Cybersecurity Perspectives 2022

Responding to Enterprise Security Gaps in People, Technology and Budget

Table of Contents

Introduction

For our sixth annual Scale Venture Partners survey,* we reached out to senior cybersecurity leaders, directors, VPs and above throughout the United States to understand their priorities at the start of 2022 in response to the evolving cybersecurity landscape.

The unprecedented level of cyber attacks last year drove higher demand for cybersecurity solutions, leading to the biggest year on record for cybersecurity investment in the U.S., more than doubling from $6.9 billion in 2020 to $17.4 billion in venture funding in 2021.[1]

> **Ransomware attacks increased more than ever last year, as firms paid cyber criminals millions of dollars to unencrypt their stolen data.**[2]

Global ransomware attacks surged 148% in the first nine months of the year,[3] with 37% of global organizations falling victim to some form of ransomware attack in 2021.[4] High-profile attacks included the Colonial Pipeline, which disclosed a $4.4 million ransomware payment in May 2021 after gas delivery was disrupted in southeastern states for an entire week.

Other attack vectors included severe zero-day vulnerabilities, with Apache announcing in December 2021 that a vulnerability in the Log4j web application framework could allow remote code execution on 95% of Java-based applications. The widespread potential impact led the FTC to threaten legal action in January 2022 against any companies neglecting to patch exposed Log4j vulnerabilities.

> **Cybersecurity budgets and spending increased this year to address the growing volume of threats and the fear of steeper regulatory fines.**

As businesses continued to feel the effects two years into a global pandemic, information security and risk management spending was projected to increase from $155 billion in 2021 to $172 billion in 2022, according to Gartner,[5] with 69% of organizations predicting a rise in cybersecurity spending this year, according to PwC's 2022 Global Digital Trust Insights.[6]

> **But the Great Resignation has kneecapped an already understaffed cybersecurity sector as organizations struggle to hire and retain skilled workers.**

While enterprise security teams received more budget to spend more money on security tools to address greater threats, the lack of skilled workers to use those tools effectively creates unique challenges for businesses and new opportunities for cybersecurity founders in the year ahead.

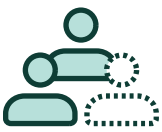
* Note: Unless specifically documented, all data sources are from Scale Venture Partners' primary survey research.

Key Findings

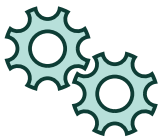
Increase in cloud, ransomware, and third-party attacks. While it's no surprise global ransomware increased, other coordinated attacks went up as well, with 50% of organizations experiencing a cyberattack against a cloud service, 37% suffering unwanted data encryption from ransomware or a third-party breach of sensitive data and 57% experiencing two to three cybersecurity incidents last year.

Rise in network, cloud, and endpoint security spending. Enterprise security budgets increased 27% on average in 2022 to address the rise in threats and continue securing work-from-home environments. Surprisingly — two years into a global health pandemic — 48% of organizations are still not prepared to secure their remote workers with only 76% expected to be "prepared" or "extremely prepared" by 2023.

Big need for better security tools. Despite bigger budgets, less than 55% of firms are satisfied with their security tools across all categories, with the biggest delta between satisfaction and importance in cloud infrastructure and zero-trust network access. Thirty-nine percent are building in-house because existing tools aren't commercially-viable, while experimental tech budgets increased 27% this year to 19.6% overall.



Lack of security staff inflamed by Great Resignation. The lack of cybersecurity staff to manage tools and defend against more attacks will have the biggest impact this year. Sixty-eight percent of firms are having difficulty finding people with the required skills and 45% are concerned about retaining existing staff who are leaving for better paid positions, while 70% believe their teams are dissatisfied with their job, salary, and workload.



Maximize effectiveness of limited security resources. Seventy-two percent of firms are focused on enforcing existing security policies more strictly and 66% on improving reporting visibility into what is and isn't working. More than 60% seek automation, AI and machine learning to improve the efficiency and effectiveness of security processes. Given the cyber skills shortage, 48% expect to outsource security operations.

Where the Threats Are

Attacks Against Cloud Services and Third Parties Top the List

The shift to the cloud has been underway for over a decade, and the importance of securing cloud infrastructure and cloud applications has been rated highly across our previous reports. And for good reason, since security leaders say the most frequently occurring incident type involved an attack against a cloud service, with **50% experiencing at least one incident**.

A second tier of incidents involved compromise due to an attack against a third-party, ransomware attacks that successfully encrypted data, and the breach of sensitive information — with **37% of security leaders saying they experienced at least one incident** in each of these three incident types.

Two of the top four incident types took place beyond the traditional security perimeter in areas where organizations often lack visibility: cloud services and third parties. With a third of organizations planning on moving more than 75% of workloads to the cloud over the next three to five years,[7] ensuring sufficient visibility and better security posture is paramount.

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

- **50%** Cloud service attacked
- **37%** Compromised through 3rd party attack
- **37%** Ransomware encrypted our data
- **37%** Sensitive information breached
- **31%** Employee stole our information
- **26%** Fined for data privacy non-compliance
- **26%** Phishing attack compromised credentials
- **25%** Misconfigured cloud access rights led to data breach

The Majority of Companies Experienced Multiple Incidents

According to Accenture Consulting, organizations experienced a 31% increase over the number of cyber attacks (both attempted and successful) between 2020 and 2021, with 270 attacks on average in 2021 (241 attempted, 29 successful) compared with 206 attacks in 2020 (184 attempted, 22 successful).[8]

As the frequency and volume of cyber attacks increased last year, the majority of organizations reported that they suffered multiple security incidents throughout 2021, with **57% of firms experiencing two or three types of cybersecurity incidents** and **21% experiencing four or more types of cybersecurity incidents**. **Only 19% of firms suffered one cybersecurity incident throughout 2021**.

