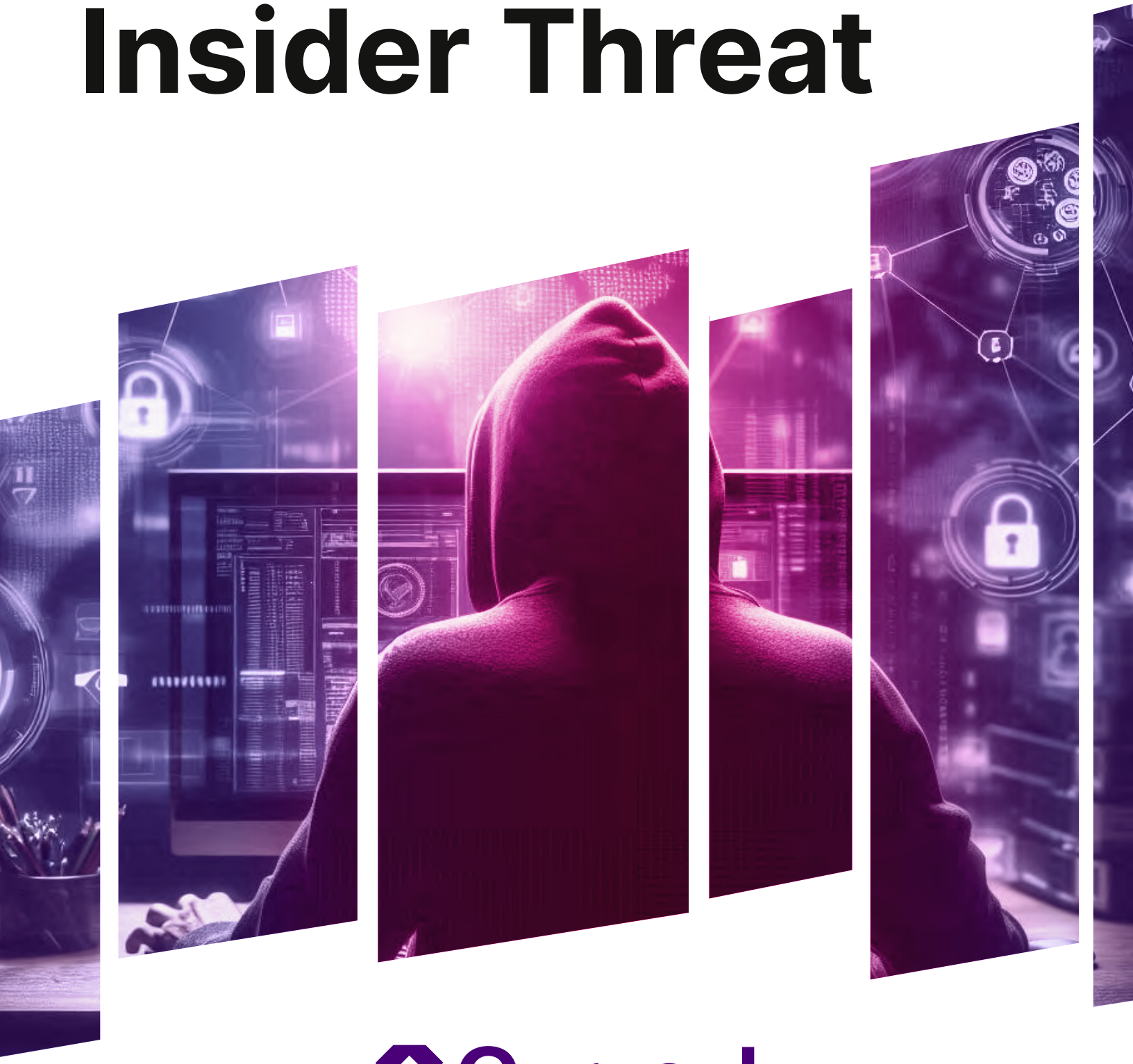
Cybersecurity
INSIDERS

2024 REPORT

Insider Threat



Gurucul

Introduction

The landscape of insider risk management continues to evolve rapidly, driven by increasing complexities in IT environments, the adoption of hybrid work models, and the rise in adoption of sophisticated GenAI tools by knowledge workers. This 2024 Insider Threat Report is based on the insights of 413 IT and cybersecurity professionals to capture the latest trends, challenges, and best practices in managing insider threats, providing a comprehensive overview of how organizations are addressing these critical security challenges today.

KEY FINDINGS INCLUDE:

- **Rising Frequency and Cost of Attacks:** 48% of organizations reported that insider attacks have become more frequent over the past 12 months. Additionally, 51% experienced six or more attacks in the past year, with the average cost of remediation exceeding $1 million for 29% of respondents.
- **Drivers of Insider Attacks:** The top three drivers behind the surge in insider attacks are complex IT environments (39%), adoption of new technologies (37%), and inadequate security measures (33%), highlighting multifaceted areas of concern that organizations must address.
- **Increased Vulnerability Perception:** A substantial 71% of organizations feel at least moderately vulnerable to insider threats, indicating heightened awareness and concern over internal risks.
- **Unified Visibility and Control:** While 93% of respondents consider unified visibility and control across environments to be critically important, only 36% have a fully integrated solution that delivers unified visibility, underscoring the need for more cohesive security strategies.
- **Tools Gap:** While 50% of respondents have a partially integrated solution, 28% of organizations still rely on limited integration, managing visibility through separate, non-integrated tools, 17% have altogether insufficient tooling, and 20% use disparate systems for monitoring users, applications, and devices, revealing a significant tools gap.
- **Obstacles to Implementation:** Technical challenges (39%) and cost factors (31%) remain the primary obstacles to implementing effective insider threat management tools, although organizations are increasingly recognizing the ROI of investing in advanced security solutions.

We extend our gratitude to Gurucul for supporting this important research project. Their commitment to advancing insider threat management solutions has made this comprehensive analysis possible. We hope that the insights provided in this report will guide you to enhance your security posture and better protect your organization from insider risks.

