Rising In Cyber 2025 Report

June 2025

Notable Capital

Morgan Stanley

Table of Contents

Introductory Letter

While AI might be what business leaders are all talking about publicly, security is dominating the conversations in private. Companies remain excited about the potential of AI to transform their businesses but are also concerned that AI will inject unmanageable amounts of risk, leading to expensive breaches and damaging leaks that could jeopardize the future of the company.

While AI is a new challenge, it's just one of many factors making it harder for organizations to defend their IT environments. Cloud workloads are growing at a rapid clip, while the number of third-party software tools continues to multiply. Traditional phishing attacks, insider threats, and other tactics that have long plagued security teams remain as troublesome as ever.

As breaches get more common and more expensive, organizations are increasingly investing in specialized tools to help in areas like identity management, application security, and endpoint detection. This has led to significant growth in the cybersecurity market over the past decade. Today, the public cybersecurity market tops $625 billion in market cap, according to a Morgan Stanley analysis, up from $116 billion just 10 years ago. And in the private market, cybersecurity continues to dominate investor attention. Just this year in 2025, Adaptive Security raised a $43 million Series A, NinjaOne raised a $500 million Series C extension, and Chainguard raised a $356 million Series D.

Meanwhile, a robust M&A market continues to reshape the sector. In fact, 51 of the 75 cybersecurity deals valued at greater than $200 million since 2022 were driven by strategic acquisitions and the interest for innovation from existing players in the ecosystem. This activity signals the ongoing need for large vendors to deliver specialized security solutions to customers through their broader platforms.

All of this activity reflects the new reality: cybersecurity is fundamental to modern society. As a result, it's now a board-level conversation within most businesses, further putting the spotlight on the Chief Information Security Officer (CISO), a role now indispensable to any modern C-Suite. Amid an onslaught of human and machine-generated attacks, CISOs are being asked to do more with less: less money, fewer people, and less time. This creates an immense opportunity for forward-looking security leaders to deploy AI in ways that combine human and machine intelligence to empower security experts to make maximum use of their unique skill sets.

Our Rising in Cyber 2025 Report aims to unpack the market activity and showcase how CISOs and founders are thinking about the future of cybersecurity, while highlighting the startups making it a reality.

Oren Yunger
Managing Partner, Notable Capital

Dave Chen
Head of Global Technology Investment Banking, Morgan Stanley

Executive Summary

The shift to an agentic AI future is exciting, but it introduces serious new security challenges. For CISOs, it means tackling long-standing problems, like application security and endpoint detection, while also confronting emerging threats, like authorizing and authenticating the identities of the growing number of machines accessing the network.

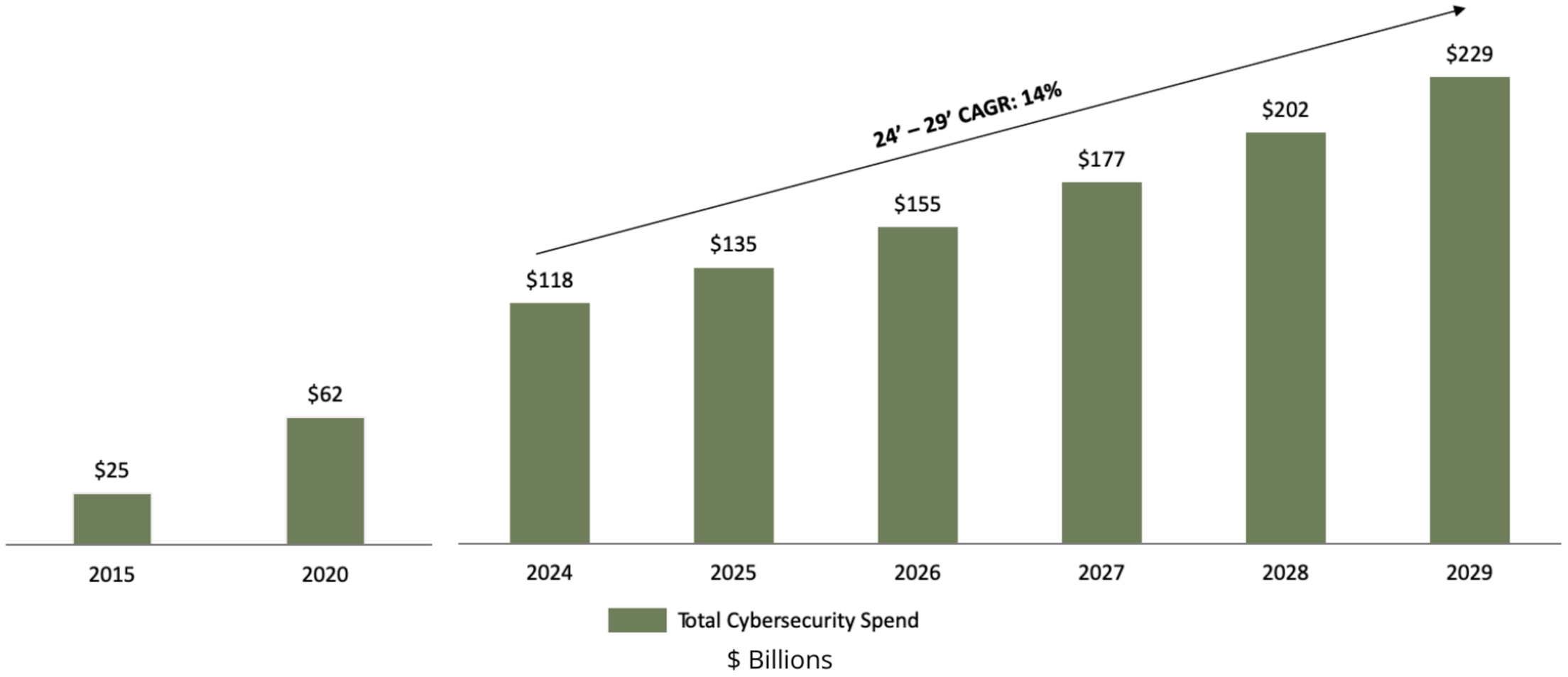
As a result, the need for specialized tools to help prevent, detect, and respond to incidents is growing. Overall, cybersecurity spending is expected to nearly double by 2029, rising to $229 billion. The M&A market also remains active. Whether it's Google acquiring Wiz for $32 billion earlier this year or Cisco acquiring Splunk for $28 billion in 2023, large players are looking to expand their solution offerings and keep up with the rapidly evolving threat ecosystem

