Firewalling in the AI Era

Results from the Cisco 2026 Firewalling Survey

Contents

1. Introduction

Firewalling has been foundational to network security for several decades. In that time, the discipline has repeatedly had to absorb major shifts in how organizations build and operate their networks, from the migration of workloads to the cloud, to the steady rise of encrypted traffic that firewalls are expected to inspect without slowing the business down. Through each of these transitions, the core purpose of firewalling has held constant: to enforce security policy across an organization's traffic, workloads, and environments.

The rise of AI is the latest shift to reshape this landscape, and it is adding a new set of considerations to an already long list. AI introduces new workloads to protect, new traffic patterns to inspect, and new expectations about what firewall controls should be able to see and do. The question we set out to answer is a practical one: How, exactly, is AI affecting the firewalling landscape today?

To find out, we commissioned an independent market research firm to survey 500 professionals familiar with their organizations' firewalling practices, spanning a range of seniority levels from Board and C-suite leaders to operational management.

Key takeaways

- **Traditional firewalling considerations remain valid, but AI-related concerns now weigh heavily on the list**. The arrival of AI workloads and AI-driven traffic appears to have made organizations more security conscious, elevating AI-related needs to the point where they have pushed some traditional considerations—such as compliance—lower in priority. AI has become a significant new factor, though not a dominant one.
- **Senior leaders and operational roles largely agree on firewalling and AI, but with notable disconnects**. The most senior people in organizations share many of the same views as those in more operational roles. Where they diverge, senior leaders are consistently more optimistic: about the progress of their organization's firewall modernization, about how fully their deployed firewall controls address the full range of workloads and traffic (including AI workloads and traffic), and about their existing firewall architecture's readiness to support threat inspection.
- **The disconnects point to a clear discipline: Verify before investing**. Where leaders and their teams see modernization, coverage, and threat inspection differently, the smarter path is to confirm what is actually deployed, and diagnose what is genuinely constraining it, before committing resources.

2. The Firewalling Modernization Landscape

Before turning to the findings, it is worth being precise about what we mean by a few core terms, since “firewall,” “modernization,” “AI workloads,” and “AI traffic” can carry different meanings across organizations.

By firewall, we mean the technologies and controls an organization uses to monitor, inspect, and enforce security policy across network traffic, workloads, applications, and environments, including on-premises, cloud, and hybrid infrastructure. Firewalling is the act of deploying those capabilities, whether through standalone firewalls or through network infrastructure such as switches and routers. And by modernization, we mean the steps an organization takes to update or evolve its firewall architecture, capabilities, or deployment approach, moving toward a more current firewall environment, typically less than three to five years old, and capable of supporting multiple use cases.

In this report, AI workloads include infrastructure, applications, data pipelines, models, and services used to train, tune, deploy, or consume AI/ML systems. AI traffic includes traffic between users, applications, models, data stores, APIs, and cloud or SaaS AI services.

With those definitions in place, the first thing the research makes clear is that firewall modernization is not a distant ambition. Most organizations have recently modernized their firewall infrastructure (~53%) or are actively modernizing it today (~31%), with only a minority (~15%) not currently pursuing modernization (see Figure 1). Firewalling, in other words, is an area of active investment rather than a settled, static layer of the security stack.

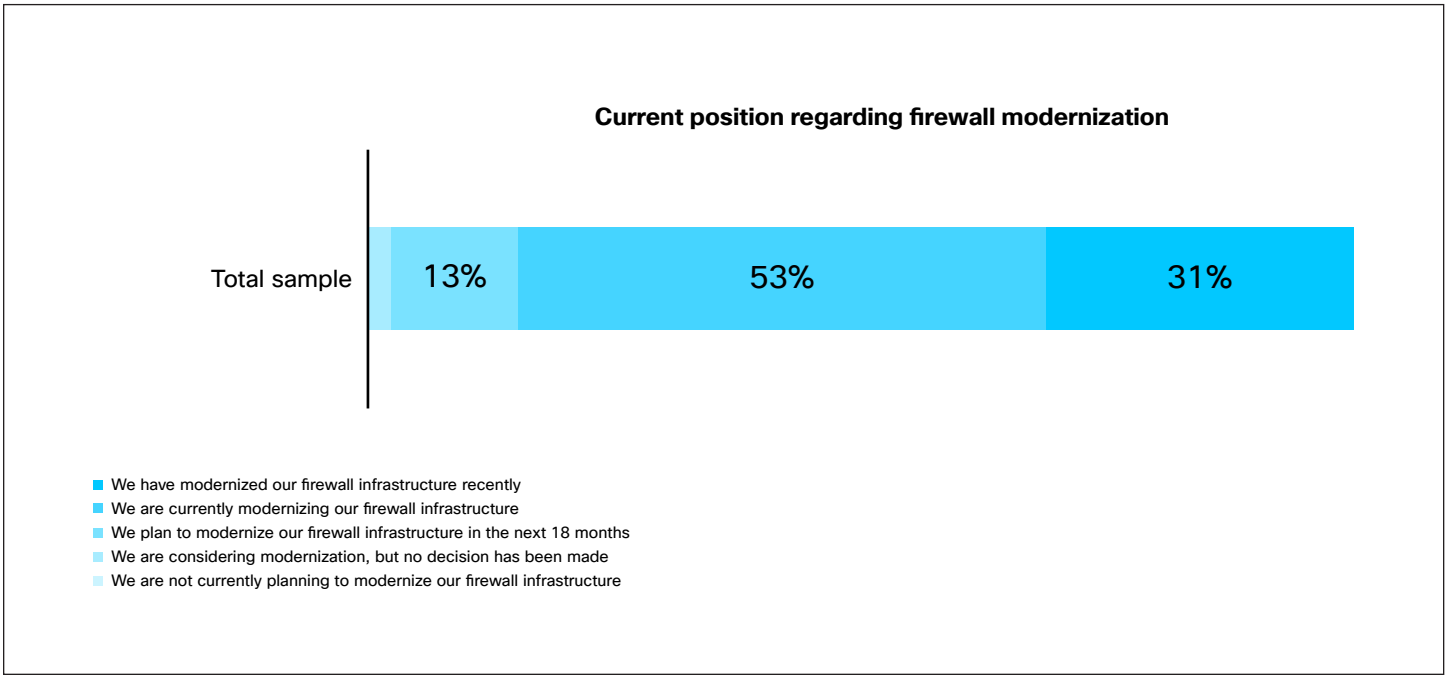


Figure 1. (Q4) Which of the following best describes your organization’s current position regarding firewall modernization?

Base: 500 respondents.

That headline picture, however, looks different depending on who is describing it. This is the first of several places in the research where the most senior leaders and those in more operational roles do not see the same thing. Board and C-suite respondents are more likely to view firewall modernization as something their organization has completed recently, while less senior respondents are more likely to describe it as ongoing (see Figure 2). The gap is not a disagreement about whether modernization matters—both groups treat it as important—but about how finished the work actually is. Leaders closest to strategy tend to see a job largely done; those closer to execution tend to see a job still underway.