Sophisticated Attacks More Severe than Frequent Attacks

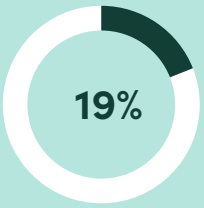
Developing a strong cybersecurity posture is not as simple as only protecting against more common types of incidents. While most organizations experienced a range of incidents last year, the number of incidents is a different measure than the impact of each incident.

For example, the Identity Theft Resource Center reported that a single data leak compromised data on 700 million individuals. It was an infrequent incident (less than 1% of all incidents reported by the Center) but 81% of the individuals compromised across all incidents.[9]

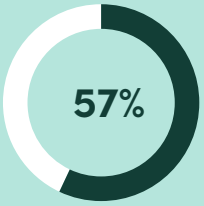
In comparison, the Capital One security breach compromised data on more than 100 million people in the United States and Canada,[10] cost Capital One an $80 million regulatory fine[11] and required a $190 million settlement for the class-action suit brought against the company.[12]

Given that commonly occurring attacks are usually of a limited or minor impact, while infrequently occurring attacks are more likely to have far reaching impacts, security leaders will need to properly prioritize their spending to protect against small scale yet frequent threats versus less frequent but potentially devastating cyber attacks.

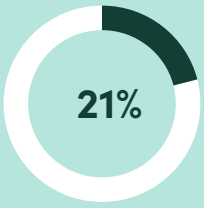
How many security incidents occurred at your organization in 2021?



Experienced only **one type** of cyber incident



Experienced **two or three types** of cyber incidents



Experienced **four or more types** of cyber incidents

How Enterprises Are Responding

Network, Cloud and Endpoint are Top 3 Cybersecurity Spending Priorities for 2022

Security leaders are rebalancing investment priorities over the next 12 months to address ongoing pandemic challenges, improve existing security processes, and make their teams more effective. **Network security has become the most important category firms will invest in during 2022**, while cloud infrastructure security dropped to second place after being the top priority the last few years. Endpoint security jumped to third place from ninth place last year, while security automation dropped off the Top 10 list entirely. **Emerging technologies that joined the list for the first time** this year include external attack surface management in seventh place and zero trust network access in ninth place.

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

2018	2019	2020	2021	2022
Cloud infrastructure security	Cloud application security	Cloud infrastructure security	Cloud infrastructure security	Network security
Cloud application security	Cloud infrastructure security	Cloud application security	Data privacy	Cloud infrastructure security
Network security	Network security	Network security	Network security	Endpoint security
Data security / DLP	Data security / DLP	Data security / DLP	Cloud application security	Data privacy
Data center / server security	Data center / server security	Data privacy	Data security / DLP	Cloud application security
Threat intelligence	Endpoint security	Data center / server security	Security automation	Data center / server security
Endpoint security	Threat intelligence	Security automation	Operational technology (OT)	**External attack surface management**
Security automation	Security automation	**Operational technology (OT)**	Data center / server security	Identity and access management
Breach/attack simulation	Breach/attack simulation	Endpoint security	Endpoint security	**Zero trust network access**
Insider risk analytics	**Quantum encryption**	Threat intelligence	Identity & access management	Data loss protection (DLP)

Rising Cyber Insurance Premiums Drives Increased Cybersecurity Spending

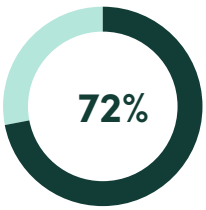
The cost of cyber insurance is rising, forcing security leaders to re-evaluate their spending between insurance coverage and cybersecurity solutions. Driven by the rising tide of ransomware attacks, underwriters faced staggering losses in their cyber insurance portfolios after massive payouts last year.[13] With underwriters doubling premiums and halving coverage limits in some cases,[14] cyber insurance is relatively more difficult to secure now than it was a year ago, resulting in **money that would have previously flowed into an insurance policy being invested in cybersecurity tools to decrease the risk of a compromise.**

41%

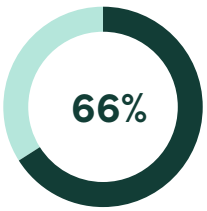
of all cyber insurance claims in the first half of 2021 were due to ransomware attacks.[15]

Focus on Improving the Effectiveness of Existing People, Processes and Technology

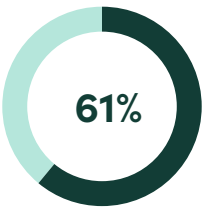
Security leaders are trying to build more mature cybersecurity capabilities over the next 12 months. To mitigate the impact of the cybersecurity skills shortage, **72% of security leaders are faced with doing more with what they already have by enforcing existing security policies, tools, and processes more strictly**. Defining security policies doesn't pay off without enforcement, which provides stronger coverage of the basics (e.g., widespread use of multi-factor authentication, encryption to protect sensitive data) and decreases the attack surface available to threat actors (e.g., reduced usage of unsanctioned collaboration tools). Sixty-six percent of executives are enhancing cybersecurity metrics and reporting to better understand what is working and what is not so as to prioritize spending, identify new threats, and improve operational performance. More than 61% of security leaders are also training software engineering and security teams on security best practices, while **48% of organizations are outsourcing security operations, given the difficulty in hiring and retaining skilled cybersecurity talent**.



