Market Guide for Insider Risk Management Solutions

12 March 2025 - ID G00805757 - 19 min read

By: Brent Predovich, Deepti Gopal

Initiatives:Cyber Risk; Build and Optimize Cybersecurity Programs

Rising incidents of intellectual property theft and employee-related breaches highlight the importance of insider risk management. Security and risk management leaders are advised to address these challenges by developing comprehensive programs and investing in solutions with robust capabilities.

Overview

Key Findings

- While most insider risks are attributed to errors and carelessness, malicious actors also exploit these risks for crimes like data theft.
- Insider risk management is a cross-functional activity, but many programs have minimal coordination among IT and cybersecurity leaders, legal, HR, finance and corporate (physical) security.
- Disparate controls can introduce potential gaps, highlighting the importance of a cohesive insider risk management strategy that integrates capabilities, policies and processes to mitigate threats.
- Most organizations believe artificial intelligence (AI) plays a central role in insider risk management, even though the market has not yet incorporated AI into the solutions.

Recommendations

Security and risk management (SRM) leaders with a responsibility for insider risk management should:

- Develop a formal insider risk program to increase visibility into risks from careless or malicious associates and partners.

- Work in collaboration with cross-functional partners in appropriate areas, including legal, HR and privacy.
- Implement a unified insider risk management framework that seamlessly integrates capabilities, policies and processes to ensure comprehensive threat mitigation.
- Dedicate a portion of the budget and personnel to track the incorporation of AI-driven capabilities, and embark on proofs of concept (POCs) to gain first-mover advantage.

Market Definition

Gartner defines the insider risk management (IRM) market as solutions that use advanced analytics, monitoring, and behavior-based risk models to detect, analyze and mitigate risks posed by trusted insiders within an organization. These solutions monitor the activities of employees, service partners and key suppliers to ensure their behavior aligns with corporate policies and risk tolerance levels. IRM platforms can be delivered as cloud-based services or on-premises solutions, or in hybrid forms. When effectively implemented alongside proper governance, they provide comprehensive visibility, real-time detection, and proactive intervention to safeguard against data theft, fraud and other malicious or unintentional insider threat activities.

Insider risk management is a critical concern across various industries, including finance, healthcare, manufacturing and government. These industries handle sensitive data, including intellectual property, making them prime targets for insider threats. Insider risks can stem from careless employees, malicious insiders or compromised credentials, and can result in data theft, fraud or system sabotage.

Historically, insider risk was managed through a combination of basic monitoring tools, siloed data and manual processes. However, as the complexity and volume of insider threats have grown, organizations have recognized the need for more sophisticated and integrated solutions. This shift has led to the development of comprehensive IRM platforms that leverage advanced technologies such as artificial intelligence and machine learning to detect and mitigate threats in real-time.

The insider risk management market exists because:

- **The threat landscape is evolving:** Insider threats are becoming more sophisticated, with attackers abusing authorized access to carry out malicious activities. This makes traditional security measures inadequate.

- **Regulatory pressure is increasing:** Governments and regulatory bodies are imposing stricter data protection and privacy regulations, requiring organizations to have robust insider risk management programs in place.
- **Remote work has expanded:** The shift to remote work has expanded the attack surface, making it more challenging to monitor and manage insider risks.
- **Insider incidents incur high costs:** Organizations face significant financial and reputational damage from insider incidents, making proactive risk management a priority.

A formal insider risk program can increase visibility into risks from both careless and malicious insiders, improve collaboration with cross-functional partners, and increase adoption of advanced technologies to enhance enterprise security posture.

Mandatory Features

The mandatory features for this market include:

- Orchestration with other cybersecurity tooling
- Monitoring of employee activity and assimilation into a behavior-based risk model
- Dashboarding and alerting of high-risk activity
- Orchestration and initiation of intervention workflows
- Endpoint agent-based monitoring
- Data-centric misuse detection
- Network interception and session reconstruction
- Active data exfiltration blocking

Common Features

Common features for this market include:

- User and entity behavior analytics (UEBA)
- Network interception and session reconstruction
- Baseline and configuration management

- Various role-based user interfaces
- Incident response and forensics
- Security frameworks compliance reports

Market Description

At its core, insider risk management involves detecting and preventing user or partner behaviors — be they malicious or unintentional — in violation of company policy that could lead to a loss of data or another undesirable outcome.

