2026 Rising in Cyber Report

May 2026

Notable.

Morgan Stanley

2026 Rising in Cyber Report

By Dave Chen, Co-Head of Global Technology Investment Banking, Morgan Stanley and Oren Yunger, Managing Partner, Notable Capital

Intro Letter

For CISOs, the early AI results are energizing: Capabilities like AI-powered penetration testing and threat detection are helping augment existing cybersecurity, overcome talent gaps, and respond to issues with more authority. But across enterprises, AI adoption is also outpacing security. Now, CISOs are quickly shifting their focus to safeguarding these new workloads, a pivot poised to shake up legacy cybersecurity markets.

Overall, the security market is bustling and expected to grow to $255 billion by 2029, based on IDC estimates. Startups are innovating, growing, and attracting investor attention at unparalleled speed and scale, while the leading AI labs are rapidly layering security capabilities over their powerful LLMs. And despite the panic in the public markets, many incumbent security software vendors appear increasingly well-positioned to survive the near-term impact — especially as they continue to pay a premium for capabilities that keep them competitive.

But when AI advancements impacting the cybersecurity sector can shed billions of dollars from the market, and landscape-shifting technical advancements are a regular occurrence, CISOs are left grappling with key questions: Should we invest in an AI-native solution, double down on existing platforms, or simply wait for the next LLM release and build our own?

The pressure is on CISOs to balance enablement and progress with safety. According to our recent survey of over nearly 150 security leaders from the world's largest and most prominent businesses, 71% say their companies already have AI agents in production, only 11% report that they have mature, well-integrated, or best-in-class tooling to secure AI workloads. This is a dangerous gap. Luckily for CISOs, innovation in cybersecurity is in full swing.

In 2025, Series A and B funding accounted for over half of the over $10 billion invested in cybersecurity startups. But with CISOs also taking a closer look at all their spending, it's incumbent on younger companies tackling the challenge of AI security to quickly prove their real-world value. Otherwise, what is a diverse market could consolidate to existing platforms and frontier AI labs that move faster to earn customer trust.

Our 2026 Rising in Cyber Report, the second year running the study, examines survey insights from leading CISOs and market data from Morgan Stanley to make sense of how CISOs are navigating a period defined by rising uncertainty, expanding attack surfaces, and rapid shifts in both risk and opportunity

Executive Summary

In the AI era, the top cybersecurity challenges may seem familiar: eliminating blind spots, securing identities, managing access, and responding to deviations. But as AI agents swarm technology environments, these long-standing problems are becoming existential threats. CISOs are trying to keep up: over 50% are already using AI agents in their own security operations, according to our survey. And budgets are growing to do even more.

“AI is really helping us work smarter and faster on challenges that have historically been difficult to scale, like triaging and prioritizing security issues. It becomes more manageable when you can augment your team with that kind of capability," said United Airlines’ Vice President and CISO Deneen DeFiore.

Meanwhile, investors are flocking to young, AI-native startups that can help secure new AI technology. And major platforms continue to scoop up specialized vendors that help them keep pace with innovation in the market, like Cisco’s acquisition of Astrix.

The Rising in Cyber 2026 Report delivers a snapshot of the current state of play of the cybersecurity industry. Based on survey insights from leading CISOs and market data from Morgan Stanley, it spotlights the ways AI is changing how CISOs think about their core technology and separates hype from reality to help investors, operators, security leaders, and founders make sense of the chaos.

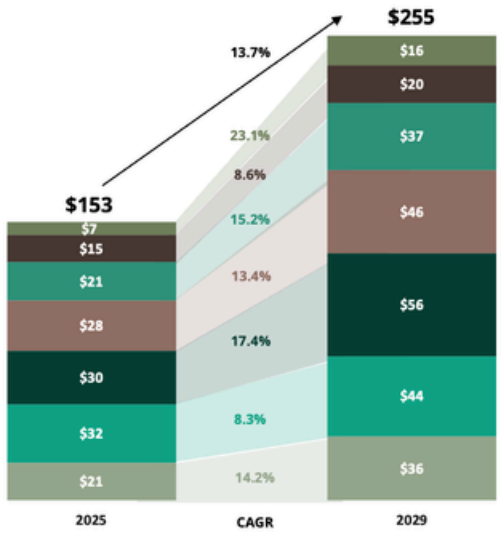
The State of the Cybersecurity Market

The 10,000-foot view: Large, growing, and diverse

There’s no shortage of demand. Overall, the cybersecurity market is expected to grow to $255 billion by 2029, according to IDC data, up from a higher-than-expected $153 billion in 2025. Powering this growth are expected double-digit increases in enterprise spend on identity and access management (IAM), data and information security, and cloud-native application protection solutions, among other segments. The market also remains highly fragmented. Few vendors command more than 20% of any vertical. But Microsoft is the dominant force in five of the largest verticals.

The TAM of Cybersecurity is Healthily Large, Growing, and Diverse...