For startups, this environment has created opportunities for liquidity at high multiples, as evidenced by Palo Alto Networks' acquisition of Protect AI announced earlier this year in 2025, Wiz's acquisition of Gem Security in 2024, and Palo Alto Networks' acquisition of Talon Cyber Security in 2023. In each of these transactions, the startups were acquired for over $300 million despite having less than $5 million in revenue. One thing is clear: In the rapidly changing cybersecurity market, acquirers are willing to pay a significant premium for the best tech – and the best teams.

"Early-stage is where all the innovation is happening. For the last 20 years, security innovation has been through acquisition. Startups are the R&D labs of the larger security companies," said Elastic CISO Mandy Andress.

The Rising in Cyber 2025 Report offers a clear snapshot of where cybersecurity is headed. Based on survey insights from leading CISOs and market data from Morgan Stanley, it highlights what security leaders are prioritizing, where capital is flowing, and the most innovative startups that are pushing the field forward, giving investors, operators, and founders a way to navigate one of tech's fastest-moving frontiers.

Forecasted Cybersecurity Spend Is Expected To Reach ~$230B In 2029



Source: Morgan Stanley derived from IDC

The State of Cybersecurity Market

Nearly every segment of the cybersecurity market (venture funding, M&A, public market valuation) is larger today compared to just several years ago. And with continued growth across each, the market evolution is unlikely to stop in the coming years.

Based on a Morgan Stanley analysis, we identified several emerging themes in the public market today that could ultimately upend the existing industry dynamics, including:

Complex Needs, Booming Market

Growing demand for highly-capable cybersecurity solutions morphed formerly niche vendors into corporate powerhouses. In the past 10 years, the overall market for cybersecurity companies has grown substantially, outpacing the S&P with a 19% CAGR. A decade ago, the largest publicly-traded cybersecurity company had a market capitalization of $15 billion. Today, two of the leading publicly-traded cybersecurity companies are valued at over $100 billion. Along with overall value, the makeup of many of these vendors has also changed considerably, reflecting the ever-evolving needs of customers and the pressure on technology providers to deliver.

In 2015, the combined market cap of the top 10 cybersecurity providers was $97 billion. Today, there are now two companies (Palo Alto Networks and Crowdstrike) each with over $110 billion in market value.

Top 10 Listed Cybersecurity Players By Market Cap Over Time

Company	2015 Value	Company	2020 Value	Company	Today's Value
paloalto	$16	CROWDSTRIKE	$49	paloalto	$130
CHECK POINT	$15	okta	$36	CROWDSTRIKE	$111
Symantec	$14	paloalto	$35	FORTINET	$81
VERISIGN	$12	splunk>	$28	CLOUDFLARE	$56
Akamai	$9	zscaler	$28	zscaler	$40
splunk>	$8	CLOUDFLARE	$25	VERISIGN	$26
f5	$7	VERISIGN	$25	CHECK POINT	$25
TREND	$6	FORTINET	$24	okta	$22
FORTINET	$5	CHECK POINT	$19	CYBERARK	$18
BlackBerry	$5	Akamai	$17	rubrik	$18

Top 10 Cybersecurity Market Value	20% CAGR	$97	$286	$526
All Cybersecurity Market Value	20% CAGR	$116	$399	$625
Market Cap of the S&P 500	11% CAGR	$18T	$32T	$48T

Source: S&P Capital IQ

Notes:
1. Today's market data as of 5/20/2025; 2020 market data as of 12/31/2020; 2015 market data as of 12/31/2015
2. Some figures may vary slightly due to rounding

Innovation is at a Premium Across the Cybersecurity Market

A slew of major M&A deals over the past few years has reshaped the cybersecurity landscape. In 2024, there were 30 acquisitions valued at greater than $200 million, totaling over $35 billion in transaction value, while in 2023 there were 20, totaling nearly $43 billion in transaction value. So far this year, one transaction alone, Google's $32 billion deal for Wiz, nearly matched the entire total for last year. The early-stage acquisition market has also been active, with 20 transactions valued between $50-$200 million in 2024 alone, and 6 already this year. While every deal served its own unique purpose, many over the last few years helped larger vendors offer more specialized solutions through their existing platforms, indicating the need for continued innovation in cybersecurity, and the willingness to pay for it.

