Gurucul

2026

Insider Risk Report

The Year AI Became an Insider

Research by

Cybersecurity INSIDERS

Executive Overview

A year ago, 17% of organizations reported zero insider incidents. Today, that number has fallen to just 10%. At the same time, the share of enterprises experiencing more than 20 insider incidents annually has doubled. Insider risk is no longer an occasional investigation; it has become a sustained operational burden that most organizations are not structurally equipped to address.

Investment and awareness both increased, but neither has kept pace with how fundamentally the operating environment has changed—or with the sheer volume of insider activity organizations now face. Access expanded faster than governance could follow. Data spread into cloud apps and collaboration platforms. AI assistants began operating inside email, calendar systems, and internal documents, often without security visibility into what they touched or what they did with what they found.

The underlying failure is architectural. Trust and access models that worked in smaller, more contained environments were never designed to scale under current conditions. AI exposed that fragility and compressed the margin for error faster than legacy controls can adapt. What followed is a steady expansion of ways for mistakes, misuse, and inherited access to become breaches.

To understand how organizations are navigating this shift, we surveyed 725 IT and cybersecurity professionals. The findings reveal a clear inflection point: insider risk programs are being forced to evolve from identifying rare bad actors to managing continuous risk across people, data, identities, and increasingly, machines.

Three converging forces define this tipping point:

- **The threat shifted from malice to mistakes:** Nearly three-quarters of organizations (74%) now rank negligent insiders as their top concern, well ahead of malicious actors (59%). Most incidents today aren't driven by intent but by systems that let small errors cascade.
- **AI is operating inside trust boundaries:** Nearly all organizations (94%) report that AI is increasing their insider risk exposure - with 74% describing that increase as moderate or significant. At the same time, more than half are deploying AI-powered detection tools. AI is expanding the attack surface while simultaneously becoming the only viable way to defend it at scale.
- **More tools haven't produced more clarity:** A third of organizations run five or more insider risk tools, yet two-thirds still cite detection accuracy as their top challenge. Tool accumulation has reached diminishing returns. Integration and consolidation are now prerequisites for progress.

The data also reveals what separates organizations that contain risk from those that absorb it. The difference isn't budget or headcount: it's how fast they move from detection to action.

Organizations succeeding at insider risk management share three traits: unified visibility across identity and behavior, governance of AI as an insider, and automation that closes the gap between finding threats and stopping them.

The pages that follow examine why this shift occurred and what it takes to get ahead of it.

Insider Incidents: No Longer Edge Cases

For years, insider incidents were easy to dismiss as rare events. That era is ending.

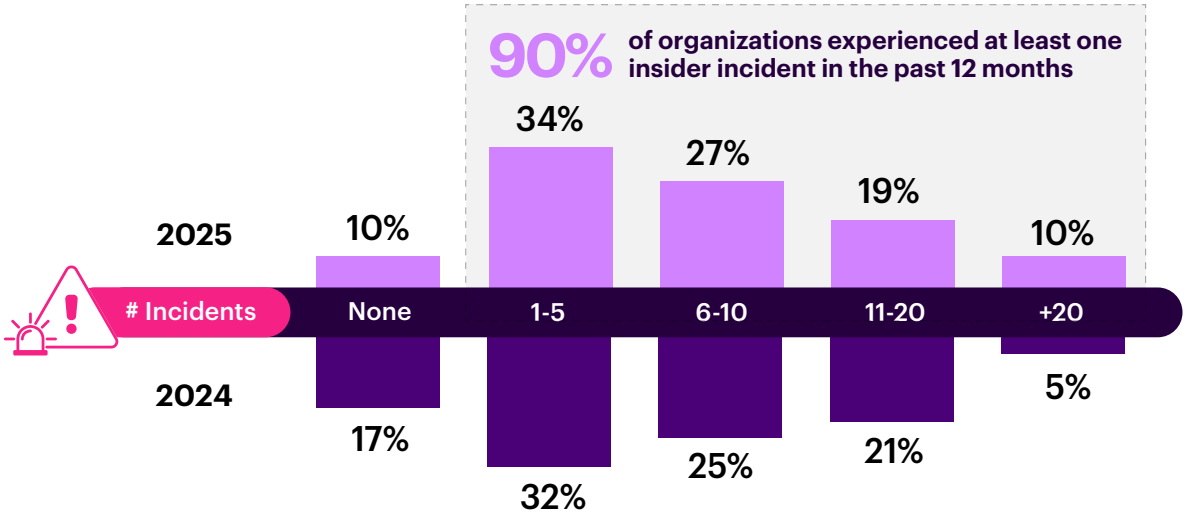
The survey data shows that insider incidents are now routine. Only 10% of organizations report zero insider incidents in the past 12 months, down from 17% in 2024. Put differently, 90% experienced at least one insider incident in the past 12 months.

The frequency distribution tells a more consequential story. More than half of organizations (56%) now report six or more insider incidents annually. The high-volume tail continues to expand. Organizations experiencing more than 20 incidents in a single year now represent 10% of respondents, double the share reported in the prior study. Importantly, this trend cannot be attributed to visibility improvements alone. When asked how insider incidents have changed over the past 12 months, a majority of respondents (55%) report that incidents are becoming more frequent, while only 13% report a decline.

The underlying drivers are structural. Data is more widely distributed across cloud platforms and collaboration tools, access privileges accumulate faster than they are reviewed, and AI-enabled workflows extend insider-like access beyond traditional users. The result is an environment where insider incidents occur more often, with smaller individual actions triggering larger downstream impact.

Insider Incidents on the Rise

How many insider incidents did your organization experience in the last 12 months?



Attack Trend Over Last 12 Months

Has the occurrence of insider attacks changed over the last 12 months?

Insider risk has crossed a threshold. The relevant question is no longer whether an organization will experience an insider incident, but how many it will face in a given quarter (and whether its security architecture is designed to contain that volume without breaking down).

The Vulnerability Shift

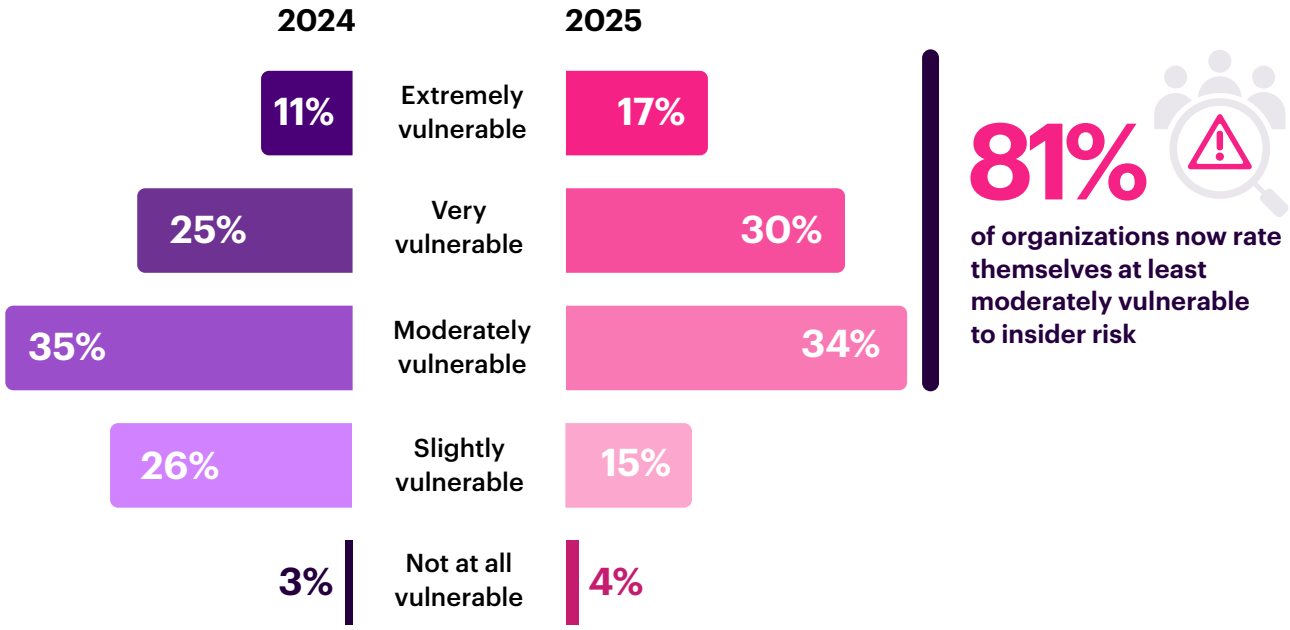
Organizations don't just experience more incidents. They recognize they are less in control than they believed.

