Kai

2026 State of Autonomous Defense Report

© 2026 Kai

Table of contents

Executive Summary

Artificial intelligence has changed the economics of cyber conflict, and the security leaders responsible for defending the enterprise are feeling the effects firsthand. In a global survey of 500 chief information security officers (CISOs), a clear majority report that attackers currently hold the advantage, that their own defensive processes remain heavily manual, and that the pace of exploitation now outstrips the pace of human response.

The findings describe an industry in transition. CISOs exhibit a general confidence in their overall readiness, yet far fewer describe that readiness as strong. They rely on human labor to carry out the core work of vulnerability and exposure management, and that reliance is slowing remediation, deepening backlogs, and contributing to burnout across security teams. At the same time, leaders are clear about their future direction. Most expect machine-led operations to become the primary model within the next 12 to 18 months, signaling growing confidence that automation will become foundational to future cyber defense.

Key findings

Attackers have the advantage.	Sixty-three percent of CISOs believe attackers hold the greater advantage today, while only 18 percent credit defenders.
Vulnerability management is slow and manual.	Sixty-five percent say at least half of their vulnerability and exposure management is still performed manually. Sixty percent take more than seven days to remediate a critical vulnerability, and 48 percent leave a quarter or more of known vulnerabilities open beyond 30 days.
Security teams struggle with the workload.	Seventy-seven percent say vulnerability and exposure management contributes to security team burnout.
Trust and governance are slowing adoption of automation.	Lack of trust in automated decisions, at 52 percent, and governance concerns, at 43 percent, outrank budget, at 21 percent, as barriers to greater automation.
Advanced organizations are embracing machine-led security.	Today only 32 percent allow automated remediation actions without human approval, but forty-five percent expect vulnerability and exposure management to be mostly or primarily machine-led within 12 to 18 months.

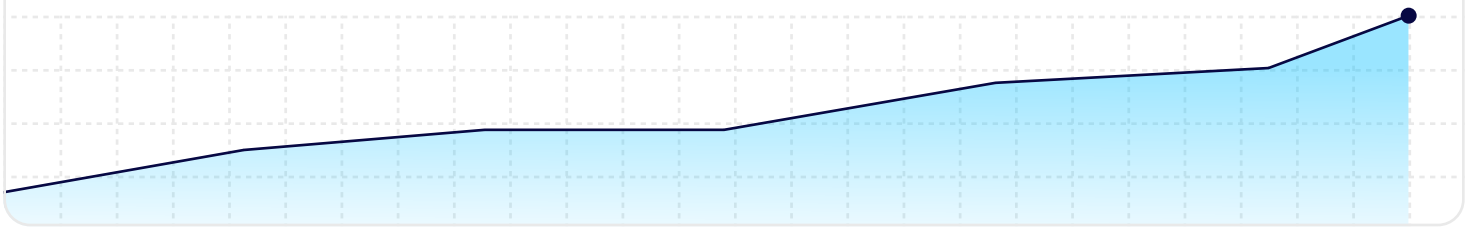
Taken together, the data points to an operating-model problem as much as a threat problem. The tools to find and prioritize risk are increasingly automated, yet the decision to act still rests with human hands. Closing that gap will be one of the central challenges of the next phase of enterprise defense.

Introduction

For most of the past decade, enterprise security has scaled by adding people, tools, and process. That model is now under strain. Adversaries have begun to apply automation and machine learning to reconnaissance, vulnerability discovery, and exploitation, compressing the interval between a disclosed weakness and an active attack. Defenders, meanwhile, continue to depend on human analysts to discover, triage, validate, and remediate.

To see an example of the imbalance that has arisen, we need look no further than the CVE program itself. The CVE program published 48,185 new vulnerabilities in 2025, an average of 132 every day, representing a 263 percent increase since 2020. The strain is now visible at the foundation of the ecosystem: in April 2026, NIST announced that the National Vulnerability Database would no longer attempt to analyze every CVE, moving instead to a triage model that prioritizes known-exploited and federally relevant flaws. The institution the entire industry relies on to score and contextualize vulnerabilities has acknowledged that the volume exceeds what its current model can process.

132 new CVEs were published every day in 2025, on average.

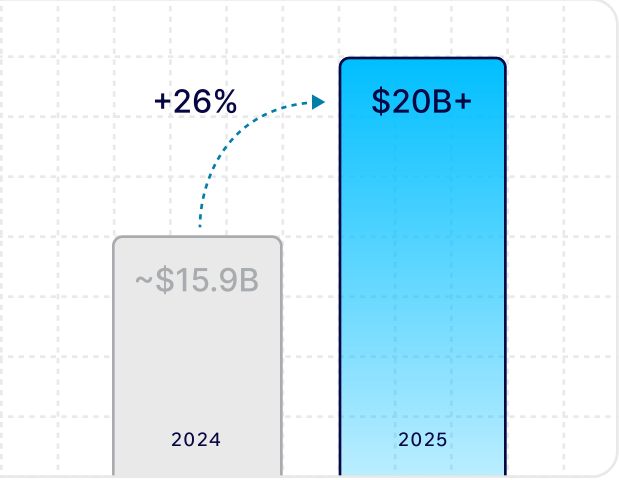


(NIST National Vulnerability Database)

Attackers are converting that volume into action faster than ever before. CISA's Known Exploited Vulnerabilities (KEV) catalog, the US government's registry of flaws confirmed under active attack, grew 20 percent in 2025. The financial consequences are climbing in parallel. The FBI logged more than $20 billion in reported cybercrime losses in 2025, a 26 percent increase over the prior year, and for the first time in the report's nearly 25-year history it tracked AI-enabled crime as its own category.

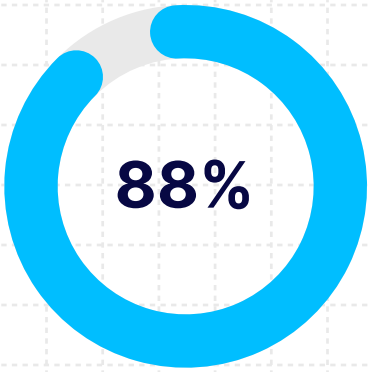
$20B+

in cybercrime losses were reported to the FBI in 2025, up 26 percent year over year.



(FBI Internet Crime Report)

The scope of today's challenges means that the traditional approaches to scaling simply won't work. In ISC2's 2025 study of more than 16,000 security professionals, 88 percent reported at least one incident or operational failure tied to a skills shortage, and a third said their organizations cannot adequately staff their teams. The gap between the work security demands and the labor available to perform it is structural, and hiring alone will not close it.



88%

of organizations report incidents tied to a skills shortage

(ISC2 2025 Cybersecurity Workforce Study)

This report examines how security leaders are responding to that mismatch. It draws on a survey of 500 CISOs at large enterprises from around the globe, conducted in June 2026. The questions were designed to measure how organizations perceive the AI-driven threat landscape and, just as importantly, how their own operations are structured to meet it, where automation already operates, where it stops, and what would allow it to go further.

01 / CISOs understand that attackers have the edge

Security leaders have a clear-eyed assessment of the current balance of power. As artificial intelligence matures on both sides of the conflict, most CISOs conclude that the advantage has shifted toward the offense.

