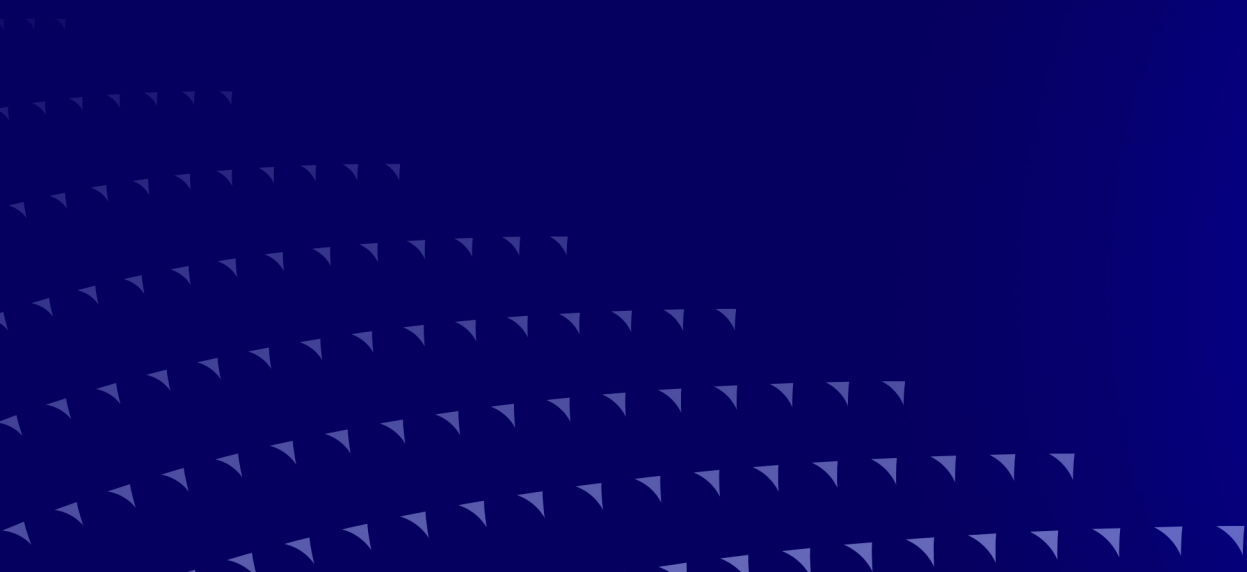


Security Budget

2025 Benchmark Summary Report



This summary report provides high-level insights from our 2025–2026 Security Budget Benchmark Report.

The complete 2025–2026 Security Budget Benchmark Report is a comprehensive, 30-page breakdown that offers a more detailed set of data and is available to IANS clients through the IANS Portal or to non-clients upon request by contacting us at info@iansresearch.com

Table of Contents

Executive Summary	4
What CISOs Will Find in This Report	5
Organizations Scale Back Security Budget Growth	6
Budget Ratios Break From a Multiyear Trend	7
How CISOs Allocate Their Budgets	9
Staffing Growth Slows Amid Budget Pinches	12
Recommendations	14
Methodology	15
About Us	17



Executive Summary

Global market volatility, fueled by ongoing geopolitical tensions, uncertainty around global tariff policies, and fluctuating inflation and interest rates, has made the business outlook for most companies unpredictable. In response, companies have become more cautious in their spending and hiring. More than in prior years, security organizations are affected as well, manifested by declining rates of growth for budgets and staff levels. Across diverse sectors and company sizes, this is causing resource constraints that are likely to set off a cascading series of events, ultimately elevating business risk and increasing the likelihood of compliance gaps.

To obtain a thorough assessment of the current state of security budgets and staffing, IANS and Artico Search conducted their sixth annual CISO Compensation and Budget Research Study from April to August 2025. To date, we have gathered data on security budget and staffing trends from 587 CISOs.¹

For additional insight, this report features expert perspectives from Artico Search executives, including Steve Martano, IANS Faculty and partner in Artico Search's cyber practice, and Matt Comyns, co-founder and president at Artico Search.

¹ Find details on the methodology and a breakdown of the sample in the methodology section of this report.

Security budget growth slows to 4% year-over-year

The headline observation from our data is that average annual security budget growth plunged to 4%—the lowest level in five years and a sharp drop from 8% in 2024. The share of CISOs reporting increasing budgets from the prior year has continued its downward trajectory. This year, there were more CISOs facing flat or reduced budgets than those who saw budget growth, underscoring a deepening challenge in securing adequate resources for cybersecurity.

Across industries, annual budget growth is lowest in healthcare, professional & business services, and retail & hospitality. Meanwhile, in financial services, insurance and tech, average annual budget growth remained above 5%. These disparities across sectors reflect the uneven impact of macroeconomic volatility, with certain sectors bearing the brunt of economic instability more than others.

CISOs prioritize cloud security and IAM for incremental budget allocations

Among CISOs with growing budgets, the top areas of priority for allocating additional spending are cloud security solutions and IAM enhancements, followed by SecOps automation and zero trust architecture. Notably, CISOs at smaller organizations with limited staff are more likely to prioritize cloud security solutions and endpoint detection, while their counterparts at multibillion-dollar enterprises with complex, distributed environments prioritize IAM enhancements and zero trust initiatives over other areas of security.

Security budget growth lags behind IT spending growth

Between 2020 and 2024, security budget as a percentage of IT spending grew steadily from 8.6% to 11.9%. This year broke that trend with a drop of one percentage point to 10.9%, indicating IT spending levels exceeded security budget growth for the first time in five years. This reversal is likely the result of a rebound in core IT spending, driven by AI and increased cloud infrastructure investments.

