Quadrant Knowledge Solutions

Security and Risk Management

SPARK Matrix™: Insider Risk Management, Q3, 2024

Market Insights, Competitive Evaluation, and Vendor Rankings

July, 2024

TABLE OF CONTENTS

Executive Overview.....1

Market Dynamics and Overview.....2

Competitive Landscape and Analysis.....5

Key Competitive Factors and Technology Differentiators.....14

SPARK Matrix™: Strategic Performance Assessment and Ranking 18

Vendor Profile.....22

Research Methodologies.....141

Executive Overview

This research service includes a detailed analysis of global Insider Risk Management market dynamics, vendor landscape, and competitive positioning analysis. The study provides competition analysis and ranking of the leading Insider Risk Management vendors in the form of the SPARK Matrix™. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendors capabilities, competitive differentiation, and market position.

Market Dynamics and Overview

Quadrant Knowledge Solutions defines an Insider risk management solution as "software that detects and mitigates advanced threats by closely monitoring and analyzing the activities of internal and external users and entities within a network." The solution provides alerts, response, and investigation workflows for high-risk insider activity that can lead to data loss, among other consequences. The solution leverages AI & ML capabilities to correlate the real-time monitored user and entity data with that of historical threat patterns and helps detect threats early.

Detection of insider threats remains a challenge for organizational security teams. The bad actors have legitimate access to the sensitive data. The problem is further compounded by insiders with elevated data access privileges. Thus, such insiders, both malicious users and pawns, have the potential to inflict severe damage before such breaches are detected and mitigated. The situation is made even more complex owing to increasingly stringent data protection laws. Noncompliance will result in financial as well as reputational loss to organizations. Organizations can lessen insider risk by adopting an insider risk management solution that can easily identify, detect, and mitigate insider risk in real-time before it harms or breaches critical infrastructure. In addition, unlike traditional security products, which do not provide advanced threat detection and prevention capabilities, insider risk management solutions leverage AI and ML technologies to monitor and warn about suspicious network traffic inside organizational IT systems.

Organizations are looking for advanced security solutions to secure against threats like data aggregation, account sharing, privileged data, and snooping. The solutions should also provide access control and detect unusual employee or third-party behavior. Additionally, they are looking for solutions that detect Intellectual Property (IP) theft, policy breaches, sensitive data leaks, confidentiality breaches, frauds, insider trading, disgruntled user behavior, and regulatory compliance issues. They are also looking for solutions that can benchmark employee behavior and issue warnings in case of any deviations. Advanced Insider risk management solutions go beyond basic monitoring, utilizing artificial intelligence (AI) and machine learning (ML) to create user behavior baselines and detect anomalies in real-time. Advanced IRM platforms analyze a vast array of data points, including access attempts (privileged and non-privileged), data downloads, file transfers, email activity, and application usage. Furthermore, Natural Language Processing

(NLP) is being used to scrutinize employee communications concerning keywords or sentiment, potentially indicating discontent or malicious intent. The adoption of advanced insider risk management solutions fulfills these requirements, allowing organizations to strengthen the security of their cybersecurity ecosystem.

The following is a detailed description of the key capabilities of an Insider Risk Management solution:

- **User and Device Monitoring:** An Insider risk management solution can monitor users and their devices. This capability enables organizations to monitor and track all user and linked device activities. The capability monitors insider user and device activity, detects suspicious user behavior, and provides advanced protection techniques to respond to security incidents. Additionally, it tracks the user's incoming and outgoing emails, applications, websites, keystrokes, IM/chats, network connections, console commands, removable as well as cloud drives, network file transfers, and search engine queries.

- **Advanced Threat Detection:** An Insider risk management solution provides visibility and control over internal data access, prevents organizational security violations, enables organizational IT systems to detect insider threats, and minimizes security vulnerabilities with its advanced threat detection capability. The capability helps analyze all the users, systems, apps, and suspicious activities to detect unusual behavior and highlight events. Additionally, the solution helps manage potential insider risks by identifying threats like data breaches, privilege abuse, application misuse, unauthorized users, risky inadvertent activities, and other anomalous and risky user and device behavior.

- **User and Entity Behavior Analytics:** This key feature detects, alerts, prevents, and responds to known and unknown user behavior or attacks before they affect the organization. The capability helps detect user and entity behavioral risks, identifies user patterns and insider threats, and provides visibility into behavioral anomalies. The capability helps identify malicious insiders and detect whether a user's credentials have been hacked or misused.

- **Risk Response Automation:** An Insider risk management solution offers risk response capability that mitigates threats automatically in real-time. Additionally, the capability monitors users' activities regarding applications as well as data and automatically blocks or restricts access to an application or privileged data in case of unusual behavior. Further, automated risk response enhances the productivity and efficiency of the Security Operation Center (SOC) team.

- **Audit and Reporting:** An insider risk management solution allows user organizations to easily audit users' and suppliers' access and provide information regarding their activities. The capability allows organizations to spot and prevent any fraudulent activity.

- **Data Loss Prevention:** An Insider Risk management solution offers Data Loss Prevention capabilities that allow organizations to identify, classify, as well as gather information on privileged data and block any unauthorized users or malicious insiders attempting to access the privileged data. Additionally, it helps monitor manipulated, encrypted, and compressed data, blocks data exfiltration by any channel, and provides complete forensic data on any attempted exfiltration to minimize insider risk.

- **Analytics and Dashboarding:** An Insider risk management solution offers Analytics and Dashboarding capabilities that help organizations get holistic insights into suspicious/unauthorized file movement and likely data exfiltration activities in the corporate network. The capability also helps users understand the impact of the implemented IRM solution by displaying the number of threats mitigated in advance by the solution. The capability also provides behavioral data through dashboards for analyzing reports and tracking suspicious application usage, website history, and USB activities. Additionally, the capability enables users to create comprehensive reports for audit trail requirements.

Competitive Landscape and Analysis

Quadrant Knowledge Solutions conducted an in-depth analysis of the major Insider Risk Management vendors by evaluating their products, market presence, and value proposition. The evaluation is based on primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall Insider Risk Management market. This study includes an analysis of key vendors, including Aware, Bottomline, Code42, Cogility, CounterCraft, Crisp, CyberHaven, Dasera, DoControl, DTEX System, Ekran System, Elevate Security, Everfox, Exabeam, Fortinet, Gurucul, Human Security, IBM, LogPoint, LogRhythm, Microsoft, Next, OpenText, Proofpoint, Rapid7, RSA, Sail Point, Secure Passage, Securonix, Splunk, Teramind, and Veriato.

Aware, Bottomline, Code42, Cogility, LogPoint, LogRhythm, Next, Proofpoint, Rapid7, SailPoint, Splunk, and Teramind are the top performers and technology leaders in the global Insider Risk Management market. These companies provide a sophisticated and comprehensive technology platform to detect, analyze, protect, remediate, and respond to insider threats in real-time. Their platforms also provide control and visibility over internal data access and data exfiltration by end-users, including employees, remote vendors, and contractors, to provide protection from insider threats like theft, fraud, and damage. Insider Risk Management helps organizations detect intellectual property (IP) theft and combat risks, policy breaches, sensitive data leaks, confidentiality breaches, fraud, insider trading, disgruntled user behavior, and regulatory compliance issues.