Enterprise Security Spend by Market, 2025 & 2029 Estimates



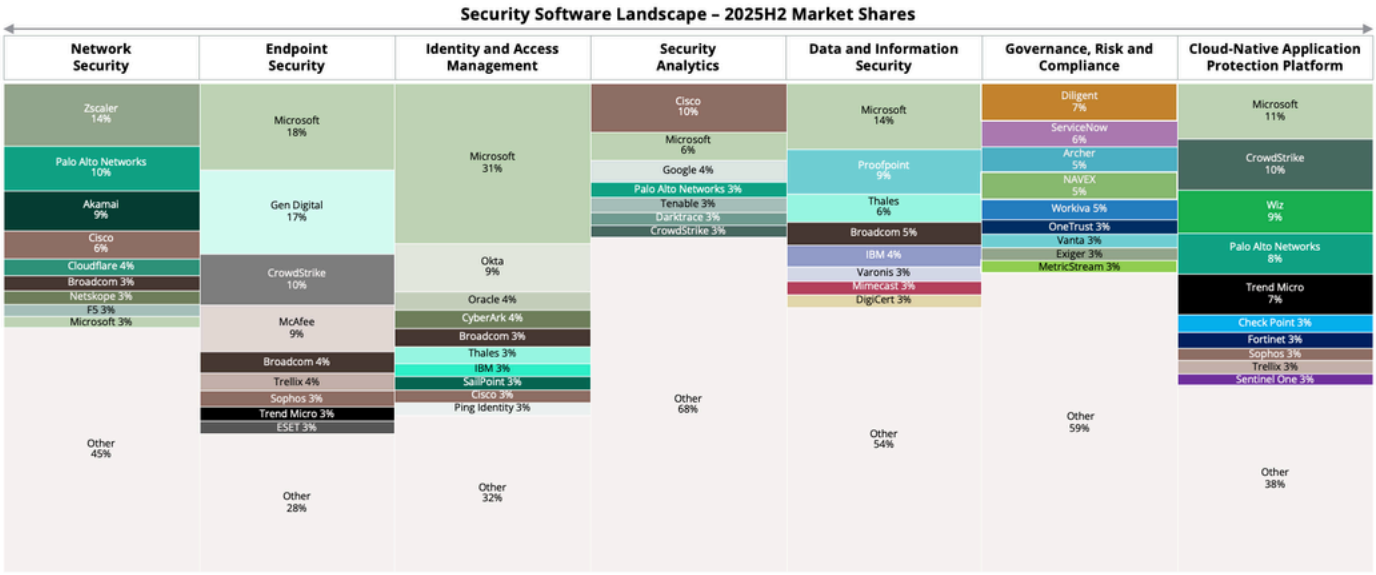
Source: IDC Security Spending Guide (February 2026)

	Key Solutions	Key Players
Cloud-Native Application Protection Platform	• CI/CD Tools • Multi-cloud Visibility	paloalto WIZ Microsoft TREND MICRO CHECK POINT CROWDSTRIKE
Governance, Risk and Compliance	• Governance Mgmt • Risk Mgmt • Compliance Mgmt	servicenow Diligent RSA NAVEX IBM
Data and Information Security	• Encryption • Key Mgmt • Certificates • Messaging • Sensitive Data Mgmt • Data Privacy and Compliance	BROADCOM proofpoint Microsoft CISCO Forcepoint
Security Analytics	• Security Information and Event Mgmt • Vulnerability Mgmt • Tier 2 SOC Analytics and Cloud-Native XDR	splunk> IBM tenable DARKTRACE Microsoft
Identity and Access Management	• Identity Mgmt • Legacy Identity • Authentication • Privileged Access Mgmt	Microsoft okta RSA IBM ORACLE
Endpoint	• Modern End Point Security • Server Security • Consumer Digital Life Protection	SentinelOne TREND MICRO SOPHOS CROWDSTRIKE Microsoft
Network	• Secure Web and Cloud Gateway • Network Sandboxing • Firewall / UTM • Segmentation • VPN / ZTNA	paloalto CISCO zscaler CHECK POINT FORTINET

