svb Silicon Valley Bank
A Division of First Citizens Bank

The Rise of CyberAI

The Intersection of GenAI and Cybersecurity

May 2024

Contents

svb Silicon Valley Bank
A Division of First Citizens Bank

CyberAI: Securing the Next Frontier

Almost exactly a year and a half after the public release of ChatGPT, the new frontier of Generative AI (GenAI) has captured public imagination. For business leaders, the increasing proliferation of GenAI creates a distinct set of challenges and opportunities as companies begin exploring ways to augment or even replace existing workflows in the enterprise. While we have started to see GenAI affect everything from how companies develop software to how they engage with their customers, we are ultimately still only at the outset of what may end up being a platform shift. This shift could be as influential as the advent of mobile or cloud computing proved to be over the past two decades.

How, though, does this emergence affect how Chief Information Security Officers (CISOs) protect their organizations? How do security leaders think about this burgeoning platform shift amidst an ever-evolving threat landscape? To what extent is the ability to secure GenAI applications an impediment to their being more widely adopted? These are some of the questions that our clients and their customers continue to grapple with. Rather than focus solely on GenAI and its proliferation, we have opted instead to explore the **intersection of GenAI and cybersecurity or, said another way, "CyberAI."**

Nearly 70% of CISOs polled for this report identified GenAI adoption as at least a top-five priority to their organization. Meanwhile, almost all of the 26% of polled CISOs who have not yet changed their cybersecurity stack in response to increased GenAI proliferation expect to within the next three years, implying ample opportunity for new startups to help fill that gap. These are just two tailwinds that we expect will drive more attention to CyberAI and accelerate startup formation. We believe that continued urgency to employ GenAI solutions will be a defining trend in the coming years and that **CyberAI will be increasingly critical to the emergence of this new landscape.**

CyberAI

noun [**sahy**-ber **ey**-ahy]

Tools and platforms that leverage GenAI to address vulnerabilities in AI infrastructure, models and applications, or to defend against external, GenAI-driven threats and attacks.

* *We expect that our conceptualization of GenAI will evolve as the space continues to emerge. If you would like to contribute further to this definition, please reach out at amccarty@svb.com.*

Andrew McCarty
Vice President
Tech Banking
Silicon Valley Bank

Emma Eschweiler
Director
Investor Coverage
Silicon Valley Bank

Natalie Fratto
Managing Director
Investor Coverage
Silicon Valley Bank

svb Silicon Valley Bank
A Division of First Citizens Bank

Macro

Drivers of CyberAI

Macro Tailwinds

Support for CyberAI Infrastructure
Government funding from programs in the CHIPS and Science Act and the Department of Defense cybersecurity budget are major drivers of investment in the infrastructure necessary for growth in the CyberAI space.

Investment from Corporates
Large corporates have grown their research arms over the past decade to support AI model growth. Microsoft has invested $10B in OpenAI, and IBM has acquired 30+ companies since 2020 to bolster AI capabilities.

Ubiquity of ChatGPT
Released in 2022, ChatGPT brought GenAI to the masses. While not the first large language model (LLM), its wide adoption marked a long-term tectonic shift in how businesses and consumers interact with the technology.

Security Concerns

Mounting Costs of Cybercrime
Cybercrime losses increased nearly nine-fold from 2017 through 2023, spiking in the post-COVID era. This has spurred increased cybersecurity demand and spend, driving investment in the space.

Shifting Attack Surfaces
Many GenAI apps were built without security in mind, increasing potential vulnerabilities. AI researchers continue to advance data security, but much of what underpins a working LLM remains vulnerable.

Use of AI by Bad Actors
AI increases efficiency not only of legitimate enterprises, but also of cybercriminals. Today, scammers can generate believable phishing emails at scale. In 2023 alone, phishing emails increased 13-fold.[1]

Emerging CyberAI Ecosystem

Formation of CyberAI Startups
New companies are forming an emerging CyberAI ecosystem. Between 2020 and 2023, the number of CyberAI companies formed was nearly 2x the number from the previous four-year period.

VCs Investing in CyberAI Companies
Capital is flowing to these new CyberAI companies. Venture capital (VC) investors continue to pump money into cybersecurity and AI startups, allowing them to maintain high burn and focus on growth.

Investor Interest in CyberAI Funds
Recognizing growth in the sector, investors are strategically focusing on CyberAI. Among US VC funds raised in 2023, those mentioning AI as a specialty were nearly twice as likely to close their funds as those that didn't.

Notes: 1) According to SlashNext, there was a 1,265% increase in phishing from Q4 '22 to Q3 '23.
Sources: The New York Times "Microsoft to Invest $10 Billion in OpenAI," IBM "IBM Acquires Manta Software Inc.," Federal Bureau of Investigation "Internet Crime Report 2023," SlashNext's "The State of Phishing 2023," PitchBook Data, Inc. and SVB analysis.

Tec(h)tonic Shifts in the Making

In the early 2000s, every pitch deck had to give a nod to the company's mobile strategy as smartphones became ubiquitous. **Today, ChatGPT has ushered in a new era of AI.** There are now more than 7,500 US VC-backed companies that have AI as part of their goods and services, and investors are increasingly incentivized to focus their attention on this space.

While not the first LLM, ChatGPT brought GenAI to the masses, marking a long-term tectonic shift in how businesses and consumers interact with the technology. Against this backdrop, companies are eagerly adopting AI to realize the potential automation and augmentation of human working hours.

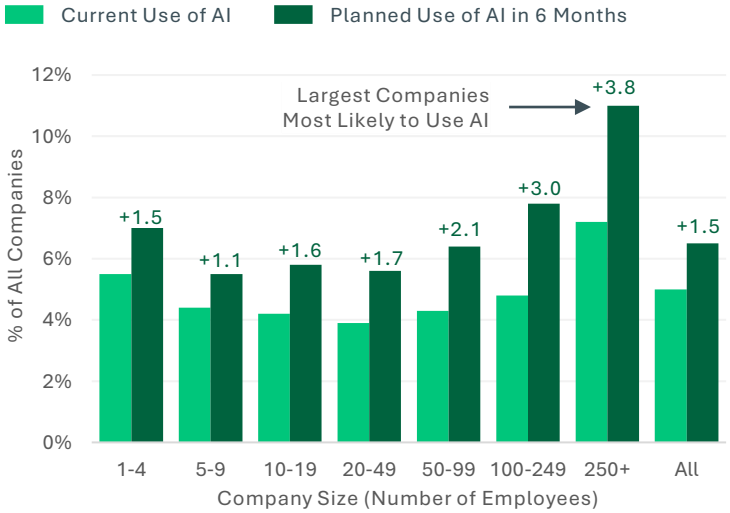
At the same time, **deploying new AI technology is expensive, both in terms of implementation and security.** This could be why the largest companies are most likely to use or plan to use AI in the near term. Cybersecurity is a primary concern among companies, as the aggregate losses from cybercrime have risen nearly nine-fold in the past six years alone. To combat this, companies are investing an increasing amount in cybersecurity, with the bulk going to security services.