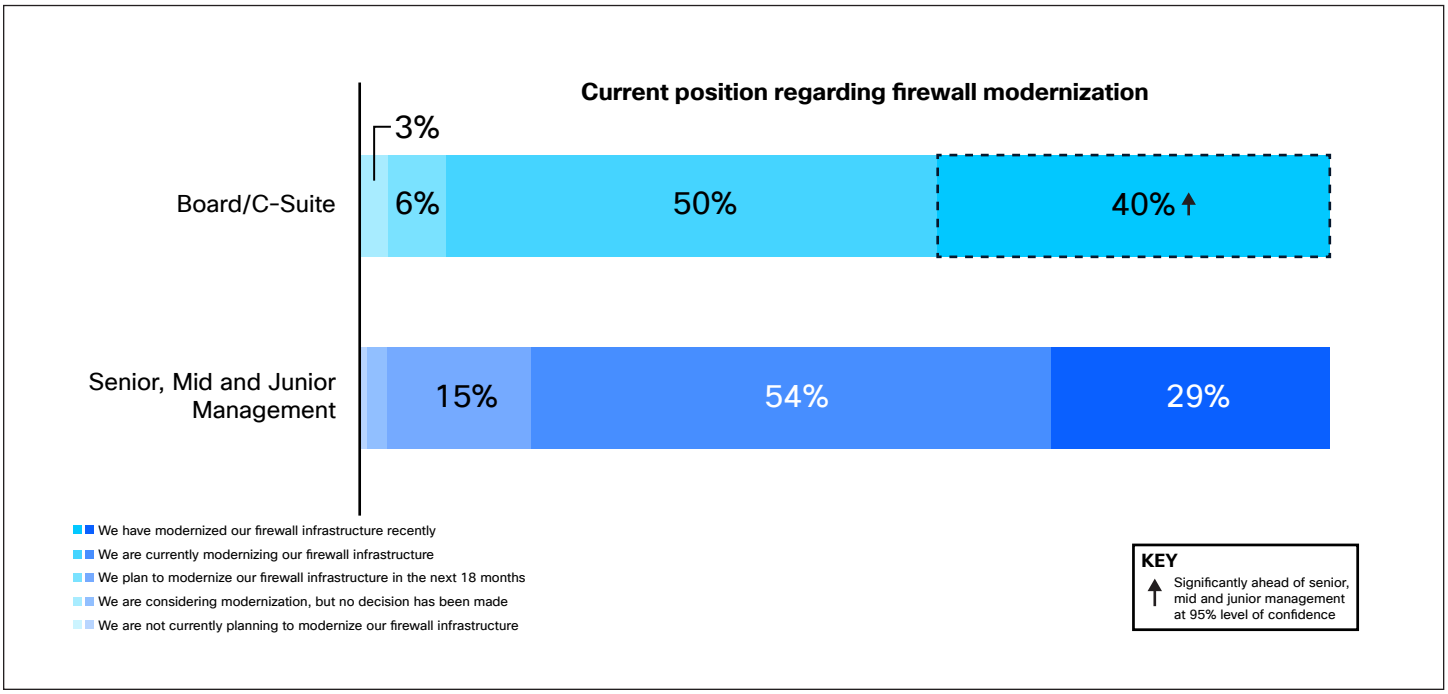


Figure 2. (Q4) Which of the following best describes your organization's current position regarding firewall modernization?

Base: 500 respondents, split by Board/C-suite [109 respondents] and other management [391 respondents].

Modernization is rarely frictionless. Among organizations that have modernized, are modernizing, or plan to modernize, the most reported challenges are competing priorities, architectural uncertainty, and concerns about migration (see Figure 3). Together, these point to a common pattern: The difficulty is less about whether to modernize than about sequencing that work against other demands, deciding on the right target architecture, and moving to it without disrupting the business in the process.

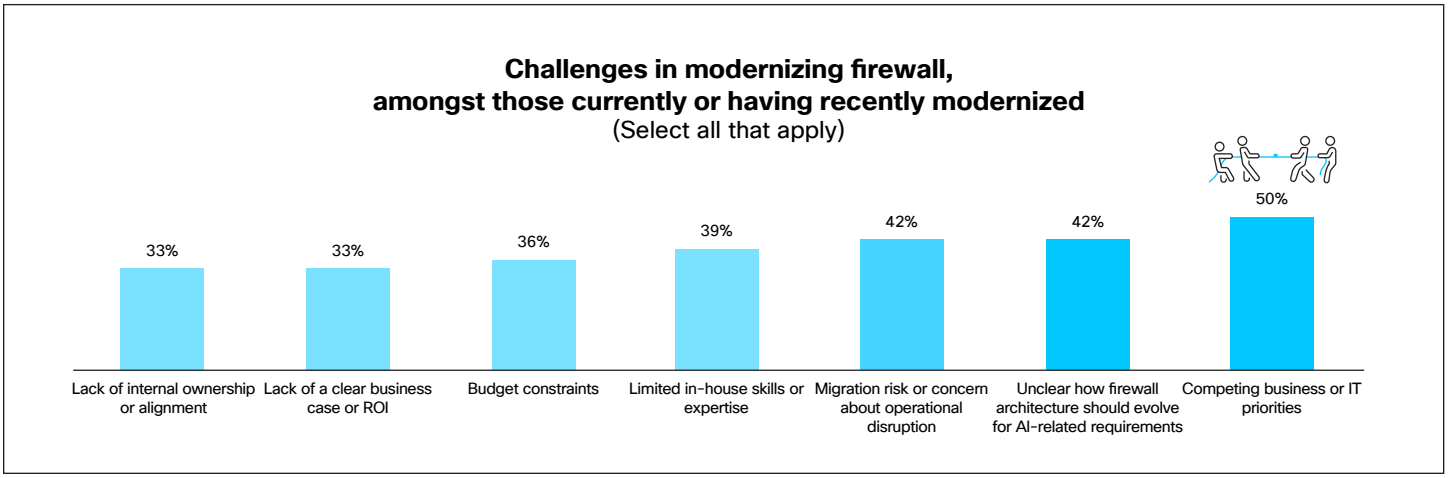


Figure 3. (Q9) What are the main challenges, if any, your organization has faced, or is facing, in modernizing its firewall environment? Base: Modernized, modernizing, or planning to modernize firewall [498 respondents].

Notably, the organizations that are not currently pursuing modernization cite many of these same factors as the reasons for holding back (see Figure 4). In other words, the considerations that make modernization difficult for those already underway are, for others, enough to defer the effort altogether. This is a comparatively small group (n=77, roughly one in six), but it is a telling one: The barriers to starting and the challenges of continuing are largely the same set of concerns, experienced at different points in the journey.