Insider risk management differs from conventional attack detection because the initial vector of attack is a properly authorized user. As a result, many traditional threat-hunting techniques or tools to detect unauthorized access fail to identify insider threats. Furthermore, unlike external threat actors who seek to escalate privileges, insiders — whether malicious or not — frequently already have elevated privileges associated with their legitimate roles.

To manage insider risks, SRM leaders must orient their strategies around the "Rule of Three" (see Figure 1). Insider risks come from three archetypical sources, which engage in three principal activities. In response, organizations must pursue three mitigation objectives.

Figure 1: The "Rule of Three" for Insider Threats

Threat Types

The archetype of the disgruntled employee stealing company secrets for sale to the highest bidder is in reality an atypical example of an insider threat. Survey data reveals that more than 50% of insider incidents lack malicious intent. [1] Insider threats can thus be classified as any one of three types of threat actors:

- **Careless user** — Someone who accidentally exposes sensitive and/or proprietary data (including errors and improper configurations).
- **Malicious user** — Someone who intentionally sabotages or steals data for either personal or financial gain.
- **Compromised credentials** — Credentials exploited by someone outside the organization for the purpose of data theft and/or sabotage.

These categories are not necessarily exclusive, and may well morph over time.

Threat Activities

Insider threat activities are typically categorized into one of three activities deemed to be a policy violation or illegal by law:

- **Fraud** — Misrepresentation, financial theft and other forms of embezzlement (including expenses fraud)
- **Data theft** — Exfiltrating or viewing unauthorized data
- **System sabotage** — Malware, ransomware, account lockouts and data deletion

Mitigation Goals

Lastly, the rule of three for insider risk focuses on three core mitigation goals intended to:

- Deter the individuals from wanting to do it in the first place
- Detect the activity
- Disrupt the effort

See 3 Actions to Maximize the Success of an Insider Risk Management Program for additional information.

Products and services in this market include monitoring and surveillance capabilities. Although “monitoring” and “surveillance” are terms that are often used interchangeably, Gartner uses them in specific ways:

- **Monitoring** refers to any technique or technology used to collect data from IT assets. Monitoring is asset-centric in its focus.
- **Surveillance** refers to the overt and covert use of monitors in pursuit of a comprehensive awareness of the activities of a defined person, or set of people, in a given context. Surveillance is people-centric in its focus.

Market Direction

Early insider management tools focused on user-created rules and workflows, but the market has since abandoned this approach. Although some of these tools were “better than nothing,” SRM leaders are now looking for technology that leverages automation and reduces the amount of rules management and modification they are required to exercise. Buyers in this market expect functionality such as monitoring of authorized user employee activity and assimilation into a behavior-based risk model to be embedded in the selected toolset.

Instead of a rule-based approach, vendors are increasingly leaning toward adopting AI for a more in-depth and comprehensive analysis of potential threats. Simultaneously, 64% of AI users are emphasizing the pivotal role it plays in enabling the creation of robust predictive models that enhance the efficacy of their insider risk management strategies. [1] This growing synergy between vendors and users highlights the significance of AI in addressing the evolving challenges associated with insider risks.

Data loss prevention (DLP) and insider risk management capabilities are increasingly converging into a unified solution. This convergence is driven by the recognition that preventing data loss and managing risks are interconnected goals. Combining DLP and risk management, organizations can create a comprehensive approach that safeguards sensitive information, as well as proactively identifies and mitigates potential threats, ultimately leading to a more robust and holistic data protection strategy.

Organizations with mature cybersecurity programs are increasingly adopting insider risk management initiatives. However, the market is now acknowledging the significance of organizations initiating insider risk management programs at earlier stages of program maturity, even if this begins solely with the development of strategies and awareness around insider risks.