While the recent spike in AI investment may reflect a bit of bluster, AI has the potential to become a horizontal platform creating efficiency gains across all industries.

svb Silicon Valley Bank
A Division of First Citizens Bank

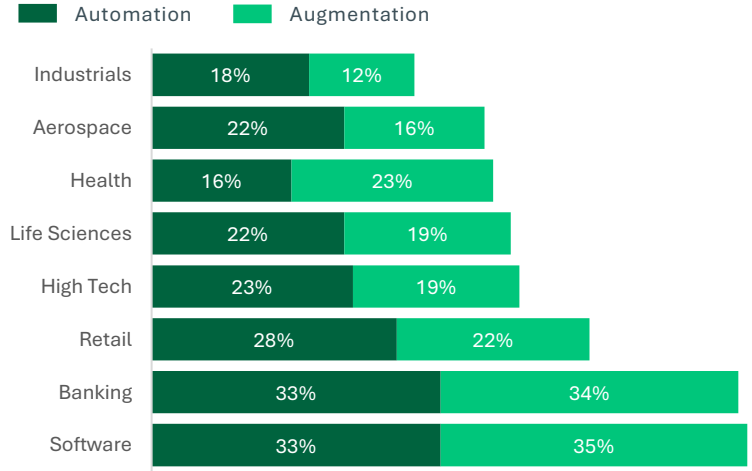
Companies' Use of AI Expected to Grow

Percentage of Companies Using or Planning to Use AI[1]



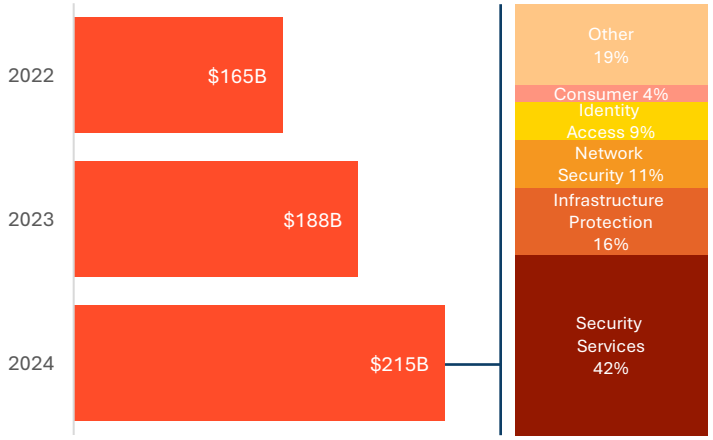
Working Hours Impacted by AI

Percent of Working Hours in Scope for Automation or Augmentation Due to GenAI[2]



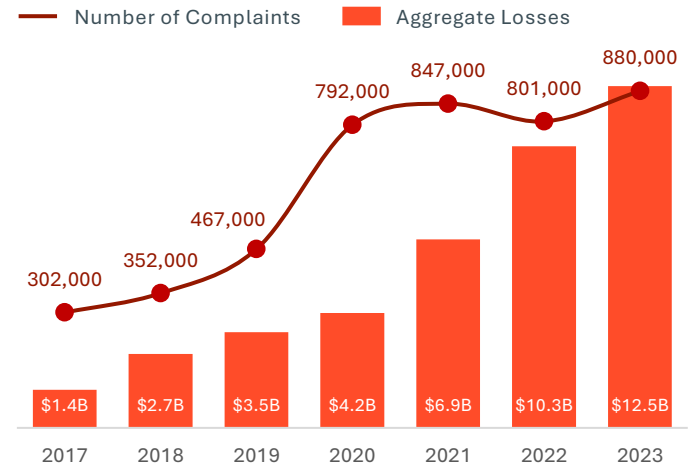
Cybersecurity Spending Skyrockets

Security and Risk Management End-User Spending Worldwide



Cybercrime Losses Continue to Climb

Number of US Cybercrime Complaints, Estimated Losses by Year[3]



Notes: 1) Companies reporting use of AI in producing goods and services in the last two weeks (currently using AI) or that plan to use AI in the next six months. Sample includes US-based respondents to the Business Trends and Outlook Survey. Employer size buckets defined by the US Census Bureau. 2) Estimates based on National Statistical Institutes and O*NET via Accenture Research. 3) Complaints to the FBI's Internet Crime Complaint Center.

Sources: US Census Bureau, PitchBook Data, Inc., Accenture "Work, Workforce, Workers," Gartner Forecasts on Global Security and Risk Management Spending, Federal Bureau of Investigation "Internet Crime Report 2023" and SVB analysis.

Dual Growth of GenAI and Cyber

What are investors really investing in when they invest in AI? Most of the companies in the AI universe are not developing the core technology, but rather finding ways to apply it. Part of this is due to an urgency among startups to present themselves as AI-enabled even if AI is not their core offering. **Among the nearly 700 US companies involved in AI that have raised more than $50M, less than one-third are building LLMs or creating new computing infrastructure.**[1]

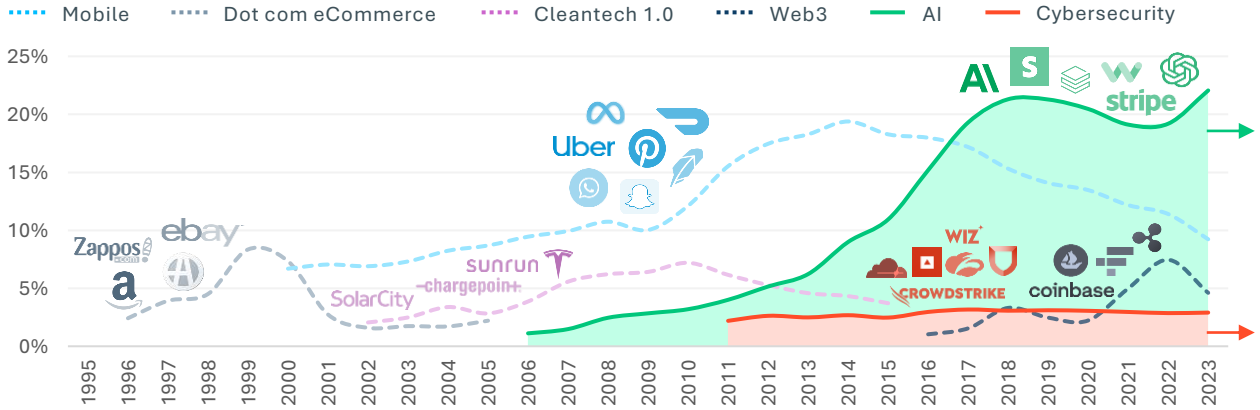
Still, leveraging AI — especially at the enterprise level — is a complex endeavor, and **cybersecurity is stalling broader AI adoption.** At the forefront of this risk is data security. Whether in the databases or code underlying AI applications, security can often be weak, exposing both developers and end users to risk. In fact, in a survey of 281 research studies on this topic, researchers identified several vulnerabilities in LLMs, ranging from security and privacy concerns to inherent model vulnerabilities such as data poisoning and backdoor attacks.

AI researchers continue to make advancements in data security to address these weaknesses, but **much of what underpins a working LLM remains vulnerable.** Cybersecurity companies that address these issues have attracted more investment over the past decade. However, scaling can be difficult among early-stage cybersecurity firms, as corporates often purchase startups for their tech before the startups can fully scale and widely deploy their security products.

svb Silicon Valley Bank
A Division of First Citizens Bank

A Once-in-a-Decade Cycle for AI While Cyber Holds Steady

VC Deals in a Given Technology[2] as a Percentage of all US VC Deals



The arrival of ChatGPT supercharged AI investing. Post-ChatGPT, AI investing has become its own beast.

