Cobalt

CISO Perspectives Report 2025

AI and Digital Supply Chain Risks

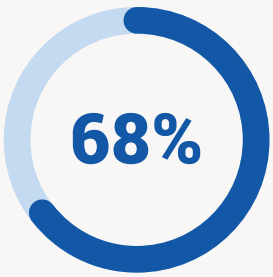
Contents

Introduction: Why CISOs Worry

The digital supply chain has become cybersecurity's weakest link—and security leaders know it. Over two-thirds (68%) are concerned about the risks these third-party software tools and components introduce across their technology stacks. In our recent survey of 225 security leaders (defined as a mix of C-level and VP-level security professionals) in organizations with 500-10,000 employees[1], we learned that, although four out of five express confidence that their organizations meet regulatory security requirements, 60% acknowledge that attackers are evolving too quickly to maintain a truly resilient security posture.

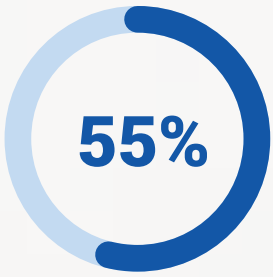
What's at stake? Both company reputation and personal accountability. More than half (55%) of security leaders say they're constantly worried that one employee mistake could put the entire organization at risk. This ever-present anxiety underscores how cybersecurity has shifted from a technical issue to a strategic imperative.

Security leaders have broad concerns, from AI to insider threats

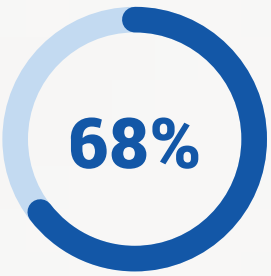


Concerned about third-party software and components

Believe attackers are evolving too quickly



Worried employees could put organization at risk



View the secure deployment of genAI as critical

[1] Survey of 225 C-suite or VP-level individuals, conducted in early 2025, by Emerald Research Group on behalf of Cobalt.

As threats evolve, cybersecurity has become a boardroom-level priority—on par with revenue growth and digital transformation. And genAI is only raising the stakes. While third-party software remains the top concern (66%), nearly half (46%) of security leaders are also uneasy about AI-driven features and large language models (LLMs). In fact, 68% say their boards now view the secure deployment of genAI as a critical priority.

These concerns are validated by actual pentests: Cobalt pentests of LLMs and AI applications found that 32% had high-risk vulnerabilities, the highest level of serious findings from any type of pentest.

Top attack vector concerns

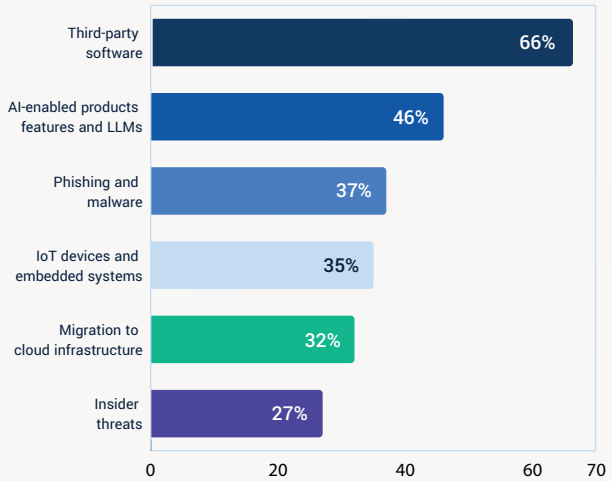


Figure 1. Source: Survey of security leaders

Security leaders are calling for stronger controls, faster remediation, and greater visibility into emerging AI risks. They understand that innovation without security is a risk multiplier, not a competitive edge. As organizations accelerate digital adoption, the margin for error shrinks. In this high-stakes environment, the pressure is on to anticipate, adapt, and act.

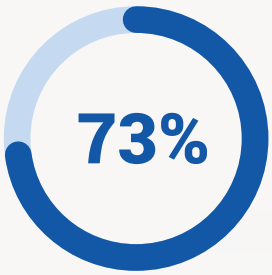
Security leaders' confidence in their organization's security posture and compliance is reinforced by the adoption of cybersecurity insurance and formal service-level agreements (SLAs) for issue resolution. A strong majority (80%) carry third-party cybersecurity insurance, while another 11% opt to self-insure. In parallel, 76% of organizations have established defined SLAs to guide the remediation process, with 43% targeting threat resolution for critical systems within three days or less. These proactive measures underscore the growing recognition among both security leaders and boards that cybersecurity is a fundamental business priority.