Who holds the advantage

Asked to weigh the current state of AI adoption for both attackers and defenders, a decisive majority of CISOs place the advantage with the attacker. Sixty-three percent say offense holds the edge, including 12 percent who describe that advantage as significant, while just 18 percent believe defenders are ahead. The remaining 19 percent see the balance as roughly even. The pattern reflects a widely held view that adversaries have been quicker to operationalize automation for discovery and exploitation than most enterprises have been to operationalize it for defense.

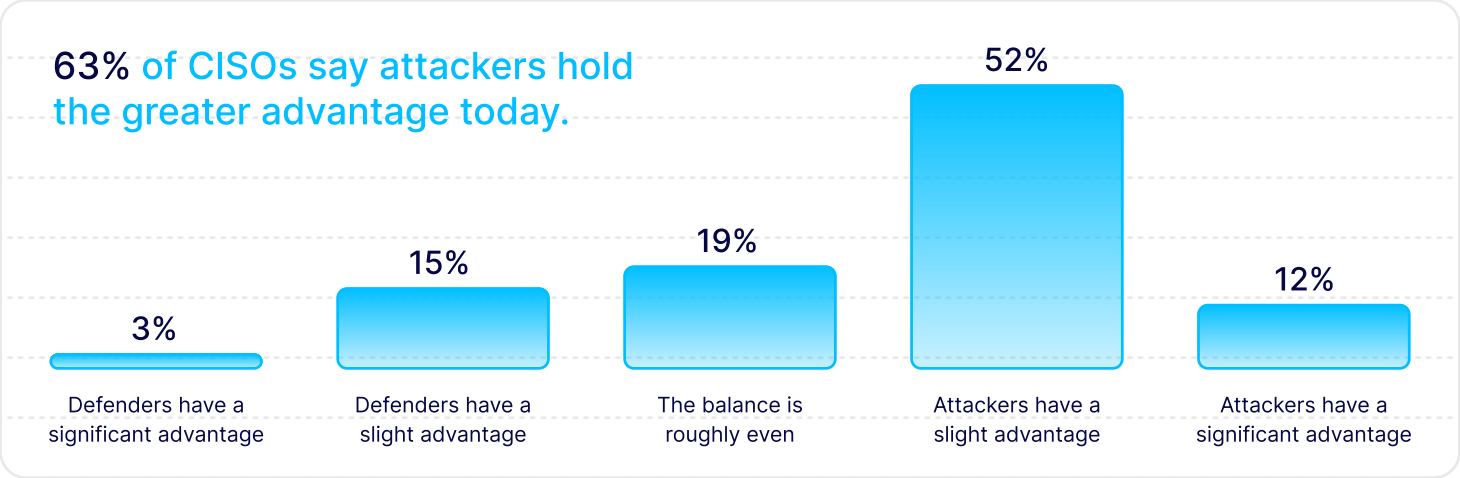


Figure 1: Thinking of the current levels of AI adoption and AI advancements for both hackers and defenders, who has the greater advantage today?

Prepared, but not confident

When it comes to being ready for AI-powered exploitation, confidence is high on the surface but thin underneath. Eighty-nine percent of CISOs say their organization is at least somewhat prepared to defend against AI-accelerated vulnerability exploitation, yet only 28 percent describe that preparation as strong. The distance between broad preparedness and genuine confidence suggests that many leaders recognize the direction of the threat without yet feeling truly equipped to meet it head on. Roughly one in nine acknowledge that their organization is unprepared.

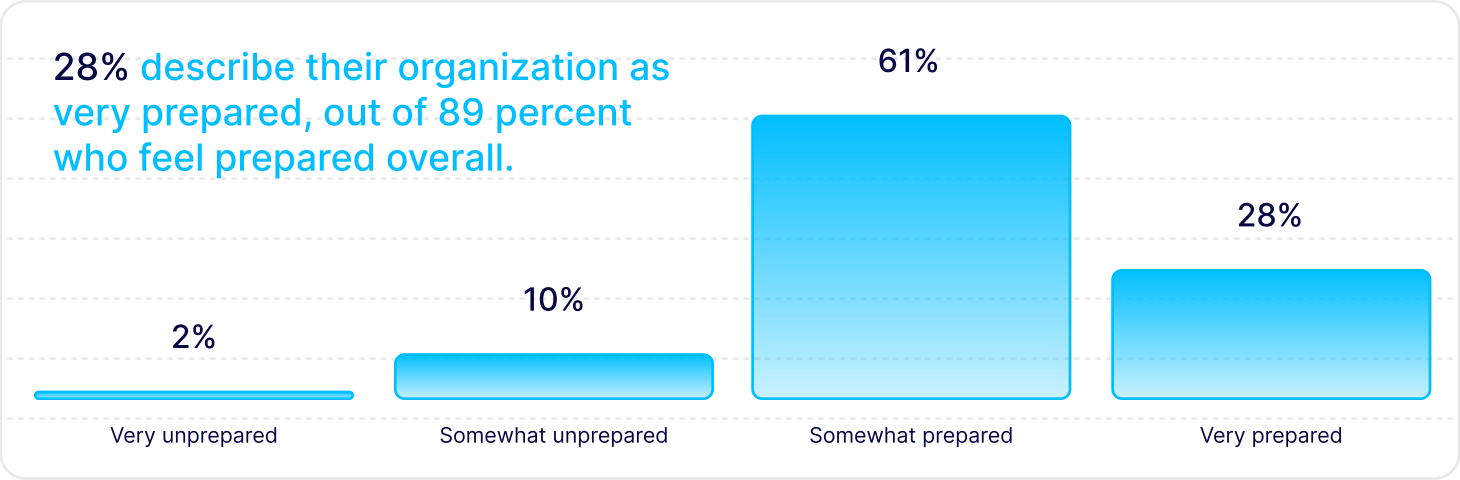


Figure 2: How prepared is your organization to defend against AI-accelerated vulnerability exploitation today?

02 / Defense is still done by hand, and it is taking a toll

The reason confidence runs shallow becomes clear when we peel back the curtains and examine how the work actually gets done. Across the survey, vulnerability and exposure management remains a fundamentally human undertaking, and the consequences appear in the speed of remediation, the size of the backlog, and the wellbeing of the teams responsible for it.

A human-led operating model

Most organizations still run vulnerability and exposure management with people at the center. Sixty-five percent of CISOs say at least half of the work is performed manually, and only 6 percent describe their approach as primarily machine-led. A further 31 percent report a roughly even mix of human and automated effort. Automation is present in most environments, yet it functions as an assistant to human analysts rather than as the primary engine of the work.