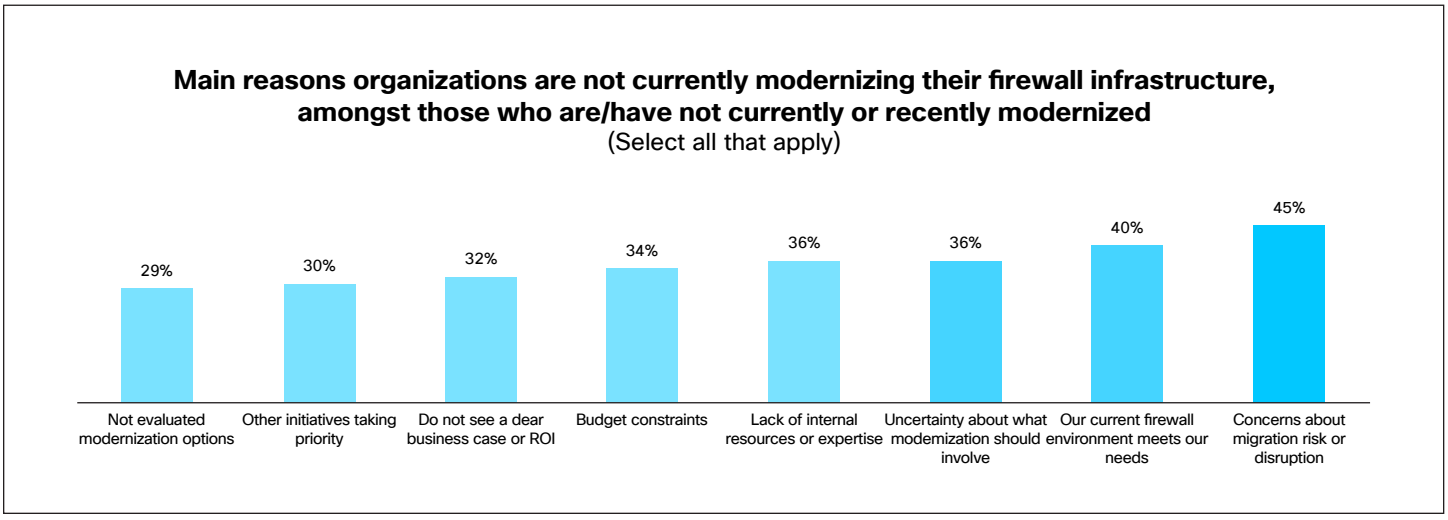


Figure 4. (Q4b) What are the main reasons your organization is not currently modernizing its firewall infrastructure? Base: Not looking to modernize today [77 respondents].

3. Perception of AI Relative to Other Firewall Considerations

Modernization tells us how organizations are investing; it does not fully tell us how they judge the firewall controls they already have, or where AI now sits among their concerns. This section turns to understanding current perception. Broadly, organizations believe their firewall coverage is well established across the areas that matter, including the emerging demands of AI workloads. Yet that confidence sits alongside a clear signal that AI workloads have become a leading security concern and a priority for modernization, and that expanding threat inspection to keep pace remains constrained. The picture that emerges is one of AI steadily climbing the list of firewalling considerations without displacing the fundamentals and, once again, of senior leaders and operational roles reading their own organization's situation with differing degrees of confidence.

3.1 Coverage is seen as established, but confidence varies by seniority

Organizations are broadly confident in the reach of their firewall controls. Across the range of areas we asked about, respondents report that firewall coverage is largely in place, and, notably, that confidence extends to the newer demands of AI workloads, not just to traditional traffic and environments (see Figure 5). On its face, this is a reassuring picture: Firewalling is seen as keeping pace with how networks are evolving, including the arrival of AI.

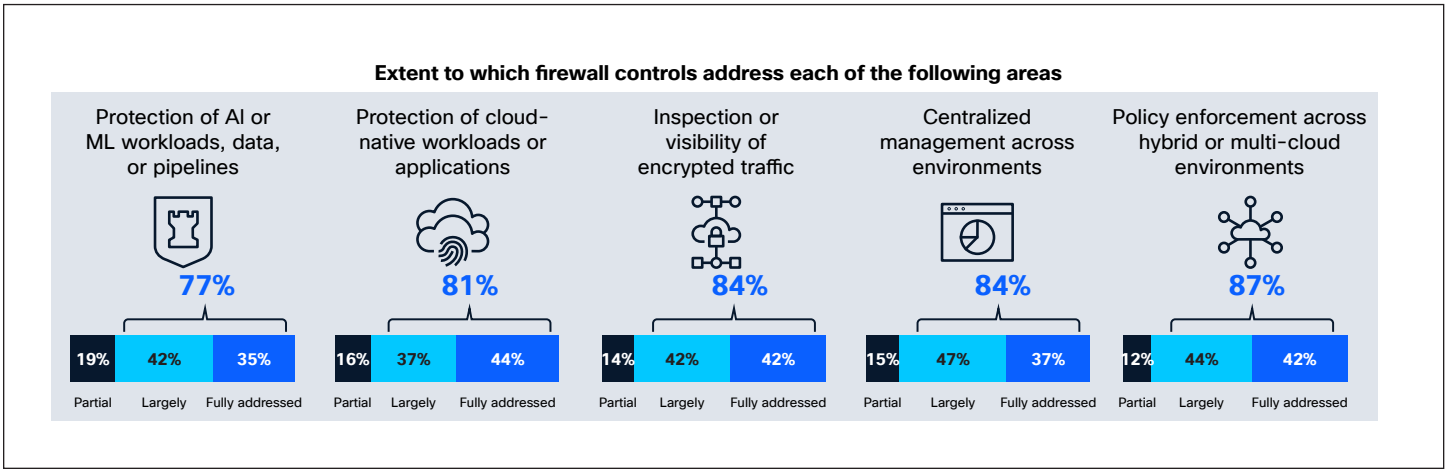


Figure 5. (Q1) To what extent are firewall controls in your organization currently addressing each of the following areas?

Base: 500 respondents.

That confidence, however, is not evenly held. When the responses are split by seniority, Board and C-suite respondents report meaningfully greater confidence in firewall coverage than their counterparts in more operational roles (see Figure 6). This is the second point in the research (after the differing views on modernization progress in Section 2) where the most senior leaders take a more optimistic view than the people closer to operational execution. The pattern is consistent: Leaders tend to see their organization's coverage as more complete, while those operating the controls see more of the gaps in what has actually been deployed.

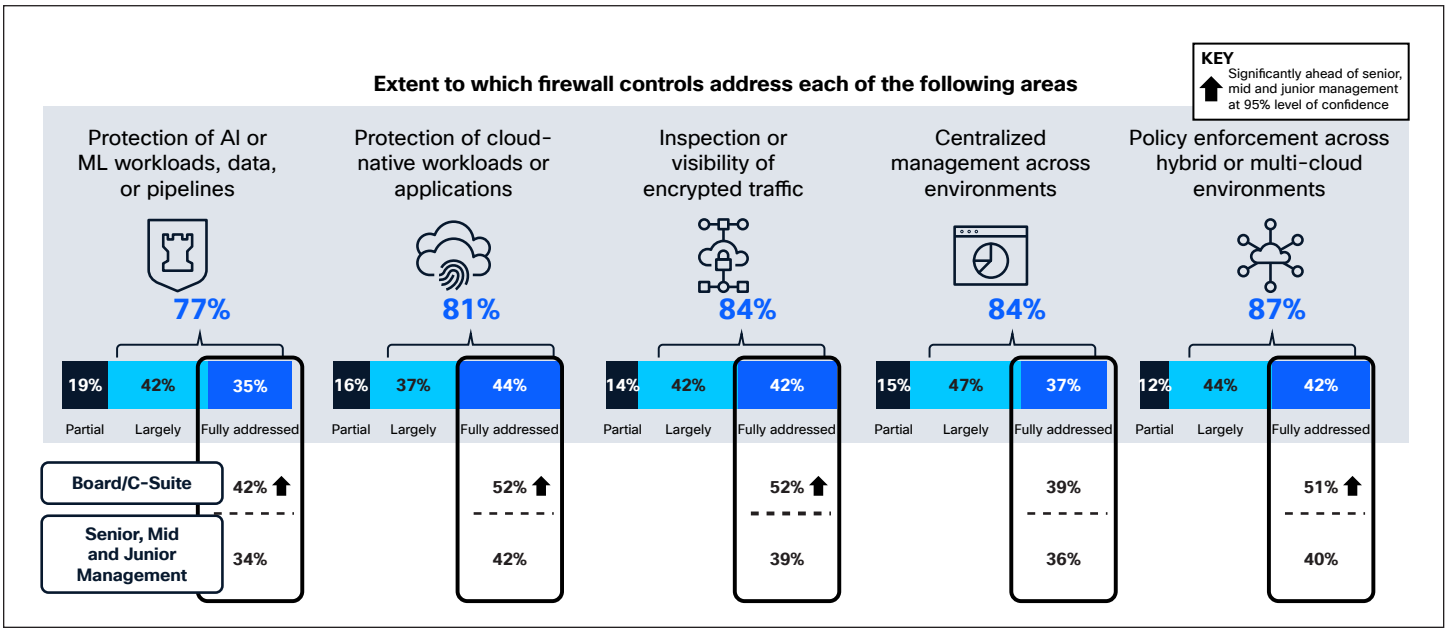


Figure 6. (Q1) To what extent are firewall controls in your organization currently addressing each of the following areas?