Security budget as a percentage of revenue remained flat, indicating that, on aggregate, company revenue grew at roughly the same pace as security budgets.

Staffing growth declines for fourth consecutive year

Tighter budgets have had a cascading effect on staff growth, which declined to its lowest level in four years, an average of 7%. The majority of CISOs saw either flat or declining security team sizes, despite the threat environment becoming more complex. Exceptions are insurance, which is experiencing record profits, and financial services, where at least half of CISOs saw their teams grow.

Nearly all CISOs reported security teams are understaffed or low on staff, citing hiring and budget constraints as the primary cause. They also noted staffing shortages led to delays and cancellations of security initiatives, caused morale issues, increased the risk of noncompliance, and elevated organizational risk in general.

What CISOs Will Find in This Report

This year's Security Budget Benchmark Report equips CISOs with relevant data and insights for the upcoming budget cycle. In it, CISOs will find:



The latest annual budget and staff growth data

The report provides self-reported data from 587 CISOs on their security budgets and staff. This data allows CISOs to compare their situation with that of peers in their industry and at organizations of similar sizes. Additionally, they can use benchmark data and the challenges of resource constraints shared by peers to advocate for additional budget and staffing in the upcoming budget cycle.



Key budget metrics

The report offers benchmark data for a set of commonly used security metrics CISOs rely on to determine budget and security headcount, including security budget as percentage of IT spend and of revenue. These metrics are often referenced in discussions with the CFO, COO, CEO and the board of directors to contextualize the size and scope of the security program within broader organizational metrics.



Security budget allocations

The report offers a detailed breakdown of budgets across key spending areas, with deeper analysis of the largest budget categories—staff & compensation and software tools—including further segmentation by function and department. This data allows CISOs to benchmark their budget allocations against those of their peers and assess how, on aggregate, CISOs distribute resources across critical security functions.



Security spending priorities

The report outlines the spending areas CISOs prioritize when receiving new or incremental budget. CISOs who have secured net new budget can use this list to guide their own spending priorities. It can also serve as a tool to advocate for increased resources, highlighting the potential risk of falling behind peers in key areas without adequate funding.



Objective vendor-neutral research

Currently in its sixth year, our process of participant recruitment, data collection, vetting and analysis ensures the report's objectivity, legitimacy and value. The complementary online data visualization tool allows clients to prepare and download custom data cuts to best match their specific situation.

Organizations Scale Back Security Budget Growth

On average, security budgets grew 4% in 2025, down from 8% in 2024. This signifies a continued and significant departure from the double-digit growth levels in the early 2020s.

The 2021–2022 post-pandemic recovery accelerated business growth and digital transformation. Government stimulus, supply chain recovery and general consumer confidence drove a surge in spending, benefitting security budgets in the process.

This period of accelerated growth ended in 2023, when growing global economic and political uncertainty, as well as rising inflation and interest rates, caused companies to spend more frugally, including on their security programs. This year’s further declining rate of growth was expected, as companies remain cautious amid market volatility and economic uncertainty.

More than half of CISOs report flat or reduced budgets

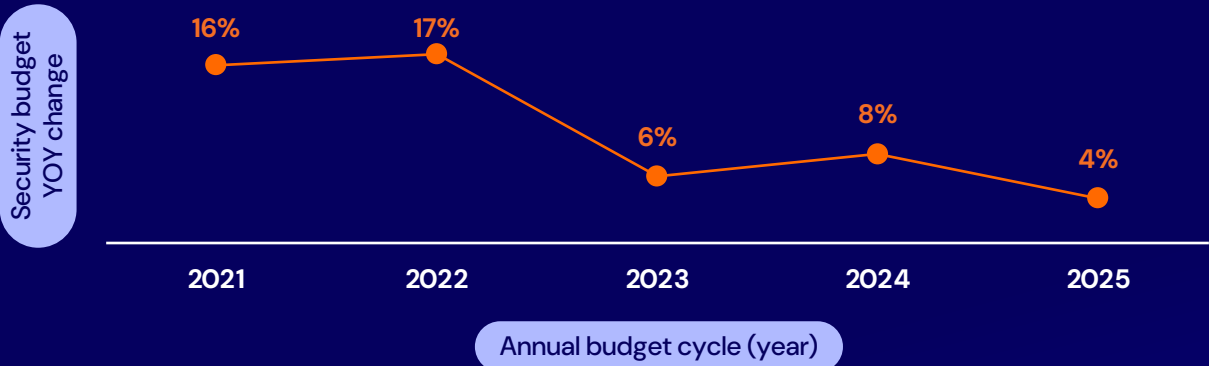
Beneath the headline average, growth levels show significant variation. Just 47% of CISOs increased their budgets—down from 62% last year and 78% in 2022. A growing share of CISOs had stagnant budgets—39% vs. 26% last year—and 15% tightened their budgets.

