



Cybersecurity Perspectives 2024

Enterprises Race to Defend Against
Accelerated Pace of Emerging Threats

SCALE

Table of Contents

Section 1:	Introduction	3
Section 2:	Key Findings	4
Section 3:	Where the Threats Are	5
Section 4:	How Enterprises Are Responding	7
Section 5:	Resource Gaps: People, Technology & Budget	9
Section 6:	Market Opportunities	15
Section 7:	Where the Funding Is	17
Section 8:	Conclusion	19
Section 9:	Endnotes & Methodology	20

Introduction

The shift to the cloud, like most transformational technologies, has been a slow transition over the past decade. In the past five years, we've seen more enterprises making the shift to cloud-based infrastructure and applications and, as they do, they become reliant on third-party cloud providers, opening new vulnerabilities and areas of exposure that didn't exist before.

As CISOs seek stable ground in the face of increasing cloud complexity, a new trend has emerged:

AI acts as an accelerant, promising efficiency, automation, and a lower barrier to entry for both defenders and attackers.

In order to keep up with threat actors, CISOs are increasingly looking at AI to improve their own security posture, with 89% of security leaders indicating that AI is important to improving their security in 2025.

As these trends converge, Scale Venture Partners has conducted ongoing research to understand the challenges CISOs are facing and how solutions are evolving. Now in its 11th year, this year's report consolidates perspectives from CISOs, CIOs, VPs, directors, and IT managers.

Our research shows more security incidents, with 76% of companies reporting three or more security incident types. Cloud infrastructure security reclaimed the top priority spot for CISOs, and data center/server security jumped in importance from 8th in 2023 to second.

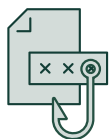
While we're still in the early days of AI adoption, CISOs are taking a proactive stance.

Although budget growth has slowed, enterprises allocated 29% more budget toward new, innovative, and experimental security solutions this year.

In the face of increased threats, contracting budgets, and continued talent shortages, CISOs are strategizing to ensure they don't fall behind in the AI arms race while navigating security in the age of cloud apps and cloud infrastructure.

* Note: Unless specifically documented, all data sources are from Scale Venture Partners' primary survey research, and YoY% is used to represent relative change (as opposed to absolute change) throughout.

Key Findings



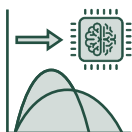
Data breaches increased, led by phishing and third-party attacks

38% more companies suffered data breaches last year, with 31% of surveyed enterprises affected. Nearly 50% of firms lost credentials to phishing and third-party attacks, as cybercriminals used legitimate identity privileges to spread ransomware, exfiltrate data, and extort victims.



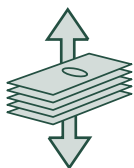
CISOs prioritized cloud infrastructure and data center security

Increased ransomware, supply chain attacks, and data breaches drove security strategies this year. Top priorities were cloud infrastructure security (1st), data center security (2nd), and identity access management (3rd), along with data privacy (4th), data security (5th), and anti-data exfiltration (7th).



Attackers targeted AI models while security played catch up

AI was the second most unaddressed challenge after ransomware. 11% of firms suffered AI model drift from security incidents last year, a 304% YoY increase, with 46% unable to observe or monitor AI drift. 63% were concerned about governing AI/ML models in third-party software.



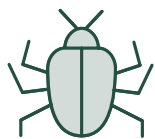
Security budget growth showed signs of slowing

Insufficient budgets ranked as the third biggest barrier for security leaders. Mid-sized security budgets declined 1%, down from growth rates of 5% in 2022 and 51% in 2023. Enterprise security budgets grew more slowly at 16% YoY, down from a 22% YoY increase last year, a 27% decline in growth rate.



Market gaps found in software supply chain security and ADX

Market opportunities were uncovered in software supply chain security, data center security, and anti-data exfiltration (ADX), with a 42%+ delta between “satisfaction” and “importance.” 47% of firms intended to build in-house tools, but of those, only 9% for ADX and 7% for software supply chain security.



Where the Threats Are

Nearly half of all companies were compromised by phishing and third-party attacks

Almost 50% of organizations experienced phishing or third-party attacks that resulted in compromised credentials last year. Around 37% of firms reported cloud service attacks, down 25% YoY from 50% the previous year.

Data breaches spiked 38% YoY, affecting 31% of enterprises, as ransomware rebounded from 25% in 2022 to 30% in 2023, allowing attackers to exfiltrate valuable data.

However, cybercriminals pivoted from ransomware-based data encryption toward immediate threats of publishing stolen data, leading to a 76% uptick in data extortion last year, according to CrowdStrike.¹

Security teams struggled to protect AI models, while trying to fully realize AI's true potential. **Security incidents caused AI model drift at 11% of enterprises last year, up 304% YoY.**

What security incidents occurred at your organization over the last 12 months?



49%

Phishing attack compromised credentials



48%

Compromised by attack on 3rd party



37%

Cloud service attacked



31%

Data breach of sensitive information



30%

Employee stole our information



30%

Ransomware encrypted our data



28%

Misconfigured cloud access rights led to data breach



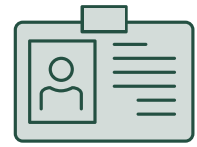
25%

Compromised by software supply chain vulnerability

Attackers gain higher ROI with identity-based attacks

Cybercriminals used stolen credentials to legitimately access cloud infrastructure and data centers instead of hacking vulnerabilities, with double-digit increases in phishing and third-party attacks YoY.

