Cybersecurity Perspectives 2023

A Macro Look at How
Enterprise Security Is Evolving

SCALE

Table of Contents

Introduction

CISOs, security analysts, and their teams have been navigating rising security incidents, talent shortages, and the increasing sophistication of attacks over the last several years.

Meanwhile, geopolitical tensions are high, with a weakening social fabric, disinformation, and economic anxiety.[1] All of these factors translate into heightened on-the-ground pressures.

To help CISOs strengthen their footing, Scale Venture Partners conducts ongoing research to understand the challenges CISOs are facing and how solutions are evolving. Now in its 10th year, this year's report consolidates perspectives from CISOs, CIOs, VPs, directors, and IT managers.

Our research found that cybersecurity protections that were effective against cyber threats in 2022 have lost efficacy due to new attack mechanisms.

> The overarching theme is a drop in efficiency despite an increase in effort, with even more challenges in 2024.

Identity access management (IAM) also increased in importance for security leaders, as enterprises continue the journey to the cloud and employees login to multiple cloud services beyond the traditional perimeter. This urgency reflects an increase in attacks, as adversaries used valid accounts to gain initial access in 43% of cloud intrusions last year, according to CrowdStrike.[2]

> Security leaders ranked IAM as their 2nd top priority in this year's survey, rising dramatically from 8th last year.

Persistent talent shortages also create bottlenecks for security leaders to focus on beyond alerts and tools. As a result, security leaders are turning to automation — and AI in particular — to strengthen their security postures.

Despite these measures, security programs are struggling with resource constraints. Even though enterprise security leaders increased their budgets for emerging security solutions by 18% in 2023, this number was down from a 27% increase from the year prior.

Keep reading for a closer, more nuanced view of these dynamics.

* Note: Unless specifically documented, all data sources are from Scale Venture Partners' primary survey research.

Key Findings

Enterprises Are Experiencing More Security Incidents

71% of organizations experienced three or more types of security incidents, a 51% increase from last year's survey. Although successful ransomware attacks and data breach attempts fell by 30%, 34% of firms suffered software supply chain compromises.

CISOs Struggle With Not Enough People; Too Many Alerts & Tools

83% of firms are enforcing existing security policies more strictly to address these issues. People issues were 4 of the Top 10 unaddressed challenges, including the cybersecurity skills gap (2nd), employee threats (4th), remote work (7th), and employee training (8th).

AI/ML Presents Opportunities and Threats for Security Teams

79% of executives believe AI/ML will be "important" or "extremely important" to improve their security posture by 2024. 68% were also worried that employees would upload sensitive data to ChatGPT and 49% that threat actors would poison AI/ML models.

Security Budgets Remained Resilient

Security budgets increased 20% on average at large enterprises, while only 5% at mid-sized enterprises. Data, cloud, and application security were the top spending priorities. Budgets for emerging security solutions increased by 18% overall this year, down from a 27% increase last year.

Cloud and Software Security Solutions Perceived as Market Gaps

Security leaders reported a 45%+ delta between "satisfaction" and "importance" for cloud application and CI/CD security solutions, with 33% building in-house cloud application security solutions, 4% software supply chain security, and 2% CI/CD security.

Where the Threats Are

Cloud Service and Third-Party Attacks Remain the Most Common Security Incidents

Cloud service attacks were the most common, with 50% of organizations reporting at least one incident over the last 12 months. More cloud services were compromised due to an attack against a third party (43% this year versus 37% last year).

There was a 58% increase in the number of firms compromised by phishing attacks that resulted in stolen employee credentials.

Two new incident types were included in the 2023 survey: compromise through a software supply chain vulnerability and attack/compromise of an AI model.

Software supply chain compromises were the 4th most frequently occurring attack for 34% of firms, while 20% of companies faced an AI model attack or compromise incident within the last 12 months.

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

50%	Cloud service attacked
43%	Compromised by attack on 3rd party
41%	Phishing attack compromised credentials
34%	Compromised by software supply chain vulnerability
31%	Misconfigured cloud access rights led to data breach
30%	Employee stole our information
26%	Fined for data privacy non-compliance
25%	Ransomware encrypted our data

Ransomware Attacks and Data Breaches Declined

Ransomware attacks and data breaches both declined over the past 12 months — from 37% each during last year's survey period to 25% and 22% respectively — which is consistent with other research on the volume of attacks in 2022, according to Verizon.[3]

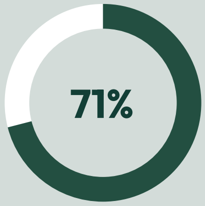
Despite the reported decrease, both threat types topped the list of trends that will drive cybersecurity strategy over the next 12 months, as ransomware attacks are on the rise again in 2023, according to IBM Security.[4]

30%

decline in ransomware attacks and data breach attempts from prior survey period.