Notable Capital

... Yet Fragmentation in the Ecosystem Still Persists

Security Software Landscape – 2025H2 Market Shares



Source: IDC Software Tracker Historical Market Shares

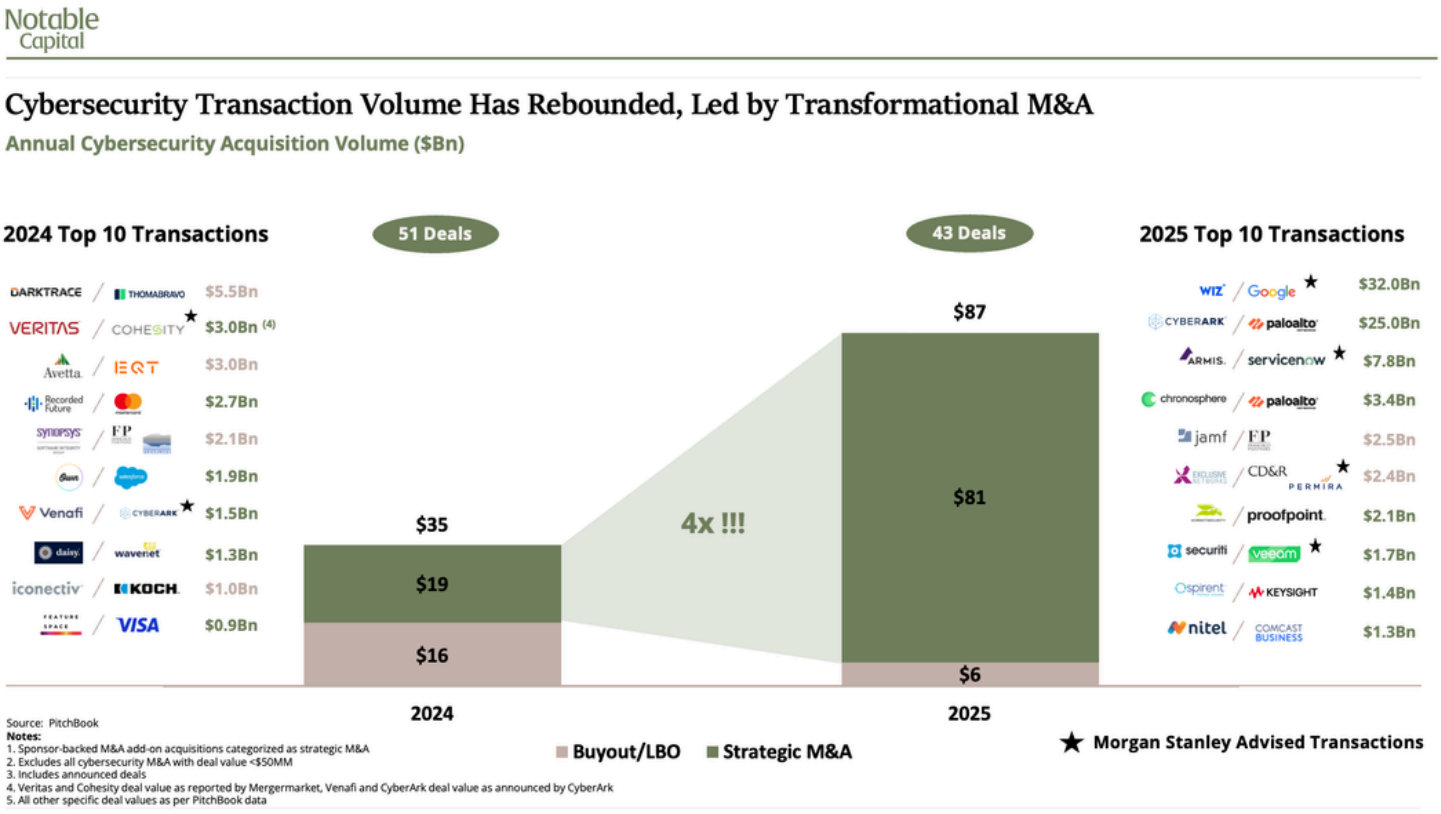
The Technology Industry is Back in the M&A Driver's Seat

In 2024, private equity firms paid up for security startups: Thoma Bravo bought Darktrace ($5.5 billion) and EQT bought Avetta ($3 billion), according to PitchBook data.

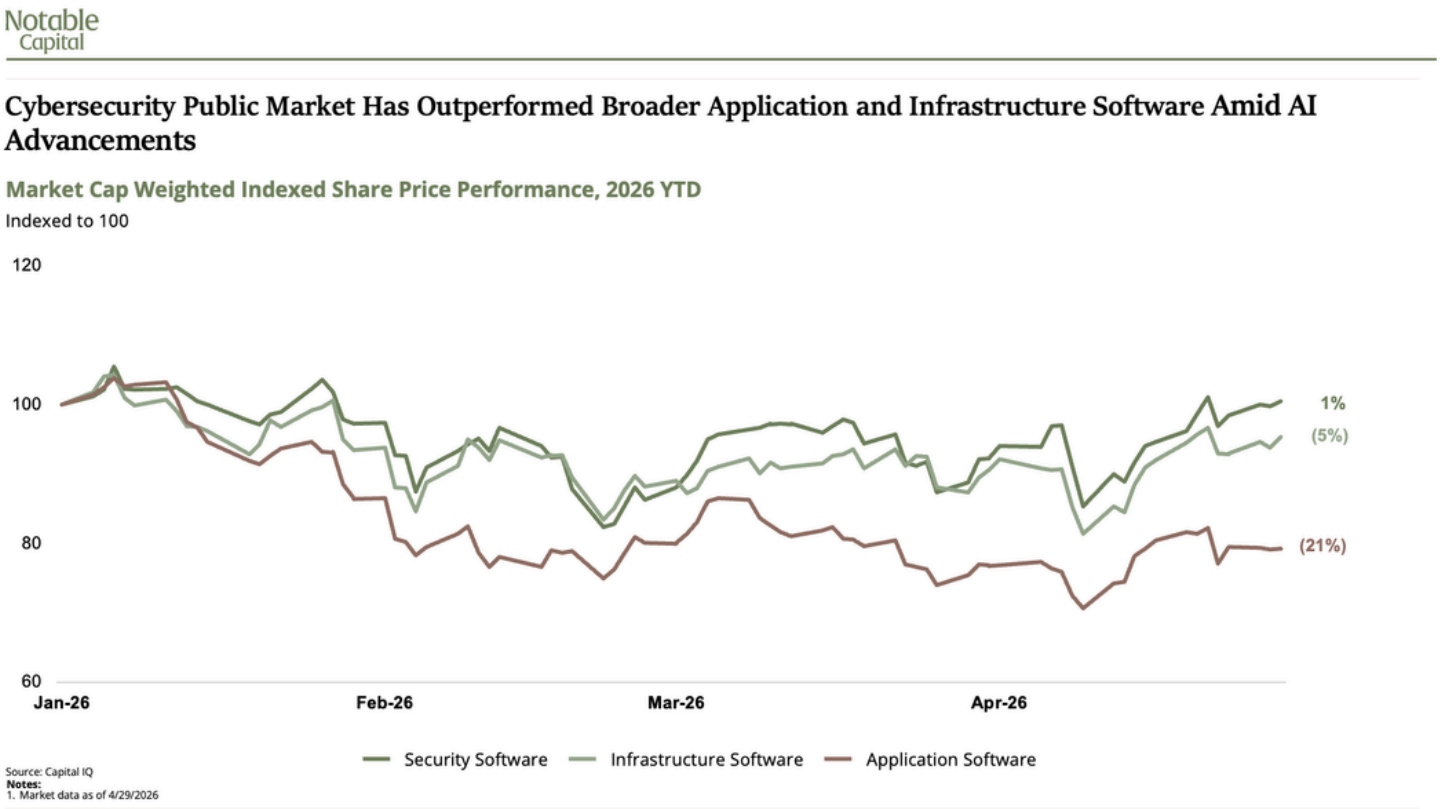
Last year marked a clear shift toward platform-led consolidation. Beyond the $32 billion Wiz deal, Palo Alto spent nearly $30 billion to acquire both CyberArk and Chronosphere, and ServiceNow bought Armis for $7.8 billion. And the number of acquirers is growing more diverse as companies like Veeam get more aggressive about security on their platforms.