Base: 500 respondents, split by Board/C-suite [109 respondents] and other management [391 respondents].

The distinction matters because perceived coverage shapes where organizations choose to invest next. If senior leaders believe the firewall estate already addresses AI workloads while their teams see remaining gaps, the two groups may reach different conclusions about how much further work is needed. This tension becomes sharper in the next finding, where AI workloads emerge not as a solved problem but as the leading firewall security concern.

3.2 AI workloads: top concern, top priority

For all the confidence organizations express in their firewall coverage, they do not regard AI as a solved problem. When asked which areas present the greatest security risk today, organizations identify AI workloads as their leading firewall security concern, cited by 27% of respondents, ahead of the next-highest area at 19% (see Figure 7). This is the pivot at the heart of the research: Coverage is believed to be broadly established, yet the very workloads that coverage is thought to address are simultaneously named the top risk. Confidence and concern coexist, a sign that AI has risen quickly up the agenda without organizations feeling they have fully caught up to it.

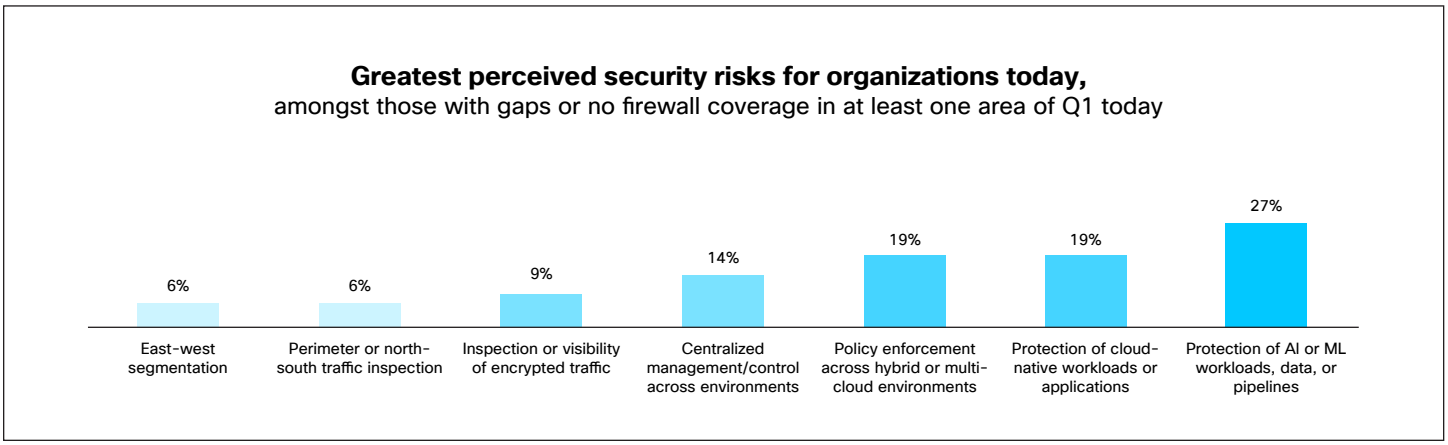


Figure 7. (Q2) Which of these areas presents the greatest security risk for your organization today?
Base: Respondents reporting gaps or no firewall control in at least one area, showing only the areas identified as having gaps or no control [475 respondents].

That concern is translating into intent. Among organizations that have modernized, are modernizing, or plan to, AI-related needs feature prominently in what they are prioritizing: AI-assisted threat detection and response sits alongside firewall coverage for AI workloads among the top three firewall modernization priorities (see Figure 8). AI is thus shaping the agenda from both directions: as a risk that organizations are working to contain, and as a capability that they are working to adopt.

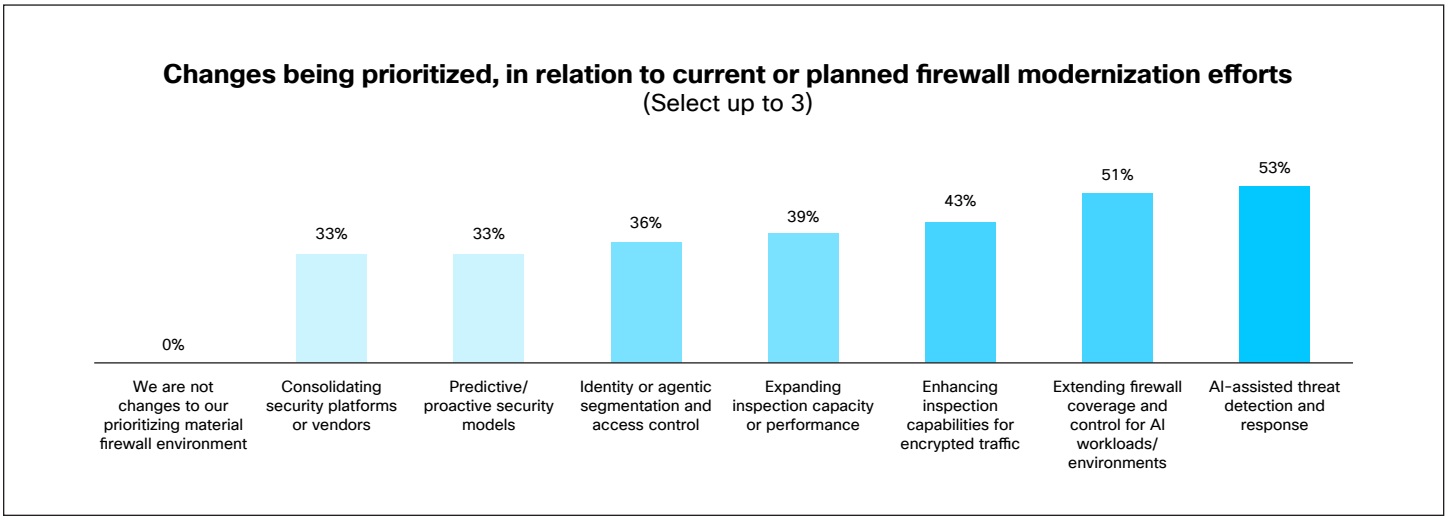


Figure 8. (Q7) What are the three main changes being prioritized in relation to your organization's current or planned firewall modernization efforts? Base: Modernized, modernizing, or planning to modernize firewall [498 respondents].

At the same time, it is worth keeping the finding in perspective. AI workloads lead the list of concerns and rank among the top modernization priorities, but they do so alongside enduring firewalling fundamentals rather than eclipsing them. The research points to AI as an important consideration—one that organizations are actively responding to—rather than a single dominant concern that has displaced everything else. That balance is a theme we return to in the next finding and again in Section 4.

3.3 Threat inspection stays constrained but diagnosed differently

If AI workloads are the leading concern, the natural next question is why organizations cannot simply extend their firewall controls to cover them more fully. The answer, in part, is that expanding threat inspection is itself constrained. When asked what limits their ability to increase threat inspection coverage today, organizations point to a range of factors; inspection of AI traffic and workloads is among them (see Figure 9). The constraint and the concern are linked. The same AI workloads organizations most want to protect are also among the harder things to inspect, which helps explain why confidence in coverage and anxiety about AI can sit side by side.

