Cybersecurity Perspectives 2025

Keeping pace with the threat velocity of AI-driven cyber attacks

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

Over the last 12 months, there is one word that best describes the cyber threat landscape: velocity.

The speed of cyber threats created an urgent and pressing need for CISOs to respond, as cybercriminals continued to leverage generative AI to increase the volume and velocity of attacks, leaving enterprises on the defense against increased threat activity.

> In response, enterprises are prioritizing strategies to respond to threats, invest in security tools, mitigate the cybersecurity skills gap and integrate AI responsibly.

In fact, threat actors are now breaking out into networks faster than ever, according to CrowdStrike,[1] with adversaries moving laterally across a compromised network in 48 minutes on average, with 51 seconds breaking the all-time low record as the fastest time ever recorded.

> Security leaders expressed serious concerns that "if we fail [to adapt] ... the losses will be immeasurable."

High-profile breaches and zero-day exploits continue to dominate headlines, while enterprise security teams remain under-resourced from a team, technology and budget standpoint. This forces organizations to make strategic investments to combat the speed, scale and complexity of attacks. The good news? It seems to be working.

AI is both cybersecurity's biggest threat and most promising savior. Three of the top six challenges related to AI this year, lead by AI-driven cyber attacks (#1), in addition to AI defenses (#5) and generative AI (#6). On the defense side, 77% of CISOs were confident in the future potential of AI to improve their security posture this year, with 75% of firms expressing interest in leveraging AI agents to automate SOC investigations using AI agents by triaging large volumes of security alerts.

As AI dominates both sides of the threat landscape, Scale Venture Partners conducts ongoing research to understand CISO challenges and evolving security solutions. Now in its 12th year, this year's report consolidates perspectives from CISOs, CIOs, VPs, directors, and IT managers.

* 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

Cybersecurity effectiveness improves for first time in three years

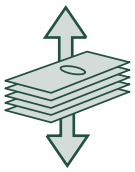
The average effectiveness of cybersecurity protections improved for the first time in three years, increasing to 61% efficacy this year from 48% in 2023. Encouragingly, 70% of security leaders were most protected against general phishing attacks, with only 28% of firms reporting compromise.

AI-driven cyber attacks top ransomware as unaddressed challenge

Three of the top six unaddressed security challenges related to some form of AI this year, while ransomware (#3) fell from first place behind the evolving threat landscape (#2). 50% of firms suffered an attack against a cloud service last year, while 45% of firms experienced a data breach.

CISOs prioritized application security and data privacy

CISO security strategies were influenced by concerns about new and emerging data privacy requirements — as well as third-party data breaches. Top priorities were application security (1st), data privacy (2nd), and threat intelligence (3rd), while network security returned to the list in 4th this year.



Security budgets bounced back to double-digit growth

Security budgets showed double-digit growth. Mid-sized security budgets increased 11% YoY, while enterprise security budgets grew 17% YoY. The top two threats from 2024 drove security budgets for 2025, with cloud security (12%) and data security (10%) ranking 1st and 2nd in this year's budget priorities.

Market gaps found in IAM, API security, and application security

Market opportunities were uncovered in identity access management, API security, and application security, with a 15%+ delta between "satisfaction" and "importance." Nearly half of firms (49%) intended to build in-house tools. Of those, 26% intended to build cloud infrastructure security solutions.

Where the threats are

45% of firms suffered data breaches from ransomware, cloud service attacks and more

Two of the most common incidents were cloud service attacks (#1) and ransomware attacks, either by encrypting data or holding it for ransom (#3).

50% of organizations experienced cyber attacks against a cloud service last year, up from 37% of firms the previous year. Data breaches affected 45% of firms, up from 31% in 2023 and 22% in 2022.

With AI models becoming more entrenched within every corner of the enterprise, 20% of organizations reported that AI models in their firm were compromised by threat actors.

Nearly one-third of all enterprises were compromised by third parties (32%), employee credentials (28%), or software supply chain vulnerabilities (28%), where poor partner security controls result in unwelcome incidents.

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

50% Cloud service attacked

45% Data breach of sensitive information

32% Ransomware encrypted our data

32% Compromised by attack on 3rd party

28% Compromised employee credentials

28% Compromised by software supply chain vulnerability

20% Employee stole our information

20% AI model was compromised by threat actors

Identity-based attacks and vulnerabilities still dominate

Credential theft contributed to 35% of cloud service attacks, with threat actors targeting "identity-based" attack vectors to gain deep access to enterprise IT environments, according to Crowdstrike.[2]

In 52% of all incidents, attackers exploited unpatched software vulnerabilities to gain "initial access," according to Crowdstrike.[3]

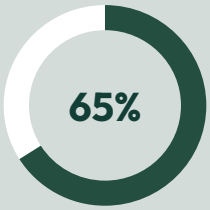
Additionally, ransom demands ranged from $3 to $1.14 million, with a median loss of $46,000 per incident, according to Verizon,[4] while extortion attacks (without ransomware) account for 9% of breaches.

52%

of all vulnerabilities were from attackers exploiting unpatched software.[5]

