FORTINET

2025

INSIDER RISK REPORT

Peer Insights to Inform Your Insider Risk Strategy

Cybersecurity INSIDERS

OCTOBER 2025

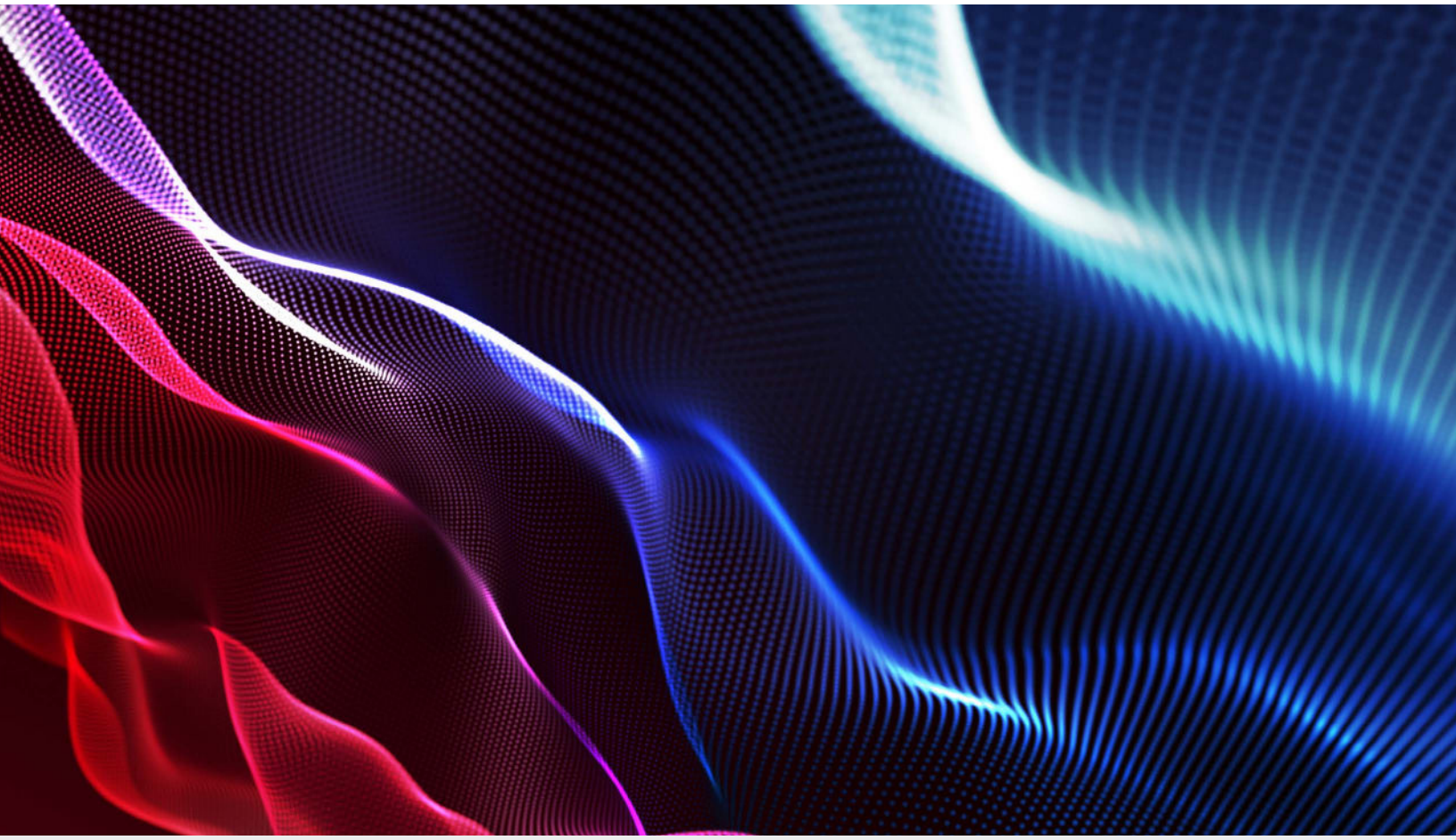
Executive Summary

Insider risk has become one of the most urgent challenges in enterprise security. As data flows freely across users, devices, cloud apps, GenAI tools, and hybrid workspaces, traditional defenses—built to block external threats or prevent leakage—fall short against insider-driven exposures. Unlike external attacks, insider risk is behavioral, context-driven, and embedded in everyday workflows. Incidents often stem from both intentional and unintentional user actions, whether by employees or contractors.

Yet most organizations still rely on fragmented tools that lack behavioral insight, contextual awareness, and real-time responsiveness. The result: persistent blind spots, delayed detection, and missed chances to act before damage occurs.

Research from this report and our earlier 2025 Data Security Study shows steady progress in building insider risk and data security frameworks. Budgets are growing, and most organizations now have structured programs in place. However, program maturity continues to lag, and the effectiveness of current tools in preventing sensitive data loss remains in question. A heavy reliance on traditional data loss prevention tools, in particular, appears to hinder programs and limit their overall impact.

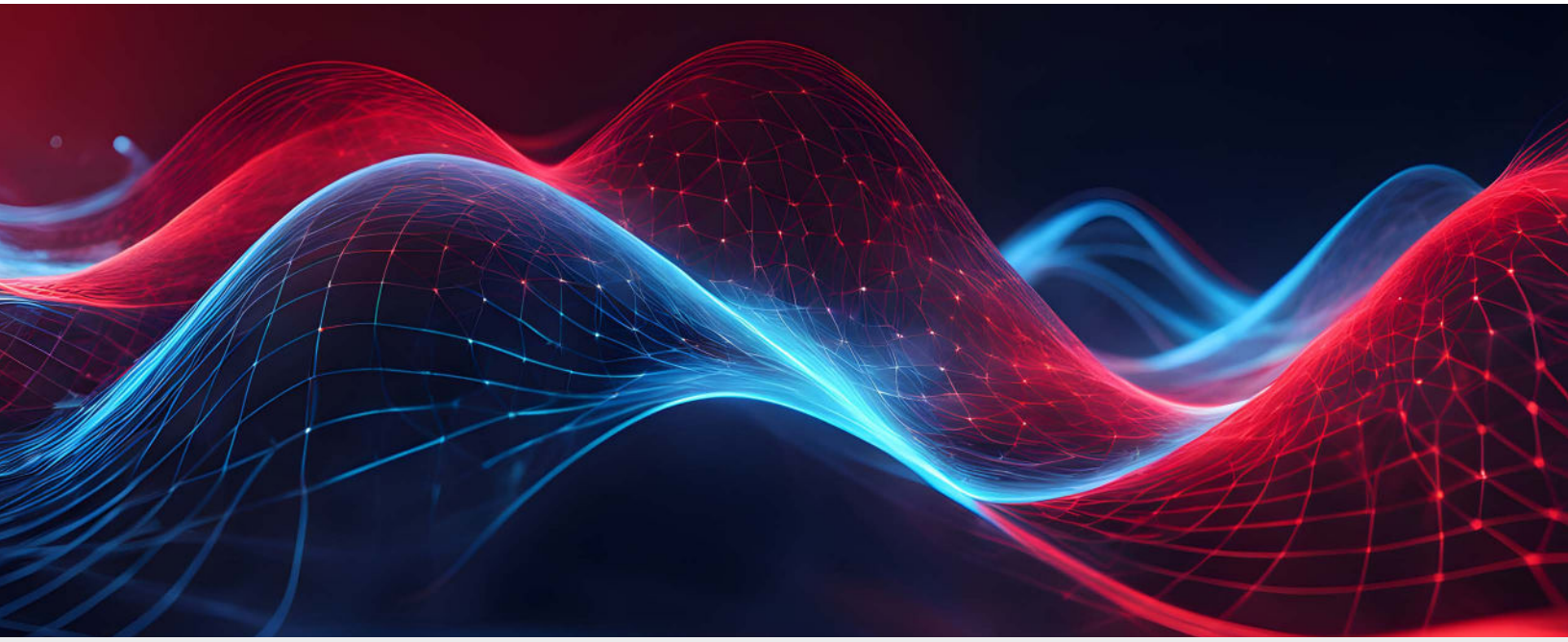
Based on a comprehensive survey of 883 IT and security professionals conducted by Fortinet and Cybersecurity Insiders, this report reveals how organizations are rethinking insider risk. It highlights a shift from reactive enforcement to behavior-aware strategies and next-gen tools—solutions that provide visibility into business data flows while addressing decentralized data, distributed workforces, and the rapid adoption of AI.



Key Findings Include:

- **Insider incidents are widespread and costly**
  77% of organizations experienced insider-driven data loss in the past 18 months, and 41% reported financial impact between $1M and $10M for their most significant incident.
- **Most incidents are unintentional**
  62% were caused by negligent or compromised users; only 16% involved confirmed malicious intent.
- **User risks proliferate**
  73% of Security pros are most concerned about careless, negligent or uninformed employees, 62% for employees directly involved in the handling of sensitive data such as PII, PHI, PCI, etc., and 55% are concerned about the risks posed by departing employees.
- **Visibility remains a significant gap**
  72% can't see how users interact with sensitive data across endpoints, cloud apps, and GenAI platforms. Only 28% have effective data discovery and classification.
- **Programs are maturing, but confidence in tools is low**
  While 64% claim to have a formal data protection program, 51% report fragmented tool integration. The result: only 14% of organizations feel fully confident in their insider threat detection capabilities.
- **GenAI is expanding the attack surface**
  56% are very concerned about sensitive data being shared with tools like ChatGPT, but only 12% feel fully prepared to respond to it.
- **DLP is increasingly a barrier**
  Only 47% of security pros strongly agree that their existing DLP tools are effective in protecting sensitive data from leaving the organization. And these tools lack the visibility critical to understanding the "who" and "why" behind when sensitive data has been put at risk.
- **Security leaders are pivoting to behavior-first, AI-aware platforms**
  66% now prioritize real-time behavioral analytics, and 52% cite SaaS and GenAI tool control as critical next-generation priorities.