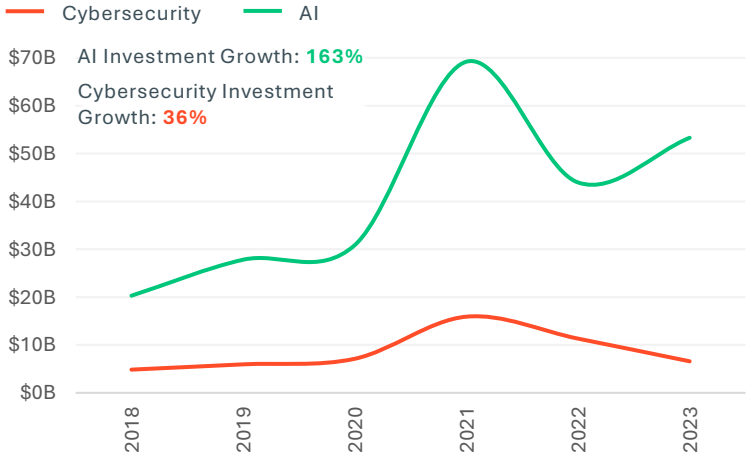
R-Squared: AI VC & All VC

Pre-ChatGPT	0.84
Post-ChatGPT	0.47

Cyber investment has held steady as many cyber startups get scooped up by larger companies before they can scale.

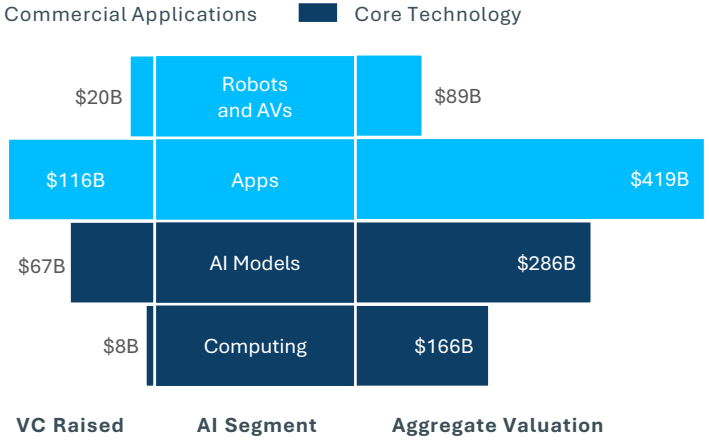
VCs Show Outsized Interest in AI

US VC Investment in AI and Cybersecurity Companies[2]



Investing in the AI Tech Stack

US VC Investment and Valuations for AI Companies with at Least $50M Raised in Single Round Since Jan. 2021[1]



Notes: 1) Aggregated VC investment and valuations for US companies that have raised more than $50M in VC with the latest deal since January 2021. Segments based on PitchBook Data, Inc. taxonomy. 2) Technology segments determined using PitchBook Data, Inc.'s vertical taxonomy.

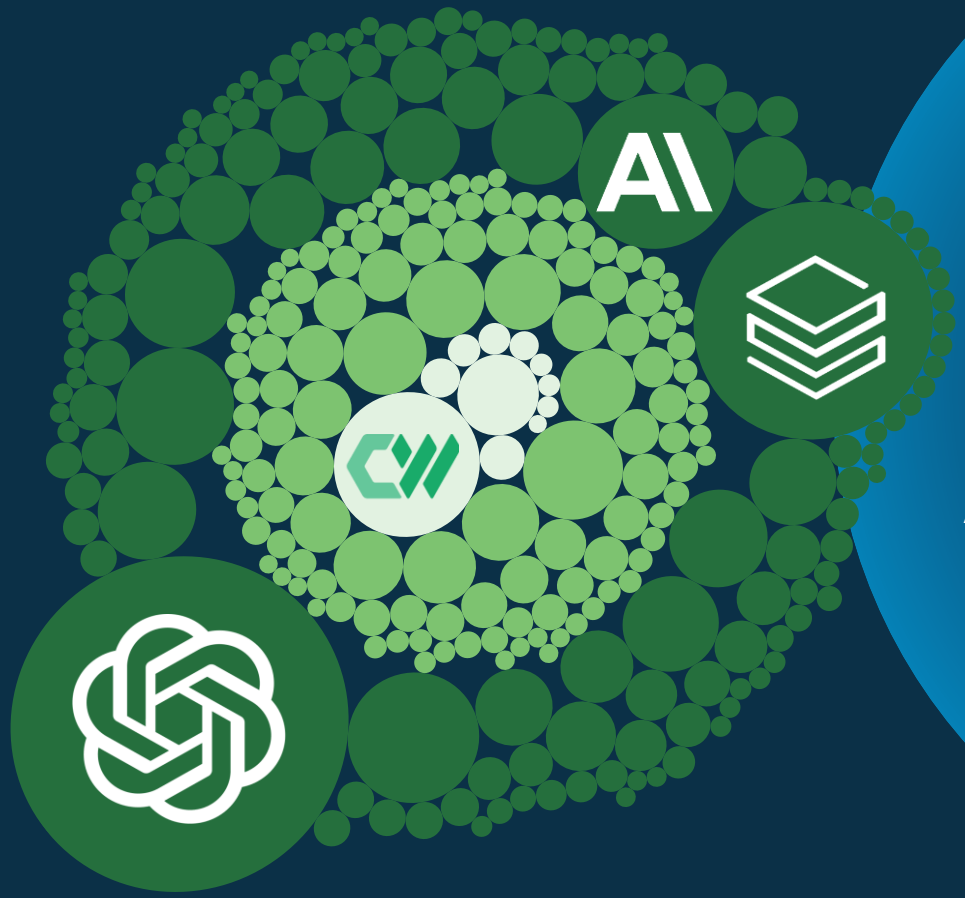
Sources: Yifan Yao et al. "A Survey on Large Language Model Security and Privacy" (High-Confidence Computing, 2024), PitchBook Data, Inc. and SVB analysis.

The Next Frontier: Exploring the CyberAI Universe

US VC-Backed Companies by Latest Valuation[1]

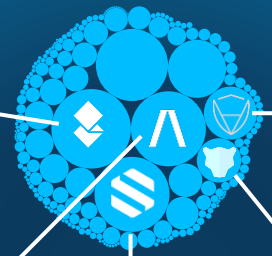
AI

Including model development, vertical applications and computing infrastructure.



CyberAI

Tools and platforms that leverage GenAI to address vulnerabilities in AI infrastructure, models and applications or to defend against external, GenAI-driven threats and attacks.



Socure
is a digital identity verification platform. The company's predictive analytics platform applies AI techniques to verify identity and authenticity.

CertiK
is a developer of a formal verification technology designed to protect and monitor blockchain protocols and smart contracts.