ORGANIZATIONS SCALE BACK SECURITY BUDGET GROWTH

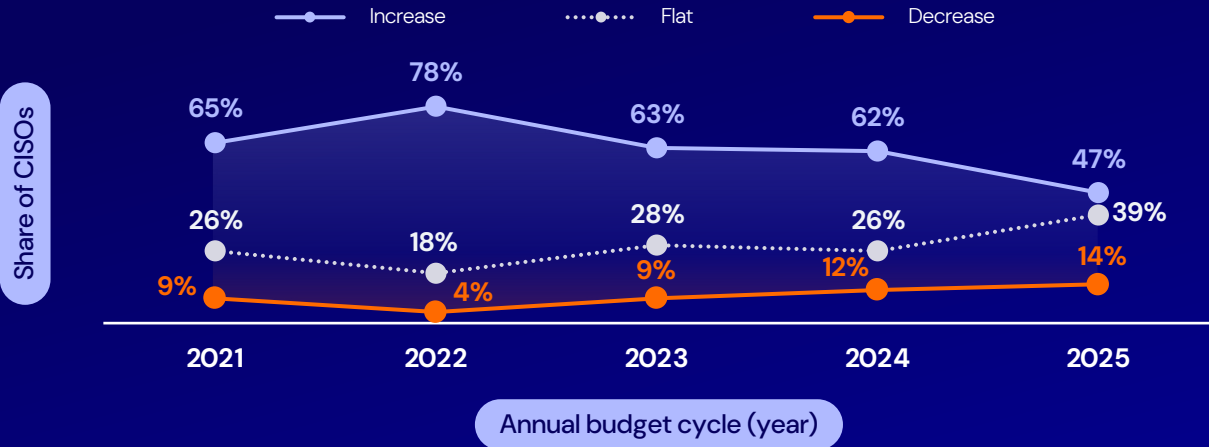
FIGURE 1 Multiyear Trend in Security Budget Growth Source: IANS & Artico Search

Multiyear Trend in Security Budget Growth

Year-over-year change in the security budget



Share of CISOs with increasing, flat and decreasing budgets



“Once again, we find security is not immune to macro conditions. Most CISOs are not receiving budget increases despite security typically being identified in the top five risks for companies.”

Steve Martano

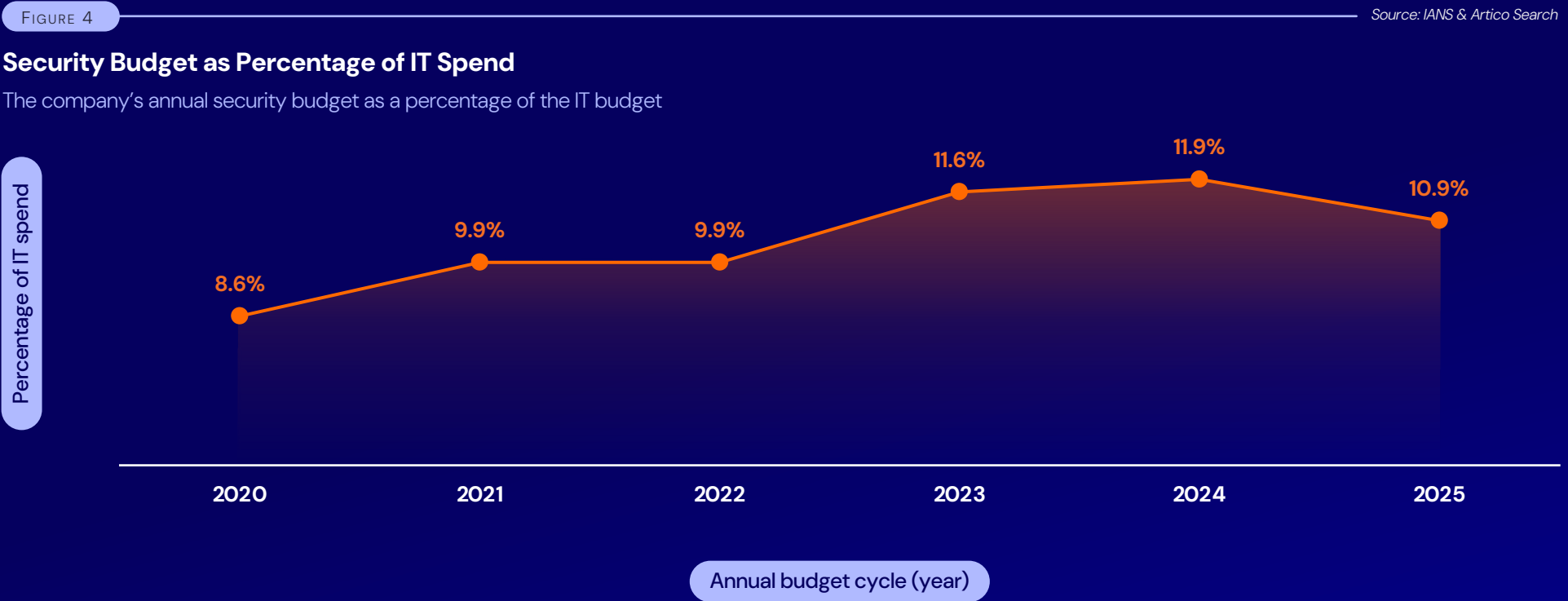
Budget Ratios Break From a Multiyear Trend

From 2020 to 2024, security budgets as a percentage of IT spend gradually increased from 8.6% to 11.9%. At companies where security is embedded in the IT budget, this meant a growing share of their IT spending was being allocated to security.

This metric fell for the first time in five years, dropping by a full percentage point to an average of 10.9%.

Several strategic and economic factors help explain this shift:

- Core IT spending has remained in low single digits in recent years and is now rebounding, driven by advancements in AI, increased cloud infrastructure investments and catch-up spending on software tools that had been delayed due to post-pandemic macroeconomic volatility.
- In many organizations, especially those in highly regulated industries, security programs have reached a level of maturity where foundational investments—such as IAM, endpoint protection, compliance tools and cloud migrations—are in place. As a result, the focus has shifted from large-scale capital expenditures on big projects to ongoing operational expenses, with an emphasis on optimization of existing systems rather than further expansion.