A single software supply chain attack or third-party attack allows threat actors to breach multiple downstream victims, thereby increasing their ROI and efficiency, according to CrowdStrike.² Results have been devastating, with “identity-based” breaches the hardest to detect (328 days) and second-most expensive to resolve (\$4.62M) on average, according to IBM Security.³

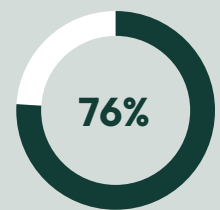


30%

of all security incidents IBM responded to last year were “identity-based” attacks.⁴

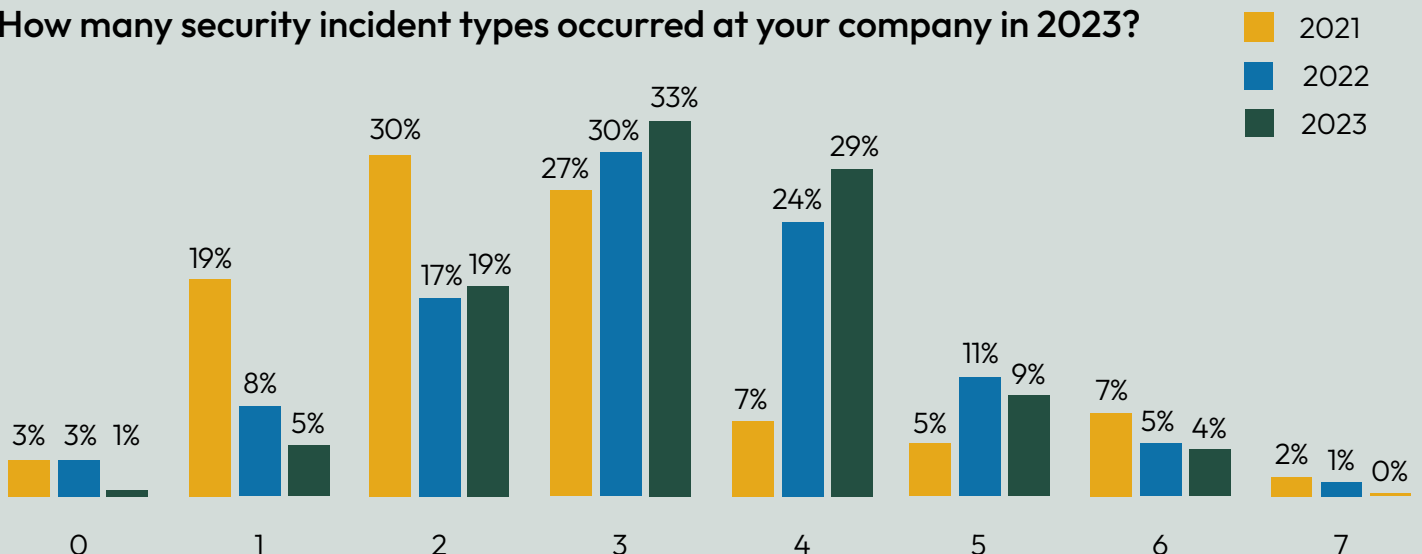
Security teams responded to three or more incident types

There was an increase in the number of companies that experienced multiple security incident types last year, as **76% of enterprises reported three or more incidents**. Firms with one incident type declined 76% YoY, down from 19% to only 5%. The number of companies **with four incident types increased 341% over the last two years, up from 7% in 2021 to 29% in 2023**. Data breaches affected mid-sized (37%) firms more than large enterprises (29%) in 2023.



Experienced three or more types of security incidents

How many security incident types occurred at your company in 2023?



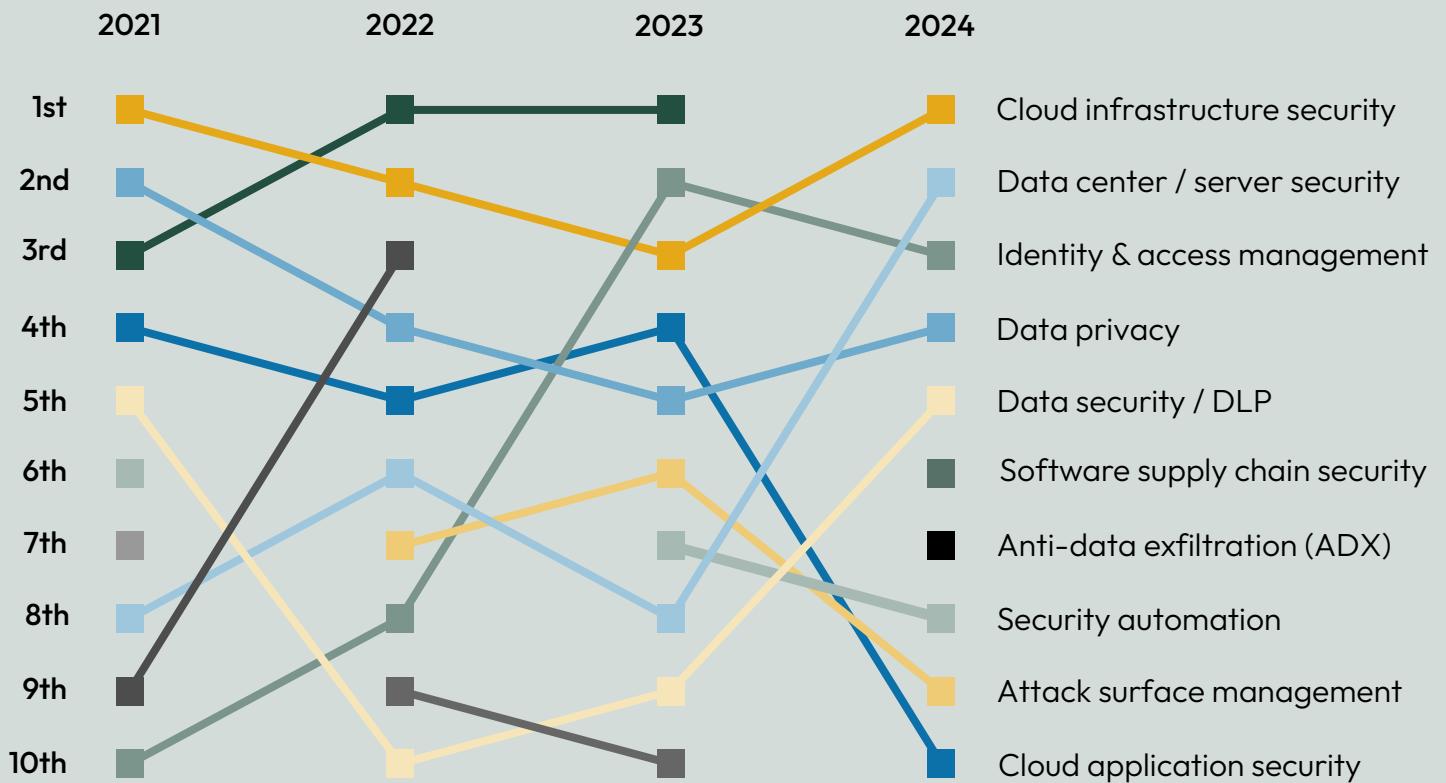


How Enterprises Are Responding

Both cloud infrastructure and data center security top list for first time since 2016