Security leaders are reassessing their exposure. The share of organizations describing themselves as only slightly vulnerable to insider threats fell sharply from 26% in 2024 to just 15% in 2025. Nearly half of organizations (47%) now rate themselves as very or extremely vulnerable, up from 36% the prior year.

The movement at the extremes is noteworthy. Organizations identifying as "extremely vulnerable" grew from 11% to 17% in a single year, while the "moderately vulnerable" group in the middle remained largely unchanged. This indicates a reassessment by organizations that previously believed their controls were sufficient and now recognize they are not.

Vulnerability Perception Is Up

How vulnerable do you think your organization is to insider threats?



This confidence decline aligns with operational reality. As insider incidents become routine and detection grows more difficult, confidence rooted in legacy assumptions erodes. Security teams are confronting the limits of architectures that were never designed for sustained insider risk.

The Price of Insider Risk

Insider incidents are no longer security hygiene issues - they are material financial events.

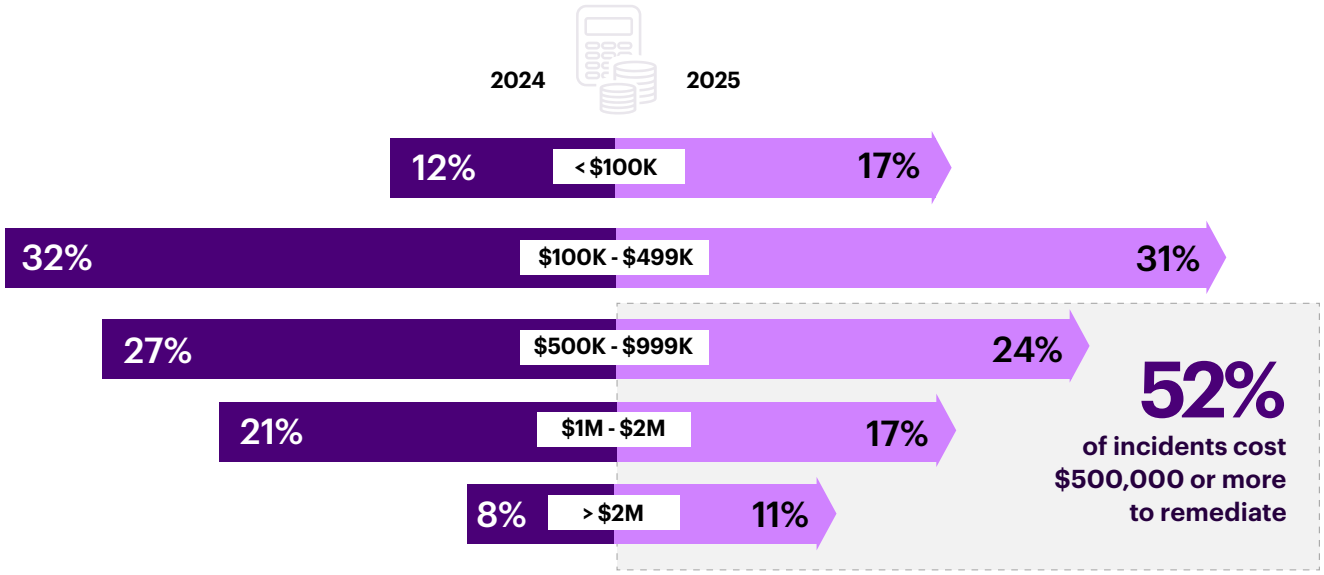
The data confirms that remediation costs are now routinely significant. More than half of insider incidents cost $500,000 or more to contain, and over a quarter exceed $1 million. And the high-end tail continues to grow, with incidents exceeding $2 million becoming more common (11%).

These figures represent a per-incident impact. When 90% of organizations experience at least one attack annually (and 56% experience six or more) the numbers add up quickly. An organization experiencing ten incidents at $500K each faces a $5 million annual exposure, before accounting for reputational damage, regulatory consequences, or lost productivity.

The distribution itself is instructive. Relatively fewer incidents now fall in the mid-range ($100K–$999K), while both low-cost containment and high-impact failures are increasing in share. This suggests a widening gap between organizations that catch incidents early and those that do not.

Remediation Costs Add Up

What is your estimated average cost of remediation after an insider attack?



Insider risk management is no longer discretionary; it's loss prevention. Organizations that fail to adapt their detection and containment capabilities are not accepting risk in theory, they are absorbing it in measurable dollars.

Progress Reversed

For a brief moment, insider threat detection appeared to be improving. That progress has reversed.

In 2024, only 37% of organizations reported that detecting insider incidents was more difficult than detecting external threats, down meaningfully from the prior year. In 2025, that figure jumps to 53%, erasing the gains security teams believed they had made and pushing detection difficulty beyond previous levels.

This regression is material. More organizations now say insider threats are harder to detect than external attacks, while fewer believe detection parity is achievable. The trend signals that legacy detection approaches are struggling to keep up with how insider risk now manifests.

What changed is not attacker sophistication alone, but the environment defenders must observe. Insider activity increasingly blends into normal behavior across cloud platforms, collaboration tools, and automated workflows. Threat signals still exist, but they are noisier, more distributed, and harder to correlate in time.

Detection Difficulty vs. External Attacks

How difficult is it to detect and prevent insider attacks compared to external cyber attacks?

53%

say insider attacks are now harder to detect than external threats

Detection models that briefly kept pace are now falling behind again. Not because teams reduced effort, but because the attack surface is expanding faster than the architectures designed to monitor it.

The Fragmentation Tax

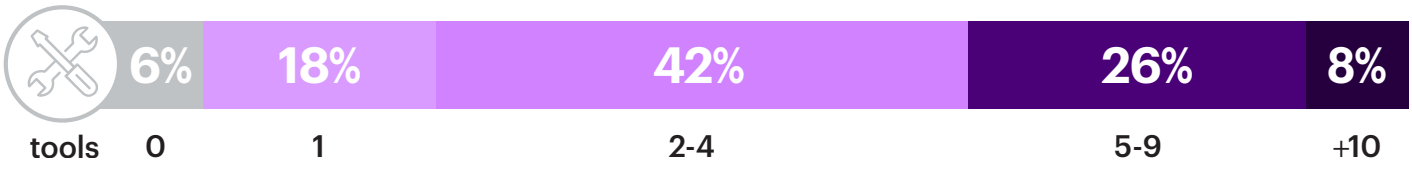
The biggest obstacle to insider risk management is disconnected capabilities.

Fifty-eight percent of organizations cite tool and data fragmentation as a primary challenge. Most enterprises now deploy multiple tools to manage insider risk: 42% use two to four solutions, while 34% operate five or more. Each addition was justified individually. Collectively, they've produced silos that actively undermine the detection and response outcomes they were purchased to improve.

The result: 66% of organizations still struggle to accurately detect insider threats despite running multiple dedicated tools. Fragmented tooling produces fragmented signals, forcing analysts to piece together context across disconnected systems while incidents continue to unfold. This fragmentation also imposes operational cost. Alerts multiply without prioritization, investigations slow as data is reconciled manually across fragmented tools, and response suffers as teams struggle to establish confidence in what they are seeing.