Thank you,

Holger Schulze

Founder, Cybersecurity Insiders

Table of Contents

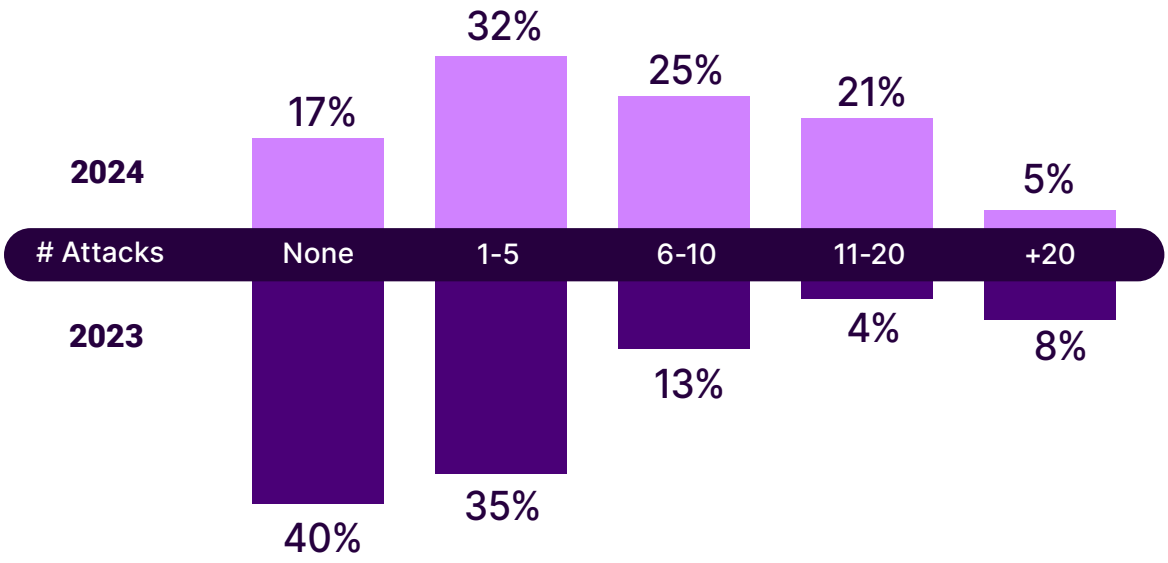
Rising Tide of Insider Attacks

We asked respondents to rate their organization's vulnerability to insider threats, and the results show a notable increase compared to last year's results. The frequency of insider attacks experienced within an organization provides critical insights into gaps in insider risk management.

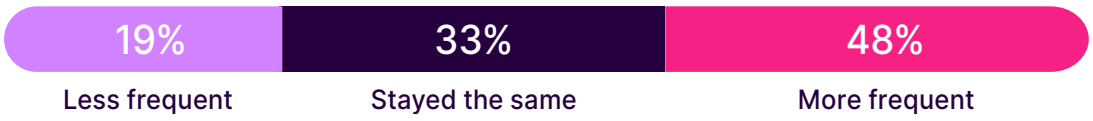
The survey results show a concerning increase in reported incidents from 2023 to 2024. In 2024, only 17% of organizations reported no insider attacks, a significant decrease from 40% in 2023. A significant number of organizations reported a small number of attacks (1-5), remaining relatively stable at 32%, compared to 35% in 2023. However, the number of organizations experiencing 6-10 attacks nearly doubled to 25% from 13%, and those reporting 11-20 attacks saw a dramatic increase to 21% from just 4% in 2023. The percentage of organizations experiencing more than 20 attacks decreased slightly from 8% in 2023 to 5% in 2024.

This dramatic shift suggests an increasing frequency and awareness of insider attacks, echoing other findings in this report where 11% of respondents felt extremely vulnerable to such threats, up from 5%. The rise in reported incidents also indicates that organizations are becoming better at detecting insider attacks that previously might have gone unnoticed. Additionally, 48% of respondents confirmed that overall, insider attacks have become more frequent over the past 12 months, while only 19% observed a decrease.

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



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



To combat this growing threat, organizations should invest in robust insider threat management programs that incorporate advanced detection technologies to identify and mitigate suspicious insider activities early. Continuous monitoring, comprehensive incident response plans, and fostering a culture of security awareness among employees are essential steps in reducing the frequency of insider attacks.

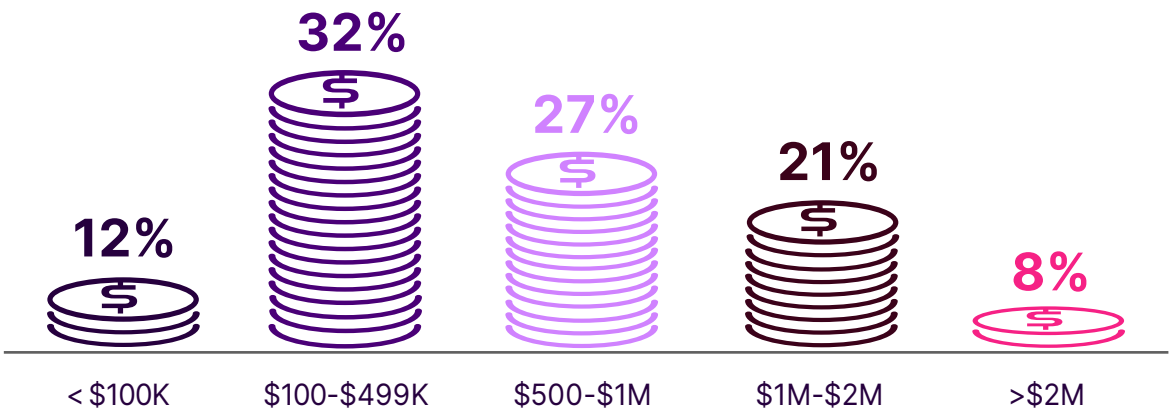
Costly Consequences of Insider Attacks

Evaluating the financial impact of insider attacks is important for understanding the full scope of their repercussions. It also strengthens the case for robust investments in insider risk management and related solutions.

When asked to estimate the average cost of remediation after an insider attack, the most common response, noted by 32% of organizations, was an estimated cost in the range of $100K to $499K.

Following this, 27% of respondents estimated their costs to be between $500K and $1M, while 21% reported costs ranging from $1M to $2M. Additionally, 12% indicated remediation costs of less than $100K, and 8% even estimate costs exceeding $2M.

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



These findings underscore the substantial financial impact of insider attacks, with many organizations incurring costs in the hundreds of thousands to millions of dollars. Considering that 51% of organizations experienced six or more attacks in the last 12 months, the financial damage can be severe. For example, with 10 attacks costing $1 million each, the total could easily exceed $10 million. This aligns with broader industry trends, where the average cost of insider threats continues to rise due to the growing sophistication of these attacks.