Overall, strategic M&A deal volume grew to $81 billion, up over 4x from 2024, while buyouts shrank to just $6 billion. Even without the blockbuster Wiz deal, overall M&A activity increased 156%.

The momentum isn't slowing down, either, as AI pushes the large incumbents to evolve their platforms. So far in 2026, CrowdStrike purchased SGNL, Palo Alto Networks purchased Koi, and Sophos acquired Arco Cyber, among other deals.



In a Turbulent Wall Street, Cybersecurity Proves Resilient



While public cybersecurity stocks weren't immune to investor whiplash, the sector performed better on average than its infrastructure and application software counterparts, indicating the resilience of security tools amid the broader IT overhaul. Overall, security software shares were up 1%, compared to a 5% decline in infrastructure software and a 21% decline in application software. Perhaps unsurprising: the biggest sell-offs were tied to market concerns about the impact of AI. Overall, all three sectors were outpaced by the S&P 500, which grew 4%.

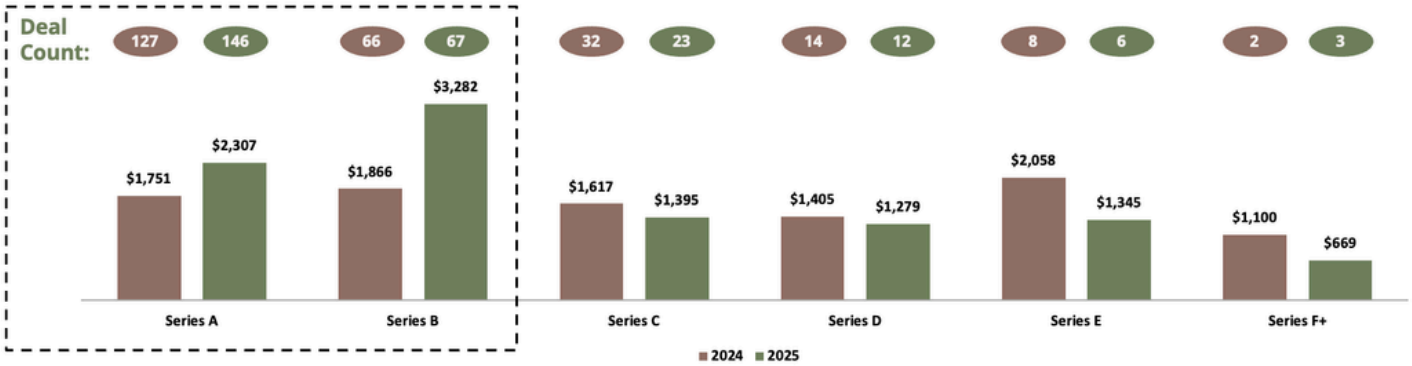
The Disruption is Just Beginning

Early-stage, AI-native startups dominated the VC funding landscape. Together, investment in Series A and B startups eclipsed $5.5 billion in 2025 — the only segment that didn't decline year-over-year.

Investments are coming earlier, getting bigger, and happening faster. For example, in total, Series B rounds grew 74% to $3.3 billion, while deal count went from just 66 to 67. Average deal size also went up around 75% to $49 million. And increasingly investor attention is on technology that will help companies secure their new AI use cases like 7AI, Adaptive, and Exaforce, which all closed early-stage funding rounds.