Number of Insider Risk Tools in Use

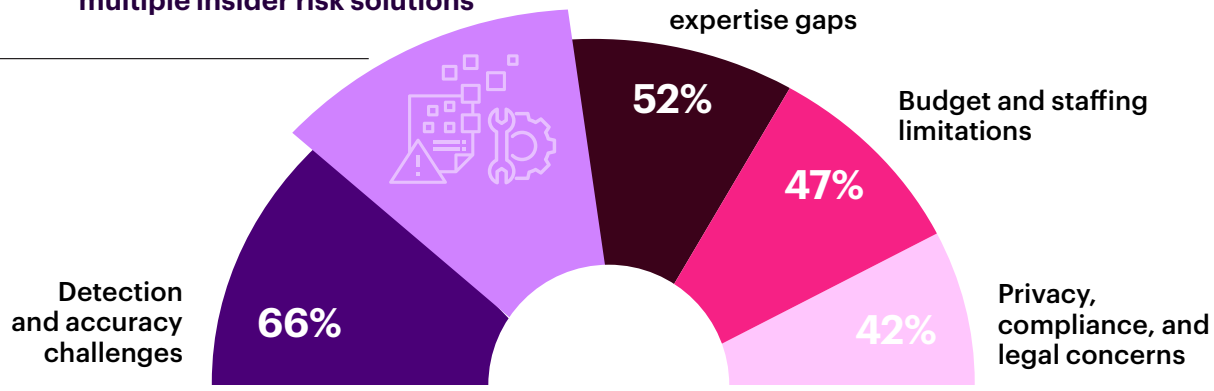
How many distinct security tools does your organization currently use for insider risk management?



Top Challenges in Insider Risk Management

What are the primary challenges preventing your organization from implementing effective insider risk management strategies?

58% **cite tool and data fragmentation as a primary obstacle, even as most organizations deploy multiple insider risk solutions**



In short: Insider risk programs are not failing from lack of investment, but because siloed investment and lack of integration are actively undermining detection, investigation, and response.

The Expanding Insider Universe

The definition of "insider" has outgrown the org chart.

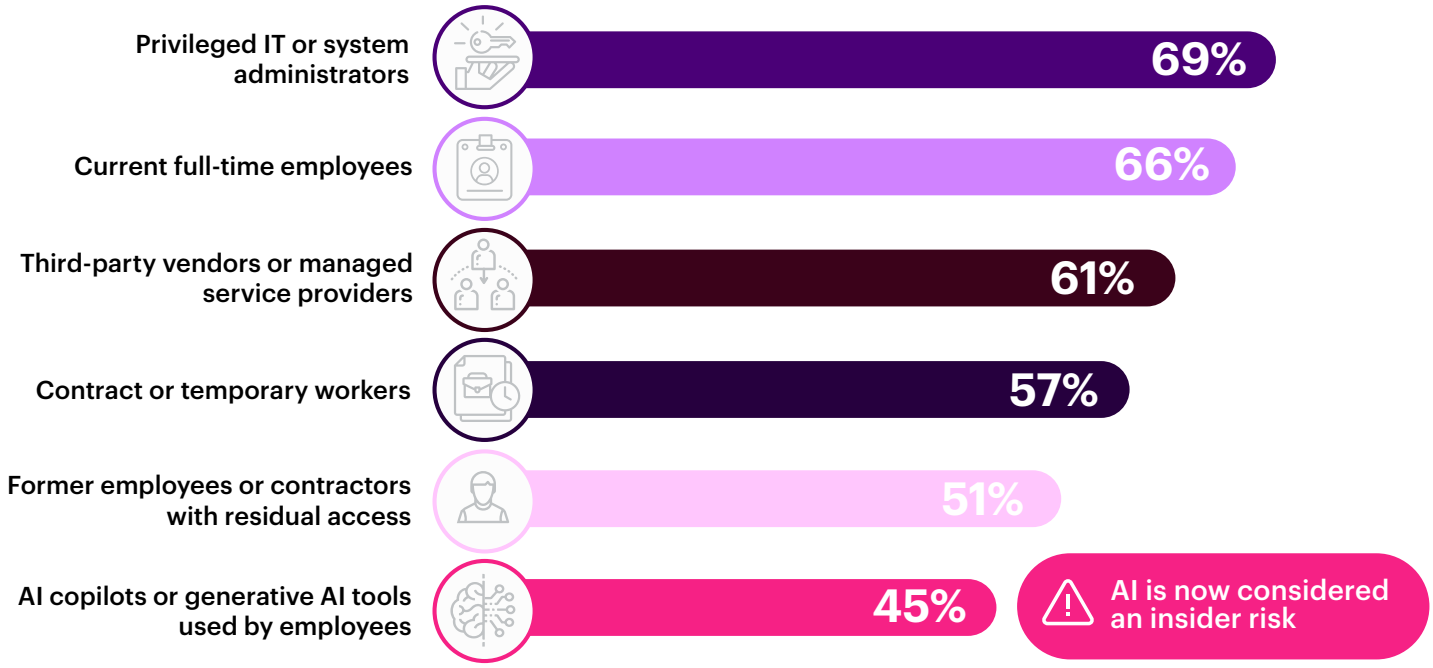
When asked which types of insiders concern them most, organizations point first to the usual suspects: privileged IT administrators (69%) and current full-time employees (66%). But the list doesn't stop there. Third-party vendors (61%), contractors (57%), and former employees with residual access (51%) all rank as majority concerns.

The more striking finding is what's new on the list. Nearly half of organizations (45%) now consider AI copilots and generative AI tools as an insider risk category – reflecting the reality that these tools operate with employee credentials, access sensitive data, and act on behalf of users. Another 24% flag autonomous AI agents or machine identities as a concern, despite their relatively early stage of adoption.

This expansion signals a fundamental shift. Insider risk is no longer confined to employees with intent, but to anyone or anything with access. Vendors, contractors, former staff, and non-human actors now participate in the same trust fabric, often without equivalent visibility or governance.

Types of Insiders that Concern the Most

Which types of insiders are you most concerned about?



Supply chain or integration partners with data/system access 37% | Outsourced or offshore operations teams 32% | Autonomous AI agents or machine identities 24% | Executive leadership or board members 20%

Insider risk models built for a human-centric environment no longer fit. As the insider universe expands, so does the need for consistent controls, behavioral context, and governance across human and non-human identities alike.

Negligent Insiders - The New #1

The dominant insider risk today is not malicious intent. It is human error—now amplified by AI.

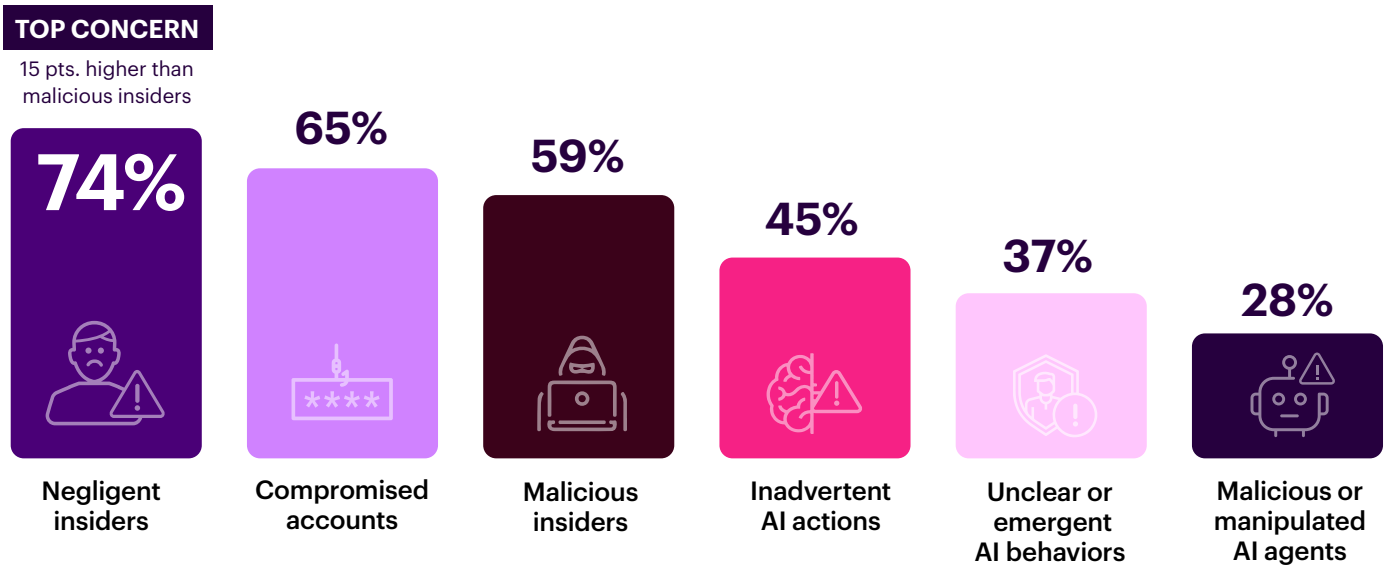
When asked which insider risk categories concern them most, 74% of organizations cite negligent insiders—well ahead of compromised accounts (65%) and malicious insiders (59%). In a pre-AI environment, a negligent action typically affected a single system or dataset. Today, when an employee pastes sensitive data into an AI assistant or grants a copilot access to their inbox, that single action can propagate across interconnected systems faster than traditional controls can respond.