Market Analysis

Because insider risk management involves a suite of technologies, it is difficult to make sweeping statements about the direction of a single market over the long term. We expect further consolidation in some segments, just as DLP controls have become standard as part of an insider risk management program. At a more granular level, it is more useful to address two key categories of tools:

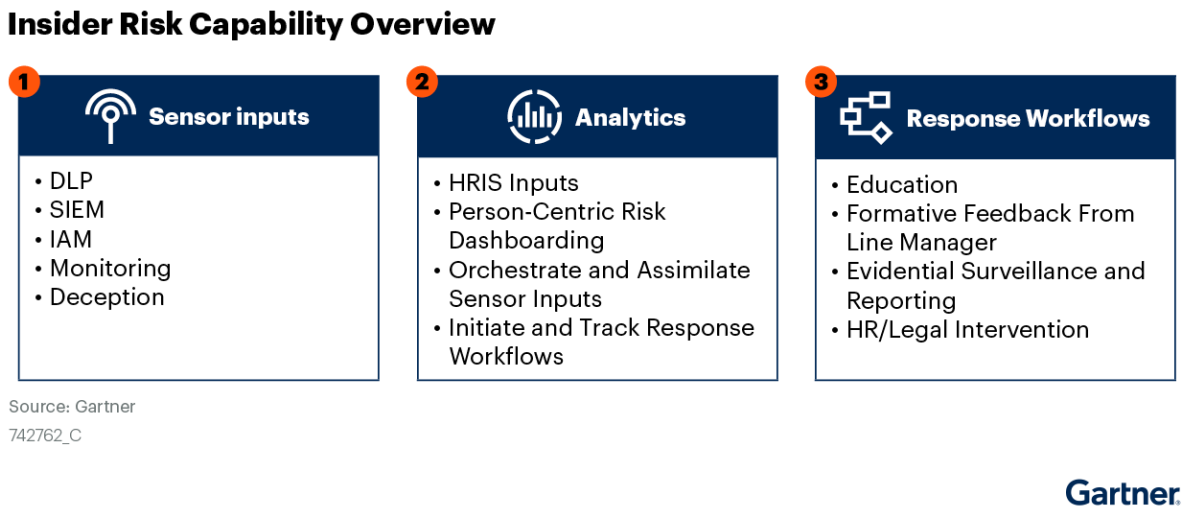
- Surveillance tools (of which there are several subcategories)
- Information governance platforms

The Facts About Insider Risk and Insider Threats

- Remote workers are the primary source of criminal prosecutions for insider risk. According to DTEX's 2022 Cost of Insider Threats: Global Report, 75% of investigations that led to criminal prosecutions for data theft occurred from inside the home. [1]
- In 2024, 48% of organizations reported that insider attacks have become more frequent over the past 12 months. [2]
- A substantial 71% of organizations reported feeling at least moderately vulnerable to insider threats, indicating heightened awareness and concern over internal risks. [3]
- In 2024, 54% of organizations reported that their insider threat programs are less than effective, highlighting the need for improved strategies. [1]
- The most common insider attack vectors in 2024 include information disclosure (56%) and unauthorized data operations (48%), emphasizing the importance of data-centric security measures. [4]
- In 2024, 70% of organizations identified technical challenges or cost as the primary obstacles preventing them from implementing effective insider threat management. [3]
- Organizations continue to invest in a program and tools to deal with insider threats, spending an average of $16.2 million in 2023, which represents an increase of 5.33% from the $15.38 million spent in 2021. [1,2]

Figure 2 presents a strategic framework for effectively managing insider threats. By integrating diverse sensor inputs with advanced analytics, it empowers organizations to proactively detect and mitigate risks, ensuring robust security and resilient operations.

Figure 2: Insider Risk Capability Overview



Surveillance Tooling

Insider risk management begins with visibility, which is not easily achieved. Any community of associates is composed of diverse individuals, each of whom interacts with technology in a unique and ever-changing way. Persistent surveillance of insiders requires a number of distinct technologies to watch for potential indicators of risk, depending on the platform or potential vector of compromise. The suite of surveillance tooling an enterprise uses should include internal infrastructure insider risk detection, social media risk monitoring, cloud service usage monitoring and mobile monitoring.

SRM leaders must acknowledge that surveillance is a controversial and sometimes uncomfortable topic, subject to complex and diverse regulatory regimes around the globe. Organizations commonly monitor internal communications systems (for example, email or collaboration platforms) and investigate suspected policy violations. However, the expansion of these activities into a more pervasive inspection of the work life of users can infringe on privacy expectations and rights in the workplace.

Organizations should obtain authorization from senior management and provide full transparency for access-monitoring activities by informing affected individuals of the objective, scope and methods of surveillance activities. It is essential to consider geographic limitations, as regulations and permissible actions can vary significantly between regions. Prior to the deployment of surveillance tools, managers should be trained in the identification, management and escalation of ethical situations that might arise from surveillance. Preemptive engagement with ethics, legal or HR teams can mitigate legal liabilities and material damage from poorly targeted or managed surveillance activities.