As a result, forward-leaning organizations are moving to integrated, behavior-driven platforms that provide unified visibility, adapt to risks in real-time, and deliver insights—not just enforcement. This report examines the current state of that transition and highlights the practices, capabilities, and priorities shaping the future of insider risk management.



Shared Stewardship of Insider Risk

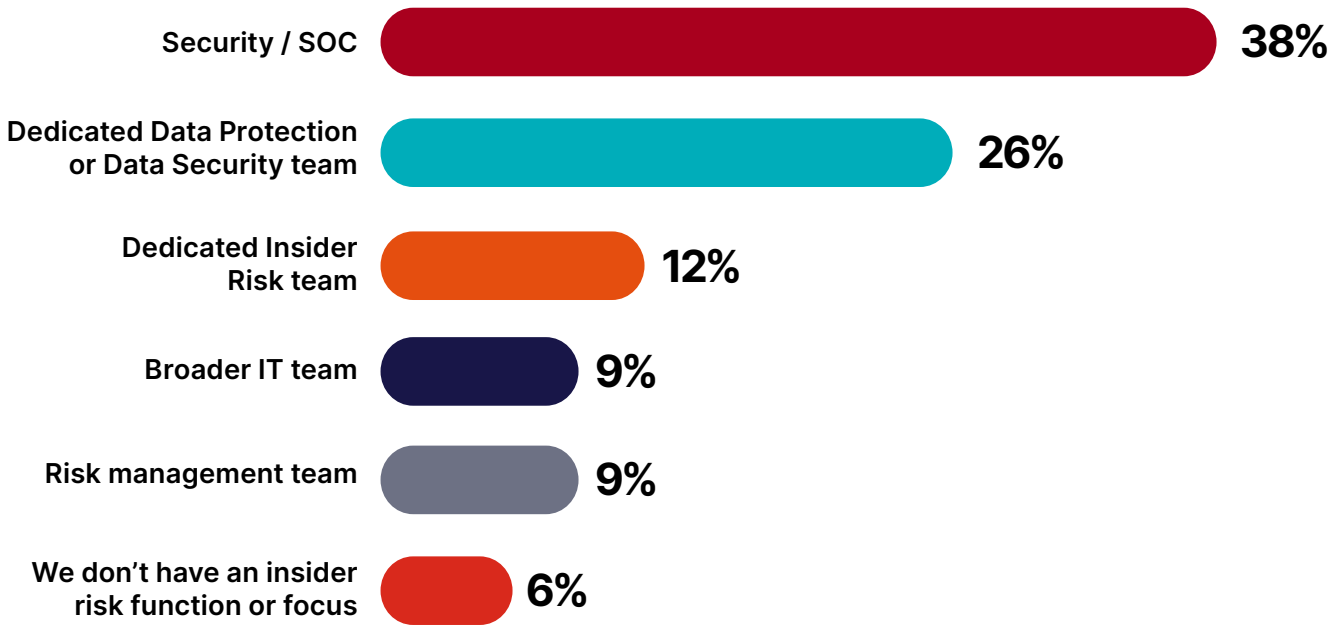
Insider risk functions are largely anchored within different teams: 38% of organizations place it in security/SOC, 26% in data protection, 12% in dedicated insider risk groups, with remaining responsibilities split among IT, enterprise risk, or not assigned at all.

This diversity underscores a critical point: effective insider risk management rarely resides in a single function. But it demands a governed, cross-functional approach, actively supported by senior leadership.

Best practices call for formal insider risk programs with directives, governance groups, and oversight to carry consistent policies, detection, and response across HR, Legal, IT, and beyond. Also essential is a senior decision-maker who owns funding and visibility to help break down data silos.

Ultimately, insider risk is not a single-team issue – it is an organization-level challenge. When governance, processes, and technology align across teams, organizations respond faster, more consistently, and with greater precision.

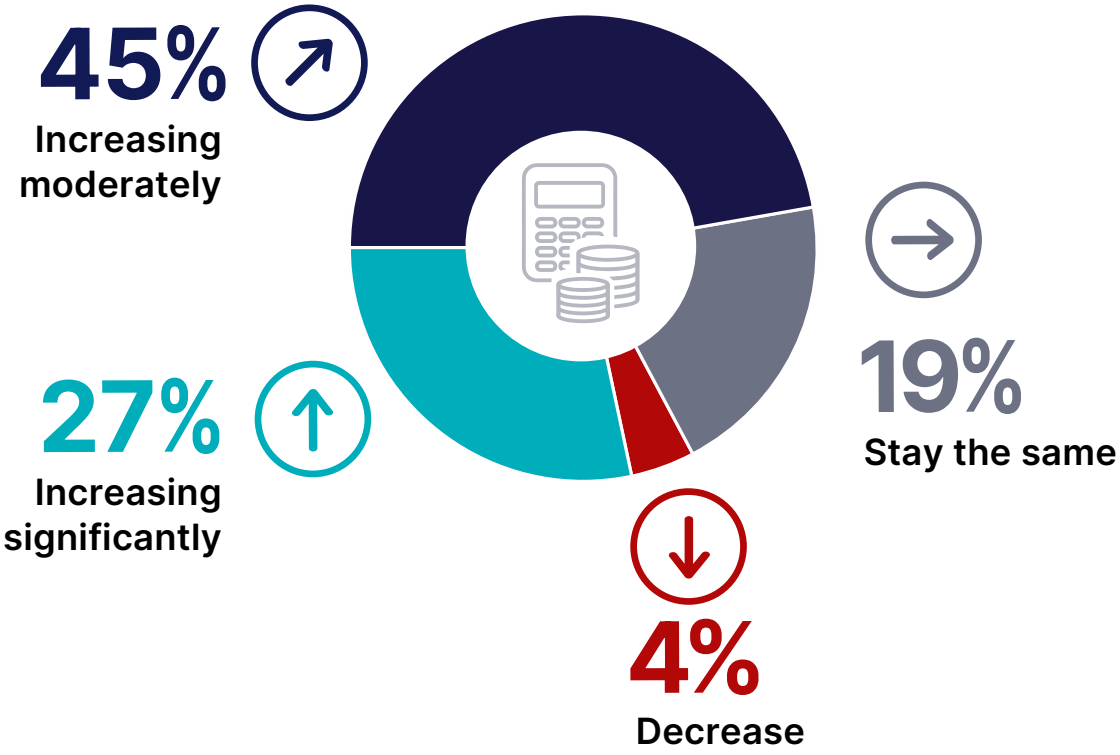
Who owns insider risk as a function in your organization?



Recognizing Insider Risk – Budgets Speak Louder

Insider risk is receiving real investment. Seventy-two percent of organizations say their budgets for insider risk or data protection are increasing, and 27% report significant growth over the past year. However, budget alone will not solve fragmented architecture, disconnected telemetry, or missing context. Without a unified approach that integrates data, behavior, identity, and policy, even the best-funded programs risk falling short.

Which best describes your current insider risk or data protection budget trend?



Unknown / not disclosed 5%

Maturity Bottlenecks at the Middle Tier

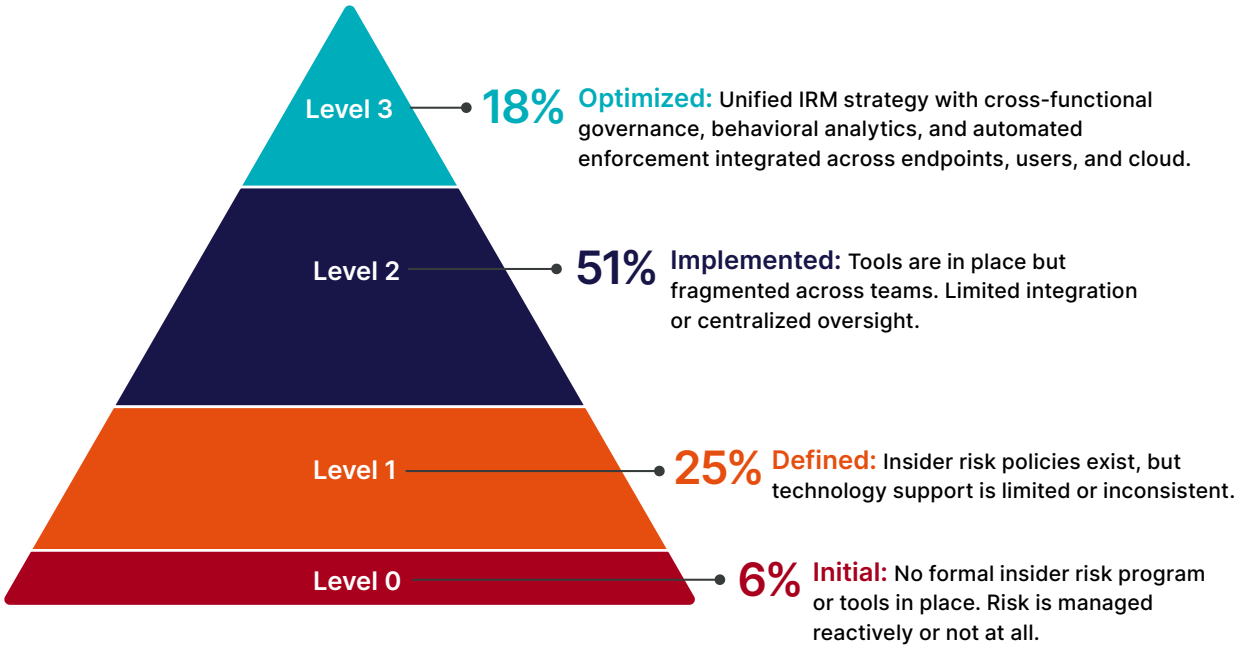
Insider risk is not just a visibility problem; it is also a maturity problem. And most organizations are stuck in the middle: More than half (51%) say they're operating at Level 2 on the 0 to 3 maturity scale: tools are in place but fragmented across teams with little integration or centralized oversight. Another 25% sit at Level 1, where policies may exist, but enforcement is inconsistent or unsupported by technology. Only 18% say they have reached Level 3, where insider risk is managed through unified strategy, cross-functional governance, behavioral analytics, and integrated enforcement across users, endpoints, and cloud.