Security budget as percentage of revenue stagnates

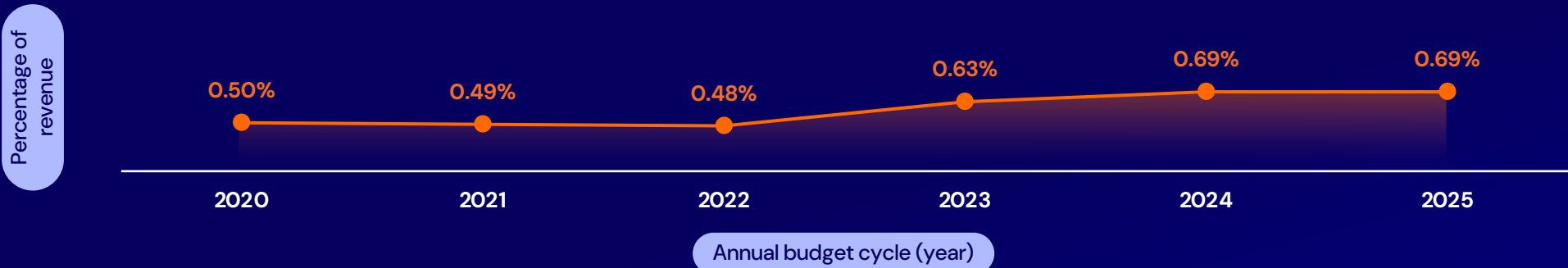
Security budget as a percentage of revenue showed a steady increase from 2022 to 2024. This year, it remained flat at 0.69%, meaning, on average, company revenue grew at about the same rate as security budgets.²

When asked how the annual growth of their security budgets compares to the organization’s annual revenue growth, about half of CISOs reported company revenue grew faster than the security budget, and 32% said they grew at about the same rate.

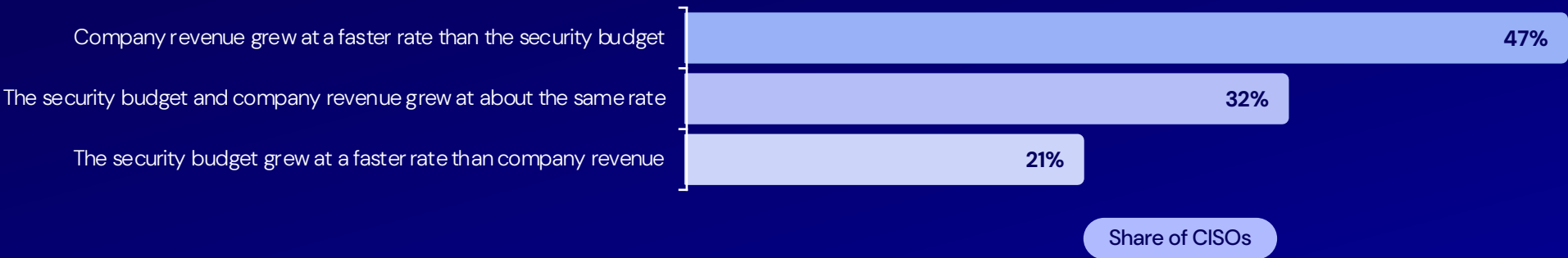
FIGURE 5 Source: IANS & Artico Search

Security Budget as Percentage of Revenue

The company’s annual security budget as a percentage of annual revenue



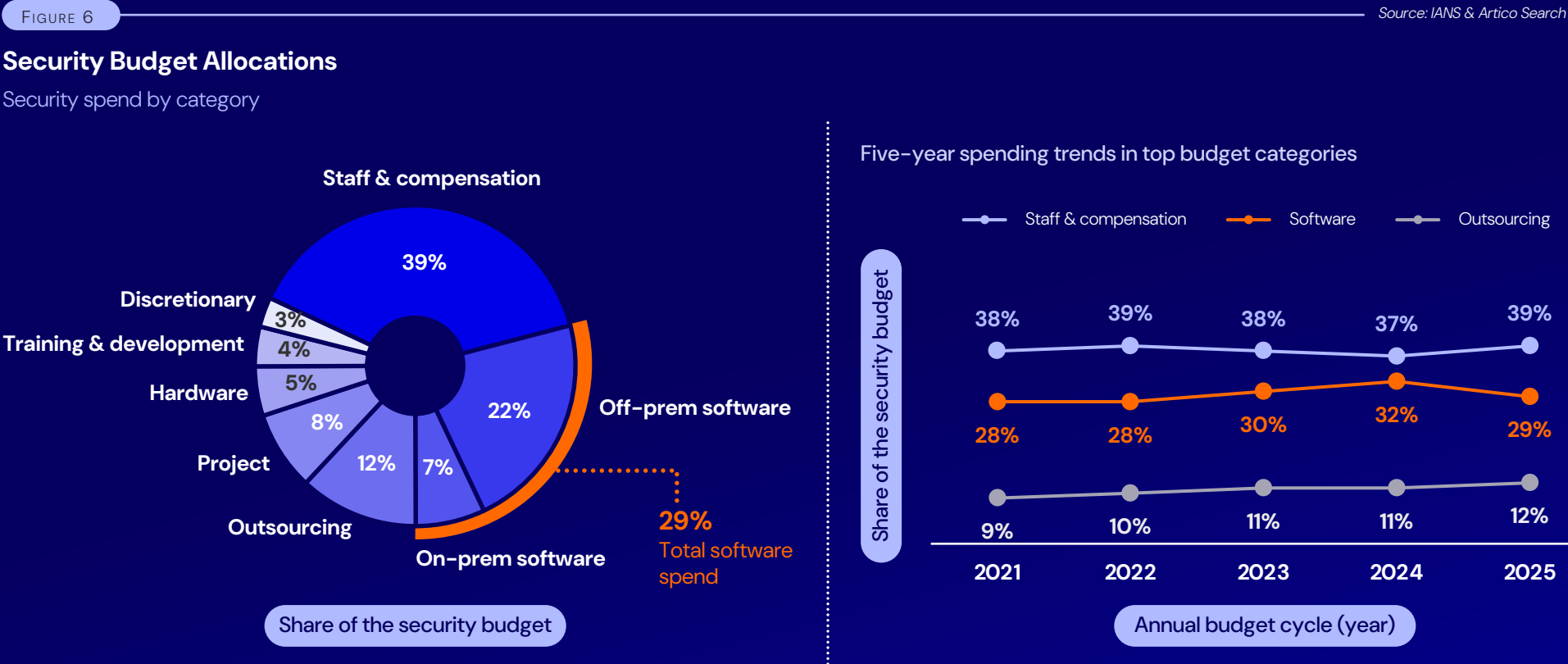
How does the annual growth of your security budget compare to the organization’s annual revenue growth?



