NIGHTDRAGON

SPECIAL REPORT: CYBER LEADERS ON 2024 TRENDS AND 2025 OUTLOOK

Top cybersecurity leaders in the NightDragon Advisor Council provide perspective on 2024 trends and 2025 spending outlook

February 2025

Foreward

As we enter 2025, cybersecurity leaders find themselves navigating an evolving financial landscape. While some CISOs report tightening budgets, they remain committed to strategic investments that drive innovation and resilience. The role of the CISO is more strategic than ever, with cybersecurity firmly established as a boardroom priority.

For the third year, NightDragon has conducted an annual anonymous survey of our Advisor Council, which includes 100 top CISOs and other cybersecurity leadership from some of the nation's most prestigious and influential firms. In this report, we share what CISOs shared about if their budgets are going up or down, where they're investing, and what innovations they're placing their bets on.

Our year-over-year data reveals a nuanced picture: although 29% of CISOs indicate a decrease in cyber spending for 2025, the majority are maintaining or increasing their budgets to stay ahead of emerging threats. Notably, 50% anticipate budget growth, underscoring the continued importance of cybersecurity in today's digital economy. Even those facing constraints are prioritizing investments in key technologies that enhance operational efficiency and risk management.

For cyber startups and platform providers, this means a refined approach to go-to-market strategies is critical. It is no longer sufficient to position solutions solely on the basis of security capabilities—CISOs demand clear, measurable value. Solutions must demonstrate not only how they enhance security posture but also how they integrate into broader business objectives and optimize costs.

Trusted advisors, partners, and investors play an increasingly vital role in this ecosystem. As CISOs balance cost pressures with the imperative to innovate, those who can provide strategic guidance and tailored solutions will be invaluable. Whether through collaborative partnerships, co-development of solutions, or expert advisory services, aligning with CISOs' evolving priorities will be key to success in 2025 and beyond.

This report delves into the shifting spending trends among CISOs, offering insights into where budgets are being allocated, which technologies are seeing increased investment, and how cybersecurity vendors can align with these strategic priorities. By understanding these dynamics, industry stakeholders can better support CISOs in their mission to protect organizations while delivering value.

Table of Contents

Introduction

The NightDragon Advisor Council includes more than 100 leading CISOs, cyber experts and former government officials. These leaders come from Fortune 500 and other large enterprise organizations from a variety of critical verticals, including healthcare, finance, travel, critical infrastructure and more.

In this survey, NightDragon Advisors anonymously provided input into spending trends for 2024 and 2025, as well as what technology investments they were making (and some they weren't). They also provided insights into what risk areas concerned them the most last year, as well as what areas of risk they were prepping for in 2025.

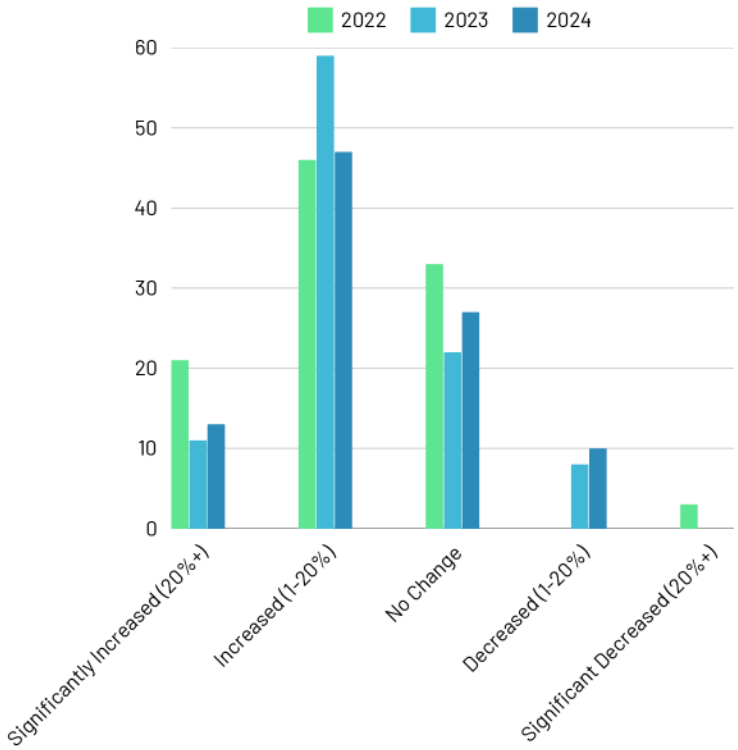
A select outline of the findings can be found below:

Findings

The majority of CISOs (60%) reported that their budgets either increased or significantly increased in 2024 from the prior year. This percentage was slightly down from prior years (70% in 2024 and 67% in 2023), but still represented the vast majority of CISOs overall.

