Shifting Ground

Federal Cyber Priorities Reshape Security Strategy

Table of Contents

Executive Summary

Recent shifts in U.S. federal cybersecurity programs, most notably reductions to CISA initiatives and the disbandment of the Cyber Safety Review Board, are sending ripple effects across the private sector. Security leaders who once relied on public-sector intelligence, coordination and funding are now contending with increased risk exposure, reduced visibility and growing operational strain.

To better understand how cybersecurity teams are adapting to this shift, Swimlane surveyed 500 IT and security decision-makers across the U.S. and U.K. The findings reveal rising pressure on private organizations to safeguard critical operations in the absence of federal support, with important implications for resilience, investment and public-private coordination. The research also highlights emerging global concerns, as international organizations reassess long-term cybersecurity strategy amid policy and funding uncertainty.

Key Findings

Federal Cuts are Rewriting Security Investment Plans

63%

63% of respondents say recent or anticipated CISA budget cuts are affecting their team structure and staffing plans.

46%

46% report that uncertainty around federal cybersecurity funding has reduced their planned investments for 2025.

57%

57% say shifting public-sector support has delayed key investments in 2025.

Security Teams are Bearing the Brunt of Cost Pressures

85%

85% of organizations have experienced budget, or resource-related changes, in the past six months.

41%

41% of organizations say threat detection and monitoring is among the most affected functions.

52%

52% report increased workloads without additional support.

48%

48% say their teams have undergone role changes or restructuring.

Organizations are Building Their Own Resilience

91%

91% of organizations have taken new steps to maintain operational resilience amid reduced federal support.

54%

54% have developed internal frameworks independent of government guidance.

51%

51% are relying more on commercial threat intelligence providers.

Confidence in Public-Private Coordination is Eroding

81%

81% of organizations believe CISA budget cuts will hinder proactive threat intelligence sharing with the private sector.

86%

86% say disbanding the Cyber Safety Review Board will reduce coordination after major incidents.

79%

79% agree that federal defunding has increased their organization's overall cyber risk exposure.

U.S. Cyber Instability Shifts U.K. Security Spending

79%

79% of U.K. respondents say U.S. cybersecurity instability has made them more cautious about U.S. vendor relationships.

53%

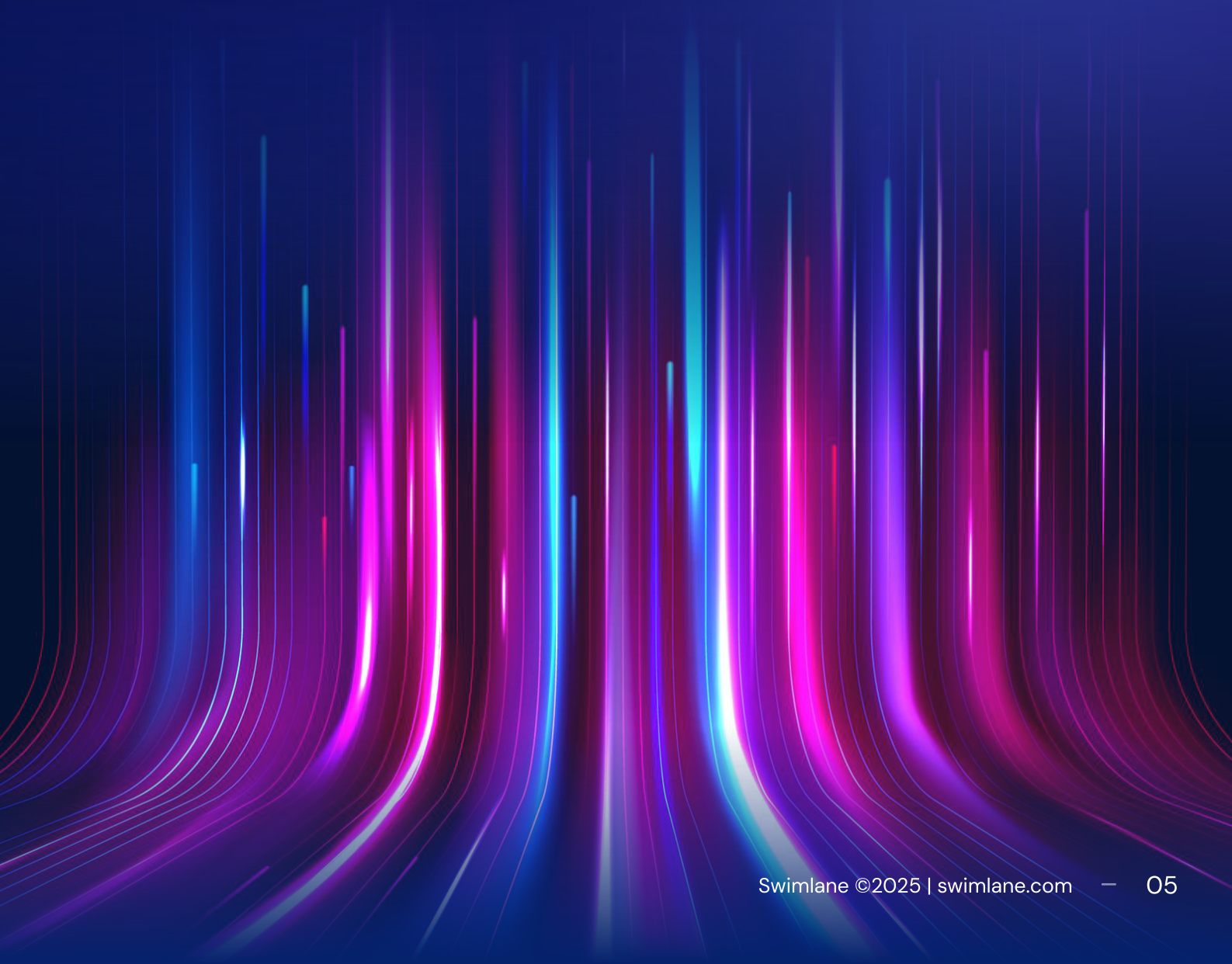
53% have increased reliance on domestic or EU-based security providers as a result.

43%

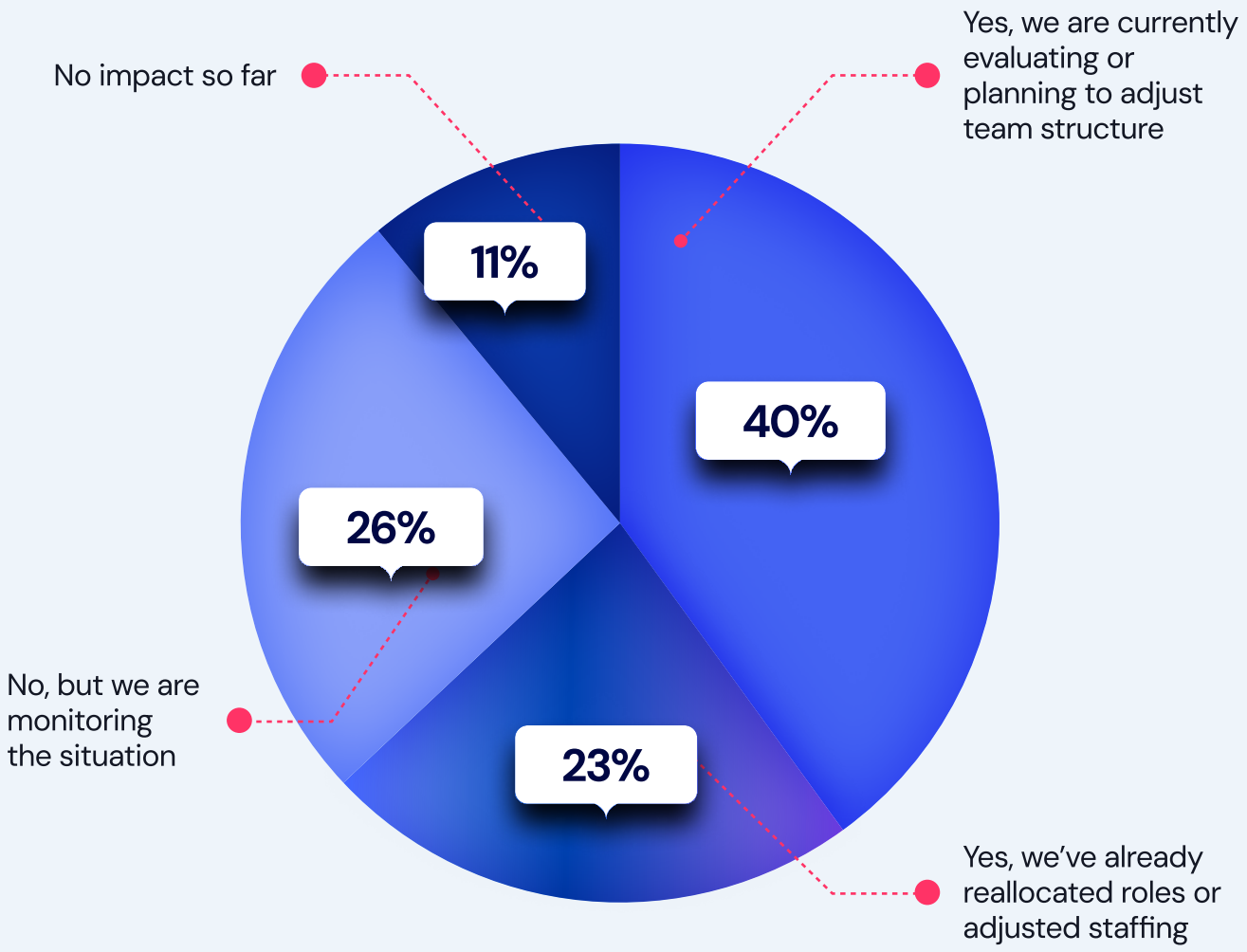
43% have reassessed existing partnerships, and 29% have delayed or canceled contracts with U.S.-based vendors.