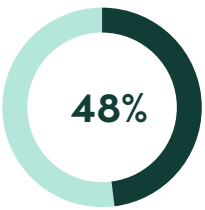
Enforcing **existing security policies** more strictly



Enhancing **cybersecurity metrics and reporting**



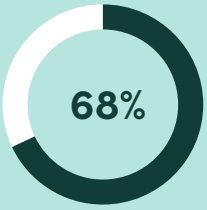
Training **software engineering and security teams**



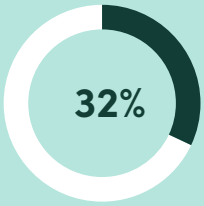
Outsourcing **security operations** due to staffing issues

Resource Gaps: People

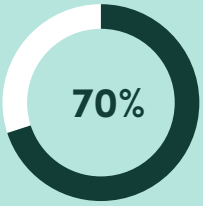
Outlook on cybersecurity hiring and retention



Experienced **high difficulty** finding cybersecurity talent



Concerned **current staff will leave** to paint or bake muffins



Believe **current staff dissatisifed** with job, salary and work culture

Not Enough Skilled Cybersecurity Talent Available

Sixty-eight percent of security leaders ranked the difficulty of finding people with the required skills as the most impactful trend on their security strategy over the next 12 months. They expect it to have an even greater impact than ransomware attacks, data breaches at third parties and supply chain attacks. Forty-two percent said insufficient security personnel was a "barrier" or "extreme barrier" to achieving their desired security posture. This ongoing lack of talent creates significant challenges for security leaders for the foreseeable future, because budget for new tools alone doesn't deliver increased cyber resilience. For example, firms that are cash rich and expertise poor don't know where to allocate budget for optimal outcomes.[16]

Hard to Retain Existing Cybersecurity Team Members

Forty-five percent of security leaders say they can't pay enough salary to attract new staff and another **45% don't have the ability to retain staff who are leaving for better paid positions at other firms**. Forty-six percent of security leaders expect turnover to increase over the next 12 months, with average turnover estimated at 17%. Only 27% expect turnover to decrease. As much as **32% of security leaders are concerned their current staff have had enough and are likely to leave the cybersecurity industry entirely** to paint or bake muffins.

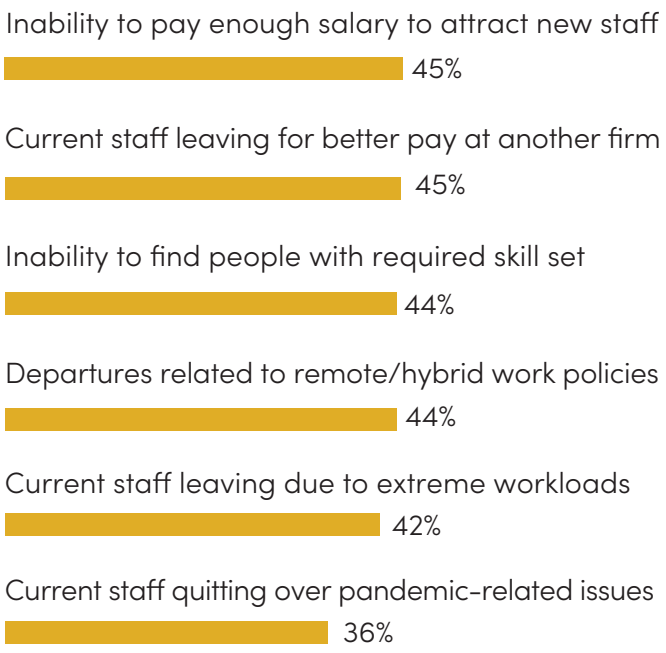
Cybersecurity Job Satisfaction Remains Low

Seventy percent of security leaders believe their current cybersecurity staff are not satisfied with the work culture, salary, and task responsibilities of their role. Remote and hybrid work policies are of particular concern currently (44%), along with extreme workloads for cybersecurity staff (42%). However, 60% of companies expect job satisfaction to improve 12 months from now, although this belief seems overly optimistic, given the lack of people, difficulty in retention, and expected increase in turnover in the months ahead.

The Human Element is the Most Common Weakness in Cybersecurity Incidents

While security leaders are facing a significant challenge in finding enough people with the right cybersecurity skills, "humans" account for other critical challenges when it comes to cybersecurity. For example, 85% of breaches involve a human element, according to Verizon, with 61% of breaches involving compromised credentials and 3% of breaches involving the exploitation of vulnerabilities.[17] Therefore, it's not enough to find cybersecurity talent, without also improving security awareness among all employees to address systemic "human" security weaknesses that cybercriminals regularly exploit during attacks. It is essential to educate employees through security awareness training so they learn to verify the authenticity of whoever they find themselves on the phone with and not to share sensitive details — e.g., user credentials, bank details — that could lead to data breaches.[18]

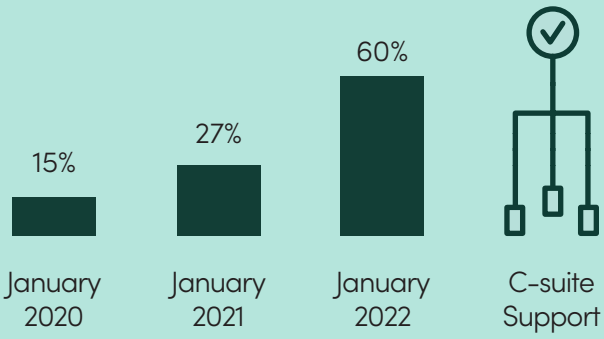
Percentage of security leaders "concerned" or "extremely concerned" about cybersecurity team staffing issues:



However, Security Leaders are Gaining More Support from C-Suite Executives

Despite ongoing hiring and retention challenges, **more than twice as many security leaders say they have gained more support from C-suite executives for cybersecurity efforts this year compared with last year**. Sixty percent of security leaders said major media coverage about high-profile ransomware attacks against critical infrastructure were significant in gaining more C-suite support. In addition, the transition to a hybrid workforce further reinforced the need for executives to back critical security initiatives.