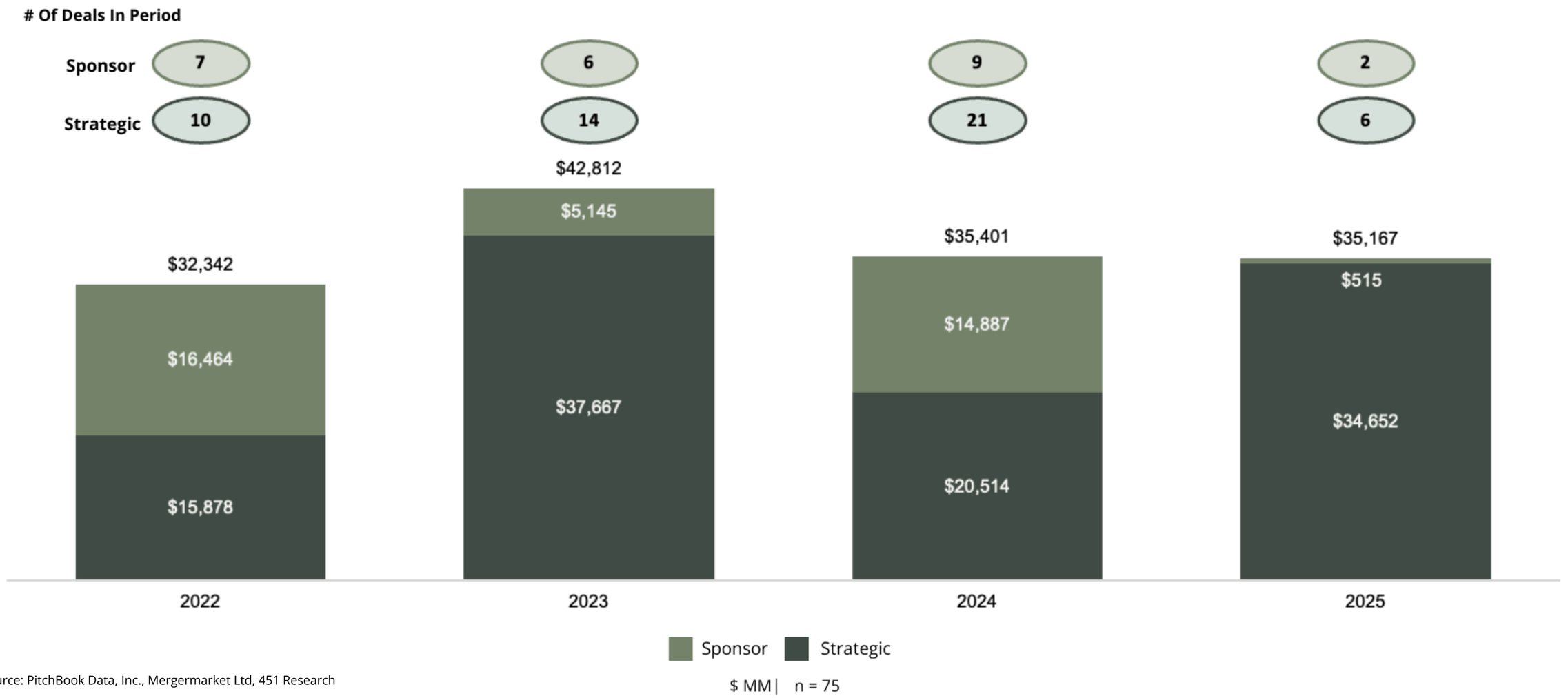
Strategic acquirers have emerged as the driving force behind cybersecurity's M&A surge, reflecting growing confidence in the sector's long-term value. From 2022 to 2025, they were responsible for over $100 billion in deal activity.

The Next Wave Of Cybersecurity Is On The Way

There is significant activity in the early-stage private capital cyber market. In 2024, there was $13 billion in investment in cybersecurity startups, up 9% compared to the prior year. And of the deals conducted, over 60% were seed or early-stage rounds led by venture capital firms. Notably, the deal value for data security startups grew 146% to $3.2 billion, and 73% for detection software providers, to $2.6 billion.

All the activity across the public, private and M&A markets shows just how vital cybersecurity is to running a modern business. As threats evolve and new problems emerge, investors and customers are constantly on the lookout for the next market leader. And with continued rapid growth at many of the most promising cybersecurity startups, the make-up of the industry could change dramatically in the coming years.