Venture Funding Dollars are Flowing to Earlier Rounds to Fund the New Wave of AI-Native Cybersecurity

Cybersecurity Venture Funding by Series ($MM)



2025 Largest Rounds by Series

Source: Pitchbook
Notes:
1. Excludes Pitchbook venture deals not categorized under a Series round

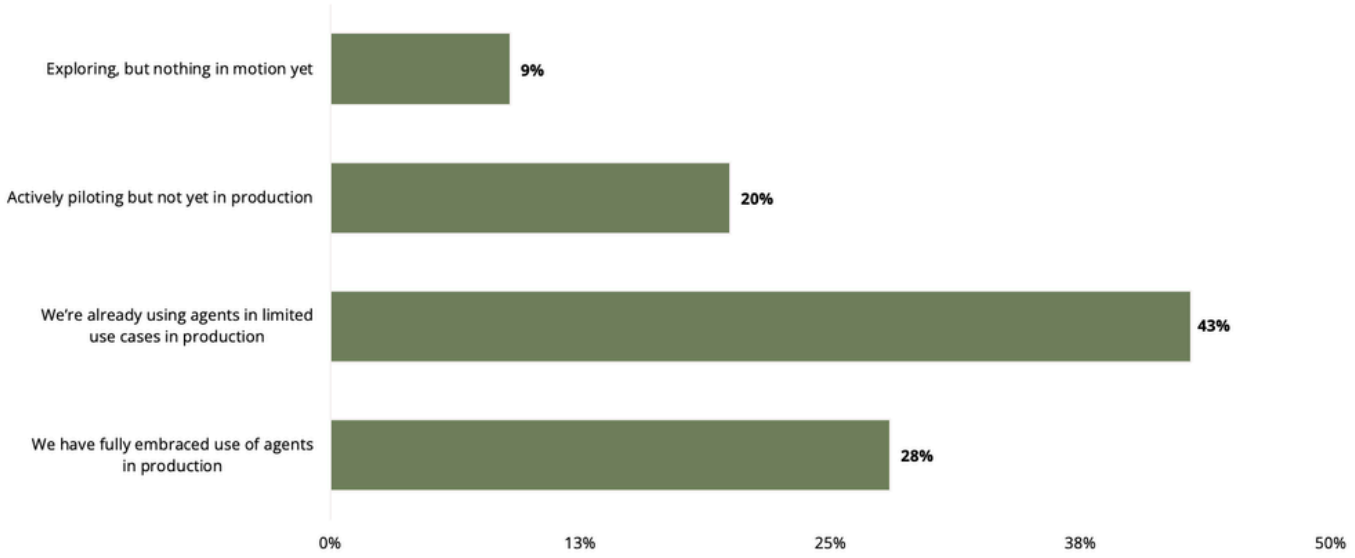
While financiers rush to back AI infrastructure and coding startups registering triple-digit growth, cybersecurity is a much different market. It's clear investors are prioritizing innovation, and are comfortable with the industry's slower pace of growth and change. And between a frothy funding landscape and hyperactive M&A market, the liquidity and exit opportunities for startups are ample.

Key Findings From Our CISO Survey

Notable Capital

AI Agents are Already in Production at Most Organizations

What is your organization's current stance on deploying AI agents in production environments?

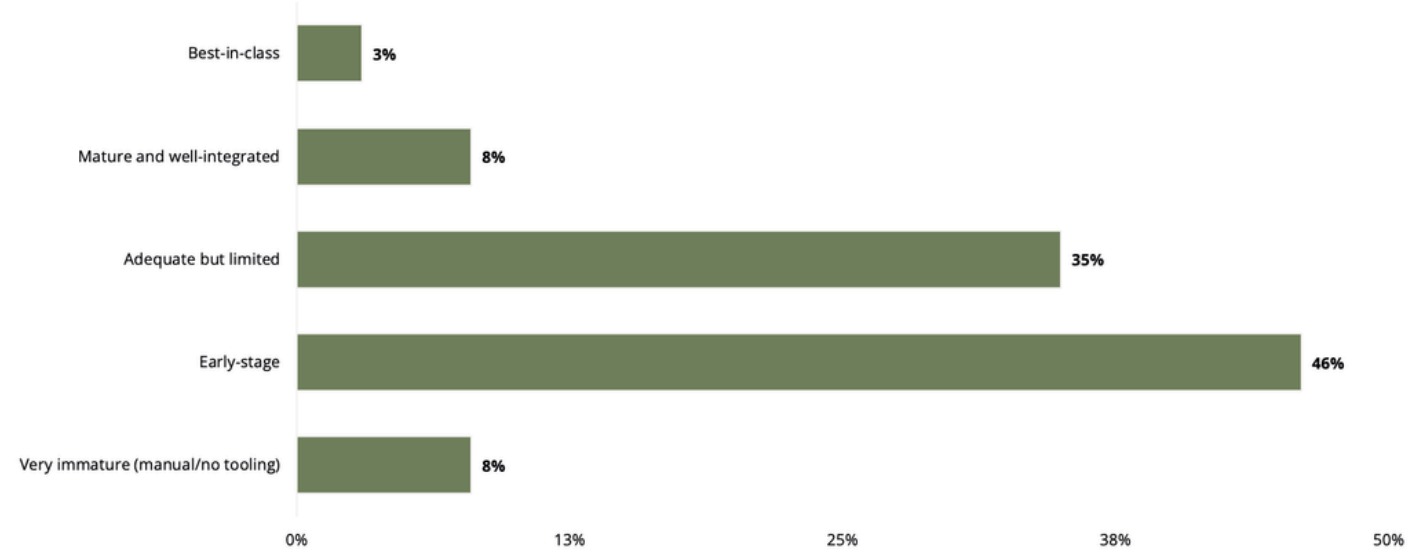


Source: Notable Capital Security Survey
Notes:
1. Represents findings from nearly 150 CISOs and security leaders surveyed

Notable Capital

Most CISOs Still Consider Their Tooling for Securing AI Workloads Early Stage or Immature

How would you rate your current tooling for securing AI workloads (including agents, MCP, etc.)?