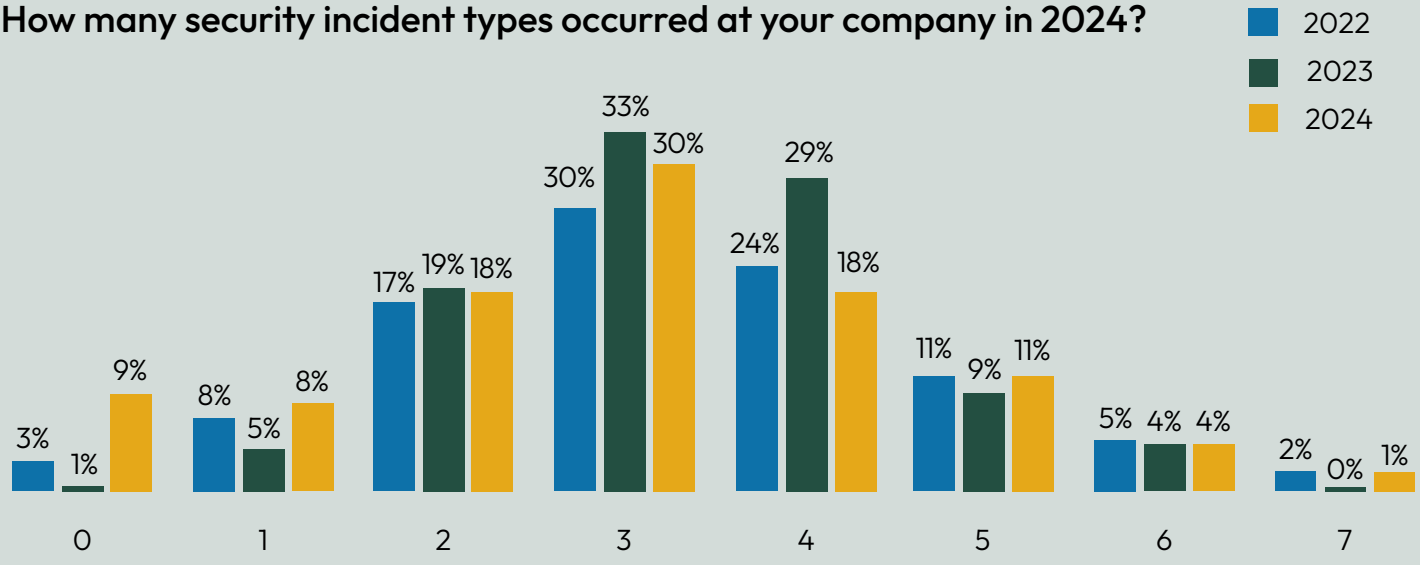
CISOs reported decrease in number of security incident types

9% of firms reported no security incidents in 2024 — up from 1% in 2023 — while the number of enterprises reporting three or four incidents decreased from 76% in 2023 to 65% in 2024, an overall positive improvement for enterprise security leaders and SOC managers. Companies with one incident type increased slightly from 5% previously to 8% last year, while two incident types fell from 19% to 18%.



Experienced **three or more types** of security incidents

How many security incident types occurred at your company in 2024?

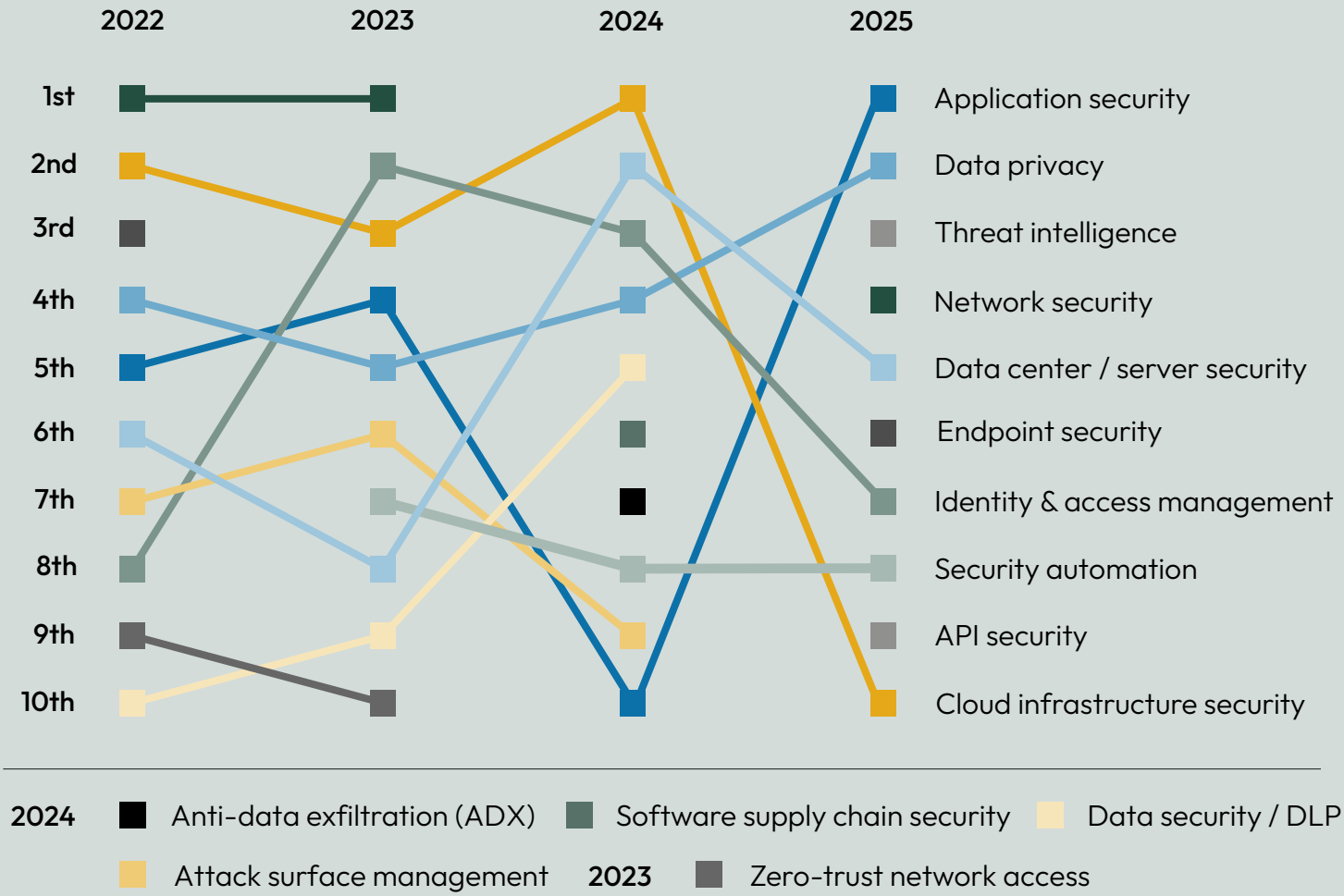


How enterprises are responding

Application security is the top priority for first time, while data privacy jumps to 2nd