Cybersecurity M&A Transactions $200MM+ From 2022-2025



Source: PitchBook Data, Inc., Mergermarket Ltd, 451 Research

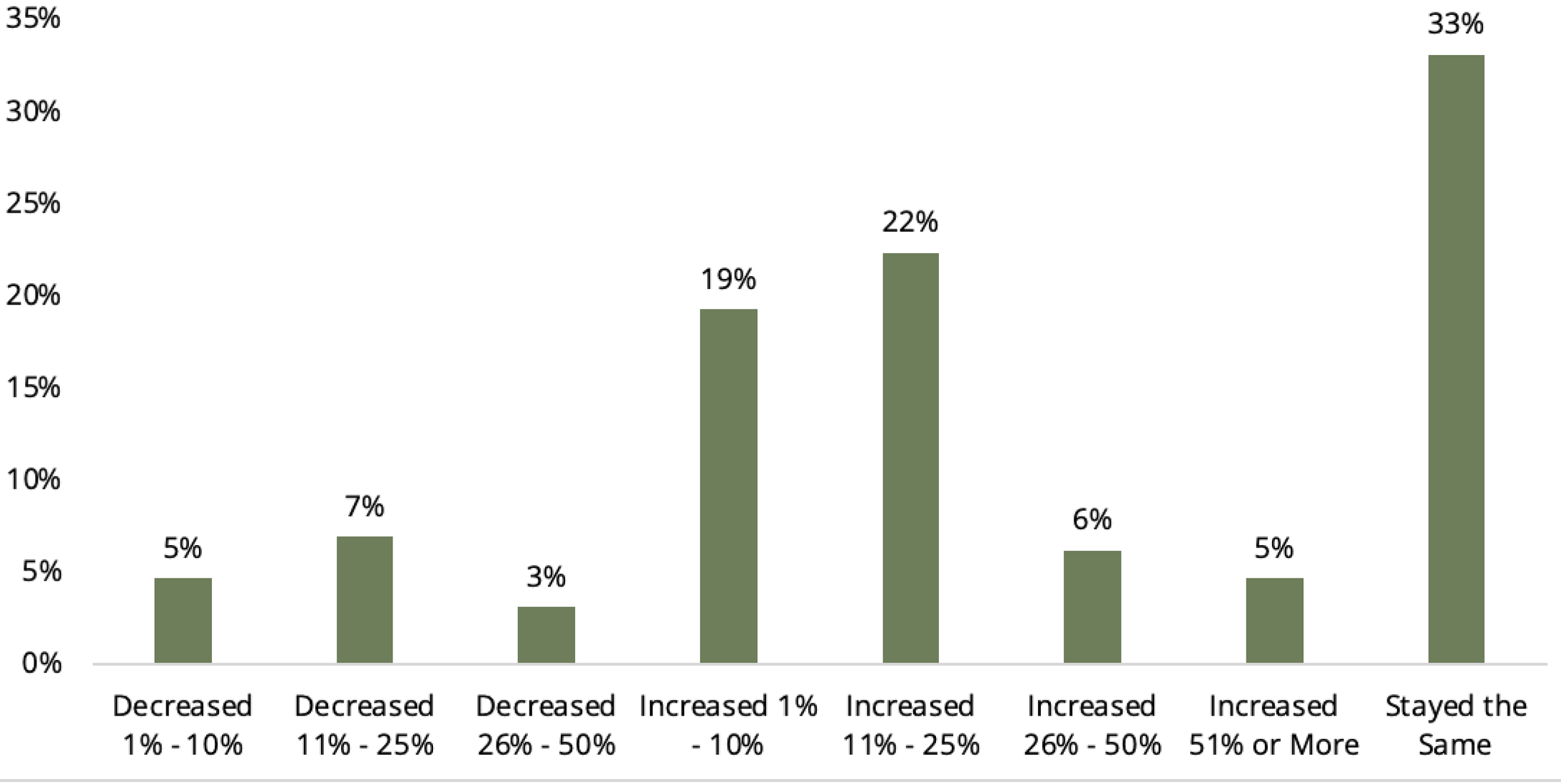
Key Findings From Our CISO Survey

The analog era is almost entirely behind us. We're entering a future where people no longer interact directly with digital tools. Instead, they're prompting virtual, AI-based assistants that then act like humans to autonomously execute actions.

This evolution is not only impacting the vendor landscape, but how CISOs spend their budgets. To understand what security leaders think about the emerging technology, and how the greater use of data and AI within organizations is impacting spending, we surveyed nearly 150 CISOs. The biggest findings include:

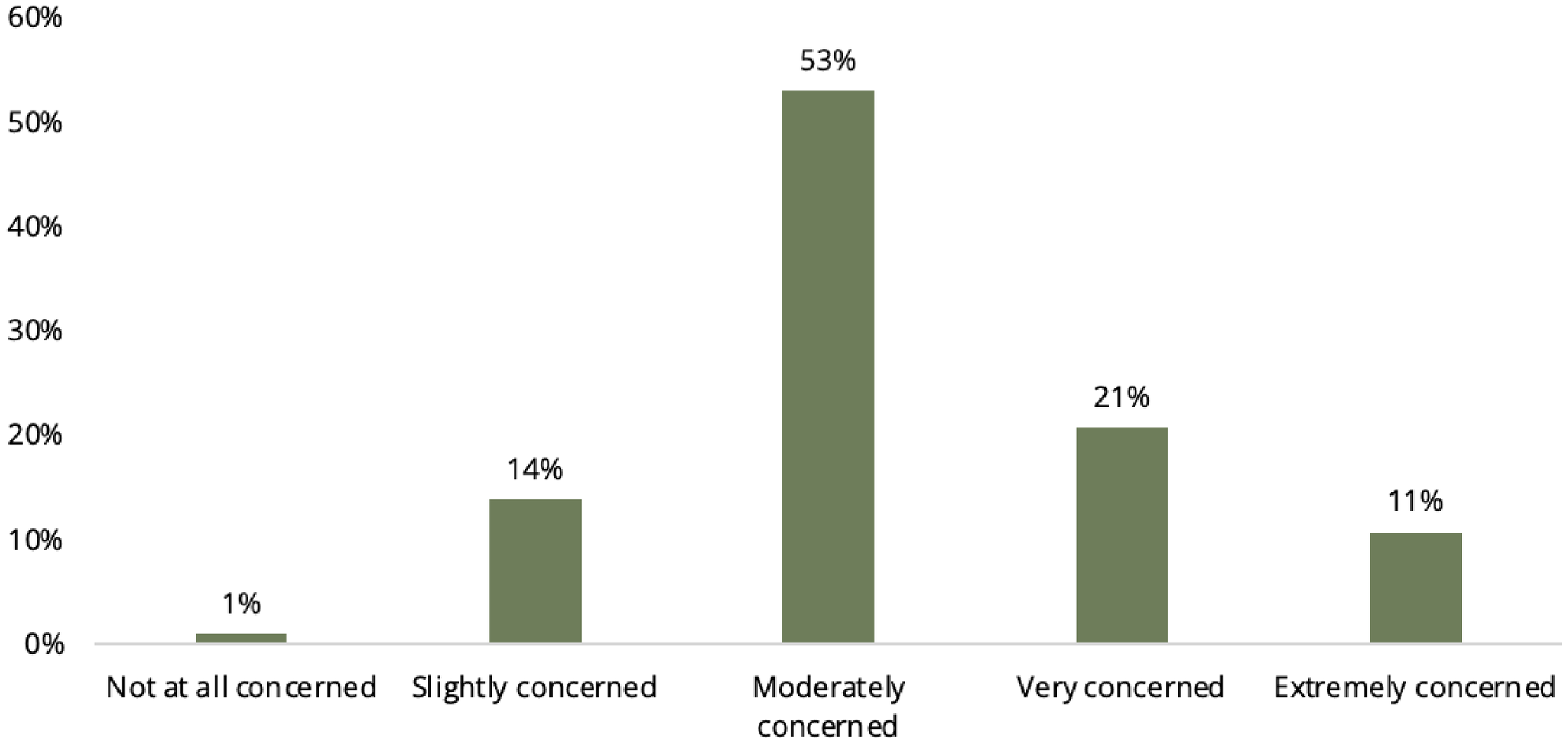
- **Cybersecurity isn't immune to budget pressure:** 33% of CISOs said their budgets stayed the same this year, while roughly 41% said their budgets increased as much as 25%. Just 5% said their budgets would increase by 51% or more. Without the ability to expand teams, CISOs will increasingly need to rely on technology solutions to fill in key gaps and help existing talent optimize their time.
- **AI is a problem, but not yet existential:** Nearly half of respondents (48%) listed AI-powered threats as a "medium priority" for their teams, while nearly 27% labeled it a "high priority" in their organizations. Meanwhile, 53% were "moderately concerned" about the risk from AI agents. Conversely, only 11% were "extremely concerned," signaling CISOs are learning how to adapt to the technology.
- **AI agents can still be unreliable:** 32% of CISOs cited uncertainty around agent behavior as a barrier to adoption, and 21% said security and governance risks were a hurdle. Just 5% said internal resistance was a problem, indicating the enthusiasm for AI agents across most businesses.
- **Identity is a foundational challenge:** 31% of CISOs are most concerned about identity and access controls when it comes to AI-based applications, while 24% of CISOs are concerned about AI-based social engineering attacks. As the number of machine identities grows at an exponential pace, CISOs will need to adopt new mechanisms to authorize and authenticate the systems, whether it's human-machine or the increasingly common machine-machines interactions.

Please indicate how your cybersecurity budget has changed between 2024 and 2025.



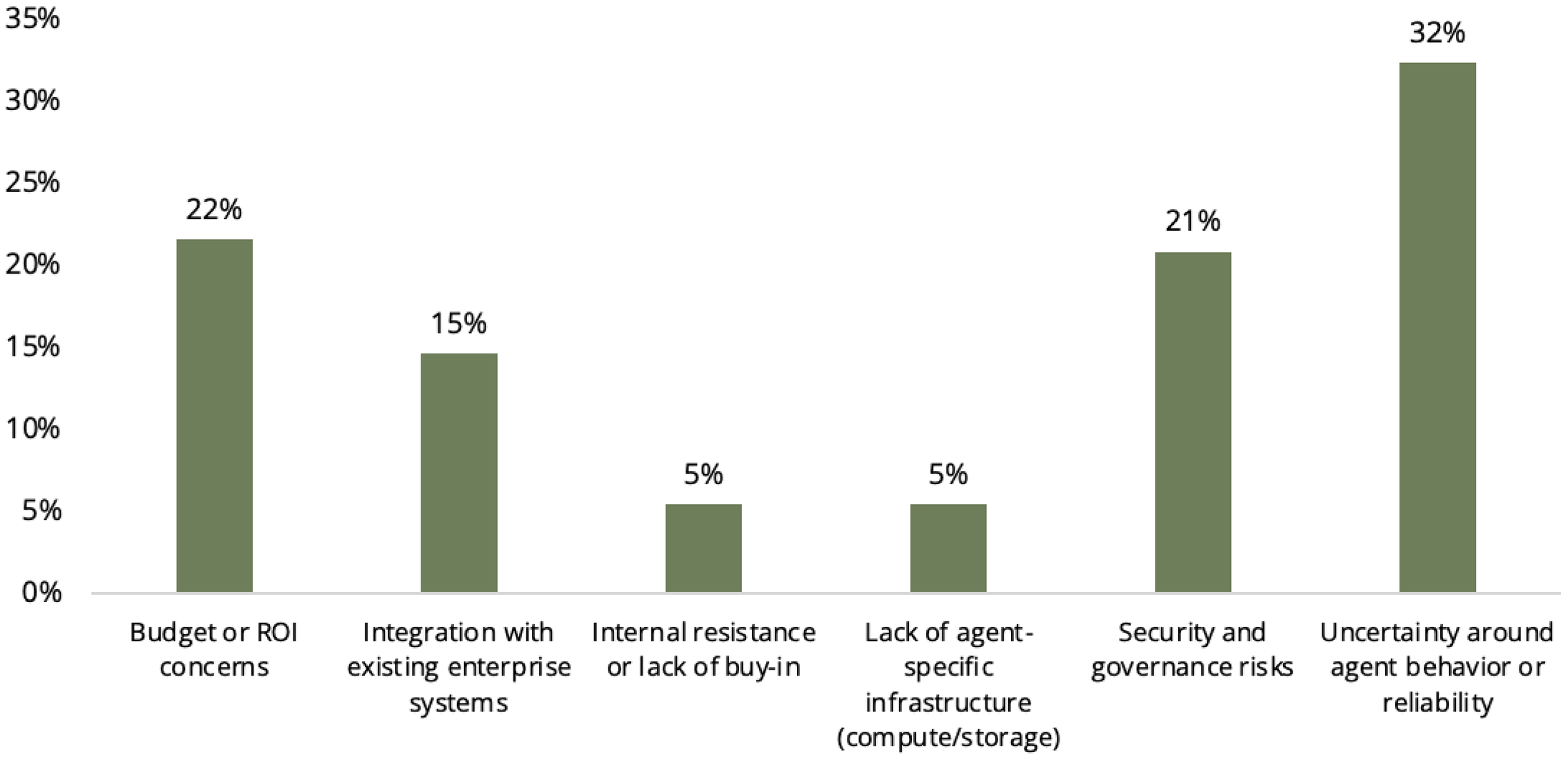
Source: Rising in Cyber CISO Survey May 2025