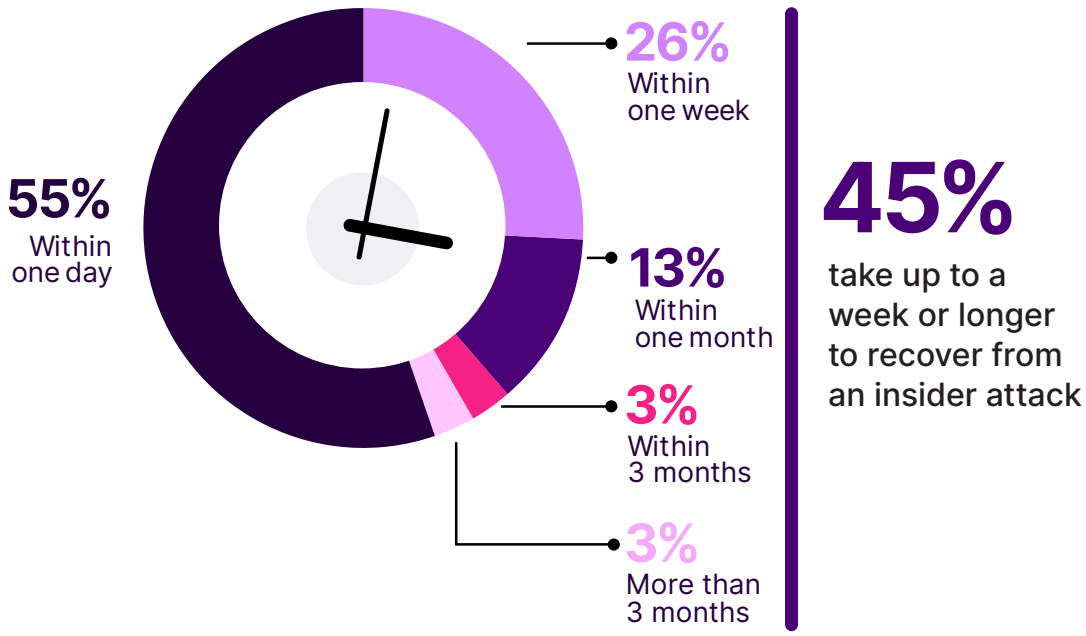
Slow Recovery from Insider Attacks

The faster an organization can recover from an insider attack, the less operational disruption and financial loss it will face.

The survey reveals that while 55% of organizations report recovering from an insider attack within a day, a significant 45% face recovery times extending up to a week or longer. This highlights a concerning trend—many organizations may be underprepared for the complexities of insider attacks, often underestimating the resources and time required for full recovery.

To address this gap, it's essential for organizations to leverage advanced incident response solutions that go beyond basic automation. These solutions integrate dynamic risk-based prioritization, machine learning, and comprehensive contextual analysis to ensure that security teams can focus on the most critical threats, thereby reducing recovery times.

How long would it typically take your organization to RECOVER from an insider attack?



By automating incident response workflows and integrating with existing security tools, these advanced platforms—like Security Orchestration, Automation and Response (SOAR)—enable organizations to swiftly isolate and remediate threats. This approach significantly reduces the time needed to recover from insider attacks and helps maintain operational continuity, even in complex threat scenarios. By addressing these gaps and adopting more realistic recovery expectations, organizations can better prepare for and respond to the complexities of insider threats, ultimately strengthening their overall security posture.

Drivers Behind Insider Attack Surge

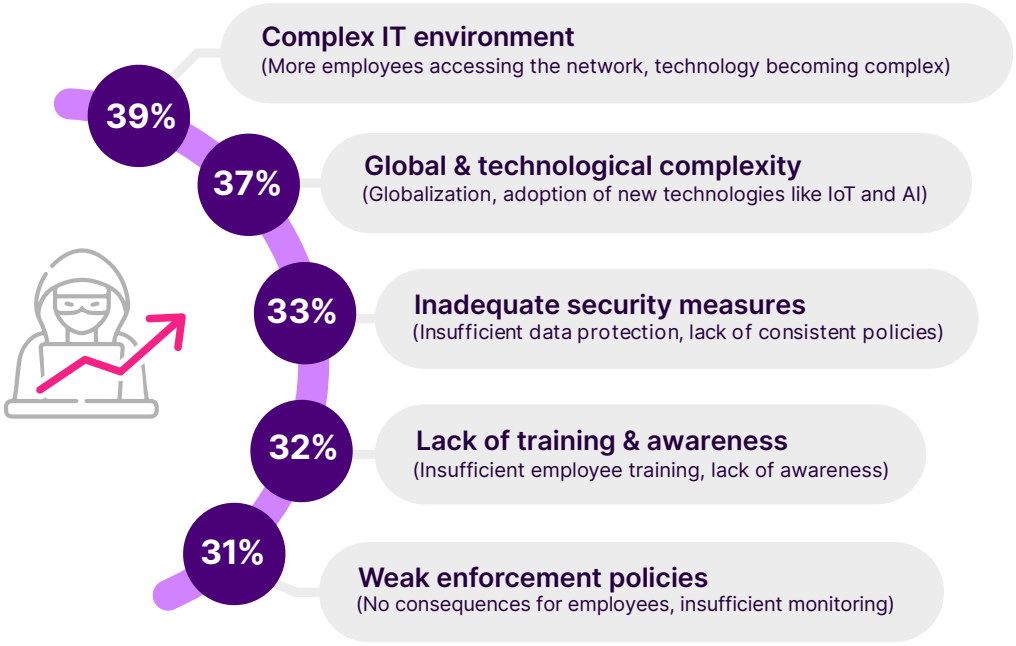
Understanding the key drivers behind the observed rise in insider attacks is essential for developing effective mitigation strategies.

The most cited reason for the increase in attacks, noted by 39% of respondents, is the increasingly complex IT environment. This includes the growing number of employees accessing the network from home and the increasing integration of cloud services and SaaS applications, adding layers of complexity and rapidly expanding the attack surface.

Close behind, 37% point to technological complexity, such as the adoption of new technologies like IoT and AI, that simultaneously increase vulnerabilities and enable new attack vectors. Inadequate security measures were noted by 33% of respondents, indicating that insufficient data protection and inconsistent policies are significant enablers of insider threats.

Additionally, 32% of respondents attribute the rise in insider incidents to a lack of training and awareness among employees, highlighting the importance of proper education and awareness programs to reduce the risk of inadvertent insider threats. Weak enforcement policies, including a lack of consequences for employees and insufficient monitoring, were identified by 31% as contributing factors.