Aware offers an automated insider threat solution through its Contextual intelligence platform. The solution identifies and responds to external threats as well as compromised users in real-time. The solution performs AI-infused activity analysis to identify blind spots in the threat environment. The solution also includes self-learning ML algorithms to reduce false positives and provide improved time to resolution by using a contextual overview of threat activities.

Bottomline Risk Solutions offer Payment Fraud, Case management and Insider Threat solutions. The solution utilizes advanced analytics and AI equipped with a patented technology that performs non-invasive recording of the users' access to corporate systems by capturing all user activity across legacy and modern applications located on-prem and in the cloud to identify subtle deviations from user baselines, enabling organizations to proactively detect and mitigate potential insider threats before they escalate. Bottomline provides SaaS application

monitoring, which helps expand threat surface monitoring to modern SaaS and Web applications using strong encryption.

Code42's SaaS-based Code42 Incydr platform provides source code protection, enables real-time threat blocking, offers better access to exfiltrated files, and provides proven performance on macOS, Windows, and Linux machines. It also provides easy browser visibility and no-gap file monitoring. The solution also provides Risk Indicators (IRI) that automatically prioritize the risks needing immediate attention by applying multi-dimensional context, including file, source, exfiltration destination, and user, to determine the risk associated with an activity and detect anomalous user behavior by pinpointing deviations from baseline user behaviors.

Cogility's Counter-Insider Threat Intelligence solution leverages its Expert AI-powered Cogynt platform for real-time analysis of massive, diverse data streams. The solution applies its Expert AI and evolving AI LLM technology within its platform to generate comprehensive risk insights and streamline decision-making processes with full traceability. Among different differentiators within its C-Int offering, Cogility has made advancements in applying the Sociotechnical and Organizational Factors for Insider Threat (SOFIT) ontology as a key component in structuring its Insider Threat potential risk indicators.

LogPoint offers an Insider Risk management solution through its LogPoint SIEM and LogPoint UEBA solutions. The solution delivers improved investigation of unexpected behavioral patterns while minimizing the time spent on threat hunting by detecting advanced threats early and mitigating risk, damage, and data loss. The unified platform ensures a direct flow of information from the SIEM to SOAR. It enables quicker detection and resolution of cyber threat incidents by collecting and prioritizing security data and threat alarms. It helps accelerate threat detection and response by spotting early signs of suspicious patterns and anomalous behavior in real-time within the cloud and on-prem networks. LogPoint's SIEM with UEBA enables organizations to securely create, manage, and transform business through powerful analytics and AI-driven automation. LogPoint UEBA also provides entity risk scoring, which leverages information from the UEBA in alerting, dashboards, reports, and search templates.

LogRhythm offers Insider Risk Management capabilities through its User and Entity Behavior Analytics (UEBA) and UserXDR solutions that enable early identification

of abnormal user and device behavioral patterns to stop critical data breaches. LogRhythm's platform ingests data from diverse sources, including user behavior logs, network activity, and security events. By leveraging machine learning and advanced analytics on this comprehensive dataset, LogRhythm pinpoints subtle anomalies in user behavior that might signal insider threats. LogRhythm UEBA provides enhanced threat detection capabilities by applying unsupervised ML algorithms for security across enormous, cloud-based centralized datasets.

Next offers an Insider Risk Management and Data Loss Prevention solution through its Reveal platform. The solution helps users identify potential data breaches as well as risky user activities and manage insider risks. It leverages a unique combination of policy-free user activity monitoring, machine learning for behavior analysis, and real-time content inspection for proactive threat detection. The Next solution includes cloud-native, ML-powered functionalities that provide enhanced data loss prevention and threat prevention capabilities. The platform's Scoped Investigations empower organizations to meet employee privacy expectations and comply with information security regulations by providing only the relevant required information to security analysts for forensic analysis. Additionally, its AI capabilities enhance the accuracy and efficiency of data classification and data loss prevention strategies, ensuring sensitive information is accurately identified and adequately protected.

Proofpoint's Insider Threat Management (ITM) solution correlates activity and data movement, empowering security teams to identify user risk, detect insider-led breaches, and ensure accelerated security incident response. It allows organizations to identify insider risk activity and prevent data exfiltration, streamline the response to instances involving insider threats and data loss, minimize downtime to value with a highly scalable SaaS deployment driven by a modern cloud-native backend, and improve user productivity with a lightweight endpoint agent. Proofpoint ITM also provides a user watch-list feature that helps prioritize users based on risk tolerance and profile. It also helps customize the threat response environment by creating rules and triggers through the flexible rules engine feature.

Rapid7 offers an Insider risk management solution through its platform titled Insight IDR. The solution detects, prioritizes, and stops cyber threats in real-time and helps curb corporate data theft. Rapid7 InsightIDR offers comprehensive incident investigation and response capabilities that auto-enrich every log line with user and asset details and correlate security breach events across different data sources to form a pattern that will be used by algorithms in advanced threat

detection. InsightIDR Insight Agent integrates with the existing organizational network and security stack to collect threat data at the endpoints. Rapid7 InsightIDR utilizes network sensor data to investigate and create alerts based on the network traffic across the organizational environment.

SailPoint offers an Insider Risk Management solution through its Identity security platform and Non-Employee Risk Management, which combine to offer protection from insider risk and secure access from "non-employees/third parties." The solution helps mitigate cyber security risks by leveraging AI and ML capabilities to assign the required access to the right identities and technology resources at the right time. The identity security platform helps execute risk-based identity access and security lifecycle strategies for diverse non-employee entities.

Splunk offers Splunk UBA to curb insider risk and cyberattacks. The solution is equipped with risk-based alerting and streaming analytics feature, which provides data-driven user insights for full breadth visibility and rapid detection Splunk allows users to integrate SIEM and UBA to improve insider threat detection and uncover unknown threats in real-time. Splunk UBA leverages machine learning and advanced cyber threat detection to detect unknown threats, anomalous behavior, advanced threats, and hidden cyberattacks. Splunk UBA helps users gain enhanced threat visibility and detection through threat analysis and exploration by visualizing threats across a kill chain to obtain context.

Teramind offers an Insider Risk Management Solution through its Teramind Starter, Teramind UAM, and Teramind DLP platforms. Teramind incorporates Optical Character Recognition (OCR) technology that allows it to extract text from screenshots, emails, and documents within applications, providing a more comprehensive view of user behavior. Teramind offers productivity analysis feature which provides valuable insights into user work patterns and potential deviations that might be linked to malicious intent.