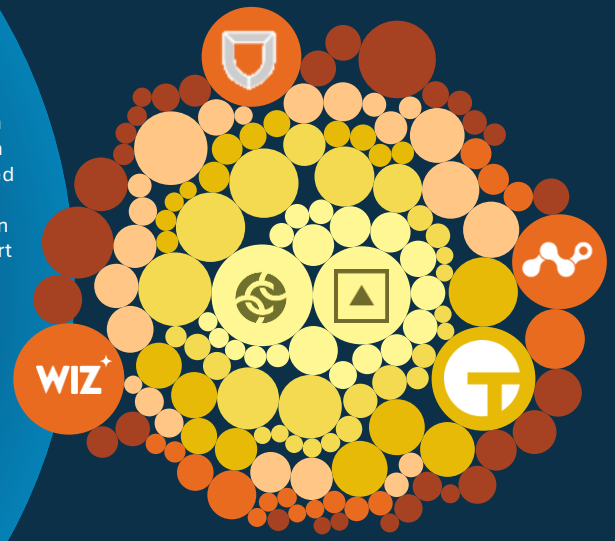
Abnormal Security
is a developer of a cloud email security platform designed to prevent cybercrimes using an AI-based approach.

Sandbox AQ
is a developer of AI quantum software including an enterprise cryptography management solution.

Panther
is an infrastructure security and compliance platform that uses AI to detect and respond to breaches.

Cybersecurity

Including security operations, network security, identity & access management, endpoint security, data security and application security.



Scale:
= $10B
= $2.3B
= $3.7B

svb Silicon Valley Bank
A Division of First Citizens Bank

Notes: 1) For US VC-backed artificial intelligence/machine learning (AI/ML) and cybersecurity companies. Only companies with valuations over $250M are shown for AI/ML and cybersecurity companies. AI/ML and cybersecurity verticals and subsegments determined by PitchBook Data, Inc. taxonomy. Circles represent valuation scale within each category (AI/ML, cybersecurity and CyberAI); each category has its own scale.

Sources: PitchBook Data, Inc. and SVB analysis.

Fundraising & Investment

Money Flows to CyberAI Startups

Funds focused on AI and cybersecurity have been a bright spot in an otherwise dull VC fundraising environment. These funds accounted for 17% of all 2023 vintage US VC funds. In some sense, this is not surprising. Among funds that raised in 2023, **those mentioning AI as a specialty were nearly twice as likely to close their funds as those that didn't.**[1]

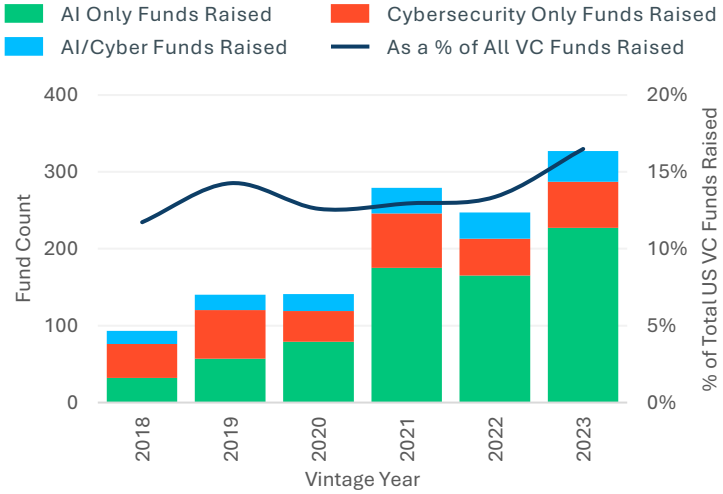
These funds have a broad base of companies to pursue, and investment into AI companies has skyrocketed over the past several years. Between 2020 and 2023, the number of CyberAI companies formed was nearly 2x the number formed in the previous four-year period. Deal activity has kept pace, at least at the early stage.

Besides the well-known VCs, **corporates have funded much of the innovation and acquisition in CyberAI.** Palo Alto Networks, for instance, has completed more than 15 acquisitions since 2018 when Nikesh Arora took over as CEO. This acquisition streak is part of Arora's strategy to develop a cybersecurity platform, especially in the age of AI, noting in a 2023 interview that GenAI "should definitely create more opportunity...not just for security but for tech companies." The corporate focus on consolidation is not unique to Palo Alto Networks, with other notable acquisitions such as CrowdStrike's March 2024 purchase of Flow Security, a cloud data runtime security solution, to bolster the parent's product offerings.

svb Silicon Valley Bank
A Division of First Citizens Bank

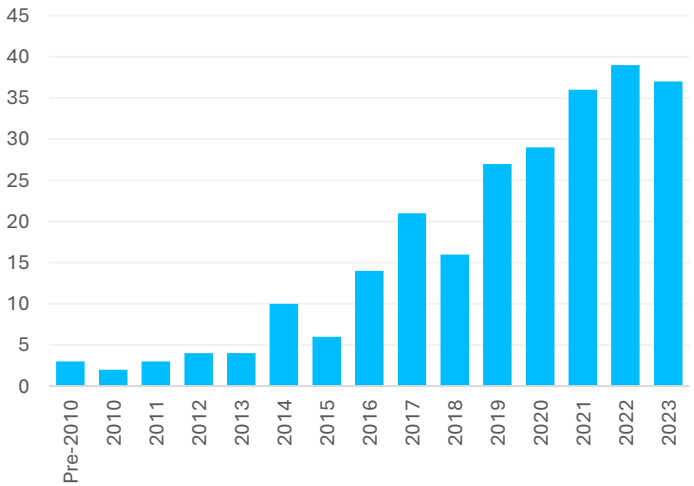
Fundraising for Hot Sectors Heats Up

US VC Funds Raised by Vintage Year with AI or Cyber Focus[1]



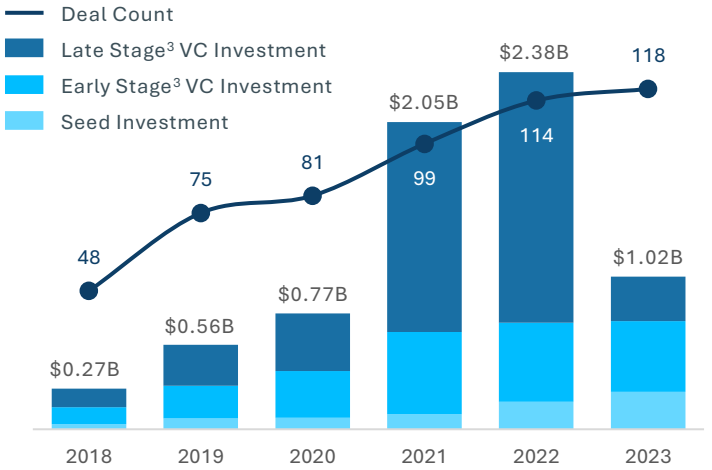
Company Formation Continues to Tick Up

Number of US CyberAI Companies Formed[2] by Year



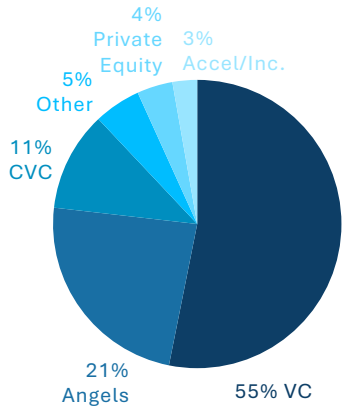
Deal Activity Resilient at the Early Stage

Deal Count and VC Investment into US CyberAI Companies



VCs and CVCs Lean into CyberAI

Top Disclosed[4] Investors by Deal Count Since 2021



Notes: 1) US-based VC funds with a stated sector focus of either AI or cybersecurity. "AI/Cyber" refers to funds that had a stated focus in both categories. 2) Company formation year determined using the founding date according to PitchBook Data, Inc. or its first financing date if the founding year is unavailable. 3) Stage defined using PitchBook Data, Inc.'s definition. Late stage defined as deals done five years after a company's founding. 4) Only includes VCs that publicly disclosed investments. CyberAI VCs are aggregated from PitchBook Data, Inc. and Momentum Cyber data.