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



These findings suggest that a multifaceted approach is necessary to address the increase in insider risk and attacks. Organizations should simplify and better secure their IT environments, ensuring that access is strictly controlled and monitored. Organizations should also leverage advanced analytics and continuous monitoring to detect and respond to suspicious activities. Embracing a Zero Trust model and gaining visibility into entitlement sprawl using identity as an indicator of compromise (IoC) can help reduce over-privileged accounts and ensure that all users and devices are continuously authenticated and authorized before granting access, further enhancing security.

Challenges in Detecting and Preventing Insider Attacks

The difficulty of detecting and preventing insider attacks compared to external cyber attacks reveals critical insights into the complexities of managing internal threats.

According to the survey, 37% of respondents find detecting and preventing insider attacks more difficult than dealing with external cyber attacks. This reveals a notable improvement from 2023 when 48% of organizations found insider attacks more difficult to detect than external ones. A majority, 55%, believe the difficulty level is about the same (compared to 44% in 2023), while only 8% consider insider attacks easier to manage than external ones.

This data underscores the inherent complexities in identifying and mitigating insider threats. Unlike external attacks, which often come from identifiable sources and follow recognizable patterns, insider attacks originate from trusted individuals within the organization, making them more challenging to detect. Insiders have legitimate access to systems and data, allowing them to bypass many traditional security measures undetected.

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

92%
find insider attacks equally or more challenging to detect than external cyber attacks

More difficult than detecting and preventing external cyber attacks

About as difficult as detecting and preventing external cyber attacks

Less difficult than detecting and preventing external cyber attacks

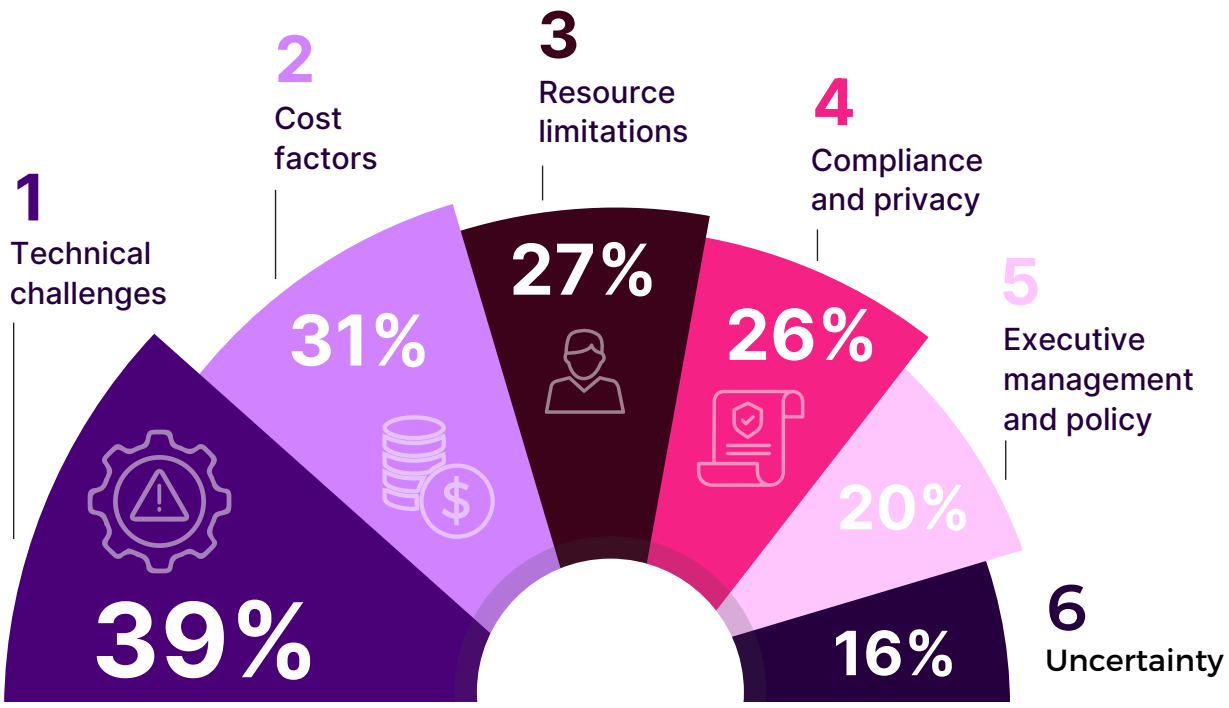
Organizations must enhance their insider threat detection and prevention strategies to address these challenges. Implement advanced monitoring solutions, such as User and Entity Behavior Analytics (UEBA), to identify anomalous activities that may indicate insider threats. Security Orchestration, Automation and Response (SOAR) platforms can further automate insider incident response and prioritize high-risk threats. Additionally, fostering a culture of security awareness among employees and conducting regular training can help mitigate the risk of insider attacks by making all staff vigilant against potential threats.

Obstacles to Effective Insider Threat Management

Implementing effective insider threat management tools and strategies is fraught with challenges.

Technical challenges are the leading obstacle to effective insider threat management, cited by 39% of respondents. These include the complexity of data classification processes, the negative impact of tools on user productivity, challenges in deploying to remote or personal devices, and concerns about vendor lock-in or compatibility. Organizations can address these issues by investing in user-friendly, interoperable security tools that minimize disruption to productivity and that are compatible with a wide range of devices. Choosing flexible, scalable solutions that integrate seamlessly with existing systems can alleviate compatibility concerns and ease deployment complexities.

What are the primary obstacles preventing you from implementing effective insider threat management tools and strategies?



Additional responses include: We are currently in the process of implementing such tools 14% | Not sure/other 21%

Cost factors are the second most significant barrier, mentioned by 31% of respondents. While costs of tools like User and Entity Behavior Analytics (UEBA), eXtended Detection and Response (XDR), Security Information and Event Management (SIEM), and Security Orchestration, Automation and Response (SOAR) can be prohibitive for some organizations, it's crucial to view these investments as essential for robust security posture. Unified insider risk management platforms not only provide significant ROI by consolidating these disparate tools but also optimize the data for cost savings and enhance operational efficiency through automation and advanced analytics. Organizations might also consider phased implementations or pilot programs to manage initial expenses while demonstrating value early on.

Resource limitations, noted by 27% of respondents, include insufficient staff to implement and maintain tools and a lack of expertise or specialized skills required to operate them. Investing in ongoing training and development for cybersecurity teams to build the necessary expertise is crucial to address this challenge. To help reduce the burden on staff we recommend seeking out tools that are more intuitive to use and that reduce alert triage and false positives by providing a complete case of evidence with context and advanced behavior analytics. Collectively this can streamline investigations, expedite response, and improve operational efficiency. Additionally, managed security services can supplement internal capabilities, ensuring that tools are effectively implemented and maintained without overburdening existing staff.