This stall isn't due to lack of investment. While resources are growing, measurable returns often lag. Too many programs remain trapped in tactical execution: deploying disconnected tools, generating alerts, spending an inordinate amount of time investigating potential incidents, and failing to operationalize response workflows.

The result is what many teams experience daily: the illusion of readiness. Dashboards are live, policies exist; yet without context and coordination, responses are delayed, misdirected, or never initiated.

Closing this gap requires more than a budget. It demands a strategic shift to unify detection, behavioral analytics, and policy enforcement within a single operational model.

How would you rate your overall Insider Risk Management maturity?

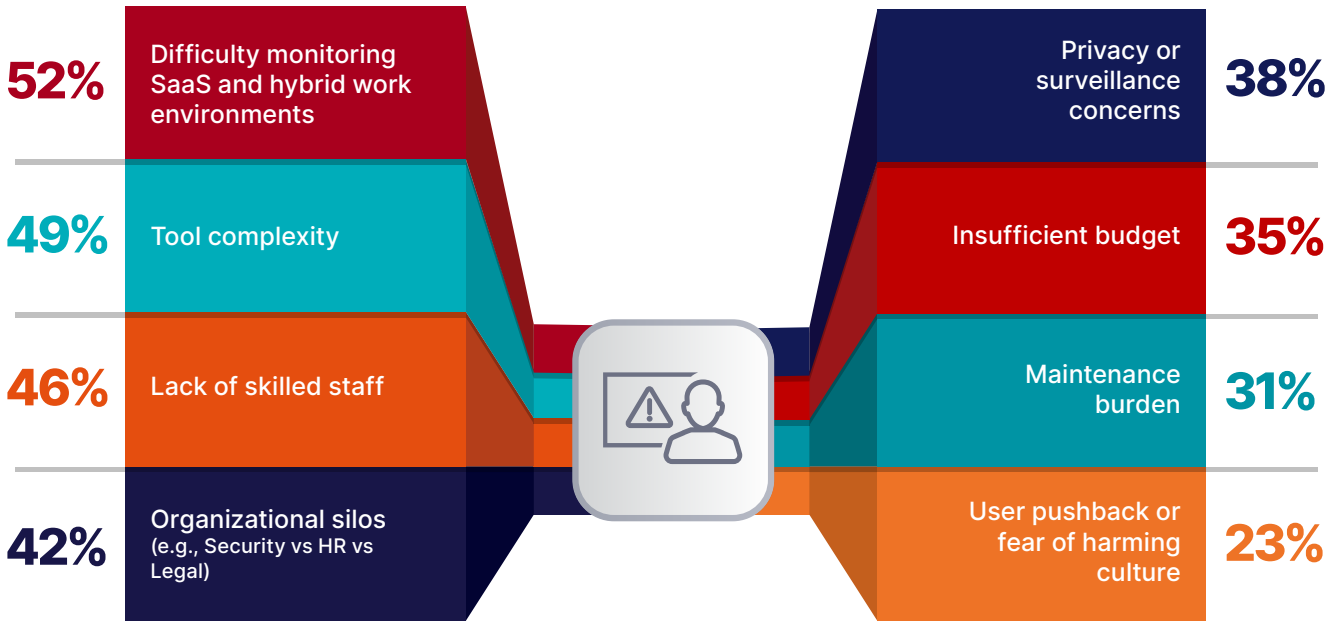


What's Holding Insider Risk Programs Back?

Fifty-two percent of respondents say the biggest barrier is monitoring SaaS and hybrid environments - now the norm for how work gets done. Tool complexity (49%) takes the number two spot. Because visibility into SaaS and hybrid environments is a tooling function, tools collectively represent insider risk teams' biggest challenge in maturing their insider risk practices.

A lack of skilled staff (46%) further highlights operational strains, while organizational silos between Security, HR, and Legal (42%) slow coordination. Privacy concerns (38%) and user pushback (23%) reflect the cultural sensitivity insider risk programs must navigate.

What are your biggest barriers to maturing your insider risk program?



Blind to Behavior - Slow to Insight

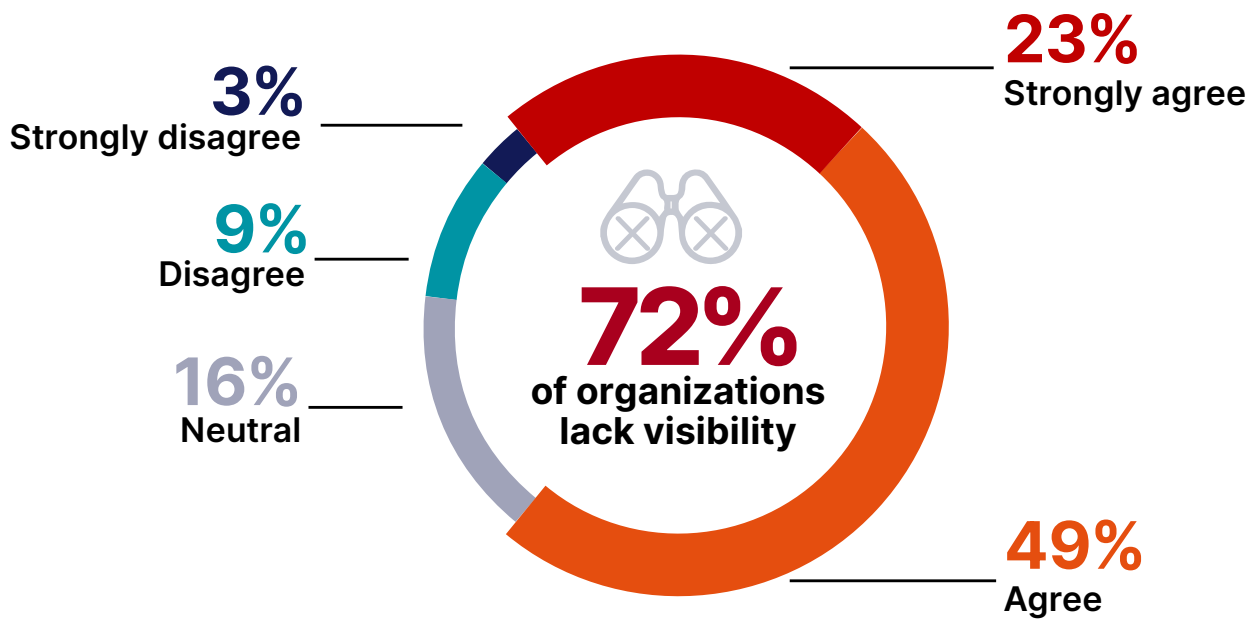
The financial consequences of insider incidents are substantial, which we cover later, but the real question is why so few are intercepted before the damage is done.

The answer, for most organizations, is visibility. Seventy-two percent admit they lack insight into how users interact with sensitive data across endpoints and cloud applications. In today's dynamic environments where data moves freely and behavior drives risk, this isn't just a gap. It's a systemic control failure.

Most tools can tell what happened, but not why, by whom, or whether it signals intent. Without behavioral context, there's no way to separate legitimate activity from early-stage risk. And without that insight, detection happens too late.

Closing this gap requires moving beyond static policy enforcement toward integrated approaches that correlate user behavior, identity, and data movement in real-time - enabling teams to see risk forming and act before it escalates.

To what extent do you agree: Our organization lacks visibility into how users interact with sensitive data across endpoints and cloud applications?