Federal Cuts are Rewriting Security Investment Plans

Security teams are being forced to reevaluate staffing and structure as federal support diminishes. Sixty-three percent of respondents say recent or anticipated CISA budget cuts are directly influencing their team planning, a signal that even internal operations are being reshaped by external policy shifts.

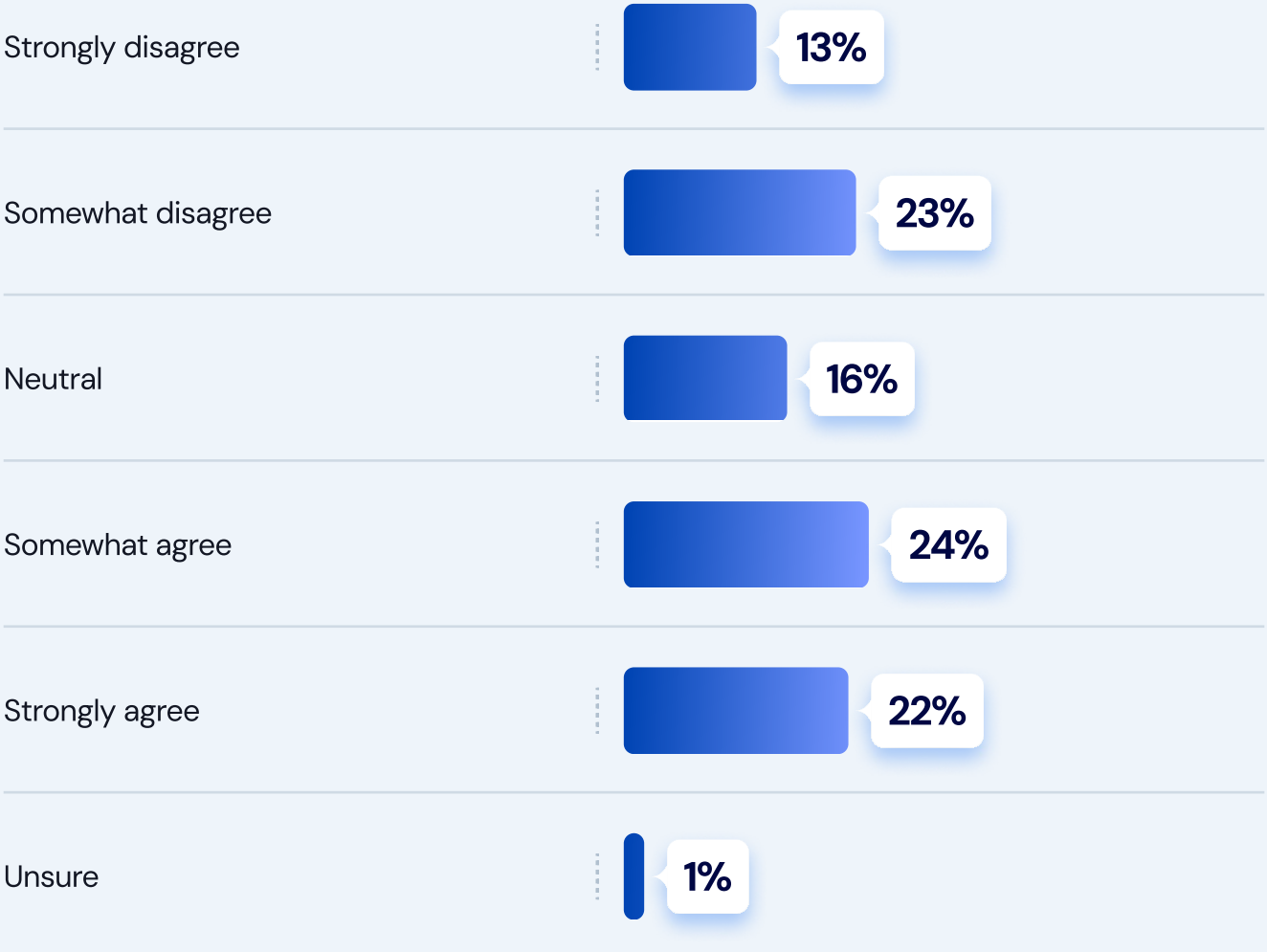


Have the recent or anticipated CISA budget cuts influenced your organization's internal cybersecurity staffing or team planning?



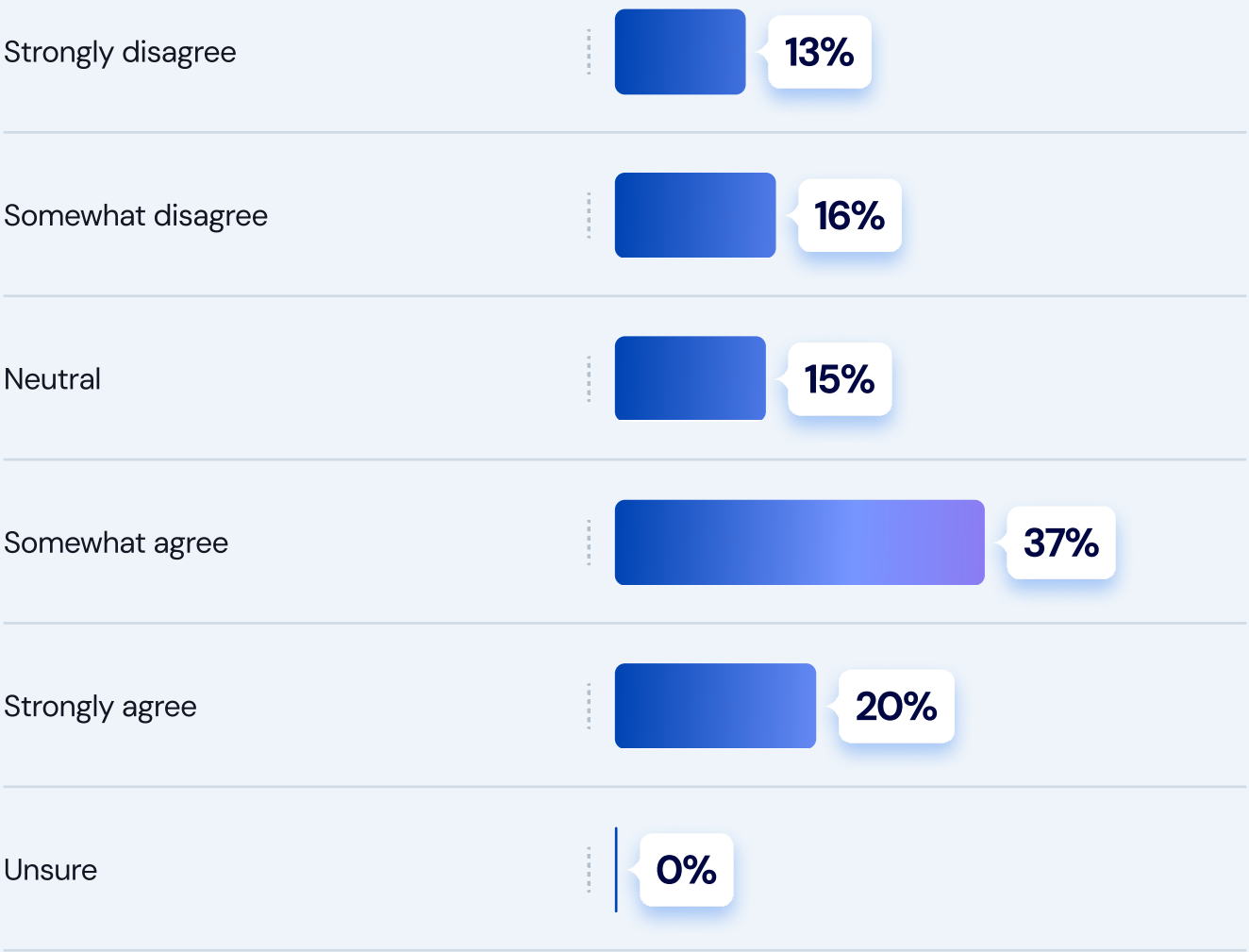
Uncertainty is also slowing investment. Nearly half of respondents (46%) say questions around future federal cybersecurity funding have caused their organization to scale back planned investments for 2025, putting long-term strategy and innovation at risk.