Application security, data privacy, and threat intelligence topped this year's list. Cloud infrastructure security dropped from 1st place to 10th place, falling from its previous low of 3rd place in 2023. Network security ranked 4th this year after failing to make the list last year, while endpoint security returned to 6th place, presumably in response to the widespread devastation of the global Crowdstrike outage, which crashed 8.5 million Microsoft Windows operating systems worldwide.[6]

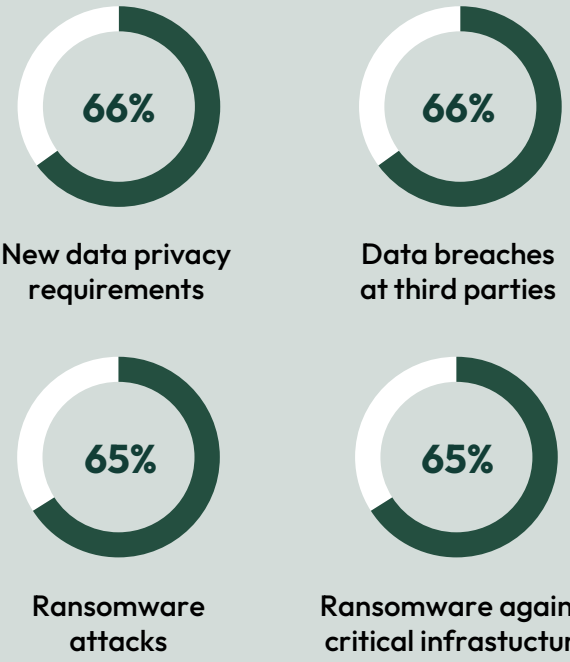
What are your top investment priorities for cybersecurity technologies and strategies?



Data protection drives CISO strategies

Concerns about new and emerging data privacy requirements — as well as third-party data breaches — influenced 66% of CISO cybersecurity strategies this year, while general ransomware attacks and ransomware attacks against critical infrastructure were close behind at 65%.

According to enterprise security leaders, two cybersecurity trends increased YoY over the last three years: ransomware against critical infrastructure (66%) and software supply chain attacks (64%).



The top 3 barriers decreased and top 3 priorities increased YoY between 2023 to 2024

In an environment where CISOs need to increasingly do more with less, the top three barriers to achieving their desired security posture were not enough security personnel (45%), too much manual labor (41%), and too many alerts/false positives (40%). Given this disparity, firms are leveraging AI to automate SOC investigations, for example, "AI analysts can cleanly mirror the workflow and thinking of the highest-performing SOC Analysts," according to Scale Venture Partners.[7] As AI adoption spreads, protecting AI/ML models and data pipelines (77%) ranked 2nd place in strategic priorities.

Resource gaps: people

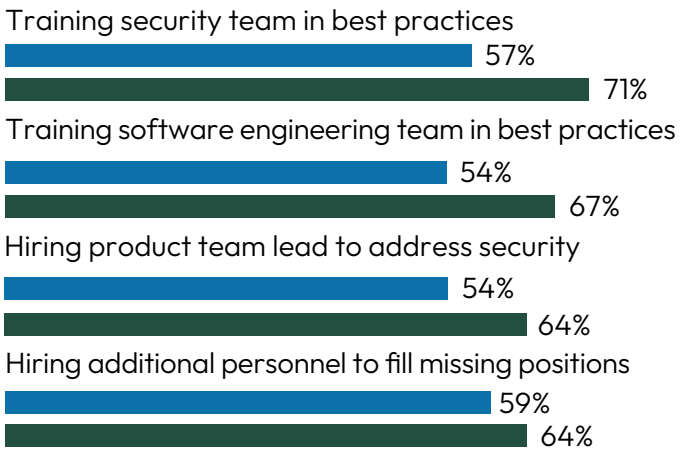
Cybersecurity skills gap widens 19% YoY as CISOs focus on training existing team

The cybersecurity skills gap continues to grow more severe each year, with a global staffing shortage of 4.8 million professionals — a 19% YoY increase — according to ISC2.[8]

71% of security leaders plan to train existing security team members in best practices over the next 12 months as their top priority.

67% plan to train software engineering teams to address application vulnerabilities hidden within source code repositories or open-source software libraries.

Security team changes: 2024 2025

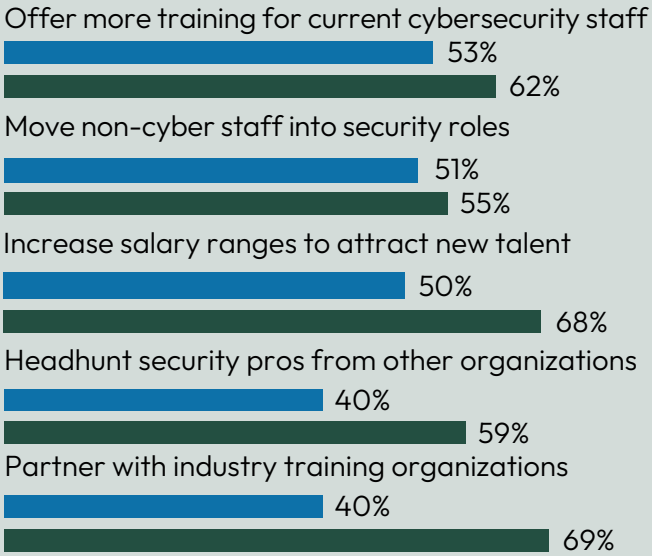


CISOs train existing staff vs. hiring

Nearly 70% of security leaders believe the most effective strategies for addressing the cybersecurity skills gap are to increase the salary range for cybersecurity roles and partner with industry training organizations, yet 50% or less of firms actually prioritized these approaches to attract new talent.

Without enough budget to hire new team members — or in many cases retain existing talent — more than 50% of firms sought to train existing security staff and non-cyber team members to fill empty roles.