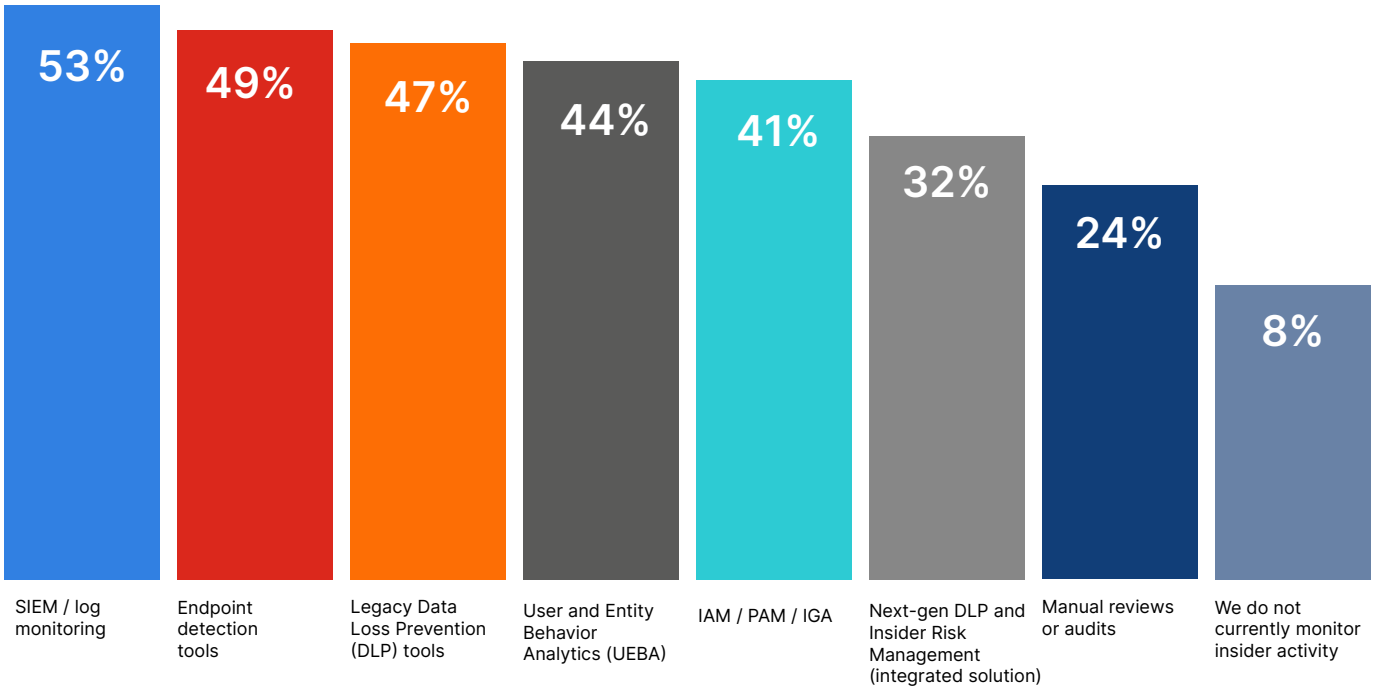
Monitoring User Activity, Or Trying To

Insider risk pros use a plethora of tools to monitor insider risk. However, we can immediately see the limitations of these tools when it comes to visibility and contextual understanding of insider risks.

SIEM and log monitoring tools, endpoint detection tools, legacy DLP solutions, and UEBA often don't work seamlessly together. More importantly, they do not create a curated dataset or a clear timeline of user behavior and interactions with sensitive data. As a result, it is challenging to determine precisely what data is being accessed, how it is being manipulated, who is responsible, and why the data may be at risk. Additionally, the disparate mix of tools requires analysts to spend excessive time collating event information before they can investigate potential incidents.

This inefficiency erodes analysts' ability to spot risky behavior and intervene before data loss occurs—especially when compared to newer tools that unify visibility, controls, detection, and response around user behavior. These next-generation solutions, such as modern data loss prevention and insider risk management, are already in use at 32% of organizations. As we'll cover later, they focus directly on how users interact with sensitive data while overcoming the limitations of legacy DLP and other older tools.

How does your organization monitor insider activity today?



Is Traditional DLP Getting in the Way of Preventing Data Loss by Insiders?

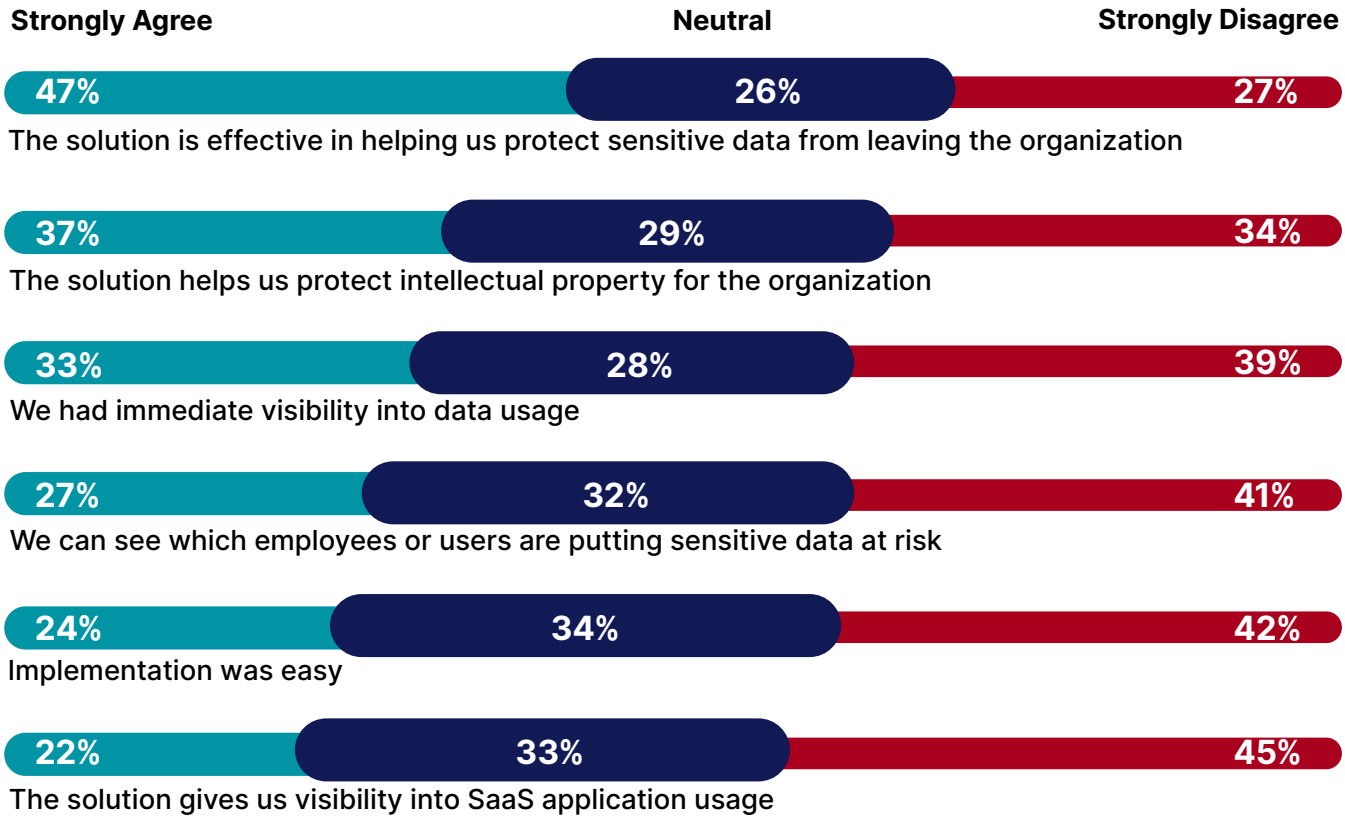
Forty-seven percent of organizations utilize legacy DLP tools to prevent sensitive data from leaving their organizations as a result of an insider, whether that be an employee or other user. In fact, this is one of the most commonly relied upon tools organizations have in place. The problem lies in what those tools do—and do not—reveal. And it's here that one has to wonder if traditional DLP tools, with their limitations and inflexibility, act as a barrier, diverting resources away from impactful tools that could help advance both data protection and overall insider risk programs.

Only 47% of respondents say their DLP helps prevent sensitive data from leaving the organization, with far fewer reporting deeper visibility. Only 33% agree they gained immediate insight into data usage, 27% can identify which users are putting data at risk, and just 22% say they have visibility into SaaS application usage and related data flows. Implementation itself remains a challenge: only 24% say it was easy.

This highlights a critical gap: traditional DLP can block known violations, but it rarely explains why they happen or surfaces the early warning signs that lead up to them. These tools struggle with the slow-drip, high-risk patterns that define insider behavior: off-hours activity, repeated low-risk access, or sensitive content moved into AI tools or personal cloud accounts.

Without behavioral visibility and contextual telemetry, most DLP solutions remain reactive, enforcing static rules while leaving teams blind to emerging patterns of insider risk.

If your organization currently uses a Data Loss Prevention solution, how would you rate the following?



What's Actually at Stake

Insider risk is playing out in real incidents, affecting real data, across every industry. To understand the scale of the challenge, we need to start with what's being exposed. If the scope of the problem is defined by how often incidents occur, the stakes are defined by the types of data involved.