Source: Notable Capital Security Survey

Notes:
1. Represents findings from nearly 150 CISOs and security leaders surveyed

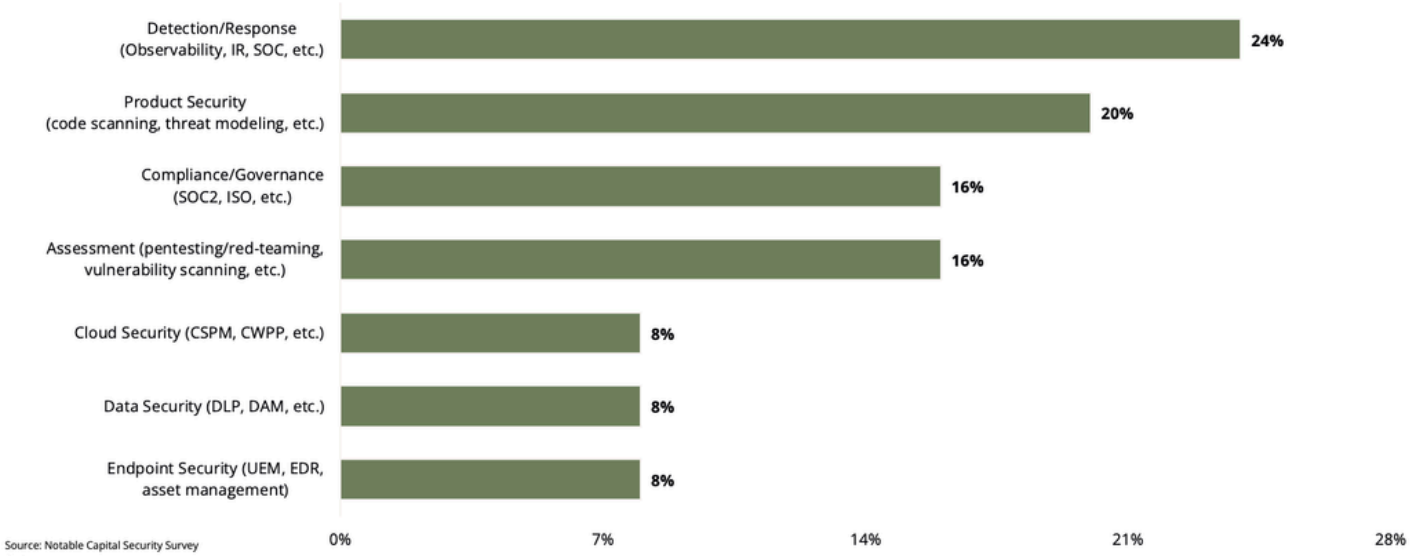
Cybersecurity teams are eager to adopt AI — and increasingly have the budget to do so. Many have already embraced AI in their own work. But as AI makes long-standing challenges like identity and access management more troublesome, the question is how quickly teams can onboard the capabilities needed to keep environments protected.

To understand how AI is shifting priorities, budgets, and operations, we surveyed nearly 150 CISOs and security leaders. The biggest findings include:

AI and cybersecurity are increasingly intertwined, and the benefits are coming into focus: Today, AI agents are helping teams overcome talent shortages, detect issues in applications, and do more with less. For example, for many companies, penetration testing used to be a bi-annual event. Now, AI agents can work continuously in the background, alerting teams to concerns in near real-time. But for some CISOs, the challenge is now turning the abundance of new intelligence into real-world results: "Across the industry, organizations are solving individual problems with great tools, and that gives us real visibility. The next frontier is turning that visibility into coordinated action," said United Airlines' Vice President and CISO Deneen DeFiore.

When it Comes to AI Making a Meaningful Impact for Security Orgs, Detection/Response and Product Security Lead The Ways

Where do you feel AI has contributed to provide better security, privacy, and compliance for your organization?



Source: Notable Capital Security Survey

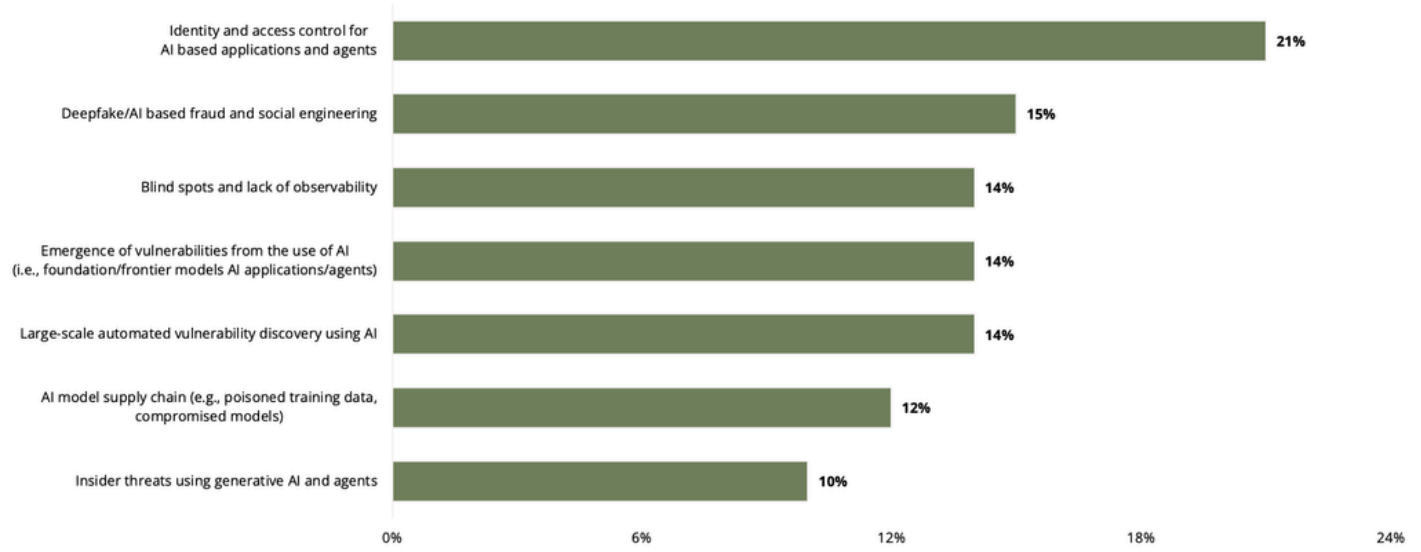
Notes:
1. Represents findings from nearly 150 CISOs and security leaders surveyed