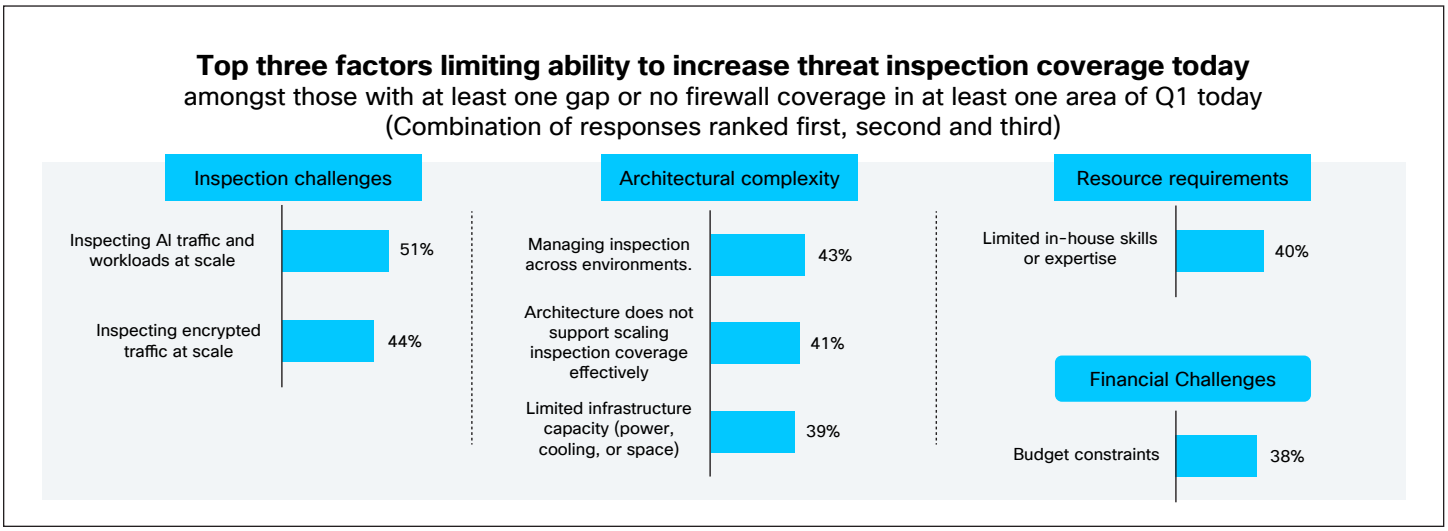


Figure 9. (Q3) What are the top three factors, if any, limiting your organization's ability to increase threat inspection coverage today? Base: Respondents reporting gaps or no firewall control in at least one area [475 respondents].

The more revealing pattern, however, is in how different roles explain the constraint. This is the third place in the research where senior leaders and operational roles diverge. Board and C-suite respondents are more likely to attribute the limitation to a skills gap—a shortage of the right people or expertise—while those in more operational roles point more readily to constraints in how their firewall estate has been deployed (see Figure 10). It is a subtle but consequential difference in diagnosis: One view locates the problem in the team, the other in the organization's current deployment.

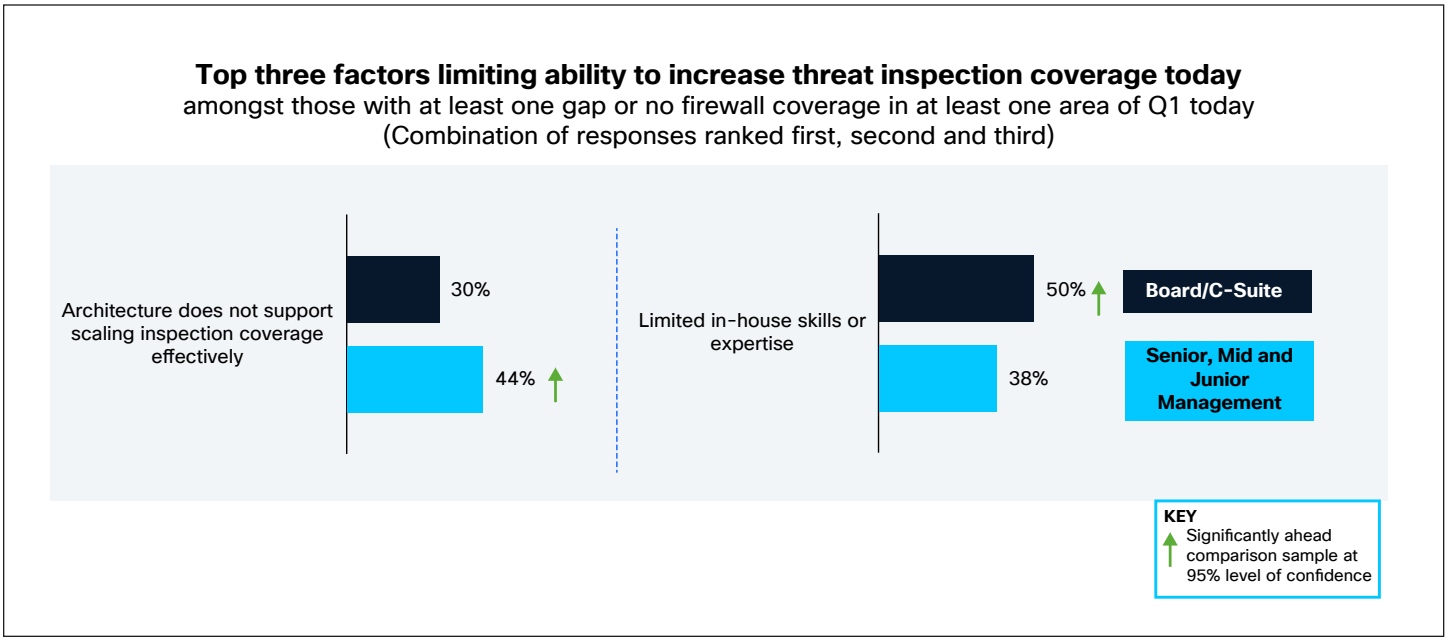


Figure 10. (Q3) What are the top three factors, if any, limiting your organization's ability to increase threat inspection coverage today? Base: 500 respondents, split by Board/C-suite [109 respondents] and other management [391 respondents].

That divergence matters because diagnosis drives remedy. A leadership team that reads the constraint as a skills gap is likely to reach for hiring, training, or managed services; a team that reads it as a deployment or architecture limit is likely to press for changes to the firewall estate itself. Where the two groups disagree about the cause, they risk investing in solutions that do not address the actual bottleneck. Taken together, the three findings in this section show AI steadily reshaping how organizations perceive, prioritize, and struggle with firewalling, while leaders and their teams do not always agree on how far the work has come or where its hardest problems lie.

4. How AI Is Changing Firewalling

The preceding sections established that AI has climbed the list of firewalling concerns and priorities. This section turns to what is actually changing on the ground: the concrete ways AI is reshaping firewall environments, how organizations are responding, and how those pressures are beginning to reorder what they value when they choose a firewall.

The first thing to note is that AI's impact is not confined to a single dimension. Organizations report that AI is driving a range of changes across firewalling at once, spanning security, operations, and infrastructure (see Figure 11). Rather than a narrow, isolated effect, AI is exerting pressure across multiple fronts of the firewall environment: new risks to defend against, new operational demands on the teams running firewall controls, and new requirements on the underlying infrastructure. This breadth is consistent with the picture in Section 3, where AI surfaced both as a leading concern and as a driver of modernization priorities.