Nearly a third of CISOs reflected their budget stayed flat year over year from 2023 to 2024. Against the economic climate, we feel these numbers are overall optimistic on the state of cybersecurity spending today.

Did Your Cyber Budget Increase or Decrease YOY?



What were your Top Investment Areas in 2024?

CISOs shared the three largest budget areas that they invested in 2024. These answers included a mix of technology and talent investments as CISOs looked to grow their teams and grapple with new cyber threats.

Only 17% said they decreased their spending on any cybersecurity category in 2024, down significantly from 32% in 2023. That said, 29% said they expect to decrease spending on at least one category in 2025.

Some of the most popular answers on most impactful investment areas over the past year included (in no particular order):

- Identity and Access Management
- Headcount Increases or Insourcing Roles
- Threat Intelligence
- API Security
- Application Security
- Data Security and Data Management (Ex. DPSM)
- Artificial Intelligence Security
- Endpoint Security
- Cloud Security Protections (Ex. SSPM)
- Breach and Attach Simulation Exercises
- SIEM
- Automation

"In 2025, CISOs are no longer just defenders. We are business enablers, driving security as a competitive advantage in a digital-first world. AI-driven threats are accelerating, but so are the tools at our disposal. The choice is simple. Innovate or fall behind. Smart investments in automation, predictive intelligence, and zero-trust are not just about risk reduction. They are the foundation of resilience, growth, and industry leadership. The organizations that see cybersecurity as a catalyst for success rather than a cost center will be the ones that dominate the future."

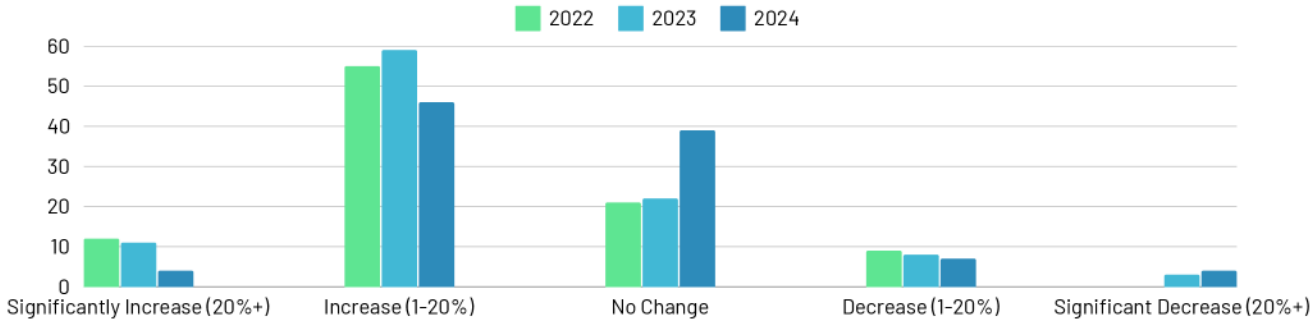
– JASON ELROD, CISO, Multicare

Are Cyber Budgets Going Up or Down?

As we look forward into the remainder of 2025, half of CISOs said they expect their budgets to increase or significantly increase over the course of the year (50%). An increasing amount of CISOs reported flat budgets expected in 2025, rising from 21% in 22 and 22% in 2023 to 39% this year.

We did see an increasing number of CISOs reporting that their budgets would decrease in 2025, rising from 8% reporting either decreasing or significantly decreasing budget last year to 11% this year. However, this still represents a small minority of the overall percentage of CISOs, showing overall cyber budgets remain strong.

I Expect my Budget Next Year to..