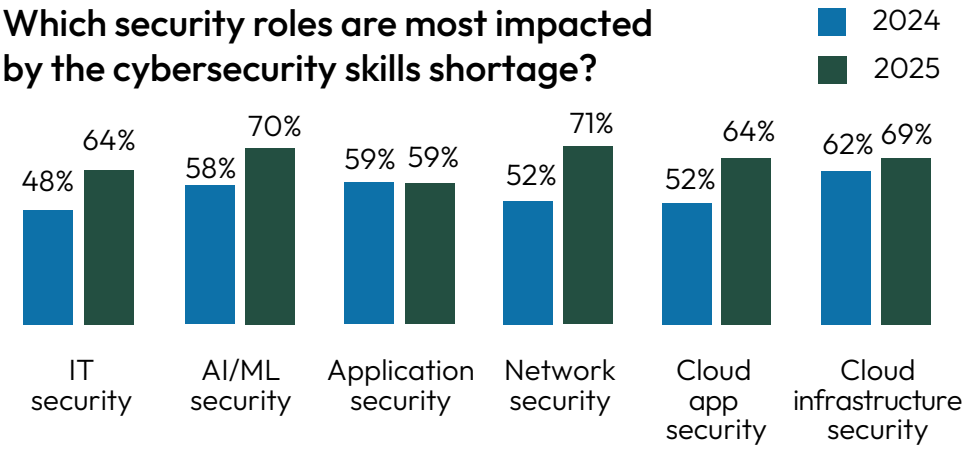
"Priority" vs. "effectiveness" of strategies to address the cybersecurity skills gap:



66% of security leaders struggle to hire for skilled cyber roles

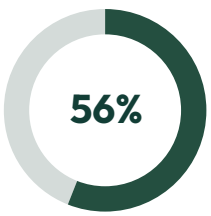
71% of enterprises had difficulty hiring and retaining network security roles, followed by 70% of firms seeking AI/ML security candidates. The biggest increase in demand between last year and this year were for IT security roles (64%) and cloud application security roles (64%). Application security roles (59%) showed no increase in demand YoY.

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

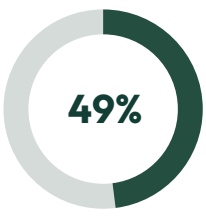


Cybersecurity turnover doubles as hiring and retention worsen

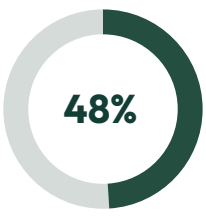
56% of security leaders expected cybersecurity team members to depart due to extreme workloads and burnout. The number of companies reporting turnover doubled since last year, increasing from 12% in 2023 to 25% in 2024. Nearly 50% of CISOs expected staff members to depart due to Return to Office (RTO) mandates or did not have the ability to pay enough salary to attract new professionals.



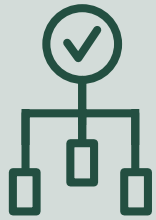
Staff departures due to extreme workloads



Staff departures due to hybrid/remote work policies



Inability to pay enough salary to attract new staff



C-Suite support:

81%

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

Cybersecurity turnover:

25%

of security teams experienced turnover within the last 12 months

Resource gaps: technology

Cybersecurity efficacy improves against common threats for first time in three years

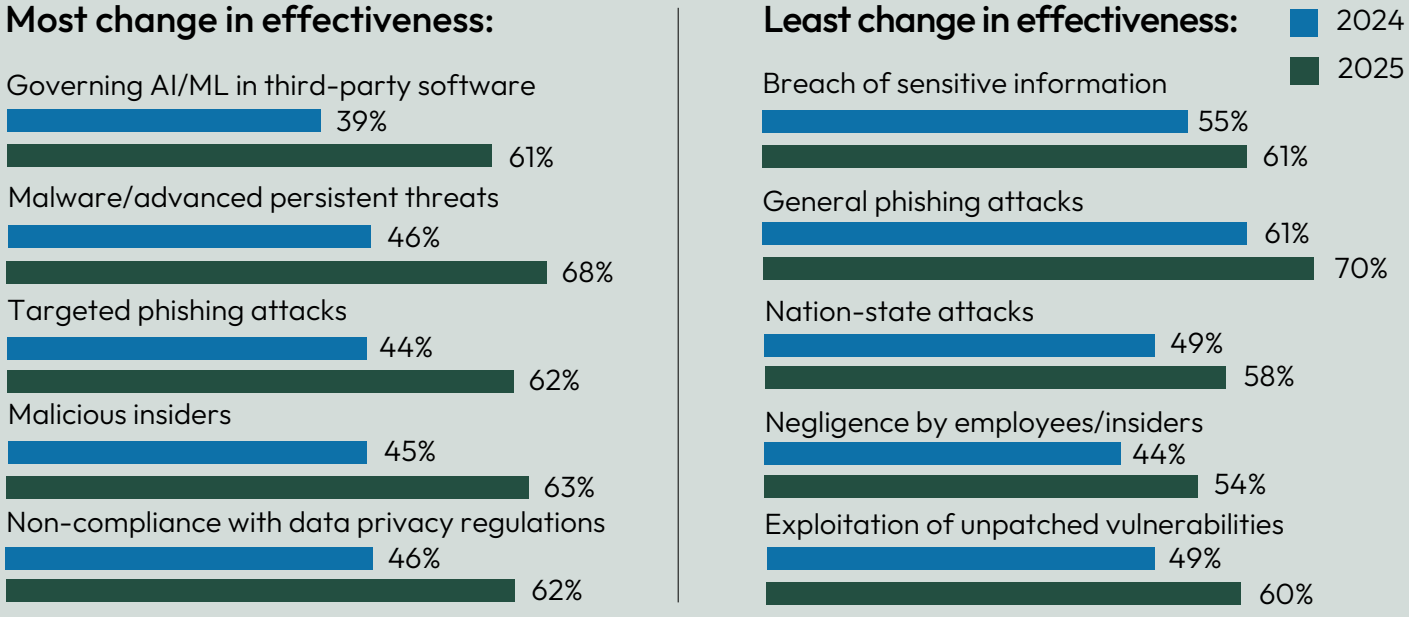
The average effectiveness of cybersecurity protections improved for the first time in three years, increasing from 48% efficacy in the 2022 and 2024 surveys to 61% in the 2025 survey.