Sources: Microsoft, CrowdStrike, Momentum Cyber's H1 2023 Cybersecurity Market Review, The Channel Co. CRN, Preqin, PitchBook Data, Inc. and SVB analysis.

CyberAI Bucks Startup Trends

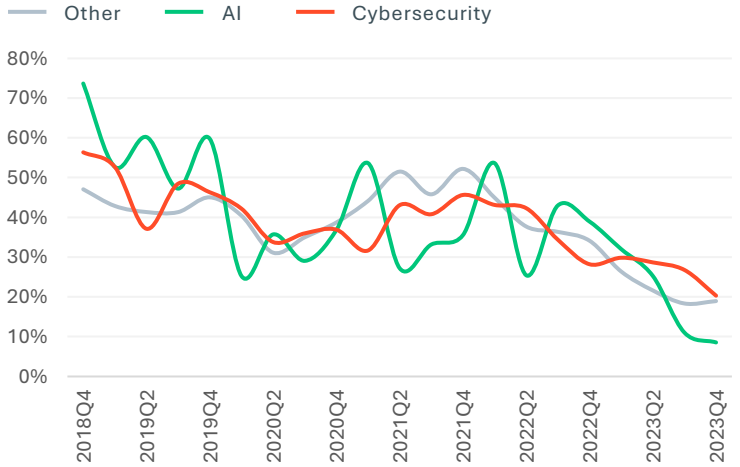
In 2022, VCs began issuing instructions to portfolio companies to extend runway, cut burn and focus on efficiency over growth, typified by a16z's "A Framework for Navigating Down Markets" posted in May 2022. Since then, founders have largely followed their advice. Beginning in 2022, revenue growth began trending down for VC-backed tech companies. At the end of 2021, annual revenue growth hovered around 40%-50%. By the end of 2023, it was less than half that. **Companies are increasingly focused on profitability, often by shrinking expenses or cutting growth initiatives.** This strategy is reflected in lower EBITDA margins as well.

For AI and cybersecurity companies, however, it is a different story. These companies continue to have burn that often far exceeds that of other VC-backed tech companies, and **AI companies have actually increased their runway over the past three years,** thanks to a favorable investment environment. Still, companies in the space are dealing with the same declining revenue growth seen in other sectors. Part of this is defining a new sales process. While cybersecurity firms typically sell to a CISO, **CyberAI companies have a less certain sales path.** Many companies today are selling into chief risk officers (CROs), but going forward we might expect to see the establishment of more AI committees to lead the acquisition of CyberAI solutions at an enterprise level.

svb Silicon Valley Bank
A Division of First Citizens Bank

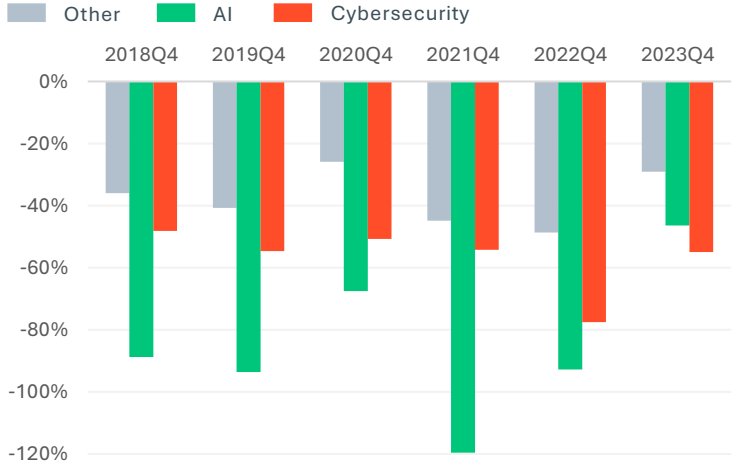
Revenue Growth May Have Bottomed

Median Revenue Growth by Tech Sector[1]



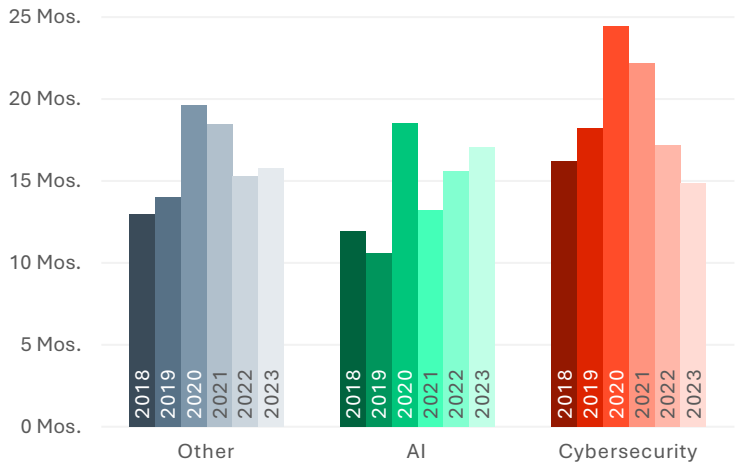
Operating Margins Continue to Improve

Median EBITDA Margin by Tech Sector[1]



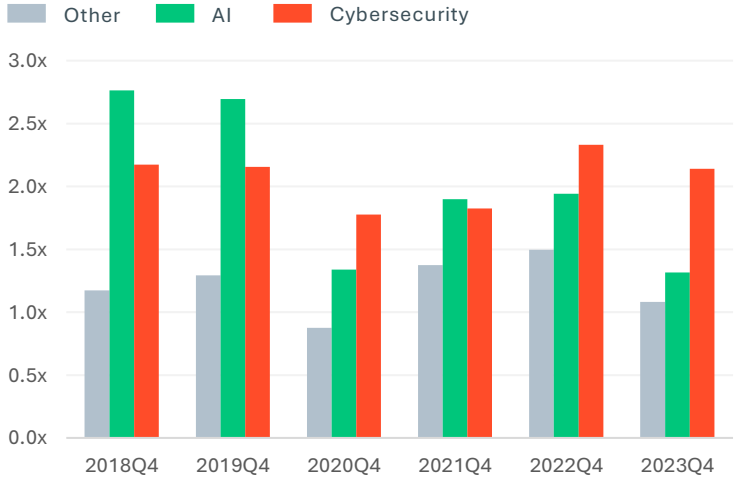
Runway Muted Across Sectors, Except AI

Median Cash Runway by Tech Sector[1, 2]



Burn Multiple Improves Modestly

Median Burn Multiple by Tech Sector[1]



Notes: 1) Sector definitions based on SVB proprietary taxonomy. Data only for US companies with more than $5M in revenue.
2) As of Q4 of each year.
Sources: SVB proprietary data and SVB analysis.