Cloud infrastructure security, data center security, and identity access management topped the list, as security leaders re-shuffled priorities in response to increased ransomware and data breaches. Data-related security filled three spots as CISOs scrambled to protect data across on-premise, hybrid, and multi-cloud environments. Anti-data exfiltration and software supply chain security joined the list, while network security dropped from first place last year off the Top 10 entirely.

What are your top investment priorities for cybersecurity technologies and strategies?

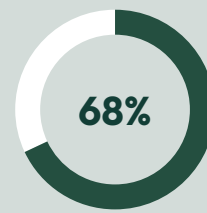


2023 ■ Network security ■ Zero-trust network access
 2022 ■ Endpoint security 2021 ■ Operational technology (OT)

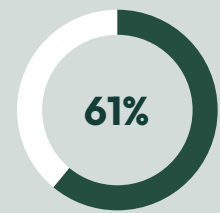
CISOs react to ransomware once again

Ransomware continued to occupy the most CISO headspace this year, influencing 68% of cybersecurity strategies, despite a 19% decline in attention from an 84% high last year.

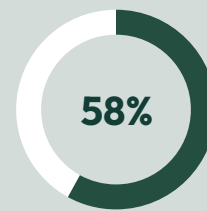
Security leaders also expressed growing concerns over supply chain attacks (61%) this year, as well as decreased cybersecurity budgets (53%), which have historically remained resilient. Long-held worries about the cybersecurity skills gap (57%) and data privacy requirements (56%) have tapered off by 18% and 9% respectively since last year.



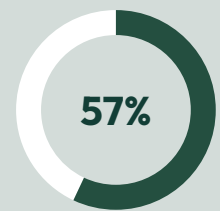
Ransomware attacks



Supply chain attacks



Hyperscale cloud data breaches



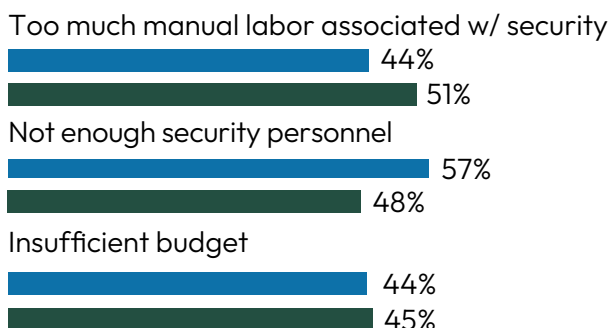
Cybersecurity skills gap

Security leaders adopted fewer strategic priorities, cooling on vendor consolidation

Security leaders ranked too much manual labor (51%) as the biggest barrier to achieving their desired security posture this year, followed by not enough security personnel (48%) and insufficient budget (45%). For the third year in a row, their top strategic priority was to enforce existing security policies more strictly (73%). With nearly 50% of firms compromised by a third-party attack last year, security leaders hoped to improve insight into third-party risk (58%) and govern AI/ML built into third-party software (63%), which debuted this year as the second priority. **After two years of security vendor consolidation, CISOs cooled on this strategy, which dropped 30% YoY from a 62% high to this year's 48% low.**

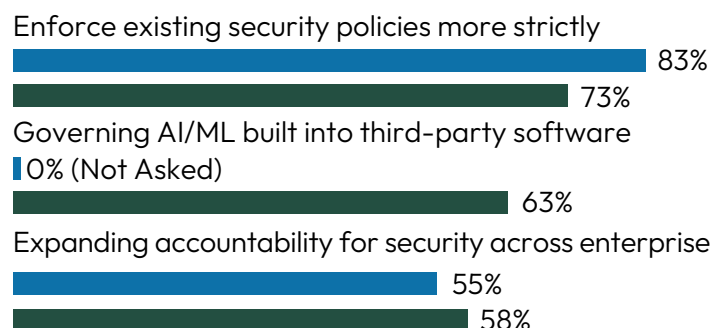


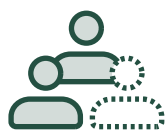
Top 3 Barriers:



Top 3 Priorities:

2022 2023





Resource Gaps: People

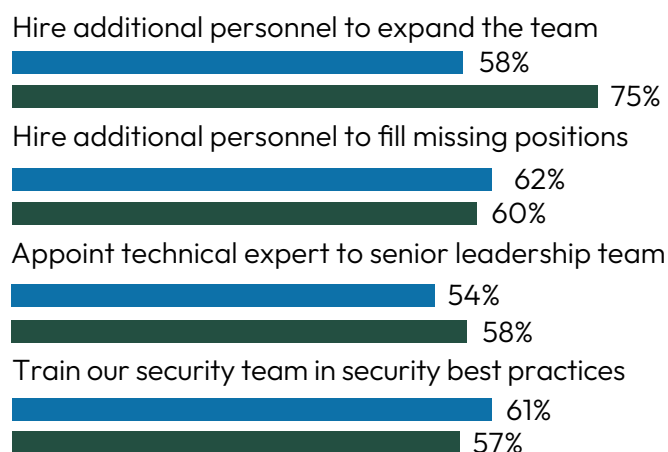
Security teams remain understaffed because of the cybersecurity skills shortage

Four million cybersecurity professionals are still needed to close the growing global cybersecurity skills gap, according to ISC2.⁵

75% of security leaders planned to hire additional security personnel over the next 12 months. However, 57% were unable to find people with the required skill set.