Cybersecurity effectiveness reportedly increased the most in governing AI/ML in third-party software (+22%), malware/ advanced persistent threats (+22%), and targeted phishing attacks (+18%).

Cybersecurity protections made incremental improvements against breach of sensitive information (+6%), general phishing attacks (+9%), and nation-state attacks (+9%), with all three greater than 58% overall effectiveness.

Encouragingly, 70% of security leaders believed they were most protected against general phishing attacks, with only 28% of firms reporting they had lost compromised employee credentials to phishing attacks.

How "effective" or "extremely effective" are your current cybersecurity protections?



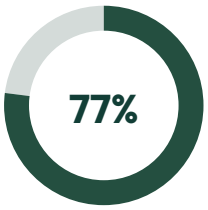
AI-driven cyberattacks top unaddressed challenges

Three of the top six challenges were related to AI this year, led by AI-driven cyber attacks (#1), in addition to AI defenses (#5) and generative AI (#6). Ransomware (#3) fell from first place last year behind the evolving threat landscape (#2), as security leaders expressed serious concerns that "if we fail [to adapt] ... the losses will be immeasurable."

Unaddressed challenges in security leaders' own words	
AI-driven attacks	"AI automates phishing, deepfakes, and exploits."
Threat landscape	"New threats emerge faster than we can adapt."
Ransomware	"Hackers encrypt data and leak sensitive info."
Cyber skills gap	"Not enough qualified staff to maintain security."

AI/ML security use cases see widespread adoption

77% of CISOs believe protecting AI/ML models and data pipelines are "important" to improve their security posture by 2025, up from 55% last year. 75% of firms expressed interest in leveraging AI to automate SOC investigations using AI agents to triage large volumes of security alerts to prevent security incidents. Another 75% were interested in leveraging more security tools that used AI/ML, with 65% seeking to govern AI/ML capabilities in third-party software.



Protecting AI/ML models and data pipelines

Leveraging AI to automate SOC investigations

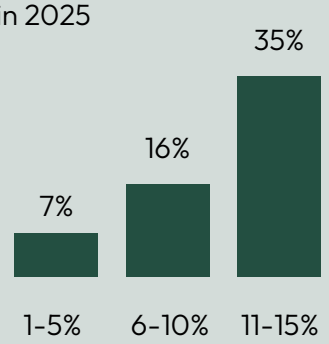
Leveraging more security tools that use AI/ML

Security tools:

43%

expected their security stack to change 16% or more

% Change in Security Stack in 2025



81%

want to deploy more security tools over the next 12 months

+12

Average # of new tools budgeted for this year

+21

Average # of new tools preferred to deploy

Resource gaps: budget

Security budgets experience double-digit growth for large and mid-sized enterprises

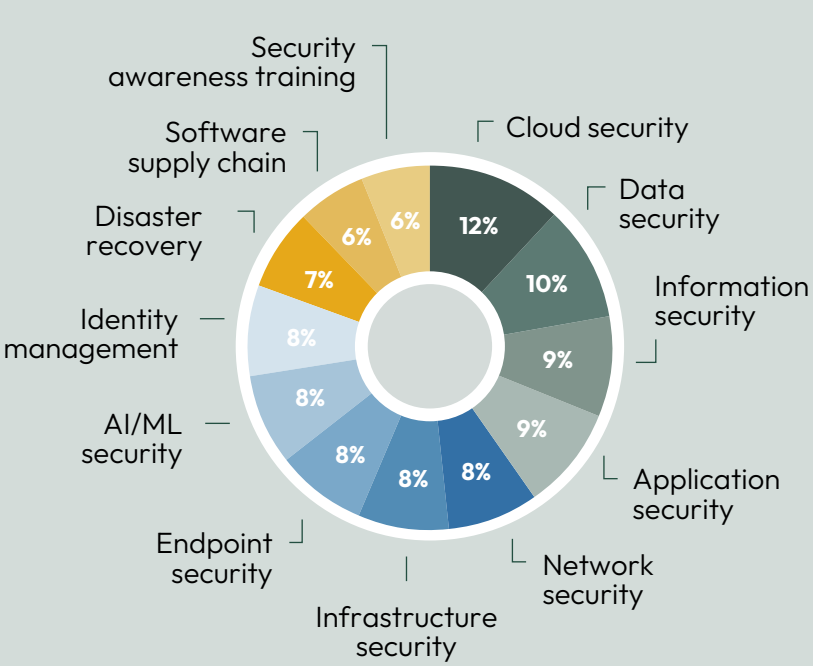
Security budgets reverted to the mean once again with double digit growth for both large (+17% YoY) and mid-size (+11% YoY) enterprises, after a year of declining budget growth for mid-size enterprises previously.

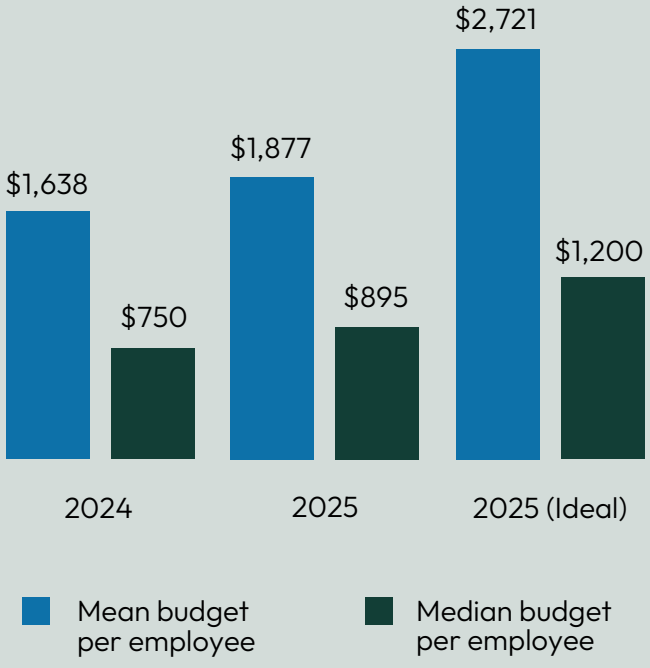
The top two threats from 2024 drove security budgets for 2025, with cloud security (12%) and data security (10%) ranking 1st and 2nd in this year's budget priorities. Cloud security was the #1 spending priority with 2% more budget allocation than data security.