To what extent do you agree with the following statement: Uncertainty around US federal cybersecurity funding or support has reduced your organization's planned cybersecurity investments in 2025



The ripple effect is already visible in project timelines. Over half of respondents (57%) say that uncertainty around federal cybersecurity funding is delaying planned investments. While delays may be less severe than outright reductions, they still create strategic uncertainty, especially as security teams face mounting pressure to stay ahead.

To what extent do you agree with the following statement: Uncertainty around US federal cybersecurity funding or support has delayed your organization's planned cybersecurity investments in 2025



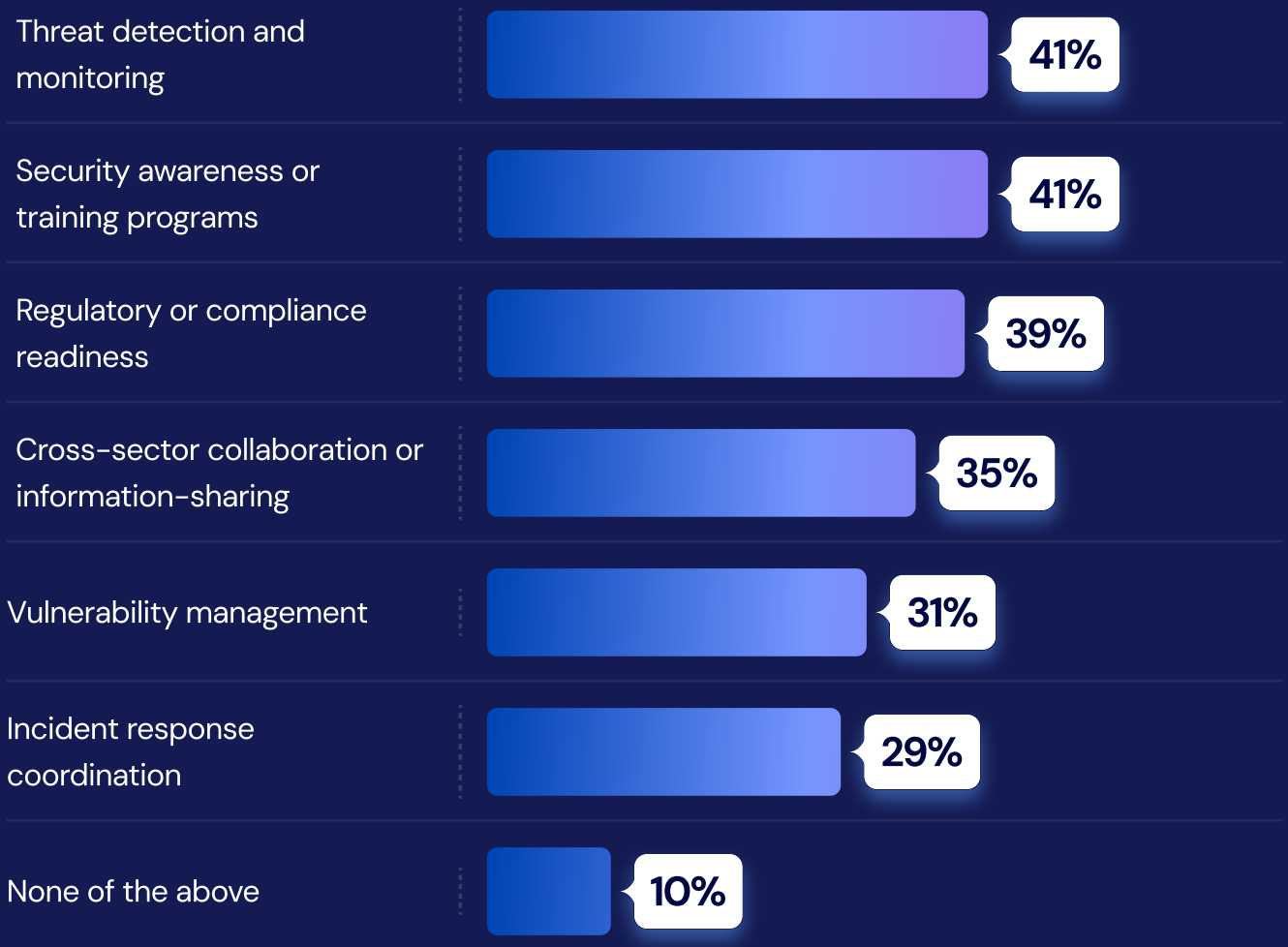
Security Teams are Bearing the Brunt of Cost Pressures

Operational resilience is starting to crack under resource pressure. Eighty-five percent of organizations say they've experienced budget, or resource-related changes, in the past six months, and the fallout shows up across critical security functions.

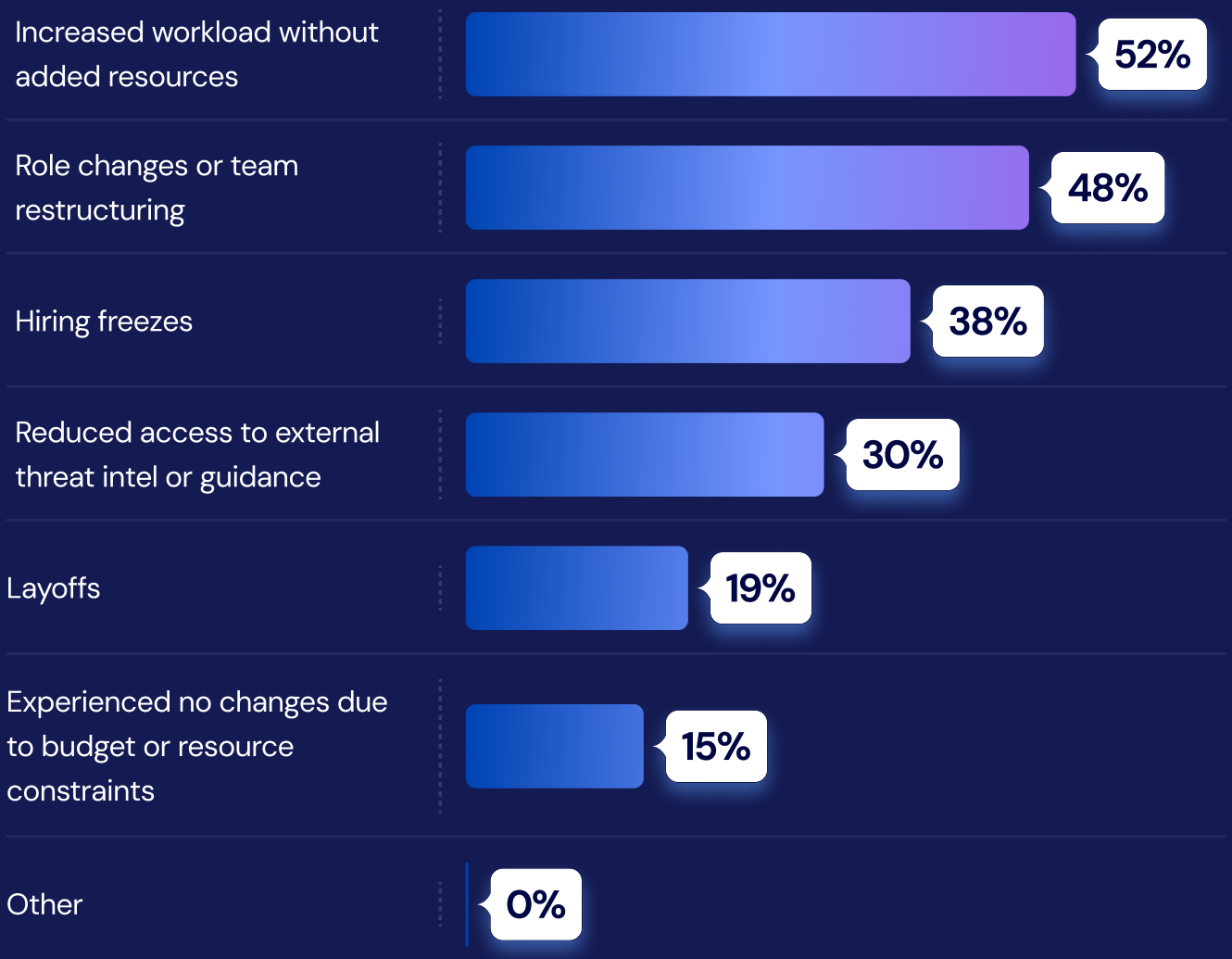
Threat detection and monitoring top the list of affected areas, cited by 41% of respondents. The same percentage says security awareness and training programs have suffered, suggesting that organizations are less equipped to prevent and identify threats in real-time. Thirty-nine percent also report diminished regulatory or compliance readiness, raising concerns about preparedness in an increasingly complicated risk landscape.