*Note 2024 answers reflect perspectives on 2025 budgets, 2023 answers reflect 2024 budget and 2022 answers reflect 2023 budget

CISOs shared what areas they expect to funnel those investments into, highlighting a number of key technology and personnel categories, including:

- Identity and Access Management
- Legacy technology coverage
- Data security
- AI Security
- Insider threat protection
- Continuous controls monitoring
- Skills advancement around AI
- SASE for cloud security
- Third-party and supply chain risk management
- Automation
- Tools rationalization

CISOs Share Biggest Risk Areas They're Watching

At the beginning of 2024, the World Economic Forum highlighted cyber insecurity as one of the biggest Global Risks in its Global Risks Report 2024, alongside extreme weather, AI-generated misinformation and disinformation, societal and political polarization and increasing cost of living.

CISOs sit on the front lines of this global threat, defending their organizations from today's biggest cyber risks. In our survey, they shared what risks kept them awake at night in 2024. Here are some of the most common answers:

- Legacy technology
- Insider threats
- Third-party and supply chain risk
- Identity compromise
- AI compromise or threats
- Ransomware
- Bot mitigation
- Phishing and social engineering (BEC and ransomware)
- Data security
- Regulation and compliance
- Operational technology threat detection and response
- Change management
- Cloud security risks

"My top cybersecurity focus for 2025 is to keep company and customer data secure, ensure that employees are following best security practices and lead a world class team of forensic and threat-intel experts."

- MIKE ROSEN
CISO, iVerify

Trends to Watch in 2025

As we look towards 2025, CISOs said they expect to see trends emerging and evolving around artificial intelligence, vendor consolidation, and new attack vectors.

Here are some of the trends they featured in their predictions for 2025:

ARTIFICIAL INTELLIGENCE EXPLOSION

The rapid expansion of AI was the most commonly cited trend by CISOs. They said they expected to see it mature as a cyber category in 2025, as well as see prioritization around safe AI usage and enhanced data security measures to mitigate emerging risks.

SCRUTINY ON CYBER SPENDING

While cybersecurity budgets are not necessarily shrinking, security leaders anticipate increased scrutiny over expenditures. CISOs are being asked to provide stronger justifications for investments, ensuring alignment with business priorities and risk mitigation strategies.

VENDOR CONSOLIDATION

The industry is witnessing a shift from a "best-of-breed" approach to a preference for integrated platform solutions. Organizations are consolidating vendors to streamline security operations, reduce complexity, and improve overall efficiency.

THIRD-PARTY RISK

The number of third-party-related cyberattacks surged in 2024, highlighting vulnerabilities in supply chains and external partnerships. This trend is expected to accelerate in 2025, pushing companies to strengthen due diligence and risk management practices.

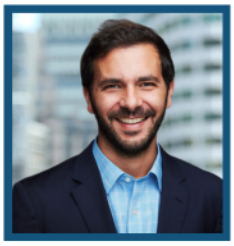
Trends to Watch in 2025

interos.ai

TED KRANTZ, CEO, INTEROS

As global interconnectivity deepens, the scale and speed of cyber breaches ripples across the globe quicker than ever, amplifying the "blast radius" of attacks. In the first 10 months of 2024, 15,137 companies were impacted by reported cyber attacks, according to interos data. This multiplied out to 1.3 million tier 1 suppliers, 3.1 million tier 2 suppliers and 3.8 million tier 3 suppliers. As today's supply chains rely more heavily on networks with many tiers of suppliers, the expanded attack surface of businesses must be approached with more diligence. In 2025, organizations must adopt advanced attack surface management strategies to gain visibility into their entire supplier networks to fully assess their exposure to cyberattacks.

These strategies include uncovering hidden supplier relationships, evaluating the cyber vulnerabilities of both direct and sub-tier suppliers, and assessing a broad spectrum of risk categories. Companies will also focus on identifying over-reliance on single suppliers and visualizing geographic clusters to mitigate cyber risks when they are impacted. By embracing these measures in the upcoming year, organizations can reduce their exposure to cyber threats, protect their digital supply chains, and ensure resilience in an era of ever-expanding cyberattack surfaces.