Securing the Digital Supply Chain

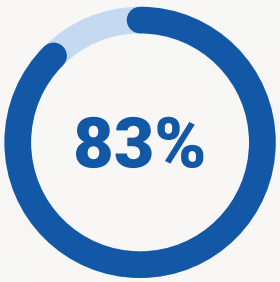
Today's software development environment is highly interconnected, relying on a blend of proprietary code, open-source libraries, and third-party services. This complexity increases exposure: 73% of surveyed executives reported receiving at least one notification of a software supply chain vulnerability or incident in the past year. For enterprises dependent on extended ecosystems, a single weak link can disrupt the entire operation.

Stakeholders have taken notice. Eighty-three percent of organizations now face formal requirements to demonstrate the security of their vendor ecosystems. This has moved beyond simple questionnaires: 56% require penetration testing for all third-party software before deployment, and 53% mandate ongoing vulnerability reports from suppliers. Security has become a continuous, collaborative effort.

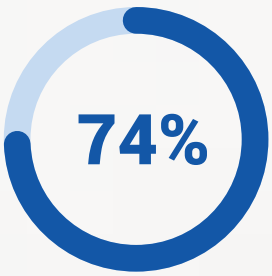
Security leaders see the digital supply chain as a strategic risk



Notified of supply chain vulnerability or incident in the past year



Now face formal requirements to demonstrate vendor security



Believe regular pentesting enhances credibility with customers

Even with these steps, concerns remain. Security leaders want greater assurance that their software partners meet the same security standards they enforce internally. To address this gap, organizations are implementing multiple layers of oversight, with pentesting (48%) at the forefront of these activities.

Methods for securing software supply chain

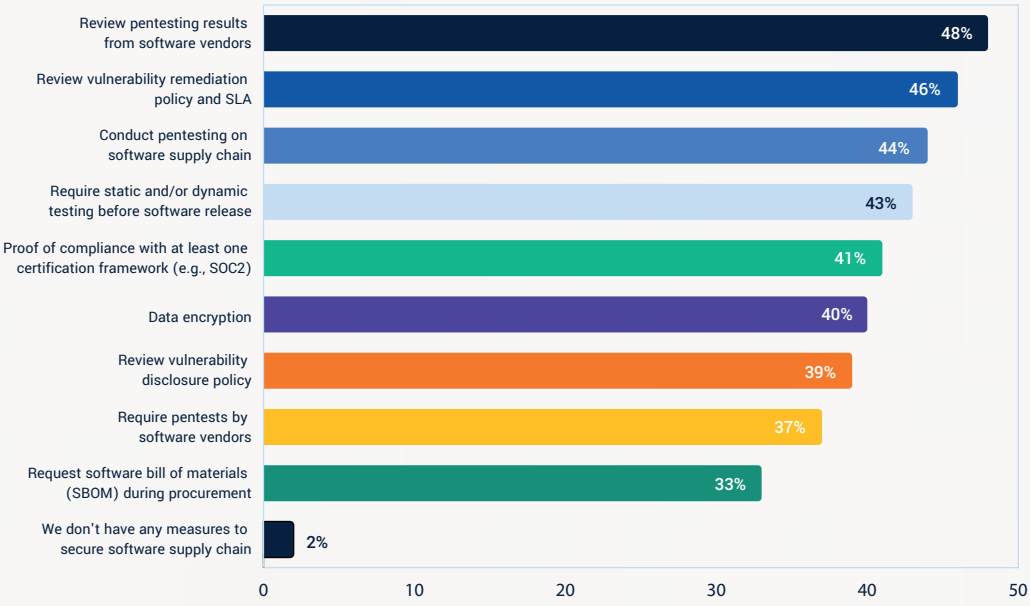


Figure 2. Source: Survey of security leaders

These measures aren't only about risk mitigation—they also reinforce customer trust. Seventy-four percent of security leaders believe regular, documented pentesting enhances credibility with clients and can offer a competitive edge in procurement.