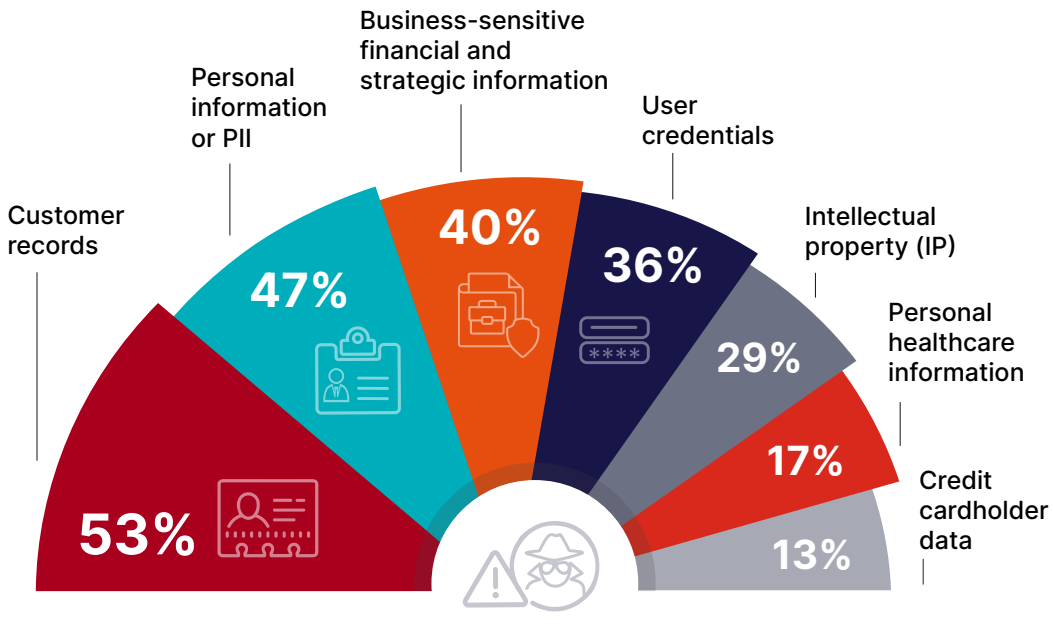
Knowing what data is compromised is just as critical as understanding how it leaves. In the most significant incidents, customer records (53%) and personally identifiable information (47%) top the list - exactly the types governed by strict compliance requirements. Business-sensitive content such as financials, strategic plans, and product roadmaps follow at 40%, with user credentials at 36%, often enabling damaging identity-driven attacks.

Intellectual property stands out as a lower-frequency but higher-impact risk. While only 29% reported IP exposure, that likely reflects the fact that not every organization has it. For manufacturers, tech companies, and biotech firms - where IP defines competitive advantage - losses can be catastrophic. Imagine a design engineer unknowingly pasting a product schematic into a public GenAI tool. That one action could expose years of R&D and collapse a competitive advantage overnight.

Crucially, this data usually isn't accessed illicitly - it's being used to get work done. Financial analysts reviewing forecasts, sales teams working customer records, engineers collaborating on designs. For software developers creating new applications, sensitive data is part of daily workflows. Exposure doesn't require malicious intent. It can stem from a misrouted file, unsanctioned sync, or data-rich AI prompt.

The diversity of exposed data - especially unstructured files such as plans, presentations, and data exports - reinforces a core challenge: static classification and content-based controls can't keep up. Without context into who's using sensitive data, for what purpose, and whether behavior signals risk, insider exposure remains both common and undetected.

What type of sensitive data was involved in the most significant incident?



Insider Risk at Scale

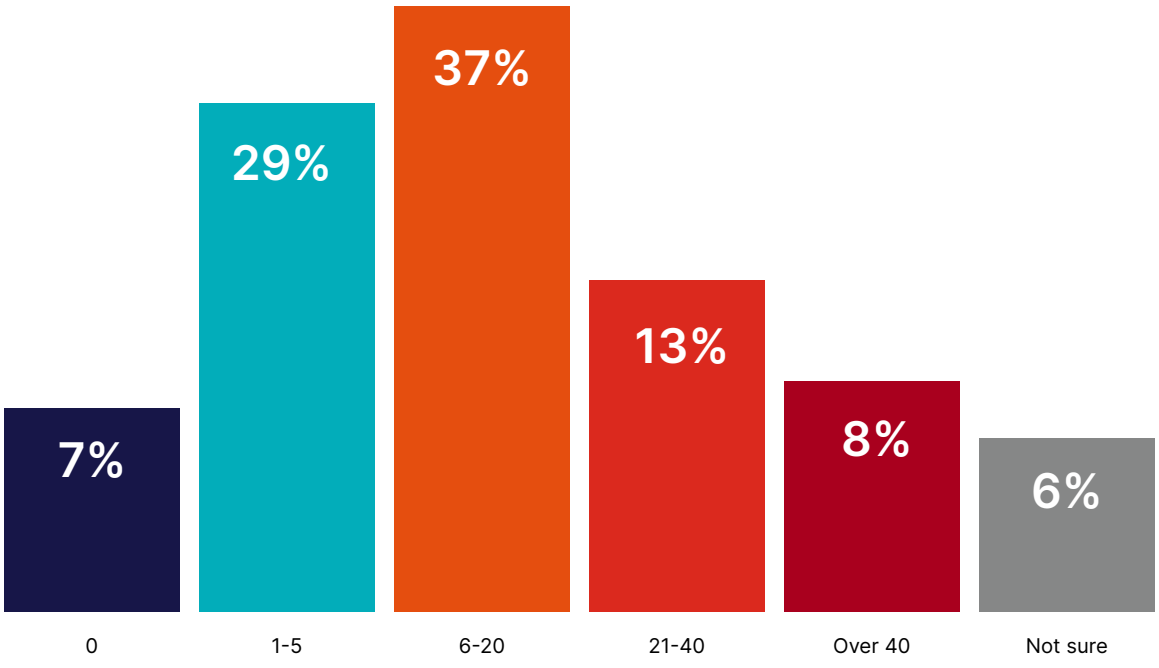
Understanding the types of data at risk is only part of the picture. Equally important is how often those exposures occur, and how rarely they are intercepted. Seventy-seven percent of organizations in our survey experienced at least one insider-related data loss incident in the past 18 months. For many, it wasn't an isolated event: 37% reported between 6 and 20 incidents, and 21% faced more than 20.

Most incidents weren't driven by malice. Nearly half (49%) resulted from accidental or negligent behavior, while another 12% couldn't be attributed at all - underscoring the challenges of detection and attribution.

These patterns reveal a deeper issue that repeated signals often go unnoticed. An employee transferring files late at night or pasting sensitive content into an AI tool may set off alerts - but without behavioral context, those warnings blend into the noise.

High frequency without prioritization leads to alert fatigue, investigation backlogs, and systemic blind spots. The real risk isn't only how often incidents happen - it's how often they pass unnoticed until damage is done.

On average, how many insider incidents (negligent, compromised, or malicious) has your organization detected in the past 18 months?



Consequences That Hit the Business

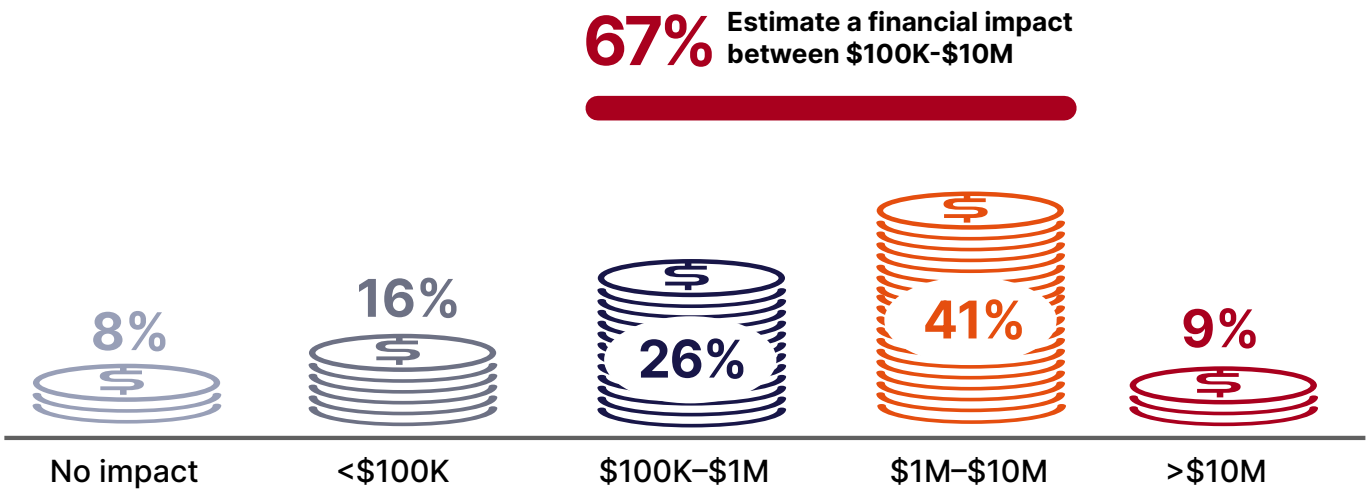
Insider incidents aren't just security events - they're business events, with real financial, operational, and reputational fallout.

Forty-five percent of organizations reported revenue or financial loss as the primary consequence of their most significant insider incident. Reputational damage followed closely at 43%, with operational disruption (39%), regulatory exposure (36%), and IP theft (29%) rounding out the top risks. Just 11% said the incident had no significant impact, underscoring that for most, insider incidents cause measurable harm.

The damage is significant: Seventy-six percent of organizations reported losses over $100,000 - including 41% with $1M–$10M losses and 9% above $10M - illustrating the far-reaching business impact of a single insider action.

These findings reinforce a central theme: insider risk is not an abstract security problem - it is a high-stakes business risk that demands the same level of executive attention as external cyber threats.

Can you estimate the financial impact of that incident?