How CISOs Allocate Their Budgets

As part of the survey, CISOs provided a breakdown of their security budget across eight common budget categories. In aggregate, staff & compensation costs account for the largest share of the budget (39%), followed by software (29%) and outsourcing (12%). Categories such as project budgets, hardware and training consume relatively smaller shares of the CISO's budget.

Over the last five years, the budget breakdown has remained relatively stable. A multiyear view of the three largest categories reveals marginal changes.



Breaking down the budget for security software

Within software budgets—which represent approximately 30% of the overall security budget—SecOps claims the largest share (16%). This makes SecOps the largest spending category in both security staff & compensation and security software, underscoring its critical role in an organization’s ability to respond to threats and meet compliance requirements (see FIGURE 8 on the next page).³

As organizations grow and scale, software spending patterns change:

The share of the software budget for SecOps and IAM grows with size. As organizations scale, the complexity of their IT environments increases, which drives a greater need for comprehensive SecOps and IAM solutions. Larger organizations typically have more endpoints, users and systems to secure, requiring advanced software tools to monitor and protect against evolving threats. Additionally, with increased regulatory requirements and a broader attack surface, larger organizations allocate more resources to SecOps and IAM software to ensure real-time threat detection, incident response and secure access management. At smaller organizations, SecOps is one of the more commonly outsourced functions, which is cost efficient and requires a slightly smaller share of the software budget.

The share going to cloud security and GRC decreases with company size. Large, established organizations, especially those in mature markets, often continue to rely heavily on legacy systems. As a result, they have higher proportionate spending levels for on-prem software and hardware needed to support these systems and relatively smaller allocations for cloud security and GRC. In contrast, smaller firms are more likely to have been cloud-native from the outset, leading to higher spending levels for cloud security and GRC.



Responsibility and ownership of IAM programs is a prime example of CISOs’ increased scope. Five years ago, most CISOs did not have direct accountability and ownership of identity programs; today, nearly all CISOs have that under their remit. IAM is an area of investment for most programs, with an increased share of software budget going toward IAM programs YOY.

Steve Martano

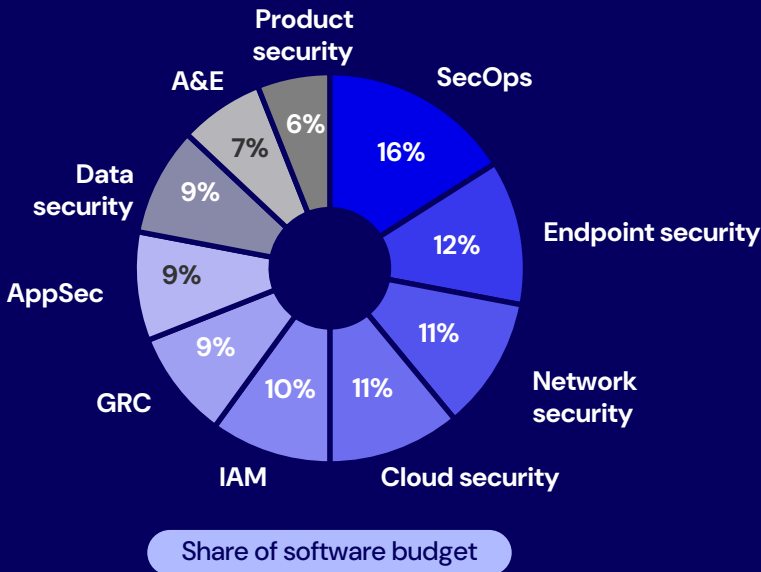
³ This breakdown accounts for situations where multiple tools are consolidated into one or more integrated platforms. In these instances, we allocated equal portions of the platform’s budget share to the functions it covers. For example, if the CISO reported 30% of the software budget went toward an integrated platform covering GRC, AppSec and cloud security, then each function would be assigned one-third of the platform’s budget share.