Compliance and privacy concerns, reported by 26% of respondents, also pose significant hurdles. Regulatory requirements and concerns about infringing on employee privacy complicate the implementation of comprehensive monitoring systems. This challenge is particularly acute in regions with stringent data protection laws, where balancing security and privacy becomes a delicate task. Adopting privacy-by-design principles ensures that compliance and privacy are embedded in security practices from the outset. Staying informed about regulatory changes and working with legal and human resource experts can help navigate these challenges more effectively. Transparent communication with employees about the importance and benefits of monitoring can further alleviate privacy concerns.

Executive management and policy issues are cited by 20% of respondents, indicating that a lack of prioritization by management and ineffective internal policies are significant obstacles. This highlights the need for stronger executive support and more effective policy frameworks to ensure that insider threat management is given the attention it deserves. Securing stronger executive support by clearly communicating the risks and potential impacts of insider threats on the organization can help address this. Developing and enforcing effective internal policies that emphasize the importance of insider threat management ensures it receives the necessary attention.

By tackling these obstacles head-on, organizations can better position themselves to implement effective insider threat management strategies and protect their sensitive information and systems.

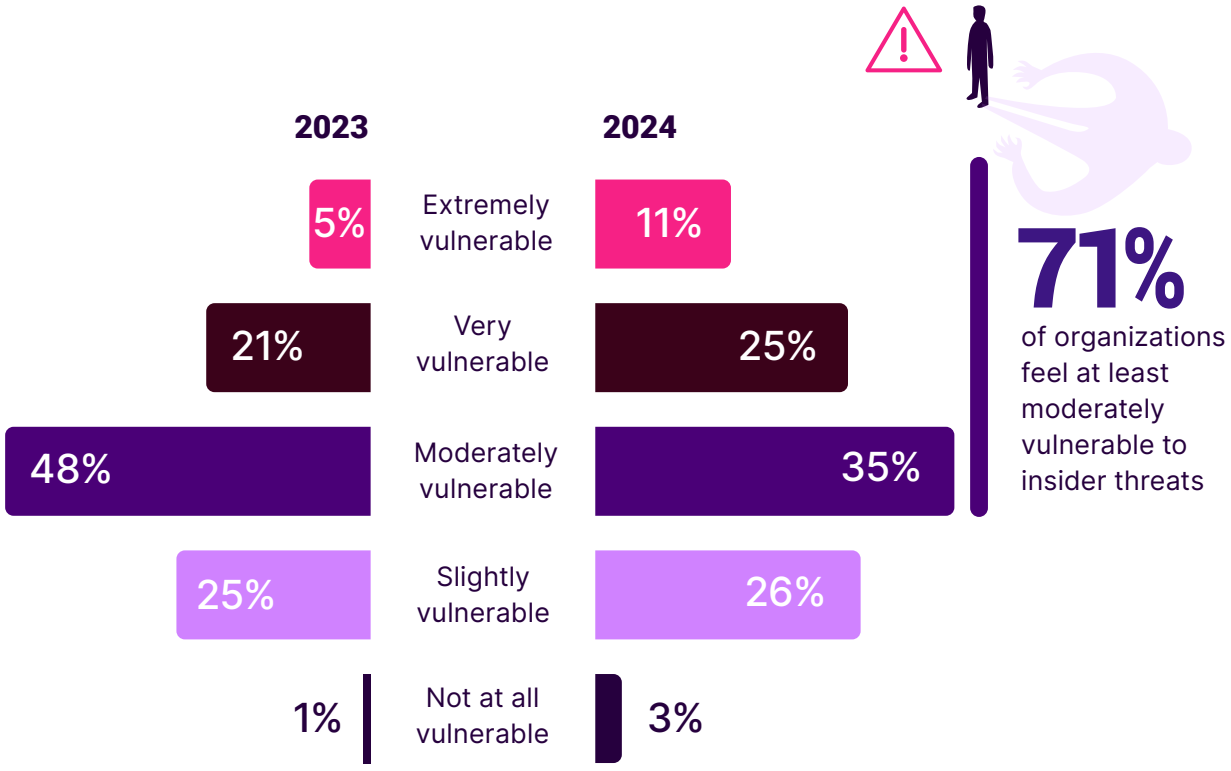
Vulnerability to Insider Threats

Understanding organizational vulnerability to insider threats is crucial, as it highlights potential weaknesses that could be exploited by insiders and informs strategies to close gaps in insider risk management.

We asked respondents to rate their organization's vulnerability to insider threats, and the results show a notable shift in perceptions to being more vulnerable. The most noticeable shift in 2024 was that 11% of respondents felt their organizations were extremely vulnerable, a significant increase from 5% in 2023. Similarly, those who felt very vulnerable rose to 25% from 21%. As a result, the moderately vulnerable category shifted from 48% in 2023 to 35% in 2024. Slightly vulnerable responses saw a slight increase, moving from 25% to 26%, while those who felt not at all vulnerable increased only marginally from 1% to 3%.

This data indicates a growing awareness and concern about insider threats among organizations, with a marked shift from moderate to higher levels of perceived vulnerability. The increase suggests that organizations are becoming more cognizant of the potential damage insider attacks can cause— a change in perception that is likely due to high-profile incidents and improving internal threat detection capabilities.

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



Organizations should prioritize enhancing their insider threat detection and response strategies to address these growing concerns. Implementing comprehensive security programs that include continuous monitoring, advanced analytics, and employee training can help mitigate these risks. Leveraging cutting-edge cloud security solutions and adopting Zero Trust architectures can also fortify defenses against insider threats, ensuring a more robust security posture.

Effectiveness in Managing Insider Threats

Assessing the effectiveness of organizations in managing insider threats reveals a complex landscape.

According to the survey, a majority (63%) believe their organization is extremely effective (24%) or very effective (39%). Another 32% describe their efforts as somewhat effective. A smaller portion (5%) rates their effectiveness as not very effective (4%) or not at all effective (1%).

These findings present a surprising contrast to earlier survey results, where a significant portion of respondents felt increasingly vulnerable to insider threats. This dichotomy suggests that despite perceiving improvements in their ability to monitor, detect, and respond to insider threats, organizations still feel a heightened sense of vulnerability.

This apparent contradiction can perhaps be explained by the evolving and sophisticated nature of insider threats, which continually challenge even the most robust security measures. The rise in insider attacks and the complexity of hybrid work environments further contribute to this persistent sense of vulnerability.