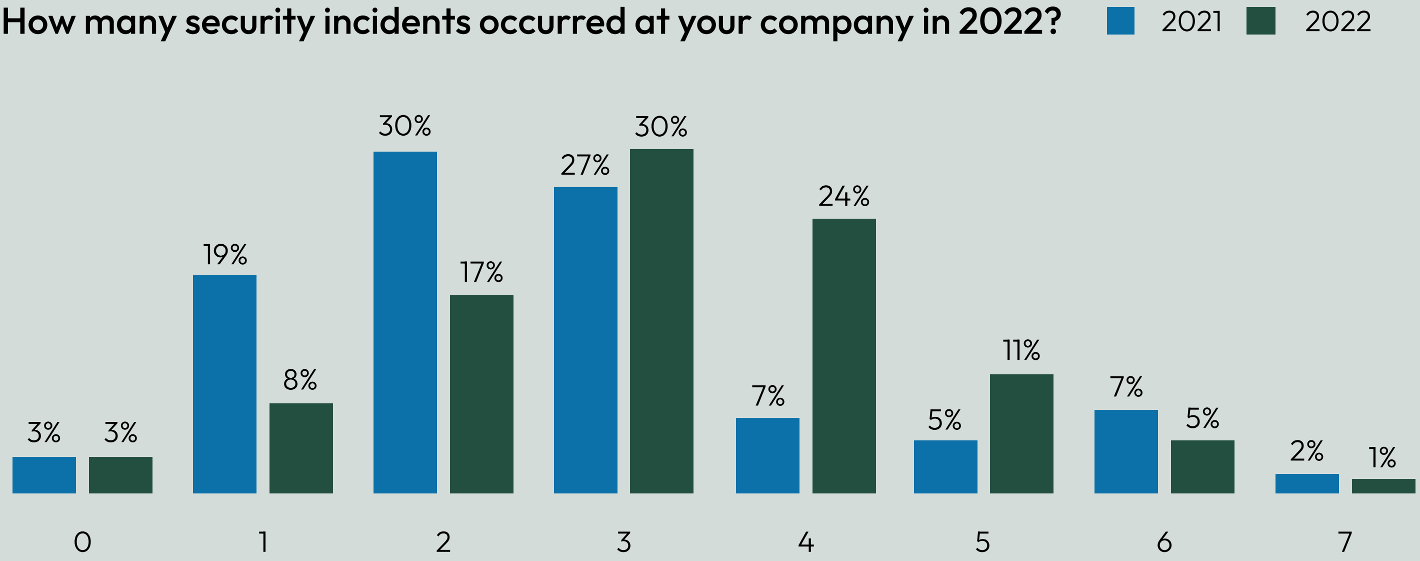
Organizations Experienced More Types of Security Incidents

71% of organizations experienced three or more types of security incidents during this year's survey period, compared with 48% for the same range of incidents in the prior year, a 51% increase year-over-year. Only 8% experienced one type of cyber incident, down significantly from 19% of companies in the previous year. The number of firms with two security incidents also dropped, from 30% to 17%.



Experienced
three or more types
of cyber incidents

How many security incidents occurred at your company in 2022?

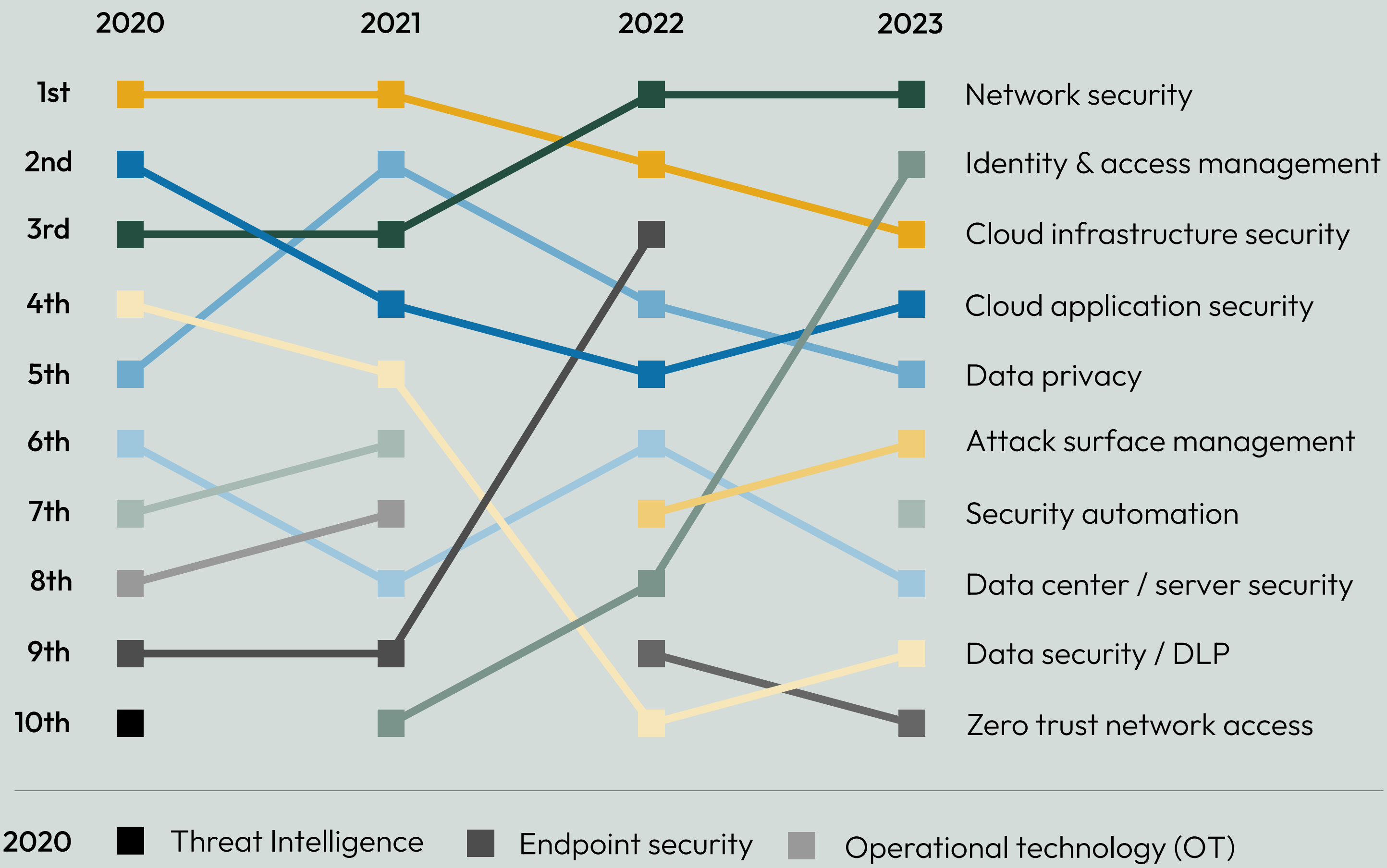


How Enterprises Are Responding

Network, IAM and Cloud are the Top 3 Cybersecurity Spending Priorities for 2023

Network security and cloud infrastructure security remain top three spending priorities for enterprise security leaders. **Identity and access management (IAM) leapt from 8th place to 2nd place this year**, which mirrors increasing market concerns around identity security in a multi-cloud world. External attack surface management moved up one place while security automation returned to the top 10 list of priorities after dropping off last year. No emerging technologies joined the list this year.