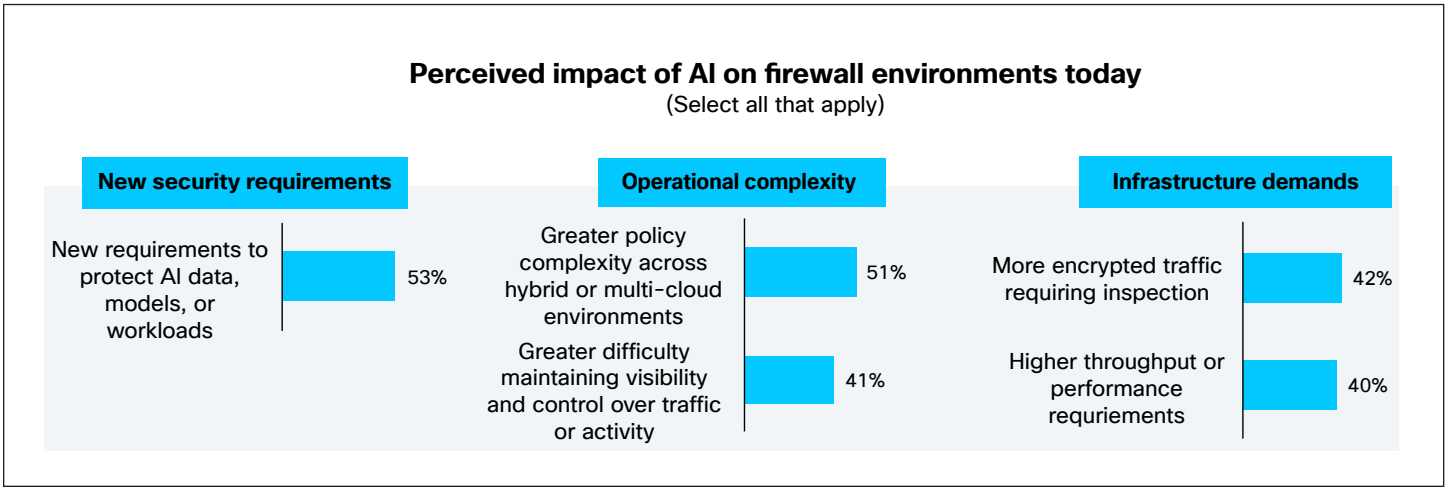


Figure 11. (Q12) How, if at all, is AI impacting your organization's firewall environment today? Base: 500 respondents.

Faced with these pressures, organizations are not standing still. Most report that they are actively adapting their firewall environments in response to AI rather than deferring the question (see Figure 12). This matters because it distinguishes AI from a purely theoretical or future concern; the impacts described in Figure 11 are already prompting concrete responses. Firewalling in the AI era is, for most organizations, an area of active adjustment rather than wait-and-see.

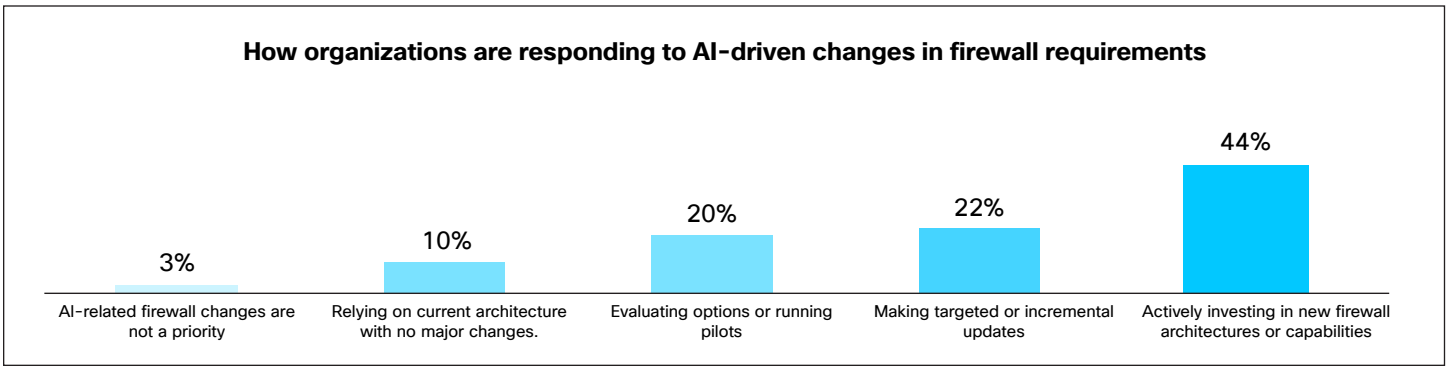


Figure 12. (Q13) How is your organization responding to AI-driven changes in firewall requirements, if at all? Base: 500 respondents.

Perhaps the clearest sign of AI's growing influence is how it is reshaping firewall vendor selection. When asked which factors will matter most in choosing a firewall vendor over the next 18 months, organizations increasingly foreground AI-related capabilities and the ability to support AI security needs and workloads (see Figure 13). In doing so, they have pushed some traditional considerations, such as compliance, lower down the list of selection criteria, and this reordering holds across most industry sectors. That is a striking shift: Named by 48% of respondents, AI-related capability now outweighs compliance at 33%, and compliance has long been a major driver of security purchasing decisions.

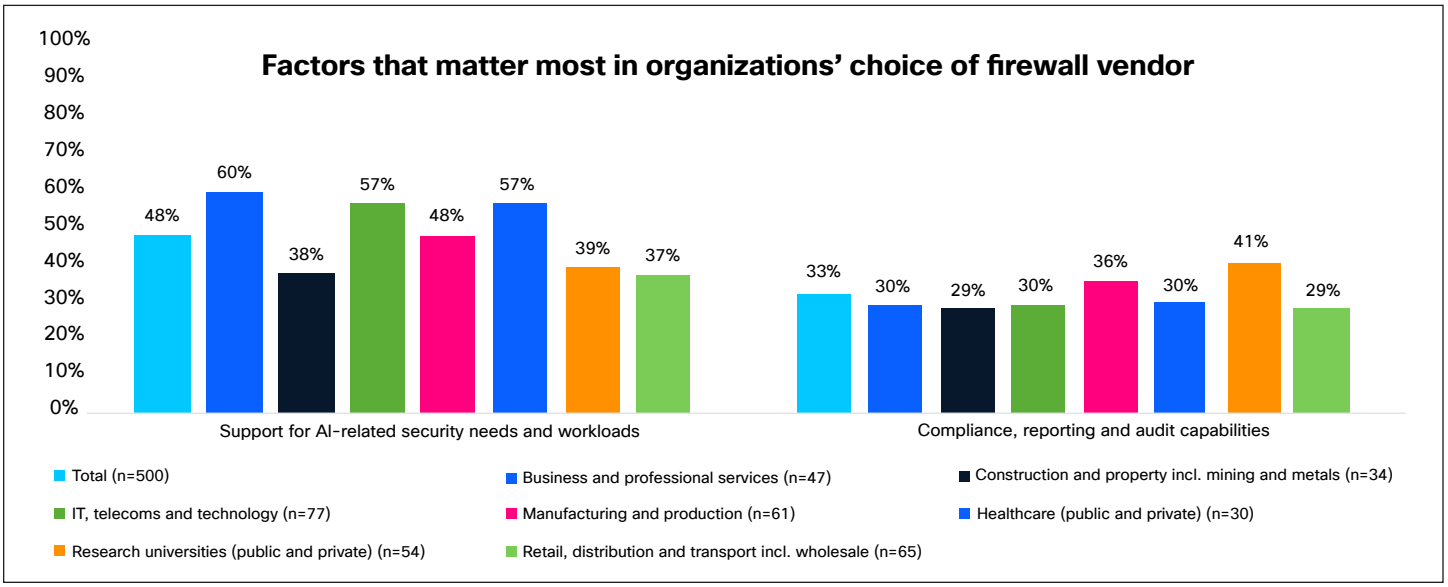


Figure 13. (Q15) Which factors are likely to matter most in your organization's choice of firewall vendor over the next 18 months? Combination of responses ranked first, second, and third. AI-related capability and compliance shown for comparison; other factors omitted for clarity. Base: 500 respondents.