Vendors such as CounterCraft, Crisp, DTEX Systems, Ekran System, Elevate Security, Everfox, Exabeam, Fortinet, Gurucul, Human Security, IBM, Microsoft, OpenText, RSA, Securonix, and Veriato have been positioned as Strong Contenders. CounterCraft offers an Insider Risk Management solution through its CounterCraft platform, which leverages active defense technology for proactive threat detection. The CounterCraft Platform™ analyzes activity within deceptive environments and user behavior patterns to provide high-confidence alerts and enable prioritized Investigations. The solution provides Contextualized threat intel to detect malicious insider activity in the early stages of the threat cycle.

Crisp offers an Insider Risk management solution through the Crisp Corporate Risk Intelligence platform. The solution mitigates cyber security insider risks by discovering and tracking risk signals through its expert teams consisting of AI and humans. The Crisp platform provides Crisis Defense, which protects organizations from insider threats by delivering real-time alerts on emerging risks on social media as well as the deep and dark web. The platform also provides actionable alerts about any threats through its threat Defense capability, which leverages AI and ML algorithms to help identify risk signals embedded within the digital network.

DTEX Systems offers an integrated Insider Risk Management Solution through DTEX InTERCEPT. DTEX InTERCEPT leverages machine learning to offer comprehensive Entity Context and Peer Group Analysis, enabling the creation of user and entity profiles for every individual within the organization. The solution is equipped with various capabilities, including Insider Threat Management, User and Entity Behavior Analytics, Digital Forensics, and Zero Trust Endpoint DLP. DTEX InTERCEPT delivers context and intelligence to enable enhanced threat detection and mitigation.

Ekran System's insider risk management (IRM) platform offers a monitoring and activity investigation feature that provides key episode search, client protection, and session video recording capabilities. The platform offers predefined custom alerts that enable rule-based incident flagging. The platform leverages advanced analytics and machine learning to detect subtle behavioral anomalies that might signal malicious intent.

Elevate Security offers an Insider Risk Management solution through Elevate Engage, Elevate Control, and Elevate Identity products. Elevate Control utilizes adaptive user profiling to continuously update individual baselines as user activity patterns change. It actively delivers personalized feedback nudges, scorecards, and direct targeted training based on individual computing behaviors and current security risks. It also feeds contextual intelligence into security operations tooling and processes to accelerate incident triage and response for improved threat detection and mitigation.

Exabeam offers an Insider Risk Management solution through Fusion SIEM, which can integrate with XDR to create a cutting-edge SecOps solution to detect, investigate, and respond to external threats as well as compromised users in real-time. The solution offers automated investigation and response to help organizations in incident detection, triage, and investigation. It is equipped with machine learning-based Smart Timelines that automatically collect information, apply risk grading, and compile it into a cohesive narrative that may be utilized

to conduct an initial inquiryExabeam Fusion SIEM solution includes a centralized, highly scalable data storage that provides comprehensive visibility into the entire organizational IT ecosystem. Fusion SIEM offers centralized log storage, rapid intelligent search, compliance reporting, turnkey threat detection, investigation, and response capabilities, as well as prescriptive workflows and threat-specific content that can be built onto any security cloud platform.

Everfox (Forcepoint) offers a robust insider risk management solution through its Forcepoint Insider Threat and Risk Adaptive protection to protect user privacy and provide holistic visibility into behavioral patterns of users to detect insider threats. Forcepoint Risk Adaptive Protection's Autopilot comes with risk assessment that detects suspicious behavior by continuously collecting, enhancing, and connecting events. It gathers user behavior and DLP incidents before calculating the user's risk with Forcepoint's Indicator of Behavior (IOB) analytic models. This risk score is actively transmitted to DLP so that policy enforcement can be automated based on the risk level.

Fortinet provides robust Insider risk management through its FortiInsight solution, which leverages machine learning analytics for monitoring endpoints, data movements, and user activities to spot abnormal, malicious behavior and policy violations. The solution enables rapid threat detection by optimizing machine learning at each stage of the investigation pipeline and identifying emerging threats. The FortiInsight solution uses machine learning and advanced analytics to detect non-compliant, suspicious, or abnormal behavior and quickly alerts admins about any compromised user accounts. FortiInsight's robust rule-based engine can detect policy violations, unauthorized data access, and exfiltration to the cloud onto a local USB device.

Gurucul offers Gurucul Risk Analytics (GRA) to predict, detect, prevent, and deter insider threats in an enterprise and cloud environment. The Gurucul SIEM offers a peer-group analytics feature that allows both static and dynamic peer-group definition and analytics. It automatically organizes users to produce baselines based on regular user behavior and detects unexpected changes from peer group baselines. GRA utilizes big data and advanced machine learning algorithms to predict, identify, and prevent threats such as insider risk, data exfiltration, cyber fraud, privileged access abuse, and more. Gurucul provides a flexible entity model that integrates with behavior-based models to offer analysis of the overall risk across multiple telemetries to detect misuse or unauthorized access to any asset in the network. It helps monitor users as well as entities such as devices, servers, and machines and defines customized entity-based risk profiles.

Human Security offers insider risk management capabilities through its Human Defense Platform, which tackles insider threats by constantly monitoring login attempts and user activity to identify anomalies that could signal malicious insider intent. The platform leverages machine learning algorithms to continuously learn and adapt to evolving threats. This ability allows the platform to identify even the most sophisticated insider attacks, including those that attempt to bypass traditional security rules.

IBM offers Insider threat security through IBM QRadar User Behavior Analytics and IBM Security Verify Privilege Vault to protect organizations from insider threats. IBM Security QRadar offers integration with Security QRadar SIEM to provide insights and workflows with broader security operations toolkits. The IBM solutions leverage out-of-the-box behavioral rules and machine learning to discover malicious insiders and compromised credentials with real-time analytics, detect and protect all services, applications, and administrator and root accounts across the enterprise, and effectively assess insider threat processes. IBM QRadar leverages AI, pre-built playbooks, automatic root-cause analysis, and MITRE ATT&CK mapping to increase the investigation process regarding cyber threats.

Microsoft offers an Insider Risk Management solution through its Microsoft 365 Insider Risk Management platform. This solution identifies, investigates, and stops malicious and inadvertent activities in real-time. The Microsoft 365 Purview solution enables policy creation using a machine learning playbooks feature that helps create policies using configurable machine learning templates that do not require the deployment of scripting or endpoint agents. Microsoft 365 Insider Risk Management solution is equipped with privacy-by-design architecture that allows organizations to balance user privacy in the context of organizational risks. It enables organizations to configure policies based on industry, geographical, and business groups.

OpenText offers an Insider Threat Mitigation solution to detect insider threats in real-time. It leverages ArcSight Intelligence's behavioral analytics, which adds contextualization to help organizations analyze cyber threats. Additionally, the solution helps organizations detect fraud, data breaches, IP theft, insider risk, abuse, as well as advanced threats and optimize analyst productivity. Micro Focus ArcSight Intelligence allows intuitive, contextualized detection and investigation and provides downloadable reports that describe current threats.

