The 2026 CISO Budget Benchmark

Real-world data from 300+ CISOs and their 2026 security budgets

Table of Contents

Executive Summary

Today's cybersecurity budgets aren't lean. The average organization is currently making an annual investment of at least $5 million in people, tools, and services to shore up their cyber defenses, and most expect to spend even more next year.

According to our survey, though, 56% of cybersecurity professionals worry that these ample budgets aren't enough to counter increasingly sophisticated threats. 85% are spending more on cloud security than they did last year, and 88% plan to increase their team's focus on the cloud over the next two years. Yet there's little confidence that these efforts will drive reductions in real-world risk.

It's never been easy to align budgets with real-world risk exposure, but tool sprawl, cloud complexity, and accelerating AI adoption are adding to the challenge. 49% of respondents believe the cloud's complexity is the number one inhibitor to the success of their security program.

Increasing automation and improving visibility are respondents' top priorities for the near future, and 99% agree that AI's impact on cloud security will be transformational. But not all organizations have yet positioned themselves to take advantage of that transformative force.

Early adopters will gain an edge, but all organizations must move quickly if they're to get—and stay—ahead of AI-powered cyber threats. This means finding solutions that actually deliver comprehensive visibility and control across intricately complex cloud ecosystems.

We created this report to help security leaders understand what their peers are prioritizing as they move into a new budget cycle. We invite you to benchmark your decision-making against that of the CISOs who participated in our survey. You'll see which bets others are making, what's getting left out and how security leaders are hedging. This information can serve as a reference point as you begin to flesh out your 2026 budget.

Key Takeaways

- ☑ 85% of organizations have increasing their security spending since last year.
- ☑ 88% anticipate a further increase for next year.
- ☑ 85% are increasing their cloud security budgets.
- ☑ 49% of respondents believe that the cloud's complexity is the number one inhibitor to the success of their efforts to secure cloud resources.
- ☑ 99% believe that AI will transform the future of cloud security.

Introduction

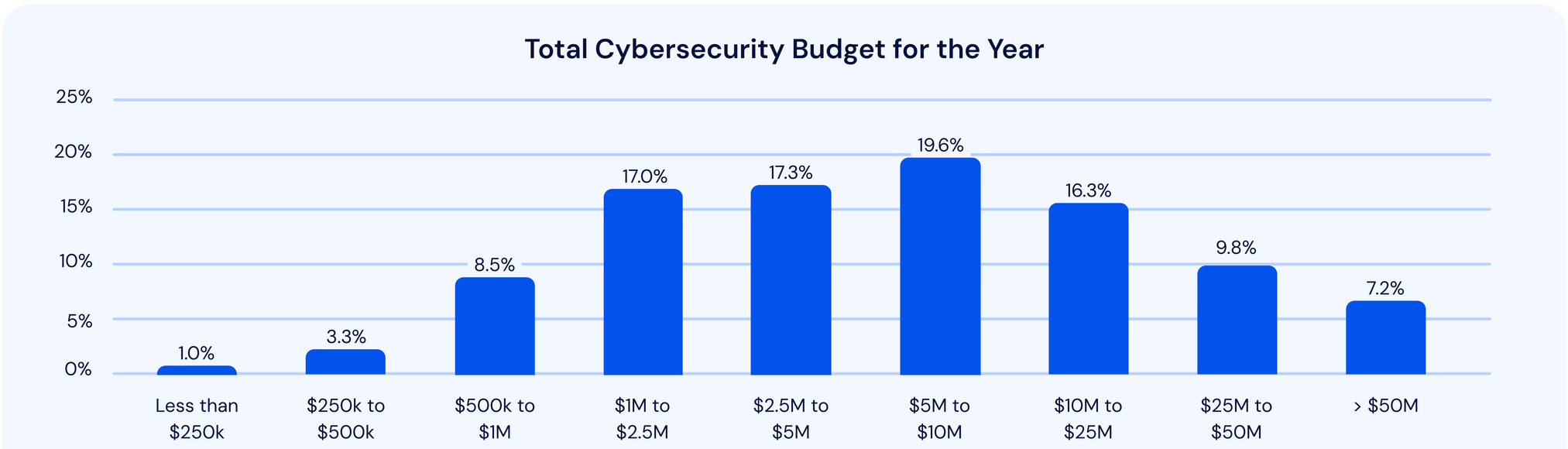
To better understand how CISOs are making tough budget calls in a high-risk, AI-powered, multi-cloud world, we recently partnered with the AimPoint Group to survey more than 300 cybersecurity leaders and practitioners. Participants included CIOs, CISOs, and Vice Presidents/Heads of Security, as well as directors, managers, and team leads in cybersecurity. Their organizations ranged in size from 1,000 employees to more than 25,000, across a broad array of industries.

In this report, we present our findings. This goes beyond the typical budget survey to provide deep insights into how today's leaders are trying to turn spending into a strategic advantage.

1 CISOs Aren't Being Asked to Do More with Less

Survey Data Insights: Cybersecurity spending is ample. When enterprise security budgets are viewed as a bell curve, the peak is between $5 and $10 million. Nearly 20% of respondents reported spending in this range. More than half of respondents (53%) indicated that their organization is spending more than $5 million annually on cybersecurity tools, staffing, and services. 17% are spending more than $25 million each year.

Which best describes your organization's total budget for cybersecurity this year — including all staff, products, and services?

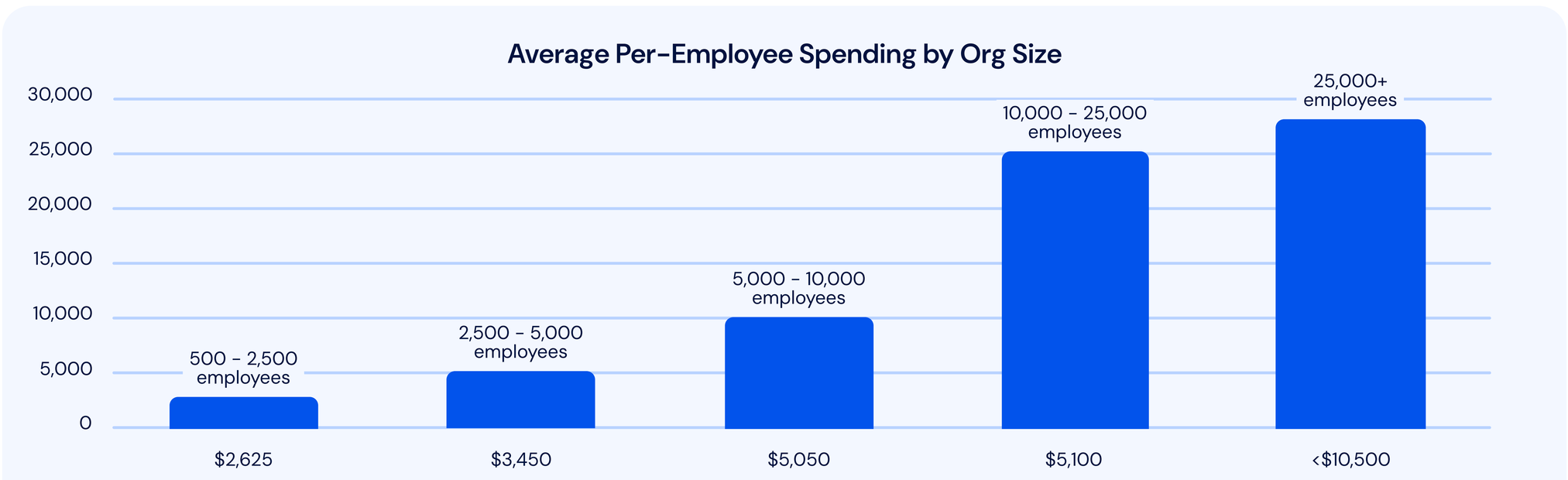


This spending doesn't align neatly with size. The smallest companies (with 500 to 2,500 employees) are spending between $250 and $5,000 per employee on cybersecurity, while the very largest (with more than 25,000 employees) are budgeting anywhere between $100 per employee and over $20,000 per employee.

There's a bit more correlation with vertical. Organizations in healthcare, technology and financial services are the biggest spenders.