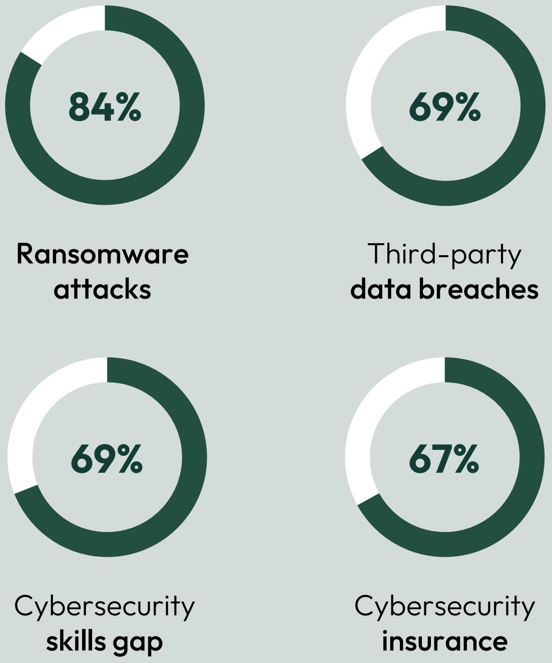
What are your top investment priorities for cybersecurity technologies and strategies?



Security Strategies Driven By Ransomware

Despite a reported 30% industry-wide decline, **84% of security leaders reported that ransomware attacks would have the biggest impact on their overall cybersecurity strategy** over the next 12 months.

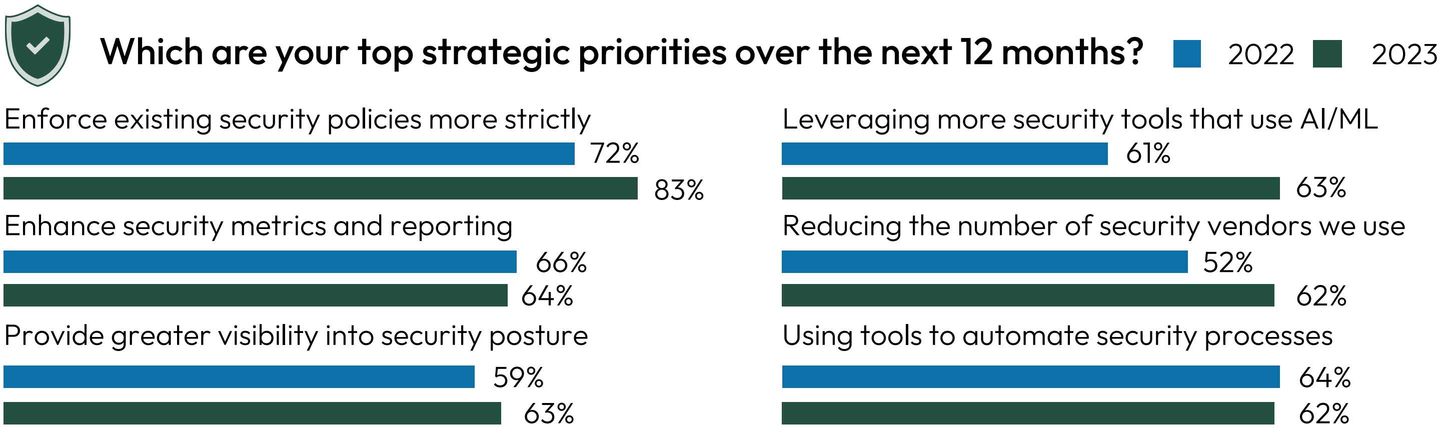
Enterprises were also concerned about third-party data breaches (69%), the cybersecurity skills gap (69%), and the increased cost of cybersecurity insurance (67%). These trends were followed closely by the weaponization of AI and machine learning (ML) for use in cyberattacks (65%).



Security Leaders Are Prioritizing Stricter Enforcement of Existing Policies

83% of firms intended to enforce existing security policies more strictly this year to address their security challenges, while 63% of organizations sought greater visibility and transparency into the state of security. Improving insight into the software supply chain was aso a high priority for security leaders (60%) as well as protecting AI/ML models and data pipelines (57%). **There was a nearly 20% year-over-year increase in the number of firms that decided to consolidate security vendors**. The importance of expanding accountability for security across the business dropped from 64% in 2021 to 54% this year, followed by re-organizing security teams at 53%.

Which are your top strategic priorities over the next 12 months?



Resource Gaps: People

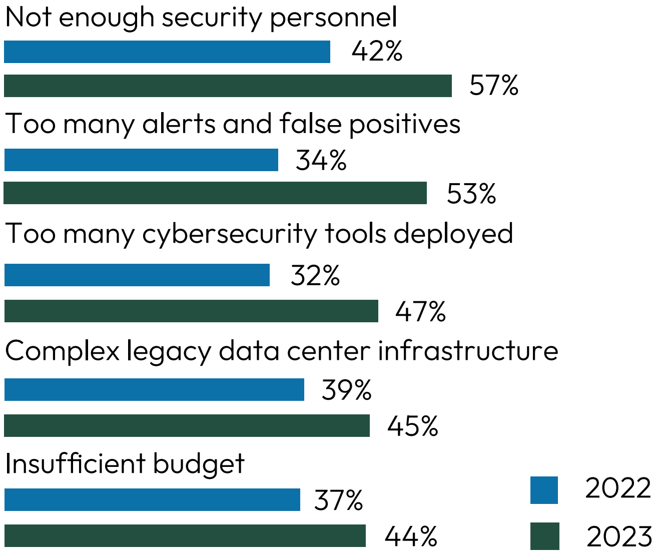
Cybersecurity Talent Remains Scarce

Enterprise security leaders are still struggling to attract, hire, and retain skilled cybersecurity professionals to respond to ongoing cyberattacks and recent threats.