RSA offers the NetWitness UEBA, which automatically detects and responds to threats in real-time while ensuring reduced dwell time. RSA NetWitness UEBA includes patented behavioral machine learning and key features like native data collection, a feature-weighting system, a simplified risk scoring engine, identity-context visualization, and reduction algorithms. The solution also provides a toolkit for investigating potential insider threats. This comprehensive set of tools includes detailed user profiles, encompassing historical activity data, access privileges, and role information. RSA NetWitness UEBA helps organizations minimize MTTD & MTTI, accelerate incident response, fewer false positives, enrich context based on identity, and quickly identify dangerous users. RSA NetWitness UEBA utilizes artificial intelligence and superior machine-learning models to baseline users and user groups, entities, and organization-wide behaviors, allowing true, actionable incident response to differentiate between normal, benign activities and malicious deviations.

Securonix offers a next-generation SIEM augmented by an industry-leading UEBA to detect and respond to both external and internal threats. The solution offers Entity Context and Peer Group Analysis, which leverages its Security Data Lake to create a comprehensive identity and risk profile for every user and entity within the user organization. Securonix's Next-Generation SIEM leverages log management as well as user and entity behavior analytics (UEBA) and security incident response to secure end-to-end security operations. It allows organizations to collect large volumes of data in real time with patented machine learning technology and offers artificial intelligence-based security incident response capabilities for quick remediation.

Veriato offers an Insider Risk Management Solution through the Veriato AI-Driven Insider Risk Detection platform, which provides AI-Based behavior analysis, Psycholinguistic Analysis, and Risk scoring to continuously track each user and automatically identify unusual or risky activity and compile various risk factors and signals into a risk score for each user monitored and on a single dashboard for enhanced Threat detection and prevention.

CyberHaven, Dasera, DoControl, and Secure Passage are the aspirants in the insider Risk Management market. These companies provide comprehensive technological capabilities and are rapidly gaining market traction across industries and geographical regions. All the vendors captured in the 2024 SPARK Matrix™ of Insider Risk Management vendors are emphasizing improving their capabilities to detect and stop risky behaviors and advanced insider threats in real time,

identify and control violations of corporate policies, monitor and manage data access governance issues, and enhance insider threat security. Additionally, these companies are looking to expand their partnership channels to support diverse use cases. Organizations are consistently looking to enhance their insider risk management products and expand support for multiple deployment options.

Key Competitive Factors and Technology Differentiators

The following are the key competitive factors and differentiators for the evaluation of Insider Risk Management solutions and vendors. While most Insider Risk Management solutions may provide all the core functionalities, the breadth and depth of functionalities may differ by different vendors' offerings. Driven by increasing competition, vendors are increasingly looking at improving their technology capabilities and overall value proposition to remain competitive. Some of the key differentiators include:

The Sophistication of Technology: Users should evaluate an insider risk management solution that alerts them during exfiltration events, determines risk tolerance, and self-adjusts to meet their users' desired tolerance levels. The solution should be easy to deploy, administer, and use with an intuitive UI. Additionally, the solution should support specific use cases, such as SAP security monitoring and Evaluation Assurance Level (EAL) 3+ certification, to meet the different organizational needs in various industry sectors. The solution must integrate with IAM, SIEM, and SOAR solutions to strengthen the IT infrastructure. Vendors should provide third-party integrations to enhance their solution's value. Additionally, the vendors' customer value proposition may vary in terms of ease of deployment, ease of use, price/performance ratio, support for a broad range of use cases, global support, flexible & elastic subscription service, and such others.

Integration and Interoperability: Users should consider insider risk management vendors that provide integration with SOAR, SIEM, PAM, UEBA, and such others and turn the data into comprehensive dashboards and search templates to analyze incidents and accelerate threat detection in real-time. Integrations with SOAR and UEBA solutions strengthen the internal security and SOC team productivity and help provide an end-to-end security platform. Integration with UEBA and SOAR capabilities also enables security teams to perform automated behavioral profiling by collaborating with IT and security systems to mitigate cyber incidents. Integration with common security IT technologies with prebuilt connectors helps perform effective threat detection, investigation, and response, while native integration with legacy security systems provides a comprehensive view of cyber threat exposure, manages non-employee and third-party resources, and replaces the existing custom-built systems, spreadsheets, and databases. Integration with intrusion detection/prevention systems (DS/IPS) and SIEM systems can create cyber security perimeters, enable threat intelligence sharing, and manage incident responses.

Scalability and Flexibility: An insider risk management vendor should offer a sophisticated solution that can detect and respond to insider threats across the increasing volume of users, including employees, vendors, and contractors, in real time. Additionally, the solution should be able to consume and process large amounts of data collected across channels without performance hindrance, extend its scalability to meet storage requirements, efficiently identify critical insider risks across organizations, and offer capabilities to remediate cyber threats and take appropriate actions effectively.

Identity Proofing: Organizations are looking for insider risk management vendors that provide identity proofing. Identity Proofing allows organizations to verify their identity using the user's life history credit report, biometrics (a facial scan), and other factors before granting them access to the organizational IT system. It strengthens user organizations' security posture by enabling applications to trust only verified users. Additionally, organizations are looking for insider risk management solution vendors that leverage user-friendly dashboards to create customized customer verification and authentication policies to establish digital trust within organizations.

Host and Network-based Sensors: Organizations are looking for Insider risk management solution vendors that can leverage host and network-based sensors (RUU) to identify discrete cyber-attack patterns or deviations from long-term user behavioral patterns. These sensors enable organizations to detect any malicious insider activity, achieve holistic security visibility into organizational IT systems, and consolidate and analyze security events from multiple IT sources.

Poly-cloud/Multi-cloud offering: Organizations should look for Insider Risk Management vendors that support advanced poly-cloud architectures, strengthening multi-cloud deployments, detection in cross-cloud environments, and responses across all common cloud stacks, including Amazon Web Services (AWS), Microsoft Azure, and Google Cloud platform. The insider risk management solution should support multi-cloud environments in IT systems, which allows organizations to enhance user experience, accelerate response to cyber threat detection, enable fast searches for better threat hunting, and ultimately reduce cost. Additionally, organizations are looking for insider risk management vendors that provide all the benefits to their SaaS customers with their own cloud infrastructure and can collectively imbibe their on-premises application and cloud infrastructure.

Identity-Centric Risk Modeling: Risk scoring assessment is critical for every organizational IT system for prioritizing threats. Organizations are opting for insider risk management vendors that provide identity-centric risk modeling, which allows organizations to create risk scores for every user who has access to the system. Organizations can leverage identity-centric risk modeling solutions to analyze every user, account, and entitlement and link them with their pending link analysis algorithms to present a holistic view (activity pattern) of every user. Additionally, organizations can also leverage identity-centric risk modeling to correlate information generated from user behavioral patterns to gain deep insights for investigations into the threat landscape.

Multilayered Analytics: Users should look for Insider Risk management vendors offering multilayered analytics. Multilayered Analytics enables organizations to detect insider fraud scenarios by leveraging a preconfigured set of business rules. Additionally, Multilayered Analytics utilizes the fraud analytics simulation tool to analyze the effect of business changes on organizations. Furthermore, Insider Risk Management solutions allow organizations to identify new features for fraud modeling.