AI intensifies this dynamic. Forty-five percent of organizations are concerned about inadvertent AI actions, and 37% cite unclear or emergent AI-driven behaviors—cases where AI tools take actions users didn't anticipate or explicitly authorize. As AI tools inherit user privileges and operate within workflows, the boundary between human error and machine-driven risk continues to blur.

The implications are strategic, not just operational. For years, insider threat programs focused primarily on detecting bad actors: employees stealing data, sabotaging systems, or selling access. That threat remains real, but it's no longer the dominant concern. The employee who misconfigures a cloud bucket, emails sensitive files to the wrong recipient, or shares proprietary data with an AI assistant now represents the more common and often more costly risk.

Insider Risk Categories of Greatest Concern

Which categories of insider risk are you most concerned about?



Defending against negligence requires a different posture than defending against malice. Intent-based detection misses most of these incidents. What's needed is unified visibility across identity, access, and behavior - so security teams can see risky actions in context before damage spreads, regardless of whether the action was deliberate.

What's Actually Driving Insider Risk?

The drivers behind insider incidents have shifted from infrastructure complexity to systemic exposure.

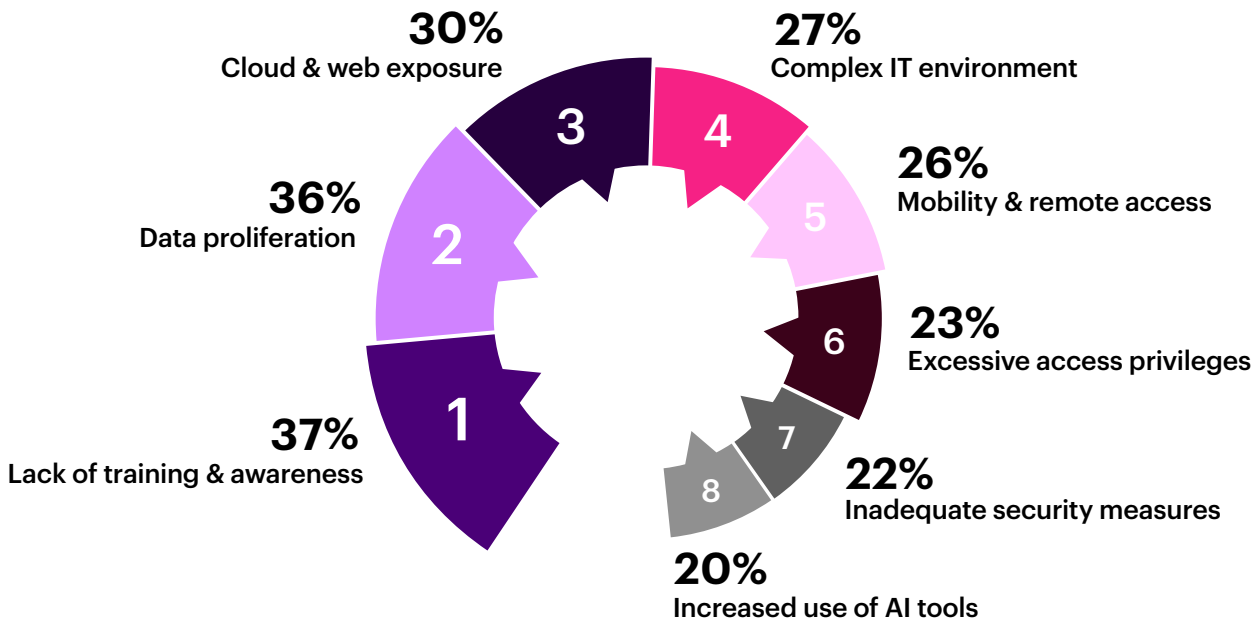
In 2024, complex IT environments ranked as the top contributor to insider risk at 39%. In 2026, that concern dropped to 27%, replaced by a new cluster of drivers led by lack of training and awareness (37%), data proliferation (36%), and cloud and web exposure (30%). The center of gravity has moved away from managing systems toward governing data and access at scale. This shift indicates that the insider risk problem emerged from architectural exposure, even before AI became a meaningful factor.

The shift reflects another deeper reality. Infrastructure complexity is now table stakes as organizations have accepted it as a permanent condition. The harder problem is that data spreads faster than governance frameworks can adapt. Access privileges accumulate without consistent review, and collaboration tools expand exposure beyond traditional boundaries. Controls designed for a smaller, more static environment are struggling to keep pace.

AI has entered this equation as a new accelerant. One in five organizations (20%) now directly attribute increased insider risk to AI tool usage, placing it alongside more established drivers such as mobility and excessive access. While not yet dominant, AI is already influencing how insider risk manifests.

Top Drivers of Insider Incidents

What do you think are the main drivers and enablers behind the increase in insider incidents?



Even with early adoption, 20% already cite AI tool usage as a main driver of rising insider incidents.

Insider risk is increasingly being driven by how systems are built—not by bad actors. Addressing it requires reducing the blast radius of routine actions instead of simply detecting malicious ones.

When AI Became an Insider

AI did not introduce insider risk. It exposed how fragile existing trust and access models had already become by operating at a scale those models were never designed to support.

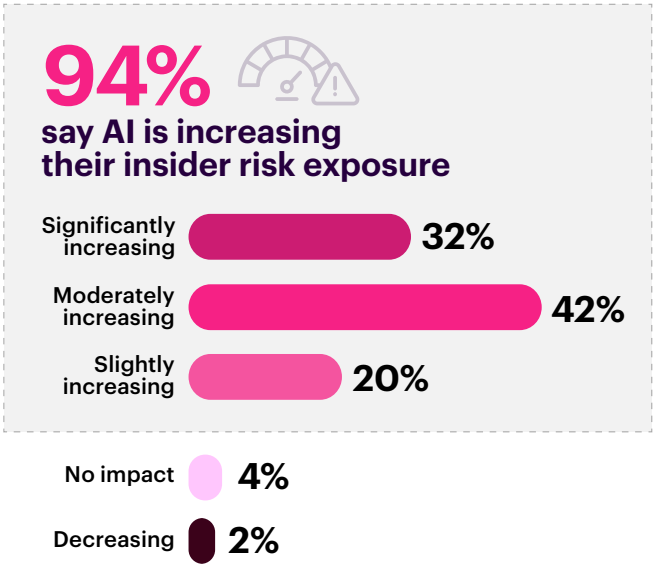
Nearly all organizations (94%) report that rapid AI adoption is increasing their insider risk exposure. For most, this isn't marginal: 74% describe the increase as moderate or significant, and nearly one-third (32%) call it significant. Only a small minority of 6% see no impact or risk reduction. AI has expanded the insider attack surface faster than governance models can adapt.

The concern extends beyond internal misuse. 65% are extremely or very concerned about AI-powered cyber threats such as deepfakes, AI-generated phishing, and automated reconnaissance targeting their organizations. AI is now expanding the attack surface from both directions: employees using legitimate AI tools without guardrails, and attackers weaponizing AI to blend in more effectively.

One common pattern looks like this: an employee connects a copilot to their inbox for productivity. The copilot can access messages, attachments, and sensitive threads, and it can act across connected systems. In many environments, security has limited visibility into what the copilot accessed, what it inferred, and what it propagated. When access is delegated to AI without equivalent controls, the blast radius of a single mistake expands materially.