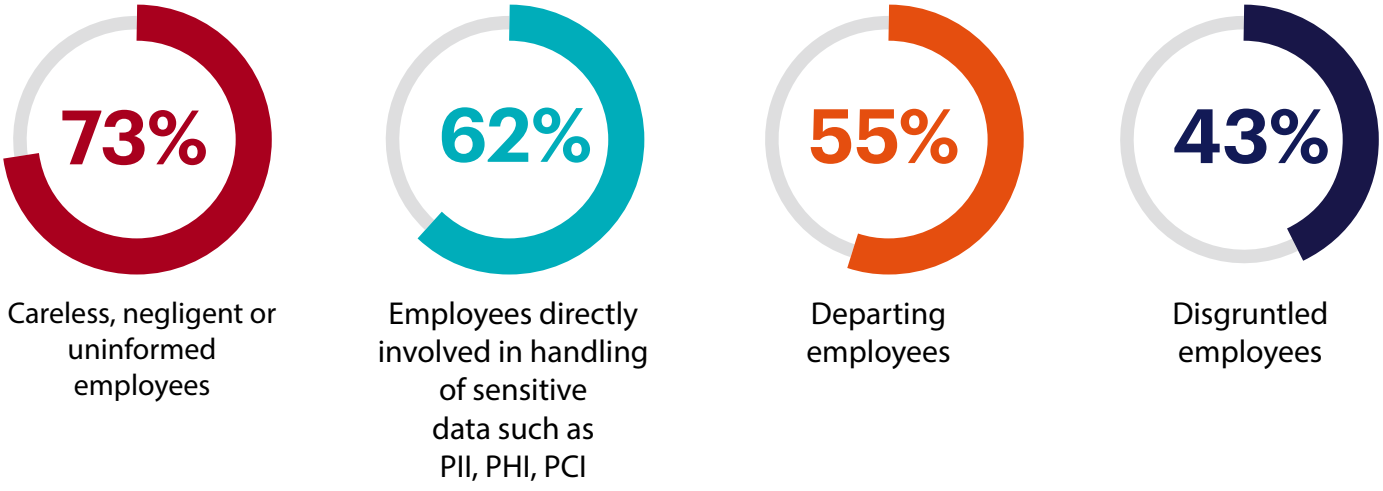
Who's Driving Insider Risk?

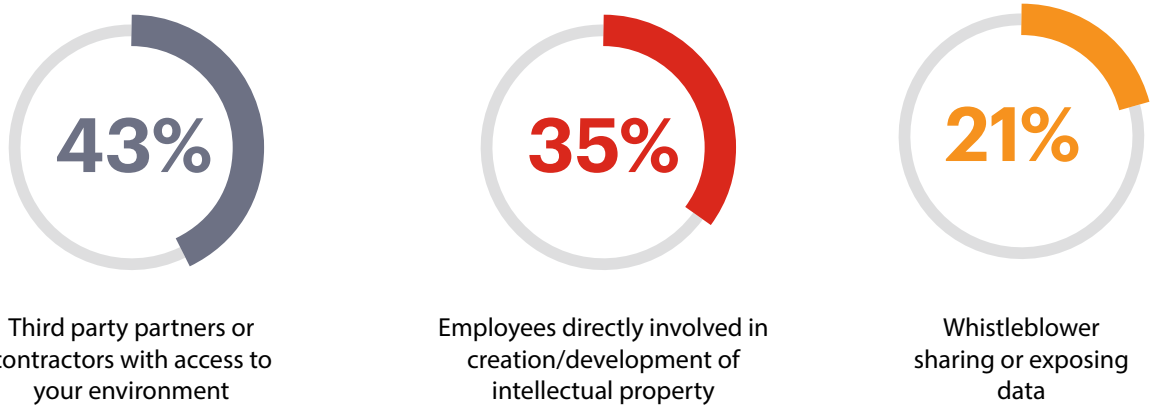
Improving insider risk maturity isn't just about deploying technology - it also requires clarity on who poses the most risk, and why.

The top concern isn't malicious insiders, but employees making unintentional mistakes. Seventy-three percent of respondents cited careless, negligent, or uninformed users as their primary source of risk. That's followed by employees who routinely handle sensitive data like PII, PHI, or PCI (62%), departing employees (55%), and disgruntled insiders (43%). Another 43% are concerned about third-party contractors with internal access, highlighting that not all insider threats originate from employees.

These profiles reflect a broader reality: insider risk isn't defined by access alone, but by how that access is used - and how intent and behavior change over time. That's why detection can't rely solely on static roles or rule sets. Instead, effective programs monitor for changes in behavior and context that indicate risk before a policy violation occurs.

Which users are your organization most concerned about when it comes to insider risk?





Modern Egress Risks Are Hiding in Plain Sight

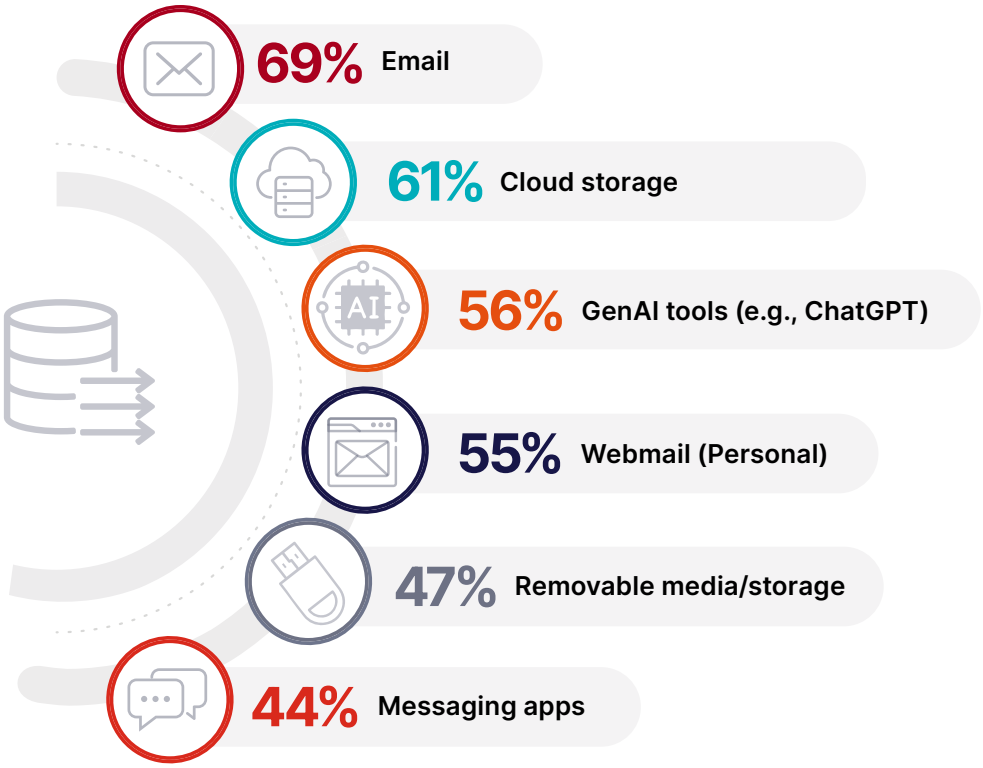
Once insider risk is understood as a visibility and behavior-driven challenge, the next question is: Through what channels is that risk most likely to materialize?

The answer lies in the tools employees rely on every day. Sixty-nine percent of organizations are very concerned about email as a primary egress channel - still the most common vector for unintentional data leaks. 61% worry about personal cloud storage, 56% about GenAI tools like ChatGPT, 55% about personal webmail, and 47% about removable storage devices like USB drives. These are mainstream workflows, not fringe exceptions - and they often operate outside traditional control points.

Tools like GenAI platforms are particularly difficult to monitor. When a developer pastes proprietary code into a public prompt to solve a technical issue, there's no file movement, no policy violation, and no alert. Yet the organization's IP has just left the building. Without context-aware visibility, this kind of behavioral exfiltration remains invisible.

The challenge is clear: static policies and content inspection can't keep up with fluid, user-driven workflows. Securing modern egress channels demands dynamic monitoring of user-data interactions; not just reliance on perimeter defenses.

What egress channels for the outflow of sensitive data does your organization worry most about?



Screen captures 31% | Video conferencing apps 29% | Printers 20% | Wireless 19% | Command Line Interface (CLI) 17%

Up Ahead - Where Security and Insider Risk Pros See Challenges

Once organizations acknowledge they can't see how users interact with sensitive data, the next concern becomes clear: which risks are most likely to evade detection?

Credential compromise sits at the top of the list, with 61% of security leaders saying they are very concerned about insiders using stolen or misused credentials. Accidental employee data leaks followed closely at 59%, further reinforcing the reality that most insider risk originates from routine behavior, not malicious sabotage.