Although budget allocations remain fairly constant between categories year-over-year, security leaders make subtle adjustments based on their priorities in a given year. For example, application security moved up from 6th to 4th place budget-wise.

As new threats emerge, however, CISOs "are wary of paying for more protection than they need," according to The Wall Street Journal,[9] because "there is no dollar amount ... that will eliminate every threat 100% of the time."

What is your total budget and category allocations for security solutions in 2025?





Cybersecurity spending reflects necessities vs. ideal budgets

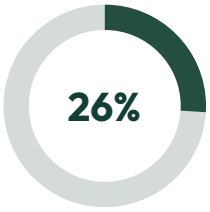
CISOs would have asked for 45% more budget than approved in 2025, compared with 52% more budget than approved in 2024. Under ideal budget scenarios, security leaders would have allocated more budget toward data security (+7%), application security (+7%), AI/ML security (+6%), and disaster recovery (+5%).

However, they would have allocated less budget for endpoint security (-15%), as well as software supply chain security (-9%), highlighting the trade-offs security leaders make to defend against new cyberattacks.

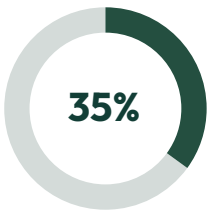
More budget is Ideal for 2025	**Less budget** is Ideal for 2025
Data security (+7%)	Endpoint security (-15%)
Application security (+7%)	Software supply chain security (-9%)
AI/ML security (+6%)	Infrastructure security (-4%)
Disaster recovery (+5%)	Information security (-3%)
Identity management (+2%)	Security awareness training (-2%)

CISOs invest in innovation to fight emerging security threats

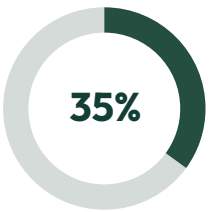
Enterprise security departments allocated 35% more budget YoY for new, innovative, and experimental security solutions this year. In order "to keep pace with evolving cyber threats and more sophisticated attackers," companies are investing in technologies such as AI/ML, cloud security, and data protection to defend enterprise assets.



Percentage of 2024 total budget for emerging solutions



Percentage of 2025 total budget for emerging solutions

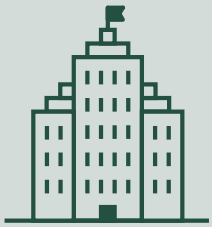


Year-over-Year budget growth for emerging solutions

Mid-sized Enterprises
(500-999 employees)

11%
Year-over-Year Budget Growth

$40K-$13M
Budget Range



Large Enterprises
(1,000+ employees)

17%
Year-over-Year Budget Growth

$45K-$310M
Budget Range

Market opportunities

The biggest market gaps exist in identity (IAM), API security, and application security

An increasing number of CISOs and security leaders were unable to find the right cybersecurity tools in the market to address their needs for the fourth year in a row, up 58% YoY from 31% in 2022 to 49% in 2025.

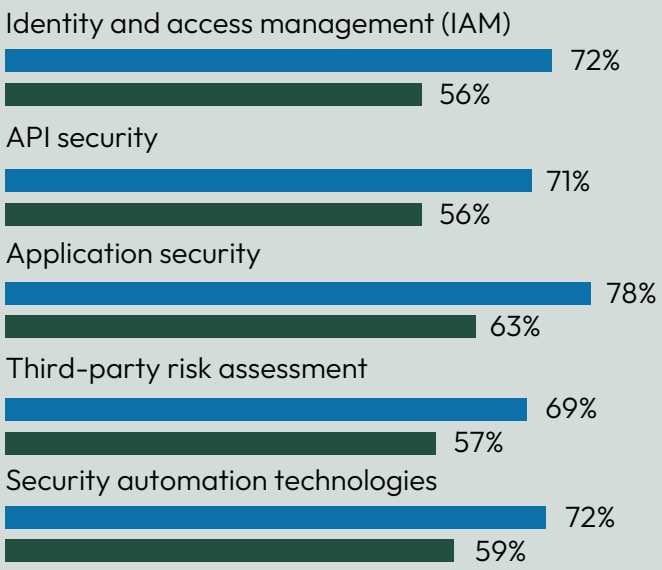
The biggest market gaps in the "importance" vs. "satisfaction" of commercially-available cybersecurity tools were found in identity and access management (22%), API security (21%), and application security (20%).

The smallest market gaps — with a delta of 10% or less — were found in external surface management (3%), zero trust network access (7%), data loss protection (8%), CI/CD security (10%), and identity posture assessment (10%).

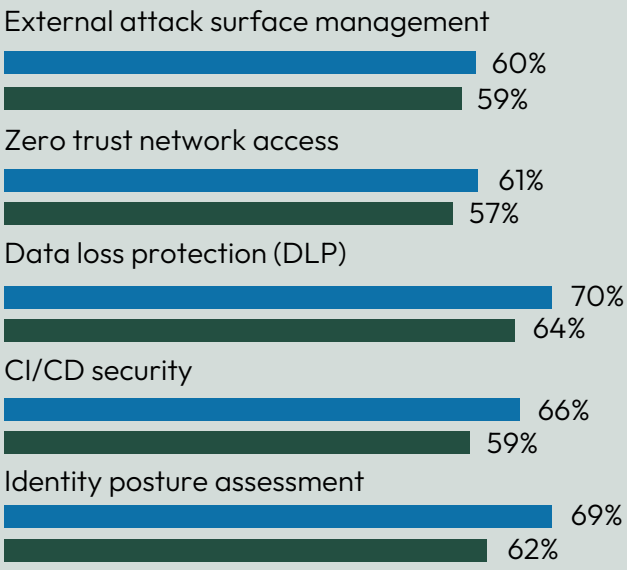
But adding more tools to the security stack might not be the answer, as 46% of security leaders are concerned that "only adds alerts, not actionable insight we can use to strengthen our security posture."