FIGURE 8

Source: IANS & Artico Search

How Budget for Software Is Allocated Across Functions

Breakdown of the annual security budget allocated to software



	SecOps	Endpoint security	IAM	Network security	Cloud security	GRC	AppSec	Data security	A&E	Product security
Less than \$400M	16%	11%	8%	11%	11%	11%	10%	9%	5%	7%
\$400M – \$1B	15%	12%	10%	9%	11%	10%	9%	10%	7%	7%
\$1.1B – \$5B	16%	13%	11%	10%	11%	8%	8%	10%	9%	4%
\$5.1B – \$10B	17%	12%	12%	13%	9%	9%	9%	8%	7%	6%
\$10B+	19%	10%	14%	11%	9%	7%	8%	9%	9%	5%

Totals do not always add up to 100% due to rounding.

Share of software budget

Staffing Growth Slows Amid Budget Pinches

The average growth rate of security team size was 7% this year—the lowest growth percentage in the past five years. Moreover, only 45% of CISOs were able to add net new headcount—down from 67% three years ago and 51% in 2023. A growing share of CISOs (47%, up from 38% in 2024 and 28% three years ago) kept their team size flat.

The staffing growth rate of 7% is considerably higher than the average security budget growth rate of 4%. While we expect budget and staffing growth trends to follow a similar pattern, the growth rates may diverge; staff & compensation represents only a portion of the overall security budget, as outlined earlier in this report.

“We continue to hear that CISOs have budget for tooling but not for staff increases, which leads to teams not being staffed adequately to take advantage of a tool’s full capabilities. As AI capabilities create efficiencies in repeatable tasks, more team members are able to find the time to utilize a platform’s capabilities.”

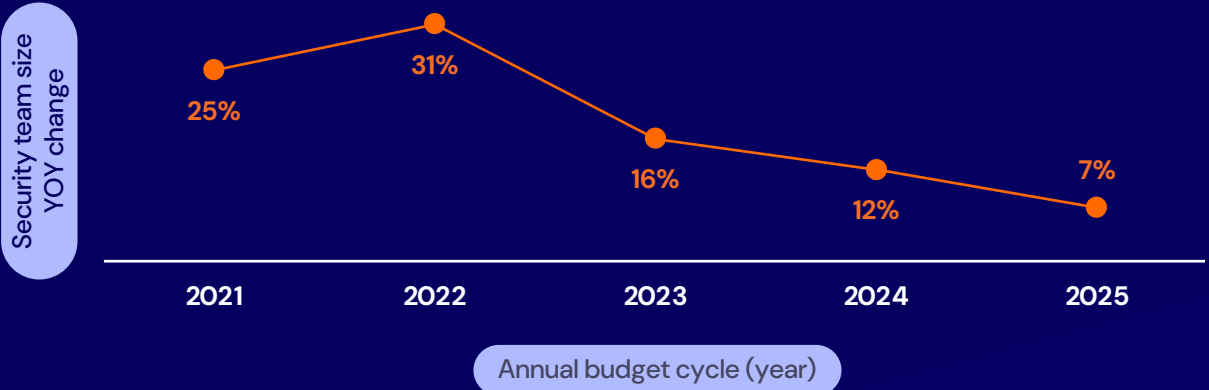
Steve Martano

STAFFING GROWTH SLOWS AMID BUDGET PINCHES

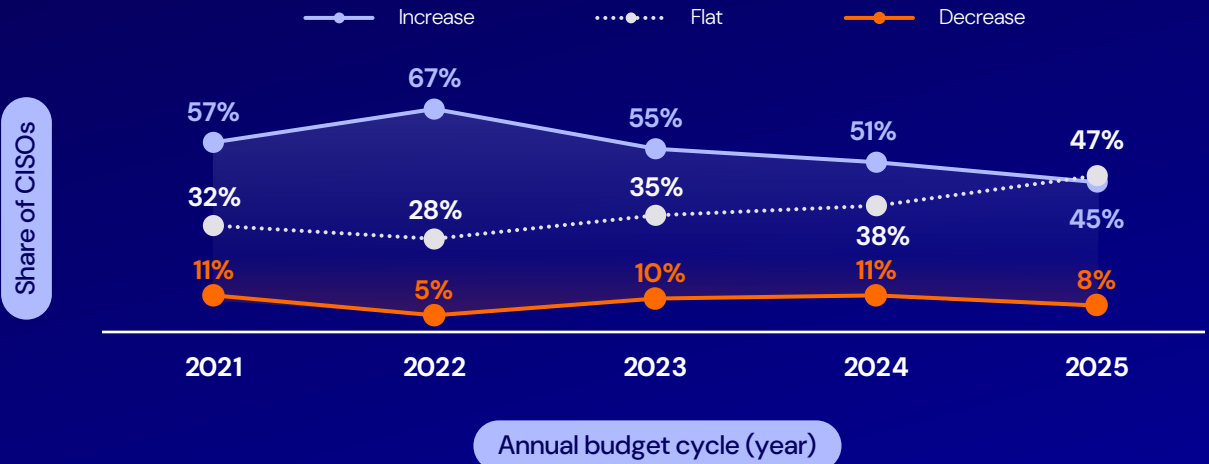
FIGURE 11 Multiyear Trend in Security Team Size Source: IANS & Artico Search

Multiyear Trend in Security Team Size

YOY change in security team size (employees and average count of independent contractors)



Share of CISOs with growing, flat and decreasing security teams (employees and average count of independent contractors)



Security teams understaffed and overwhelmed, according to CISOs

Despite 45% of security organizations growing their staffing levels, just 11% of CISOs indicated their organizations are adequately staffed. More than a third said they are stretched thin, and 53% said their teams are somewhat or severely understaffed.

Security teams with fewer than 10 members face the greatest staffing shortfalls, as they must provide a baseline level of security across key functions without the staff numbers to assign dedicated roles, unlike larger teams.