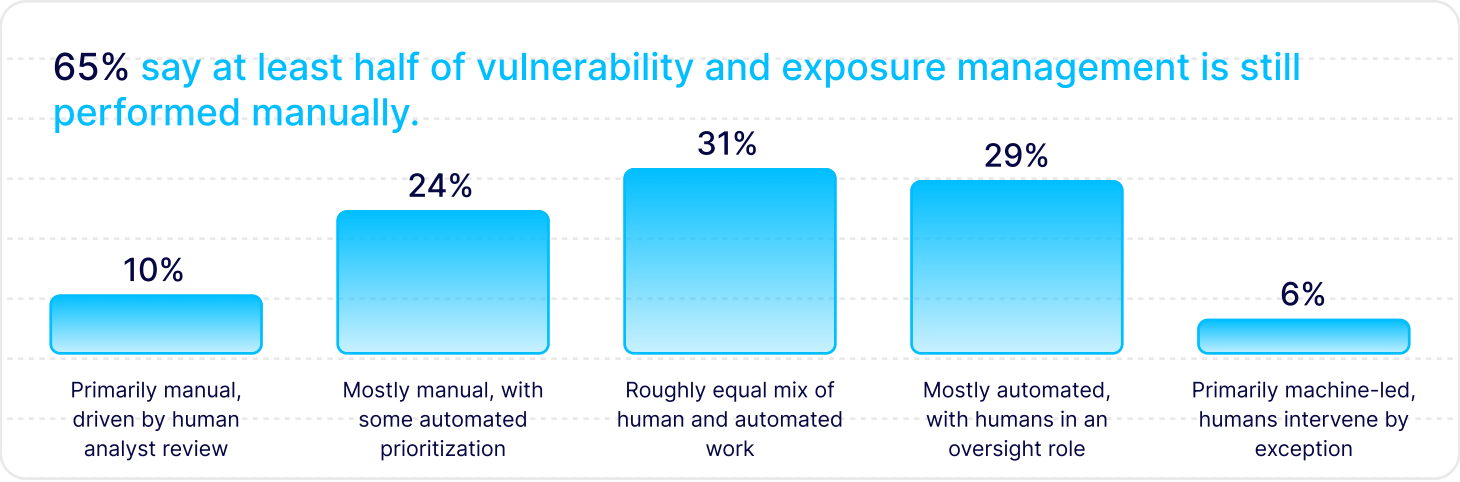


Figure 3: How would you describe your organization's current approach to vulnerability and exposure management?

Remediation measured in days, not hours

The manual model shows its cost most directly in remediation time. For 60 percent of organizations, closing a critical vulnerability after it has been identified takes more than seven days, with 44 percent landing in the eight-to-fifteen-day range. Only 16 percent resolve a critical issue within three days. In an environment where the interval between disclosure and exploitation is compressing, a remediation cycle measured in weeks leaves a meaningful window of exposure open.

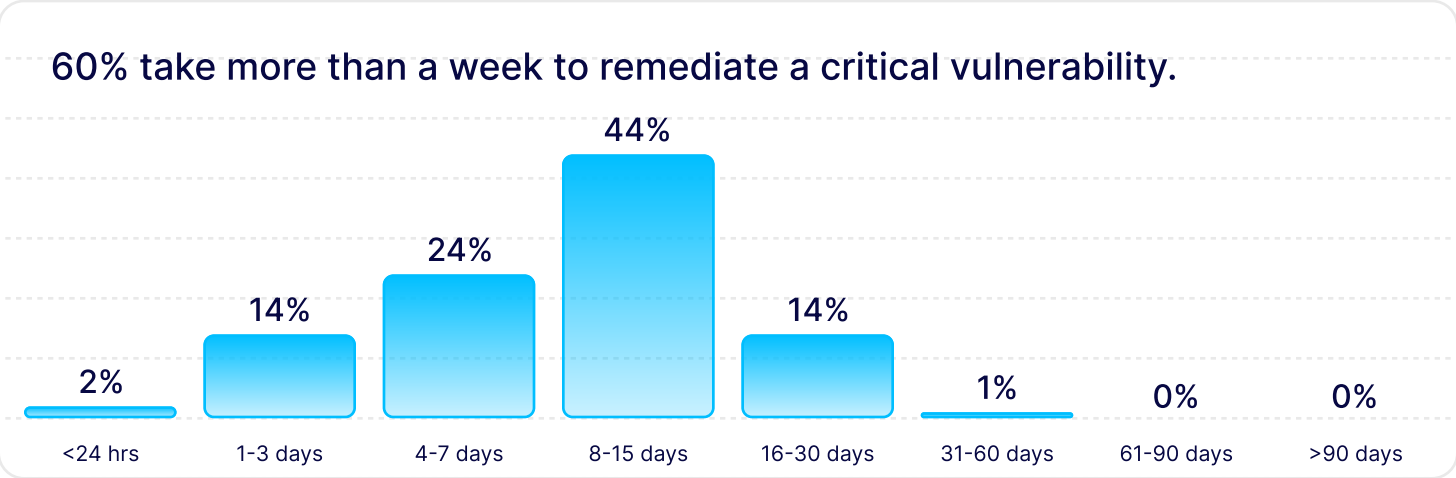


Figure 4: On average, how long does it take your organization to remediate a critical vulnerability after it is identified?

A backlog that compounds

Slow remediation accumulates into a persistent backlog. Nearly half of CISOs, at 48 percent, estimate that a quarter or more of known vulnerabilities in their environment go unremediated for longer than 30 days, and 17 percent put that figure at half or more. This standing population of known, unaddressed weaknesses is exactly what adversaries now find and exploit faster than defenders can close.

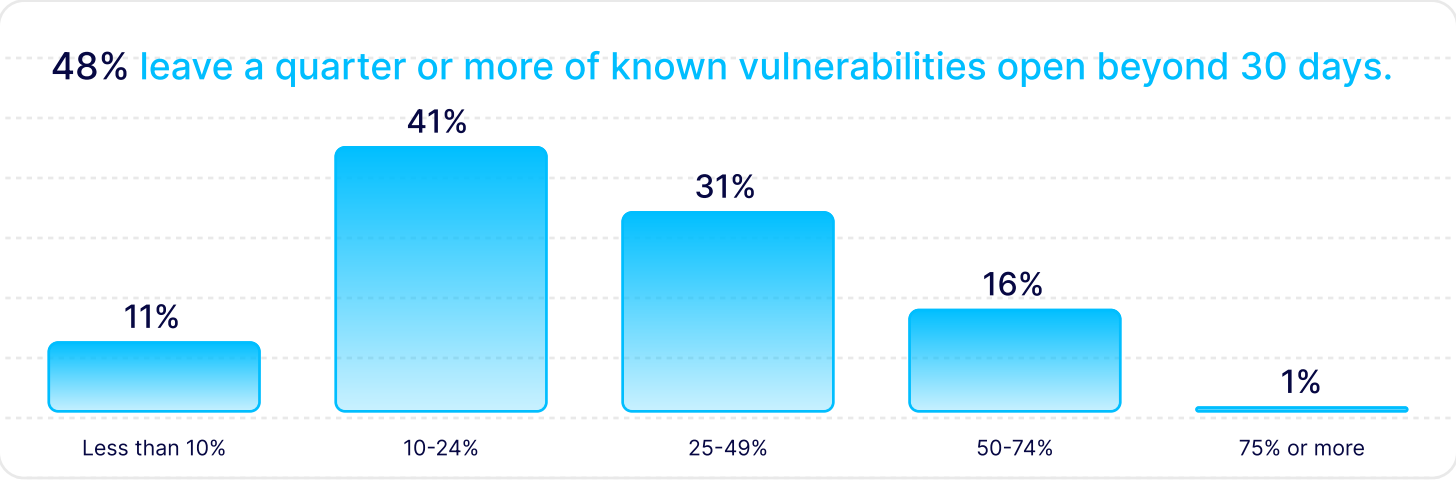


Figure 5: To your knowledge, what percentage of known vulnerabilities in your environment go unremediated for more than 30 days?

