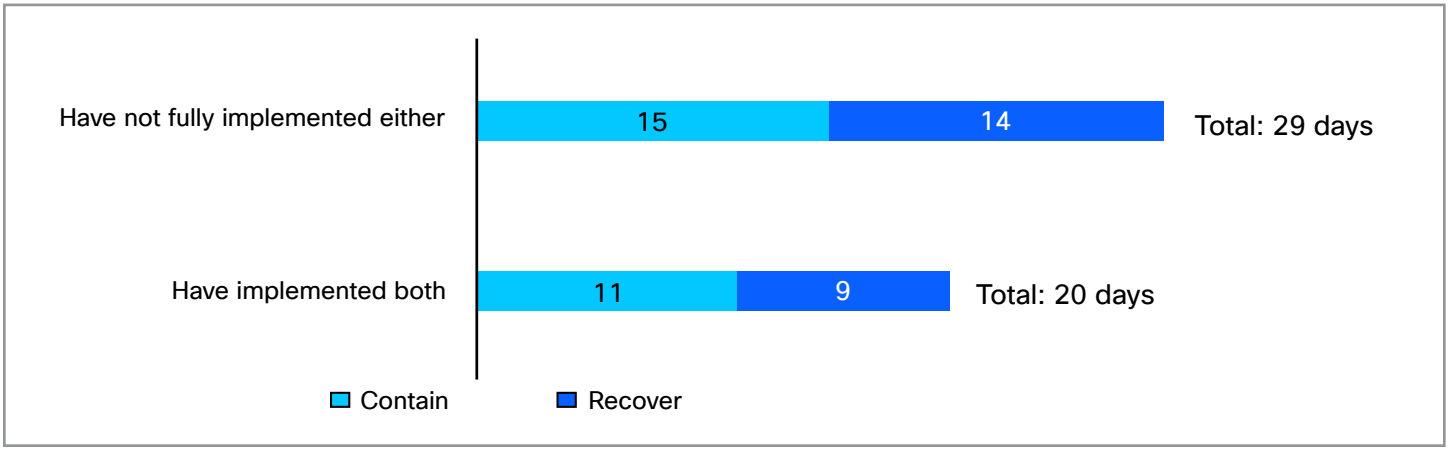


Figure 15. Showing the average time it takes organizations to contain and fully recover from their most recent breach. Base:1000 respondents. Data split by organizations with full implementation of both macro- and micro-segmentation [327 respondents] and organizations who have not fully implemented either [667].

This shows that partial progress isn't enough—only full implementation of both macro- and micro-segmentation approaches delivers real resilience gains.

Looking ahead, organizations recognize the need to strengthen their defences and accelerate response times. Respondents report that improving breach resilience requires them to prioritize greater visibility into their environments, stronger alignment across teams, and increased automation to support faster detection and containment. Together, these improvements—alongside full implementation of both macro- and micro-segmentation—provide an effective path toward reducing breach impact and achieving resilience.

> "I would improve the granularity of network segmentation to isolate critical systems more effectively, minimizing the blast radius in case of a breach and enhancing overall security posture."
>
> – India, IT, financial services