Level of C-suite understanding about the business impact of security:



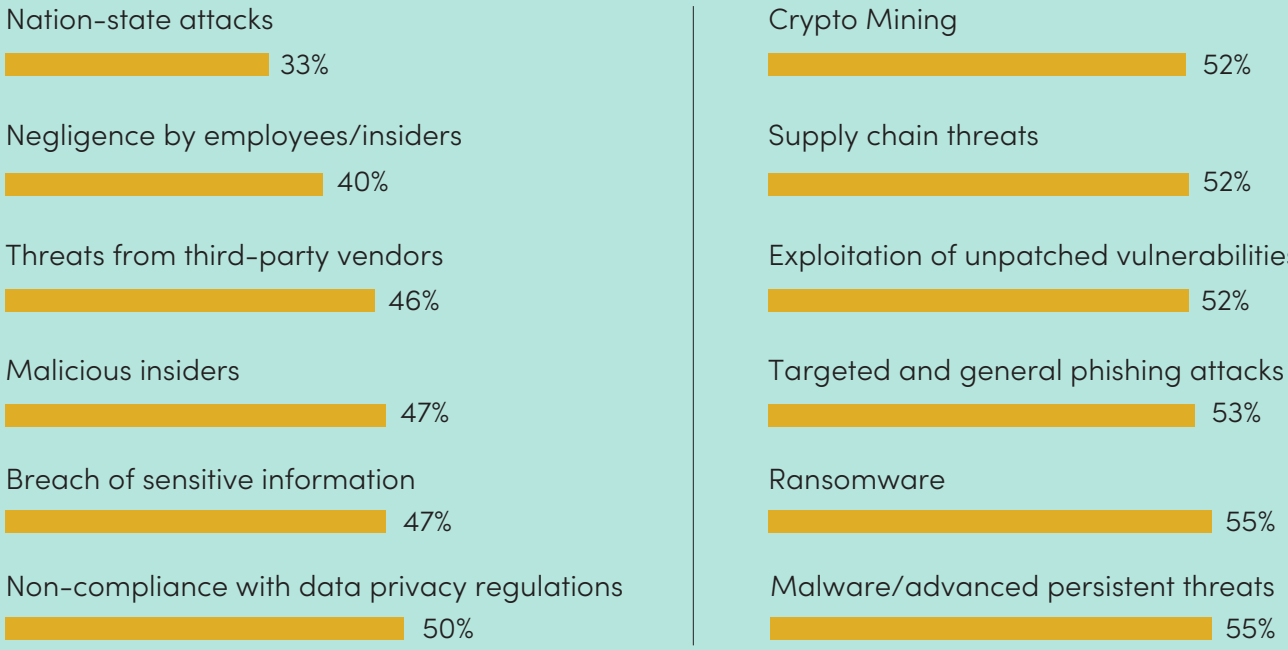
Resource Gaps: Technology

Many Companies Believe They Lack Protection Against Common Attacks

Security leaders feel ill-prepared to meet a wide range of cybersecurity risks and threats. While only 33% of security leaders believe their current protections would be sufficient against nation-state attacks (given the scale of resources at play), **only 55% feel sufficiently prepared for common attacks such as phishing, malware and ransomware.** The growth in ransomware attacks was especially marked throughout 2021,[19] and among the most frequent threats seen in the wild last year along with crypto mining, phishing, and trojans.[20]

Given the rapid shift to work from home over the last two years, cybercriminals have exploited this disruption by increasing their frequency of attacks. In fact, 76% of organizations said the number of attacks they faced have increased since the pandemic began.[21] These groups have also pivoted to new attack techniques to obtain credentials to corporate networks.[22] With employees dispersed across homes, cafes, and office locations, the need to support a remote workforce is not going to abate any time soon as organizations need more visibility and protection.

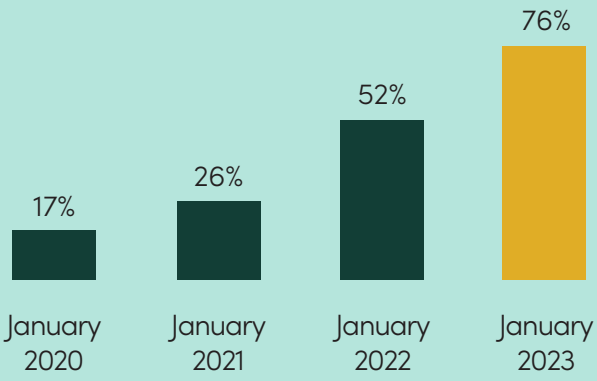
How "effective" or "extremely effective" are your current cybersecurity protections?



Nearly Half of Firms Are Still Not Ready to Fully Secure Work-from-Home Employees

Two years into a global health pandemic, 48% of organizations still say they are not well prepared to support secure work-from-home initiatives in January 2022. While preparedness has doubled over the last 12 months, enabling employees to work from home securely remains a challenge. Although this is a vast improvement from pre-pandemic levels at 17% in January 2020, it's surprising that leaders believe it will take until 2023 to reach 76% preparation, as hybrid options begin to replace work-from-home initiatives.

Level of preparation for employees to securely work from home:



More Tools Are Needed to Address Growing Threats

The appetite for security tools is growing again, with 64% of security leaders wishing to deploy more tools over the next 12 months. Only 29% of companies want fewer tools this year, unlike the majority of respondents in previous surveys. Companies have 12 security tools currently deployed on average and expect to have 14 security tools deployed over the next 12 months, although 16 tools would be ideal. **Thirty-one percent of firms say they cannot find cybersecurity solutions in the market to meet their desired security posture.**

Yet Security Leaders Still Overestimate Level of Protection

Many security leaders state they currently have effective cybersecurity protections in place, yet still experienced security incidents during the previous 12 months. For example, 51% of firms suffered a malicious employee incident during 2021, yet claimed to have "effective" or "extremely effective" protections against such attacks. The same over-confidence played out with ransomware, with 50% of firms having their data encrypted by a successful ransomware attack over the last 12 months, despite feeling protected against those types of threats.