- 67% of healthcare organizations are spending more than $5 million annually on cybersecurity
- 57% of tech companies are spending above $5 million
- 54% of financial services firms are spending more than $5 million

Financial services firms are the most likely to be super-high spenders, with 11% reporting annual budgets in excess of $50 million.



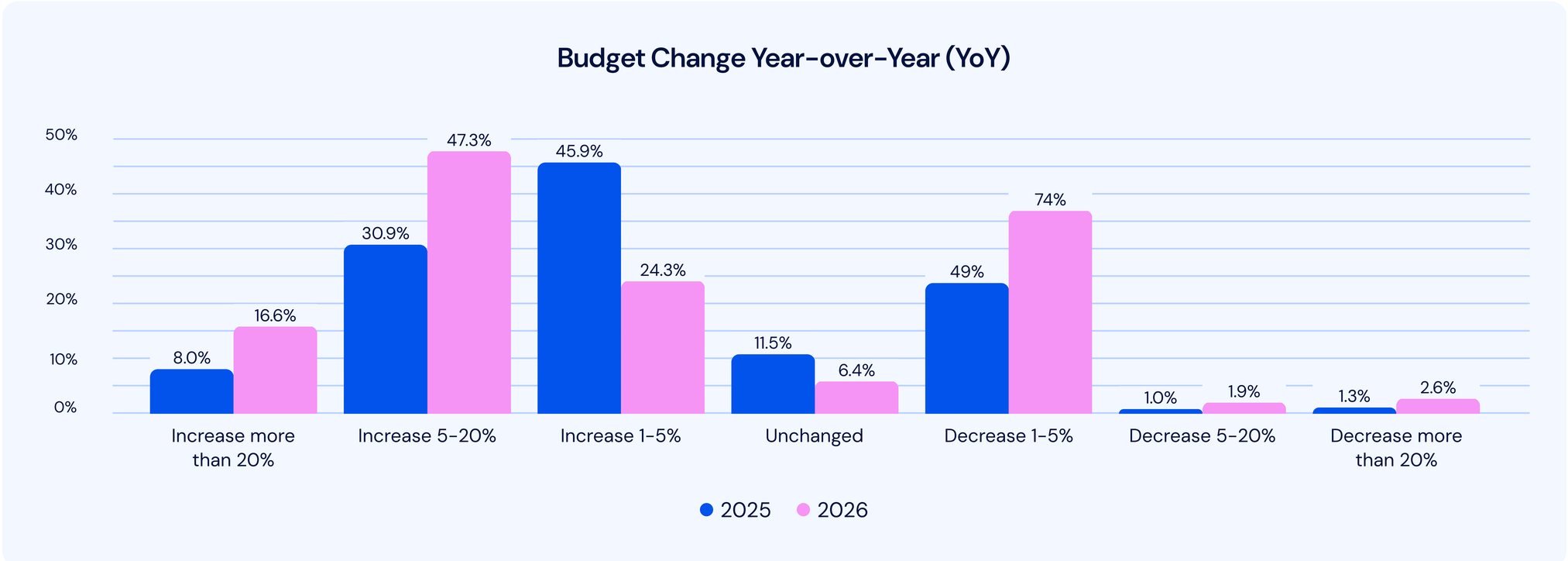
Budget growth is on the horizon. 85% of respondents report that their organization's cybersecurity spending has increased since last year, and 88% anticipate further increases next year. The largest group (46%) is seeing a small increase (between one and five percent) this year, but larger increases are expected the following year. **64% expect to see a budget increase greater than five percent next year, with 47% looking forward to budget increases between five and 20%.**

These numbers are roughly in line with what analysts have forecasted. Gartner, for instance, has projected a 15.1% increase in overall cybersecurity spending for 2025, while IDC forecasted a 12.2% increase globally for the coming year.

Perhaps because their budgets are already very generous, fewer very large enterprises (those with more than 25,000 employees) are making major increases. Only 38% of very large enterprises are increasing their budget by more than five percent this year, and just 41% will do so next year.

Across verticals, organizations in manufacturing are most likely to be increasing their budgets this year (96%) are doing so, while retailers are least likely to be increasing their budgets (though 73% are still doing so). Retailers and e-commerce companies are also the most likely to be shrinking their budgets for next year (8% plan to do so).

Which best describes the expected change in your organization's cybersecurity budget for each period?



Why This Matters: These results indicate that today's CISOs are not being called upon to do more with less. Instead, they're being asked to do more with more. This may be due to greater board-level awareness of cyber risks, or simply because executive leaders anticipate inflation. The US Consumer Price Index currently projects inflation at 2.74%, with some analysts expecting increases throughout the second half of 2025 and into 2026. Nonetheless, in the vast majority of organizations, cybersecurity budgets are increasing significantly faster than consumer prices.

2 Healthy Budgets Still Don't Satisfy

Survey Data Insights: Most security professionals don't believe that even these growing budgets are enough to counter today's threats. 56% of respondents agree that their organization's overall security spending is not enough to mitigate the risks that they face. A similar number (55%) agree that their cloud security spending isn't adequate.

The closer they are to the hands-on action, the less satisfied respondents are likely to be. 62% of security managers don't believe that overall security spending is sufficient, and 59% don't believe that current cloud security spending is enough. Discontent is also running high among architects and engineers, 60% of whom are dissatisfied with both overall security spending and cloud spending.

Interestingly, respondents in the organizations that are spending the most (those with total annual budgets over $25 million) are among the least satisfied, with 60% of the members of this group reporting that their overall and cloud security spending are insufficient to protect against today's threats.

Describe your agreement with each statement: "My organization's level of spending on ..."

Statement	Strongly agree	Somewhat agree	Somewhat disagree	Strongly disagree
"... cybersecurity overall is NOT sufficient given the current state of our defenses and/or the risks we face."	12.9%	43.1%	33.0%	11.0%
"... cloud security overall is NOT sufficient given the current state of our defenses and/or the risks we face."	14.2%	40.6%	34.0%	11.3%

CISO Viewpoint

"I don't know of any security program that feels like it has enough budget to do everything its leader wants to do, but I recognize, from an operational perspective, that there are limits to how fast we can scale. A lot of the time, CISOs are put in an untenable position, because we have to protect the business from every threat that's out there, and the budget doesn't change as quickly as attackers' capabilities do. For this reason, it's essential for the company to understand its risk appetite, and then budget appropriately."

CISO, Financial Services

Why This Matters: Even CISOs with the biggest budgets aren't satisfied. Their budgets might be healthy — and rising — but confidence isn't, especially among the biggest spenders. These doubts highlight the disconnect between spending and results that has long been a problem across the industry. CISOs are under growing pressure to demonstrate outcomes, not effort, to organizational leadership and boards, but it's harder than ever to prove ROI on many of today's most widely adopted toolsets.

Call to Action: CISOs must adopt ROI frameworks that directly link spending to risk reduction. By taking a structured, data-driven approach to risk prioritization — one that's grounded in deep, contextual risk analysis — they can ensure that they're addressing the threats and vulnerabilities with the greatest potential impact on the business first.