Burnout as a security risk

This labor-intensive model comes with a substantial human cost. More than three-quarters of CISOs, 78 percent, say vulnerability and exposure management contributes at least moderately to burnout on their security teams, and 17 percent call it a major contributor. Burnout registers as more than a workforce concern. When the people responsible for triage and remediation are stretched thin, the quality and consistency of defensive work degrade, which makes fatigue a security exposure in its own right.

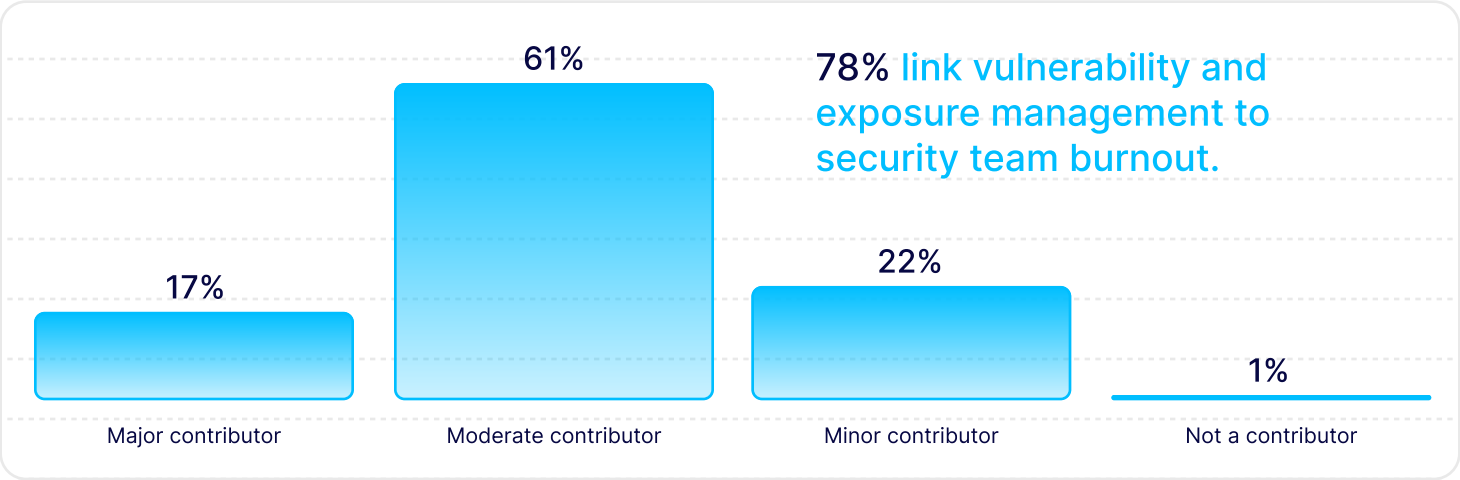


Figure 6: To what extent is vulnerability and exposure management contributing to security team burnout in your organization?

03 / Automation is moving toward action

Automation in vulnerability management is expanding across the full workflow, and forward-looking organizations are authorizing machines to act, not just observe and analyze. While automation has historically clustered in the earlier, lower-risk stages, a meaningful share of organizations are now giving machines authority at the point where risk actually gets closed.

The shift from automated analysis to automated action is underway

The data reflects a clear progression toward autonomous action. Fifty-five percent of organizations already allow automated asset discovery and inventory, and 49 percent allow automated vulnerability prioritization. But the more significant signal is at the end of the workflow: 32 percent of organizations are already permitting automated remediation actions, a meaningful indication that CISOs are becoming comfortable letting machines change the environment when the context is right. With 44 percent allowing automated escalation and 40 percent allowing remediation validation, the infrastructure for fully autonomous remediation is already in place for a significant portion of enterprises.

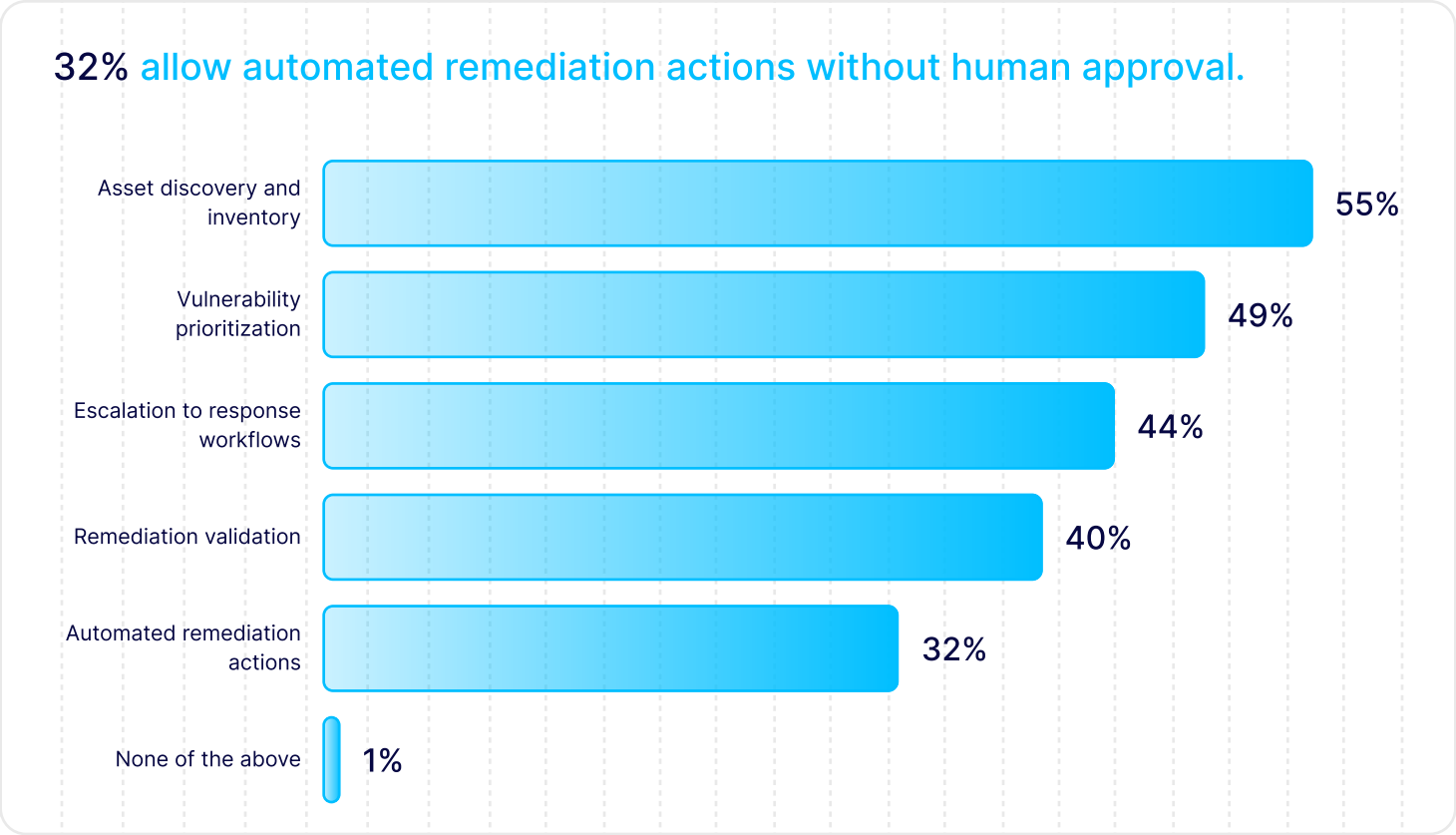


Figure 7: Which of the following activities can technology systems perform in your organization today without requiring human approval?