Additionally, organizations must consult legal counsel and HR leaders to establish clear boundaries on the capture, storage, sharing, analysis and destruction of data regarding activities. This ensures that surveillance practices are not only compliant with regional laws and regulations, but that they also respect the privacy and rights of individuals involved.

Internal Infrastructure Insider Risk Detection

Internal infrastructure monitoring tools support security assurance, as well as productivity optimization. This agent-based set of tools is the most common form of employee surveillance.

Employee surveillance via internal infrastructure monitoring can capture, record, review and report on employees' digital behavior. In some implementations, contextual data is also captured to provide a framework for employees' actions. Such tools primarily monitor email exchanges; internet activity (segmented by websites, time spent and other basic parameters); user activity and inactivity; instant messaging (IM); file transfers; file manipulation; online searches; and general network activity. These actions are monitored mainly by keystroke detection, continuous screenshot recording, and the cataloging of websites visited and data moved by any digital mechanism — for example, file copy, file print and FTP. This form of monitoring is predominantly driven by static rules focused on keywords, URLs, document tracking and specified endpoints. It does not generally provide the ability to automatically respond to changes in context.

For gauging productivity, these tools monitor actions such as user inactivity and web-surfing data, including time spent on social media and IM conversations. This ensures that these metrics are captured, and policies can be made to ensure cost savings and increased efficiency in the system. Many solutions support alerts when predefined illicit activity is detected. In some cases, alerts can be used to automatically increase the frequency of collection or scope of data actively analyzed and investigated.

Social Media Risk Monitoring

Social media risk monitoring tools have become increasingly vital for organizations, particularly in industries where compliance and client interactions are closely regulated. These specialized tools bring essential capabilities to the forefront. First and foremost, they enable organizations to identify, register and closely monitor employees who engage with clients or prospects through social media platforms. This ensures transparency and accountability in client communications, while adhering to industry regulations.

Moreover, these tools excel in content management, enabling organizations to identify and filter social media content in accordance with their policies. This feature aids in maintaining brand consistency, adhering to compliance standards and swiftly addressing potential policy violations.

Social media risk monitoring tools also offer a robust workflow framework for handling approvals, exceptions or policy breaches; streamlining the decision-making process; and ensuring swift and effective responses. Further, they often provide integrated archiving solutions, enabling organizations to retain and manage social media communications in a secure and compliant manner, in the tool itself or through integration with enterprise information archive solutions. By amalgamating these capabilities, these tools offer a comprehensive and efficient approach to mitigate potential compliance and reputational risks associated with social media interactions.

Cloud Service Usage Monitoring

External cloud service monitoring tools need to address three subsets of services: social media, SaaS, and consumer and enterprise file sharing and synchronization (such as Microsoft OneDrive and Dropbox). This category can be further divided into two segments: sanctioned and unsanctioned cloud services.

Employees may regularly use public cloud services that are not officially approved for work purposes (unsanctioned). Sanctioned public cloud services include apps that are approved and adopted by the organization and integrated with internal IT systems for use cases such as enterprise resource planning (ERP) and customer relationship management (CRM). SaaS security posture management (SSPM) facilitates compliance and protects data within SaaS environments. Security service edge (SSE) is a service that enables the monitoring of both sanctioned and unsanctioned cloud services (see Magic Quadrant for Security Service Edge).

Mobile Monitoring

Mobile monitoring is different from traditional location-based monitoring carried out through mobile phones. These tools monitor how the mobile device is used — for example, data transfers, app usage, mobile internet usage — and not where the device is located. Mobile monitoring tools typically include the components of unified endpoint management (UEM) suites to manage the devices, content and applications that are accessed (see Market Guide for Endpoint Management Tools). This is often done to mitigate threats emanating from employer-owned and employee-owned bring-your-own-device (BYOD) instruments.

A more detailed approach to address problems arising out of BYOD involves mobile endpoint monitoring, SSE tools and virtual private networks (VPNs). Always-on VPNs ensure that user activity is monitored in real time and prevent unknown devices from entering the corporate network. They can track only the service or website visited and the size of file exchanges. Sensitive documents and files can be tracked by watermarking, which ties them to the user, date and transaction as they are accessed and traversed through cloud services, and can be blocked when such an activity is detected.