ONAPSIS

MARIANO NUNEZ, CEO, ONAPSIS

More organizations will need to accelerate their critical SP cloud transformation projects in 2025. With the 2027 migration deadline looming, many companies are already behind and will face increasing pressure to rush these critical initiatives. Given the heightened exposure and risks associated with moving SAP to the cloud, it will be imperative that CISOs and CIOs collaborate to prioritize compliance and secure-by-design controls to avoid delivering transformations exposed to significant risk. We're enabling more organizations to do this through our newly released Onapsis Secure RISE Accelerator, designed to help organizations achieve these goals while embedding security from day zero. Those who decide to go down this path will be able to accelerate and de-risk their transformations projects and go-lives, without sacrificing security and compliance.

Trends to Watch in 2025

HUMAN

STU SOLOMON, CEO, HUMAN

In 2025, the combination of artificial intelligence and cybercrime will transform the threat landscape. Large-scale bot operations will continue to enable fraudsters to carry out automated attacks with unprecedented speed and sophistication. Digital advertising, content publishing, and customer accounts will become key battlegrounds as AI-driven tools enhance the scale of fraud, account takeovers, and synthetic identity creation. New hybrid monetization models on AI chatbot platforms will become targets for exploitation.

Meanwhile, traditional defenses, such as image-based CAPTCHAs, have become ineffective. Businesses must prepare for this new reality by adopting advanced cybersecurity solutions to maintain trust and ensure the authenticity of digital interactions in an increasingly automated world. Learn more in "The Hidden Hand of AI: How Bots Shape Cyber Threats in 2025.

iboss

PAUL MARTINI, CEO, IBOSS

2024 was a major year for SASE, or Secure Access Service Edge, which consolidates networking and security functions into a cloud delivered service. The idea of leveraging a large number of network appliances and various network security point products for malware defense and data loss prevention is no longer a sustainable strategy from the perspective of complexity, cost, and management overhead. The consolidation of SD-WAN, ZTNA VPN replacement, and Secure Internet Access accelerated as well with a drive toward consolidation. The vast amount of visibility SASE provides has also accelerated the use of AI to identify and remediate compliance and security threats within an organization.

Best-of-Breed vs. Best-of-Suite?

For years, cybersecurity decision-makers have debated whether to adopt a "best-of-breed" approach—selecting top solutions from different vendors for specific security needs—or a "best-of-suite" strategy, which consolidates security tools within a single vendor's ecosystem.

Best-of-breed solutions are designed to excel in specific areas, whether endpoint detection and response (EDR), identity and access management (IAM), or cloud security. Organizations that embrace best-of-breed solutions are more likely to also embrace innovative, cutting-edge startups that likely focus more on a specific feature or category, versus a broad set of solutions. However, integrating multiple best-of-breed solutions can present challenges, including higher complexity and increased overhead costs.

However, in recent times, the growing complexity of cybersecurity, coupled with the shortage of skilled professionals, has led many organizations to lean recently toward best-of-suite offerings. Large security vendors now provide end-to-end platforms covering everything from network security to endpoint protection, and more. Best-of-suite approaches can be more cost effective, less complex and with easier management, but can leave gaps in functionality, cause vendor lock-in and have slower innovation cycles.

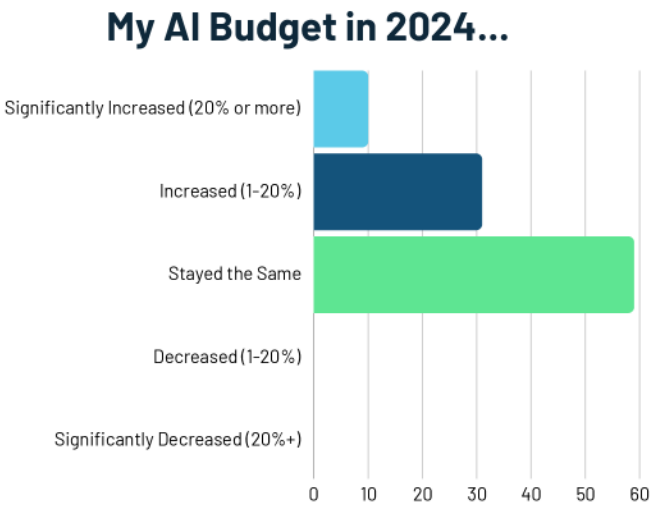
The pendulum has swung between best-of-breed and best-of-suite – and vice versa – as the threat landscape has evolved and economic situations have changed, causing cyber budgets to open or constrict in response. In addition, regulatory changes and overall changes in IT infrastructure trends have helped move the pendulum over time.