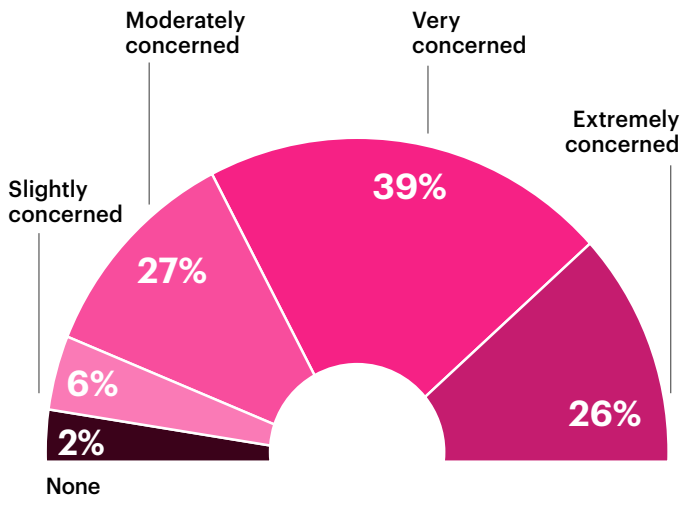
AI Impact on Insider Risk Exposure

To what extent is the rapid adoption of AI increasing your organization's insider risk exposure?



Impact of AI on Cyber Threats

How concerned are you about your organization's exposure to AI-powered cyber threats (such as deepfakes, AI phishing, LLM-driven reconnaissance or exploitation)?



AI must be governed as an insider with delegated authority, not treated simply as a neutral productivity layer. Organizations that fail to do so will continue to expand access faster than they can contain risk.

The Incidents Organizations Won't Admit

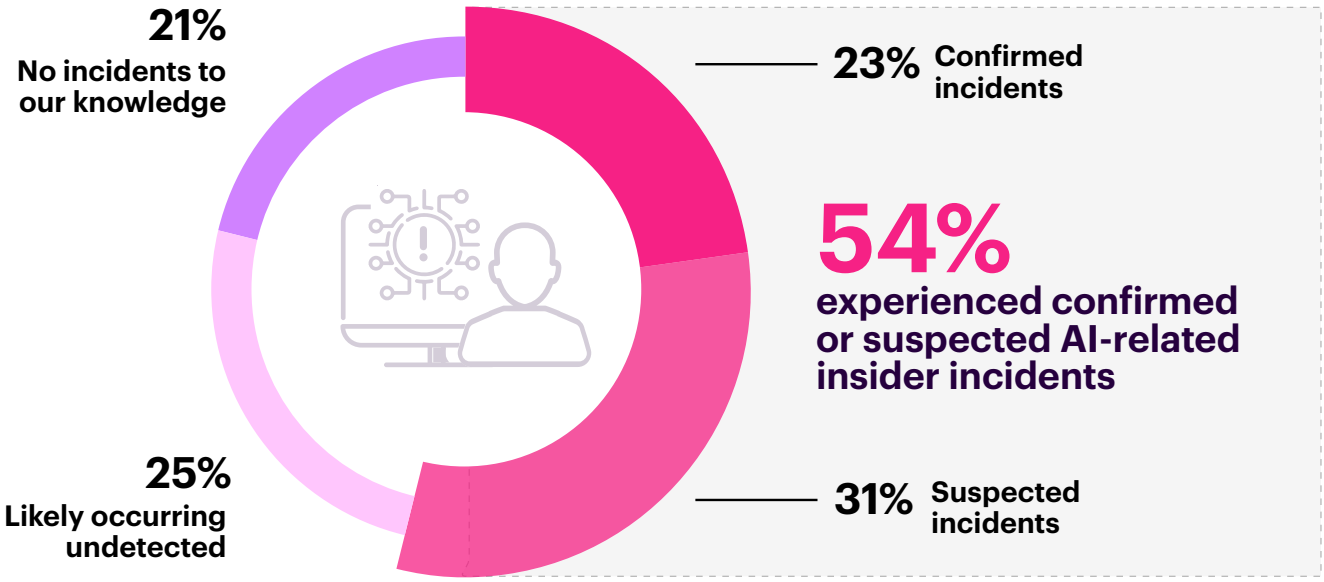
AI-related insider incidents are already occurring, even when organizations hesitate to label them as such.

More than half of organizations (54%) acknowledge AI-related insider incidents within the past 12 months: 23% report confirmed incidents and another 31% report suspected ones. A further 25% believe incidents are likely occurring but remain undetected. Only 21% report no AI-related incidents to their knowledge.

We've seen this pattern before. In earlier phases of insider risk management, incidents went underreported until a major breach forced the conversation. AI-related incidents appear to be following the same trajectory - widespread in practice, underlabeled in reports.

AI-Related Insider Incidents

Has your organization experienced any security incidents directly related to employees misusing or mishandling AI tools within the past 12 months?



As AI becomes more deeply embedded, organizations that lack visibility into AI-driven actions will continue to underestimate both incident frequency and exposure.

Non-Human Insiders

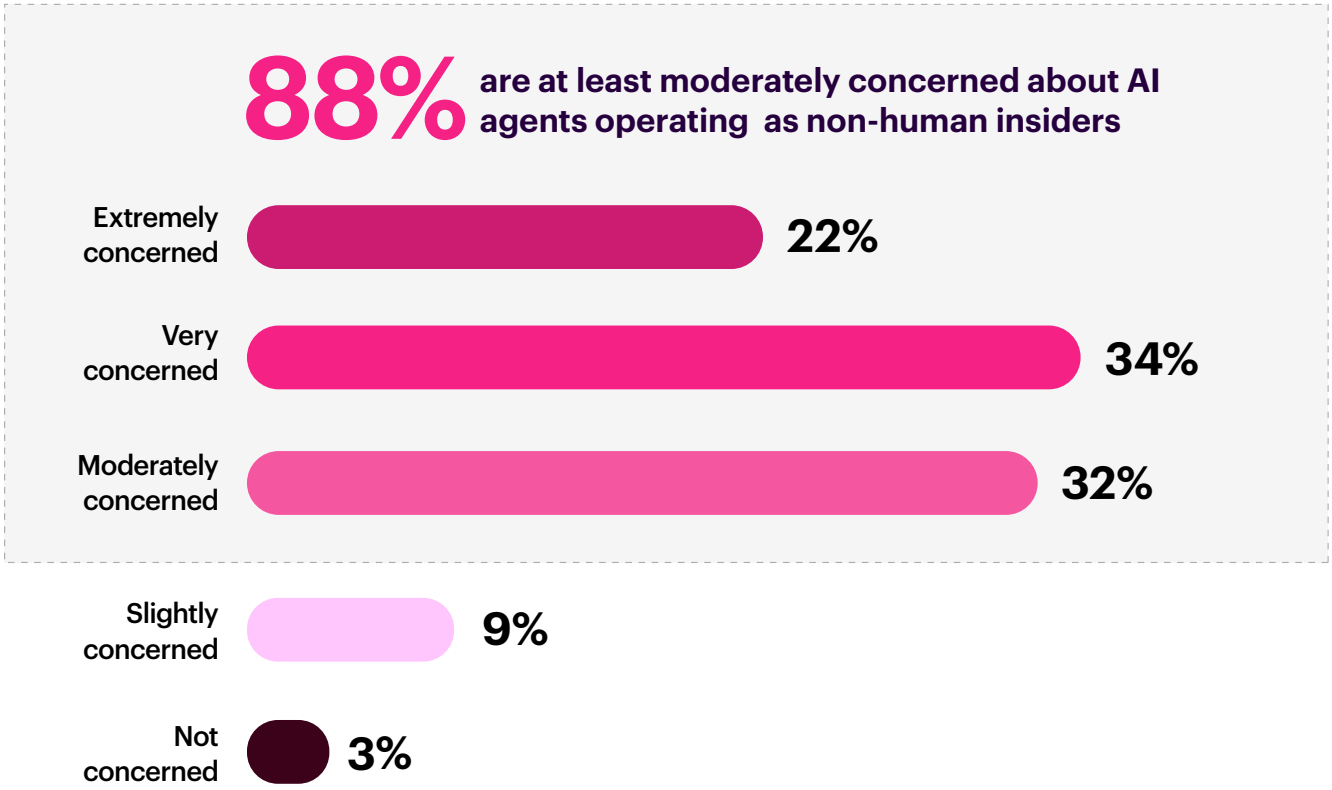
AI agents aren't just tools. They're becoming autonomous actors with insider-level access.

A clear majority of organizations express concern about non-human insiders. Fifty-six percent are extremely or very concerned about AI agents operating as digital employees, with another 32% moderately concerned. Only a small minority report limited or no concern.

This concern reflects how these agents operate in practice. AI agents authenticate using service or delegated accounts, access sensitive systems, and execute workflows without continuous human oversight. When they misbehave, are manipulated, or drift beyond intended scope, they create insider incidents without a human actor behind it.