Information Governance Platforms

These tools provide an underlying architecture to address information capture and archiving. Insider risk management tools collect a great deal of information that must be archived securely, but in a way that facilitates subsequent analysis and review (see Note 2 for Gartner's definition of information governance).

Information governance capabilities found in insider risk management tools are gaining prominence as the regulatory and legal compliance burden increases for many organizations. Accordingly, these tools are most popular with large organizations in regulated industries that may have to ensure consistent compliance across multiple vectors, such as internal infrastructure, employee-owned devices and public cloud services.

Delivery Model

For many applications, analysis, dashboarding and reporting modules are delivered as cloud-centric software as a service (SaaS). Where endpoint agents, security information and event management (SIEM) sensors or network traffic monitors are needed, this requires a physical or software presence.

User Type

Insider risk management requires broad stakeholder participation and proper governance. SRM leaders must work with other business leaders, including:

- CISOs/cybersecurity leaders
- CHROs/HR leaders
- CLOs/legal leaders

Although insider risk management requires broad stakeholder participation, the tools used are primarily the domain of cybersecurity leaders. HR leaders make active use of tools that monitor communications channels and user activities for compliance with corporate codes of conduct and performance monitoring.

Representative Vendors

The vendors listed in this Market Guide do not imply an exhaustive list. This section is intended to provide more understanding of the market and its offerings.

Market Introduction

The vendors listed in Table 1 represent the broader insider risk detection market, because the products are either marketed and sold specifically for this purpose, or because the providers offer products with insider threat use cases.

Table 1: Representative Insider Risk Management Solution Vendors

(Enlarged table in Appendix)

Representative Vendors	Product	Headquarters
ActivTrak	ActivTrak Platform	Austin, Texas
CANDA Solutions	Fresh Haystack	Columbia, Maryland
Cyberhaven	Data Detection and Response	Palo Alto, California
DoControl	SaaS Security Platform	New York, New York
DTEX Systems	DTEX InTERCEPT	Saratoga, California
Everfox	EverShield	Herndon, Virginia
Exabeam	Fusion SIEM, Fusion XDR, Exabeam UserXDR	Foster City, California
Fortinet	FortiInsight	Sunnyvale, California
Fortinet (Next DLP)	Reveal Platform	London, U.K.
Gurucul	Gurucul Risk Analytics	El Segundo, California
Logpoint	Logpoint user and entity behavior analytics (UEBA)	Copenhagen, Denmark
OpenText (Micro Focus)	ArcSight Intelligence	Waterloo, Canada
Microsoft	Microsoft Purview Insider Risk Management	Redmond, Washington
Mimecast	Mimecast Incydr	London, United Kingdom
NetWitness	NetWitness	Burlington, Massachusetts
Proofpoint	Proofpoint Insider Threat Management	Sunnyvale, California
Rapid7	InsightIDR	Boston, Massachusetts
Red Vector	Fulcrum	Chesterbrook, Pennsylvania
Securonix	Securonix UEBA	Addison, Texas
Splunk	Splunk User Behavior Analytics (UBA)	San Francisco, California
Syteca	Syteca	Newport Beach, California
Teramind	Teramind Starter, Teramind User Activity Monitoring (UAM), Teramind Behavioral Data Loss Prevention (DLP)	Miami, Florida
Veriato	Cerebral, Vision, Veriato Workplace Investigator	West Palm Beach, Florida

Source: Gartner (March 2025)

Market Recommendations

SRM leaders should:

- Create an internal policy that governs the use of insider threat monitoring and surveillance tools, as well as the data that is collected. Include within the policy the retention period for the data and who can request surveillance or access the collected data.
- Select technology aligned with your use case (agent or agentless).