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

Biggest "market gap" for security tools:

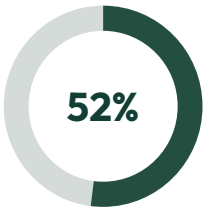


Smallest "market gap" for security tools:



AI again tops list of emerging innovations with greatest potential

More than 50% of security leaders have faith that AI will be the emerging innovation to save them, compared with zero trust network access (4%), biometric authentication (3%), and quantum-safe cryptography (2%). CISOs were confident in the future potential of AI to "enable real-time threat detection, automate response systems, and improve anomaly detection, allowing for proactive defense against cyberattacks."



Believe AI will offer the greatest potential boost to their cybersecurity

Cloud infrastructure security tops list of solutions CISOs intend to build in-house

Nearly half of all enterprises (49%) intend to build in-house cybersecurity tools because commercially-available security tools do not currently meet the needs of security leaders.

Of those firms interested in building in-house tools, 69% were large enterprises with more than 1,000 employees and 31% were mid-sized companies with 500 to 999 employees.

CISOs were most likely to build in-house solutions for cloud infrastructure security (26%), data privacy (20%), threat intelligence (19%), and application security (19%).

Firms were least likely to build in-house tools for third-party risk assessment (8%), CI/CD security (8%), insider risk analytics (7%), and external attack surface management (7%).

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

26% Cloud infrastructure security

20% Data privacy

19% Threat intelligence

19% Application security

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

8% Third-party risk assessment

8% CI/CD Security

7% Insider risk analytics

7% External attack surface management

Where the funding is

Cybersecurity investment increased 8.3%, driven by late stage and venture growth

The funding environment for cybersecurity showed signs of improvement last year, increasing to $13.1B from $9.6B in 2023, according to Pitchbook.[10]

Later stage funding (Series E, etc.) was responsible for an additional $1.4B in funding alone, a 48% YoY increase. Early-stage (Series A & B) and late stage (Series C & D) were relatively flat, while pre-seed and seed decreased 23% YoY from $1.3B to $1B.

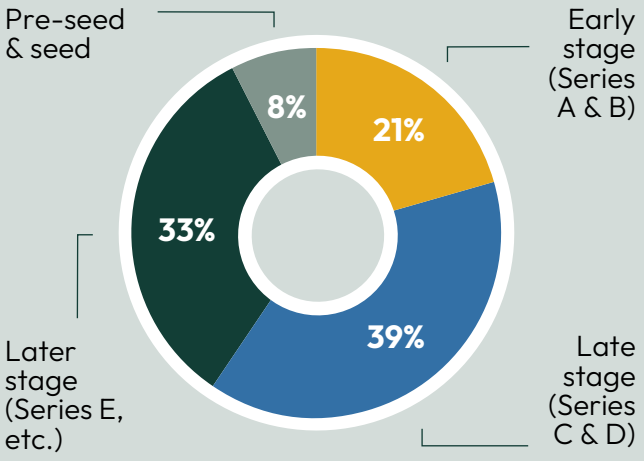
910 deals were done in 2024, down from 1,041 deals in 2023. Venture growth increased 6% YoY, "reflecting investor confidence in more mature cybersecurity companies over riskier early stage bets," according to Pitchbook.[11]

Cybersecurity exit value was the largest in three years at $13.7B, up 112% YoY since 2022. "The cybersecurity index returned 10%, trailing SaaS (17%) and AI (14%)," according to Morningstar.[12]

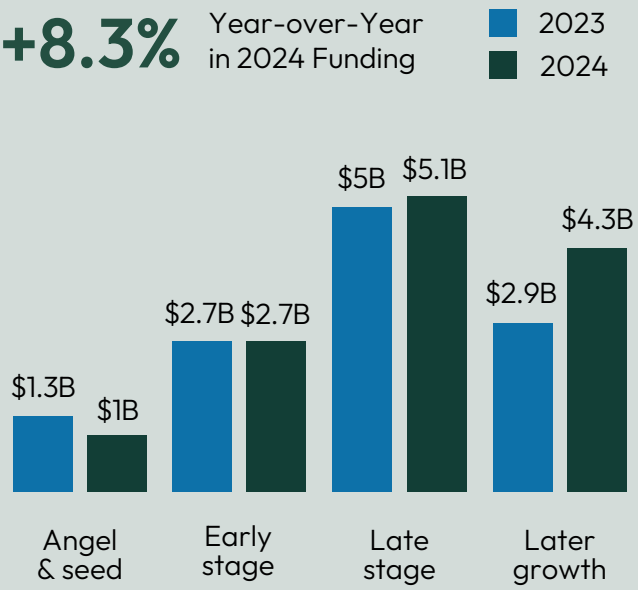
Global security investment by funding stage:

(Source: Pitchbook Emerging Tech Research)