This shift, too, should be kept in perspective. AI has clearly begun to displace long-standing considerations in vendor selection, but "lower in priority" is not the same as "no longer relevant." Compliance and the other established fundamentals of firewalling remain firmly in the picture; AI has simply grown large enough to reorder the list rather than rewrite it.

5. Conclusion

Firewalling has weathered major shifts in network security for decades, and AI is no exception. This research makes clear that AI has already reshaped where organizations see risk, what they prioritize when they modernize, and what they value in a firewall vendor. For executives, three implications stand out:

- **AI is now a decisive firewalling consideration, but the fundamentals still hold**. AI emerged as the leading security concern, a top modernization priority, and a rising factor in vendor selection, pushing considerations such as compliance lower. It has reordered priorities, not replaced them. Leaders should treat AI as a first-class requirement without abandoning the disciplines that still matter.
- **Close the gap between confidence and operational reality before spending against it**. In three separate findings, the most senior view was more optimistic than the operational one. This is not just perception; it shapes where money goes. A team that believes coverage is more complete than it is will underinvest in real gaps, and one that misreads a deployment constraint as a skills gap will fund the wrong fix. The remedy is better-targeted spending, not more of it: Reconcile the two views first, then commit resources.
- **Firewalling in the AI era is active adjustment, not wait-and-see**. Most organizations are already modernizing and adapting to AI. The question is not whether to act, but how to act with a clear-eyed view of one's own coverage gaps, constraints, and priorities.

6. About the Research

Cisco® commissioned independent market research specialist Vanson Bourne to conduct this research. The study surveyed 500 professionals familiar with their organizations' firewalling practices, spanning a range of seniority levels from Board and C-suite leaders through to operational management. Respondents were screened for eligibility to ensure they had sufficient knowledge of their organizations' firewall environments, and their responses were quality-checked before being included in the final dataset.

The charts below summarize the composition of the respondent base by seniority, region, industry sector, and organization size.

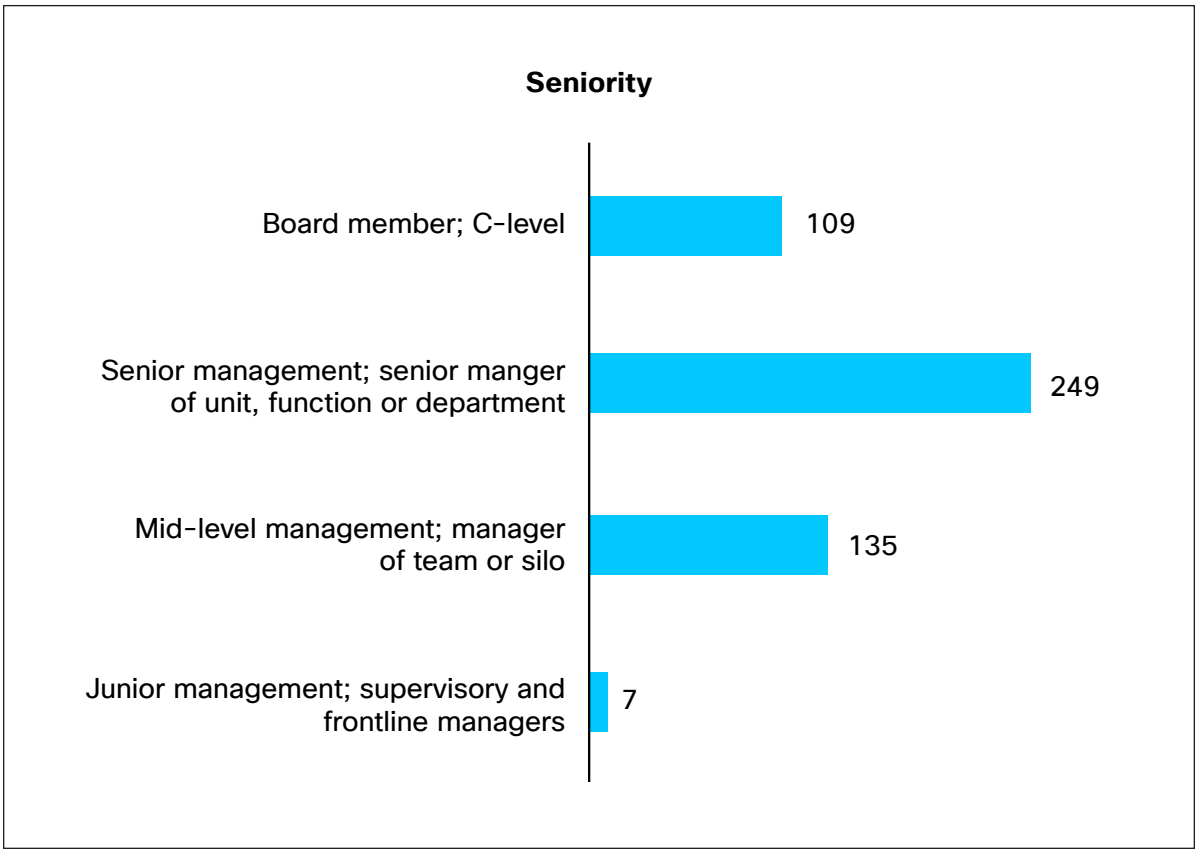
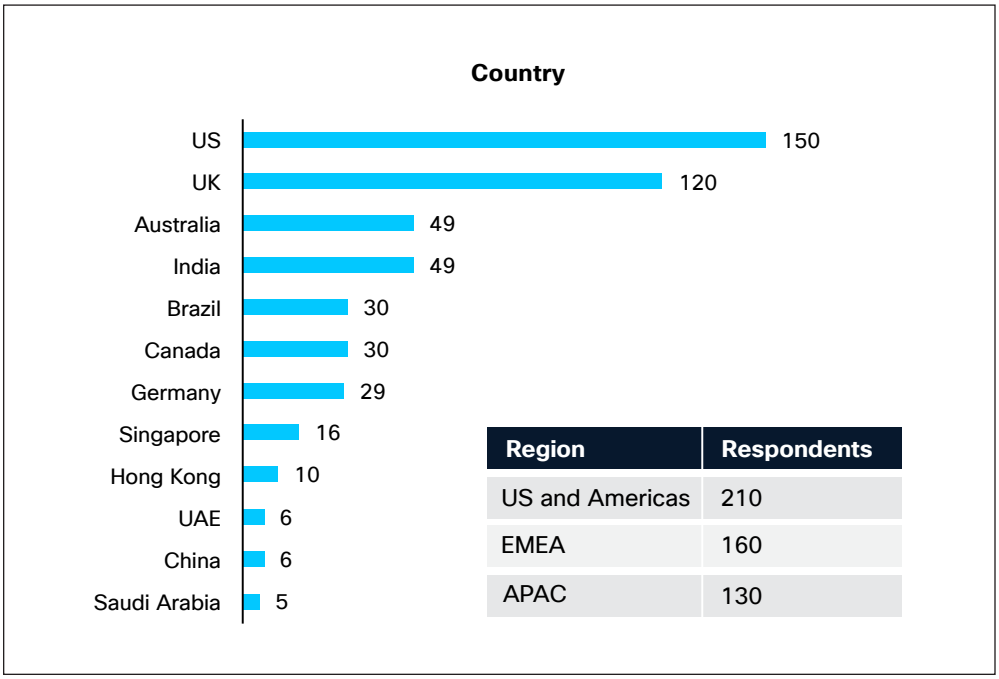


Figure 14. Respondents by seniority. Base: 500 respondents.