Behind these disruptions are strained teams. Over half (52%) of respondents report increased workloads without added resources, while 48% say their teams have been restructured or reassigned. As staff are stretched thinner, the ability to execute on core security functions is increasingly at risk.

What operational activities have been most affected by limited public-sector cybersecurity support or shifting budgets? Select up to three.

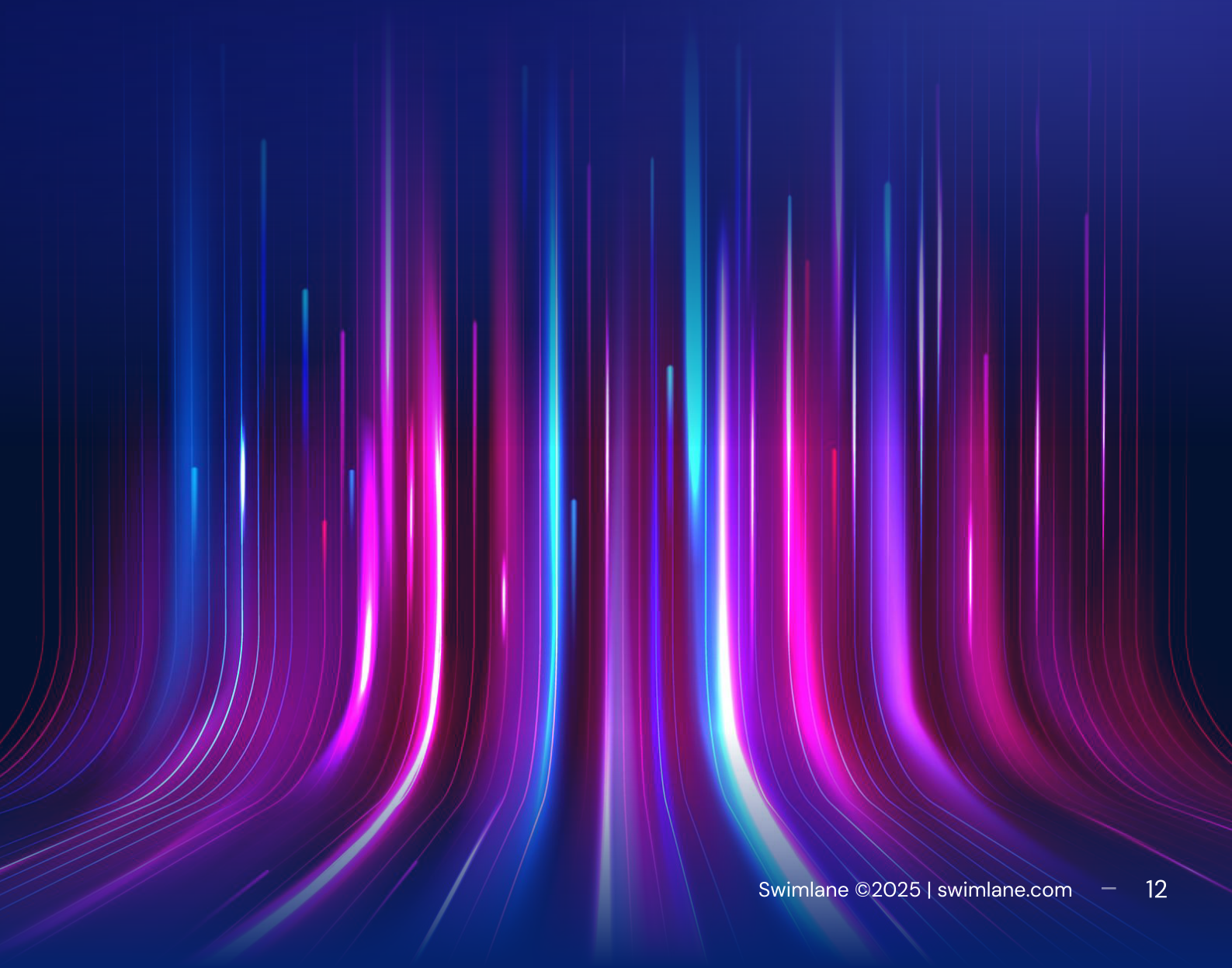


Have you or members of your cybersecurity team experienced any of the following in the past six months due to budget or resource constraints? Select all that apply.