In fact, **57% of firms indicated the biggest barrier to achieving their desired security posture was not enough security personnel**, up 42% from last year's survey period.

Security teams are also facing other barriers, including too many alerts, too many false positives, and too many tools to achieve their desired security posture.

What are the biggest barriers to achieve your security posture?

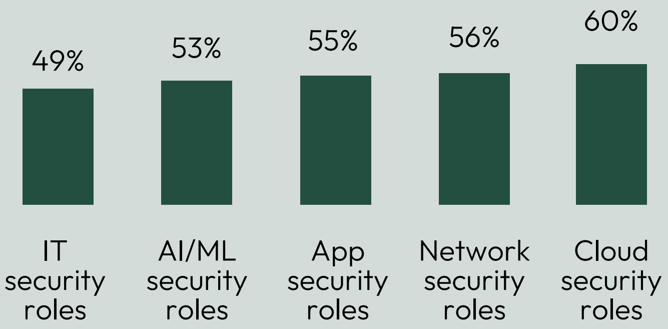


Cloud Security Roles Difficult to Fill

Sixty percent of security leaders considered cloud security the most difficult role to fill, with network security (56%) and application security roles (55%) not far behind.

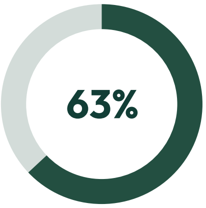
Talent shortages for these key roles may be a source of concern for security leaders who rated network security (71%) and cloud infrastructure security (70.6%) as their two most important security strategies.

How much of an impact is the cybersecurity skills shortage having on your ability to hire and retain the following types of cybersecurity staff?

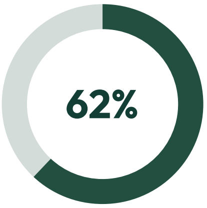


Security Leaders Want Tools to Amplify Cybersecurity Talent

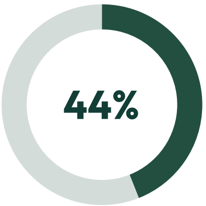
Over the next 12 months, security leaders are seeking to implement strategies to improve the effectiveness of their limited cybersecurity teams. **63% of companies reported an interest in leveraging security tools with AI and Machine Learning capabilities**, while 62% were interested in tools to automate manual security processes to identify, contain and remediate the most urgent cybersecurity threats.



Leverage more security tools that use **AI/ML**



Use tools to **automate security processes**



Too much **manual labor** associated with security

People Issues Were 4 of the Top 10 Unaddressed Challenges

Security leaders were given an opportunity to respond to an open-ended question about their single, greatest unaddressed challenge. Unsurprisingly, four of the top 10 challenges related to persistent people issues, including the cybersecurity skills gap (2nd), employee threats (4th), remote work (7th), and employee training (8th).

Unaddressed Challenges in Security Leaders' Own Words	
Cybersecurity skills gap	"Lack of skilled labor to prevent issues."
Employee threats	"Employees unaware of cyber risks."
Remote work	"Protecting remote workers."
Employee training	"Lack of security training for employees."

C-Suite Support:

74%

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

Malicious Insiders:

66%

of security leaders believed their security protections were **ineffective against malicious insiders**

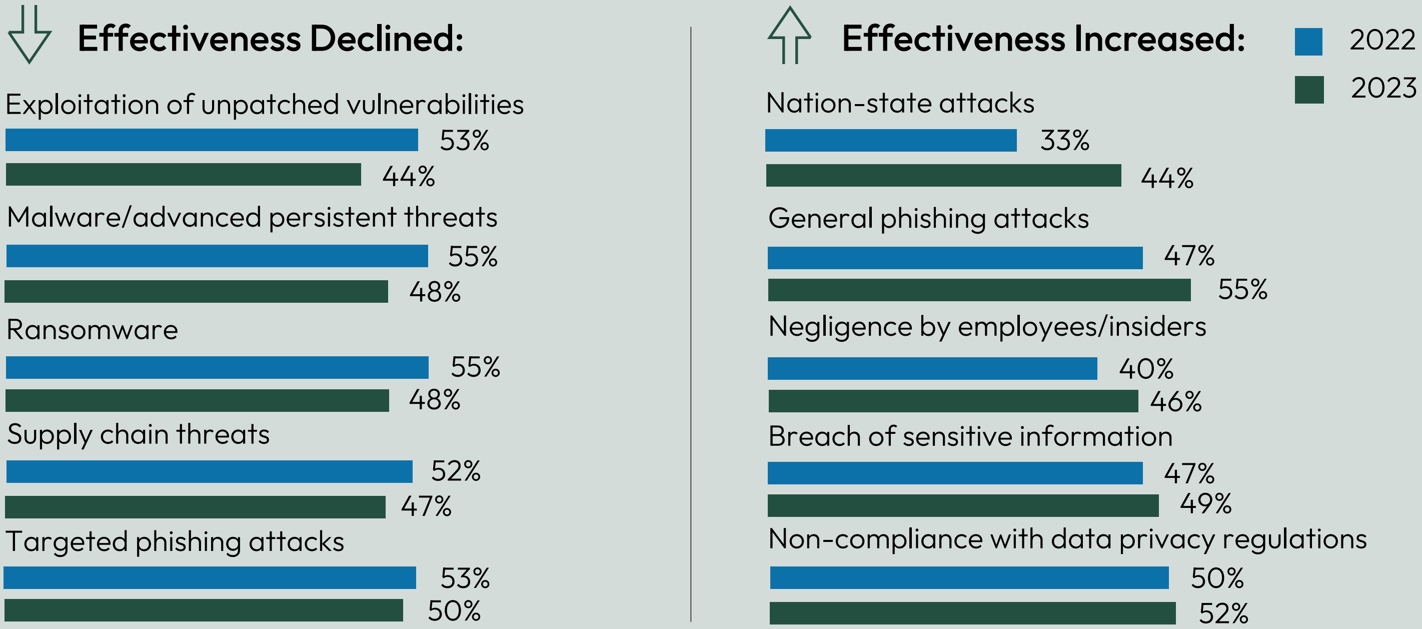
Resource Gaps: Technology

Cybersecurity Protections Are Losing Efficacy Against Common Cyber Attacks

Cybersecurity protections that were effective against cyber threats in the prior survey period have lost efficacy — as threat actors unleashed new attacks, unsettled AI/ML data models, and discovered new attack mechanisms. **Only 48% of security leaders indicated their cybersecurity defenses were effective against common security threats**. Threat actors haven't stood still over the past year and security leaders can't afford to do so either.