Execution remains mostly manual

The same reservation appears in how remediation itself is carried out. For 57 percent of organizations, less than half of remediation workflows are partially or fully machine-led, and only 7 percent report that machines lead three-quarters or more of the work. Automation has moved into the assessment and prioritization phases, yet the act of remediating, the point at which a decision becomes a change in production systems, remains mostly a human responsibility.

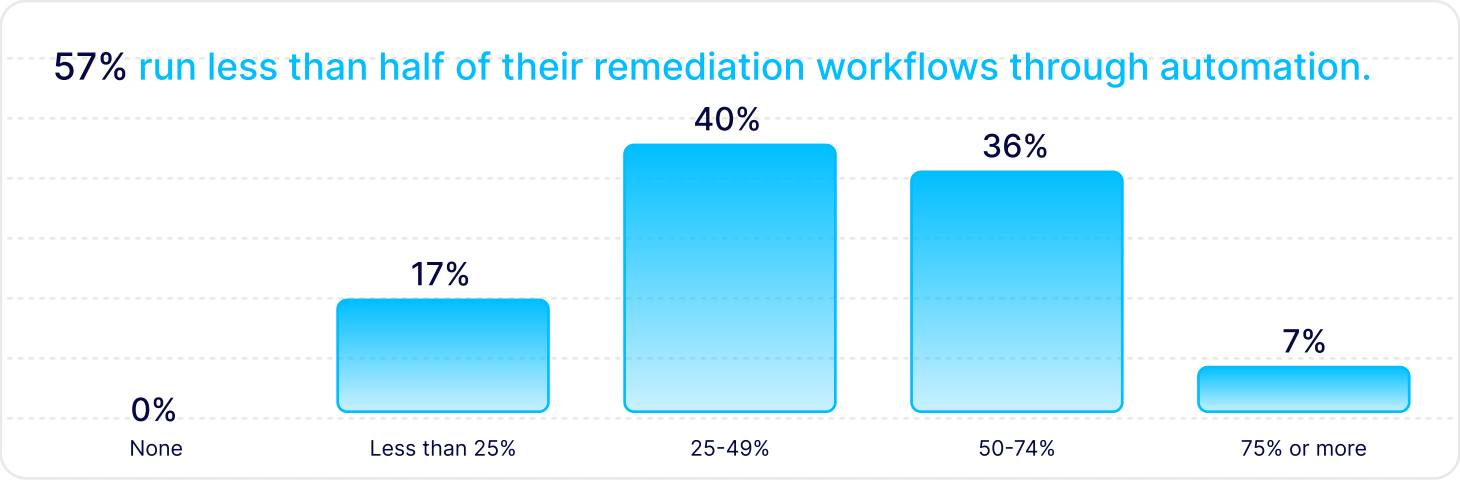


Figure 8: Approximately what percentage of your vulnerability remediation workflows are partially or fully machine-led?

04 / The trust and governance gap

If automation delivers speed, and speed is what defenders need most, the natural question is: what holds back broader adoption? For the security leaders surveyed, the biggest barriers are confidence and control, not cost.

Trust, not budget, is the constraint

Asked to name the biggest obstacles to greater automation, CISOs point first to confidence in the technology itself. Fifty-two percent cite a lack of trust in automated decisions, followed by governance or compliance concerns at 43 percent, and skills gaps and integration complexity, each at 38 percent. Budget constraints rank far lower at 21 percent. The message is that most organizations are not waiting for funding. They are waiting for reasons to believe that automated action will be correct, accountable, and defensible.

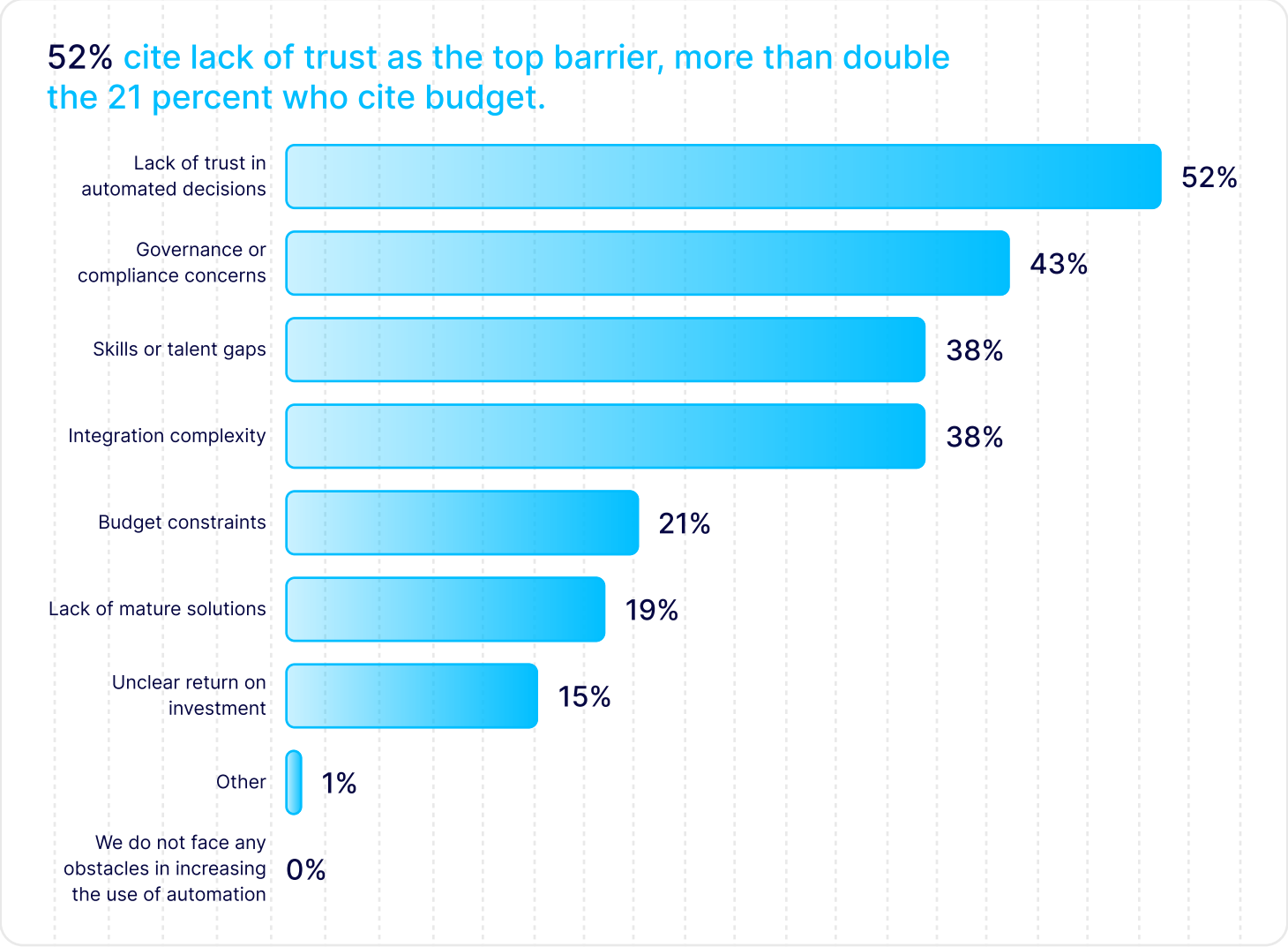


Figure 9: What are the biggest obstacles preventing your organization from increasing the use of automation in vulnerability and exposure management?