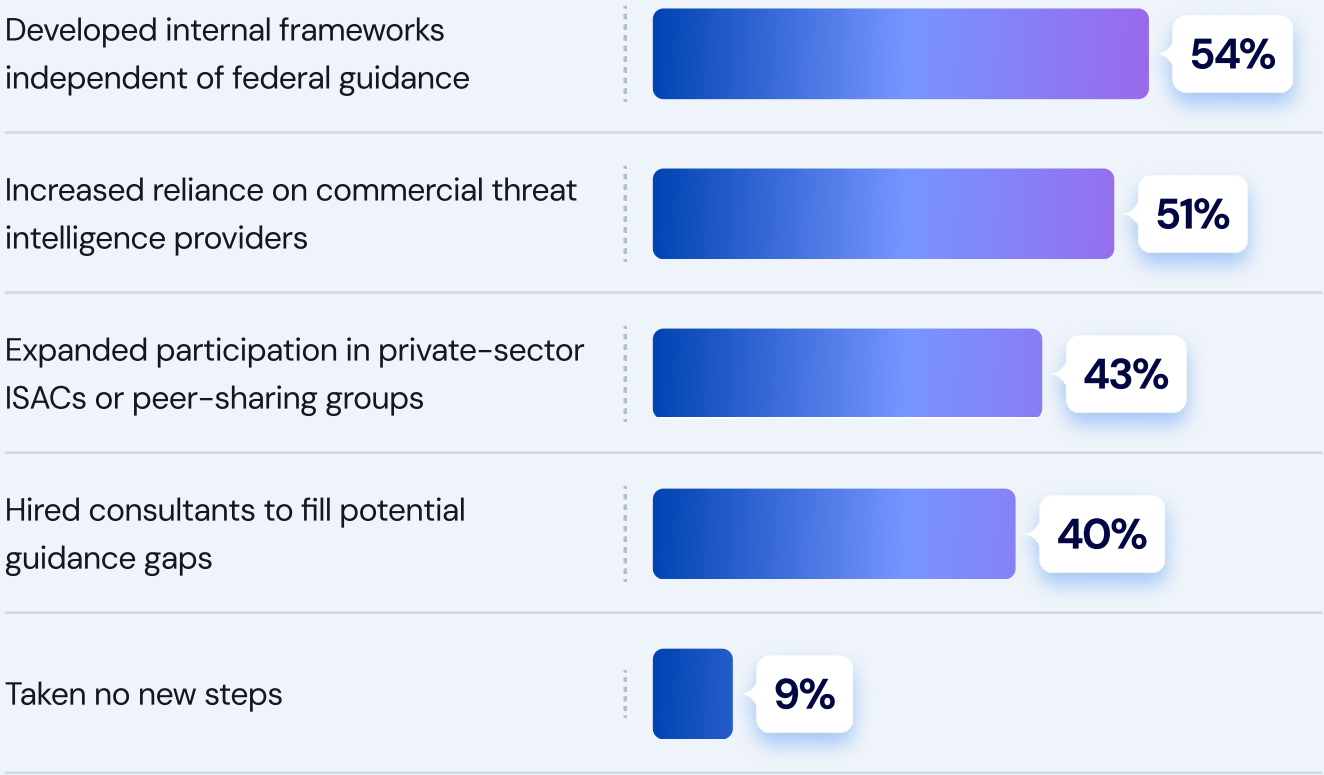


Organizations are Building Their Own Resilience

In the face of shrinking federal support, most organizations aren't standing still. They're adapting. Ninety-one percent of respondents say they've taken new steps to maintain operational resilience, with more than half (54%) developing internal frameworks independent of government guidance.



What steps, if any, has your organization taken to maintain operational resilience amid reduced federal cybersecurity support? Select all that apply.



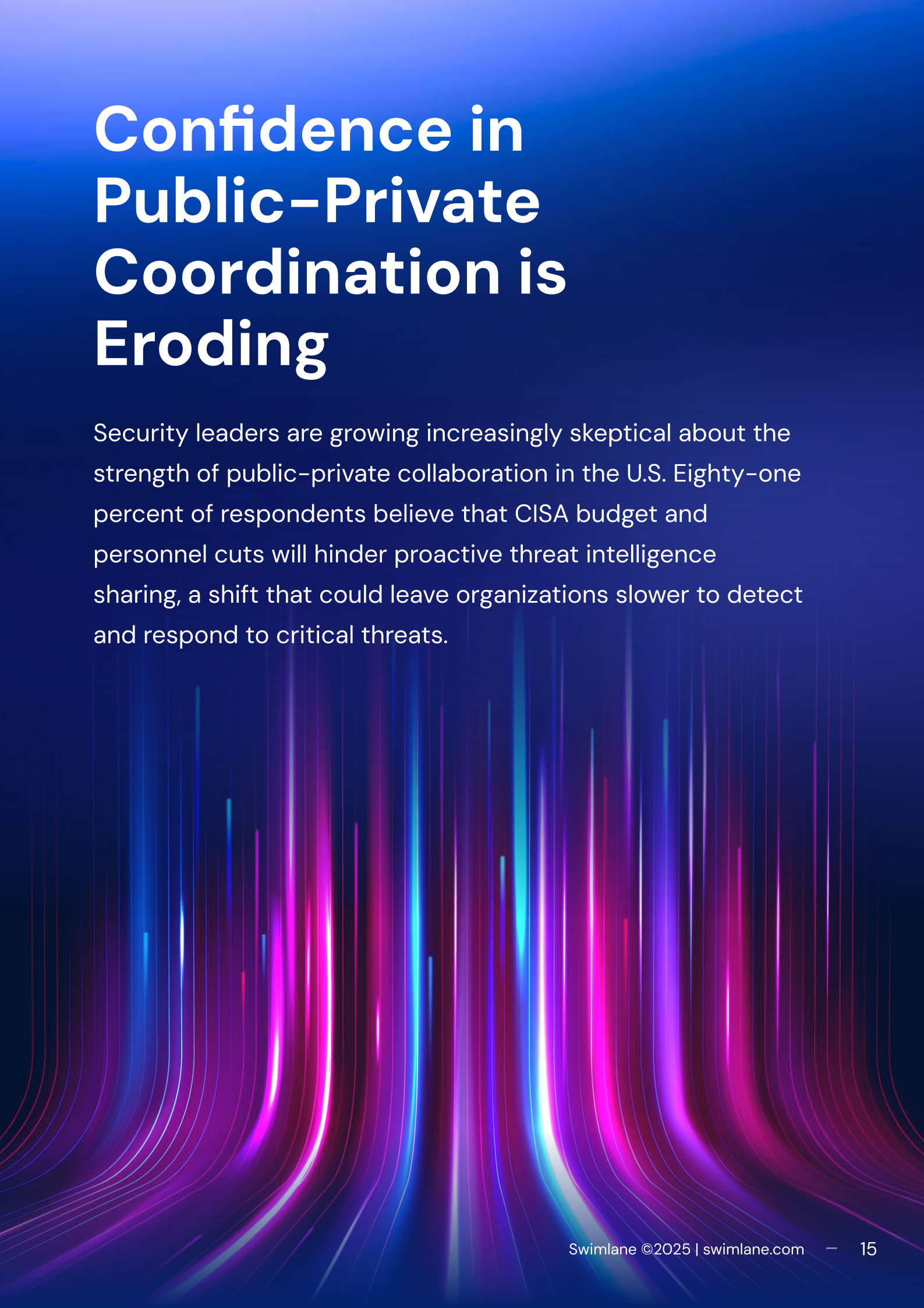
Many are turning to the private sector to fill the gaps. Fifty-one percent say they're relying more on commercial threat intelligence providers, while others are expanding their participation in peer-sharing groups or bringing in consultants to access expertise that was once provided through public-sector programs.

"Looking ahead, organizations are prioritizing tools and capabilities that can help offset staffing and coordination gaps." The top areas of interest include improved coordination across security tools and teams (44%), more actionable threat intelligence (41%) and automation of high-volume tasks (39%), all aimed at maintaining agility and coverage without increasing headcount.

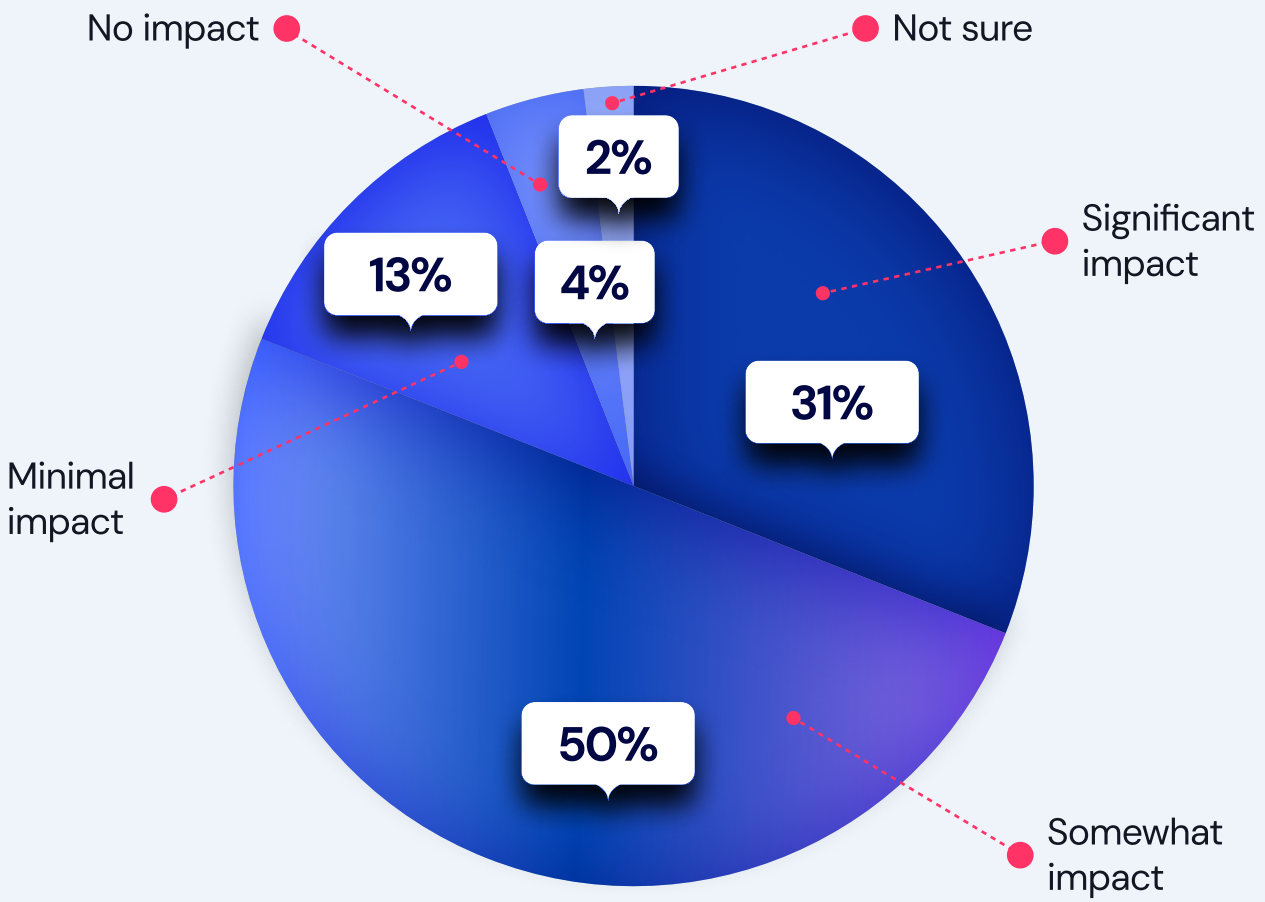
Considering reduced resources and shifting public-sector support, which capabilities is your organization most interested in adopting or expanding to help offset staffing or operational gaps? Select up to three.