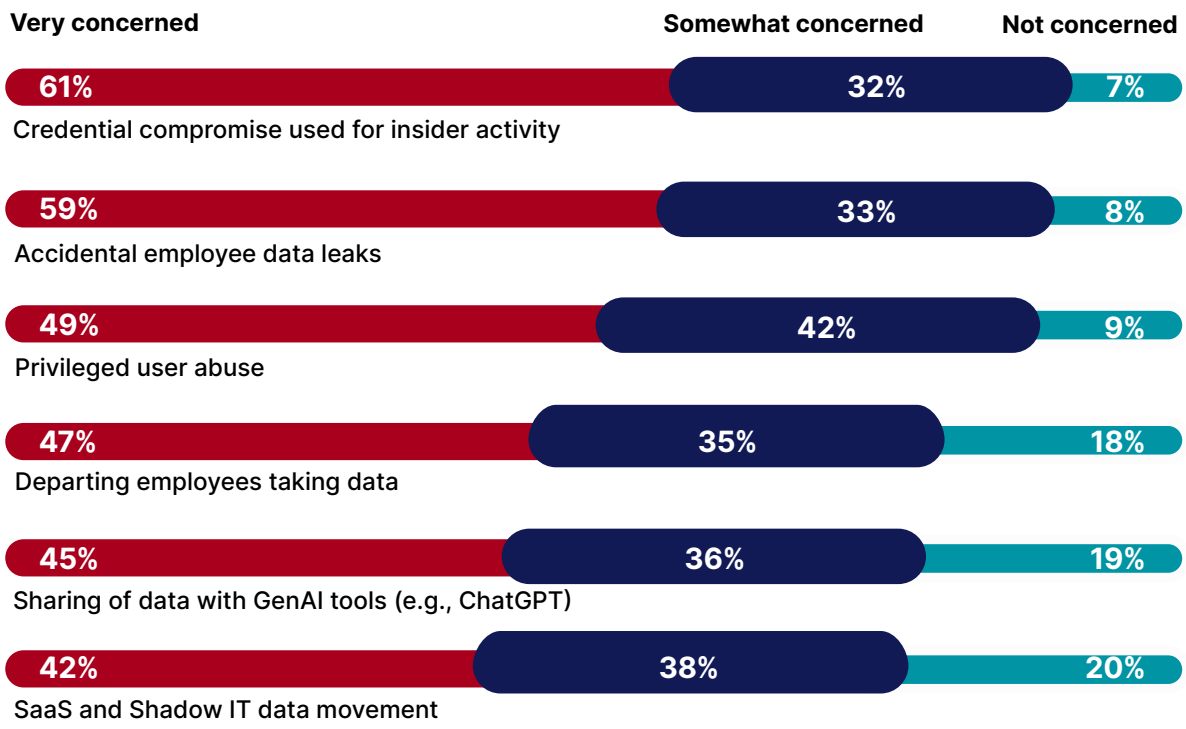
But intentional abuse is still a factor. Nearly half (49%) are very concerned about privileged users misusing their access, while 47% cited departing employees taking sensitive data on the way out.

Concerns about GenAI and SaaS data exposure also rank high: 45% of respondents are very concerned about sensitive data being shared with generative AI tools like ChatGPT, and 42% worry about data movement through unsanctioned or unmanaged SaaS platforms.

The mix of concerns - spanning negligence, compromised accounts, and deliberate abuse - highlights why insider risk programs must detect patterns across all user categories, not just focus on known 'high-risk' roles.

Effective mitigation demands real-time insight into user behavior, access patterns, and the actual tools in use - not just the sanctioned ones.

How concerned are you about the following insider risks over the next 12 months?



Emerging AI Risks Outpace Control

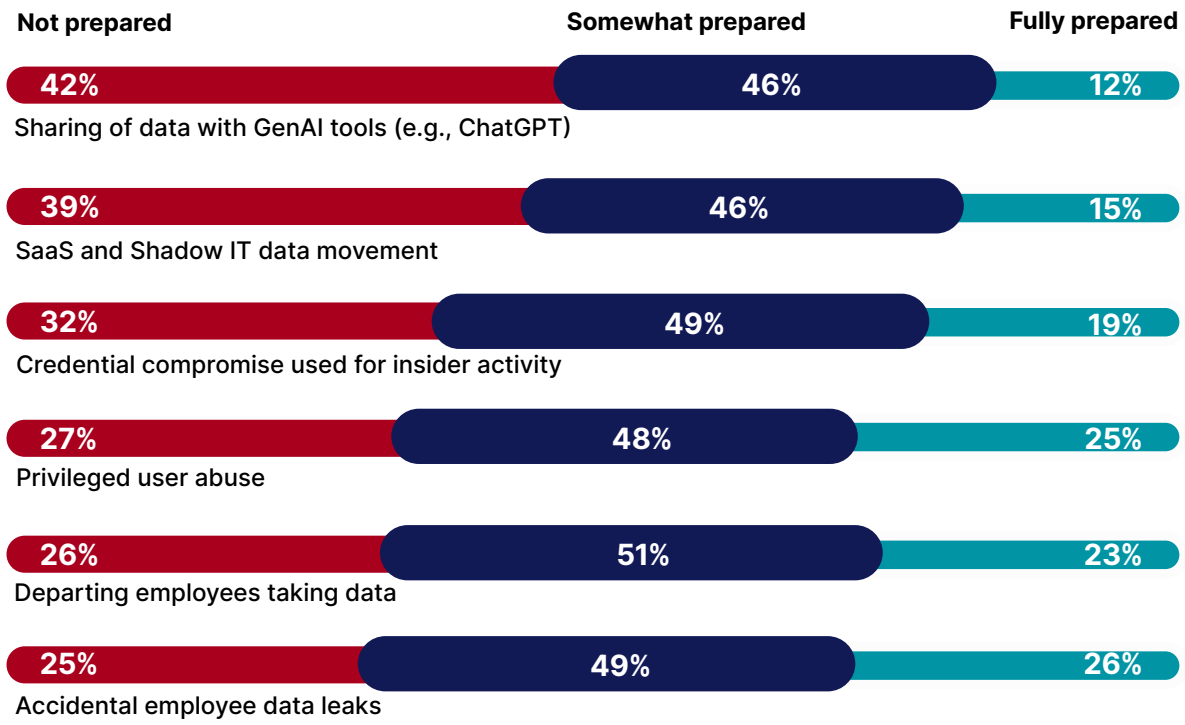
Organizations clearly understand where insider risk is likely to emerge—but most admit they aren't ready to detect or respond when it does.

This gap is most pronounced for modern risks to sensitive data. While concern around GenAI data exposure is high (42% are very concerned), only 12% feel fully prepared to detect or respond to it. Similarly, only 15% feel fully prepared to handle the movement of sensitive data through SaaS and Shadow IT tools, despite these channels being widely used and difficult to monitor.

Even for more established threats, readiness is limited. Fewer than one in four respondents feel fully prepared to address credential compromise (19%), departing employee data theft (23%), or privileged user abuse (25%). For accidental data leaks - the most common insider risk - only 26% say they're ready to respond effectively.

These preparedness gaps illustrate why even mature tools underperform without context on what's normal for a given user and early detection of deviations from that baseline.

How prepared is your organization to detect and respond to those same insider risks?



The Convergence of DLP and Insider Risk Management

Traditional DLP failed to evolve - and insider risk filled the gap. In response, next-generation platforms have emerged that unify data loss prevention with insider risk management. These solutions aren't point fixes - they represent a shift in architecture in direct response to the shortcomings of legacy DLP solutions.

Built for modern work, they combine traditional data loss prevention capabilities, real-time behavioral analytics, visibility into sanctioned and unsanctioned SaaS and AI tools, and dynamic enforcement across endpoints, cloud, and users. What used to be separate domains - data protection and user risk - are now converging into a single, behavior-first control plane.

In fact, 32% of security and insider risk pros are already adopting these solutions as a way to advance their programs' maturity, consolidate tools, enable preemptive and early intervention into potential risks, and gain time and cost advantages associated with investigation and response.

What Security Leaders Expect from Next-Gen DLP

Traditional DLP focused on file movement. Modern integrated data loss prevention and insider risk management solutions focus on user behavior, intent, and context.

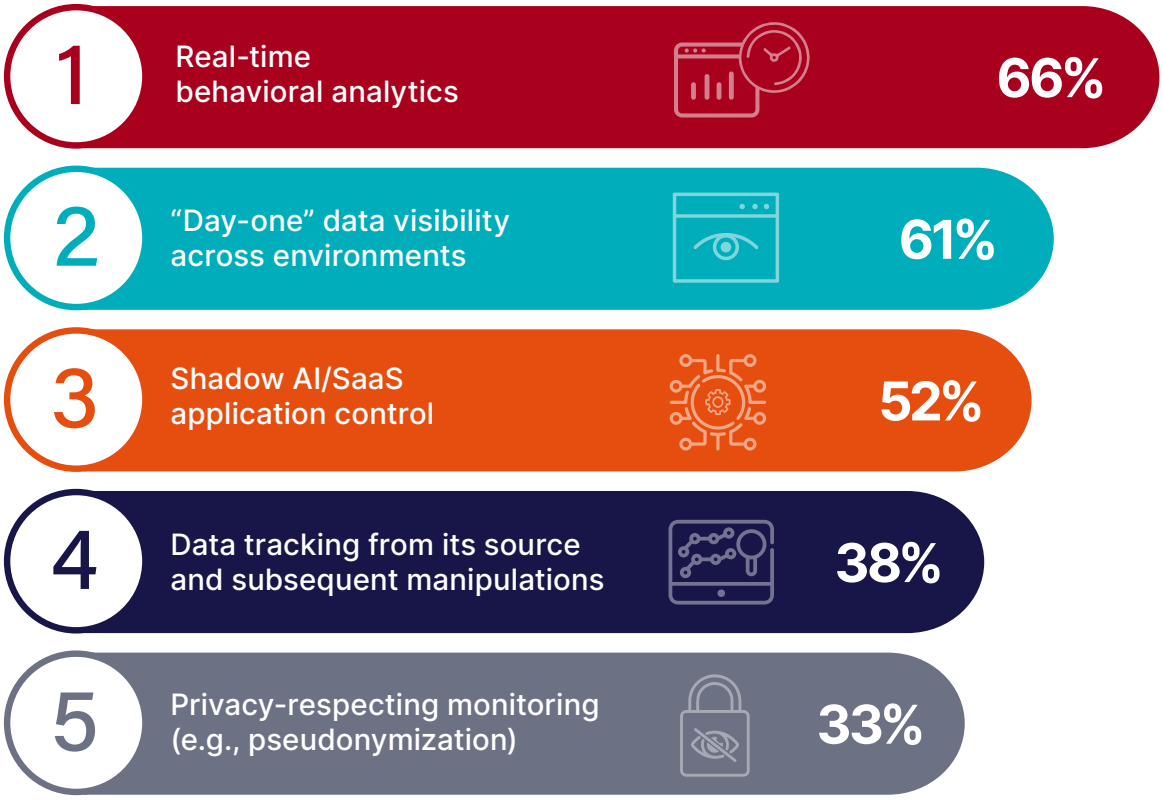
Traditional DLP Solutions	vs.	Next-Gen DLP Solutions
Business Use Case(s): DLP Only		**Business Use Case(s):** DLP + IRM
Data Protection: Sensitive		**Data Protection:** Sensitive + IP
Deployment: On-prem or cloud-based		**Deployment:** Cloud-native + Multi-tenant
Time-to-Value: Weeks to Months		**Time-to-Value:** Days
Visibility: Policies Required for Visibility		**Visibility:** Policy-less, Immediate Visibility
Insights into SaaS and GenAI: Limited		**Insights into SaaS and GenAI:** Yes
Inspection: Content		**Inspection:** Content, Data Origin, Context
Behavioral Analytics: None		**Behavioral Analytics:** Integrated
Incident Fidelity: Single Alert		**Incident Fidelity:** Sequenced Alerts with Data Lineage
Forensics: Files		**Forensics:** Clipboards, Files, Screenshots
Case Management: None		**Case Management:** Integrated with AI Assistant