Governance is catching up

Governance frameworks are in motion but not yet built for autonomous vulnerability management and remediation. Eighty-one percent of CISOs describe their governance approach as human-led and being adapted for greater machine-led operations, and taken with the 10 percent whose frameworks are already designed for it, more than nine in ten are moving in the same direction, even if most organizations remain early in the journey. Only a small minority have governance purpose-built for machine-led action today.

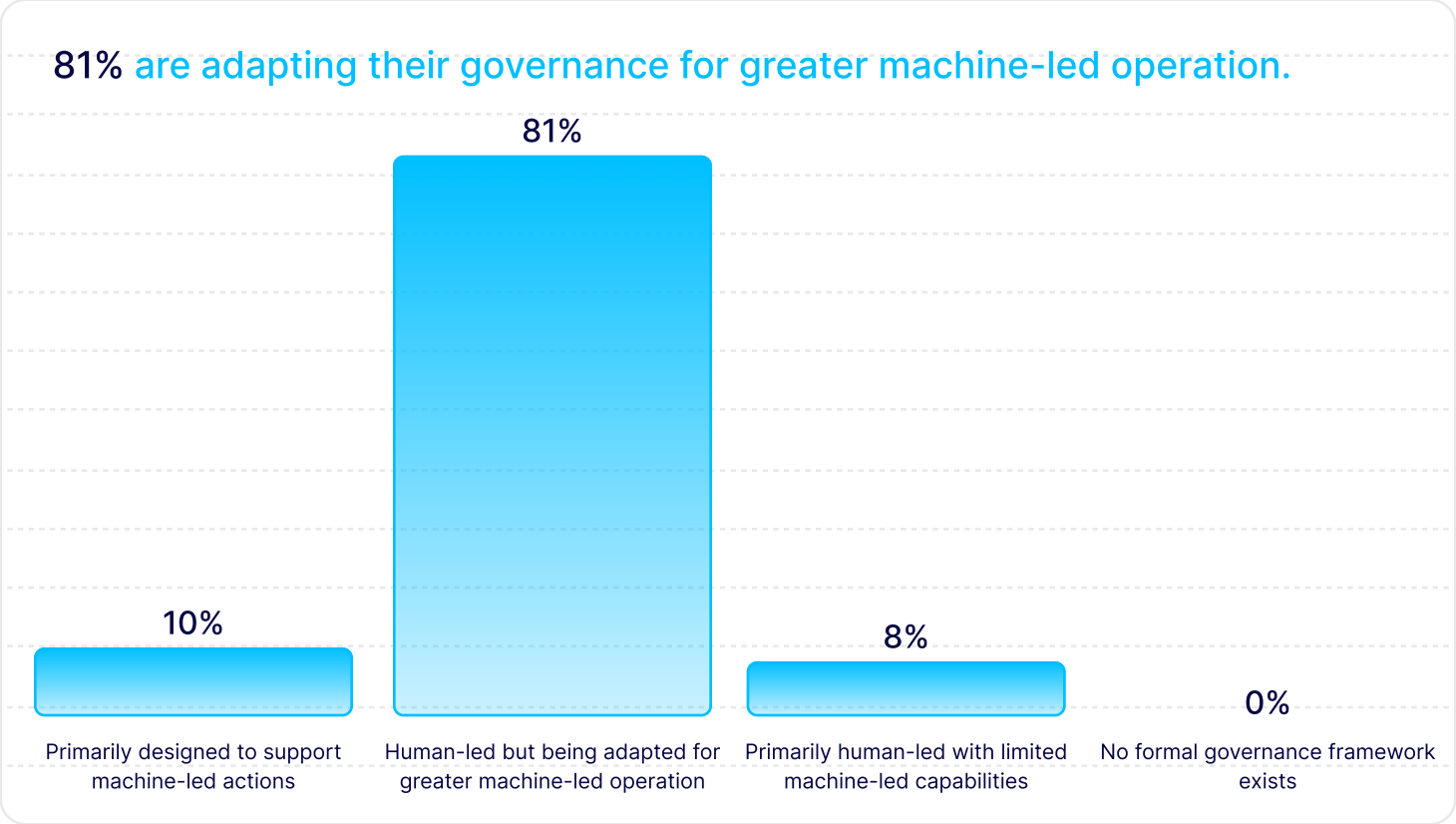


Figure 10: Which statement best describes your organization's governance approach to machine-led security actions?

What would build confidence

Leaders have a clear wish list that would help make them comfortable delegating more of their remediation responsibilities to machines. Fifty-two percent point to auditability and explainability, the ability to see and understand why a system acted, and 51 percent to vendor accountability and liability protections. Regulatory clarity follows at 46 percent. Transparency and shared responsibility are key requirements; CISOs are prepared to grant automated systems more authority once they can verify the reasoning behind an action and are not left to bear the risk of that authority alone.