Region	Respondents
US and Americas	210
EMEA	160
APAC	130

Figure 15. Respondents by country/region. Base: 500 respondents.

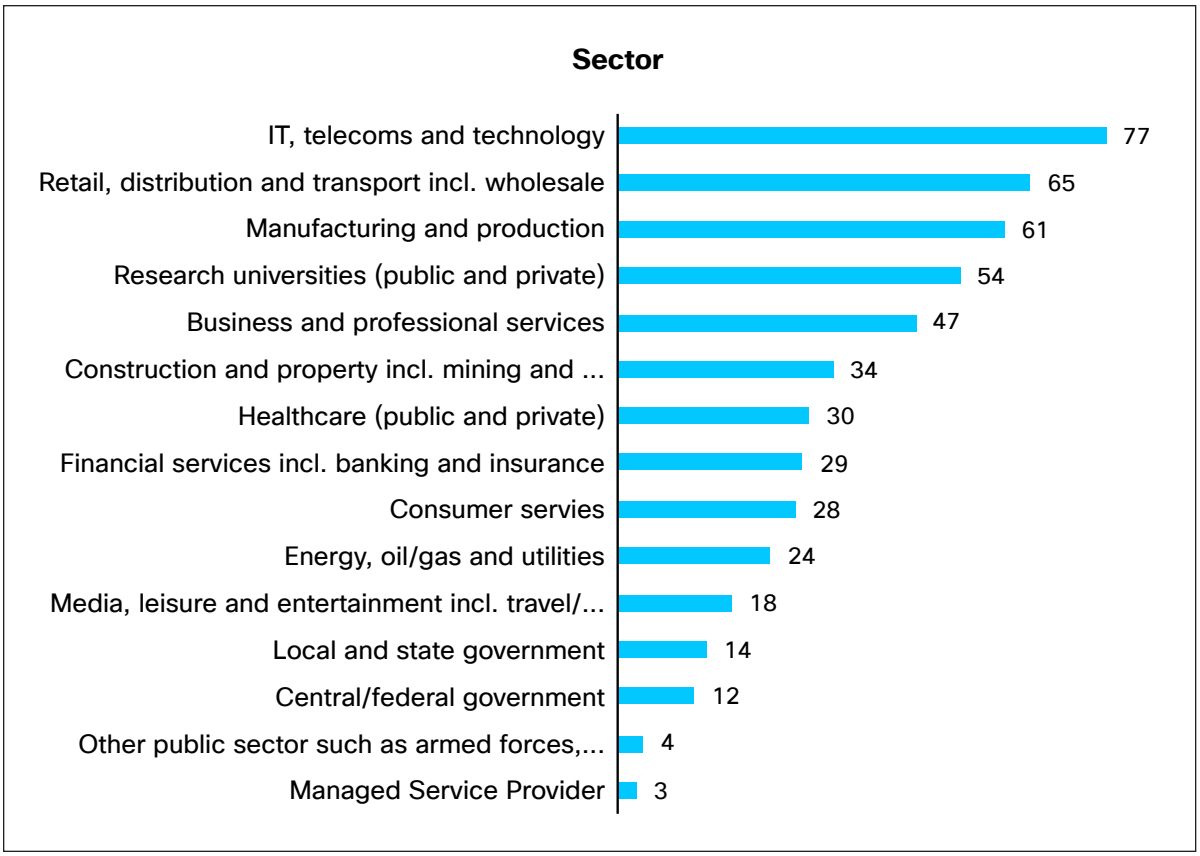


Figure 16. Respondents by industry sector. Base: 500 respondents.

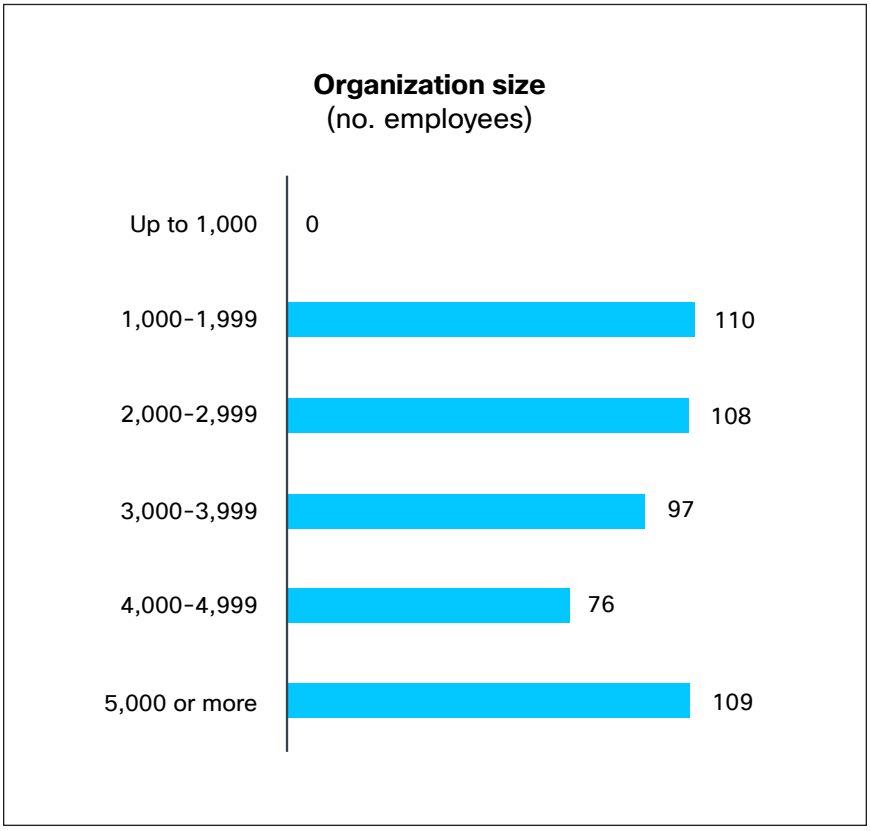


Figure 17. Respondents by organization size. Base: 500 respondents.

7. References

[1] Cisco Systems, Inc., “The Segmentation Report.” Oct. 2025. https://www.cisco.com/c/en/us/products/collateral/security/hypershield/segmentation-report.pdf

[2] Cisco Systems, Inc., “Why Network Segmentation Projects Fail, and What to Do About It.” May 2026. https://www.cisco.com/c/en/us/products/collateral/security/hypershield/segmentation-report-2026.pdf

[3] R. Dube, “A Taxonomy of Segmentation in Network Security.” IEEE Access, vol. 14, pp. 16921–16935, Feb. 2026. https://ieeexplore.ieee.org/document/11364135

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.

C99-6590782-00 08/26