Another 50% were unable to pay enough salary to attract new staff or were concerned their current staff would leave for better paid positions at another firm.

Security team changes: ■ 2022 ■ 2024

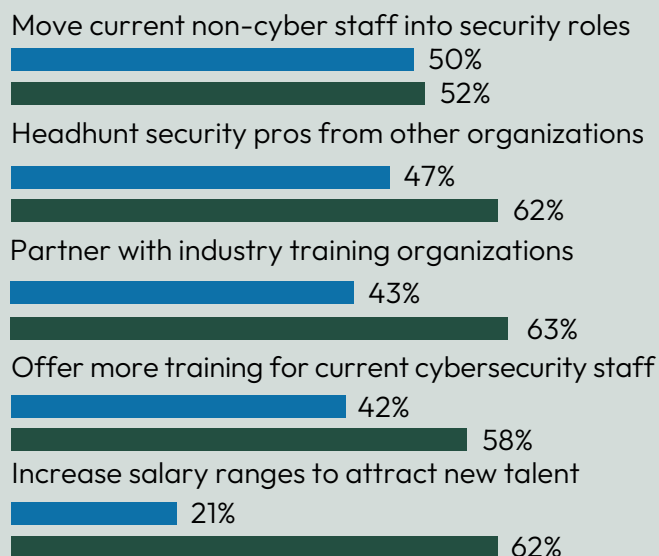


CISO hiring strategies constrained

62% of security leaders believed the most effective strategy for addressing the cybersecurity skills gap was to increase the salary range for cybersecurity roles, yet **only 21% of firms actually intended to increase salaries to attract new talent.**

50% of CISOs intended to identify current staff in non-cyber roles who could move into security roles, despite only 52% of companies believing this strategy was effective. Training strategies were less prioritized, but considered more effective.

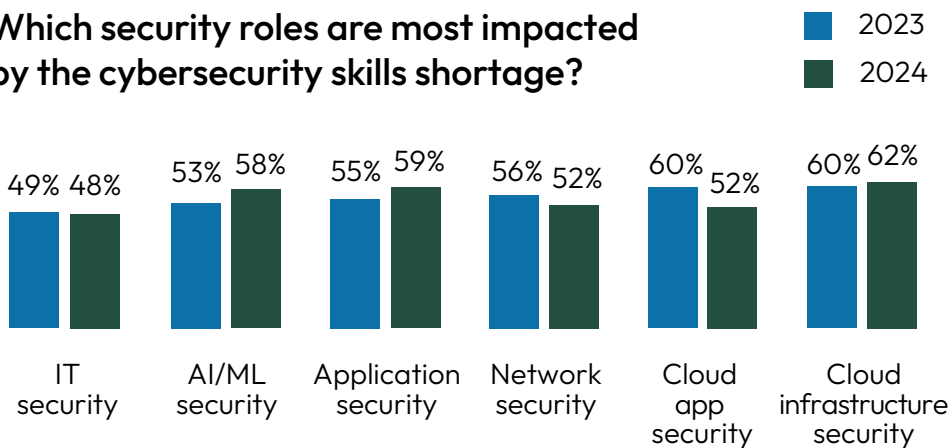
“Priority” vs. “effectiveness” of strategies to address the cybersecurity skills gap:



Cloud infrastructure security roles are hardest to fill

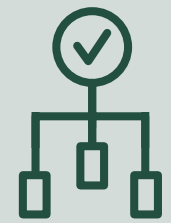
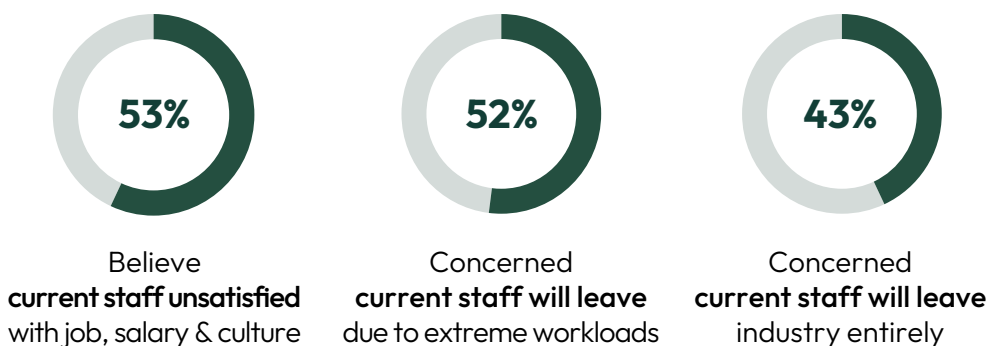
Security leaders had the most difficult time hiring and retaining cloud infrastructure security roles (60%), followed by application security roles (59%), and AI/ML security roles (58%). The cybersecurity skills shortage has had less impact on cloud application security roles (52%), network security roles (52%), and IT security roles (48%) since last year.

Which security roles are most impacted by the cybersecurity skills shortage?



Cybersecurity staff retention challenges persist

More than half of security leaders believed cybersecurity team members were unsatisfied with their jobs, salary, and work culture. Although 12% of security teams turned over last year, 52% of CISOs were concerned their teams would soon leave because of burnout and extreme workloads. 43% of security leaders were worried their staff would leave the cybersecurity industry to do something else entirely.



C-Suite Support:

86%

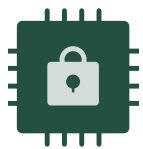
of security leaders believed their C-suite understands the business impact of security



Cybersecurity Turnover:

12%

of security teams experienced turnover within the last 12 months



Resource Gaps: Technology

CISOs underestimate protections against rising phishing attacks and data breaches

The average effectiveness of cybersecurity protections declined for the third year in a row, falling the most against crypto jacking (-18%), targeted phishing attacks (-15%), and data privacy compliance (-14%).