5. Conclusion

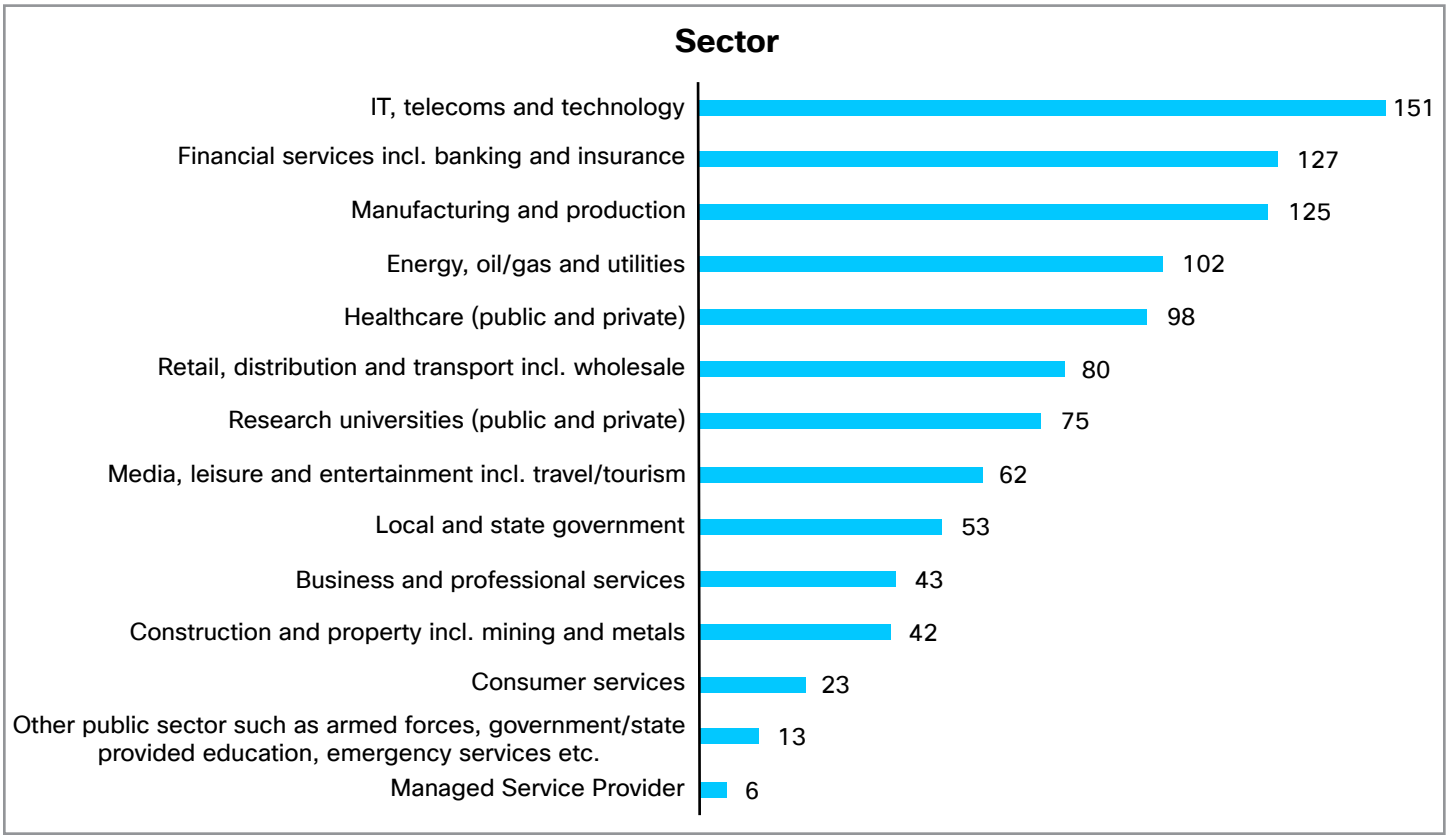
The research revealed three key takeaways:

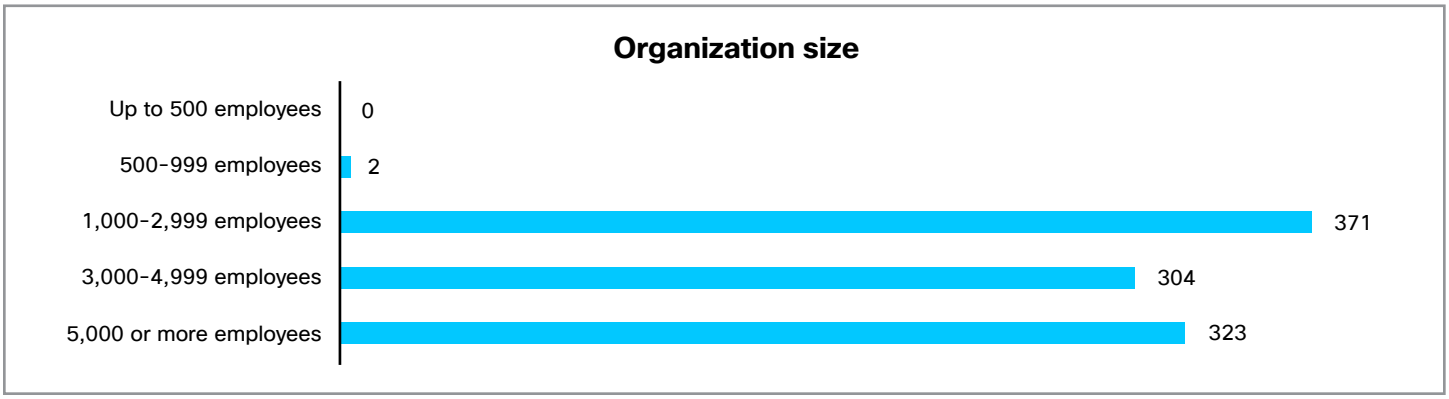
- Segmentation is a critical pillar of modern network security, directly linked to protecting high-value assets.
- The journey to full segmentation maturity remains unfinished—with many experiencing ongoing implementation challenges.
- The advantages of pursuing full macro- and micro-segmentation strategies in tandem are evident—with organizations seeing stronger team alignment, faster recovery times, and the ability to scale sustainably.