Confidence in Public-Private Coordination is Eroding

Security leaders are growing increasingly skeptical about the strength of public-private collaboration in the U.S. Eighty-one percent of respondents believe that CISA budget and personnel cuts will hinder proactive threat intelligence sharing, a shift that could leave organizations slower to detect and respond to critical threats.

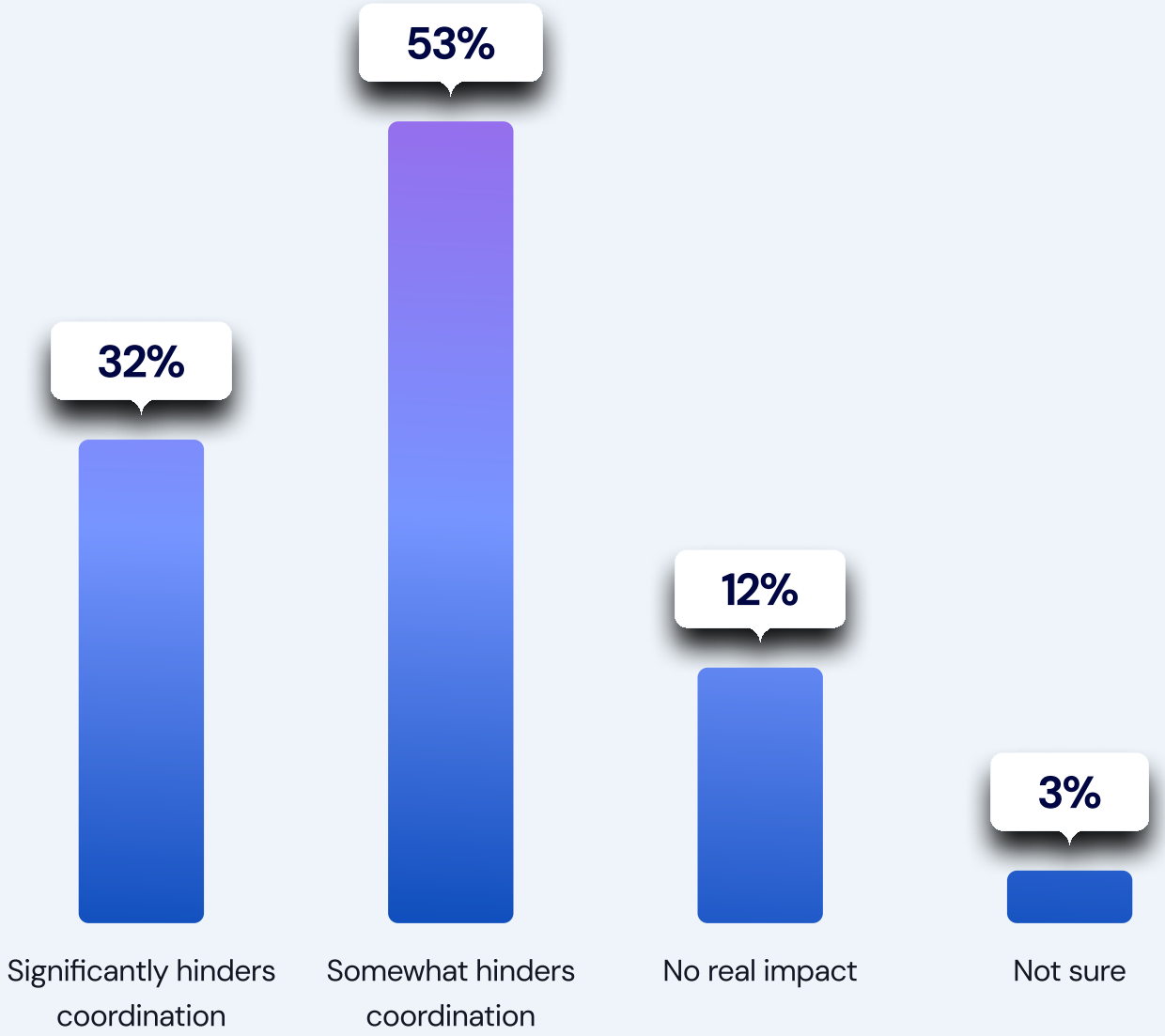


How do you believe CISA budget and personnel cuts will impact the sharing of proactive threat intelligence between the U.S. government and the private sector? (Select one)



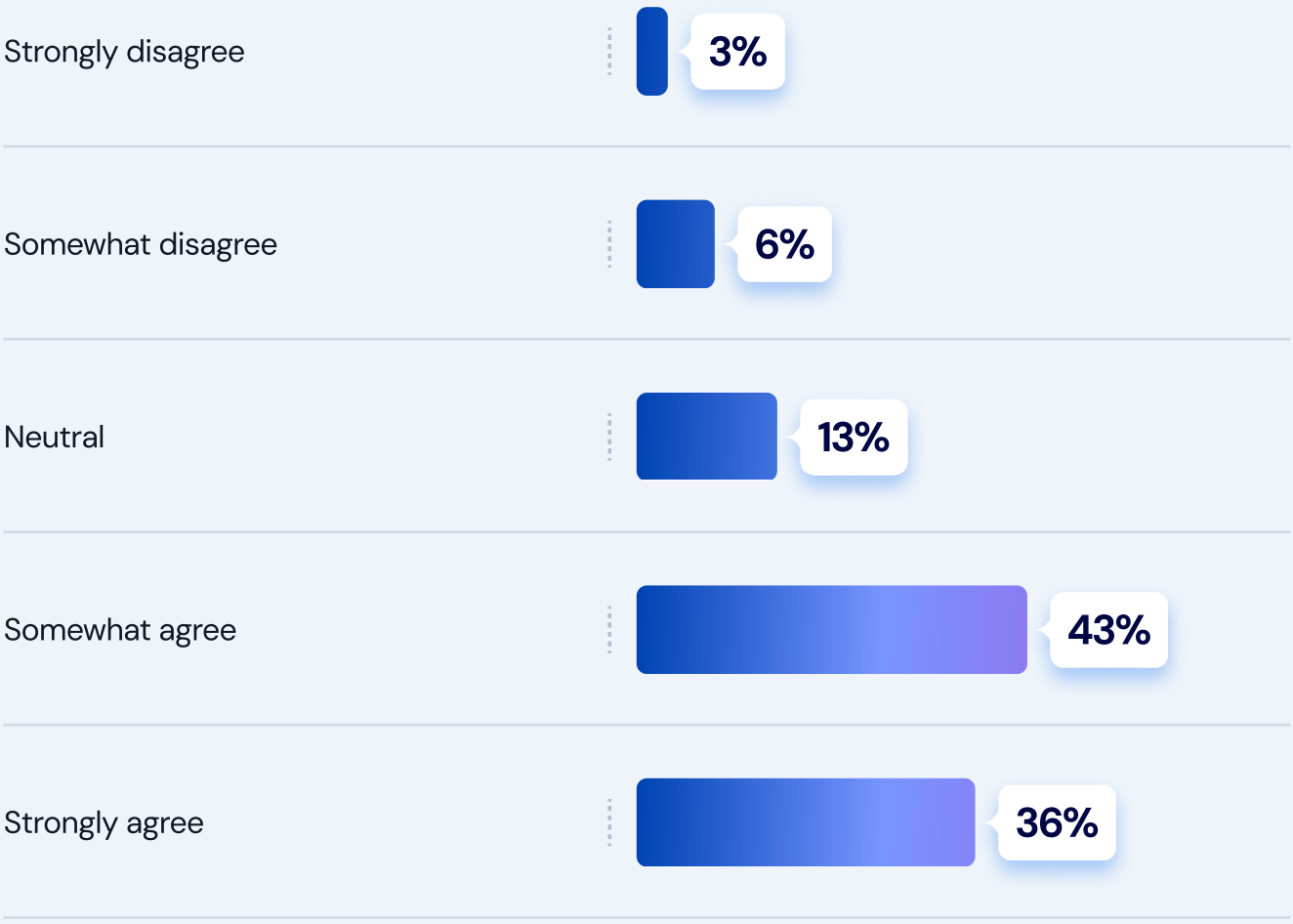
Concerns extend beyond day-to-day operations. Eighty-six percent say the disbandment of the Cyber Safety Review Board will reduce coordination after major cybersecurity incidents, raising questions about who will lead response efforts during national-scale attacks.