Concern Over AI Agents as Non-Human Insiders

How concerned are you about the risk of non-human insiders (AI agents as digital employees to handle tasks, automate processes, and work alongside human employees)?



The governance challenge is acute because insider risk programs built around human behavior, training, and accountability do not translate cleanly to autonomous systems. As non-human insiders proliferate, governance, visibility, and control must extend to machine identities with the same rigor applied to people.

The AI Duality

AI is simultaneously expanding insider risk and becoming the primary mechanism organizations expect to control it.

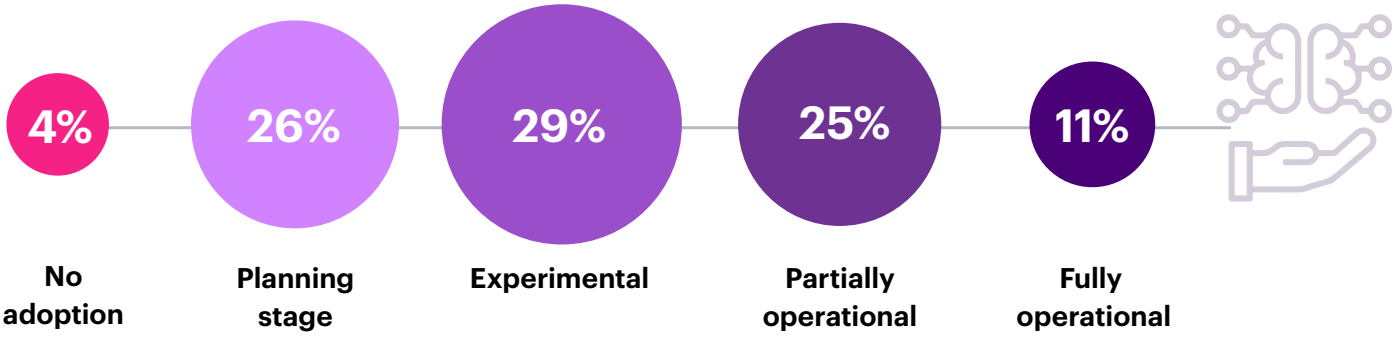
Earlier findings show that AI adoption is already reshaping insider risk exposure. Ninety-four percent of organizations report that AI is increasing their insider risk, and 54% acknowledge confirmed or suspected AI-related insider incidents within the past 12 months. AI is no longer a theoretical concern; it is already inside operational workflows.

At the same time, organizations are turning to AI as a defensive necessity. A third are fully or partially operational (36%). More than half (55%) are piloting or planning to deploy AI-powered insider risk capabilities within the next 12 months, driven by rising incident volume and limited ability to scale human analysts alone.

This tension exists because AI amplifies weaknesses that were previously manageable, transforming latent gaps in identity, access, and behavioral governance into active failure points. AI accelerates insider risk by inheriting access, amplifying mistakes, and obscuring intent. Yet human-centric monitoring and response models are proving insufficient against fragmented signals and sustained insider activity.

AI Adoption in Insider Risk Management

What best describes your organization's current adoption of AI tools within Insider Risk Management operations?



Not sure 5%

Insider risk management is entering an era where AI is no longer optional on either side of the risk-defense equation. Organizations must govern AI as an insider while simultaneously relying on it to defend against insider risk at scale.

The Confidence Gap

Organizations recognize that AI is creating insider risk. Few believe they can stop it in time.

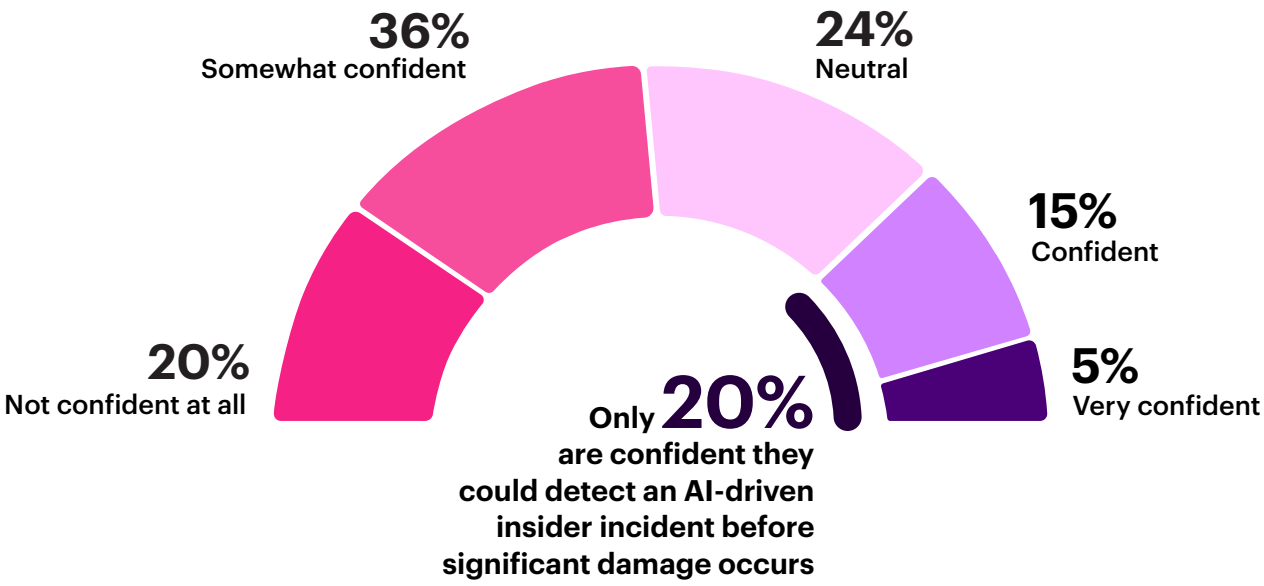
Only 20% of organizations say they are confident they could detect and contain an AI-related insider incident before significant damage occurs. The majority sit below that threshold: 36% are only somewhat confident, and 20% are not confident at all. This gap between awareness and capability is now a defining control failure in modern insider risk programs.

The contrast with earlier findings is stark. While 94% report that AI is increasing insider risk exposure, only one in five believes their detection and response capabilities are sufficient to intervene early. The result is a widening window where AI-driven misuse, mistakes, or manipulation can unfold without timely containment.

Most organizations are responding to close the gap, but unevenly. Nearly half have deployed or plan to acquire AI-powered detection capabilities within the next 12 months, and another 29% are actively evaluating options. Intent is high, but confidence has not yet followed.

Confidence Detecting and Containing Insider Incidents Involving Misuse of AI

How confident are you that your organization could detect and contain an insider incident involving misuse of AI tools or AI-generated attacks before significant damage occurs?



The implication is that awareness without capability creates false assurance. Until detection, investigation, and response mature together, organizations will continue to recognize AI-driven insider risk faster than they can control it.

Headcount Won't Scale

Rising insider risk volume is colliding with fixed human capacity.

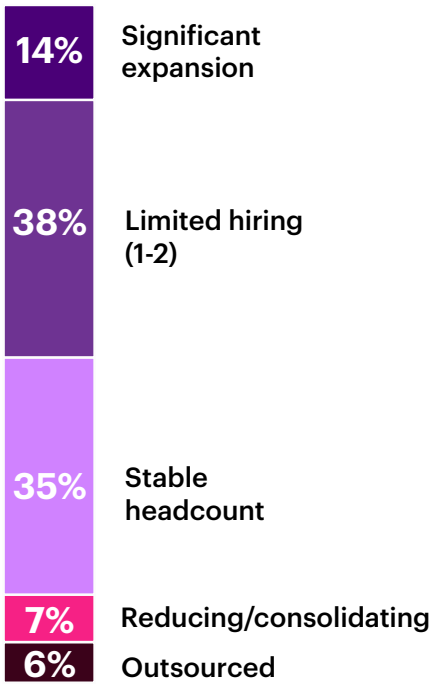
More than half of organizations (52%) plan to hire additional insider risk personnel over the next 12-24 months, but only 14% anticipate significant expansion. At the same time, 35% expect headcount to remain flat and 7% plan to reduce or consolidate. These plans do not align with the scale of insider activity organizations now report. The mismatch is structural. Insider incidents are increasing, detection is becoming harder, and AI-driven activity is expanding the attack surface. Incremental hiring cannot absorb sustained incident volume, nor can it close the detection-response gap created by continuous insider activity.