Compared to last year's survey, **security leaders reported a drop in the effectiveness of cybersecurity protections against several types of cyber attacks.** The most extreme decline related to the exploitation of unpatched vulnerabilities, which fell from 53% last year to 44% this year. Additional declines in protection between last year and this year were from malware / advanced persistent threats, ransomware, supply chain threats and targeted phishing attacks.

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



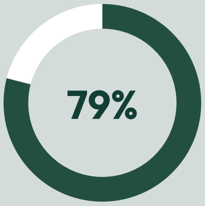
The Rise of AI/ML is a Potential Blessing and a Curse for Security Leaders

Four out of five security leaders indicated that AI and Machine Learning would be "important" or "extremely important" by 2024, up from one in five two years ago.

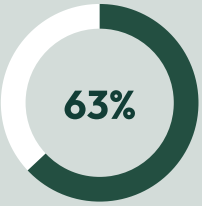
In regards to the use of AI/ML, 63% were concerned about the risk of employees uploading confidential company documents to services like ChatGPT.

62% of firms were worried about governing AI/ML models and 52% about observing and monitoring both malicious and non-malicious AI model drift.

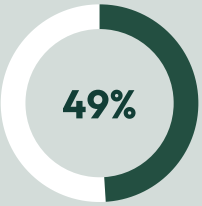
Less than 50% of companies were concerned about the risk of AI/ML models being poisoned by threat actors, despite more potential damage to the organization.



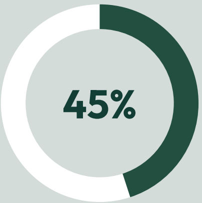
Believe AI/ML is important to **improve their security posture** by 2024



Concerned employees will **expose sensitive data** to ChatGPT



Concerned poisoned AI/ML models will **circumvent security**



Concerned poisoned AI/ML models will **alter business decisions**

Security Leaders Need More Tools, Want Less Vendors

88% of security leaders intended to deploy more security tools over the next 12 months, up from 64% in the previous year. On average, organizations allocated budget for four new tools. However, 37% of firms were unable to find the right cybersecurity solutions in the market to address their needs.

Although security leaders wanted more tools, **62% indicated they were interested in consolidating security vendors.** This disparity could indicate a desire to deploy integrated software platforms. The number of organizations that wanted fewer security tools over the next 12 months fell from 29% last year to 15% this year.

88%

want to **deploy more security tools** over the next 12 months

+4

Average # of new tools budgeted for this year

+9

Average # of new tools preferred to deploy

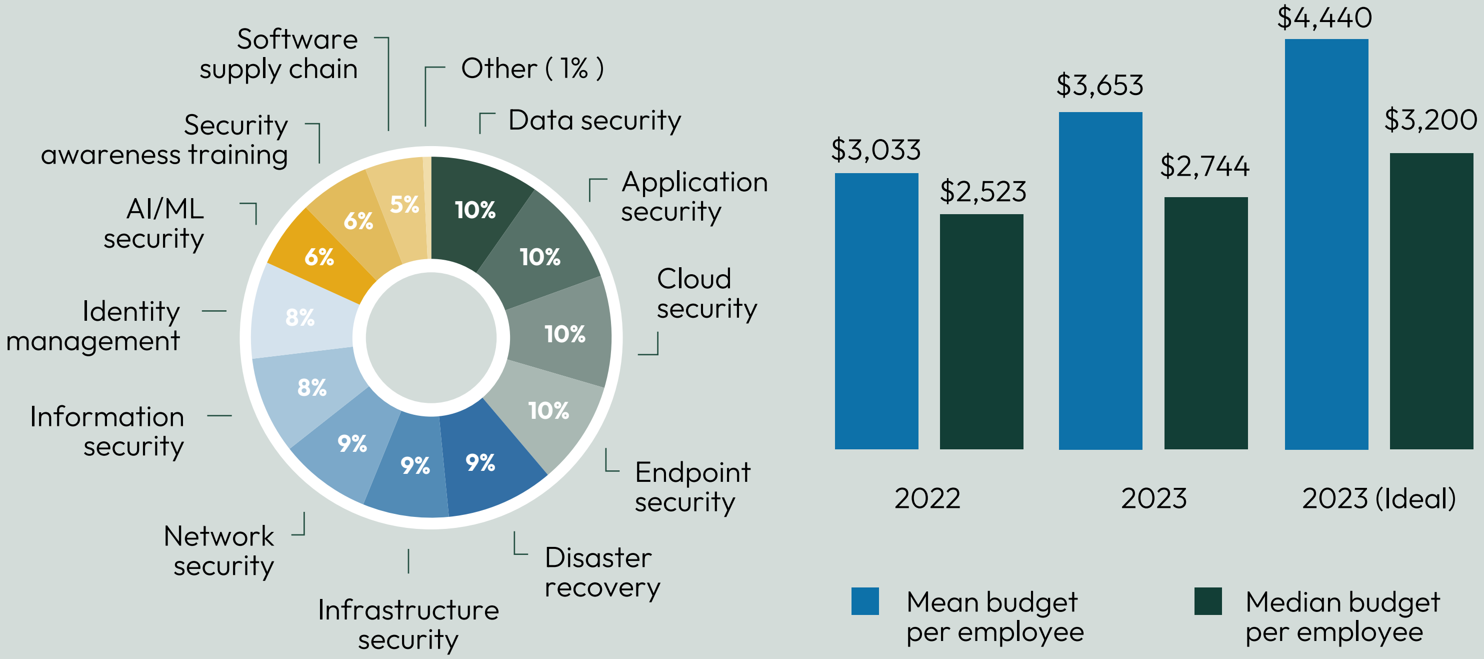
Resource Gaps: Budget

Security Spending at Large Enterprises Increased, while Mid-Size Spending Grew Less