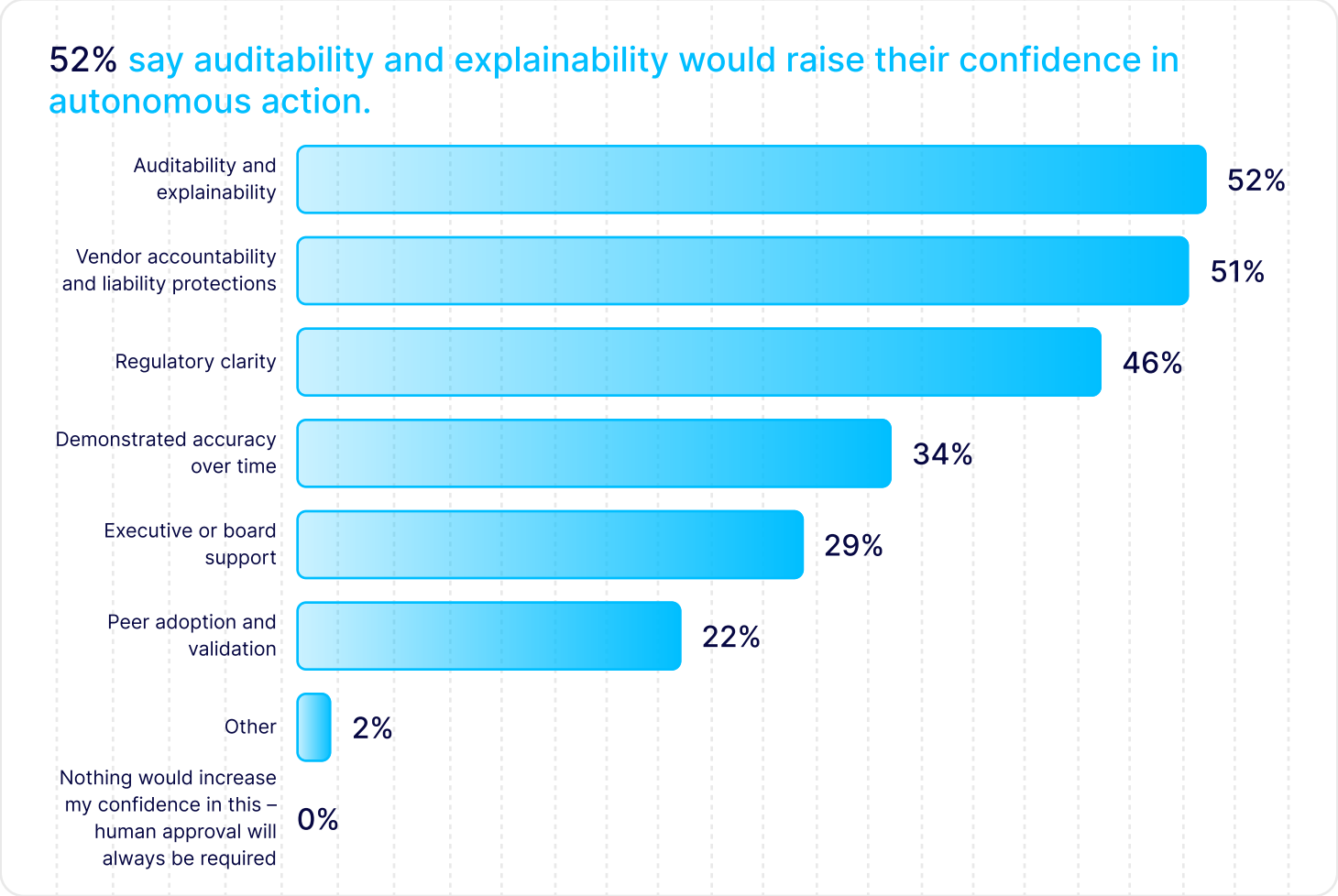


Figure 11: What would increase your confidence in allowing machine-led systems to execute remediation actions without human approval?

05 / Advanced organizations are embracing machine-led security

For all the caution, security leaders are not content to stand still and let their adversaries win the automation arms race. They expect the balance of their operations to tip toward machines, and they are already planning how to pay for the transition.

Which categories fade first

Asked which parts of their stack will lose effectiveness in a machine-speed environment over the next three years, CISOs point first to human-driven ticketing and remediation workflows at 51 percent, followed by signature-based detection at 39 percent, traditional vulnerability management platforms at 38 percent, and manual patch management at 37 percent. What these categories share is a dependency on people, whether to write the rules, triage the findings, or apply the fixes. In each case, that dependency sets the pace, and CISOs expect automated threats to move faster than human-driven workflows allow.

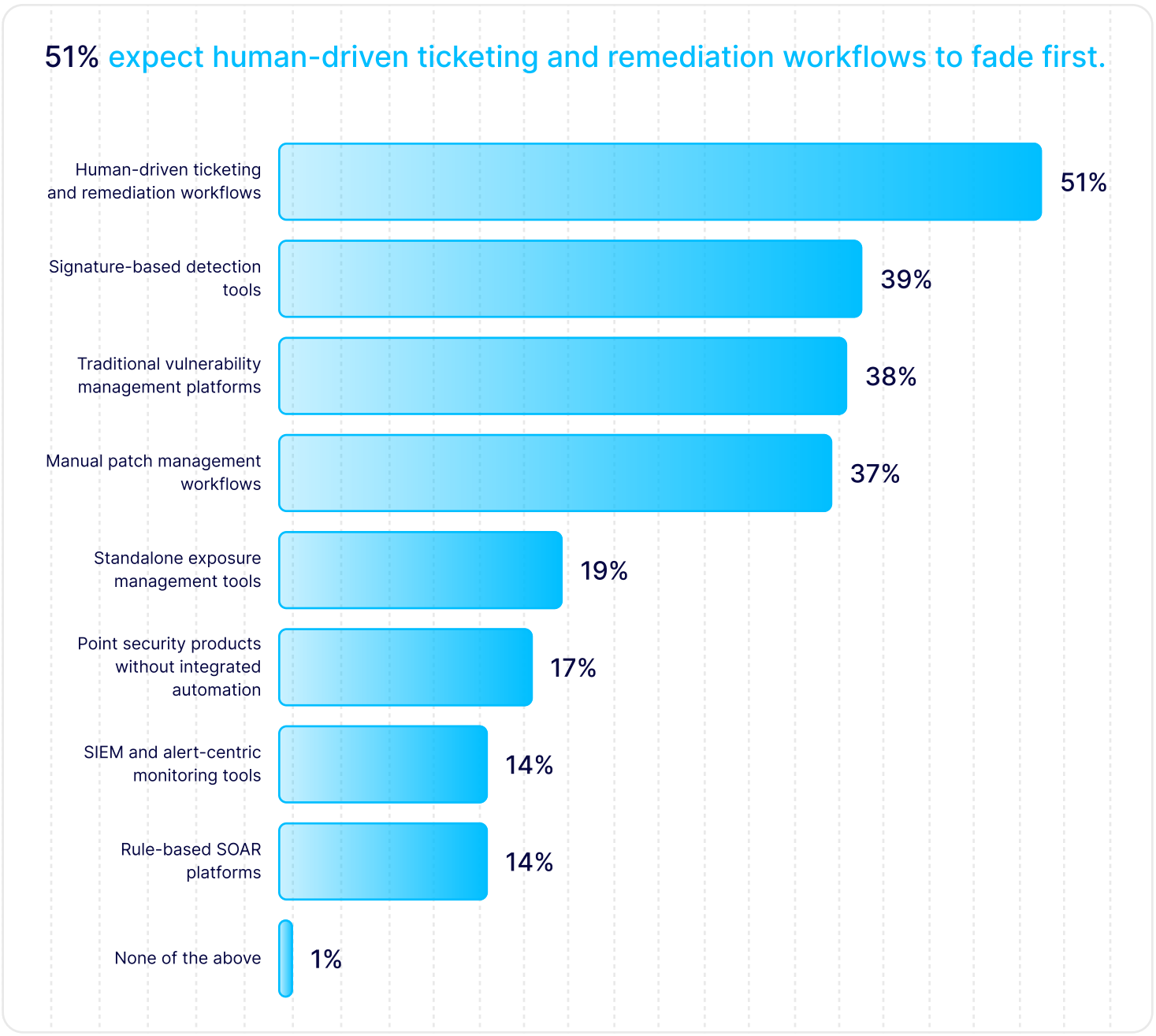


Figure 12: Which of these cybersecurity categories are most likely to become less effective in a machine-speed threat environment over the next three years?

The next 12 to 18 months

Looking ahead, leaders expect a decisive move toward machine-led operations. Forty-five percent anticipate that vulnerability and exposure management will be mostly or primarily machine-led within the next 12 to 18 months, including 12 percent who expect autonomous operations to become their primary model in that timeframe. That figure represents a notable rise from the 35 percent who describe their current approach in those terms, while only 23 percent expect to remain mostly or primarily manual.