3 People: The Number One Line Item in Cybersecurity Budgets

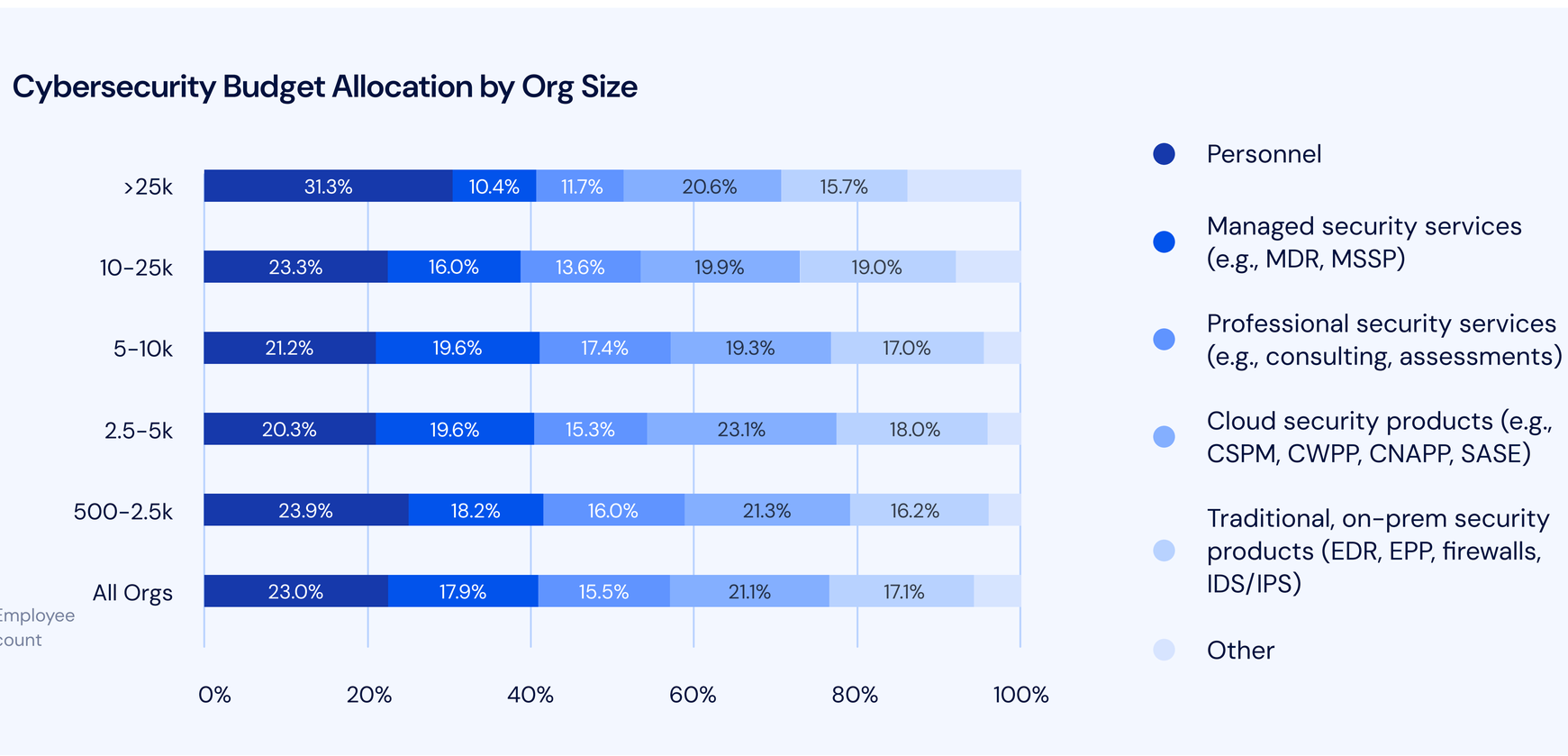
Survey Data Insights: Overall, organizations are spending more on labor than any other aspect of cybersecurity. Considering that employees with these specialized and sought-after skills can command top salaries, this is no surprise.

Because they're more likely to be operating in-house security operations centers (SOCs), larger enterprises are spending more on payroll than others. Organizations with more than 25,000 employees allocate significantly more of their total budget to personnel costs than average (31% vs. 23%).

Smaller and midsized companies direct more funds towards managed security services such as managed detection and response (MDR). In fact, for organizations of all sizes, almost 40% of the total cybersecurity budget goes towards the combination of managed services and personnel.

The second-highest line item for most companies is cloud security products, including cloud security posture management (CSPM), cloud workload protection platforms (CWPP), and cloud-native application protection platforms (CNAPP). On average, cloud security products consume almost as much of the total cybersecurity budget as labor (21% vs. 23%). Organizations with between 2,500 and 5,000 employees are allocating more of their budget to cloud security than labor (23% vs. 20%), perhaps because these companies are among the most heavily reliant on outsourced services.

Which best describes your organization's total budget for cybersecurity this year — including all staff, products, and services?



CISO Viewpoint

"For us, outsourcing is sometimes a bit more expensive, but then you get more value, so it balances out. We use an MSSP so that we can have around-the-clock monitoring 24/7, while respecting work-life balance for our internal team. This reduces turnover and burnout, while giving our team more time to focus on learning about emerging technologies and other high-value activities."

CISO, Healthcare

Why This Matters: Cybersecurity talent has long been both scarce and valuable, so it isn't news that organizations are making major investments in personnel. What's noteworthy, though, is that outsourcing isn't solving the problem. Engaging a managed service provider might reduce the cost burden associated with hiring and retaining staff, but it doesn't necessarily simplify operations or reduce spending overall.

Call to Action: Outsourcing key aspects of security can be a huge asset for your organization, but finding the right provider is crucial. Outsourcing is particularly valuable when the third-party provider can deliver full-stack visibility across cloud assets, categories and vulnerabilities without introducing operational friction. The provider should support the model (fully managed or co-managed) that best suits the size and maturity level of your organization, and should align its processes with your engineering and DevOps workflows. Avoid black boxes. Instead, look for a provider who is open about what's being flagged and why.

4 Cloud Consumes up to Half the Security Team's Time—with an Appetite for More

Survey Data Insights: Organizations are directing a large amount of their valuable human resources towards cloud security. In the majority of organizations (60%), between 20 and 40% of security team members focus their efforts on the cloud. Nearly one-third (32%) of organizations are focusing more than half of their security team on the cloud.

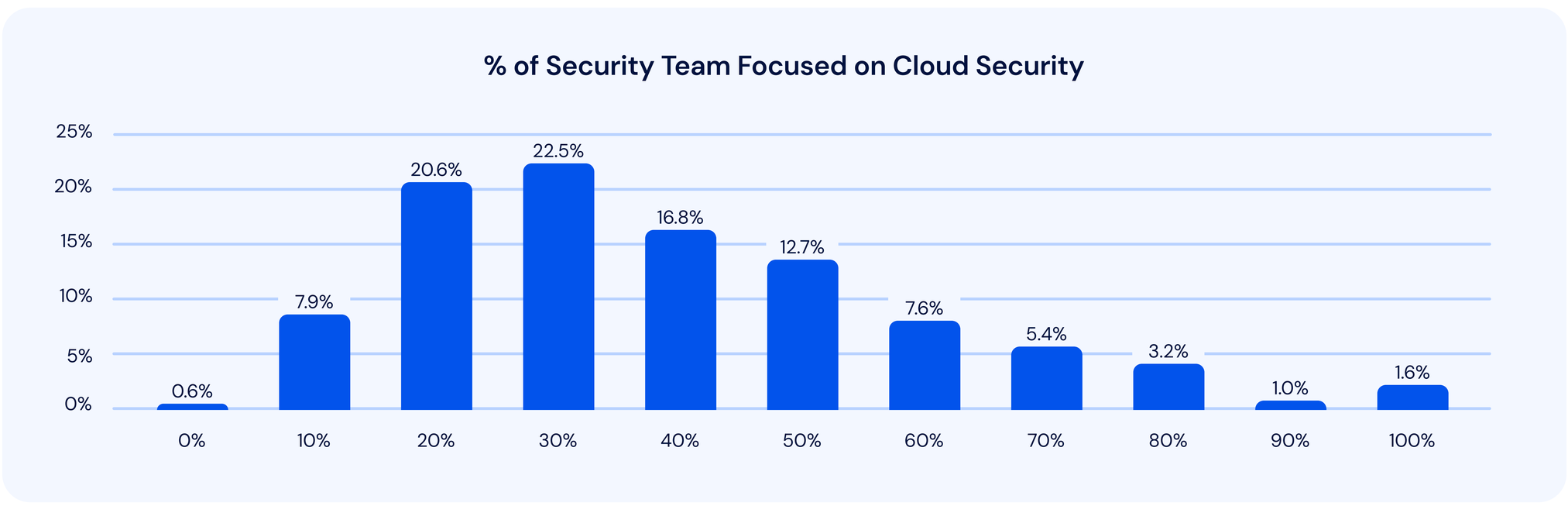
This tendency is especially pronounced in the very largest enterprises and those with the biggest budgets.

1. 38% of enterprises with more than 25,000 employees are focusing more than half of their security team on cloud security
2. 39% of organizations with annual cybersecurity budgets greater than $2.5M are focusing more than half of their security team on the cloud

Among verticals, retail is far less likely than average to have more than half of the security team focused on the cloud.