How concerned are you about the security risks posed by autonomous or semi-autonomous AI agents?

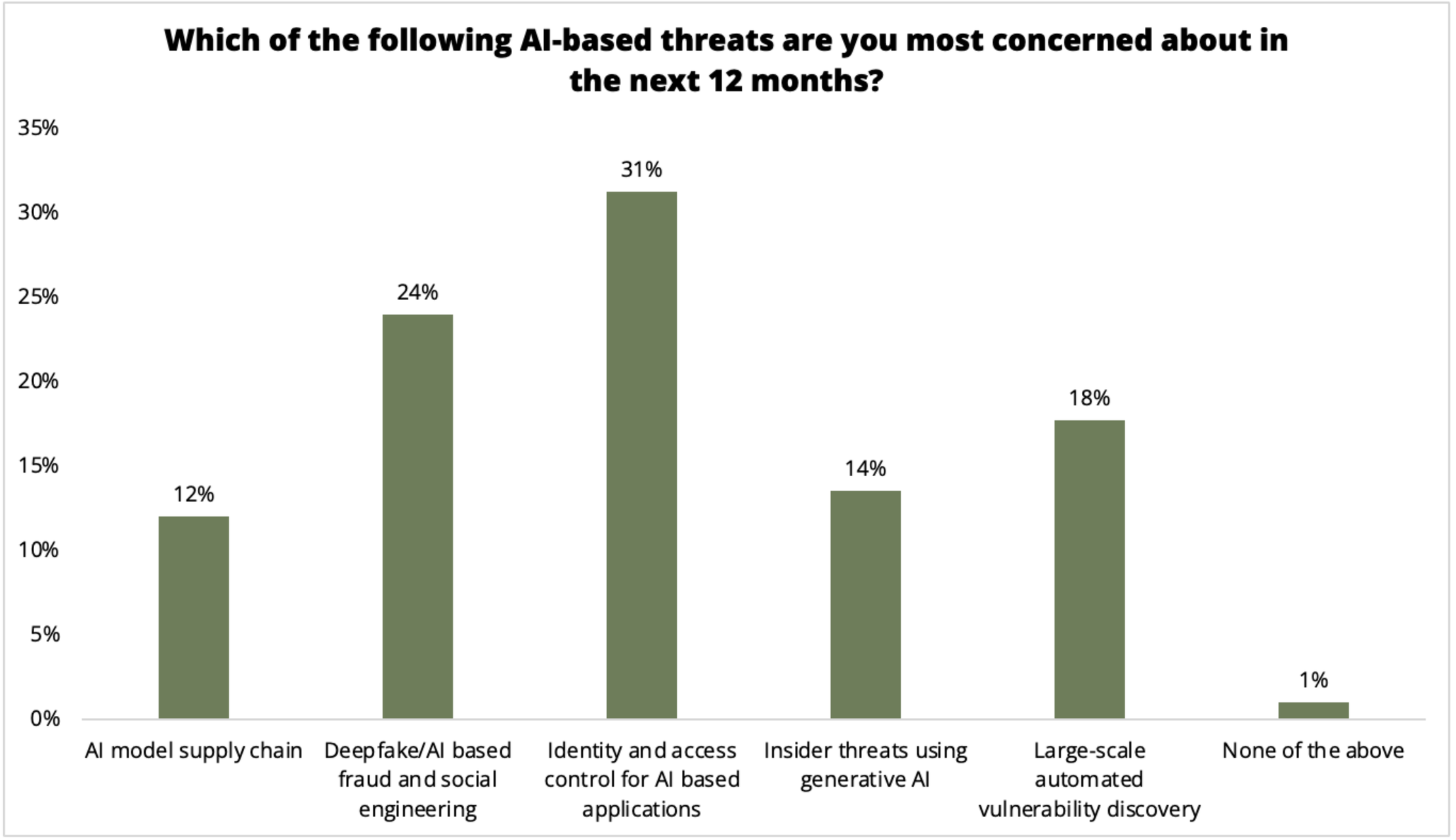


Source: Rising in Cyber CISO Survey May 2025

What do you view as the biggest barrier to adopting AI agents in your organization?