Cybersecurity protections were least effective in governing AI/ML capabilities built into third-party software (39%), a question which was asked for the first time in this year’s survey.

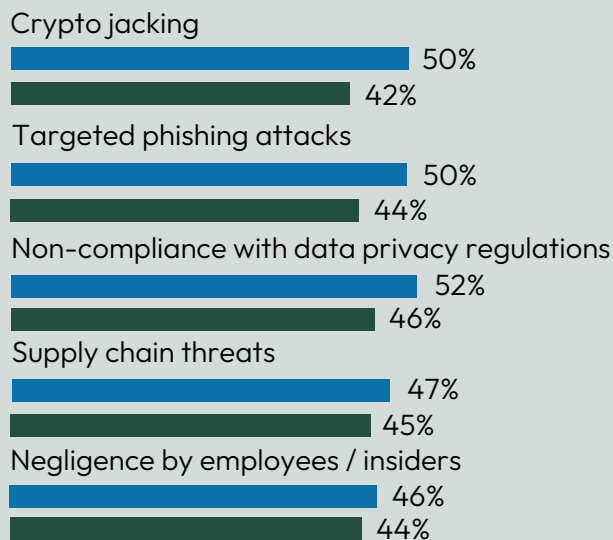
Despite an increase in the frequency and volume of attacks, cybersecurity effectiveness reportedly increased the most against data breaches (+11%), unpatched vulnerabilities (+10%), and nation-state attacks (+10%).

Although **61% of security leaders believed they were most protected against general phishing attacks**, almost 50% of firms lost compromised credentials to phishing attacks last year with 31% affected by data breaches.

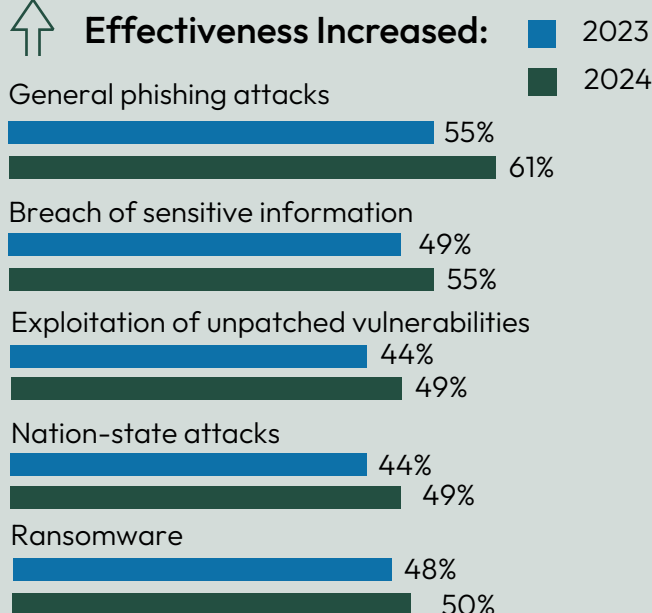
How “effective” or “extremely effective” are your current cybersecurity protections?



Effectiveness Declined:



Effectiveness Increased:



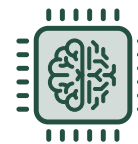
Ransomware is the top unaddressed challenge



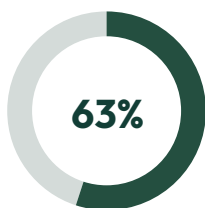
Four of the top five challenges aligned with an increase in the types of security incidents enterprises experienced last year. Ransomware was the top unaddressed challenge, with security leaders worried about “double extortion attacks,” followed by AI/ML (2nd), third-party attacks (3rd), and cyber attacks (5th).

Unaddressed Challenges in Security Leaders’ Own Words	
Ransomware	“Ransomware is more sophisticated.”
AI/ML	“AI makes hackers harder to defend.”
Third-party attacks	“Third-party threats compromised credentials.”
Cyber attacks	“Data breaches are escalating.”

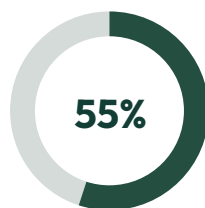
AI/ML is the second most unaddressed challenge



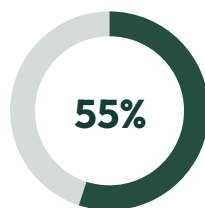
89% of security leaders believe AI/ML is “important” to improve their security posture by 2025, up from 79% last year. 63% of firms were concerned about governing AI/ML capabilities built into third-party software. 55% of companies were worried about drift in AI models over time, as well as the risk of AI/ML models being poisoned by threat actors to circumvent security. CISOs were less concerned about employees uploading sensitive data to ChatGPT (53%) this year.



Governing AI/ML capabilities built into third-party software



Drift in AI models over time



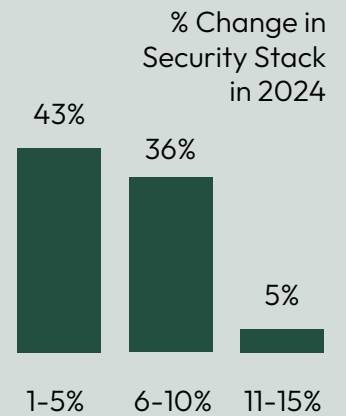
Poisoning of AI/ML models to circumvent security



Security Tools:

43%

expected their security stack to change 1-5%



91%

want to deploy more security tools over the next 12 months

+8

Average # of new tools budgeted for this year

+18

Average # of new tools preferred to deploy



Resource Gaps: Budget

Large enterprise security budget growth slowed, while mid-sized budgets stalled

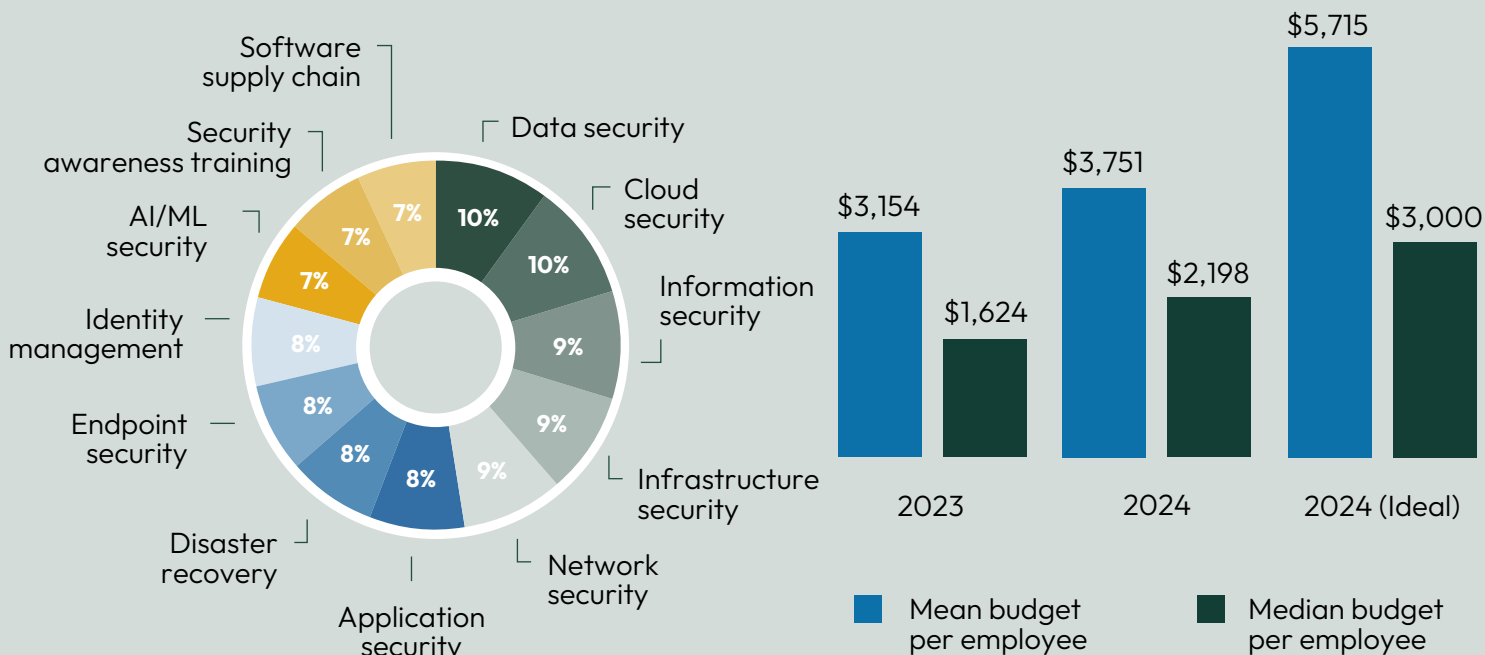
Once resilient security budgets showed signs of fatigue against economic headwinds, as security leaders ranked “insufficient budgets” the third biggest barrier to achieving their desired security posture.

Large enterprise security budgets still went up 16%, increasing at a slower pace this year after achieving growth rates of 22% and 19% over the last two years. **Mid-sized security budgets went down 1%**, falling slightly after 5% and 51% growth in 2022 and 2023.

As security budgets came under pressure, CISOs were “very smart and almost surgical with the precision” in which technologies they invested in to prevent ongoing threats, according to The Wall Street Journal.⁶

Security leaders allocated 10% of security budgets to data security and cloud security, the top two spending categories this year. Information security, infrastructure security, data security, and AI/ML security all received budget increases this year.

What is your total budget and category allocations for security solutions in 2024?



CISOs adjusted to smaller security budgets than expected

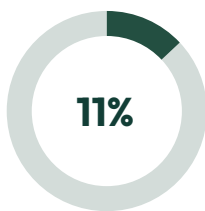
CISOs would have asked for 52% more budget than approved in 2024, compared with 24% more budget than approved in 2023, a 117% YoY gain mirroring the fiscal constraints security leaders faced this year.

Under ideal budget scenarios, security leaders would have allocated more budget toward infrastructure (+3%), data (+3%), AI/ML (+2%), information security (+2%), and disaster recovery (+1%). They would have prioritized less budget for application (-4%), network (-4%), endpoint (-3%), software supply chain (-3%), and cloud security (-1%).

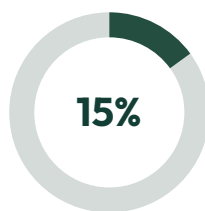
More Budget is Ideal for 2024	Less Budget is Ideal for 2024
Infrastructure security (+3%)	Application security (-4%)
Data security (+3%)	Network security (-4%)
AI/ML security (+2%)	Endpoint security (-3%)
Information security (+2%)	Software supply chain security (-3%)
Disaster recovery (+1%)	Cloud security (-1%)

Security leaders invested in experimental security budgets

Enterprises allocated 29% more budget for new, innovative, and experimental security solutions this year, up from 11% to 15% of total budget. Security leaders expressed interest in the potential of emerging technologies, such as AI, zero trust network access, blockchain, and machine learning to “stay ahead of threat actors.”



Percentage of 2023 total budget for emerging solutions



Percentage of 2024 total budget for emerging solutions



Year-over-Year budget growth for emerging solutions



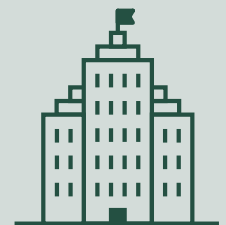
Mid-sized Enterprises
(500-999 employees)

-1%

Year-over-Year Budget Decline

\$200K-\$13M

Budget Range



Large Enterprises
(1,000+ employees)

16%

Year-over-Year Budget Growth

\$300K-\$155M

Budget Range



Market Opportunities

Market gaps found in software supply chain security and anti-data exfiltration

“Better security solutions” were reported as one of the top five unaddressed challenges this year for enterprises to “save time, resources, and improve accuracy.”

43% of CISOs were unable to find the right cybersecurity tools in the market, a 37% YoY increase over the last three years.