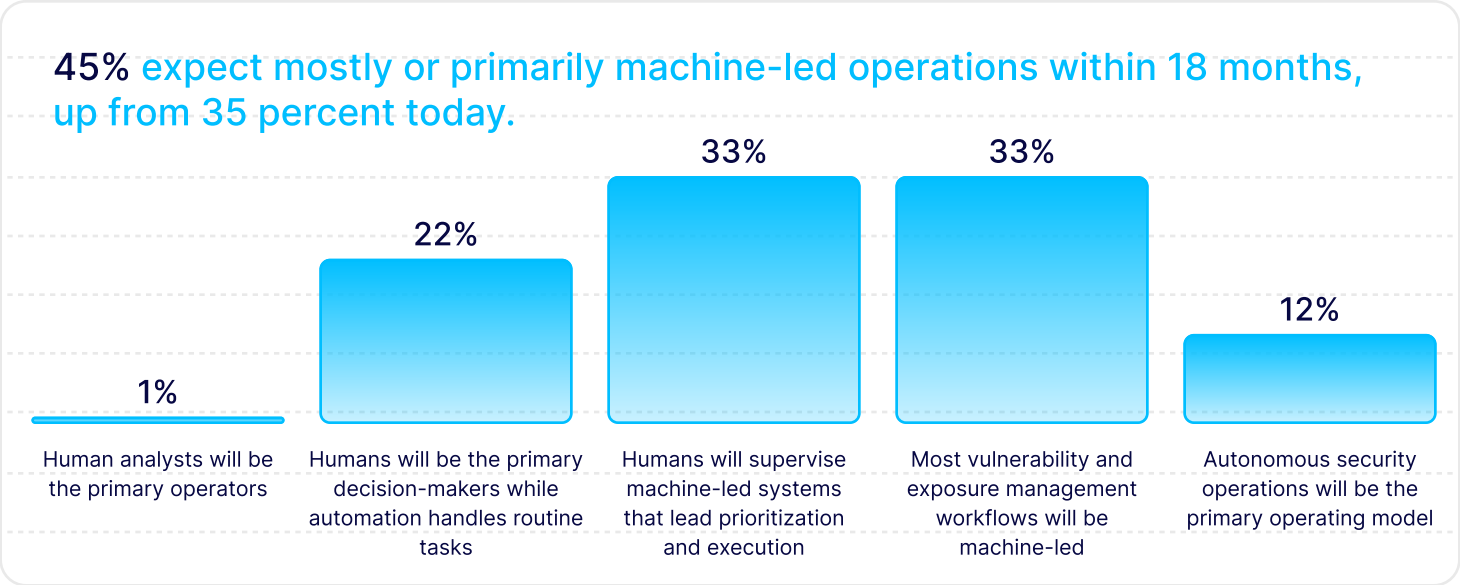


Figure 13: Which statement best reflects your organization's expected approach to vulnerability and exposure management within the next 12 to 18 months?

How the transition gets funded

The way organizations plan to pay for this shift shows how they view it within the context of their broader security program. Rather than treating automation as a separate experiment, most fold it into existing budgets. Forty-eight percent expect to fund future investment through broader IT or digital transformation budgets, and 31 percent plan to reallocate from existing security spending. Only 21 percent maintain a dedicated AI or security innovation budget. Automation is increasingly regarded as a core part of how security operates, financed like infrastructure rather than as an experimental pilot.

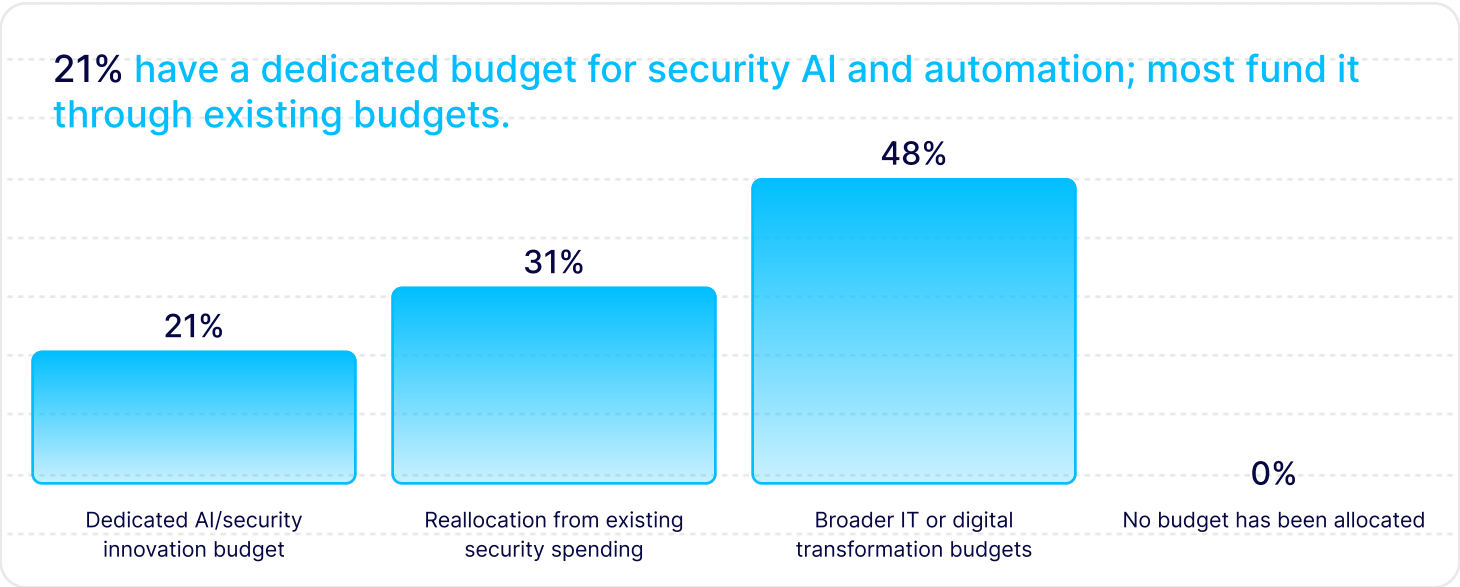


Figure 14: Which best captures how your organization expects to fund future investments in security automation and AI-enabled security capabilities?

Conclusion

The survey reveals an industry that understands its predicament clearly and is moving, deliberately and unevenly, to address it. Security leaders recognize that attackers have gained an edge, that their own operations remain too manual to match machine-speed threats.

What separates intent from progress is confidence. The obstacles that matter most are trust, governance, explainability, and accountability. As confidence develops, the survey suggests the operating model will follow, with machine-led operations moving from the exception to the norm within a remarkably short horizon.

The next phase of enterprise defense will be defined less by whether organizations adopt automation and more by how quickly they can build the trust to let it act. The organizations that meet those conditions first will be the ones that close the gap between the speed of the threat and the speed of the response.

Methodology

The 2026 State of Autonomous Defense Report is based on a survey commissioned by Kai and conducted by Wakefield Research among 500 chief information security officers at private-sector companies with a minimum annual revenue of 500 million dollars. The research was fielded between June 15 and June 29, 2026, using email invitations and an online survey.

About Kai

Kai is the AI company rebuilding cybersecurity for the machine-speed era. Trusted by Fortune 500 and Global 2000 enterprises, the Kai Autonomous Defense Platform replaces fragmented tools and human-limited workflows with agentic AI that works continuously across cyber asset management, application security, infrastructure vulnerability management, and detection engineering. It contextualizes, reasons, and acts at machine speed and enterprise scale. What takes human-led teams weeks, Kai executes in hours, driving risk toward zero through autonomous remediation. Human defenders don't just keep up. They become superhuman. Learn more at https://www.kai.security