1. Just 8% of retailers have more than half of their security team focused on the cloud
2. 77% of retailers have between 20 and 40% of their security team focused on the cloud.

Approximately what percentage of your organization's security team is focused on cloud security?



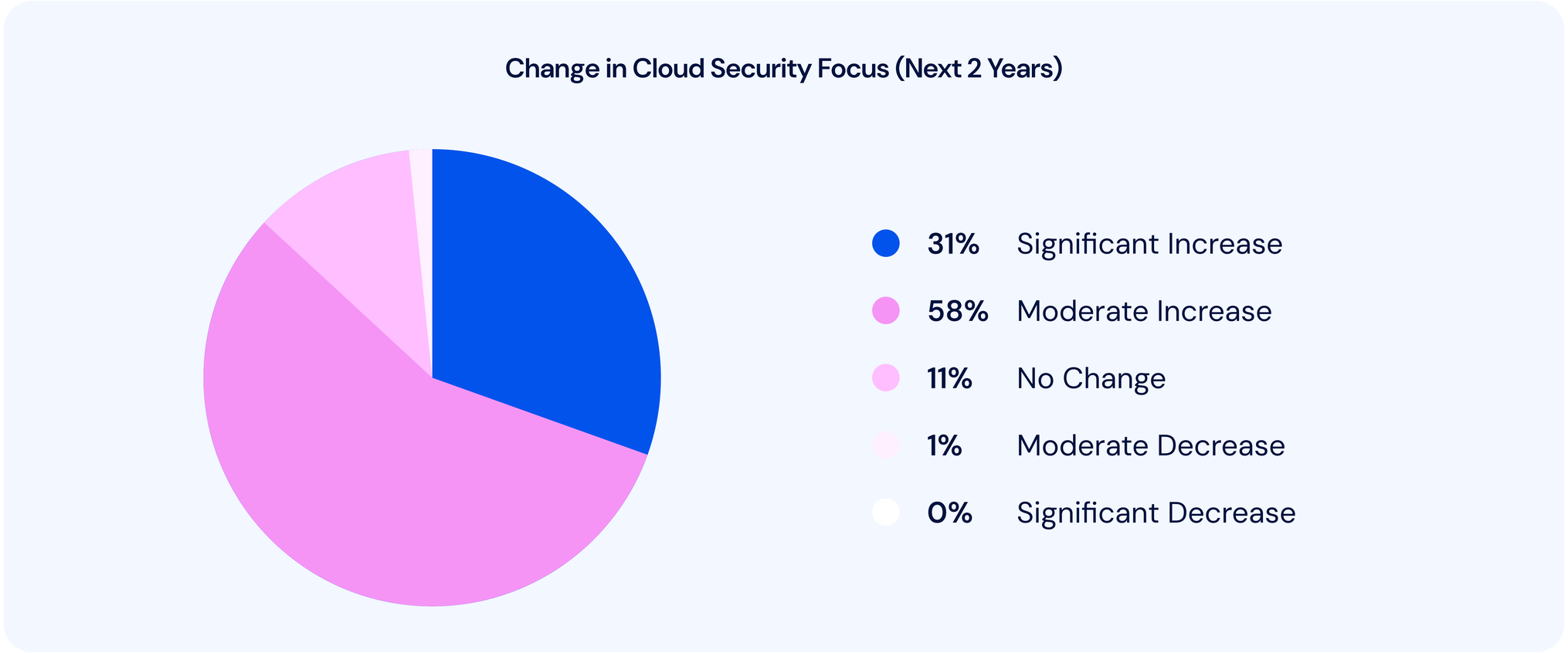
Not only are these investments of labor and skills significant, but they're going up. 88% of organizations plan to increase their security team's focus on the cloud in the next two years. Nearly one-third of organizations (31%) are planning for a significant increase in their team's cloud focus.

Small to midsized organizations are especially likely to be planning to increase their security team's cloud focus. 93% of respondents from organizations with between 2,500 and 10,000 employees report that their companies will be focusing more of their security efforts on the cloud in the near future.

Interestingly, the organizations with the very largest security budgets are more likely to be increasing their focus on the cloud. Among those spending more than $25 million each year on cybersecurity, 92% are planning for an increase in cloud focus, and 42% anticipate a significant increase there.

Retailers are less likely than the average organization across verticals to be planning for a major increase in cloud focus. Only 23% of respondents in retail said that they plan for a significant increase, but they're playing catch-up overall, with 89% of retailers planning for some increase in their team's focus on the cloud.

How do you expect that percentage to change over the next two years?



Why This Matters: The cloud already commands up of half of security teams' time and attention, and the problem's only getting worse. The complexity, scale, and dynamism of cloud risks can rapidly overwhelm manual processes, leading to alert fatigue and opening gaps in protection. When security teams are constantly engaged in the context switching that fragmented toolsets demand, they can't focus on the most urgent risks to the business.

Call to Action: A platform-driven approach that's grounded in automation and consolidation is the antidote to cloud complexity. Not only does adopting this approach reduce the burden on security teams, but it also unlocks the organization's ability to move faster, reduce risks more effectively, and foster operational resilience.

5 Cloud Leads the Pack Among Spending Priorities

Survey Insights: Cybersecurity spending might be increasing overall, but some categories are seeing more growth than others. In 85% of organizations, cloud security spending has increased since last year, while data security spending is up in 77% of organizations. In addition, cloud security spending is increasing significantly in 32% of organizations, and data security spending is increasing significantly in 26%.

The professional services category is at the bottom of the heap, with only 50% of organizations increasing their spending in this area, and only 15% making significant increases.

Among technology companies, the top area for increased spending is data security, with 86% indicating an increase in this area. The same is true of manufacturers, 85% of whom indicated that data security spending is up.

How has your organization's spending changed since last year for each category?

Security Category	Significant increase	Moderate increase	No change	Moderate decrease	Significant decrease	Net increase
Application	15.7%	54.3%	25.9%	3.5%	0.6%	70.0%
Cloud	32.1%	53.1%	12.9%	0.9%	0.9%	85.2%
Data	25.8%	51.6%	21.7%	0.6%	0.3%	77.4%
Endpoint	16.4%	47.3%	34.4%	1.6%	0.3%	63.7%
Identity & Access	16.4%	53.3%	28.1%	1.6%	0.6%	69.7%
Network	22.5%	45.9%	28.8%	1.9%	0.9%	68.4%
Managed Services	19.1%	43.0%	33.1%	3.5%	1.3%	62.1%
Professional Services	14.7%	34.8%	41.9%	7.0%	1.6%	49.5%
Awareness & Training	15.6%	45.1%	35.2%	3.5%	0.6%	60.6%
SOC	15.7%	45.4%	35.5%	2.9%	0.6%	61.0%

> **CISO Viewpoint**
>
> "Data protection is our most business-critical priority. If we don't protect our clients' data, we won't have clients. If we don't have clients, we don't have a business. A lot of our data lives in the cloud, so maintaining a secure cloud environment is absolutely essential for our business."
>
> **CISO, Financial Services**

Why This Matters: When it comes to security spending growth, the cloud remains king. Other areas are still playing catch-up. It makes sense that the cloud is this important: cloud infrastructure supports the majority of digital business operations, so it's home to an enormous amount of cyber risk.

Call to Action: Prioritizing cloud security spending makes good business sense, since cloud security risk translates directly into business risk. Spending wisely is key, however. Top-line investments in modernizing cloud security can drive long-term savings by introducing efficiencies, enabling automation, and reducing waste—all while safeguarding operations and the business's reputation.

6 Tool Sprawl Is Real, and the Call to Simplify Is Loud

Survey Insights:

1. Today's cybersecurity tool stacks are far from simple.
   - 58% of organizations are running more than 25 different cybersecurity tools
   - 28% operate 50+ tools
   - An unlucky 13% have 100 or more tools.
2. Enterprise size matters. Among organizations with more than 25,000 employees:
   - 36% run 50+ tools
   - 25% run 100+ tools
3. Bigger budgets mean bigger toolsets. Among companies spending $25M+ annually on cybersecurity:
   - 71% have 25+ tools
   - 35% have 50+
4. Tool sprawl is also common for cloud security solutions:
   - 29% of organizations run 25+ cloud security tools
   - 12% run 50+

Feeling the tool sprawl? Download the CISO Security Tool Evaluation Framework to systematically assess your toolset, align security impact with business value, and streamline renewal decisions.