- Select a solution with capabilities aligning with the characteristics of:
  - The work environment
  - Employee populations
  - Cultural expectations
  - Risk assessment outcomes
  - Applicable regulations
  - The company's resilience appetite

- Provide transparency for surveillance activities, and define and document activities that are prohibited, or to be avoided, while using company infrastructure as part of comprehensive policies.
- Ensure that privacy laws are not violated by having an open dialogue with all relevant stakeholders, including the legal and HR departments.
- Ensure support intervention, whether formal or informal, is carried out by those best placed to do so — including HR and line-of-business management.
- Build a business case for insider risk management that identifies the activities and services that should be monitored, including external and public cloud services. The business case should also define the use cases of value to your organization, such as the capture of regulated communications.
- Address risk emanating from unsanctioned consumer cloud services. Assess which consumer cloud services are critical to enterprise operations to justify the application of internal controls (such as encryption) augmenting security, while supporting employee use cases. Consider blocking or aggressively filtering access to consumer cloud services that are not required for enterprise operations.
- Follow standardized procedures with an investigation trail to ensure that monitoring data is not used for inappropriate purposes (such as an internal appraisal process) and does not violate employee privacy rights or expectations.
- Align insider risk data collection with data analysis capabilities. Avoid collecting data that your organization is not prepared to analyze and leverage for improvement in detection accuracy.

Evidence

[1] 2023 Cost of Insider Risks Global Report, DTEX Systems.

[2] 2022 Cost of Insider Threats: Global Report (download), Proofpoint.

[3] Insider Threat Report 2024, Cybersecurity Insiders.

Note 1: Active Versus Passive Controls

Insider risk management constitutes a passive behavioral control. Passive controls do not directly mitigate risk, but provide the situational awareness that enables the application of an appropriate active control (for example, altering the configuration of a content filter in a secure web gateway). The active controls (and additional passive controls) that leverage employee activity data in insider risk management solutions include:

- User behavior analytics
- Physical security controls, such as facility access mechanisms
- DLP
- Access privilege management
- User authorization management
- Fraud detection and escalation

Note 2: Definition of Information Governance

Gartner defines information governance as the specification of decision rights and an accountability framework to ensure appropriate behavior in information valuation, creation, storage, use, archiving and deletion of information. It includes the processes, roles and policies, standards, and metrics that ensure the effective and efficient use of information in enabling an organization to achieve its goals.

Document Revision History

Market Guide for Insider Risk Management Solutions - 13 November 2023

Market Guide for Insider Risk Management Solutions - 18 April 2022

Market Guide for Insider Risk Management Solutions - 29 December 2020

Recommended by the Authors

Some documents may not be available as part of your current Gartner subscription.

Market Guide for Digital Forensics and Incident Response Retainer Services

Market Guide for Managed Detection and Response

Market Guide for Data Loss Prevention

Hype Cycle for Cyber-Risk Management, 2024

Developing Use Cases for User Behavior Monitoring and Insider Threat Detection

CISO Foundations: Build a Culture of Security Consciousness: Introducing the Gartner PIPE Framework

Table 1: Representative Insider Risk Management Solution Vendors

Representative Vendors	*Product*	*Headquarters*
ActivTrak	ActivTrak Platform	Austin, Texas
CANDA Solutions	Fresh Haystack	Columbia, Maryland
Cyberhaven	Data Detection and Response	Palo Alto, California
DoControl	SaaS Security Platform	New York, New York
DTEX Systems	DTEX InTERCEPT	Saratoga, California
Everfox	EverShield	Herndon, Virginia
Exabeam	Fusion SIEM, Fusion XDR, Exabeam UserXDR	Foster City, California
Fortinet	FortiInsight	Sunnyvale, California
Fortinet (Next DLP)	Reveal Platform	London, U.K.
Gurucul	Gurucul Risk Analytics	El Segundo, California
Logpoint	Logpoint user and entity behavior analytics (UEBA)	Copenhagen, Denmark
OpenText (Micro Focus)	ArcSight Intelligence	Waterloo, Canada
Microsoft	Microsoft Purview Insider Risk Management	Redmond, Washington
Mimecast	Mimecast Incydr	London, United Kingdom

Representative Vendors	*Product*	*Headquarters*
NetWitness	NetWitness	Burlington, Massachusetts
Proofpoint	Proofpoint Insider Threat Management	Sunnyvale, California
Rapid7	InsightIDR	Boston, Massachusetts
Red Vector	Fulcrum	Chesterbrook, Pennsylvania
Securonix	Securonix UEBA	Addison, Texas
Splunk	Splunk User Behavior Analytics (UBA)	San Francisco, California
Syteca	Syteca	Newport Beach, California
Teramind	Teramind Starter, Teramind User Activity Monitoring (UAM), Teramind Behavioral Data Loss Prevention (DLP)	Miami, Florida
Veriato	Cerebral, Vision, Veriato Workplace Investigator	West Palm Beach, Florida

Source: Gartner (March 2025)