Organizations appear to recognize this reality. Fifty-four percent have already deployed, are piloting, or plan to adopt a virtual AI analyst within the next 12 months, and 79% expect adoption within 24 months. The direction is clear: AI augmentation is replacing human expansion as the primary scaling strategy.

This shift does not diminish the role of experienced insider risk analysts. On the contrary, human expertise remains essential for contextual judgment, investigation, and decision-making—particularly in ambiguous or high-impact cases. AI augments analyst capacity by reducing manual workload and accelerating signal triage, but it does not replace the need for skilled practitioners who understand intent, risk tolerance, and organizational context.

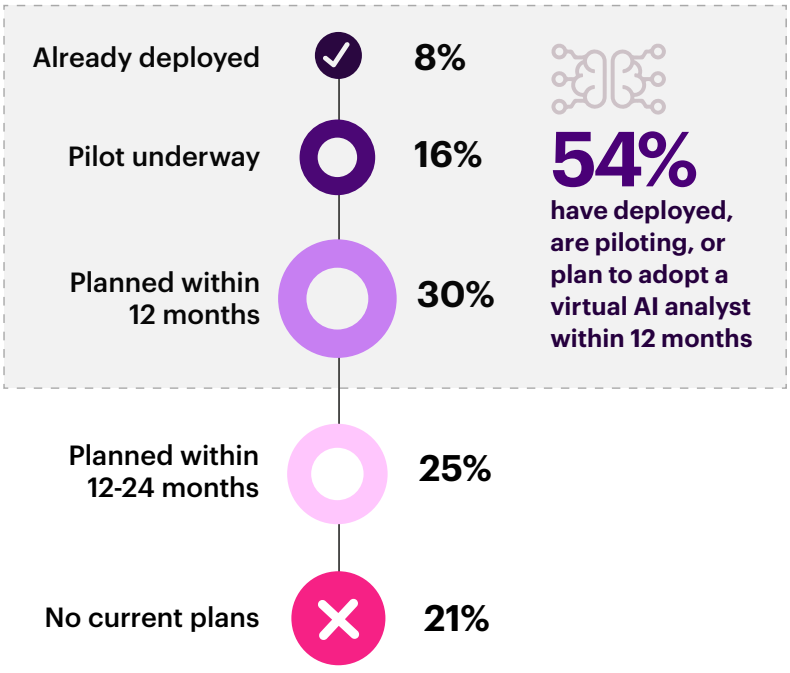
IRM Hiring Plans

Do you plan to hire additional full-time Insider Risk Management employees or analysts over the next 12-24 months?



Virtual AI Analyst Adoption Plans

What are your organization's plans for adopting a virtual 24/7 AI analyst to help scale your Insider Risk Management (IRM) team without adding headcount?



Insider risk programs that rely solely on human analysts will struggle to keep pace. The organizations that succeed will govern AI like any other insider - and use automation to scale beyond human limits.

Integration Over Addition

Leaders no longer expect incremental fixes to deliver meaningful improvement. Architectural change is becoming the only viable path to regaining control.

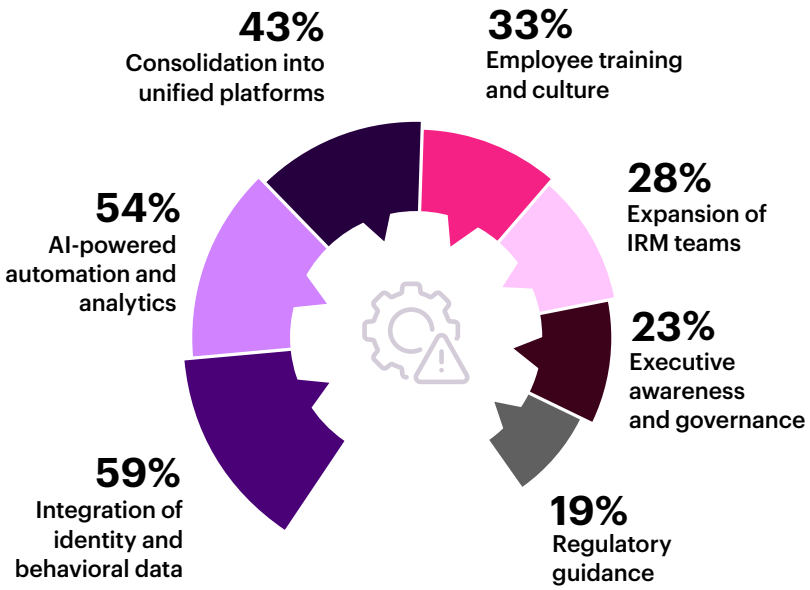
When asked what will have the greatest impact on insider risk management over the next 24 months, organizations converge on three priorities: integration of identity and behavioral data (59%), AI-powered automation and analytics (54%), and consolidation into unified platforms (43%). Traditional levers rank lower with only one-third citing employee training (33%), and fewer than three in ten prioritizing expanding IRM teams (28%).

This prioritization reflects the constraints surfaced earlier in the report. Rising incident volume, fragmented tooling, and limited headcount have reduced confidence that people-centric or tool-additive approaches can scale. Leaders are instead favoring changes that reduce complexity and improve signal quality at the system level.

Budget intent reinforces this shift. Seventy-five percent of organizations expect AI-powered solution budgets to increase over the next 12–18 months, including 27% anticipating significant growth. Very few expect reductions, indicating strong conviction that automation and integration are now central to insider risk outcomes.

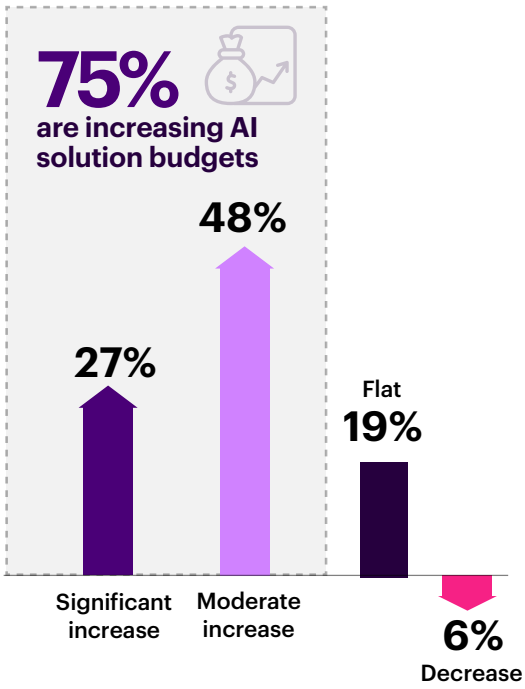
Top Impact Drivers for IRM

Looking ahead 24 months, what will have the greatest impact on improving insider risk management in your organization?



AI-Powered Solution Budget Trends

What are your budget trend expectations for AI-powered solutions over the next 12–18 months?



Organizations believe insider risk will be won through better architecture, not more human effort. Integration, automation, and consolidation are viewed not as enhancements, but as prerequisites for regaining control.

The Detection-Response Gap

Organizations that contain insider risk share a profile. Those that absorb it share a different one.

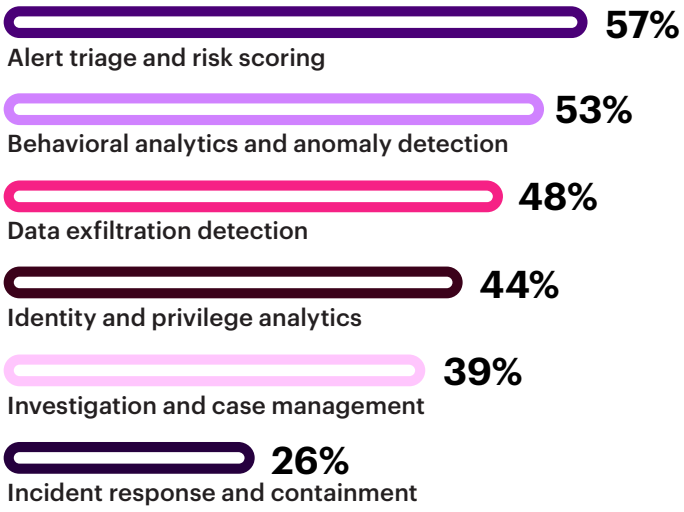
Leaders say they want faster detection and fewer false positives, but outcomes reveal a gap between finding risk and stopping it. Among organizations using AI in insider risk workflows, 57% report success in alert triage and risk scoring, and 53% in behavioral analytics. That progress collapses downstream: only 39% succeed in investigation and just 26% in incident response.