Risk Response Automation: Users should look for Insider Risk management vendors offering the Risk Response Automation feature to streamline IT operations before deploying a bot for insider incident response management. An insider risk management solution allows organizations to automate risk response workflows with out-of-the-box, customizable playbooks to mitigate known insider threats. It should enable organizations to update the risk score in real-time according to changes in threat detection and risk levels. Additionally, organizations are also looking for insider risk management vendors that provide a response to Risk automation by leveraging governance, risk, and compliance (GRC), and enterprise risk management (ERM) tools and technologies, which allow organizations to manage risks programmatically and eventually meet compliance requirements, such as HIPAA, CMMC, or PCI.

Sentiment Analysis: Sentiment analysis is strengthening the IT industry in risk management and long-term decision-making. Sentiment analysis allows organizations to leverage natural language processing (NLP), computational linguistics, and text analysis to analyze the perception behind keywords or any text in the organizational IT system. Sentiment analysis detects malicious insider threats by enabling organizational IT systems to deliver productive insights to security analysts to alert them in the early stage of the threat cycle. Additionally,

sentiment analysis allows organizations to detect, monitor, and effectively report potential threats before any damage occurs to organizational IT systems.

AI-powered Deception Technology: Organizations are looking for vendors offering a flexible solution that can help create simulated environments or data to lure potential insider threats into revealing their malicious intent. Organizations can identify individuals attempting unauthorized access or data theft by strategically placing "honeypots" containing fake sensitive information. It employs machine learning to create dynamic and highly realistic decoy environments within the network. These deceptions mimic legitimate systems and data, tricking potential insider threats into interacting with them. The AI analyzes this interaction, identifying suspicious behavior patterns and alerting security teams in real time, allowing for swift intervention and investigation.

Insider Risk Management for Third-Party Access: Organizations are looking for vendors who can provide a flexible solution that helps tighten third-party access through granular Role-Based Access Control (RBAC), enforcing Multi-Factor Authentication (MFA), monitoring and potentially recording user sessions, securing API access points, and implementing DLP for shared data strengthens insider risk management by minimizing potential avenues for unauthorized access, data exfiltration, and misuse by third-party users with legitimate credentials.

Whole Person Insider Threat Management: Organizations are looking for vendors who can provide a flexible solution that goes beyond basic user profiling by considering a user's complete behavior. It should analyze both technical activity and behavioral patterns (including social and psychological factors) to predict and detect potential insider threats with greater accuracy. This holistic approach minimizes false positives and allows for targeted interventions to mitigate risks.

Entity Profiling: Organizations are looking for vendors who can provide a flexible solution that can help in monitoring beyond users, devices, servers, and machines. Flexible Entity profiling helps identify and profile sensitive files and documents as entities. It also helps monitor these files and documents along with other entities by integrating them with the user and entity monitoring feature. Entity profiling helps in granular monitoring and enhanced visibility into all profiled entities.

SPARK Matrix™: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix™ provides a snapshot of the market positioning of the key market participants. SPARK Matrix™ provides a visual representation of market participants and provides strategic insights on how each supplier ranks related to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact. Quadrant's Competitive Landscape Analysis is a useful planning guide for strategic decision making, such as finding M&A prospects, partnerships, geographical expansion, portfolio expansion, and similar others.

Each market participant is analyzed against several parameters of Technology Excellence and Customer Impact. In each of the parameters (see charts), an index is assigned to each supplier from 1 (lowest) to 10 (highest). These ratings are designated to each market participant based on the research findings. Based on the individual participant ratings, X and Y coordinate values are calculated. These coordinates are finally used to make SPARK Matrix™.

Technology Excellence	Weightage
Advanced Threat Detection	30%
User and device Monitoring	15%
Alert, Response Workflow, and Investigation	15%
Analytics, Dashboard, and Reporting	15%
Competitive Differentiation Strategy	10%
Integration & Interoperability	10%
Vision & Roadmap	5%

Customer Impact	Weightage
Product Strategy & Performance	20%
Market Presence	20%
Proven Record	15%
Ease of Deployment & Use	15%
Customer Service Excellence	15%
Unique Value Proposition	15%

Evaluation Criteria: Technology Excellence

- **Advanced Threat Detection:** The capability to proactively detect threats with the help of past data using ML algorithms and Identification of data breaches, privilege abuse, application misuse, unauthorized users, and risky inadvertent activities.

- **User and device Monitoring:** The capability to monitor behavioral patterns of all the Users, devices, and other IT resources within a Network to prevent data exfiltration through DLP policies.

- **Alert, Response Workflow, and Investigation:** The capability to implement automated incident investigation and response with uninterrupted workflow.

- **Analytics, Dashboard, and Reporting:** The capability of the solution to provide Analytics, Dashboard, and Reporting of High-Risk activity.

- **Competitive Differentiation Strategy:** The ability to differentiate from competitors through functional capabilities and/or innovations and/or GTM strategy, customer value proposition, and such others.

- **Integration & Interoperability:** The ability to offer a product and technology platform that supports integration with multiple best-of-breed technologies, provides prebuilt out-of-the-box integrations, and open API support and services.

- **Vision & Roadmap:** Evaluation of the vendor's product strategy and roadmap with the analysis of key planned enhancements to offer superior products/technology and improve the customer ownership experience.

Evaluation Criteria: Customer Impact

- **Product Strategy & Performance:** Evaluation of multiple aspects of product strategy and performance in terms of product availability, price to performance ratio, excellence in GTM strategy, and other product-specific parameters.

- **Market Presence:** The ability to demonstrate revenue, client base, and market growth along with a presence in various geographical regions and industry verticals.

- **Proven Record:** Evaluation of the existing client base from SMB, mid-market and large enterprise segment, growth rate, and analysis of the customer case studies.

- **Ease of Deployment & Use:** The ability to provide superior deployment experience to clients supporting flexible deployment or demonstrate superior purchase, implementation and usage experience. Additionally, vendors' products are analyzed to offer user-friendly UI and ownership experience.