Despite inflationary and recessionary fears, **cybersecurity budgets at large enterprises (more than 1,000 employees) remained resilient in early 2023, with a 22% year-over-year increase**. Mid-sized enterprises (500-999 employees) saw a small 5% increase, falling sharply from 51% budget growth last year. However, some CISOs are preparing for belt-tightening measures, greater scrutiny over spending decisions and longer decision-making timeframes, according to The Wall Street Journal.[5]

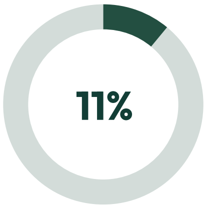
Data, application, cloud and endpoint security were the top spending categories in 2023, each representing 10% of security budgets. Budgets for security awareness training, endpoint security, and identity management increased the most between 2022 and 2023. AI/ML security and software supply chain security debuted on this year's survey with 6% and 5% of security budgets respectively. Security budgets per employee averaged $3,653 this year, up 20% from $3,033 per employee last year.

What is your total budget and category allocations for security solutions in 2023?

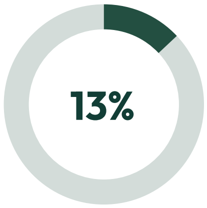


Budgets for Emerging Security Solutions Increased By Less

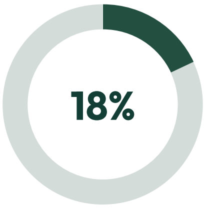
Enterprises continue to invest in emerging security solutions to address perceived weaknesses in the available solutions from leading vendors. **Security leaders increased budgets for new, innovative, and experimental security solutions by 18% this year**, although this was down from a 27% increase last year. In dollar terms, the budget for new solutions from emerging cybersecurity founders increased from $321 to $457 per employee on average across companies of all sizes.



Percentage of **2022 total budget** for emerging solutions



Percentage of **2023 total budget** for emerging solutions



Year-over-Year **budget growth** for emerging solutions

CISOs Would Spend More on Security Awareness Training

If ideal security budgets for 2023 were approved, security leaders would have gained 46% more budget, compared to the 20% year-over-year gain above approved budget levels. Enterprises would have requested more budget for security awareness training, infrastructure security, and cloud security and less budget for disaster recovery, network security, and AI/ML security.

More Budget is Ideal for 2023	**Less Budget** is Ideal for 2023
Security awareness training (+12%)	Disaster recovery (-8%)
Infrastructure security (+8%)	Network security (-6%)
Cloud security (+7%)	AI/ML security (-6%)
Identity management (+5%)	Software supply chain security (-5%)
Information security (+3%)	Endpoint security (-4%)

Mid-sized Enterprises
(500-999 employees)

5%
Year-over-Year Budget Growth

$75K-$9M
Budget Range

Large Enterprises
(1,000+ employees)

22%
Year-over-Year Budget Growth

$100K-$100M
Budget Range

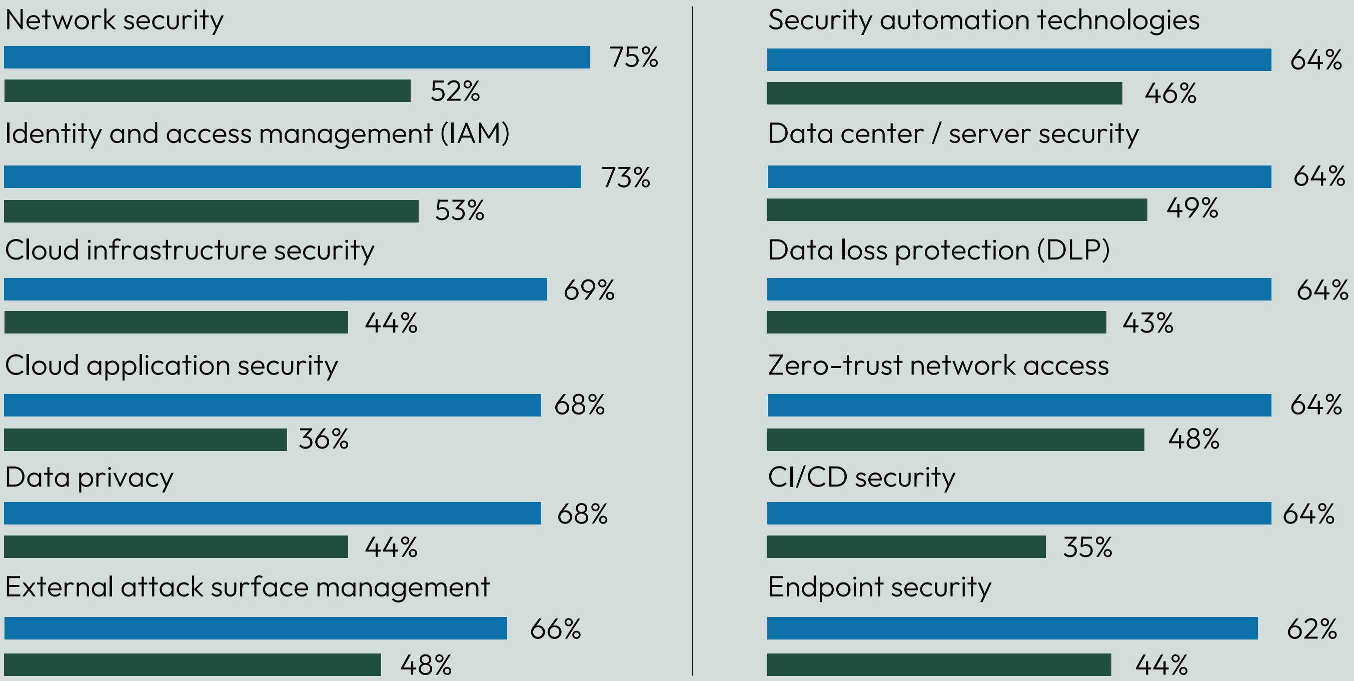
Market Opportunities

Cloud Application and CI/CD Security Solutions Perceived as Biggest Market Gaps

Security leaders reported gaps between the "importance" of and "satisfaction" with commercially-available cybersecurity solutions. Network security (75%), identity and access management (73%), and cloud infrastructure security (69%) were ranked the most important security tools. Security leaders were least satisfied with AI/ML model security (34%), CI/CD security (35%), and cloud application security (36%) tools.