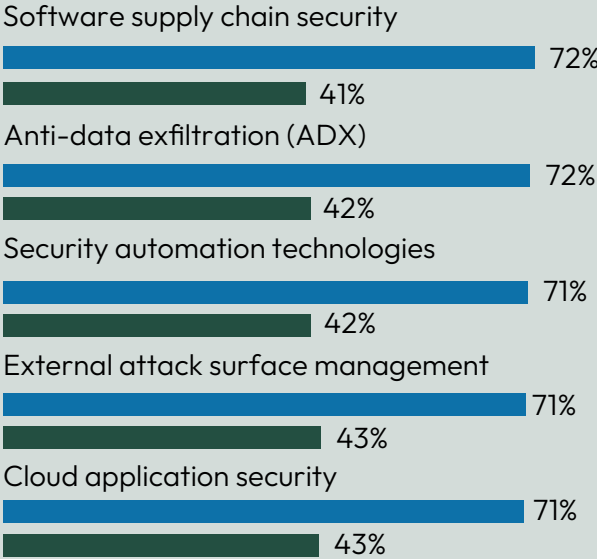
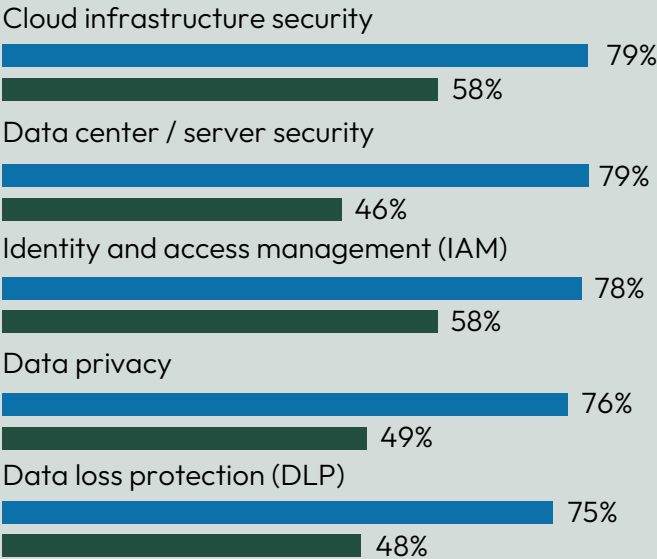
Security leaders were least satisfied with software supply chain security (41%), along with endpoint security, security automation, and anti-data exfiltration (42%) tools.

Cloud infrastructure security (79%), data center security (79%), and identity access management (78%) were the most important tools.

The biggest market gaps were found in software supply chain security, data center security, and anti-data exfiltration, with a 42%+ delta in “importance” and “satisfaction.”

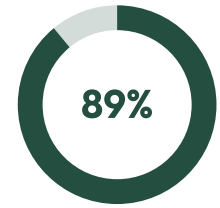
47% of firms intended to build in-house tools, but of those, only 9% for ADX and 7% for software supply chain security, compared with 30% for data center security.

Current “importance” vs. “satisfaction” for commercially-available cybersecurity tools:



AI tops list of emerging innovations with greatest potential

The majority of security leaders believe AI is the emerging innovation that offers the greatest potential to boost cybersecurity. Respondents were hopeful in AI’s ability to “self-react to threats,” “streamline risk evaluation,” “enhance efficiency and accuracy,” “enable prompt issue resolution,” and “leave more time and energy for our teams.”



Believe AI/ML is important to **improve their security posture** by 2025

Interest in building cloud infrastructure security solutions jumps 145% YoY

The number of firms that intended to build in-house tools increased for the third year in a row, up 21% in that period to 47% this year, as **interest in cloud infrastructure security solutions skyrocketed 145% since last year.**

Of those firms interested in building in-house tools, 75% were large enterprises with more than 1,000 employees and 25% were mid-sized companies with 500 to 999 employees.

Security teams were most likely to build in-house solutions for cloud infrastructure security (40%), identity access management (35%), threat intelligence (34%), and cloud application security (33%).

Firms were least likely to build in-house tools for anti-data exfiltration (9%), AI/ML model security (9%), software supply chain security (7%), and CI/CD security (1%).

Most likely solutions to build in-house over the next 12 months:



Least likely solutions to build in-house over the next 12 months:





Where the Funding Is

Cybersecurity investment dropped 46%, falling sharply across all stages of funding

Cybersecurity funding declined last year, falling 46% over four consecutive quarters to reach \$9.6B in 2023, down from its \$24.6B all-time peak in 2021 and \$17.8B in 2022, according to Pitchbook.⁷

Funding dropped across all stages, driven by a 60% reduction in late-stage (Series C and D) deal activity, unlike 2022 when angel, seed, and early-stage (Series A and B) funding increased despite the downturn.

Deal count fell to 693 deals in 2023, down 14% YoY from 919 deals in 2022, with 34% fewer angel/seed deals and 23% less early-stage deals, as “generalist VCs shied away from the vertical,” according to Pitchbook.⁸