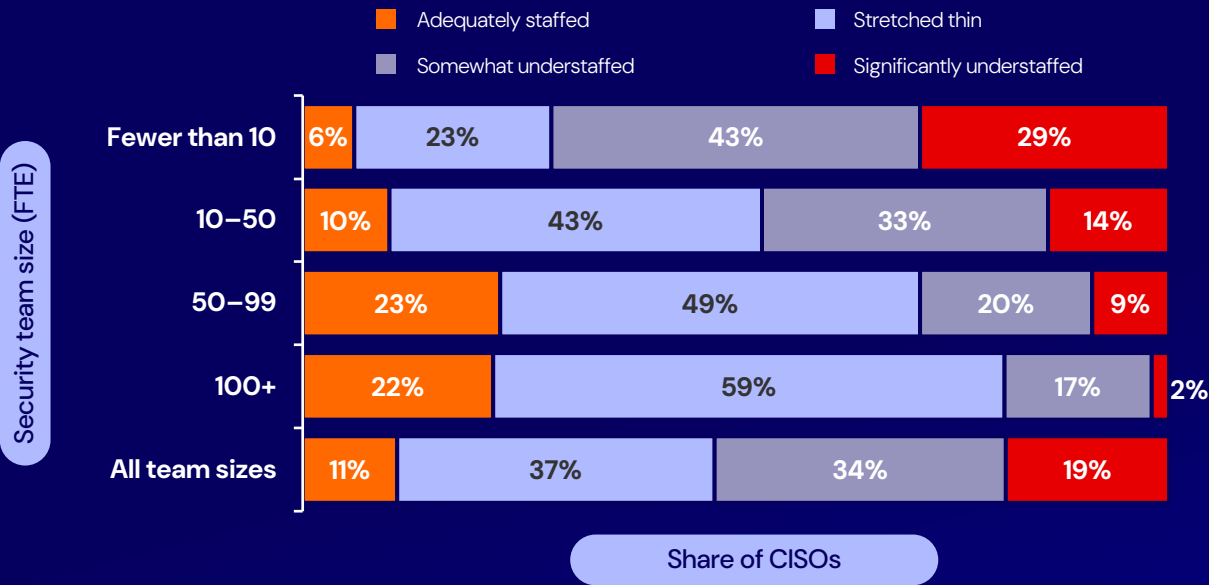
However, security programs tend to be more complex at larger organizations, and staffing growth typically does not keep pace with organizational expansion. As a result, even among CISOs with teams of 50 to 99 or 100-plus, more CISOs report being stretched thin or understaffed than adequately staffed.

STAFFING GROWTH SLOWS AMID BUDGET PINCHES

FIGURE 13 Source: IANS & Artico Search

Most CISOs Cope With Staffing Shortages

Does your organization have sufficient staff to effectively execute your security agenda?



Recommendations

If you are a CISO who has not received an increase in budget or staffing—or if your organization lacks sufficient resources or personnel—what steps should you consider taking?

The following recommendations provide practical strategies for security leaders to align with business objectives, prioritize effectively and manage resources in today's challenging organizational environments.

Align security objectives with business goals

To ensure security initiatives are relevant and effective, it's essential to connect them to the organization's broader business objectives. This alignment helps security leaders justify their priorities and demonstrate value to executive stakeholders.

Recommendations

- ✓ Understand the company's main business drivers, growth plans (such as M&As), product launches or market expansion.
- ✓ Tailor your security budget priorities to support these objectives, considering the risks, compliance requirements and regulatory implications for each business direction.
- ✓ Use your team's alignment with business objectives to defend existing resources and reprioritize efforts as needed.

Prioritize security efforts strategically

With limited resources, not every task can be treated as equally urgent. Strategic prioritization ensures the most critical assets and risks receive the attention they deserve, while less urgent items are appropriately deferred.

Recommendations

- ✓ Identify and focus on protecting the organization's "crown jewels," the most vital assets.
- ✓ Get executive buy-in on initiatives you need to delay, outlining the trade-offs and potential impacts. Revisit your roadmap, consider how reprioritization will impact your ability to hit long-term goals and clearly communicate the value of prioritizing around the most critical tasks.

Submit budget requests realistically

Effective budget management requires a clear understanding of both internal and external business environments. Security leaders should make well-informed budget requests and show how existing investments can be optimized for greater effectiveness.

Recommendations

- ✓ Research budget trends—such as those offered in this report—within your sector and peer groups to inform your requests.
- ✓ Align budget asks with the company's current business context and growth trajectory.
- ✓ Maximize the use of existing tools and automation to reduce manual workloads, as it's often easier to secure funding for technology than for additional staff.

Methodology

IANIS and Artico Search fielded their sixth annual CISO Compensation and Budget survey in April 2025. From April until August, we received survey responses from 587 security executives at a diverse set of companies.

Key steps in the research process are:

Survey design

We improve our surveys on an ongoing basis by incorporating feedback from respondents and adding topics based on client demand.

Respondent recruitment

We recruit from last year's already-vetted respondents. We grew the sample by recruiting from diverse CISO audiences. Respondents receive a complimentary copy of the research. There is no monetary compensation attached to taking the survey.

Data hygiene

The survey design and data collection process includes precautions to prevent fake respondents and survey response errors. For example, respondents can skip questions if they don't have access to the requested information.

Analysis

A five-member team runs the analysis, builds the storyline and writes the report. This is a multidisciplinary team with combined expertise in data science, cybersecurity, CISOs' key imperatives, and cyber executive talent and recruitment.