To reconcile these findings, organizations should continue to enhance their security frameworks by integrating advanced monitoring tools, conducting regular training, and continuously updating incident response plans. Ensuring unified visibility and control across all environments, both on-premises and in the cloud, is crucial for maintaining a strong defense against insider threats.

Confidence vs. Reality: Tool Gaps in Insider Threat Protection

Evaluating whether organizations feel equipped with the right tools to protect sensitive information and systems from insider threats reveals significant gaps in capabilities.

According to the survey, a majority (52%) reveal they do not have the tools to confidently handle insider threats today. 28% acknowledge having some tools but recognize shortcomings that need to be addressed. Additionally, 6% report a lack of critical tools necessary for effective monitoring and protection, and 18% are uncertain about the tools they have or their effectiveness.

On the flipside, 48% of respondents believe they have all the necessary tools and are fully confident in their ability to handle insider threats. This high level of confidence contrasts with earlier findings where many organizations reported feeling increasingly vulnerable to insider threats. This discrepancy suggests that even with robust tools, the dynamic nature of insider threats and evolving attack methods continue to generate concern and perceived vulnerability.

Do you feel you have the right tools for protecting your sensitive information and systems from insider threats?

Organizations reporting gaps or partial toolsets should prioritize identifying and integrating advanced security solutions to cover these deficiencies. Leveraging comprehensive Identity Threat Detection and Response (ITDR) tools and platforms that unify visibility across on-premises and cloud environments can help bridge these gaps.

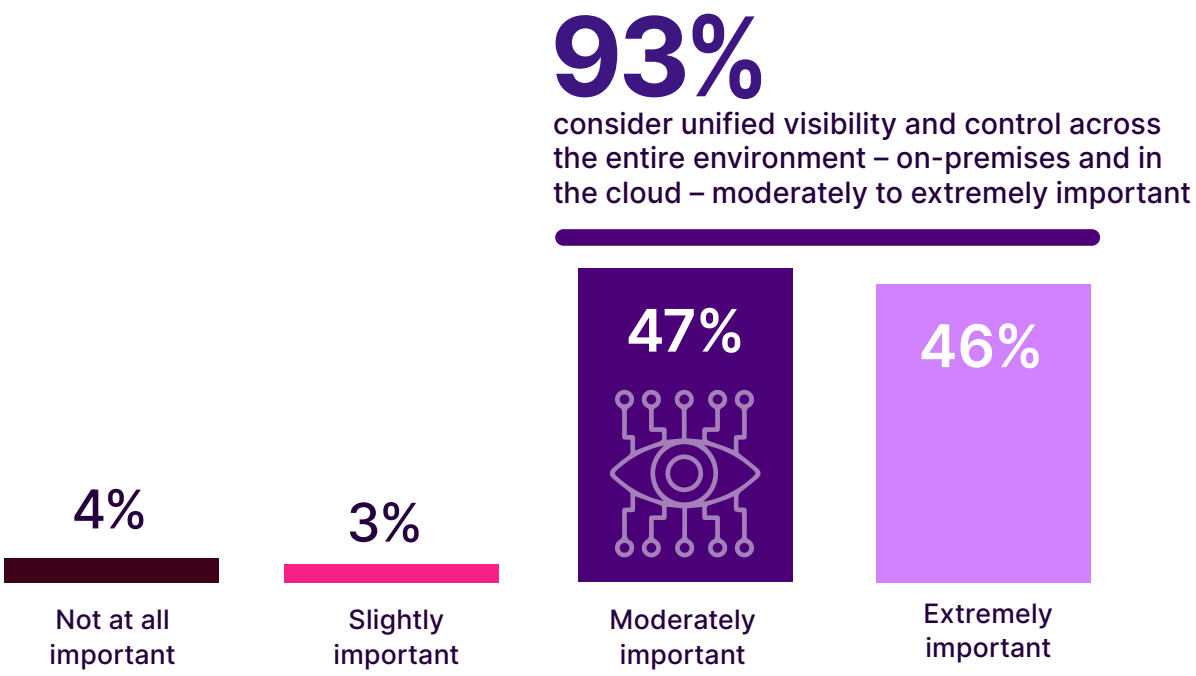
Importance of Unified Visibility and Control

Unified visibility and control across the entire IT environment, both on-premises and in the cloud, is critical for effectively managing insider threats. However, it's not just about visibility—data optimization also plays a key role in ensuring that only the most relevant data is ingested and analyzed, keeping costs down and ensuring that critical threats are identified without overwhelming the system with unnecessary data or false positives.

The complexity of managing security across disparate systems without unified control can lead to gaps and blind spots, increasing the risk of insider threats going undetected. The survey reveals that 93% of respondents recognize the critical role of unified security measures. However, to make these measures truly effective, organizations must prioritize the optimization of data feeds.

By integrating data optimization techniques with unified visibility and control, organizations can enhance security across hybrid environments while reducing operational costs. Advanced platforms filter and enrich data, ensuring that only critical insights are analyzed, which minimizes false positives and improves detection accuracy. This approach allows security teams to focus on real threats without being overwhelmed by irrelevant data, ultimately making the system more efficient and effective in mitigating insider risks.

When it comes to insider threats, how important is unified visibility and control across your entire environment – on-premises and in the cloud?



Organizations should prioritize implementing integrated security solutions that offer unified visibility and control. These solutions should encompass all areas of the environment, including on-premises systems, cloud infrastructure, and hybrid configurations. By doing so, organizations can ensure a more cohesive and effective approach to insider threat management.