What impact do you believe the disbandment of the Cyber Safety Review Board will have on public-private coordination after major cybersecurity incidents? (Select one)



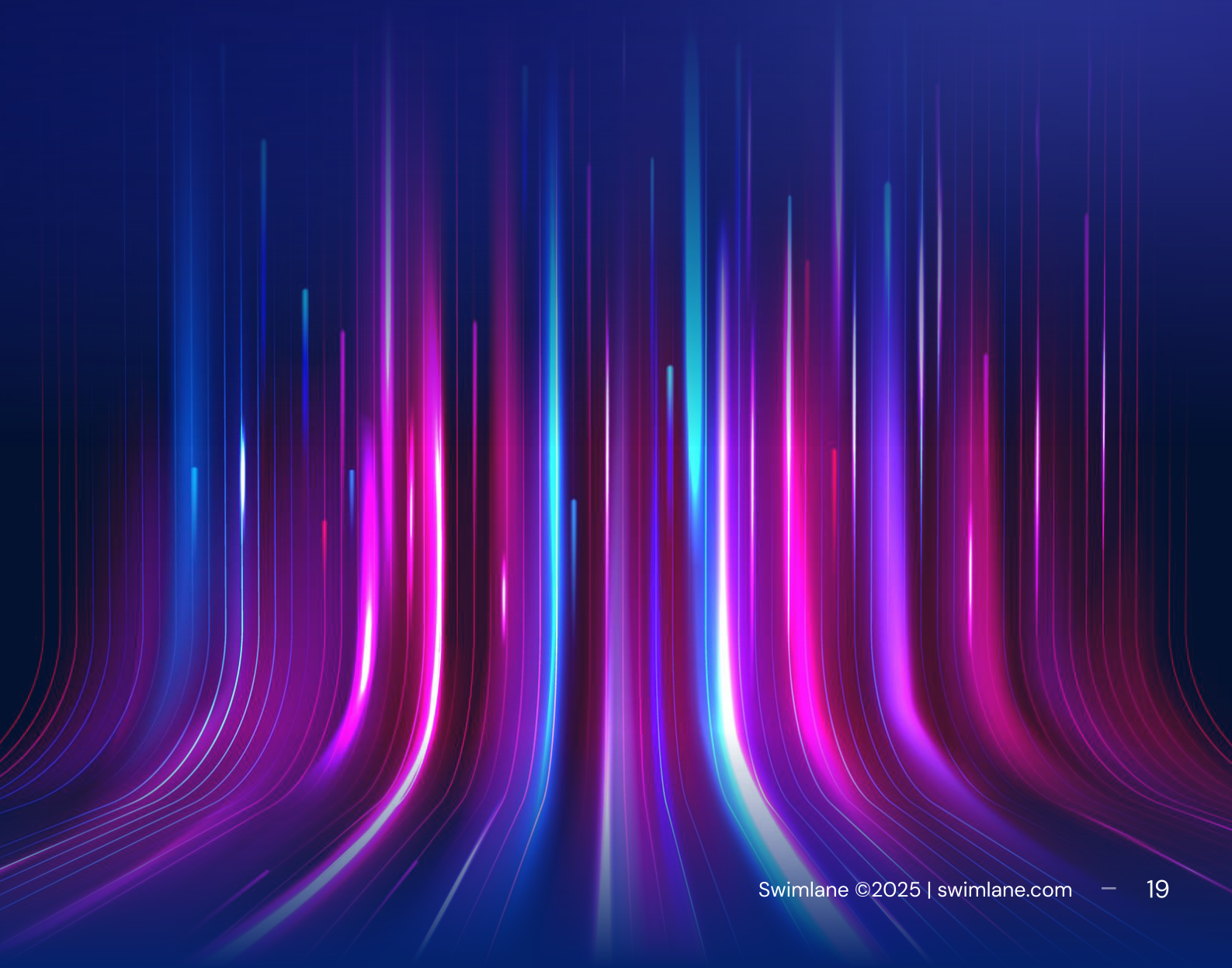
Most concerning, 79% of respondents agree that federal defunding has directly increased their organization's cyber risk exposure, highlighting the broader consequences of reducing public-sector support in an era of rising threats.

To what extent do you agree with the following statement? Reduced funding for U.S. cybersecurity programs has increased the overall cyber risk exposure for private sector organizations like mine.



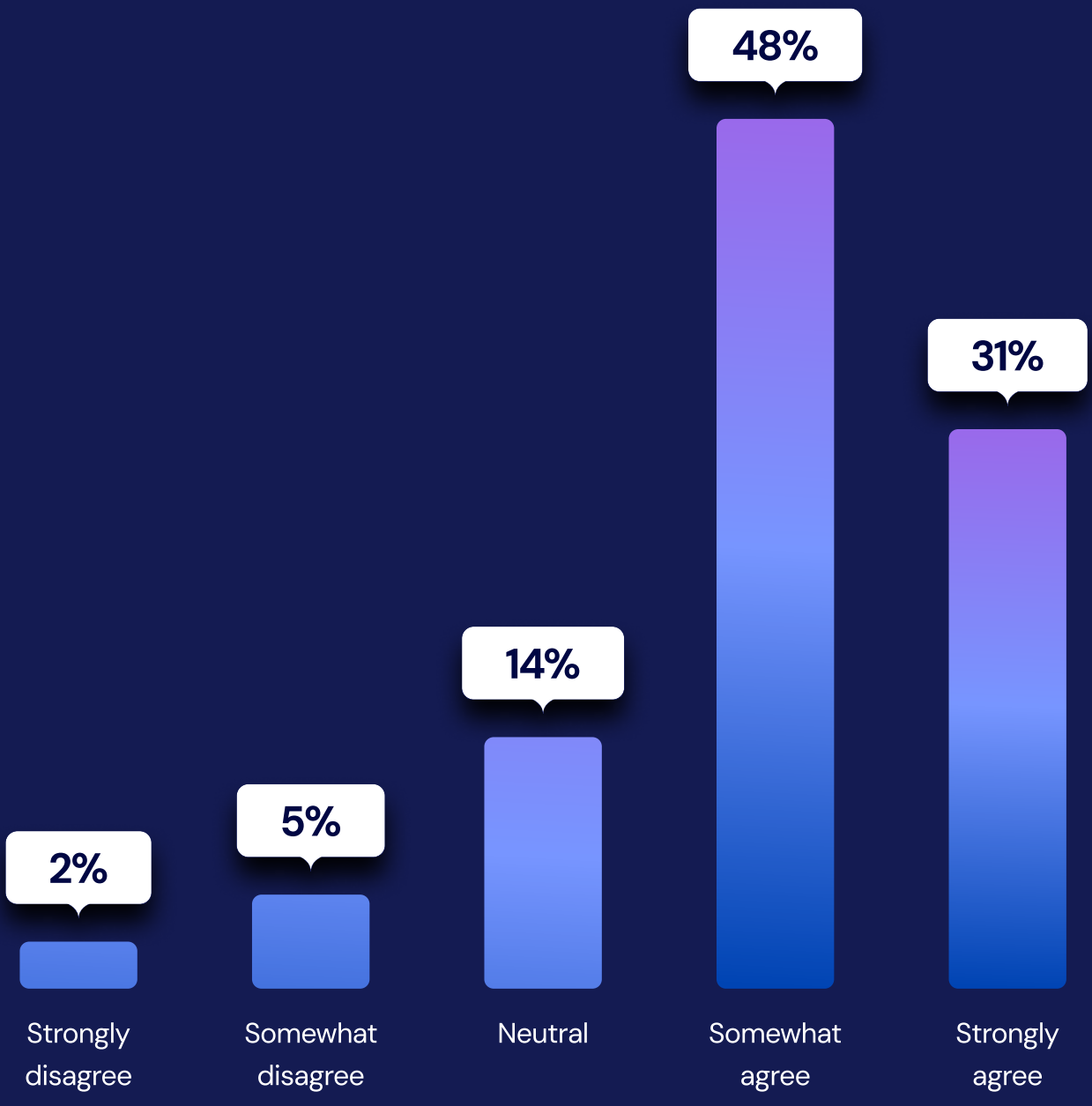
U.S. Cyber Instability Shifts U.K. Security Spending