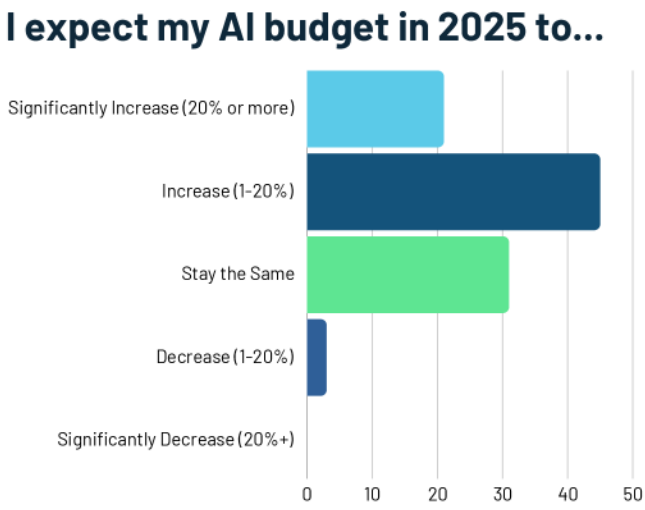
However, it's not a universal all-or-nothing pivot, as CISOs pointed out. Ultimately what matters most is the best cybersecurity outcomes for customers. "Cybersecurity has long been framed as a choice between platforms and best-of-breed solutions—but customers need both. The real measure of a platform isn't just its technology, but how seamlessly it unites best-in-class solutions at scale, delivering an optimized end-to-end experience," said Raja Patel, Chief Product Officer, at Sophos.

2025 Investment in AI

As artificial intelligence continues to reshape the cybersecurity landscape, CISOs said they are prioritizing strategic investments in AI-driven technologies to enhance security outcomes while also ensuring the security of AI itself as it sees increased adoption across the enterprise.

In 2024, AI investment among security leaders ranked AI as a 6.7/10 average priority level within their organization, reflecting a strong but evolving commitment to the technology. While 58% of CISOs reported that their AI budgets remained the same in 2024 versus the year prior, a combined 41% saw increases, with 10% experiencing significant budget growth of 20% or more. Looking ahead to 2025, the trend toward greater investment is even more pronounced, with 66% of CISOs expecting budget increases and 21% anticipating significant growth.





This upward trajectory underscores the expanding role of AI in cybersecurity, as organizations leverage its capabilities across a wide range of security functions. CISOs cited governance risk and compliance, threat intelligence, email security, access monitoring, threat hunting, insider defense, anomaly detection, and risk modeling as some of the most impactful AI-driven use cases in 2024. These applications demonstrate AI's ability to automate complex security tasks, enhance threat visibility, and accelerate response times—critical advantages in an era of escalating cyber threats.

Beyond threat detection and response, AI is also being deployed to improve team efficiency and productivity, offering support in areas such as coding assistance and security operations automation. By reducing manual workloads and optimizing resource allocation, AI is helping

2025 Investment in AI

security teams manage growing attack surfaces with greater agility.

However, as organizations integrate AI into their security ecosystems, they must also invest in securing the very AI technologies they deploy. The rapid adoption of AI introduces new risks, from adversarial attacks to data poisoning, making AI governance and security a top priority. Enterprises are increasingly focusing on AI model integrity, data protection, and regulatory compliance to ensure their AI-driven defenses do not become security liabilities themselves.

As 2025 approaches, the dual imperative for CISOs is clear: harness AI to strengthen cybersecurity while fortifying AI systems against emerging threats. With increased budgets and a growing number of proven use cases, AI is set to become an even more indispensable tool in the security arsenal.

"In 2025, AI in cybersecurity is no longer optional—it's an imperative. The rapidly evolving threat landscape necessitates the adoption of artificial intelligence (AI) in cybersecurity. AI's capacity to readily scale and automate attacks currently provides a significant advantage to malicious actors. Effective defensive AI deployment, however, requires robust orchestration and coordination across security tools, a capability currently hindered by the lack of transparency and explainability in many existing AI-powered defense systems. We have to prioritize AI solutions that are explainable, resilient, and secure by design—ensuring that while we leverage AI to outpace cyber threats, we don't create new vulnerabilities and risks in the process."