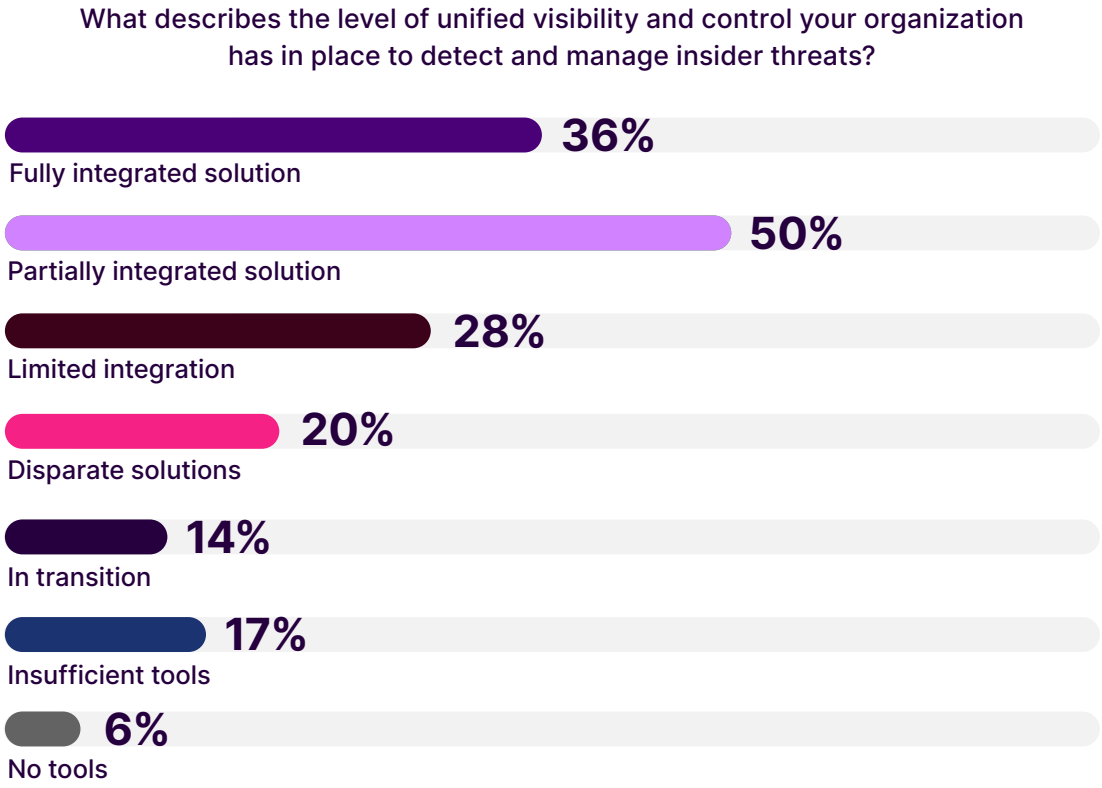
Levels of Unified Visibility and Control in Insider Threat Management

Understanding the level of visibility and control organizations have in place to detect and manage insider threats is crucial for evaluating their preparedness and response capabilities.

Most commonly, 50% of organizations use partially integrated solutions, where multiple products are integrated for visibility and control. Meanwhile, 36% have fully integrated solutions, with a single platform delivering unified visibility and control.

However, 28% still rely on limited integration, managing visibility through separate, non-integrated tools, and 20% use disparate systems for monitoring users, applications, and devices.

Additionally, 14% are in transition, upgrading or integrating tools, while 17% lack sufficient tools for unified visibility and control. Alarmingly, 6% have no tools in place for insider threat management. These findings highlight the need for more robust and cohesive solutions, as fragmented systems increase the risk of missed threats.



To strengthen their defenses, organizations should consolidate their tools into fully integrated solutions that not only provide unified visibility but also leverage advanced technologies like machine learning and behavioral analytics. Such platforms enable real-time data optimization, filtering only critical data for analysis, which reduces noise, improves detection accuracy, and accelerates response times. By making this transition, organizations can better detect, manage, and mitigate insider threats efficiently.

Additional responses include: Not sure 21%

Integrating Non-IT Data Sources in Insider Threat Programs

Incorporating non-IT data sources into insider threat programs can significantly enhance an organization's ability to detect and mitigate internal threats by providing a broader context for behavior analysis.

For example, legal data, such as court records and credit reports, has been successfully incorporated by 55% of qualified respondents. This integration helps organizations identify potential red flags related to financial instability or legal issues that could predispose individuals to malicious activities. Access to such data enables a more comprehensive risk assessment, aligning with best practices for insider threat management which recommend using diverse data sources to build a complete profile of potential threats.

Human Resources (HR) data, including information on leavers, performance data, and background checks, has been integrated by 45% of respondents. HR data is invaluable for insider threat programs, as it provides insights into employee behavior, satisfaction, and history, which are crucial for detecting early warning signs of potential insider threats. Patterns such as sudden drops in performance, disciplinary actions, or imminent departures can indicate heightened risk and help organizations take preemptive measures.

Public data sources, including social media, forums, and the dark web, have been utilized by 43% of respondents. Monitoring public data can provide external context that might influence insider behavior, such as engagement with potentially harmful groups or discussions of sensitive information. This type of data helps in identifying potential insider threats who might be influenced by external actors or are actively seeking ways to exploit organizational vulnerabilities.

Have you been successful in incorporating any of the following non-IT data sources into your insider threat program?

While the integration of these non-IT data sources enhances the effectiveness of insider threat programs, it also presents challenges, such as privacy concerns and the technical complexity of data correlation. Organizations must ensure they are compliant with legal and ethical standards when accessing and utilizing this data. Implementing robust data governance policies and ensuring transparent communication with employees about the use of such data can help mitigate these concerns. Continuous training for security teams on the importance and handling of non-IT data is also essential for maximizing the benefits of these additional data sources.

To further improve the integration of non-IT data sources, organizations can leverage advanced analytics and machine learning technologies that can handle diverse data types and provide actionable insights. By incorporating a wide range of data sources into their insider threat programs, organizations can achieve a more comprehensive understanding of potential threats, enhancing their ability to detect, prevent, and respond to insider risks effectively.

Best Practices for Insider Threat Management

1 | Implement Advanced Monitoring Solutions

Given that 37% of organizations find insider threats more difficult to detect than external attacks, leveraging advanced monitoring tools like User and Entity Behavior Analytics (UEBA) can help identify anomalous activities that may indicate insider threats. Look for solutions that provide comprehensive visibility across on-premises and cloud environments, enabling quicker and more accurate threat detection through integrated analytics and machine learning.

2 | Integrate Non-IT Data Sources

Incorporating non-IT data sources such as legal records, HR data, and public data can provide a more comprehensive view of potential insider threats and provide additional context for detections and investigations. As the survey indicates, 55% of organizations have successfully integrated legal data and 45% use HR data. Solutions that can integrate diverse data sources into a unified analytics platform will enhance the ability to identify and mitigate risks early.

3 | Leverage Automated Threat Detection and Response

Automation can significantly enhance the efficiency and effectiveness of insider threat and risk management. Automated tools can handle large volumes of data and identify threats more quickly than manual processes. Seek solutions that include advanced AI-driven analytics and automation features to streamline threat detection and response, reducing the burden on IT security teams.