Source: Rising in Cyber CISO Survey May 2025



Source: Rising in Cyber CISO Survey May 2025

Pivoting From Reactive To Proactive

Today, most cybersecurity professionals operate in firefighter mode, constantly pivoting to another crisis or deadline. But with the ability to operate autonomously to eliminate manual toil, identify vulnerabilities, anticipate risks and neutralize threats, AI is empowering more teams to proactively identify challenges and opportunities, helping turn cybersecurity from a cost-center to a key business driver.

“We shouldn’t be waiting for our metrics to tell a story. We should be proactively looking for issues, when things are breaking down. We want to know earlier so we can fix it quicker,” said Israel Bryski, the CISO at MIO Partners.

Functions critical to modern security programs, like threat detection or governance, risk and compliance, still require significant human involvement. Many specialists spend their time navigating multiple underlying technology solutions to manage alerts, document issues, and coordinate across departments. Their time is dominated by filling out spreadsheets and forms, examining policies to make sure they align with evolving regulatory demands, chasing down false alerts, reviewing metrics and navigating information silos. As a result, many breaches or potential security issues are discovered only after the damage is done. And investigations and recovery efforts are conducted under immense pressure from internal and external stakeholders.

In the new era of proactive cybersecurity, AI systems will do the tedious job of crunching massive datasets to correlate threat intelligence and deliver targeted, actionable insights to specialists. The technology will be able to help predict what could potentially happen so proper action can be taken and automatically run audits to identify gaps in compliance, whether in the company’s own solutions or vendor applications, as well as coordinate with stakeholders across the organization.

“We’ll be able to off-load a lot of repetitive, manual tasks,” said Andress. “If AI is taking care of the initial, reactive work, cybersecurity teams can be more proactive going forward.”

Armed with better insights and unburdened by tedious, low-value tasks, security professionals can focus on using their expertise to contribute to the company's overall strategic growth areas. "Bringing AI-driven automation removes bottlenecks, helps companies stand-up and scale key programs like compliance, and gives them real-time, continuous insight into how secure and compliant they are," said Drata CEO Adam Markowitz.

Rethinking Security Operations Center (SOC) Teams in the Age of AI

The burden of monitoring environments, triaging alerts, investigating incidents, and coordinating responses has historically been a human task. But with the growing complexity of IT networks, as well as the increasing speed and scale of attacks, these tasks can and should be augmented with technology.

Consequently, a resounding 93% of IT professionals plan to, or have already deployed AI to help defend their digital ecosystems. But as AI systems begin to serve as the front-line defense, CISOs must reimagine SOC teams to more seamlessly blend human and artificial intelligence. This requires more than reworking workflows; it requires CISOs to retrain staff, adopt new technologies, rethink KPIs, and potentially even revamp the culture of the team.

By having bots handle the monotonous tasks, and humans the more complex ones, organizations will be much better equipped to anticipate threats to their organizations by ever-vigilant digital adversaries. For example, with an increasing amount of security information and event management solutions, logs, and telemetry data to manage, so-called "alert fatigue" is a very real problem for security teams. In fact, overwhelmed by the sheer volume of notifications, many employees miss or ignore important information. While the bulk of these alerts are likely false positives, it's a risk businesses can't afford.

“We’ve created a big data problem for ourselves. We thought we didn’t have enough data, we needed a single pane of glass, so vendors found ways to show us everything. But I don’t think people realized how much ‘everything’ really was,” said Pieter VanIperen, CISO at Own Company. “With AI, we can determine with a much larger degree of certainty whether something can harm us or not, and that is going to drastically change things.”

Instead of hoarding every piece of information produced by their systems, fearing important data might be lost, companies can deploy a security data fabric to aggregate, normalize, enrich, and correlate only relevant inputs. Applying AI, they can then extract insights and reduce noise, enabling faster and more confident decision-making. With employees no longer having to chase down continual false alerts, they can refocus time to the high-value areas that AI can’t currently handle, such as advanced threat hunting, behavioral analysis, and adversary emulation.

This isn’t just a new way to store logs. It’s a complete rethinking of detection and response to cut false positives, boost analyst efficiency, and lower costs – all by eliminating unnecessary data. It’s just one example of how the modern SOC team isn’t going away. It’s just becoming more strategic – and better armed.

Securing the Application Layer

Despite all the advances in detection, intelligence and automation, many of the most damaging breaches have the same origin: third-party applications. Whether it’s misconfigured OAuth tokens, exposed APIs or broken access control in continuous integration/continuous delivery pipelines, hackers are increasingly adept at exploiting weaknesses in third-party tools, leading to massive breaches at organizations like Okta.