When asked what they prioritize most in a next-gen platform, security leaders made their expectations clear.

Real-time behavioral analytics topped the priority list, with 66% of respondents saying their next-generation solution must be able to interpret user intent, detect deviations, and intervene before damage is done. Right behind it, 61% want immediate, day-one visibility across all environments: no more rollout blind spots or delayed insight. And 52% emphasized the need to control shadow AI and SaaS usage, reflecting the growing urgency to detect and govern sensitive data exposure across tools like ChatGPT, Dropbox, and unsanctioned cloud platforms.

Security teams want platforms that reveal how users behave, not just what files move. They expect tools to work on day one, not week eight. And they need visibility into browser-based workflows, AI prompts, and decentralized file flows that occur within tools such as ChatGPT, Notion, Dropbox, and personal cloud storage. The expectation is unified context, accelerated response, and actionable insights from the outset.

What would you prioritize in a next-generation DLP or insider risk solution?



5 Essential Best Practices for Managing Insider Risk

To effectively contain insider threats, organizations must move beyond static enforcement and embrace a behavior-aware, context-driven approach.

Most insider incidents stem not from malice, but from negligence, compromise, or a lack of visibility into how users interact with sensitive data. As information flows freely across SaaS apps, GenAI tools, and unmanaged endpoints, legacy DLP tools designed for data in motion are no longer enough.

These best practices distill the core lessons from the findings in this report, translating survey data into actionable steps that can improve readiness and resilience.

1 **See Risk From Day One**
Seventy-two percent of organizations lack visibility into how users interact with sensitive data across endpoints and cloud applications. Delayed visibility leads to missed signals. Programs must prioritize immediate, real-time telemetry across users, devices, cloud, SaaS, and GenAI tools - starting at deployment, not months later.

2 **Monitor Behavior, Not Just Movement**
While 47% of organizations say their DLP prevents data loss, only 27% can identify which users are putting data at risk. Traditional enforcement catches outcomes, not intent. Behavioral analytics helps teams detect deviations, including off-hours access, repeated low-risk actions, or sensitive data flowing into unmonitored channels - before policy is breached.

3 **Extend Controls to Where Work Actually Happens**
Top egress concerns now include email (69%), personal cloud storage (61%), and GenAI tools like ChatGPT (56%). These are everyday workflows and programs that must cover browser-based activity, unsanctioned SaaS use, and AI interactions that sit entirely outside traditional perimeter or agent-based controls.

4 **Align People, Process, and Technology**
Only 18% of organizations have reached full maturity, and just 12% have a dedicated insider risk team. Meanwhile, ownership is spread across security, IT, risk, and legal. Effective programs require cross-functional governance, shared visibility, and response workflows that reflect the multidisciplinary nature of insider risk.

5 **Shift from Enforcement to Adaptation**
Tool complexity and fatigue is real: 49% cite complexity as a top barrier, and 42% say implementation is difficult. Static rules alone can't keep up. Security teams need adaptive enforcement that adjusts based on behavior, access context, and risk severity - reducing false positives and improving containment.

Collectively, these practices form the foundation for a program that can see risk forming, understand its context, and respond before damage is done.

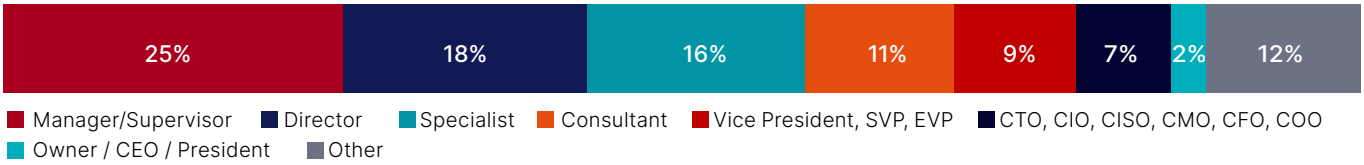
Demographics & Methodology

This report is based on a 2025 survey of 883 IT and cybersecurity professionals, conducted by Cybersecurity Insiders in partnership with Fortinet. Respondents represented a broad cross-section of industries, company sizes, and roles - including CISOs, security architects, SOC leaders, risk managers, and data protection professionals.

The survey examined the state of insider risk management in modern enterprises, with a focus on incident frequency, data types at risk, organizational ownership, maturity levels, and priorities for next-generation solutions. It also explored how organizations are addressing emerging challenges such as GenAI-driven data exposure, SaaS and shadow IT activity, and the shift toward behavior-aware detection.

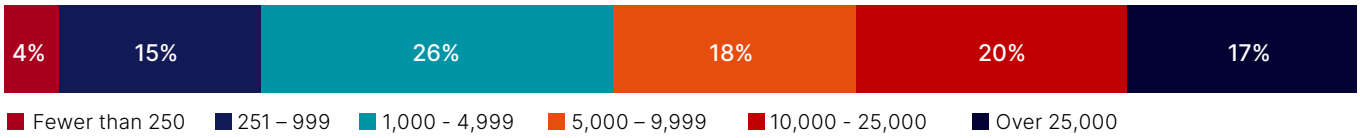
All responses were self-reported and collected via structured multiple-choice questions. With 883 qualified responses, the survey has a margin of error of ±3.3% at a 95% confidence level, providing a statistically meaningful snapshot of current enterprise insider risk practices, challenges, and strategic priorities.

CAREER LEVEL

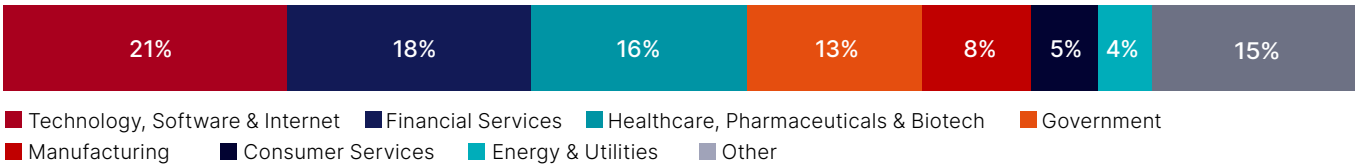


DEPARTMENT

COMPANY SIZE



INDUSTRY



Fortinet (NASDAQ: FTNT) secures the largest enterprises, services providers, and government organizations around the world. Fortinet empowers our customers with complete visibility and control across the expanding attack surface and the power to take on ever-increasing performance requirements today and into the future. Only the Fortinet Security Fabric platform can address the most critical security challenges and protect data across the entire digital infrastructure, whether in networks, applications, multi-cloud, or edge environments. Fortinet ranks #1 as a security company, with more than 800,000 clients who trust their solutions and services to protect their businesses.

www.fortinet.com

Cybersecurity
INSIDERS

STRATEGIC INSIGHT FOR CYBERSECURITY LEADERS

Cybersecurity Insiders delivers evidence-backed insights that empower security leaders to make informed, strategic decisions. Backed by over a decade of research and a global network of 600,000+ cybersecurity professionals, we provide actionable intelligence to help leaders navigate emerging threats, evaluate new technologies, and shape forward-looking strategies with confidence.

For cybersecurity vendors, we turn research into results — delivering credibility, visibility, and demand through high-impact formats such as:

- Data-powered market reports that establish thought leadership,
- Webinars that build trust with buyers through credible, expert-led narratives,
- CISO guides that showcase best practices,
- Product reviews that independently validate solutions,
- Thought leadership articles that educate buyers, and
- Award programs that elevate brand reputation.

By combining this content with built-in distribution, we help brands earn trust, amplify awareness, and drive demand in a crowded cybersecurity market.

For more information, visit

cybersecurity-insiders.com