4 | Adopt a Zero Trust Framework

A Zero Trust approach ensures that all users and devices are continuously authenticated and authorized, reducing the risk of insider threats. This method aligns with the need for unified visibility and control across all environments, which 93% of respondents consider important. Look for platforms that offer detailed identity and access management and analytics to support Zero Trust principles.

5 | Enhance Employee Training and Awareness

With 32% of respondents highlighting a lack of training and awareness as a major driver behind insider threats, implementing regular and comprehensive training programs is crucial. These programs should educate employees about security best practices, recognizing suspicious behavior, and understanding the importance of data protection. Opt for platforms that offer insights into user behavior to tailor effective training programs.

6 | Foster a Security-Conscious Culture

Creating a culture of security awareness is vital. Executive management should prioritize insider threat management and lead by example. This includes developing and enforcing robust internal policies and encouraging open communication about security issues. Create an insider threat stakeholder advisory board to help build and enforce all internal policies. Seek solutions that provide continuous monitoring and enforcement capabilities to support this cultural shift.

7 | Conduct Regular Security Audits and Assessments

Regular audits and assessments can identify vulnerabilities and gaps in your insider risk management strategy. This practice is particularly important for the 18% of respondents uncertain about the effectiveness of their tools. Continuous evaluation and improvement ensure that your defenses remain robust against evolving threats. Choose platforms that offer comprehensive reporting and analytics to facilitate ongoing assessments.

8 | Implement Comprehensive Incident Response Plans

Having a well-defined incident response plan that includes specific procedures for dealing with insider threats is crucial. This plan should be regularly tested and updated to reflect the latest threat landscape. As noted in the report, a significant portion of organizations are unsure about their recovery times, highlighting the need for robust and tested incident response strategies. Opt for solutions that provide actionable insights and customizable response playbooks to guide security teams during incidents.

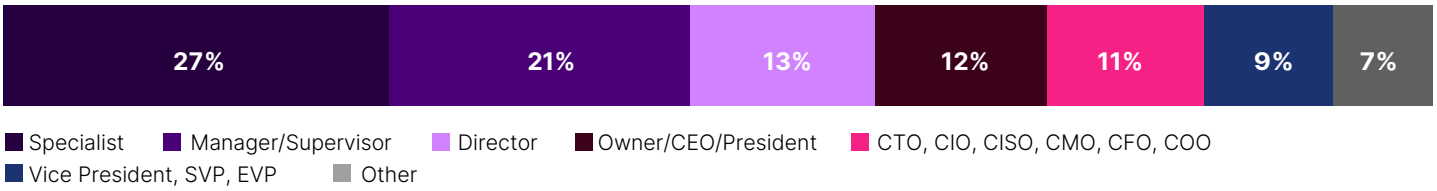
By adopting these best practices and leveraging advanced, integrated cybersecurity solutions, organizations can significantly enhance their ability to manage insider threats, protect sensitive information, and maintain a secure operational environment.

Methodology and Demographics

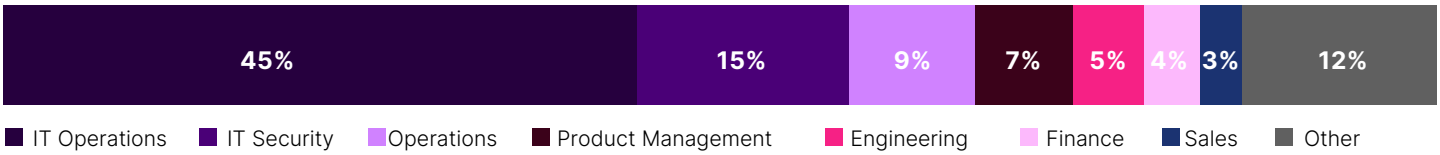
This 2024 Insider Threat Report is based on a comprehensive online survey of 413 cybersecurity professionals, conducted in August 2024, to gain deep insight into the latest trends, key challenges, and solutions for insider threat management.

The survey utilized a methodology ensuring a diverse representation of respondents, from technical executives to IT security practitioners, across various industries and organization sizes. This approach ensures a holistic and balanced view of the insider threat landscape, capturing insights from different organizational perspectives and experiences.

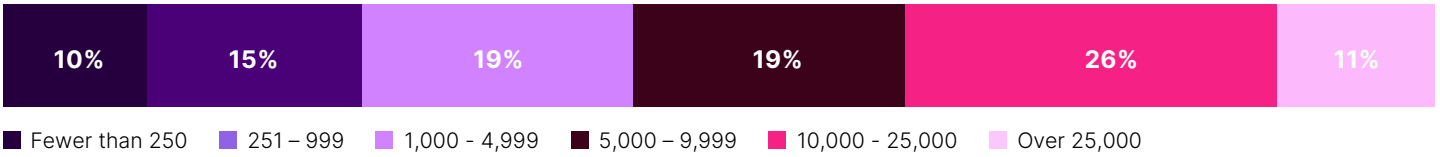
CAREER LEVEL



DEPARTMENT



COMPANY SIZE



Reseach Notes: Results shown in this report are focused on organizations larger than 1,000 employees, unless noted otherwise. In "Select all that apply" survey questions, the total percentage can exceed 100% because respondents could pick more than one answer.

Gurucul is the only cost-optimized security analytics company founded in data science that delivers radical clarity about cyber risk. Our REVEAL security analytics platform analyzes enterprise data at scale using machine learning and artificial intelligence. Instead of useless alerts, you get real-time, actionable information about true threats and their associated risk. The platform is open, flexible and cloud native. It conforms to your business requirements so you don't have to compromise. Our technology has earned us recognition from leading industry analysts as the most Visionary platform and an Overall leader in product, market and innovation. Our solutions are used by Global 1000 enterprises and government agencies to minimize their cybersecurity risk.

To learn more, visit Gurucul.com

and follow us on LinkedIn and Twitter.

Cybersecurity
INSIDERS

Cybersecurity Insiders brings together 600,000+ IT security professionals and world-class technology vendors to facilitate smart problem-solving and collaboration in tackling today's most critical cybersecurity challenges.

Our approach focuses on creating and curating unique content that educates and informs cybersecurity professionals about the latest cybersecurity trends, solutions, and best practices. From comprehensive research studies and unbiased product reviews to practical e-guides, engaging webinars, and educational articles - we are committed to providing resources that provide evidence-based answers to today's complex cybersecurity challenges.

Contact us today to learn how Cybersecurity Insiders can help you stand out in a crowded market and boost demand, brand visibility, and thought leadership presence.

Email us at info@cybersecurity-insiders.com or visit cybersecurity-insiders.com