64%

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

12

Average # of tools currently deployed

+2

Average # of new tools budgeted for this year

+4

Average # of new tools preferred to deploy

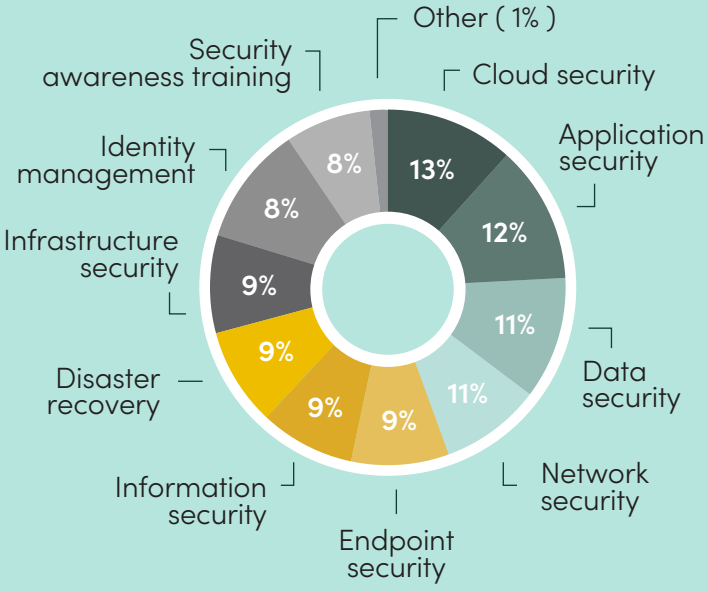
Resource Gaps: Budget

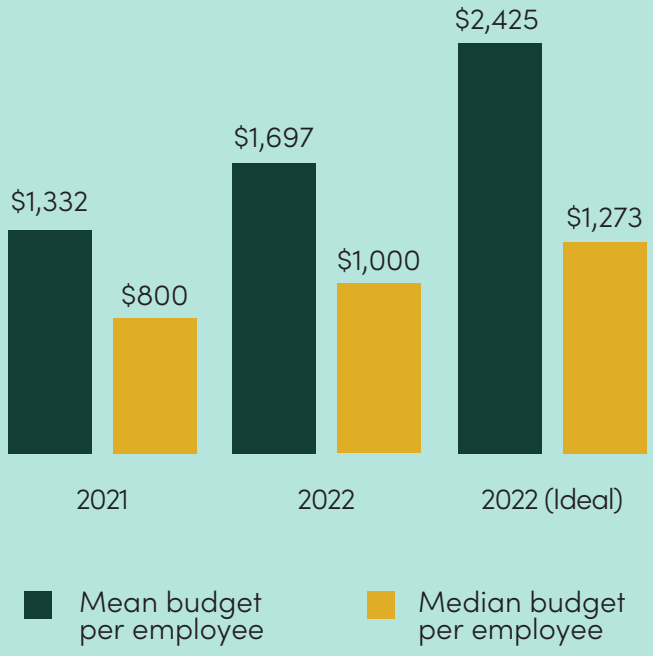
Overall Cybersecurity Budgets Increased Significantly in 2022

Security budgets increased 27% on average this year compared to last year, having risen from an average of $1,332 per employee in 2021 to $1,697 per employee in 2022. **Budget growth at mid-sized enterprises (500-999 employees) was 51% year-over-year compared to 19% year-over-year at large enterprises (more than 1,000 employees).** Mid-sized companies expect to spend significantly more per employee this year than large companies, which benefit from greater economies of scale in security expenditures than smaller companies can achieve.

The overall budget allocation between spending categories was fairly fixed between 2021 and 2022, with **application, cloud, data, and network security each more than 10% of the overall security budget in 2022**. While security leaders are spending more on network, infrastructure, and identity management in 2022 compared with last year's budget, they would prefer to spend less on endpoint security and identity access management than they budgeted this year. Two critical investment areas driving these spending priorities are securing the hybrid workforce and improving protection and recovery capabilities for urgent attack vectors such as ransomware.[23]

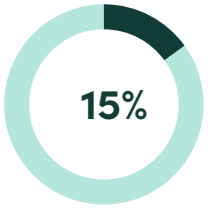
What is your total budget and category allocations for security solutions in 2022?



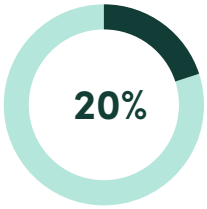


Budgets for Emerging Security Solutions Also Increased

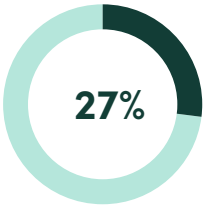
Security leaders indicate a growing appetite for new, innovative, and experimental solutions in 2022, with a **27% uplift in the budget set aside for emerging solutions** (from 15% last year to 20% this year). Security leaders are on the hunt for new solutions to address emerging and enduring threats better than the current set of tools in market. The changing threat landscape is challenging the efficacy of current tools and security leaders are willing to spend more budget to find better alternatives that enable them to stay ahead of attackers.



Percentage of **2021 total budget** for emerging solutions



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



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

Security Leaders Could Put Even More to Productive Use

Despite overall security budget increases on average this year, **security leaders believe they could have put 43% more budget to productive use**. For example, companies would have spent even more on application, cloud, infrastructure, and network security in 2022 in an ideal budgeting scenario than what was ultimately approved. **If security leaders' entire ideal 2022 budget was authorized in full, it would reflect an average increase of 82% year-over-year from 2021**, for an average of $2,425 per employee in 2022.