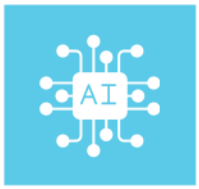
- DR. CHRISTOPH PEYLO, Chief Cyber Security Officer, Bosch

"CISOs in 2025 are aggressively evaluating AI investments to enhance security, but we must be just as vigilant about the risks these technologies introduce. We're prioritizing AI solutions that are explainable, resilient, and secure by design—ensuring that while we leverage AI to outpace cyber threats, we don't create new vulnerabilities in the process. Smart AI adoption is about balance: innovation with caution, automation with oversight, and speed with security."

- VIJAY BOLINA, Chief Information Security Officer, Google DeepMind

NightDragon Perspective

As we move into 2025, the cybersecurity market presents a compelling landscape for investors, driven by evolving threats, shifting enterprise priorities, and strategic budget allocations by CISOs. While cybersecurity spending is under heightened scrutiny, investment in critical areas remains robust, signaling strong market opportunities for security vendors, platform providers, and innovative startups.



AI IS CYBERSECURITY GAME CHANGER

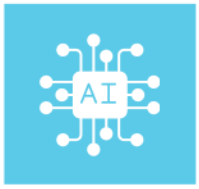
Artificial intelligence is emerging as one of the most impactful investment areas in cybersecurity, both as a defensive tool and as a risk factor requiring mitigation. For investors, this presents a dual opportunity: backing AI-powered cybersecurity platforms that enhance threat intelligence, anomaly detection, and risk modeling, while also supporting solutions that address the security challenges AI itself introduces, such as adversarial attacks and data integrity risks. Companies that can provide AI security governance and assurance frameworks will see growing demand as enterprises seek to mitigate AI-related vulnerabilities.

CONSOLIDATION DRIVING PLATFORM INVESTMENT

With vendor consolidation emerging as a key trend, cybersecurity companies that provide end-to-end security solutions and seamless integrations are positioned for success. This presents an opportunity for established security vendors to expand market share through acquisitions, while startups with strong interoperability and automation capabilities will attract enterprise adoption.

From an investment standpoint, cybersecurity companies that emphasize efficiency, interoperability, and cost savings will have a competitive edge. With CISOs facing greater scrutiny over spending, security solutions must not only demonstrate technical efficacy but also provide measurable business value. Investors should prioritize companies that enable automation, reduce operational complexity, and improve security outcomes without requiring excessive resource allocation.

NightDragon Perspective



THIRD-PARTY RISK AND SUPPLY CHAIN SECURITY AS A GROWTH MARKET

Third-party and supply chain attacks surged in 2024, and CISOs expect this trend to intensify in 2025, creating significant demand for risk management solutions. With increasing regulatory pressure around supply chain security, companies providing continuous monitoring, risk assessment, and attack surface management for third-party ecosystems are positioned for growth. Companies that offer the capabilities to provide visibility into supply chain vulnerabilities and integrate risk assessment into broader cybersecurity platforms will benefit from this dynamic.

CLOUD AND IDENTITY SECURITY AS PRIORITY INVESTMENT AREAS

CISOs identified identity and access management, data security, and cloud security as major budget priorities heading into 2025. The acceleration of Secure Access Service Edge (SASE) adoption and the growing importance of zero trust architectures present significant investment opportunities. Vendors offering identity-based security, privileged access management, and cloud-native security solutions will remain attractive targets for funding and acquisition.

A MARKET RIPE FOR STRATEGIC INVESTMENT

While cybersecurity budgets are under scrutiny, spending remains strong in key areas, particularly AI, vendor consolidation, supply chain security, and identity protection. Investors should focus on companies that address enterprise efficiency needs, integrate seamlessly into existing security frameworks, and align with the evolving threat landscape. With cybersecurity firmly positioned as a boardroom priority, the sector remains a compelling space for strategic investment and long-term growth.

Media Contact

NightDragon
Sarah Kuranda Vallone, VP Marketing
sarah@nightdragon.com