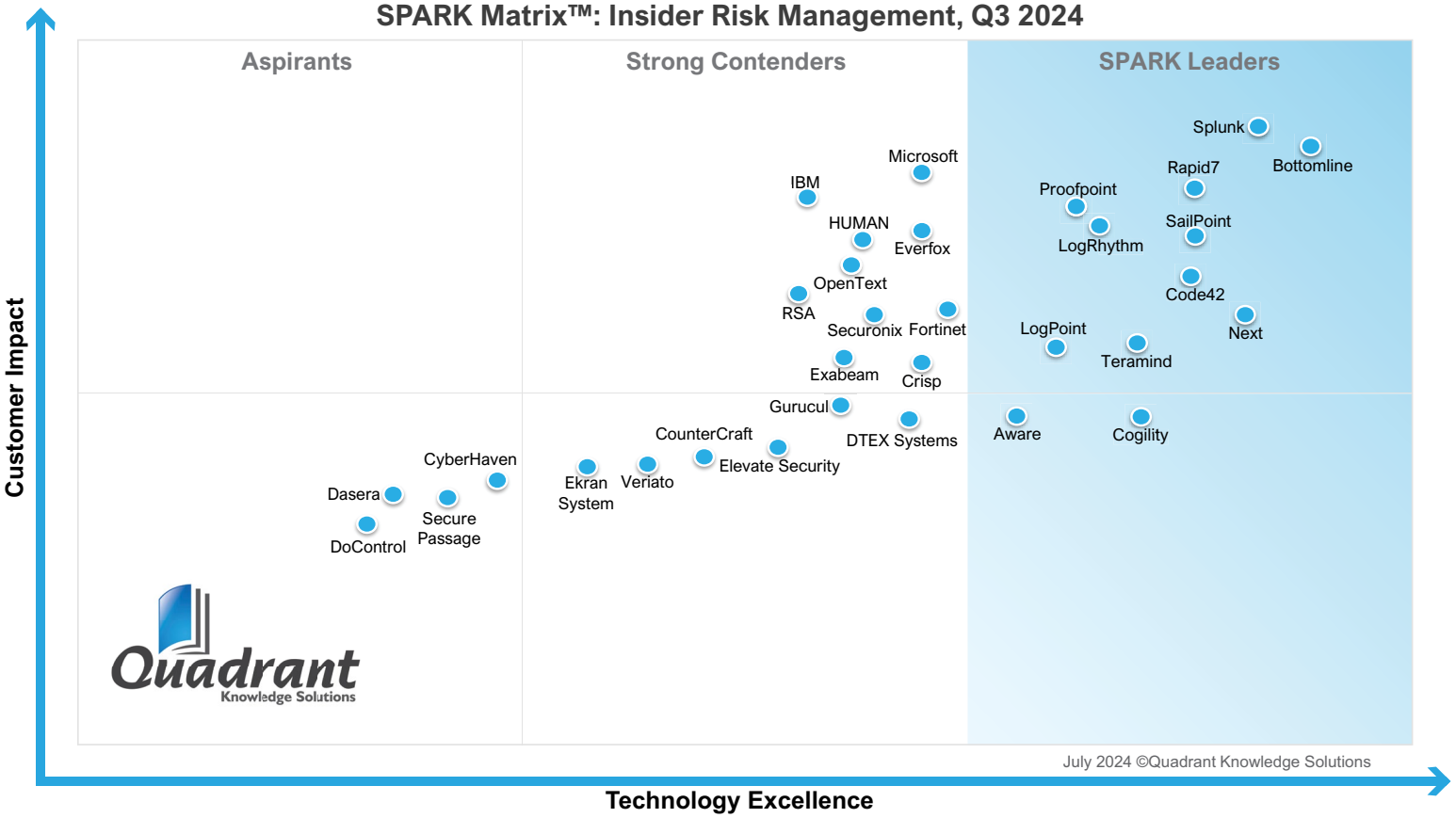
- **Customer Service Excellence:** The ability to demonstrate vendors capability to provide a range of professional services from consulting, training, and support. Additionally, the company's service partner strategy or system integration capability across geographical regions is also considered.

- **Unique Value Proposition:** The ability to demonstrate unique differentiators driven by ongoing industry trends, industry convergence, technology innovation, and such others.

SPARK Matrix™: Insider Risk Management, Q3, 2024

Strategic Performance Assessment and Ranking

Figure: 2024 SPARK Matrix™
(Strategic Performance Assessment and Ranking)
Insider Risk Management, Q3, 2024



Vendor Profiles

Following are the profiles of Insider Risk Management vendors with a global impact. The following vendor profiles are written based on the information provided by the vendor's executives as part of the research process. Quadrant research team has also referred to the company's website, whitepapers, blogs, and other sources for writing the profile. A detailed vendor profile and analysis of all the vendors, along with various competitive scenarios, are available as custom research deliverable to our clients. Users are advised to speak directly to respective vendors for a more comprehensive understanding of their technology capabilities. Users are advised to consult Quadrant Knowledge Solutions before making any purchase decisions, regarding know your customer technology and vendor selection based on research findings included in this research service.

Aware

URL: https://www.awarehq.com/

Founded in 2017 and headquartered in Columbus, Ohio, USA, Aware offers comprehensive AI solutions for governance, risk, compliance, and insights.

Aware's contextual intelligence platform uses AI and machine learning to identify and reduce risks, strengthen security and compliance, and uncover business insights from digital conversations. The platform can ingest data from a variety of collaboration tools, including Slack, Teams, Zoom, and Workplace from Meta. The Aware platform helps organizations identify and mitigate insider threats, ensure security and compliance, and gain valuable business insights from their digital communications. Aware can leverage AI and machine learning to process information from a wide range of collaboration tools to identify trends and relationships within the data.

Analyst Perspective

Key Differentiators

- Aware's platform offers comprehensive contextual intelligence that doesn't rely solely on predefined rules or alerts. Instead, it analyzes collaboration data and unstructured data like emails, chat messages, and documents in real-time, considering the context of each interaction and identifying potential insider threats more accurately. This analysis enables deeper insights, as it captures the true nature of communication.

- Unlike traditional solutions, Aware emphasizes behavioral analytics. It tracks user behavior patterns within collaboration tools to detect anomalies and deviations, including unusual file sharing, excessive data access, or suspicious communication. Aware tailors its AI models to analyze data for various functionalities to specific needs, such as preventing fraud, identifying insider threats, or ensuring regulatory compliance.

- Aware streamlines incident response with automated workflows through predefined actions, such as notifying relevant personnel, restricting access, or launching investigations, which helps in reducing manual intervention and enabling swift and effective response.

Product Strategy

- Technology Roadmap: Aware has added a risk assessment calculator among its features to insider risk, which helps IT, compliance, and risk teams quantify and mitigate the risks lurking within their collaboration data by delivering contextual intelligence. The calculator is the latest application designed by Aware to help organizations bolster their risk and compliance posture. By leveraging the Aware platform and backed by Aware's Future of Work benchmark research series, businesses can now receive insight into risks present in digital workplace conversations.

- Strategic Roadmap: Aware has entered a strategic partnership with Luminous, which designs and manufactures hardware for demanding generative AI inference applications. This collaboration harnesses Luminous' hardware to enhance Aware's data platform.

Market Strategy

- Geo-expansion Strategy: Aware has a strong customer base in North America, followed by EMEA. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: Aware caters to manufacturing, healthcare, banking & investment services, and the insurance sector.

- Use Case Support: Aware supports various use cases, such as acceptable use policy, content moderation, data back-up and Data Loss Prevention (DLP).