More Budget is Ideal for 2022	**Less Budget** is Ideal for 2022
Application security	Disaster recovery
Cloud security	Endpoint security
Data security	Identity management
Information security	Infrastructure security
	Network security
	Security awareness training

Mid-sized Enterprises
(500-999 employees)

51%
Year-over-Year Budget Growth

$12K-$4M
Budget Range

Large Enterprises
(1,000+ employees)

19%
Year-over-Year Budget Growth

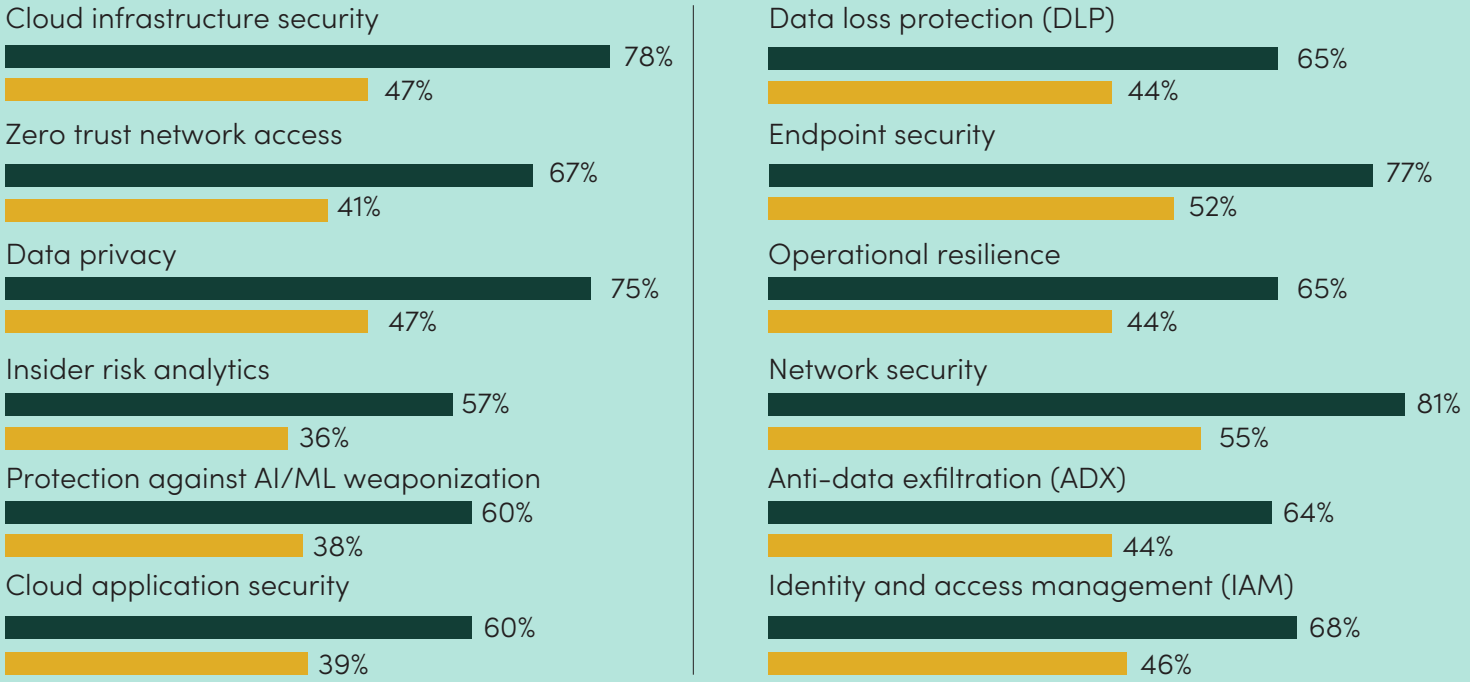
$50K-$25M
Budget Range

Market Opportunities

Security Leaders are Dissatisfied with Current Cybersecurity Offerings

Security leaders want more effective cybersecurity solutions based on the large variation between how important solutions are to their organization and their level of satisfaction with commercially-available offerings from security vendors. While network security tools are rated as the most important (81% of security leaders rate these as "important" or "extremely important"), only 55% of security leaders say they are "satisfied" or "completely satisfied" with commercially-available offerings. **Cloud infrastructure security has the greatest variation between the two ratings**, at 78% importance and 47% satisfied for a negative 40% variation between the two. **Solutions for zero trust network access, data privacy, and insider risk analytics have similar variations**. In the wider scheme of things, the number of sanctioned cloud services is increasing at many organizations, driving the need for cross-cloud threat visibility,[24] which makes it essential for organizations to solve the cloud security challenge or face increasing exposure to attacks.

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



Companies Building In-House Solutions Due to Lack of Confidence in Existing Tools

Thirty-nine percent of security leaders are building security solutions in-house because they believe there are a lack of commercially-viable solutions, with 60% planning on building three to five solutions. Network security (44%), cloud infrastructure security (43%), and threat intelligence (42%) are the most common solutions for in-house development. Thirty-one percent of security leaders believe this inability to find solutions to meet their current cybersecurity needs is a significant barrier to improving their security posture. Large enterprises with more than 1,000 employees were more likely to build in-house (57%) than mid-sized firms with 500 to 999 (43%).