“There’s been a lot of breaches related to out-sourced software,” said Bryski “If we don’t have good visibility into vendor accounts, then a threat actor can do whatever they want,”

In response, security teams are trying to regain control of their sprawling application environments, with a focus on uncovering unsanctioned systems, monitoring behavior and enforcing controls directly at the interaction layer, rather than the edge, to minimize risk. This requires a new level of visibility for most organizations, one that extends to everyone accessing the network, including full-time employees and contractors.

“We’re always using more third-party tools, the inventory never decreases,” said Andress. “AI can help identify what’s missing. Humans are good at reacting to what’s there, but we don’t think about what’s not there. AI can help call out gaps in our intelligence.”

Getting Identity and Access Management Under Control

It’s a very real fear among CISOs: an AI agent trained to triage a customer complaint accidentally accesses internal personally identifiable information (PII) data. Suddenly, the company is exposed to potential legal risk – maybe without anyone even knowing it.

As agentic capabilities advance, so does the need for greater autonomy. But without visibility or control, this becomes a new class of insider risk. It’s why a future where AI machines act on our behalf to push code, move money, and approve workflows hinges on a critical foundation: identity. And not employee identity, but non-human identity (NHI). “Identity is the foundation of every security program. And if your foundation is faulty, your program is going to be faulty,” said Bryski.

Many organizations have made significant strides in their ability to verify and manage the identity of the humans accessing their network. Now, there’s a massive (and growing) number of NHIs that must also be verified, monitored and controlled, including service accounts, APIs, and, increasingly, AI agents.

“Identity and access management is coming to a head. It is too big, too sprawling; it needs to be solved,” said VanIperen.

But technology designed to protect against malicious human activity, like multi-factor authentication, doesn't work with machines. And as the challenge of managing NHIs becomes orders of magnitude greater, securing them and controlling access permissions is no longer just an IT concern; it’s a front-line imperative that extends across the business.

31% of CISOs worry about identity and access controls when it comes to AI-based applications, while 24% of CISOs are concerned about AI-based social engineering attacks.

Luckily, there’s a number of visionary startups already focused on NHI visibility, authentication, and privilege enforcement. With infrastructure that tracks agent activity, enforces least privilege, and audits actions across dynamic environments, businesses can reduce risk from increasingly autonomous machine behaviors.

“The big majority of identities are NHIs, and they are still being overlooked. And the way people are targeting this problem now is not scalable,” said Token Security CEO and co-founder Itamar Apelblat. “There’s a lot of identity management software for enterprises, but they’re very human-centric. And CISOs are being pushed to adopt agentic AI in their platforms, but they’re still struggling with controls in their legacy solutions, so there’s a lot of chaos when it comes to NHIs.”

Conclusion

The pace of advancement of AI and other technology is only getting faster. And businesses are only increasing their investment in new data-heavy AI workflows. As a result, cybersecurity professionals need to be able to move with greater agility to provide the organization with the right guardrails and the ability to detect and remediate issues.

While AI agents introduce new risks to manage, they are quickly becoming a necessary tool for CISOs and their teams to manage the growing demands on their time and expertise. As the systems become more adept, CISOs must rethink how their teams operate, with a focus on using AI to eliminate tasks that pull professionals away from proactively identifying issues.

That means staying connected to a thriving startup ecosystem that continues to push the boundary of what's possible in cybersecurity, exemplified by companies on the Rising in Cyber 2025 List. So while the threats may continue to evolve, CISOs can be confident that the solutions to detect and defend against them will keep pace.

Legal Disclaimer

We have prepared the information contained in this report solely for informational purposes. You should not definitively rely upon it or use it to form the definitive basis for any decision, contract, commitment or action whatsoever, with respect to any
proposed transaction or otherwise.

We have prepared the information contained in this report based, in part, on certain assumptions and information obtained by us from various sources. Our use of such assumptions and information does not imply that we have independently verified or necessarily agree with any of such assumptions or information, and we have assumed and relied upon the accuracy and completeness of such assumptions and information for purposes of preparing the information contained in this report. Neither we nor any of our affiliates, or our or their respective officers, employees or agents, make any representation or warranty, express or implied, in relation to the accuracy or completeness of the information contained in this report or any oral information provided in connection herewith, or any data it generates and accept no responsibility, obligation or liability (whether direct or indirect, in contract, tort or otherwise) in relation to any of such information. We and our affiliates and our and their respective officers, employees and agents expressly disclaim any and all liability which may be based on the information contained in this report and any errors therein or omissions therefrom. Neither we nor any of our affiliates, or our or their respective officers, employees or agents, make any representation or warranty, express or implied, that any transaction has been or may be effected on the terms or in the manner stated in this report, or as to the achievement or reasonableness of future projections, management targets, estimates, prospects or returns, if any. Any views or terms contained in this report are preliminary only, and are based on financial, economic, market and other conditions prevailing as of the applicable date(s) such information is presented and/or as of the date such information is first presented and are therefore subject to change. We undertake no obligation or responsibility to update any of the information contained in this report. Past performance does not guarantee or predict future performance.

This report and the information contained in this report do not constitute legal, regulatory, accounting or tax advice. We recommend that you seek independent third party legal, regulatory, accounting and tax advice regarding the information contained in this report. This report and the information contained in this report do not constitute and should not be considered as any form of financial opinion or recommendation by us or any of our affiliates. This report is not a research report.

This report is provided by Notable Capital Management, L.L.C. and/or certain of its affiliates or other applicable entities in collaboration with other third parties.