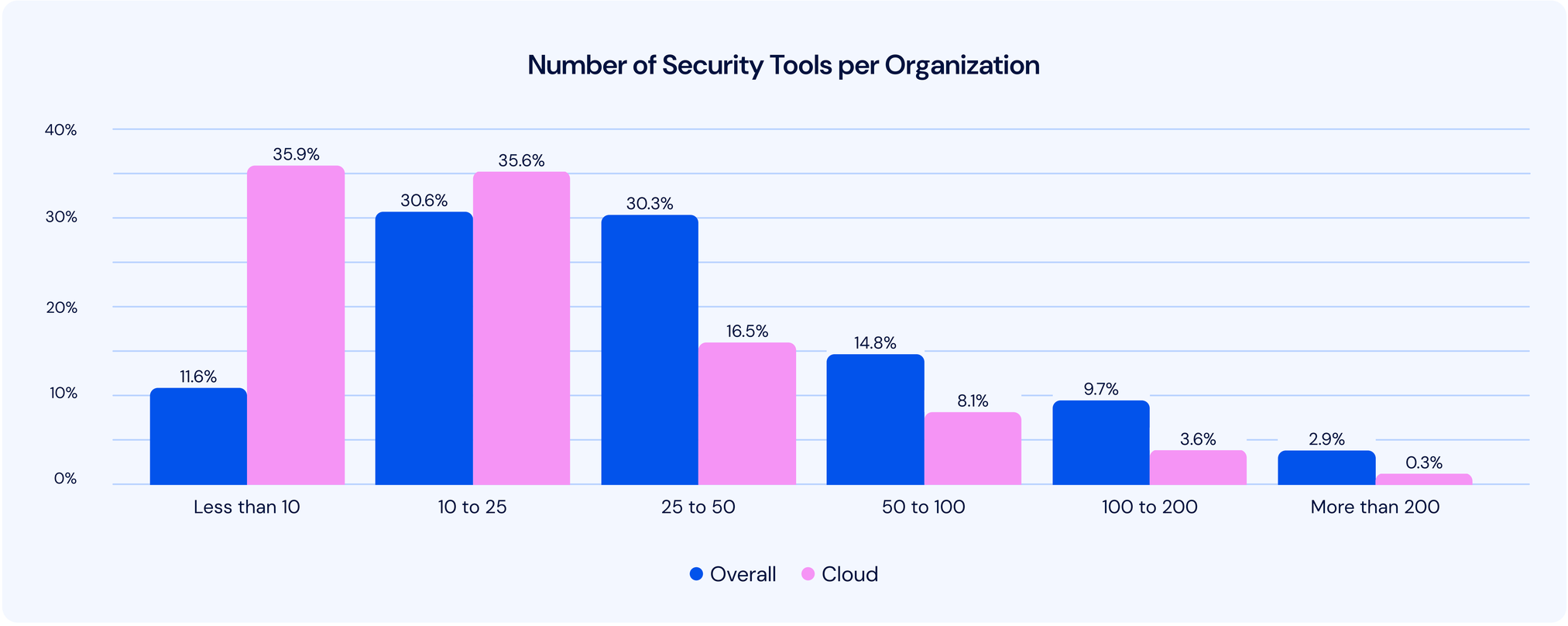
5. Mid-sized organizations operate the most cloud security tools:

    - 49% organizations with 5,000 - 10,000 employees run 25+ cloud security solutions
    - 24% run 50+

6. Retailers operate fewer cloud security tools than organizations in other industries.

    - Just 23% of retailers have 25+ cloud security solutions
    - Only 8% have 50+

Approximately how many cybersecurity tools/products does your organization have overall? And how many does it have that are focused on cloud security?



Cloud complexity is inhibiting security effectiveness. When asked which factors were holding them back from having effective security in the cloud, respondents top-ranked complexity and resource sprawl. 49% of respondents listed complexity as the biggest inhibitor to the success of their cloud security program.

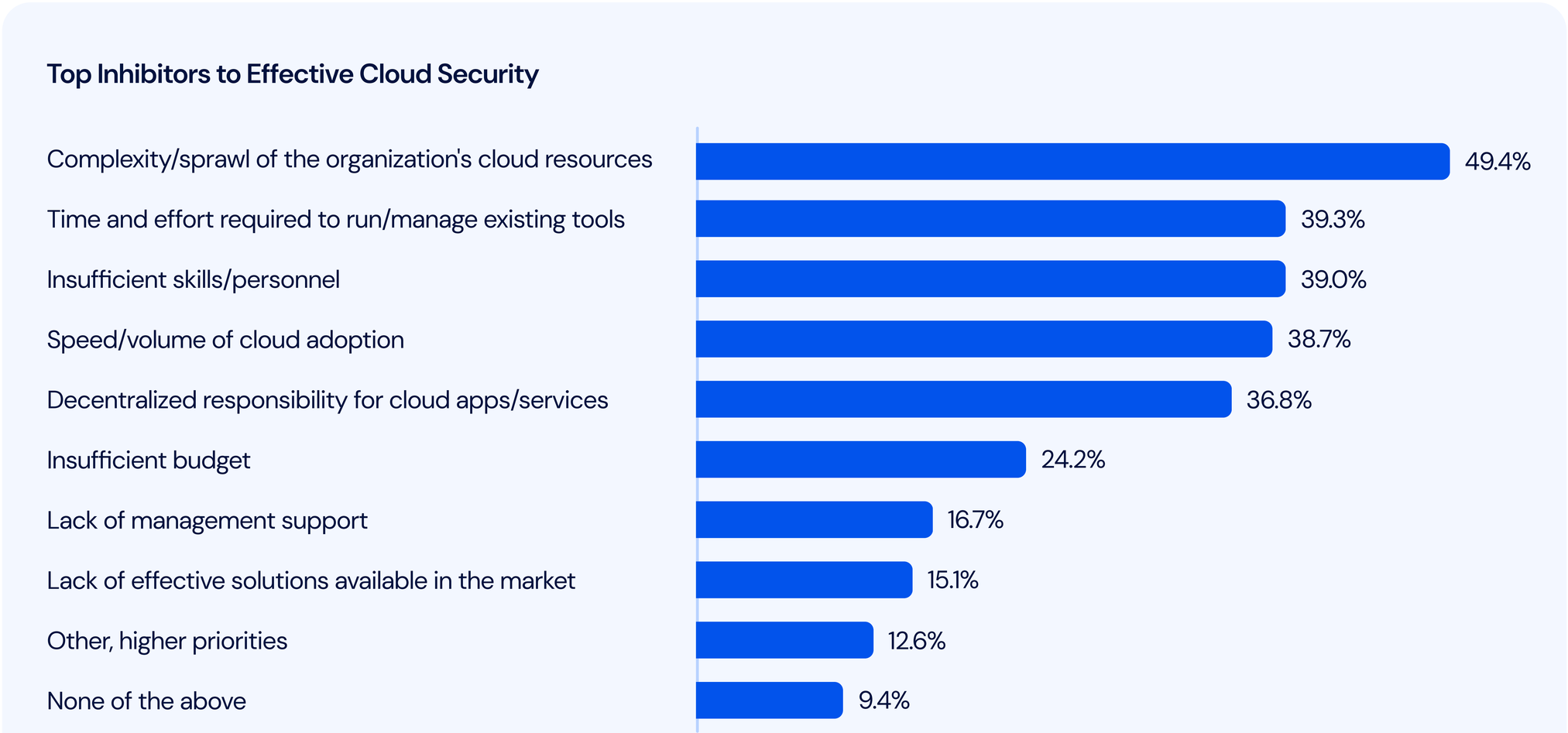
Three other responses were nearly tied for second place. These are:

- The time and effort required to run/manage cloud security tools (mentioned by 39%)
- Insufficient skills/personnel (mentioned by 38.7%)
- The speed and scale of cloud adoption (mentioned by 38.7%)

Near the bottom of the list were lack of management support (mentioned by 17%), lack of effective solutions (mentioned by only 15%), and other, higher priorities (mentioned by 13%). CISOs and security executives were especially unlikely to say that lack of management support is the problem (89% didn't mention this inhibitor).