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

44% Network security

43% Cloud infrastructure security

42% Threat intelligence

36% Data center/ server security

34% Identity and access management

34% Cloud application security

30% Data privacy

29% Endpoint security

26% Data loss protection (DLP)

21% API security

19% Security automation technologies

18% Third-party risk assessment

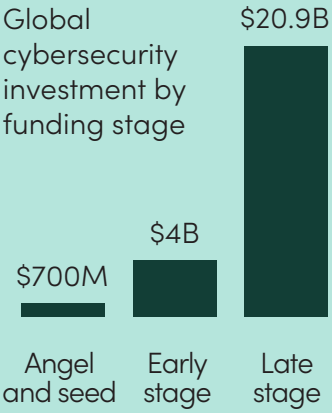
Automation, AI and Machine Learning Will Double in Importance Throughout 2022

Given the shortage of skilled cybersecurity talent worldwide, security leaders expect **the importance of security automation tools to increase from 32% currently (rank as "important" or "extremely important") to 69% in 12 months**. The outcomes that organizations want the most from security automation are better detection of cyberattacks (80% ranked this as "important" or "extremely important"), correlation of threat signals across multiple tools (75%), and enhanced protection for endpoints (74%) — which is of particular concern when supporting a remote and hybrid workforce. **Solutions that leverage artificial intelligence (AI) and machine learning (ML) will also double in importance from 31% currently to 67% in 12 months** by providing critical capabilities that eliminate manual tasks, improve the efficiency of their security teams, and increase the effectiveness of overall security operations.

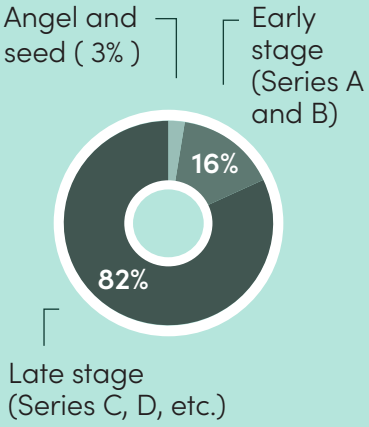
Where the Funding Is:

$25.6B
Global cybersecurity VC deal activity in 2021

Global cybersecurity investment by funding stage



130%
Year-over-Year Funding Growth



(Source: Pitchbook Emerging Tech Research)

Cybersecurity Funding More than Doubled in 2021

Cybersecurity companies raised $25.6B in venture capital funding across 938 deals worldwide last year, which represented a 130% year-over-year increase of investment from 2020 with $11.1B across 811 deals, according to Pitchbook.[24] This record-shattering amount was primarily driven by late-stage (Series C, D, etc.) deal activity, which was responsible for triple-digit growth in VC funding across every cybersecurity category last year, accounting for 82% of the total amount of funding raised at $20.9B. The majority of overall funding went to U.S. cybersecurity companies, which accounted for $17.4B in 2021, up from $6.9B in 2020, according to Crunchbase.[25]

Network Security and Identity Access Management Top List

Network security and identity and access management received the most funding across all stages last year, with almost $5B each in global deal value.[26] This correlates with protecting cloud workloads outside the traditional network perimeter, as well as authenticating employees in work-from-home environments. The number of VC-backed acquisitions also grew from 58 in 2020 to 87 last year, after experiencing little to no growth over the last seven years, with endpoint security and identity and access management companies accounting for more than 50% of all exits, according to Pitchbook.[27]

Early-Stage Deal Activity Increased to $4B Last Year

Despite late-stage cybersecurity deals making headlines, however, angel, seed, and early-stage (Series A and B) deal activity is more instructive to founders building the next-generation of innovative cybersecurity companies. To that end, **early-stage deal activity increased 43% year-over-year from $2.8B in 2020 to $4B in 2021, representing 16% of all cybersecurity VC funding last year**. Angel and seed deal activity also grew from $600M to $700M last year, or 17% year-over-year, but only accounted for 3% of overall funding.

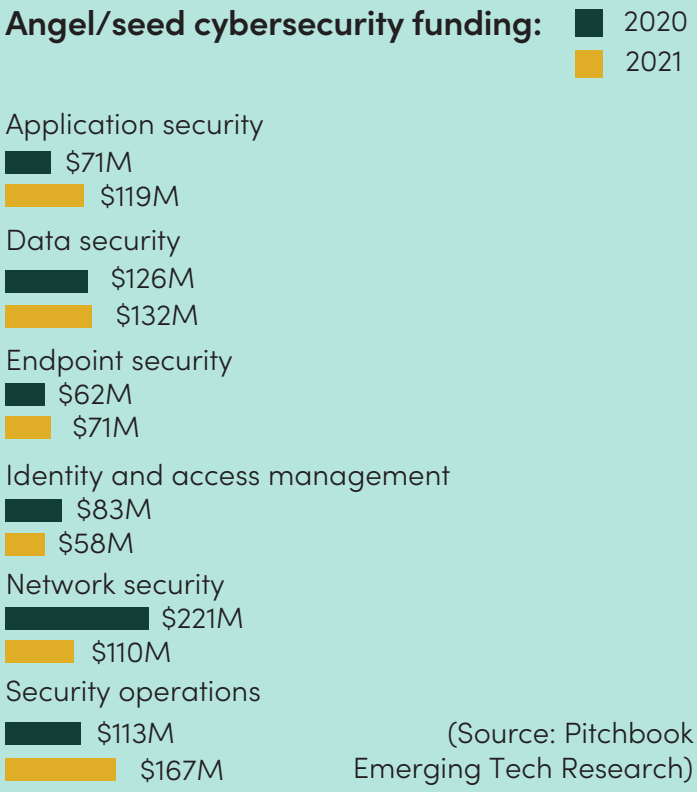
Security Operations Software Experienced Triple-Digit Growth in Early-Stage Funding

For seed and angel deal activity, application security had the biggest increase in funding, up 68% last year at $119M from $71M in 2020. Security operations software funding at this stage also grew by 47% year-over-year, up from $113M in 2020 to $167M in 2021.