The opportunity for AI startups is securing rapidly growing AI use cases: Over the next 12 months, rapid AI adoption will make evergreen problems worse. According to the survey, 21% of CISOs labeled identity and access management the most concerning AI-based threat, while 14% highlighted observability: "The market has not figured those two domains out," said Delta Dental Plans Association CISO Alex Green. "In a perfect world, AI should be able to observe how agentic identities operate and infer what data they actually need to access and under which circumstances. That would solve the vast majority of our problems as agents proliferate," he added.

Notable Capital

AI Makes Long-Standing Challenges Like Identity and Access Management More Troublesome

Which of the following AI-based threats are you most concerned about in the next 12 months?



Source: Notable Capital Security Survey

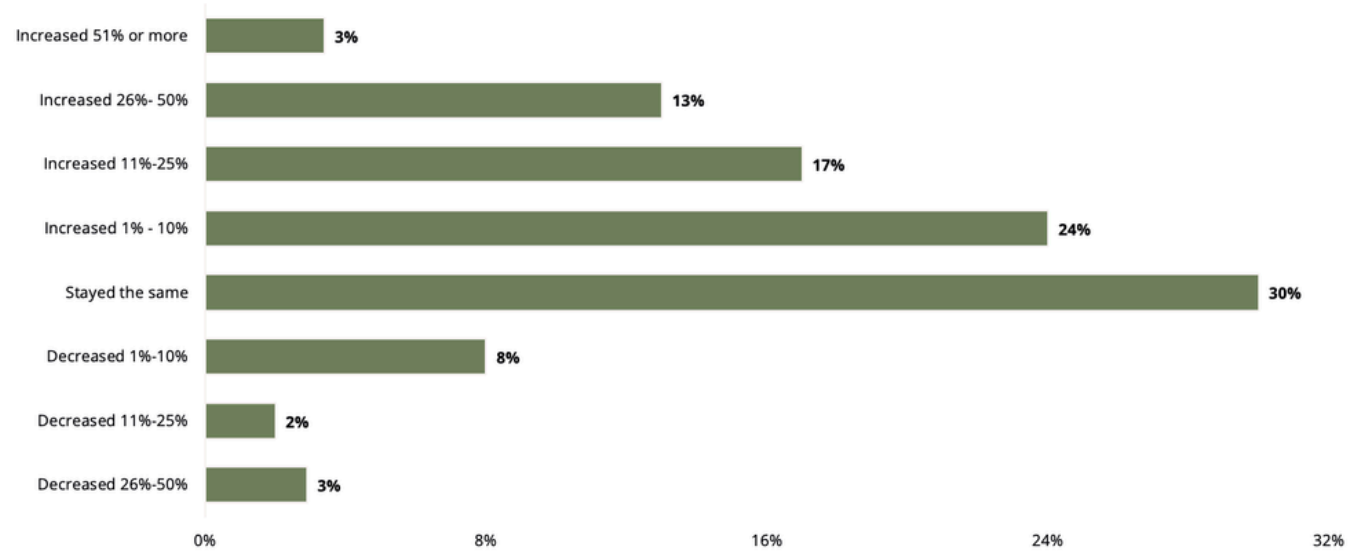
Notes:
1. Represents findings from nearly 150 CISOs and security leaders surveyed

CISOs have more money to spend, but more demands on their budgets: A quarter of security leaders expect budgets to increase as much as 10%, while nearly one-third expect gains of as much as 30%. But while coffers may be growing, so are the demands on those funds. More money doesn't necessarily mean more talent or vendors. Increasingly, CISOs are also looking at how they can build agentic capabilities to enhance their preventative, detective, and response capabilities, while also reducing costs.