Objectivity

This research is neither influenced by nor paid for by third parties. We report on the data objectively and free from personal bias and opinions. Clarifying insights are drawn from Artico's cyber practice and clearly marked as quotes.

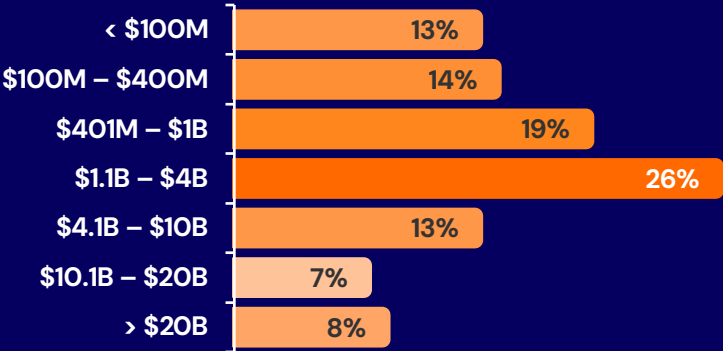
Sample breakdown

Respondents provided a range of budget data, including the absolute and relative size of their company's security budgets, the annual growth rate of the budget, and how the budget breaks down into a set of commonly used spending categories. Using respondents' data, we calculated averages (the statistical mean).

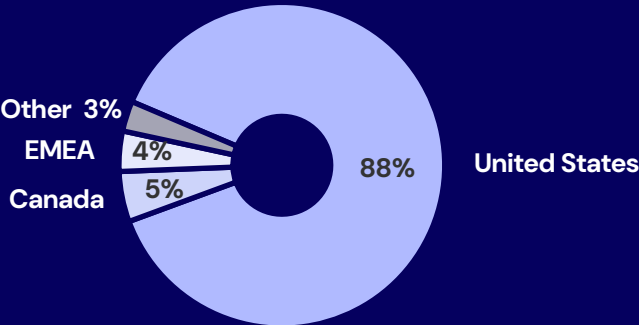
FIGURE 15
 Source: IANS & Artico Search

Sample Breakdown

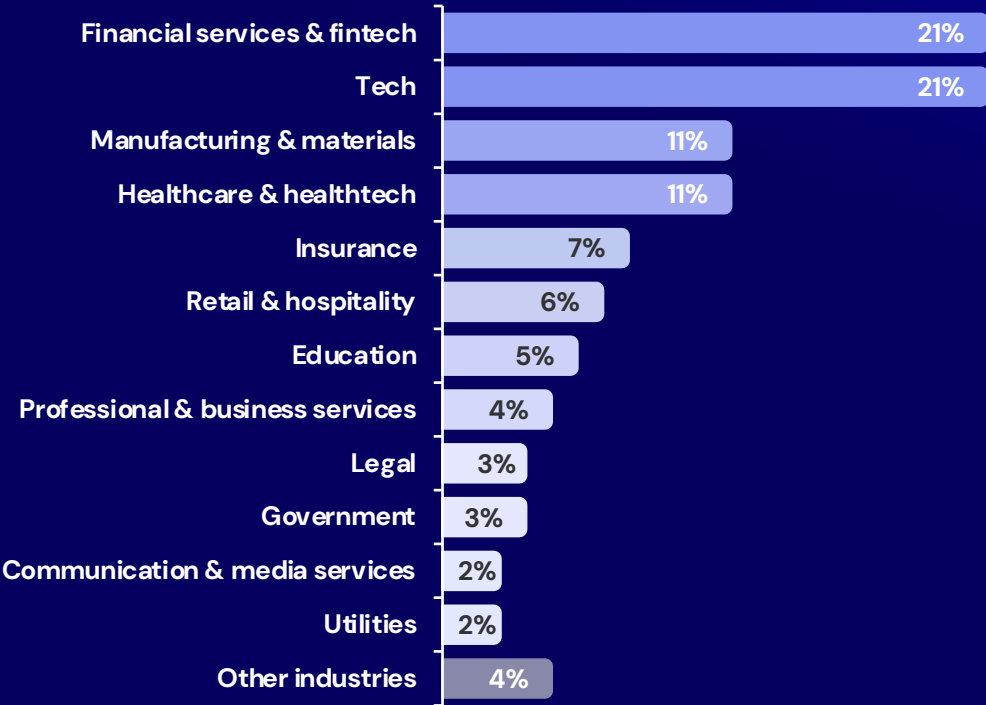
Breakdown by annual revenue in USD



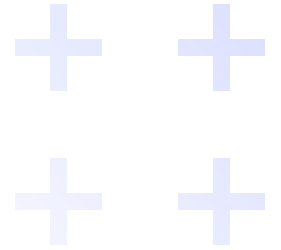
Breakdown by CISO primary location



Breakdown by primary industry



"Other industries" includes energy, transportation, real estate, affinity groups & nonprofit organizations, and holding companies & conglomerates.



About Us

This publication is created in partnership between IANS and Artico Search.

IANS

iansresearch.com

For the security practitioner caught between rapidly evolving threats and demanding executives, IANS is a trusted resource to help CISOs and their teams make decisions and articulate risk. IANS provides experience-based insights from a network of seasoned practitioners through Ask-an-Expert inquiries, a peer community, deployment-focused reports, tools and templates, and executive development and consulting.



Artico Search

articosearch.com

Founded in 2021, Artico Search's team of executive recruiters focuses on a "grow and protect" model, recruiting senior go-to-market and security executives in growth venture, private equity and public companies. Artico's dedicated security practice delivers CISOs and other senior-level information security professionals for a diverse set of clients.