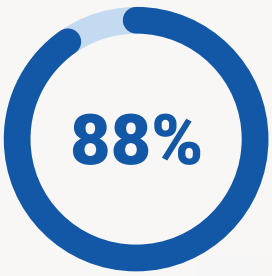
Pentesting: A Strategic Priority

There's always been a level of risk and concern associated with vendors and the supply chain process. With the integration of genAI into tools and workflows that process sensitive data, third- and fourth-party vendors are essentially creating new attack surfaces.

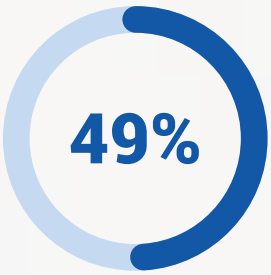
There is strong consensus among security leaders that the digital supply chain is a risk that must be evaluated proactively, and pentesting has emerged as a frontline tactic in their strategy. Nearly nine in ten security leaders (88%) consider pentesting to be a vital component of their organization's overall security efforts. It is not just a checkbox—it is a proactive measure designed to uncover and address vulnerabilities before they can be exploited.

Pentesting is increasingly integrated into the software development process as well, to provide assurances to regulators and customers, who are also concerned with third-party risk. Over half (58%) of security leaders report that their organizations are using pentesting to validate the security of the software they develop. This emphasis on independent testing is further supported by the use of third-party code reviews (55%), to supplement internal security testing (53%). These practices signal a deep commitment by security leaders to ensure the integrity and resilience of the software they create.

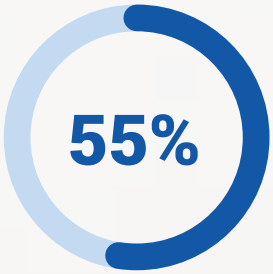
Pentesting is an essential part of software procurement and development



Consider pentesting vital to their organization's overall security



Plan to use pentesting to identify software supply chain vulnerabilities



Use third-party code reviews for secure software development

Require third-party pentests to validate security for customers

The application of pentesting is both widespread and strategic. Security leaders deploy it not only to assess critical systems (54%), but also to evaluate the security of web-facing applications (50%) and any systems that handle personally identifiable information (48%). Its usage spans the entire technology ecosystem, demonstrating its value as a core element of a comprehensive, risk-based security program.

Looking ahead, pentesting remains a top priority for future planning. Nearly half of security leaders (49%) intend to leverage it to identify vulnerabilities within their software supply chains—an area of increasing concern as third-party components become more embedded in enterprise environments. Additionally, 44% plan to apply it to uncover insider threat vulnerabilities, acknowledging that risks can arise from both external actors and within the organization itself.

Top pentesting objectives over the next 24 months

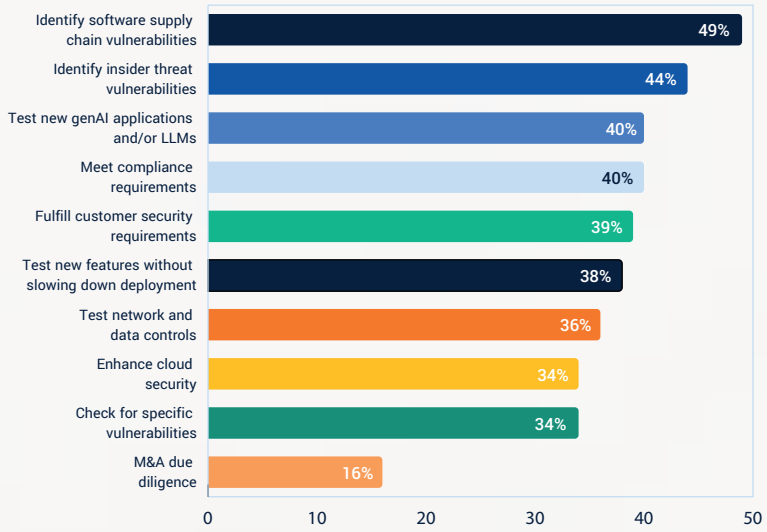


Figure 3. Source: Survey of security leaders

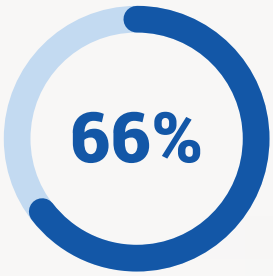
In an era where cyberthreats are more complex and dynamic than ever, pentesting provides not just validation, but actionable insights. It enables security teams to move from reactive defense to proactive risk management—an approach essential to protecting business continuity, customer trust, and long-term growth.