Notable Capital

Cybersecurity Budgets are Growing

Please indicate how your cybersecurity budget has changed between 2025 and 2026



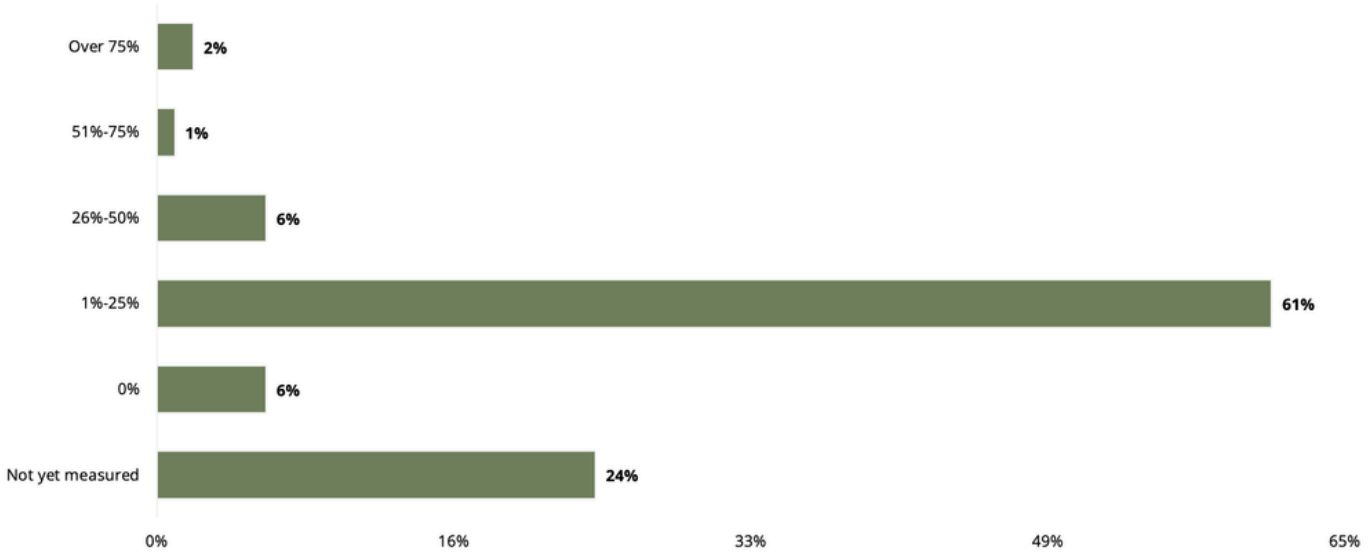
Source: Notable Capital Security Survey

Notes:
1. Represents findings from nearly 150 CISOs and security leaders surveyed

Notable Capital

For Most CISOs, AI Enablement is a Smaller Portion of the Security Budget

What percentage of your security budget is currently allocated to supporting AI enablement within your organization?



Source: Notable Capital Security Survey

Notes:
1. Represents findings from nearly 150 CISOs and security leaders surveyed

Build or buy? The classic question gets more complicated.

AI is adding new wrinkles to the classic "build vs. buy" debate, and many CISOs are still figuring out the new balance.

AI coding tools make it easier than ever for internal teams to build applications or extend existing platform capabilities. Security leaders are embracing the opportunity to consolidate a vendor-heavy landscape with custom-built tools and flexible systems that their employees can easily integrate.

"Teams, especially engineering-driven ones, will innovate with the latest AI products and tools faster than ever before," said Jiphun Satapathy, CISO at Motive.

Platforms showcase their staying power

While CISOs may be able to sunset some external point solutions, replacing the foundational, battle-tested platforms will be much tougher — especially as AI makes it easier for these large providers to innovate at the speed of smaller rivals.

"Building or adding new capabilities will be much less expensive and much faster than it used to be," said Jiphun Satapathy. As a result, "platforms are expanding much quicker than they have in the past," he added.

For example, web application firewalls used to be one of the largest portions of Delta Dental's security budget. Now, with WAF a largely commoditized capability and available within most security platforms, the team can monitor and block suspicious or malicious network traffic for much cheaper. As a result, investment was redirected to data security, a growing problem as AI expands access.

"Because AI has helped us be more effective with legacy problems, we've been able to find the money for newer problems," said Delta Dental's Alex Green. "Now, data security is the largest line item in the budget."

CISOs play the AI waiting game

Security teams have a reputation as early technology adopters. But cutting-edge capabilities are now replicated by competitors in months, not years — either by platform providers, other startups, or the AI labs. In the time it takes to implement and integrate a new tool, a more appropriate one may have already come along.

It's why CISOs are more willing to wait longer to invest in best-of-breed solutions: "When there's a great, niche AI security capability, a month later it's now in six other tools that also have way more functionality," said Green.

But despite tougher competition from platform providers and more stringent evaluations from potential customers, specialized, standalone applications will still be vital to security operations, especially to keep CISOs from consolidating too much to a single provider.

“We don't want to get tightly tied to a vendor product. Lock-in is a real issue,” said Motive’s Jiphun Satapathy.

Conclusion

Whenever there are technology transformations of this magnitude, adoption always outpaces security. But AI is much different than past revolutions, and the consequences of poor security are far more significant. Now, even minor issues can quickly become crises that tarnish brand reputations and impact growth.

There’s an urgent need for more powerful security tooling, but CISOs have more flexibility than ever before in how they onboard the capabilities they need. The smartest CISOs will use a combination of building, buying, and extending existing platforms to improve how their own teams function, and protect the business as the AI generation progresses.

Our Rising in Cyber 2026 list is evidence of how quickly AI-native startups are challenging legacy markets. While CISOs may be one step behind AI adoption today, the technology is here to help them get back to a confident security stance.

Legal Disclaimer