Customer/ User Success Strategy

- Aware offerings provide support for on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- Aware has established partnerships with various system integrators and third-party integrations, including Slack, Microsoft Teams, Workplace from Meta, Zoom, Outlook, Cisco Webex messaging, Google Drive, Workjam, and Viva Engage.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, Aware utilizes advanced data analytics and AI integration to process information from various collaboration platforms. This allows them to identify trends, risks, and sentiments within a company. Aware's platform is designed to be scalable and customizable for various business needs. For instance, Aware offers pre-built applications to address security and compliance concerns while also giving users the ability to create custom applications. Aware prioritizes user experience through a single pane of glass interface, allowing users to see information from various collaboration tools in one place.

Final Take

- Aware positions itself at the forefront of insider risk management with its focus on advanced technologies. By leveraging AI and real-time data analysis, Aware empowers organizations to proactively identify and mitigate potential threats within their communication channels. Its customizable platform offers both pre-built solutions and the ability to tailor risk management to specific needs. This, combined with a user-friendly interface, empowers security teams to make informed decisions and safeguard valuable data.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA and rapidly expanding in the JAPAC region, offering various use cases in industry verticals such as manufacturing, healthcare, and BFSI can choose Aware Insider Risk Management platform.

Bottomline

URL: https://www.bottomline.com/risk-solutions

Founded in 1989 and headquartered in Portsmouth, NH, USA, Bottomline is a provider of e-payment, invoice, and document automation solutions. Bottomline offers Payment Fraud, Case Management and Insider Threat Management (ITM) solutions that prevent malicious activities and protect users from advanced external attacks, insider threats, payment fraud, and money laundering.

The company offers a comprehensive threat detection solution, which minimizes risk by detecting anomalous user behavior and high-risk transactions in real time. The solution allows for the monitoring of real-time user activity, and its behavioral monitoring capability helps detect attackers and high-risk insider activity. The solution also utilizes machine learning to help identify irregularities, reduce false positives, and collect data from all channels for analysis, reporting, and investigations.

Analyst Perspective

Key Differentiators

- Bottomline Insider Threat solution is equipped with a complete enterprise financial crime prevention capability. Its screen recording feature captures data from screens and feeds it to the analytic engine to enable advanced threat detection. The solution records and replays user activity without invading employees' privacy. It also provides a Google-like search of the recorded sessions across multiple systems to allow forensic investigations to replay the activities and review the user actions.

- The Bottomline solution's configurable alert and case management capability provides extensive information, such as employee/account/customer profiles, anomalies, as well as visual replays of the recorded user session in which the suspicious activities were performed. This solution enables cases and alerts to be visible on dashboards with a flexible reporting engine and pre-defined reports.

- The Bottomline solution supports a wide variety of features, including SaaS application monitoring, which helps expand threat surface monitoring to mod-

ern SaaS applications and Monitoring Web applications using strong encryption.

- The solution utilizes cross-platform monitoring to identify and deter fraud and data theft. In addition, it is equipped with an analytics engine to provide statistical profiling of users and peer groups and alert correlation. It also includes predictive risk scoring, the ability to visually replay all user activity, and a key layer of security with extensive fraud analytics and behavioral tracking. Additionally, Bottomline's Insider Threat solution allows organizations to ingrain accountability in authorized users, move from transaction tracking to human behavior tracking, and enhance organizational security. These things are mainly performed by providing centralized visibility into user behavior across applications as well as discovering, analyzing, and documenting suspicious behavior using records and replies.

Product Strategy

- Technology Roadmap: Bottomline is focusing on building out internal threat management capabilities centered around its core Record & Replay capabilities. The Internal and Employee Fraud solution will be expanded into an industry-agnostic offering that can be deployed via public APIs and standard integrations for monitoring the most common core/sensitive applications.

- Strategic Roadmap: Bottomline's strategic roadmap is primarily focused on Internal threat management of the Fraud and Financial Crime group. Bottomline's R&D, sales, and marketing efforts will work to capture a greater share of this market and expand within the existing customer base through new, innovative offerings. It is also looking to expand its presence in the government and telecom domains.

Market Strategy

- Geo-expansion Strategy: Bottomline has a strong customer base in North America, followed by EMEA. The company plans to expand its presence in LATAM.

- Industry Strategy: Bottomline is expanding its offering in BFSI, Government & Public sector, Healthcare and Retail.
- Use Case Support: Bottomline focuses on various use cases, including pre-

venting financial crimes through misuse of credentials, snooping, policy/regulation/data breaches, and embezzlement.

Customer/ User Success Strategy

- Bottomline offerings provide support on-premises and cloud deployments. Its primary offering is on-prem but offers deployment flexibility for cloud and hybrid deployments.

- Bottomline's Record & Replay solution can be deployed within a single day. It also offers more robust implementations based on customer requirements. Bottomline's Managed Service deployments further reduce customer upkeep.

- Bottomline has established partnerships with channel partners such as DataDog and Trellix, providing pre-integrated Record & Replay capabilities. Bottomline also has different local channel partners in Australia, Taiwan, Cyprus, Hungary, Nigeria, South Africa, Spain, Italy, and Latin America.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- Bottomline's Insider Threat solution leverages AI and predictive analytics engine to provide deeper insights and decision-making. It is also investing in the continued adoption of the cloud for core, sensitive applications, and data through innovation around how to monitor applications, providing the tools to seamlessly maintain functionality while moving applications to the cloud. Bottomline's core technology for monitoring user activity is based on non-invasive network sniffing, which monitors access of employees to corporate data (including sensitive customer information) but does not invade employees' privacy as it does not monitor employee's activity on their own devices and the solutions are targeted at monitoring and protecting sensitive data without invading employee privacy.

Final Take

- Bottomline provides a robust insider threat management solution that leverages its expertise in real-time data capture and behavioral analytics. Powered by machine learning and enriched with years of experience protecting financial institutions, the solution goes beyond simple anomaly detection. It utilizes advanced analytics and AI to identify subtle deviations from user baselines, enabling organizations to proactively detect and mitigate potential insider threats before they escalate. Furthermore, Bottomline prioritizes scalability and customization through modular design, allowing organizations to tailor the solution to their specific needs.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA, and rapidly expanding in JAPAC region offering various use cases in industry verticals such as BFSI, government and public sector, healthcare and retail can choose Bottomline's Insider Threat management platform.

Code42

URL: https://www.code42.com/

Founded in 2001 and headquartered in Minneapolis, MN, USA, Code42 is a provider of data loss and insider threat protection. The company provides an Insider Threat solution through its Code42 Incydr data protection solution.

The company offers a comprehensive platform called Incydr, which helps organizations protect data without disrupting collaboration by offering full visibility into risk and distilling alerts to save analysts' time.

Code42 Incydr offers a wide range of features that include the Incydr Risk Exposure Dashboard, Risk Trends Dashboard, Incydr Risk Indicators, Response Controls, Watchlists, Forensic search, Cases, Security Integrations, Incydr Exfiltration detectors, and cloud-native SaaS architecture.

Analyst Perspective

Key Differentiators

- Code42 offers a SaaS-based insider threat solution that allows organizations to mitigate risks related to file accessibility and exfiltration without affecting employee productivity and communication capabilities. The solution's cloud-native SaaS architecture provides source code protection, enables real-time threat blocking, better access to exfiltrated files, and provides proven performance on Mac, Windows, and Linux machines, as well as easy browser visibility, visibility into Salesforce and no-gap file monitoring.