Survey Results

An Urgency to Deploy GenAI

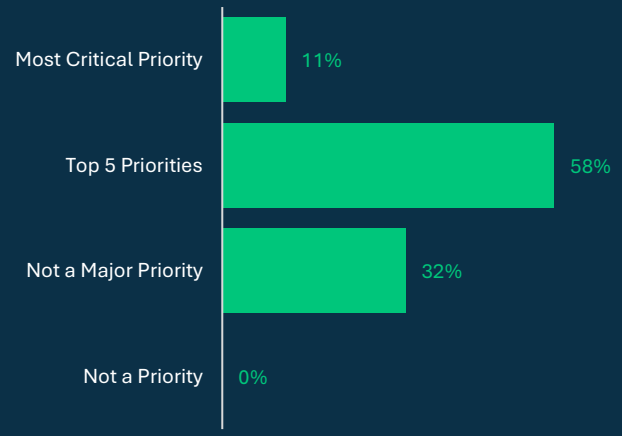
There is an urgency to leverage GenAI within organizations, according to a panel of CISOs polled for this report.[1] **More than two-thirds of CISOs report that GenAI is among the top five priorities at their organizations,** putting increased pressure on CISOs to strategically manage the rollout. To manage implementation and the security concerns associated with these new GenAI tools, **most CISOs are focused on developing security capabilities in-house.** At a high level, this is to maintain control and minimize external risks. Still, integrating external solutions can be significantly easier than developing new capabilities internally, and 74% of CISOs see this as important in the near term.

Developing and deploying GenAI tools, however, is only half the battle; securing these systems while in use is critical. Fortunately, **most CISOs either have a specific GenAI policy or are applying an existing general framework successfully.** CISOs often turn to traditional cybersecurity tools, with some seeing GenAI as more of a capability vs. a specific toolset to secure against. Others continue to evaluate their options, seeking tools that enable security of various aspects of LLMs, from training data to live usage. In terms of specifics, CISOs report a wide range of tools used for GenAI security. This could reflect the industry's early stage of development, with more consolidation likely in the future.

svb Silicon Valley Bank
A Division of First Citizens Bank

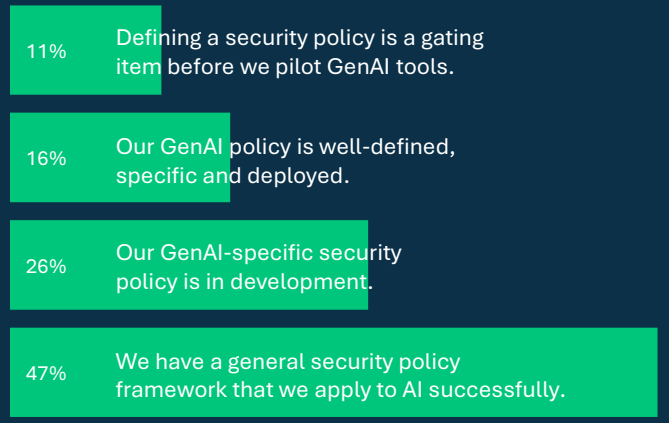
GenAI Among Companies' Top Priorities

Q: How much of a priority to your organization is adopting GenAI into your workflows or product offerings?



Most Have Successful AI Security Policies

Q: Which statement best describes your organization's security policy for GenAI?



Focus on Developing Capabilities In-House

Q: How important is each in leveraging AI?

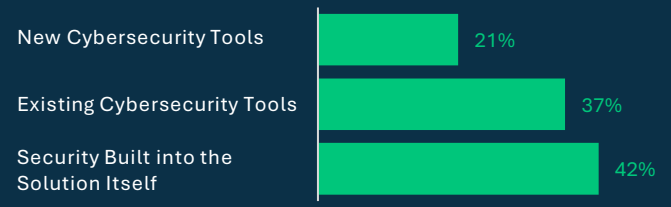
	Developing Capabilities In-House	Leveraging Existing Vendors	Adopting New GenAI Solutions
Very Important	42%	21%	21%
Somewhat Important	37%	53%	37%
Neutral	11%	16%	37%
Somewhat Unimportant	11%	5%	5%
Very Unimportant	0%	5%	0%

Q: How important do you expect each to be in the next 3 years?

	In-House	Existing	New
Very Important	42%	32%	26%
Somewhat Important	42%	47%	47%
Neutral	11%	16%	21%
Somewhat Unimportant	0%	5%	0%
Very Unimportant	5%	0%	5%

Solutions Sought from a Variety of Sources

Q: If you have been adopting GenAI solutions, how have you been primarily securing those solutions?



Q: What are the primary tools you are using to secure GenAI solutions, to the extent that you are doing so?[2]

Access Controls	CSPM	In-house Built Platform
Abnormal Security	DLP	Microsoft Copilot
AWS	DSPM	Netskope
Calypso AI	GitHub Copilot	Network Firewalls
CASB	IAM	User/Data Monitoring

Notes: 1) SVB survey fielded in April 2024 of a curated group of CISOs with experience implementing enterprise GenAI cybersecurity solutions.
2) Selected responses from survey respondents.
Sources: SVB survey and SVB analysis.

AI Brings Change in Cybersecurity Stack

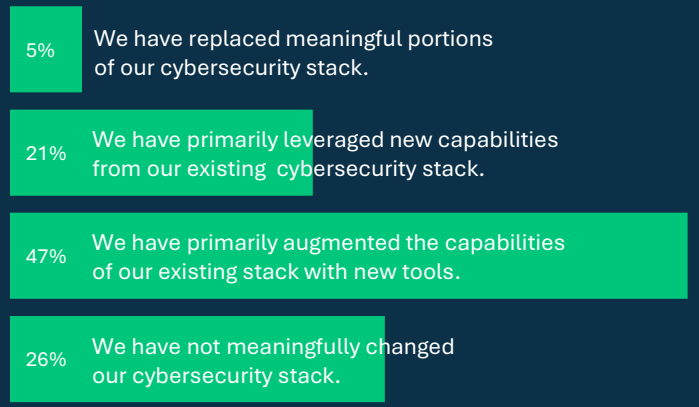
As enterprises deploy GenAI tools at scale, **CISOs are reacting quickly to update their cybersecurity positioning** and guard their organizations from a wider attack surface. Just 18 months post-release of ChatGPT, 74% of CISOs have already changed the composition of their cybersecurity stack, with the majority of that group primarily augmenting their existing stack with new tools. Among the 26% who have not yet changed their cybersecurity stack, nearly all will add new cybersecurity tools within the next three years. **This is a growth opportunity for CyberAI startups, which are well-poised to fill this gap.**