This detection–response gap defines the difference between organizations that contain insider risk and those that silently absorb it as operational cost. Detecting insider activity without the ability to investigate and contain it quickly converts alerts into backlog, not risk reduction. As incident volume rises, delayed response only aggravates impact and cost.

Desired outcomes reinforce this divide. Organizations prioritize faster detection and response (56%), higher accuracy with fewer false positives (51%), and reduced manual workload (45%). These are core operational requirements for teams managing continuous insider activity with limited headcount.

The Detection-Response Gap

Which IRM workflows have been most successfully automated using AI?



Compliance and policy automation 21%
High-risk user monitoring 18%

Desired Outcomes from AI-Powered IRM

Which operational outcomes does your organization hope to achieve from adopting AI-powered Insider Risk Management platforms?

Enhanced compliance and data protection 19%

The choice is straightforward: close the loop from signal to action through integrated data, automation, and response orchestration or keep detecting problems you can't actually stop.

The Path Forward

The data in this report points to a clear conclusion: insider risk failures are structural, not behavioral - and structural problems do not resolve through incremental change. Three strategies separate those that regain control from those that continue to absorb risk:

1

UNIFY VISIBILITY AND BEHAVIOR BEFORE ADDING ANYTHING ELSE

Fragmented visibility is the most consistent inhibitor of progress. Integration of identity and behavioral data ranks as the top driver of improvement for 59% of organizations, while 66% still cite detection accuracy and 58% cite tool and data fragmentation as primary challenges. Without a unified view of who is acting and how, insider risk remains invisible until damage is already underway.

2

TREAT AI AS BOTH AN INSIDER AND A DEFENDER

AI has expanded insider risk exposure for 94% of organizations, and 54% have already experienced confirmed or suspected AI-related insider incidents. At the same time, more than half are deploying or acquiring AI-powered insider risk capabilities within the next 12 months. Organizations that succeed, govern AI like any other insider while using AI automation to scale detection and response beyond human limits.

3

CLOSE THE GAP FROM DETECTION TO ACTION

While 57% report success using AI for alert triage and 53% for behavioral analytics, only 26% succeed at incident response. This detection–response gap determines outcomes. Organizations that contain insider risk prioritize execution speed and automation, not just alert quality.

The path forward isn't more tools or more people, it's architectural re-design that assumes continuous insider activity, governed AI access, and automated response by default.

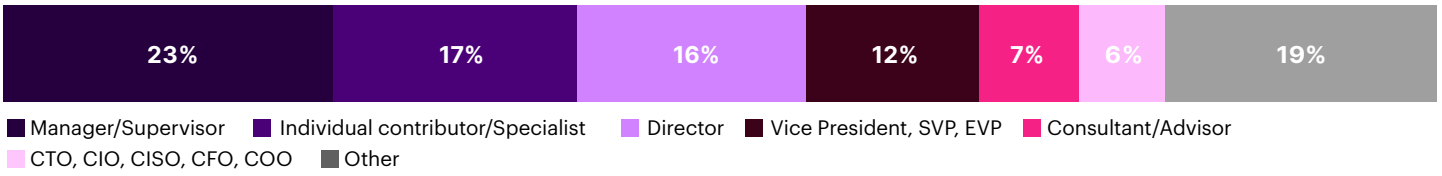
Methodology and Demographics

This report is based on a comprehensive online survey of 725 IT and cybersecurity professionals, conducted in late 2025 to capture the current state of insider risk management across enterprises.

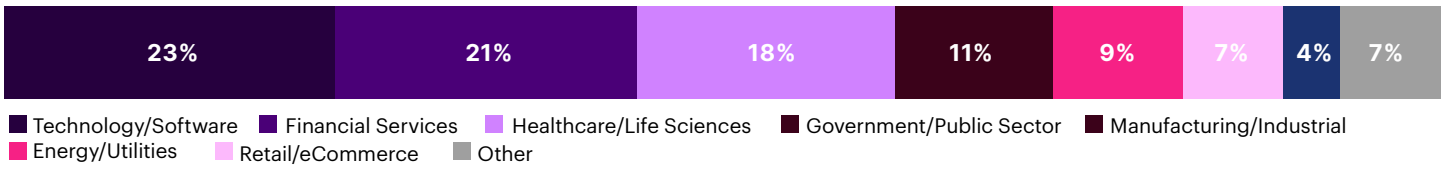
The survey utilized a methodology ensuring diverse representation across roles, industries, and organization sizes, from technical practitioners to security executives. This approach provides a balanced view of the insider risk landscape, capturing perspectives from those who set strategy and those who execute it daily.

Statistical Note: Year-over-year comparisons reference the 2024 Insider Threat Report, which surveyed 413 professionals using comparable methodology. With 725 respondents, this survey carries a margin of error of approximately +/- 3.6 percentage points at a 95% confidence level.

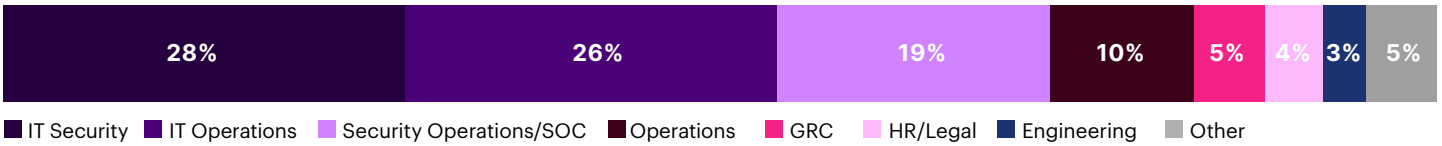
CAREER LEVEL



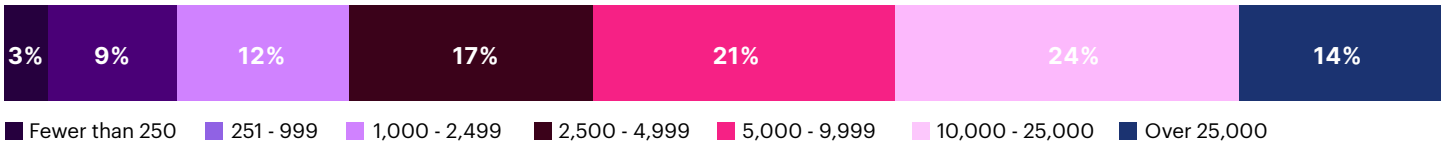
PRIMARY JOB FUNCTION



DEPARTMENT



COMPANY SIZE



Reuse of content

Gurucul delivers identity-centric and behavioral security analytics that give security teams radical clarity into cyber risk across external adversaries, insider threats, and identity-based attacks. Our REVEAL platform applies advanced machine learning and AI to enterprise data at scale so SOC and Insider Risk teams can predict, prioritize, and mitigate true threats instead of chasing useless alerts.

With an open, cloud-native architecture and built-in data optimization, Gurucul gives Global 1000 enterprises complete data independence—bring your own lake, control your pipeline, and slash SIEM data ingestion costs by up to 87% while unlocking SOC and IRM program efficiencies with AI embedded across the entire TDIR lifecycle.

Recognized by leading industry analysts as a leader in SIEM, insider risk, AI-SOC, and ITDR, Gurucul is proven to materially lower organizations cybersecurity risk.

To learn more, visit Gurucul.com

and follow us on LinkedIn and X.

Cybersecurity
INSIDERS

STRATEGIC INSIGHT FOR CYBERSECURITY LEADERS

Cybersecurity Insiders provides independent research and analysis focused on the operational reality of enterprise cybersecurity. We gather insights from senior security and IT leaders to examine how high-level strategies translate into day-to-day execution. Our analysis identifies the measurable gaps between intended strategy and actual risk exposure, offering a credible, data-driven foundation for security decision-making and industry benchmarking.

For more information, visit
cybersecurity-insiders.com

Feb 2026 // Version 1.8