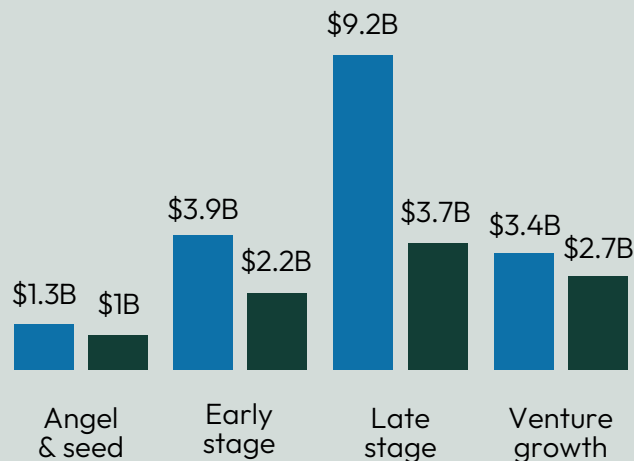
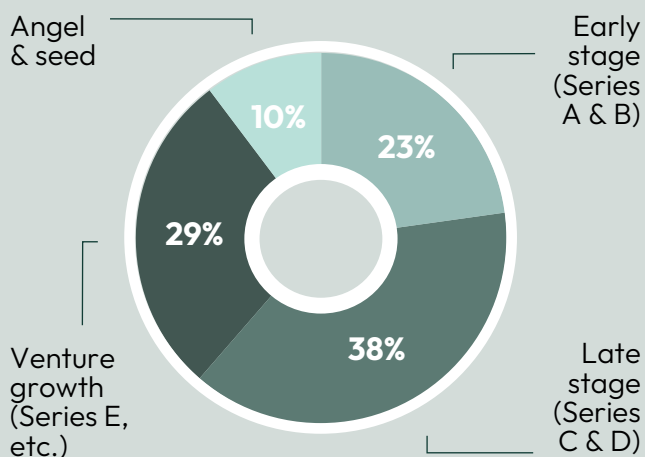
Exit value actually increased to \$4.4B in 2023, up 52% YoY from \$2.9B in 2022, despite less overall deal flow. That value is an 86% contraction from the industry’s all-time peak of \$30.8B in 2021.

Global security investment by funding stage:

(Source: Pitchbook Emerging Tech Research)

\$9.6B Global cybersecurity VC deal activity in 2023

-46% Year-over-Year in 2023 Funding




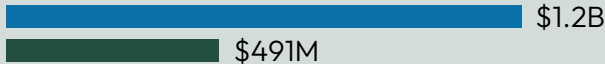

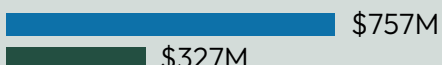

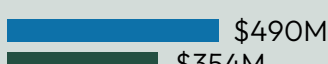

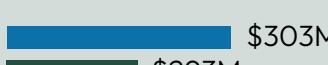
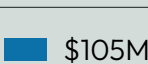


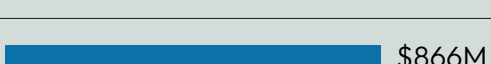
Application security accounted for 25%+ of all angel, seed, and early-stage funding

Application security received the most funding last year, despite falling 33% YoY in angel/seed capital from \$430M in 2022 to \$289M in 2023 and receding 59% YoY across early-stage rounds from \$1.2B to \$491M.

Angel/seed funding saw double-digit growth YoY between 2022 and 2023 in security operations (+16%), increasing from \$158M to \$184M, along with identity access management (+12%) from \$140M to \$156M. All other categories contracted, with data security (-58%) experiencing the steepest decline, down from \$258M to \$107M.

Early-stage funding fell further YoY from 2022 and 2023, down heavily across all but two categories. Security operations (-65%) fell from \$866M to \$306M, while data security (-57%) dropped from \$757M to \$327M, and endpoint security (-28%) shrunk from \$490M to \$354M. Identity access management (-3%) slipped slightly, down from \$303M to \$293M.

Despite 19% YoY growth in early-stage rounds, **network security companies raised the least funding across angel, seed, and early-stages last year**, echoing its decline from this year’s Top 10 List of security spending priorities.

	Angel/seed:	YoY %	Early-stage (Series A & B):	YoY %
Application security	 \$430M \$289M	-33%	 \$1.2B \$491M	-59%
Data security	 \$258M \$107M	-58%	 \$757M \$327M	-57%
Endpoint security	 \$161M \$122M	-24%	 \$490M \$354M	-28%
Identity & access	 \$140M \$156M	+12%	 \$303M \$293M	-3%
Network security	 \$105M \$88M	-16%	 \$199M \$237M	+19%
Security operations	 \$158M \$184M	+16%	 \$866M \$306M	-65%

■ 2022 ■ 2023

(Source: Pitchbook Emerging Tech Research)

Conclusion

There have been some new challenges facing CISOs in the last year. From a resourcing perspective, the macroeconomic headwinds in tech that security teams had previously been resilient to have impacted budget growth, while staffing remains a persistent obstacle.

While securing technology has always been an arms race, with AI it's moving at a new velocity.

Still, it's encouraging that even with slowing budget growth, CISOs are leading the charge to make sure their security posture is as robust as it can be in the face of increasing complexity.

CISOs are finding ways to invest in innovative security solutions that address the changing threat landscape.

As investors, we have a shared interest with CISOs in making sure security is keeping pace with emerging technologies. Despite the drop in venture funding, we are excited about the market opportunities we see in cybersecurity. We're particularly interested in cloud security solutions, application security solutions, and tools powered by AI/ML.

While this is the first year of slowed budget growth, the drop in funding and dearth of security talent may be the new normal. Security teams will continue to be creative and look to innovative solutions to bridge the gap.

Endnotes

1, 2. CrowdStrike, [2024 Cloud Risk Report](#): From Breakout to Breach in Under Three Minutes; Cloud Infrastructure Under Attack, February 2024

3, 4. IBM Security, [Cost of a Data Breach Report 2023](#), July 2023

5. ISC2, [2023 Cybersecurity Workforce Study](#): How the Economy, Skills Gap and Artificial Intelligence are Challenging the Global Cybersecurity Workforce, October 2023

6. Catherine Stupp, James Rundle, [Cyber Leaders With Tight Budgets Still Must Secure AI, Cloud](#), The Wall Street Journal, January 2024

7, 8. Pitchbook, [Emerging Tech Research: Q4 2023 Information Security Report](#): VC trends and emerging opportunities, January 2024

Methodology

Scale Venture Partners commissioned Everclear Marketing and Osterman Research to conduct a survey of 300 security leaders in the United States who are responsible for buying decisions, the success of security deployments, or the overall security of the company. The web-based survey was fielded March 4-15, 2024, focused on the 12 months prior and 12 months upcoming, with a +/- 3.395% margin of error.

You can view Scale's past Cybersecurity Perspectives reports here:

[2023](#) | [2022](#) | [2021](#) | [2020](#) | [2019](#) | [2018](#) | [2017](#)

SCALE

scalevp.com