Decentralized responsibility for cloud apps and services is a larger concern among CISOs, 40% of whom mentioned this as a top inhibitor. This is also the number one concern among practitioners, mentioned by 59% of security operations professionals. Lack of centralized responsibility and control is also among the top concerns of respondents from organizations with 10,000 to 25,000 employees (mentioned by 45% of the members of this group), those in healthcare (mentioned by 48%), and in retail (mentioned by 42%).

What are the top factors keeping your organization from having more effective cloud security? Select three.



Why This Matters: Security teams are buried under tools, not empowered by them. In and of itself, security spending does little to ease complexity, especially if it means adding more tools. When every problem has its own platform, overall effectiveness suffers.

Call to Action: CISOs need to consolidate solutions if they're to improve visibility. It's also critical to clarify ownership and responsibility, and to invest in solutions that simplify the stack rather than adding to the complexity. Most importantly of all, CISOs need new models and approaches that will improve their collaborative relationships with the business, as well as with growing AI teams that tend to bring their own tools.

7 AI Is Reshaping Security... But Not Everyone Feels the Impact Yet

Survey Insights: Organizations are investing heavily in AI to boost operational efficiency and counter AI-driven threats. The top factors driving security spending include a desire to invest in AI-powered security solutions (mentioned by 54%), improving the speed and/or efficiency of security operations (mentioned by 49%), and countering AI-driven threats (mentioned by 47%).

The following responses were nearly tied for fourth place:

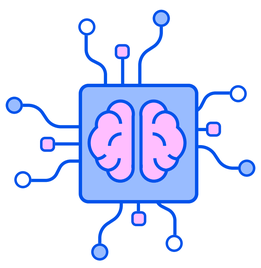
- Securing cloud infrastructures and services (mentioned by 45%)
- Addressing the skills gap (mentioned by 44.7%)
- Meeting regulatory requirements (mentioned by 44.7%)

At the bottom of the list were responding to incidents and breaches (mentioned by 19%), board or cyber risk insurance requirements (14%), and tool sprawl and vendor consolidation (only 11%). It may be that vendor consolidation is so low-ranked because it is more often perceived as a means to achieve cost savings than as a driver of spending.

Also near the bottom: economic and political uncertainty, which was mentioned by only 20% of respondents. This is good news for risk reduction, since it shows that people are interested in countering real-world threats, regardless of the macroeconomic or geopolitical landscape. If anything, such uncertainties might motivate stakeholders to increase budgets, since nation state actors are more likely to launch attacks under such conditions.

It's no surprise that the very largest enterprises (those with 25,000 employees or more) indicate that regulatory compliance is a major driver of spending (mentioned by 59% in this group). Nor is it shocking that security executives have significant compliance concerns (47% of these respondents mentioned compliance).

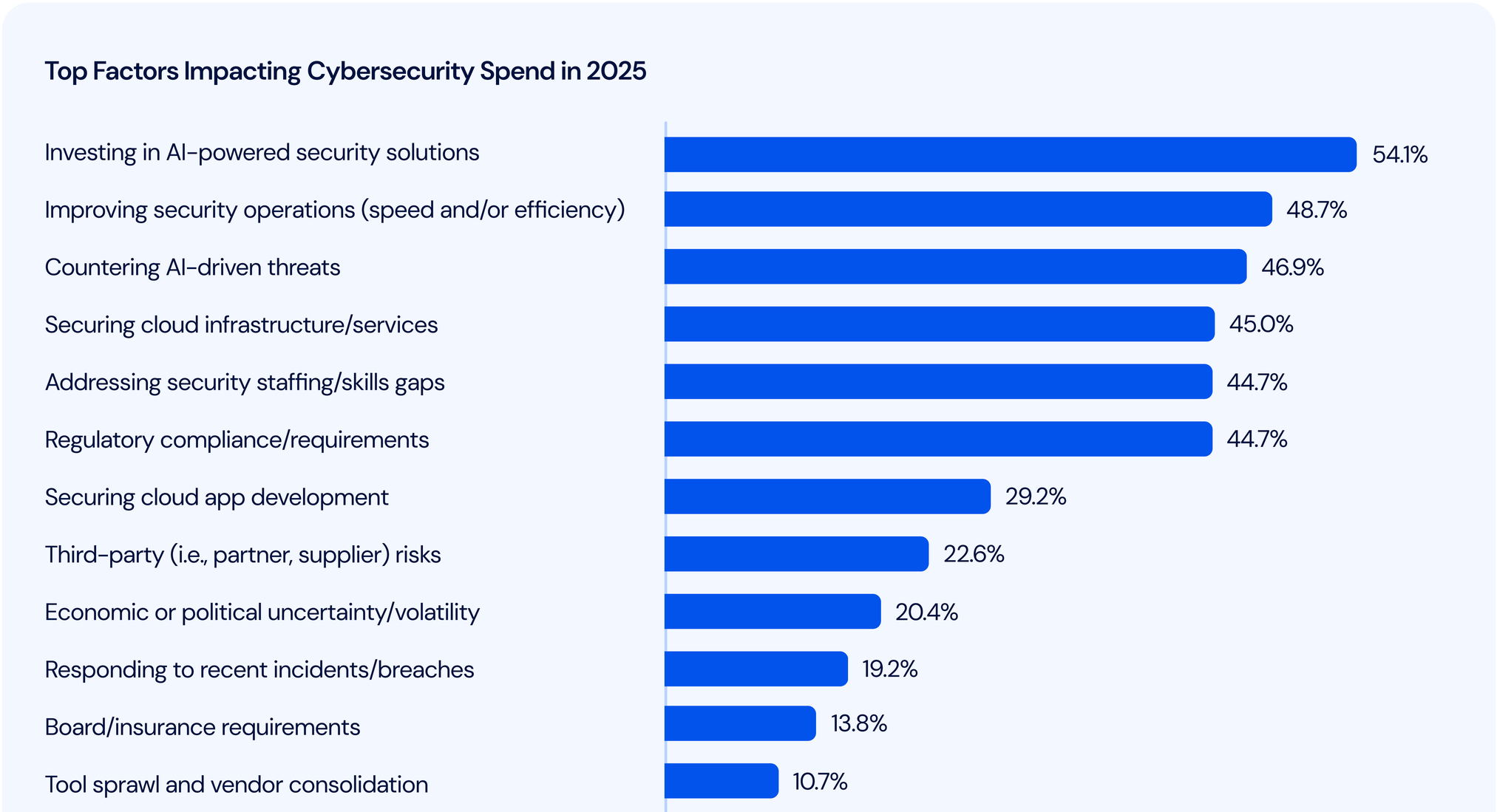
As would be expected, respondents in healthcare see compliance as a major driver of cybersecurity spending (mentioned by 48%). Healthcare organizations are particularly likely to be adopting AI-powered security solutions (68% mentioned spending on this), as are retailers (69% mentioned). Financial services firms, meanwhile, are more concerned about countering AI-driven threats (61% mentioned).



AI-related spend isn't always coming from the traditional security budget.

Some enterprises are now setting aside corporate-level AI funds that security teams can tap into for AI-focused projects. Security leaders who position their initiatives as part of the organization's AI strategy may gain access to these additional funds — even when core security budgets are flat.

What are the top issues/factors impacting your organization's cybersecurity spending this year? Select four.



The new wave of AI-driven threats

Respondents aren't wrong to be worried about AI's impact on the threat landscape. It is indeed upending it, which AI models (and the data that feed them) have the potential to open new vulnerabilities that organizations will need to counter strategically.