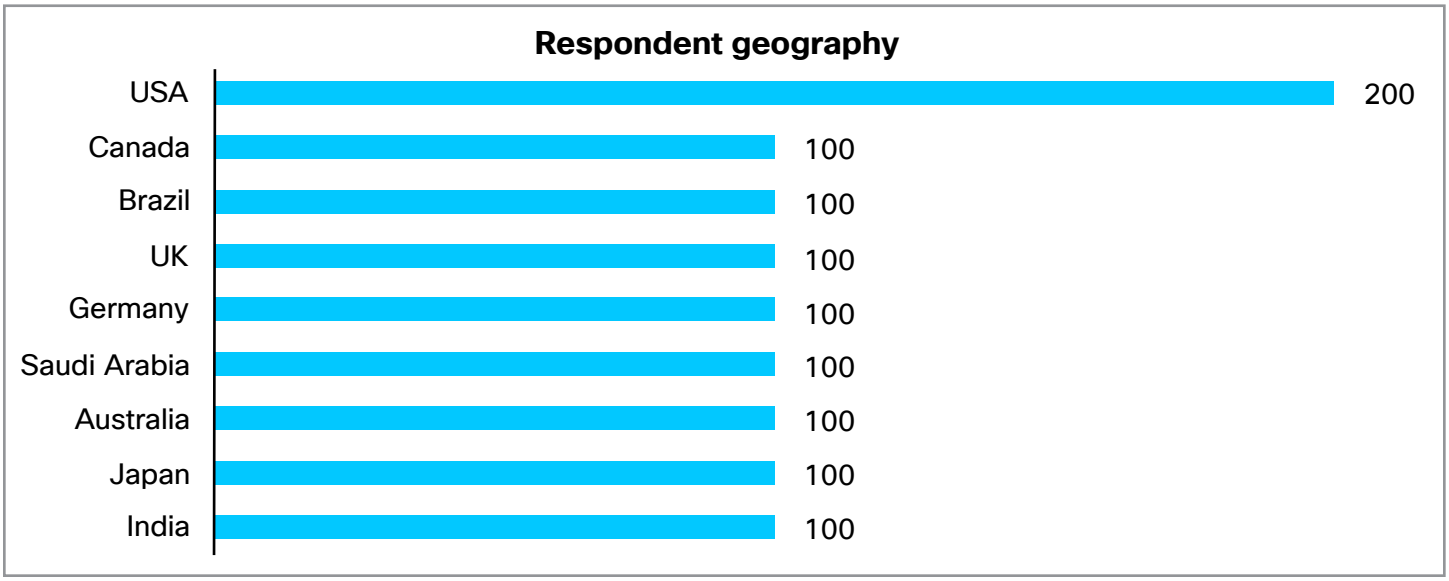
6. About the research

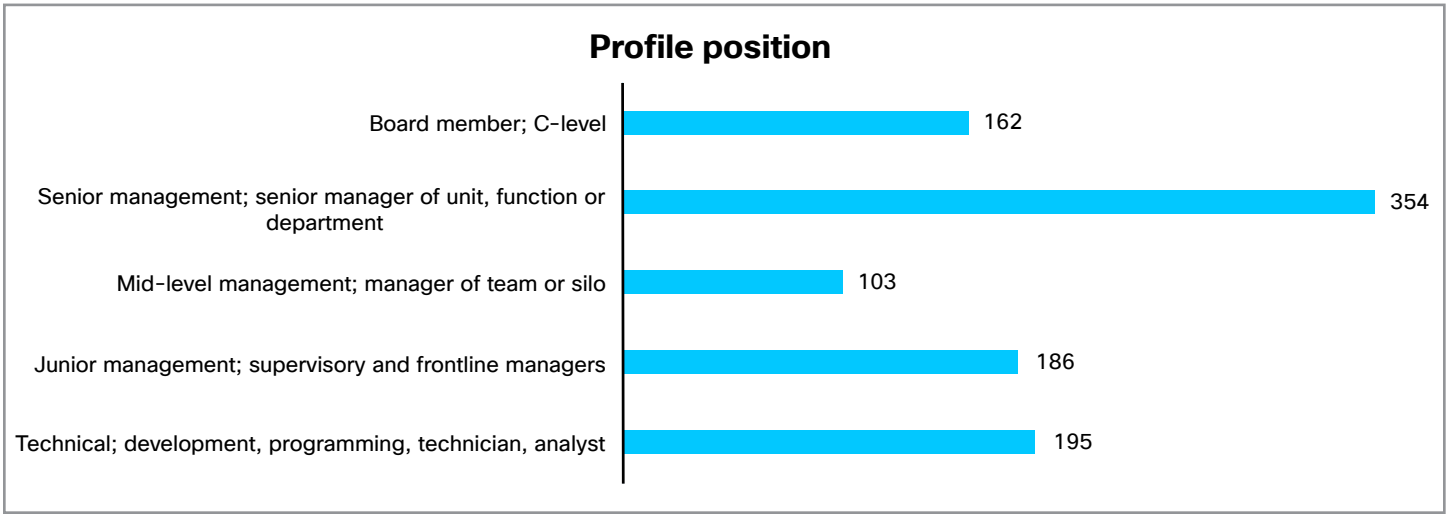
Cisco commissioned independent market research specialist Vanson Bourne to conduct this piece of research. The study included surveying 1000 respondents from organizations with 1000 employees or more across the following countries: U.S., Brazil, UK, Germany, Saudi Arabia, Australia, Japan, and India.