The effects of U.S. federal defunding aren't just domestic. They're reshaping how global partners view cybersecurity risk. Among UK respondents, 79% say recent U.S. cyber policy shifts have made them more cautious about forming or maintaining partnerships with U.S.-based cybersecurity vendors.



FOR UK-BASED RESPONDENTS ONLY

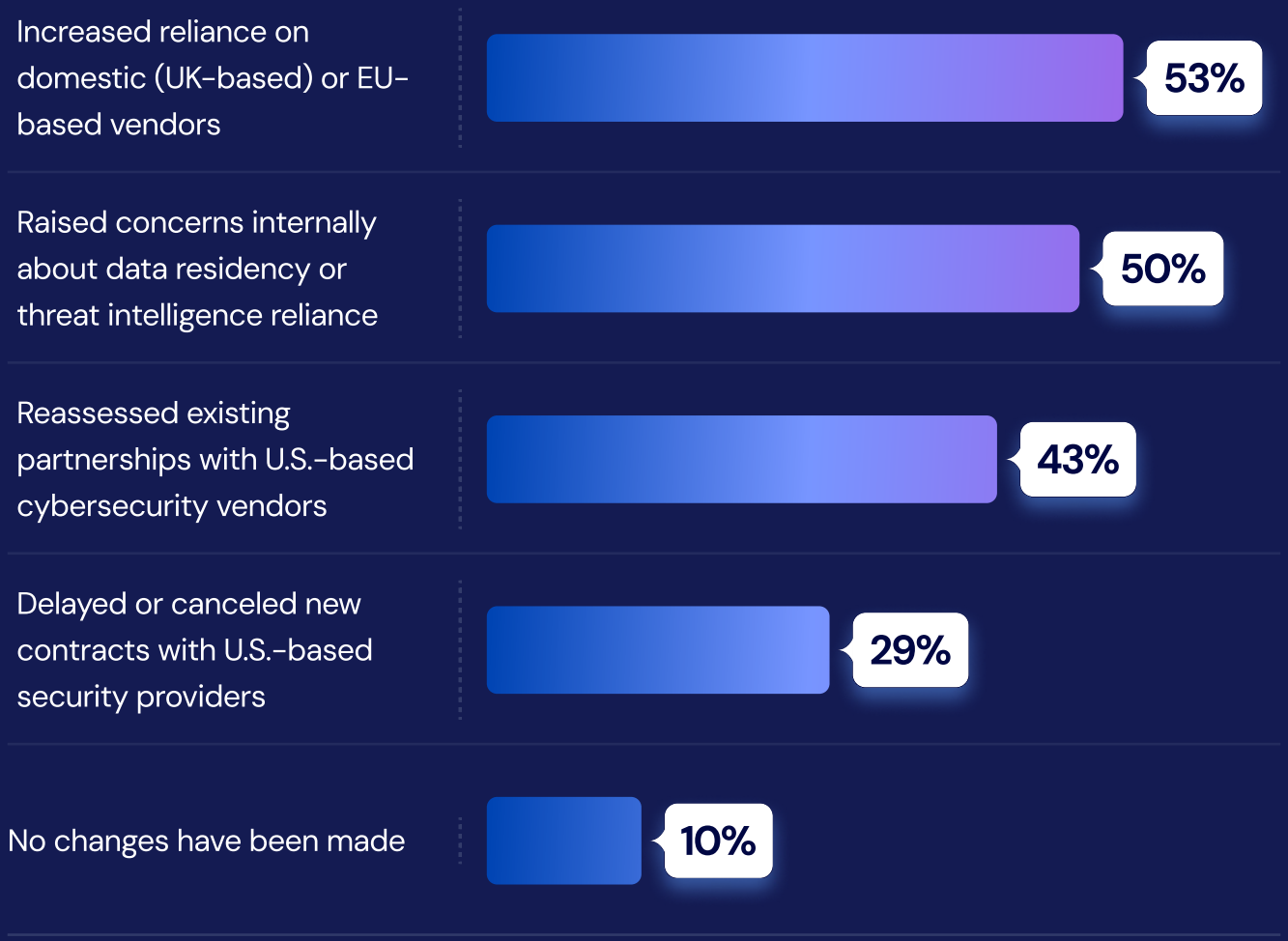
To what extent do you agree with the following statement? Recent reports of U.S. cybersecurity defunding (e.g., CISA cuts) have made my organization more cautious about maintaining or forming cybersecurity partnerships with U.S.-based companies.



More than half (53%) say they've increased reliance on domestic or EU-based vendors as a result, and 43% have reassessed existing U.S. relationships. Nearly a third (29%) have taken further action, delaying or canceling new contracts with U.S.-based security providers. These shifts reflect not just short-term caution but a long-term recalibration of trust and vendor strategy on the global stage.

FOR UK-BASED RESPONDENTS ONLY

Has your organization taken any of the following actions in response to perceived cybersecurity instability in the U.S.? Select all that apply.



A Turning Point for Cyber Resilience

As federal cybersecurity support shifts, the pressure on private-sector security teams is mounting. Budget constraints, staffing challenges and reduced access to public-sector resources are leaving organizations to navigate rising risk with fewer tools and less certainty.

This research underscores a critical inflection point: operational resilience can no longer rely on manual effort, fragmented intelligence or overstretched teams. With 85% of organizations experiencing budget or resource changes, the path forward will depend on doing more with less and doing it smarter. Security teams need solutions that reduce complexity, close coordination gaps and automate what can no longer be sustained manually. In an era of shrinking support and escalating threats, resilience won't come from working harder. It will come from working differently.

Methodology

The survey was conducted among 500 IT and cybersecurity decision-makers at enterprise companies with at least 1,000 employees in the United States and the United Kingdom. The interviews were conducted online by Sapio Research and under the guidance of Swimlane, between June and July 2025, using an email invitation and an online survey.

About Swimlane

At Swimlane, we believe the convergence of agentic AI and automation can solve the most challenging security, compliance and IT/OT operations problems. With Swimlane, enterprises and MSSPs benefit from the world's first and only hyperautomation platform for every security function. Only Swimlane gives you the scale and flexibility to build your own hyperautomation applications to unify security teams, tools and telemetry ensuring today's SecOps are always a step ahead of tomorrow's threats.

Learn more: swimlane.com

About Sapio Research

Sapio's passion is giving clients confidence in their decisions, creativity, or storylines—helping them look good and be more productive. We do this by collecting and synthesising insight from qualitative, quantitative, or secondary research data sources. We focus on three key services: audience understanding, brand research, and thought leadership research.

Our high-quality tailored insights help improve lead generation and reputation, get you closer to your audience, and gain an edge against the competition. Through understanding, honest counsel, collaboration, and a swift approach we deliver projects you'll be proud of.

Best new agency finalist, Sapio is adept at opinion polling (we have access to 80 million people internationally), focus groups, face-to-face interviews, telephone interviews, online research, desk research and statistical modelling, to mention just a few techniques. We love B2B research and consultancy. Our business is based on partnership principles inspired by social enterprise.