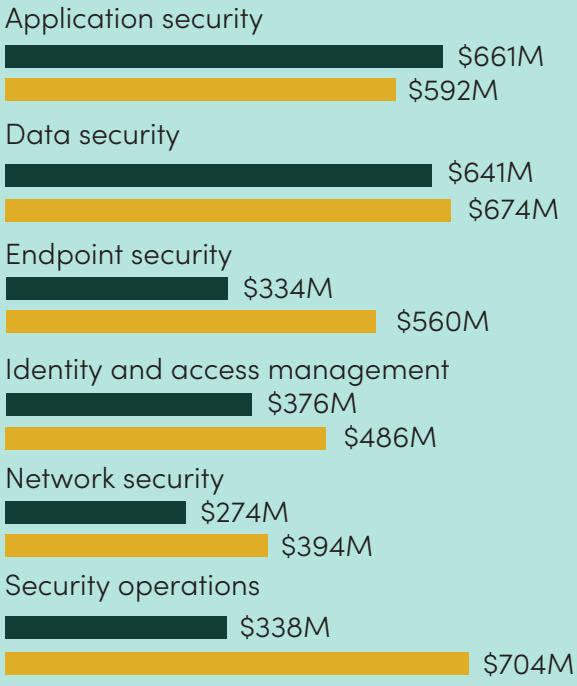
However, **seed and angel funding for network security and identity and access management companies both decreased (30% and 50% respectively)**, with more funding in these categories focused on early- and late-stage investments in companies with more mature technologies.

For early-stage deal activity, security operations software had the biggest increase in funding last year, going up from $338M in 2020 to $704M in 2021, an 108% year-over-year improvement, which parallels security leaders' focus on improving the efficiency of their limited teams this year.

Endpoint security investment at this stage increased by 68% year-over-year, from $334M in 2020 to $560M in 2021, given the proliferation of end-user devices and the importance of securing a large and growing attack surface from increased cyber threats.



(Source: Pitchbook Emerging Tech Research)



Conclusion

Cybersecurity founders have plenty of opportunity ahead of them this year, with the majority of enterprise security leaders having access to significantly more overall cybersecurity budget, as well as budget for emerging solutions to work with in 2022. There's also a growing appetite for more technology to address the growth in incidents, the increased attack surface in the cloud and the need to better secure the proliferation of endpoints from work-from-home employees.

> **Cybersecurity funding and exits have broken all-time records as investors fuel innovation to address today's opportunities and pick tomorrow's winners.**

Given the difficulty in hiring and retaining cybersecurity talent that is projected to continue this year, however, security leaders need to be more effective with current people and processes. Without the in-house expertise to manage new technologies effectively, however, there's also an increase in interest in outsourcing some security operations, like extended detection and response, given the lack of internal cybersecurity talent available for security leaders to leverage.

Because demand for cybersecurity solutions continues to outpace internal cybersecurity staffing capacity, however, network, cloud, and endpoint solutions that leverage AI, machine learning, and automation to improve the efficiency and effectiveness of an expanded enterprise footprint best meet the needs of security leaders struggling to secure hybrid and work-from-home initiatives against frequent attacks. With 2022 well underway, optimism remains in the year ahead.

> **Security leaders expect greater stability to resume in 2023 with the help of new cybersecurity tools to restore order among the chaos of a hybrid workforce.**

Methodology

Scale Venture Partners commissioned Everclear Marketing and Osterman Research Group 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 December 15-30, 2021 with a +/- 3.35% margin of error.

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

2021 | 2020 | 2019 | 2018 | 2017

Footnotes

1, 24, 26, 27. Pitchbook, **2021 Annual Information Security Report**: VC trends and industry overview, January 2022

2. U.S. Treasury's Financial Crimes Enforcement Network (FinCEN), **Financial Trend Analysis**: Ransomware trends in Bank Secrecy Act data between January 2021 and June 2021, October 2021

3, 19. SonicWall, **SonicWall Cyber Threat Report**: 2021 Mid-Year Update, July 2021

4, 15. IDC, **IDC 2021 Ransomware Study**, July 2021

5. Mary K. Pratt, **Cybersecurity spending trends for 2022: Investing in the future**, *CSO Magazine*, December 2021

6. PwC, **2022 Global Digital Trust Insights Survey**, October 2021

7, 8, 16, 23. **Accenture Consulting, State of Cybersecurity Resilience 2021**: How aligning security and the business creates cyber resilience, June 2021

9. Identity Theft Resource Center, **ITRC 2021 Q3 Data Breach Analysis**, October 2021

10. Greg Kumparak, **Capital One Hacked, Over 100 Million Customers Affected**, *Techcrunch*, July 2019

11. Office of the Comptroller of the Currency, **OCC Assesses $80 Million Civil Money Penalty Against Capital One**, August 2020

12. Karen Hoffman, **The high cost of mishandling data breaches, security reporting for financial services**, *SC Magazine*, January 2022

13. Aon, **2021 Cyber Security Risk Report**, January 2021

14. Carolyn Cohn, **Insurers run from ransomware cover as losses mount**, *IT News*, November 2021

17. Verizon, **2021 Data Breach Investigations Report**, May 2021

18, 22. Check Point Research, **Check Point Cyber Security Report 2021**, January 2021

20. **Cisco Umbrella, 2021 Cybersecurity Threat Trends**: Phishing, Crypto Top the List, April 2021

21. VMware, **Global Security Insights Report 2021: Intelligence from the Global Cybersecurity Landscape**, April 2021

24. Okta, **Businesses at Work 2021**, March 2021

25. Chris Metinko, **Cybersecurity Venture Funding Surpasses $20B In 2021, Fourth Quarter Smashes Record**, *Crunchbase News*, January 2022

SCALE

scalevp.com