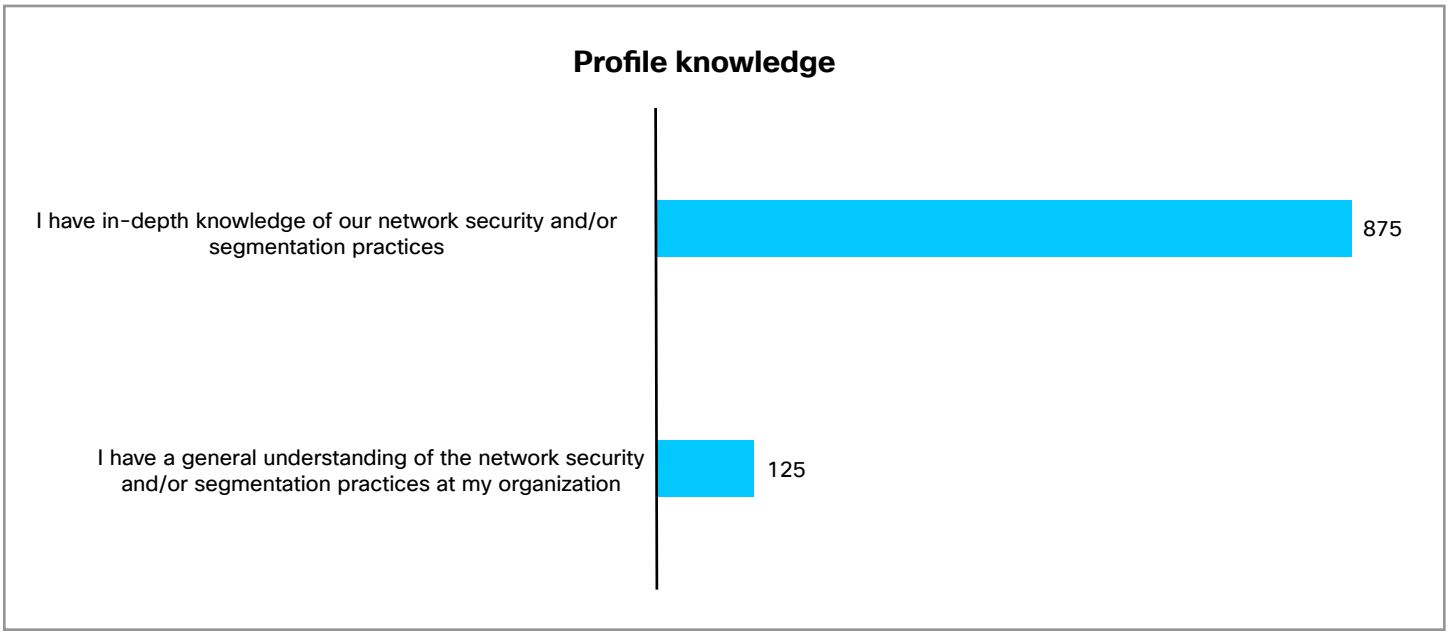
Organizations are from several public and private sectors, but there was a strong representation from IT, telecoms and technology, financial services (including banking and insurance), manufacturing and production, energy, oil & gas, and utilities, healthcare, local government, and research universities. Respondents were required to have knowledge of their organization's network security and segmentation practices.