When surveyed,[1] CISOs report a wide variety of AI tools that are impacting their organizations, and fortunately for CyberAI firms, CISOs expect a 13% increase of cybersecurity budgets on average. This suggests that there is a wide opportunity set for CyberAI startups to address security issues around everything from code generation tools to knowledge management systems. One of the VCs interviewed for this report explained the opportunity for CyberAI solutions: "Attack campaigns that would have been carried out over months will be compressed to days or hours. We have very little defense against these 'intelligent attacks.' Automation in our defenses is becoming more essential. **The future will increasingly become AI versus AI."**

svb Silicon Valley Bank
A Division of First Citizens Bank

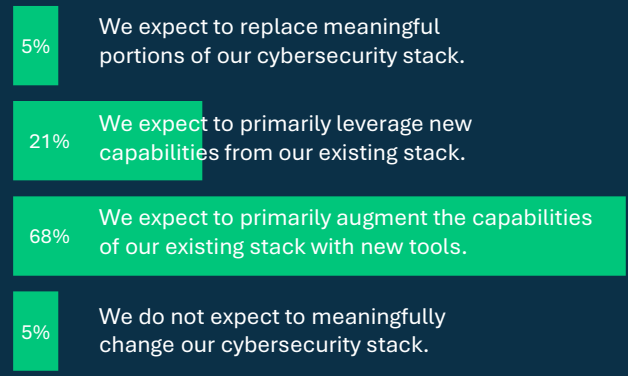
CISOs Reacted Quickly to GenAI

Q: How has the increased proliferation of GenAI affected the composition of your cybersecurity stack to date?



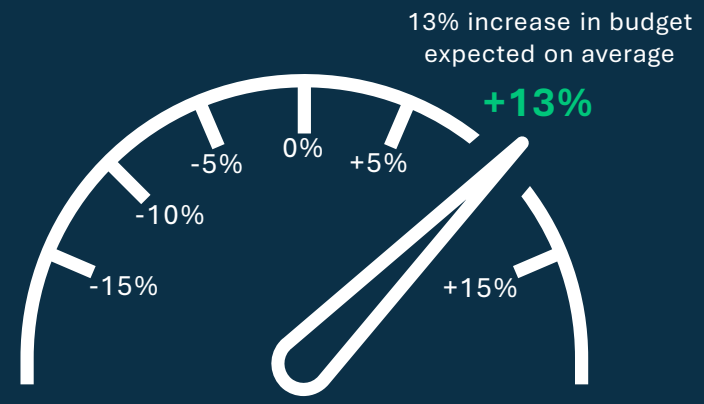
Almost All CISOs Will Change Cybersecurity Stack Within 3 Years

Q: How do you expect the continued proliferation of GenAI to affect the composition of your cybersecurity stack in 3 years?



More Cybersecurity Spend Is Coming

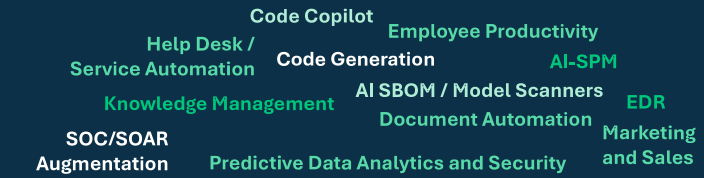
Q: How has the increased proliferation of GenAI changed your cybersecurity budget?



AI Tools Expected to Bring Impact

Q: What are the AI tools or application categories you expect to have the biggest impact on your organization?[2]

Application Categories



Tools

Notes: 1) SVB survey fielded in April 2024 of a curated group of CISOs with experience implementing enterprise GenAI cybersecurity solutions. 2) Selected responses from survey respondents.
Sources: SVB survey and SVB analysis.

Exits

Looking Ahead to CyberAI Exits

CyberAI is an emerging space, still too early in the development cycle for many significant exits. But as investors and founders approach the industry, how are they thinking about future exit opportunities?

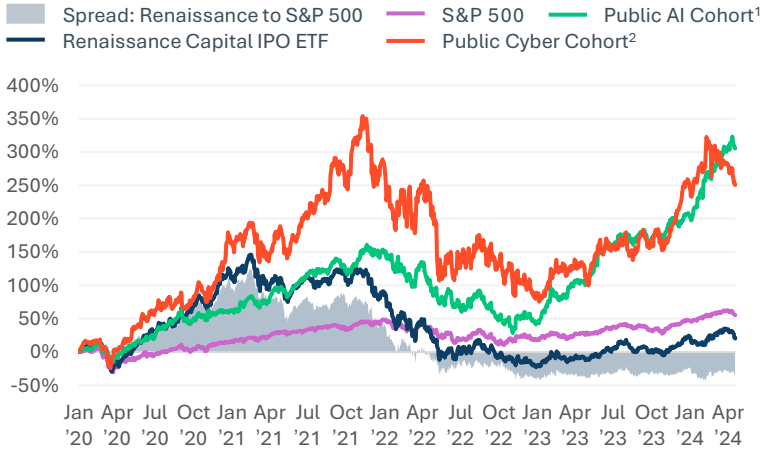
Early in the development of a new vertical, M&A tends to be the most common exit route. CyberAI is proving to be no different. Among recent large deals, Gem Security, a cloud detection and response firm, was bought by Wiz for $350M, and Silk Security, a cyber risk platform, was bought by Armis for $150M. Strong performance by related public companies and significant cash on hand provide strong tailwinds for additional acquisition activity.

IPOs could take more time, however. One interviewee noted that "It is too early to tell if [cybersecurity and AI] categories can support large IPOs, but I'd bet the early demand from customers will drive approximately $100M+ in M&A." PitchBook Data, Inc.'s exit expectation analysis for the CyberAI cohort suggests that while most have a high probability of a successful exit, few will be via IPO. Still, it could just be a matter of time, with one interviewee predicting that "For IPOs, the time horizon is more like 3-5 years or more." The industry is in the early stages of growth and development, with one expert explaining, "AI will dramatically change cyber, but it will not happen overnight. **We are on a 3-5 year journey, and we are barely one year into it."**