The biggest market gaps were reported in cloud application and CI/CD security, with a 45%+ delta between satisfaction and importance. With only one-third of security leaders satisfied with these two commercially-available solutions, founders may have an opportunity to build better tools. Of the firms intending to build in-house, 34% would build cloud application security solutions, while only 2% would build CI/CD security solutions.

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



Large Enterprises Intend to Build In-House Solutions to Address Market Gaps

43% of organizations intend to build in-house security solutions this year, compared with 39% last year. Of those companies, **large enterprises with more than 1,000 employees were more likely to build in-house (83% this year vs. 57% last year)** than mid-sized firms with 500 to 999 employees (17% this year vs. 43% last year). Threat intelligence (36%) and network security (35%) remained in the top three focus areas this year, while **endpoint security (38%) displaced cloud infrastructure security as the top in-house development priority this year**.

In what areas are you planning to build an in-house solution over the next 12 months?

38%	Endpoint security
36%	Threat intelligence
35%	Network security
34%	Identity & access management
34%	Cloud application security
33%	Data center/ server security
31%	Data privacy
28%	API security
27%	Insider risk analytics
20%	Security automation
16%	Zero-trust network access
16%	Cloud infrastructure security

Security Automation Needed to Make Constrained Security Teams More Effective

82% of security leaders sought security automation tools to help contain and mitigate malware, as well as identify misconfigurations in cloud services. Another 76% of firms expressed a need to stop data privacy leaks, provision identities and access rights for new employees, and configure new cloud services securely. Security automation efforts were also driven by continued cloud attacks, difficulty in hiring cloud security professionals, and the desire for greater cloud security protections.

Where the Funding Is:

Cybersecurity Funding Declined 32% From Last Year's Peak

After breaking all-time cybersecurity funding records in 2021, the pace of investment decreased last year, amidst rising interest rates, industry-wide layoffs, and fears of recession. **Overall deal value declined 26.5% in 2022, with cybersecurity companies finishing the year with $17.5B**, down from $25.6B during the prior year, according to Pitchbook.[6] Despite the reduction, cybersecurity investment remained 75% higher than the $10B raised in 2020, and up more than 800% over the last decade from the $1.9B invested in 2012.

Funding Rounds, Deal Volume, and Exits Remained Down

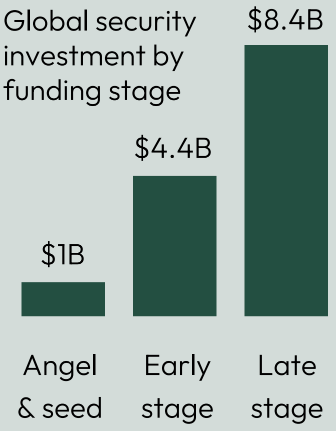
Deal count declined 14% year-over-year, dropping from 890 deals in 2021 to 769 deals in 2022, driven by fewer early-stage deals closing than late-stage deals, according to Pitchbook.[7] In fact, **cybersecurity deal flow dropped the past four quarters, with only $2.4B invested in Q4 2022**, according to Crunchbase.[8] Exit values also reached their lowest levels in six years at $2B in 2022, falling from the industry's all-time peak at $29.4B in 2021, and even dropping below the $2.4B in exit value the industry saw in 2016.

Angel, Seed, and Early-Stage Funding Actually Increased

Although overall cybersecurity funding decreased last year, late-stage (Series C and D) and venture growth (Series E+) were responsible for the biggest decline, while angel, seed, and early-stage (Series A and B) investment increased. **Angel and seed funding grew 43% year-over-year, increasing from $700M to $1B last year and doubling from 3% to 6% of overall cybersecurity funding**. Early-stage deal value also went up 12% last year, growing from $4B in 2021 to $4.4B in 2022, rising from 16% to 25% of all cybersecurity funding.

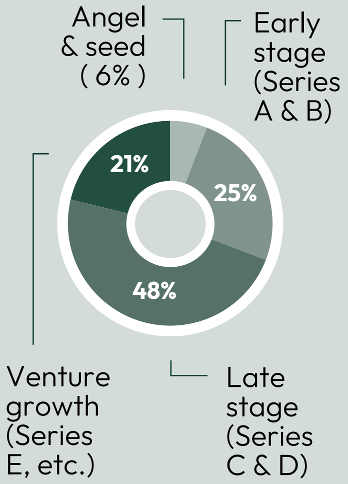
$17.5B

Global cybersecurity VC deal activity in 2022


Global security investment by funding stage

-26.5%

Year-over-Year in 2022 Funding



(Source: Pitchbook Emerging Tech Research)

Application Security Grew 34%+ Year-Over-Year in Angel, Seed & Early-Stage Funding

Application security was the only category that experienced funding growth across angel, seed, and early-stage rounds last year, with more than 34% growth in 2022.