$13.1B Global cybersecurity VC deal activity in 2024



+8.3% Year-over-Year in 2024 Funding



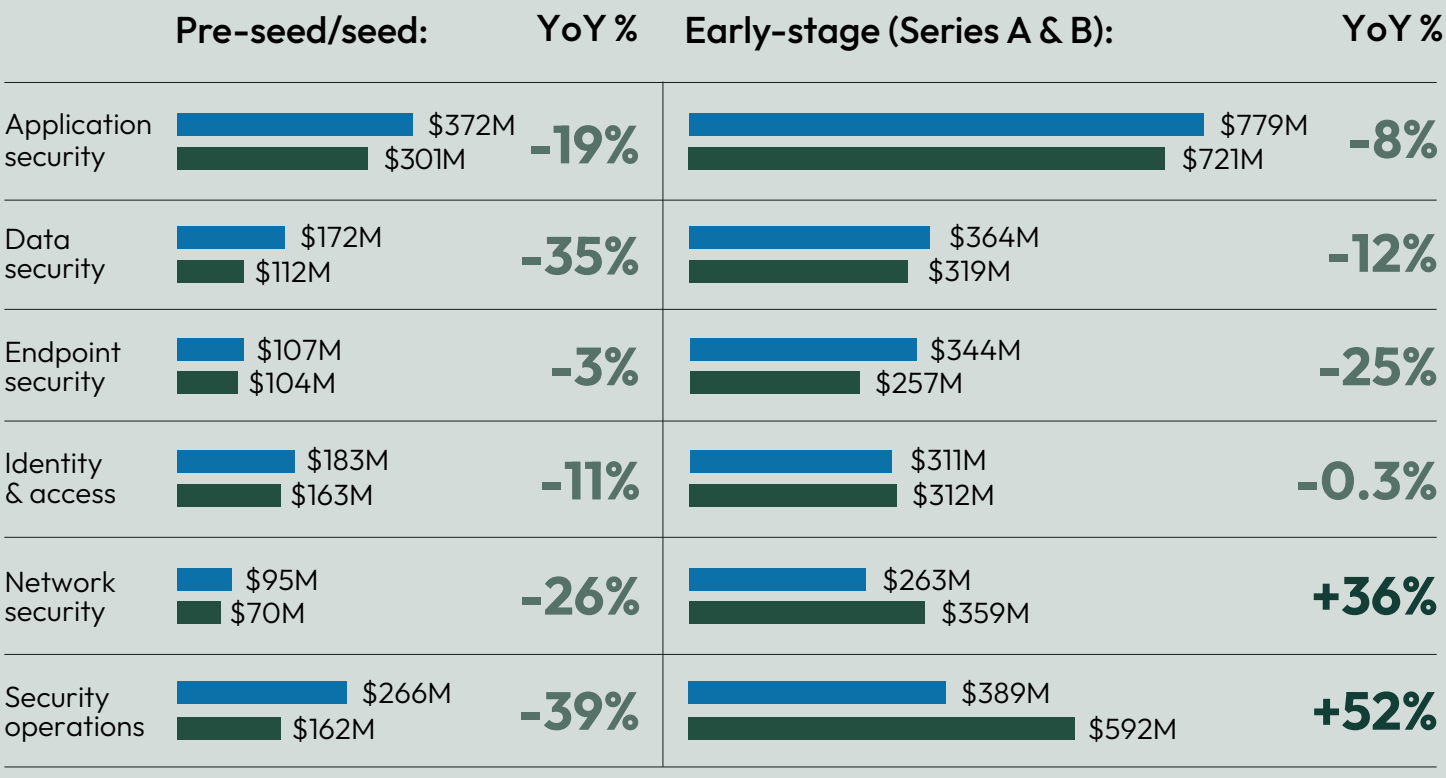
Application security and security operations were 50% of seed and early-stage funding

Application security again received the most funding across pre-seed, seed and early-stage, accounting for more than $1B in capital combined. Security operations ranked second with a combined $754M in funding across stages.

Pre-seed/seed funding saw double-digit declines at -24% YoY, down from $1.2B in 2023 to $912M in 2024. Every category contracted, led by security operations (-39%), data security (-35%), and network security (-26%), followed by application security (-19%), identity access management (-11%), and endpoint security (-2%).

Early-stage funding increased modestly 4% YoY, despite heavy gains in network security (36%) and security operations (52%). All other categories declined last year, led by endpoint security (-25%), data security (-12%) and application security (-8%), with identity and access management flat at (-0.3%).

Endpoint security received the least amount of funding across early stages with $361M, despite the number of breaches where endpoints were affected, while identity access management received more than $100M more at $457M in funding.



(Source: Pitchbook Emerging Tech Research)

Conclusion

Over the past year, security budgets and VC funding for security startups have increased. At the same time, CISOs have reported a decrease in the number of security incident types, and the average effectiveness of cybersecurity protections improved for the first time in three years.

> While we can't say to what degree it's causal, we see this as a positive signal for security innovation.

For the first time since 2021, budgets and cybersecurity protections are trending in a positive direction. CISOs are investing in external tools and building in-house, with innovation budgets up 35% YoY. Startups have an opportunity to run head-on at the threats facing most enterprises.

> More than 50% of security leaders have faith that AI will be the emerging innovation to save them.

At a high level, many of the big problems CISOs face are holding: the talent gap persists and AI will continue to act as an accelerant for bad actors. Of course, we're still facing an existential threat with AI. As the ever-changing threat landscape continues to evolve, the future of security depends on how fast AI advances on the defensive side.

Endnotes

1, 2, 3, 6. CrowdStrike, 2025 Global Threat Report: The Rise of the Enterprising Adversary, February 2025

4. Verizon, 2024 Data Breach Investigations Report: May 2024

7. Shayan Shafii, Ariel Tseitlin, AI SOC Analysts: LLMs find a home in the security org, Scale Venture Partners, September 2024

8. ISC2, 2024 Cybersecurity Workforce Study: Employers Must Act as Cybersecurity Workforce Growth Stalls and Skills Gaps Widen, September 2024

9. Oliver Staley, Cybersecurity Budgets Should Reflect Business Risks, Corporate Leaders Feel, The Wall Street Journal, February 2025

10, 11, 12. Pitchbook, Emerging Tech Research: Q4 2024 Information Security Report: VC trends and emerging opportunities, March 2025

Methodology

Scale Venture Partners commissioned Everclear Marketing and Osterman Research to conduct a survey of 301 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 January 31, 2025 through February 7, 2025 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:

2025 | 2024 | 2023 | 2022 | 2021 | 2020 | 2019 | 2018 | 2017

SCALE

scalevp.com