Top threats in a world where AI has become a core business asset:

- **Prompt injection attacks:** Attackers manipulate AI models' behavior by inputting prompts specifically designed to steer the AI to take unsafe actions, reveal sensitive data, or generate undesirable outputs. Even large-scale, state-of-the-art models like Google's Gemini have been corrupted in these types of attacks.
- **Training data poisoning:** Attackers undermine model integrity by introducing malicious data into training datasets. This can cause models to produce faulty or biased predictions.
- **Model extraction:** Attackers reverse-engineer AI models to steal intellectual property or replicate the models themselves, leading to the loss of proprietary algorithms or other trade secrets.
- **Over-permissioned AI agents:** When AI systems are given more access than they need—to data, systems, or services—and trust boundaries aren't explicitly defined and enforced in the environment, attackers may be able to exploit that access to move laterally, leading to a large-scale breach.

Over 75% of CISOs report concerns about emerging AI security risks, but few feel they have the right tools or frameworks to tackle the problem at scale.

CISO Viewpoint

"When it comes to AI-powered threats, what we're seeing now is just the tip of the iceberg. Some of the attack types—like impersonation and business email compromise—have been around a long time, but some types of social engineering, where threat actors are learning about and mimicking the behavior of our employees in order to infiltrate the environment, are unlike anything we've ever encounterd before."

CISO, Healthcare

Cloud security is already being reshaped by AI, but the transformation is just beginning. Survey participants overwhelmingly agree that AI's impact on their cloud defenses will be sweeping. They're split on whether this impact is already here (45% agree that it is) or whether it's yet to come (55%).

54%

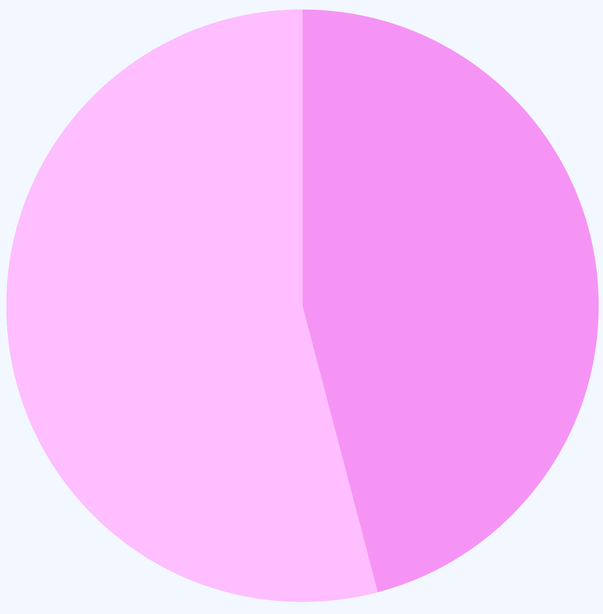
Security executives are more likely to believe that AI's impact on cloud security is already significant (54%), while a very large majority of architects and engineers (90%) believe that the disruption remains in the future.

Organizations with smaller security budgets are also less likely to be seeing an impact from AI thus far (38% say that it's already here, whereas for 60%, the impact is still in the future).

Big tech sees an impact now. 64% of respondents from technology companies say that AI is having a major impact on cloud security. Healthcare and professional services, in contrast, see it coming later. Just 29% of respondents in healthcare believe that AI's impact is already here, while 71% think it's yet to come. These numbers are similar for professional services (29% vs. 71%).

Which best describes the impact of including AI technology within cloud security solutions on your organization's cloud security capabilities/defenses?

Impact of AI on Cloud Security Solutions



45%	AI is already having a significant impact
55%	AI is expected to eventually have a significant impact
0%	AI is not ever expected to have a significant impact

Why This Matters: There's clear consensus that AI's impact on cloud security is—or will be—transformative. It's also apparent that not all organizations have yet positioned themselves to take full advantage of that transformative force. Early adopters stand to gain an edge, increasing efficiencies and accelerating security operations.

Call to Action: Turning to AI to power risk prioritization, threat detection, and response is a must-do for organizations that want to stay ahead of today's fast-evolving threats. Most organizations have already woven AI into their fabric, and "fighting fire with fire" is critical for securing AI implementations as well as boosting your overall security posture.

8 Where CISOs Are Placing their Bets for Next Year: Automation and Visibility

Nearly all respondents are looking to advance their cloud security posture within the coming year. 98% indicated that improving cloud security is among their organizations' top priorities.

What are the prevailing strategies for driving these improvements? 62% of respondents mentioned increasing automation. 48% indicated that improving visibility was of prime importance. And 42% mentioned increasing training, perhaps to help large cloud security teams make better use of ever-expanding toolsets. When every cloud service provider has its own security and management tooling, it's near-impossible to be an expert in all of them. At the very least, the learning curve is steep.

Dissatisfaction with the status quo abounds. Respondents are more interested in replacing their current cloud security solutions than supplementing them.

- 31% prioritize replacement
- Only 26% prioritize adding on to the current cloud security toolstack

Architects and engineers are especially likely to favor replacing current cloud security solutions over supplementing them:

- 45% of these respondents prioritize replacement
- Only 25% prioritize adding on to the toolstack

Architects and engineers highly prioritize investing in automation (mentioned by 70%).

Some respondents are looking for help from third-party partners. 33% plan to increase their reliance on managed services for cloud security support within the next 12 months.

Respondents in very large enterprises are especially interested in increasing automation, replacing their current tools and increasing visibility:

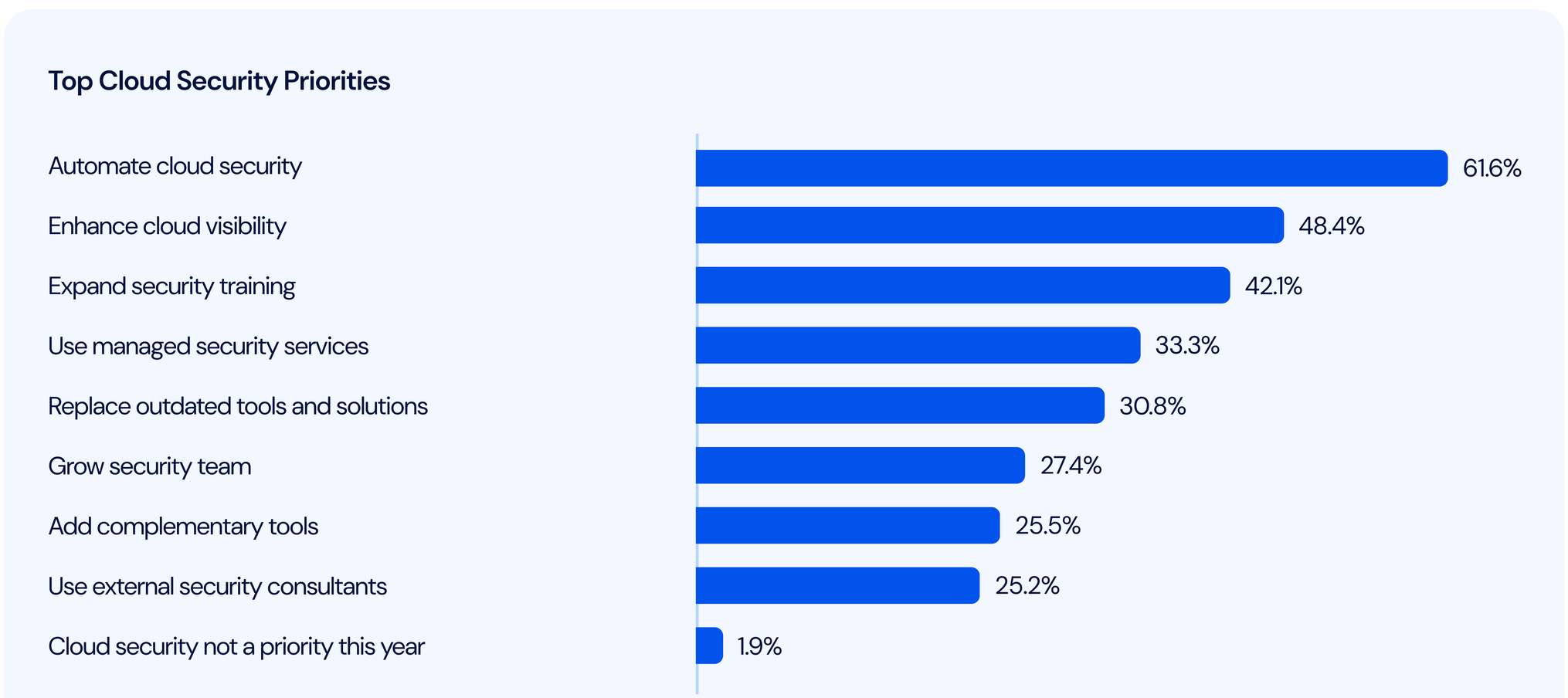
- 76% of respondents from organizations with 25,000+ employees prioritize increasing automation
- 41% prioritize replacing their current tools
- 41% prioritize increasing visibility
- Only 24% prioritize increasing training
- Only 24% prioritize increased reliance on managed services

Financial services firms and manufacturers are also interested in automation:

- 74% of financial services organizations prioritize increasing automation
- 64% of manufacturers do, too.