References

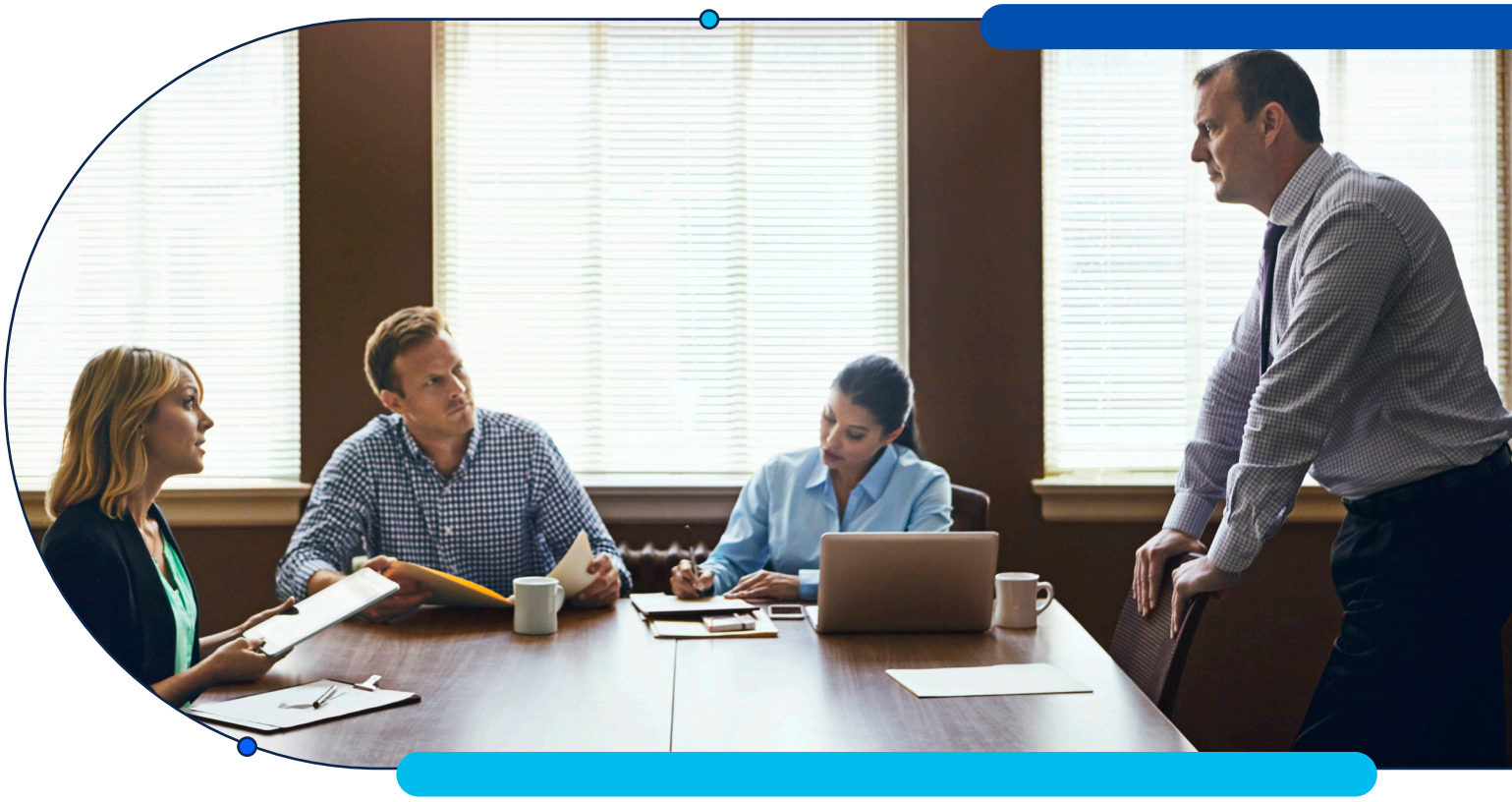
A taxonomy for segmentation, Cisco Systems, Inc., August 19, 2025.

About vanson bourne

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 vansonbourne.com.

About Cisco

Cisco is the worldwide technology leader that securely connects everything to make anything possible. Our purpose is to power an inclusive future for all by helping our customers reimagine their applications, power hybrid work, secure their enterprise, transform their infrastructure, and meet their sustainability goals. For more information visit www.cisco.com.



C99-5483135-00 10/25