The Double-Edged Sword of GenAI

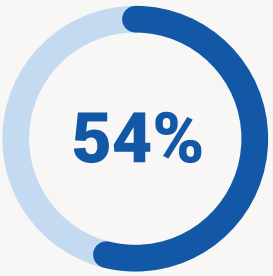
As organizations accelerate the integration of AI into core operations, security leaders are acutely aware that cyber adversaries are keeping pace—and, in many cases, staying a step ahead. Sixty-six percent of surveyed security leaders report that genAI is enabling attackers to rapidly analyze massive datasets, identify exploitable patterns, and evade traditional security defenses with greater precision and speed.

More than half (54%) are concerned that AI can now automate the entire attack lifecycle—from generating malicious code to adapting exploits in real time. Adding to the complexity, 62% worry that AI-assisted development tools may introduce hidden flaws and vulnerabilities that elude manual review processes, increasing the risk of supply chain compromise and codebase erosion.

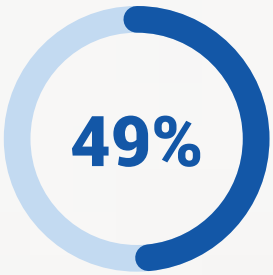
Security leaders cite genAI as a major source of risk in their organizations



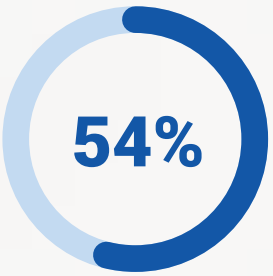
Say genAI helps attackers analyze data and evade defenses



Concerned AI can automate entire attack life cycle



Worried about sensitive information disclosure



Want dedicated tools to assess genAI security before deployment

At the center of this growing concern is data security. Forty-four percent of leaders cite model poisoning and intellectual property theft as their most pressing genAI-related risks. Others point to a wide range of threats, including training data leakage, unauthorized platform use, and the propagation of bias through AI-generated outputs. These vulnerabilities not only threaten technical integrity but also pose reputational and regulatory risks, especially as AI becomes a fixture in customer-facing applications.

Top genAI security concerns

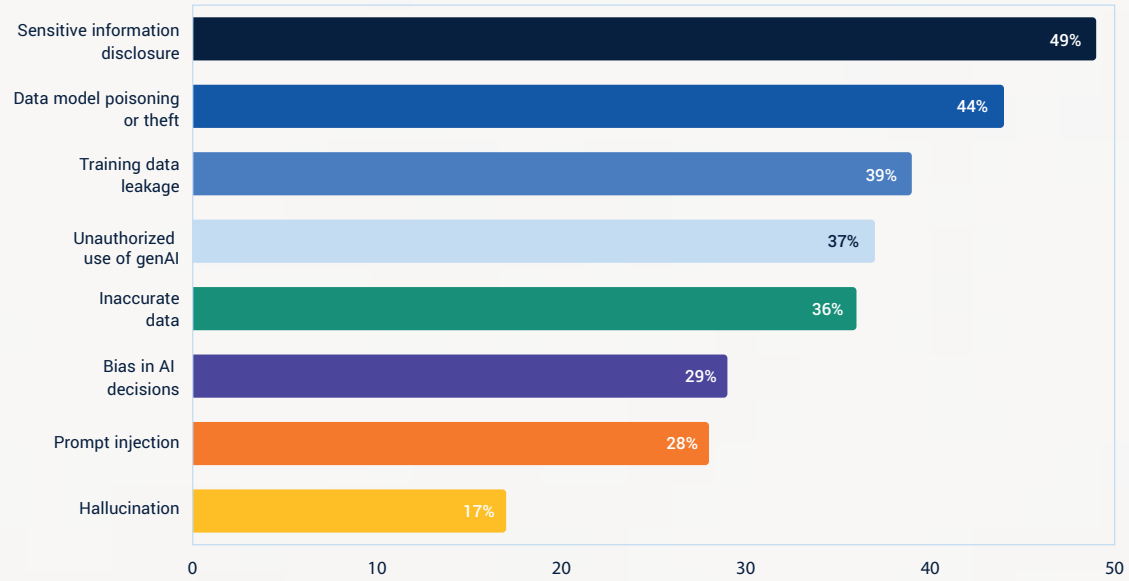


Figure 4. Source: Survey of security leaders

These survey responses point towards an emphasis by security leaders on protecting data assets from exposure, manipulation, or leakage through or by AI systems. These concerns are validated by findings from Cobalt pentests, with a caveat. The most prevalent issues are not unique to LLMs, but include many classic web application vulnerabilities. For example, the most common vulnerability was SQL injection, accounting for 19.4% of findings in these AI-focused tests. Another traditional web vulnerability, stored cross-site scripting (stored XSS), also ranked high at 9.7% (see Figure 5).