svb Silicon Valley Bank
A Division of First Citizens Bank

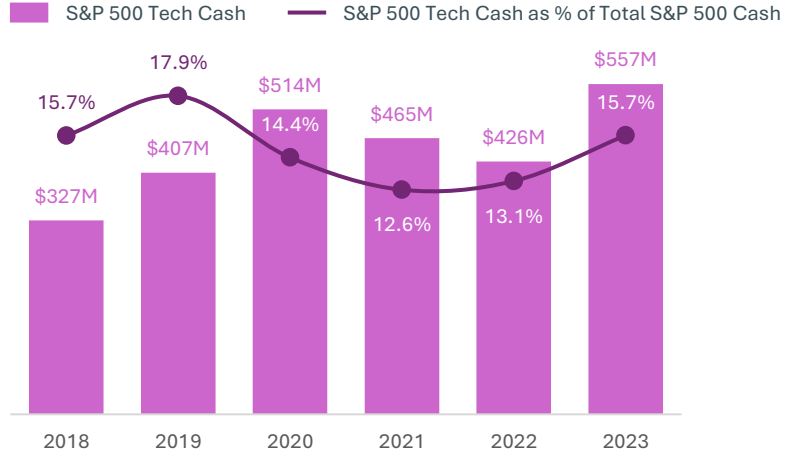
Big Tech Lifts Public Markets

Returns of AI Stocks, Cyber Stocks, Tech IPOs and S&P 500



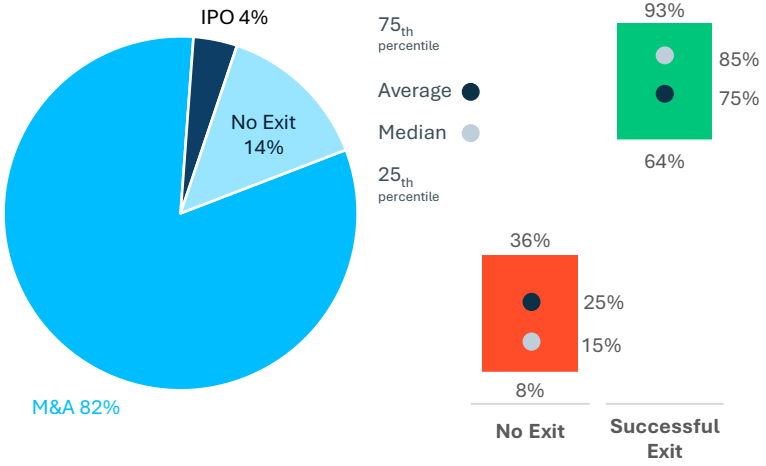
Growing Cash On Hand Could Boost M&A

S&P 500 Tech Cash and as Percent of Total S&P 500 Cash



Exits Expected for CyberAI Cohort

Expected Exit Route and Probability of Successful Exits3



Experts Split on Exit Expectations

Select Quotes from Interviews

"AI is going to raise the 'table stakes' for cybersecurity companies. Those that integrate the new functionality effectively will differentiate themselves, deliver more value to their customers and will be better received in the capital markets, be it M&A or IPO."

"Ecommerce on the internet started in 1996, but it was not until an industry reboot that in 2002 ecommerce took off as we know it today. CyberAI is still in 1996 or 1997. **We are still in the experimentation or forming stage."**

Notes: 1) Public AI cohort is an equal weighted basket of public AI companies including META, MSFT, GOOGL, AMZN, NVDA and TSM. 2) Public cyber cohort is an equal weighted basket of public cyber companies including CRWD, ZS, OKTA, S, NET, CYBR, PANW and FTNT. 3) Exit probabilities for each company are calculated by PitchBook Data, Inc.'s exit probability methodology.

Sources: CTech, Armis, S&P Capital IQ, PitchBook Data, Inc. and SVB analysis.

Authors and Methodology

Lead Authors

Andrew McCarty
Vice President
Tech Banking
Silicon Valley Bank
amccarty@svb.com

Andrew McCarty is a Senior Vice President on SVB's NorCal Enterprise Software team. In this role, he advises a portfolio of venture-backed enterprise software clients in the San Francisco Bay Area from seed to pre-IPO. Andrew advises startups and their founders on creative banking and financing solutions while leveraging SVB's network to maximize clients' probability of success.

Before his current role, Andrew spent six years on SVB's NorCal Credit Solutions team, specializing in structuring and deploying debt facilities for enterprise software clients.

Andrew graduated from Santa Clara University with a bachelor's degree in history and political science and a minor in economics.

Emma Eschweiler
Director
Investor Coverage
Silicon Valley Bank
eeschweiler@svb.com

Emma Eschweiler is a Director for SVB's Investor Coverage & Business Development team. She is responsible for the growth and development of institutional VC and corporate relationships on behalf of SVB, with a focus on partners making direct investments, acquisitions or partnerships principally within the enterprise software ecosystem, including areas such as cybersecurity, developer tools, applications, data infrastructure and open-source initiatives.

Before her current role, Emma was a vice president in SVB's NorCal Enterprise Practice, where she managed a portfolio of growth-stage, venture-backed enterprise software clients in the region. Emma earned her bachelor's degree in government and global studies from Colby College and continued her education at Georgetown University and Sciences Po in France.

Natalie Fratto
Managing Director
Investor Coverage
Silicon Valley Bank
nafratto@svb.com

Natalie Fratto is a Managing Director on SVB's Investor Coverage & Business Development team. In this role, she seeks to be a thought partner to general partners on the financial journeys of both their portfolio companies and their firms.

Earlier in her finance career, Natalie opened the SVB Canada office and led alternative investing into venture funds as part of the Corporate Development & Strategy team at Goldman Sachs. Before entering finance, she led operations for a Y Combinator-backed services marketplace company and spent time as a management consultant focused on M&A within the semiconductor industry.

Ever passionate about new technologies, Natalie writes and contributes technology pieces for *Fortune*, *Motherboard* and other tech outlets. Her viral 2019 TED Talk on adaptability has been viewed four million times and was one of the top 10 most-watched talks of the year.

Market Insights Team Authors

Andrew Pardo, CFA
Senior Analytics Researcher
SVB Market Insights
Silicon Valley Bank
apardo@svb.com

Jake Ledbetter, CFA
Senior Analytics Researcher
SVB Market Insights
Silicon Valley Bank
jledbetter@svb.com

Methodology

Information for this report was gathered from a variety of sources.

Quantitative data was sourced from proprietary SVB databases, industry publications and data providers such as PitchBook Data, Inc. Quotes and many of the insights included in the commentaries are sourced from conversations with investors and operators in the CyberAI space, all of which were conducted during April and May 2024.

Survey respondents were recruited from a curated list of CISOs who are SVB clients. Each of the CISOs has experience leading organizational adoption of new technologies and brings a wealth of experience in the CyberAI space. All respondents are US-based.

About Silicon Valley Bank

Silicon Valley Bank (SVB), a division of First-Citizens Bank, is the bank of some of the world's most innovative companies and investors. SVB provides commercial and private banking to individuals and companies in the technology, life science and healthcare, private equity, venture capital and premium wine industries. SVB operates in centers of innovation throughout the United States, serving the unique needs of its dynamic clients with deep sector expertise, insights and connections. SVB's parent company, First Citizens BancShares, Inc. (NASDAQ: FCNCA), is a top 20 U.S. financial institution with more than $200 billion in assets. First Citizens Bank, Member FDIC. Learn more at svb.com.

Silicon Valley Bank

www.svb.com

See complete disclaimers on the following page.

Disclaimers

The views expressed in this report are solely those of the authors and do not necessarily reflect the views of SVB.

This material, including without limitation to the statistical information herein, is provided for informational purposes only. The material is based in part on information from third-party sources that we believe to be reliable but which has not been independently verified by us, and, as such, we do not represent the information is accurate or complete. The information should not be viewed as tax, accounting, investment, legal or other advice, nor is it to be relied on in making an investment or other decision. You should obtain relevant and specific professional advice before making any investment decision. Nothing relating to the material should be construed as a solicitation, offer or recommendation to acquire or dispose of any investment, or to engage in any other transaction.

All non-SVB named companies listed throughout this document, as represented with the various statistical, thoughts, analysis and insights shared in this document, are independent third parties and are not affiliated with Silicon Valley Bank, a division of First-Citizens Bank & Trust Company. Any predictions are based on subjective assessments and assumptions. Accordingly, any predictions, projections or analysis should not be viewed as factual and should not be relied upon as an accurate prediction of future results.

Investment Products:

Are not insured by the FDIC or any other federal government agency	Are not deposits of or guaranteed by a bank	May lose value