Meanwhile, professional services companies are particularly likely to invest in training (mentioned by 53%).

What are your organization's top priorities over the next 12 months for improving its cloud security capabilities/defenses? Select three.



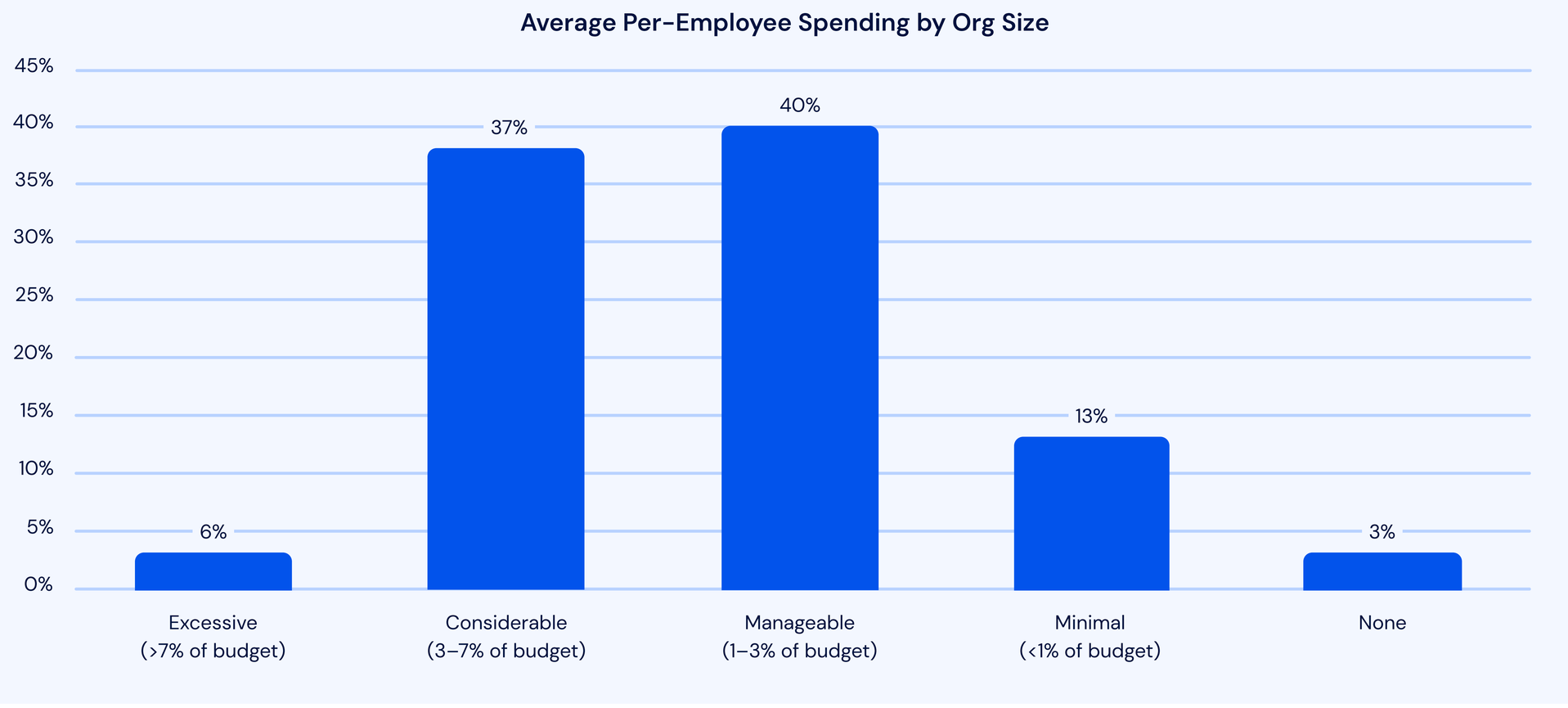
Innovation and transformation are driving spending far more than compliance is. Nearly half of respondents (44%) said that compliance is leading to considerable spending without significantly improving the organization's security posture. Just three percent of respondents feel that all of their spending on compliance has real risk-reduction value.

The problem is at its worst for mid-sized organizations (those with between 5,000 and 10,000 employees). 62% of survey participants in this group feel that their organizations are spending on compliance without seeing ROI. This is also a major issue in manufacturing (59% spending without getting value in return) and healthcare (55%).

The lack of real-world risk reduction (and ROI) may be because stakeholders are buying tools for specific use cases (or spending on audit preparation) rather than investing in platforms that can meet compliance requirements while also mitigating actual risks.

> **CISO Viewpoint**
>
> "Gaining certifications such as SOC 2 Type 2 is among my top priorities for the future. In the financial services industry, there are many prospective clients who won't even talk to you if you don't have SOC 2, and that represents tens if not hundreds of millions of dollars in revenues. For us, demonstrating compliance can open up vast new markets."
>
> **CISO, Financial Services Firm**

To what extent are security and data privacy regulations that are applicable to your organization leading to security spending that does not significantly improve the organization's overall security posture?



> **CISO Viewpoint**
>
> "When we look at compliance requirements, we find that what they dictate—in terms of controls—is less mature than the framework we follow as an organization [NIST CSF]. The framework has a lot more detail and is more prescriptive. As long as we follow that, the compliance requirements just get folded in automatically."
>
> **CISO, Healthcare**

Why This Matters: There's clear consensus that AI's impact on cloud security is—or will be—transformative. It's also apparent that not all organizations have yet positioned themselves to take full advantage of that transformative potential.

Call to Action: Growing cloud and AI adoption are creating a whole new world of security challenges. The environment is more complex and dynamic than ever before, while attack sophistication is climbing through the stratosphere. It's time to eliminate silos, visibility gaps, and unwieldy tools that undermine performance.

Introducing Wiz

Wiz is a cloud security platform built for the way modern teams build in the cloud. It connects directly to every environment, scans every layer, and gives security and development teams a clear view of risk all in a single platform.

Organizations choose Wiz because it lets them:

- **See everything, instantly.** Wiz connects via APIs to deliver fast, frictionless visibility across AWS, Azure, GCP, and more. It covers every resource, from VMs to containers and serverless, without performance overhead or gaps.
- **Prioritize what matters.** Wiz's Security Graph correlates vulnerabilities, identities, permissions, data, and network exposure to reveal toxic combinations that represent real attack paths. Teams get clear, contextual insights so they can fix what matters most.
- **Secure everything in one place.** From misconfigurations and secrets to over-permissioned identities and vulnerable pipelines, Wiz replaces fragmented tooling with one platform that surfaces all your cloud risks in one view.
- **Bring teams together.** Wiz gives cloud, security, and development teams shared context to shift security left in pipelines and act fast in production. Less friction, faster remediation.
- **Detect threats at cloud speed.** Wiz continuously monitors cloud environments for active threats and attack paths. It scales effortlessly to match the speed of the business, helping teams stay one step ahead.

AI adoption is accelerating in the cloud, and with it comes a new layer of risk. That includes misconfigurations, unsecured pipelines, and shadow AI use. Wiz gives teams visibility into the entire AI stack, from model exposure to data access. Our researchers uncover critical risks across the ecosystem and feed that insight back into the platform. It's how we help organizations move fast without creating blind spots.

See Wiz in action
Explore how Wiz helps your team surface real risk, cut through the noise, and secure every layer of your cloud.

Request a demos | Watch a 12-minute demo video