While data protection is the top concern, the vulnerabilities that pentests of LLMs and AI applications have uncovered are most often the methods and pathways (like prompt injection or insecure outputs) that could potentially lead to a data breach, if not properly addressed.

Top vulnerabilities in LLM pentests

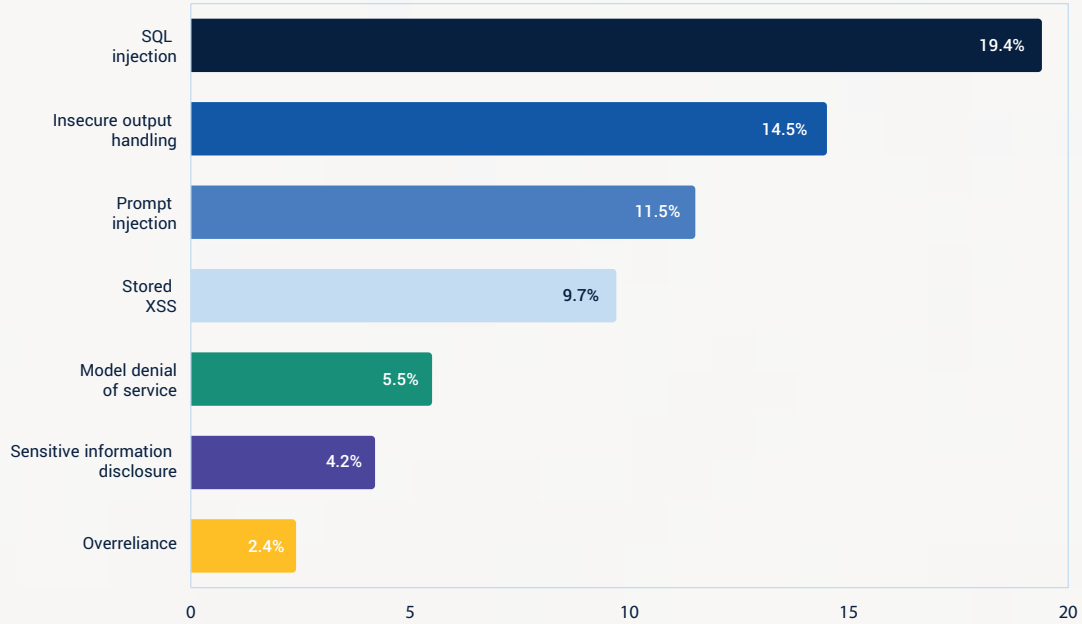


Figure 5. Source: Cobalt pentests.

In response, security leaders are calling for stronger safeguards and clearer standards. Over half (54%) want dedicated tools to assess the security of genAI systems before deployment, ensuring vulnerabilities are identified and mitigated early in the life cycle. An equal number are seeking strategic guidance on how to harness AI for defensive purposes—turning the technology from a liability into an asset. Additionally, 53% of security leaders are advocating for expanded educational initiatives to help teams understand the unique threat landscape introduced by AI. Nearly half (48%) want robust frameworks to detect and respond to AI-generated attacks, which are often more complex and dynamic than traditional threats.

As genAI becomes deeply embedded in digital products and services, 46% of executives emphasize the need for formal security protocols to protect user data and preserve customer trust. Without such guardrails, the promise of innovation may come at the expense of long-term security and brand reputation.

This evolving landscape underscores a critical truth: in the race to innovate with genAI, security can no longer be an afterthought. It must be a parallel track—fully integrated, continuously assessed, and rigorously enforced.

Conclusion: From Defensive to Offensive Security

Today's security leaders are updating security strategies to keep pace with new cyberthreats and digital risks. Their initiatives include:

- Integrating offensive security into every stage of the digital life cycle.
- Baking pentesting into vendor agreements.
- Pentesting AI features and capabilities as they are embedded in the organization.
- Setting aggressive timelines for mitigation of vulnerabilities.