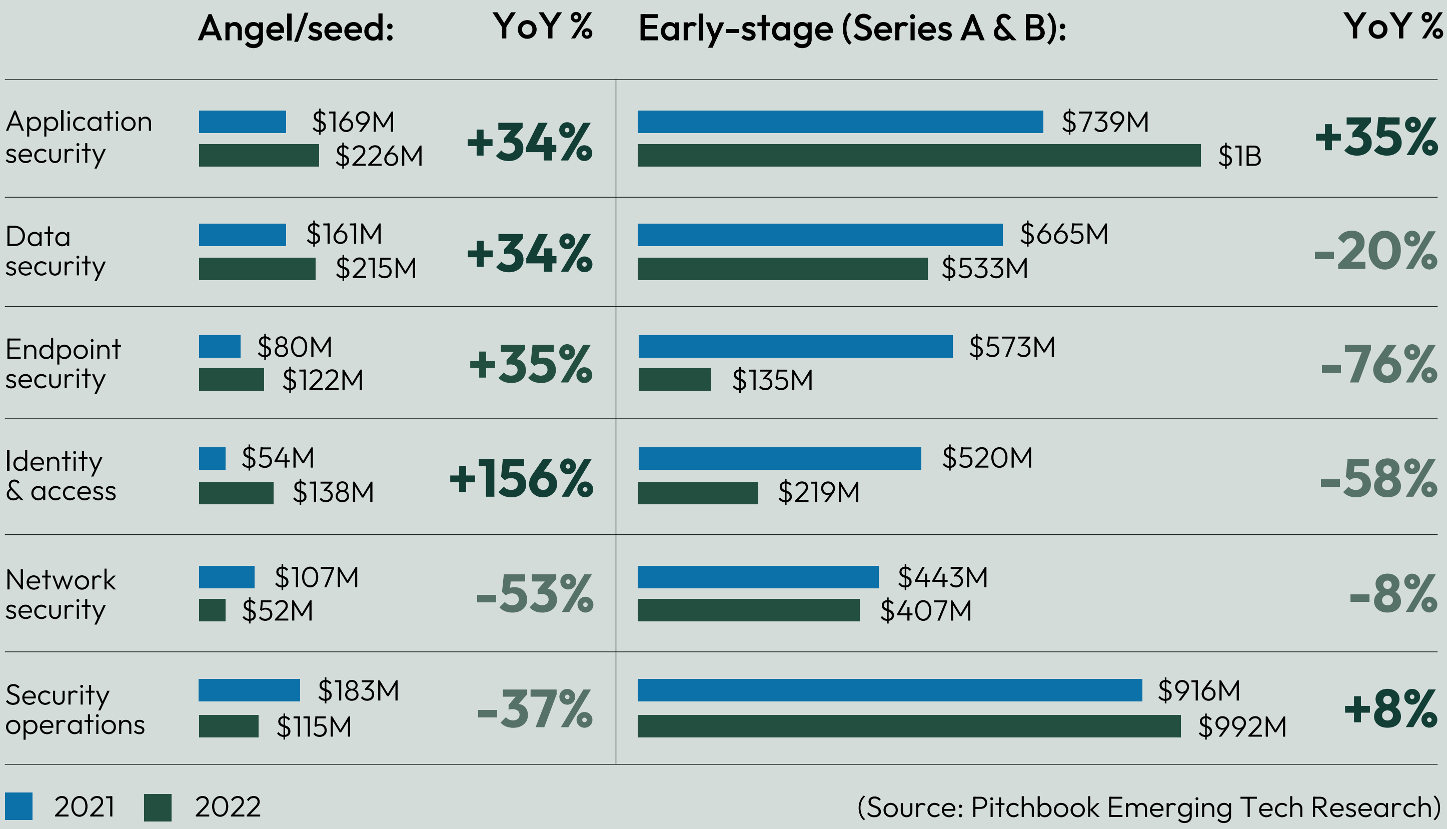
Although identity access management companies received a staggering 156% more angel and seed funding last year, from $54M in 2021 to $138M in 2022, early-stage funding for the category dropped 58% overall.

Data security funding at the angel and seed stage also grew 34%, up from $161M in 2021 to $215M in 2022, with declines elsewhere.

Early-stage funding decreased in all but two categories last year, with application security and security operations at or near $1B in total funding, nearly double all other categories.

Application security software funding increased from $739M in 2021 to $1B in 2022, while investment in security operations tools increased by 8% since 2021, up from $916M in 2021 to $992M in 2022.

Network and endpoint security companies fared worse, competing for a smaller pool of angel, seed, and early-stage funding last year.



(Source: Pitchbook Emerging Tech Research)

Conclusion

Given the findings from this year's survey, a question we're thinking about at Scale is how to support the next generation of emerging enterprise security startups.

> Funding is down, which means every dollar matters to early-stage companies and founders more than ever.

With an investing focus at the application and security layers, particularly with respect to AI/ML solutions, we're paying close attention to solutions that address data integrity, role provisions, and models of production. We're also looking at compliance-driven approaches, particularly with respect to AI explainability and governance, as we anticipate that more enterprises will be defining their security frameworks at the data layer.

> What past years teach us, however, is that new attack vectors will continue to pop up.

While automating certain security practices to ensure better and more consistent coverage is a good first step, however, the industry may be looking at short-lived solutions without the necessary human capital to think strategically and problem-solve in the year ahead. We'll know more in 2024.

Footnotes

[1] Edelman, 2023 Edelman Trust Barometer: Navigating a Polarized World, January 2023

[2] CrowdStrike, 2023 Cloud Risk Report: The Rise of the Cloud-Conscious Adversary, February 2023

[3] Verizon, 2023 Data Breach Investigation Report, June 2023

[4] IBM Security, Cost of a Data Breach Report 2022, July 2022

[5] Kim S. Nash, Cybersecurity Budgets Aren't Untouchable, The Wall Street Journal, May 2023

[6, 7] Pitchbook, Emerging Tech Research: Q4 2022 Information Security Report: VC trends and emerging opportunities, January 2022

[8] Chris Metinko, Cybersecurity Funding Continues Slide In Q3, Crunchbase News, October 2022

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 May 9-13, 2023, focused on the 12 months prior and 12 months upcoming, with a +/- 2.21% margin of error.

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

2022 | 2021 | 2020 | 2019 | 2018 | 2017

SCALE

scalevp.com