This research shows that an offensive mindset may be the best defense in a world where a breach can happen at any moment. The digital supply chain is a primary battleground, with 66% of security leaders citing third-party software as their top concern. The rapid integration of genAI has introduced new, complex attack surfaces, with 68% of boards viewing its secure deployment as a critical priority. In response, an overwhelming 88% of security leaders now see pentesting as a vital component of their security strategy. More than half now require third-party pentest reports to validate the security of software they provide customers.

As organizations navigate this high-stakes environment, a proactive, offensive security approach is essential for building resilience and maintaining trust. An offensive security program moves beyond passive, reactive measures and adopts an adversarial mindset to proactively identify and remediate vulnerabilities before they can be exploited.

Key components of an offensive security program include pentesting of networks, applications, and cloud infrastructure; red team exercises that mimic advanced persistent threats (APTs) to test detection and response capabilities; and a programmatic

> "From a CISO's perspective, we need to reevaluate how we assess or conduct supply chain and third-party vendor risk assessment. We should update third-party assessment to include genAI disclosure, and classify models based on risk, data types, and potential exposure. We must also apply robust controls to all AI code pipelines, including model scanning testing and pentesting by security experts who understand these attack vectors."
>
> ANDREW OBADIARU, CISO, COBALT

approach to ensure full coverage across the organization's assets. A mature program integrates these activities directly into the development lifecycle and procurement processes, ensuring that security is a proactive consideration, not a reactive afterthought. The goal is not simply to find flaws but to understand their potential business impact and build a more resilient, battle-tested security posture.

A defensive-only approach, which waits for alerts, is fundamentally ill-equipped to handle attackers who use AI to automate exploit discovery and adapt their tactics in real time. Likewise, the interconnected nature of the digital supply chain means an organization's risk is extended through countless third-party tools and open source components, creating hidden attack surfaces.

An offensive security strategy is essential for illuminating these blind spots. By actively probing AI models for weaknesses like data poisoning and testing third-party software with the same rigor as in-house applications, organizations can uncover the very vulnerabilities that attackers seek to exploit. It provides the actionable intelligence needed to stay ahead of adversaries in a landscape where the perimeter is constantly shifting and expanding.

Recommendations for Security Leaders

To build a more resilient and proactive security posture, CISOs should consider the following:

1. **Demand greater transparency from vendors**
   Mandate that vendors disclose their use of genAI, including model origins and training data practices, to allow for proper risk assessment.

2. **Update vendor risk assessments for AI**
   Revise third-party assessments to include specific questions about genAI. Classify AI models based on their associated risks, the types of data they process, and their potential exposure.

3. **Integrate security into AI development**
   Apply DevSecOps principles to all AI code pipelines. This should include model scanning and pentesting by security experts who understand the unique attack vectors associated with AI.

4. **Proactively test the software supply chain**
   Make penetration testing a non-negotiable part of procurement and the entire software development life cycle.

5. **Secure the software you build**
   Embed security into your development life cycle with narrow-scope pentests for new features and secure code reviews for all software under development. This allows you to find and fix vulnerabilities before they reach production, turning security into an enabler for rapid innovation.

6. **Adopt a programmatic approach to offensive security**
   Move beyond ad-hoc testing to a structured program that secures your applications, infrastructure, and cloud environments. Layer comprehensive pentests on critical assets with regular attack surface monitoring to gain a complete and up-to-date view of your risk posture.

7. **Conduct regular red team exercises**
   Simulate real-world attack scenarios to test the effectiveness of your people, processes, and technology together, revealing how your defenses hold up against a determined adversary.

About Cobalt

Cobalt is the pioneer in pentesting as a service (PTaaS) and a leader in offensive security services.

We are focused on combining talent and technology with speed, scalability, and expertise. Thousands of customers and hundreds of partners rely on the Cobalt Offensive Security Platform, along with the industry's largest exclusive community of 450+ trusted pentesters and security experts, to find and fix vulnerabilities across their environments. By enabling faster pentest launches, real-time collaboration with testers, continuous scanning, and seamless integration with remediation workflows, we help organizations identify critical issues and accelerate risk mitigation so they can operate fearlessly and innovate securely.

Download the State of LLM Security Report

DOWNLOAD REPORT