- The platform offers a forensic search feature for in-depth examination of event details and customized queries in a comprehensive, cloud-based activity metadata database. Incydr automatically sets up the Forensic Search parameters for insider threat investigations and allows users to create tailored searches based on critical activity factors. It aids in reviewing contextual metadata and file information by accessing files to validate content value, conducting swift customized queries, and executing saved searches.

- Incydr's Exfiltration Detectors feature enables organizations to detect data exfiltration from and within the cloud by Box, Google Drive, Microsoft OneDrive, Slack, Teams, Salesforce, Gmail, Microsoft 365

Product Strategy

- Technology Roadmap: Code42 is dedicated to advancing its data protection solution by integrating cutting-edge technologies such as machine learning, and advanced analytics. These enhancements aim to elevate user experience and enable more informed decision-making by predicting future outcomes based on comprehensive data analysis.

- Strategic Roadmap: Code42's strategic roadmap for insider threat solutions includes further strengthening its capabilities in threat detection, prioritization, investigation, and response. The strategic focus also extends to enhancing integration with existing security ecosystems and aligning with industry best practices to ensure robust protection against insider threats. This strategy is closely aligned with customer feedback and emerging threat landscapes to deliver proactive and effective solutions for mitigating insider risks.

Market Strategy

- Geo-expansion Strategy: Code42 has a strong customer base in the United States and is planning to expand its presence further in North America.

- Industry Strategy: Code42 is catering its offering in manufacturing, business services, life sciences, federal government, and software technology.

- Use Case Support: Code42 supports various use cases such as departing employees, remote workforce, IP theft, contractors, high-risk employees, lay-offs, shadow IT, source code detection, repeat offenders, Mac environments, reorganizations, mergers and acquisitions, security policy validation, and security awareness training.

Customer/ User Success Strategy

- Code42's offerings include cloud solutions with a deployment time of 2 weeks.

- Code42 has established partnerships with key technology vendors allowing enterprises to integrate their existing security solutions which helps in recognizing and responding to Insider Risk more quickly powered by integrations with Business applications, Cloud service, Data security, EDR/XDR, HCM, ITSM, PAM and IAM, SOAR, SIEM. Business applications supported by

Code42 include Gmail, Microsoft 365, Teams, Salesforce, and Slack. Cloud service integration supports OneDrive, Google Drive and Box with API-based integrations.

Trend Analysis

- The Insider Threat market is moving towards technological trends, which include advanced data analytics, organizational agility and resilience, customization, and scalability, focus on user experience and interactivity.

- In these spaces, Code42's data protection solution leverages advanced technologies such as predictive analytics to deliver deeper insights into threat landscape and facilitate informed decision-making. Code42's platform enhances threat detection capabilities, uses a robust prioritization model, and provides actionable intelligence to mitigate insider risks effectively.

Final Take

- Code42's data protection solution follows a comprehensive approach to mitigate insider threats within organizations through complete threat detection, prioritization, and response automation. Code42 empowers organizations to proactively identify and address insider threats, facilitating informed decision-making and effective risk management. The platform's user-friendly interface ensures an intuitive experience, enabling security professionals to navigate seamlessly and access pertinent insights for managing insider risks.

- Users looking for an Insider Threat solution that is easy to use and has a strong customer base in North America offering various use cases in industry verticals such as manufacturing, business services, life sciences, federal government, and software technology can benefit from the Code42 Incydr data protection solution.

Cogility

URL: https://cogility.com/

Headquartered in Irvine, California, USA, Cogility offers an end-to-end, whole person Counter- Insider Threat (C-InT) software solution built upon its integrated data stream processing and Expert-AI based behavioral analytic platform, Cogynt. The company helps automate insider risk management programs with comprehensive risk modeling, continuous monitoring and predictive scoring, analyst workflow, case management, and program visualization. Its C-InT platform goes beyond traditional security violation and anomaly monitoring by applying a whole-person approach that processes and analyzes technical data and behavioral data to identify potential risk indicator (PRI) patterns over time. A calculated whole-person risk score allows for prioritization. By continuously updating and analyzing an employee's PRI footprint, Cogility C-InT can detect, predict, and send alerts on explicit and high-risk insider threats and expedite analyst assessment and coordinated action – even before activities escalate into high consequence incidents.

Cogility C-InT provides insider threat management with a "single pane of glass" interactive view presenting high risk insider threats and facilitating case development processes with supporting evidence based on its extensible analytic engine. The solution offers diverse data source ingestion flexibility, high performance data processing, and no-code risk modeling to identify express and high probability threats dynamically correlated from PRI patterns like suspicious access, file transfers, communications, and privilege admin activities from technical data sources to more complex, longer-term PRI patterns determined from behavioral data such as HR, social media, law enforcement, and financial data sources. Identified insider threats include full traceability.

The customizable C-InT platform allows for quicker and more informed decisions about potential insider threats, at enterprise scale, enabling government entities and large commercial organizations to take preventative action and streamline response to mitigate risk.

Analyst Perspective

Key Differentiators

- Cogility's Counter-Insider Threat (C-InT) solution is built upon its Cogynt continuous intelligence platform, which allows for high-speed processing of massive volumes of data streams to determine actionable insider risk insights with full explainability. The Cogynt platform employs its patented Hierarchical Complex Event Processing (HCEP) technology designed to analyze data streams concurrently across multiple sources and diverse data types in real-time and at scale. It applies expert AI-based modeling to enable machine speed pattern matching analytics based on subject matter expertise while overcoming limitations in Artificial Intelligence (AI) solutions' ability to recognize infrequent events or complex threat indication patterns occurring over long periods of time, as well as AI bias and non-traceability effects.

- Cogynt provides a no-code authoring tool that facilitates expert-based pattern matching logic across technical and behavioral data sources to identify potential risk indicators that are combined hierarchically to determine insider risk. Cogility's C-InT system ships with a predefined set of insider threat risks, such as espionage, fraud, data extraction, and workplace violence. These are ascertained from weighted technological-based potential risk indicator patterns, such as security violations derived from endpoint, network, identity access, and physical data sources, and from weighted behavioral potential risk indicator patterns, such as job performance, personal history, and psychosocial data sources. Through the no-code authoring, the behavioral analytic logic can be further expanded, customized, and tuned. This wide variety of data feeds, consisting of both structured and unstructured data, is ingested, and assessed leveraging their Lexicon matching engine.

- Among numerous differentiators within its C-Int offering, Cogility has made advancements in applying the Sociotechnical and Organizational Factors for Insider Threat (SOFIT) ontology as a key component in structuring its Insider Threat potential risk indicators. Cogility can deliver a SOFIT-based model or create a new model. Incorporating the SOFIT standard within their proprietary HCEP modeling engine, Cogility has further advanced the state of the art in whole person insider risk detection.

- Cogynt's continuous, real-time insider threat risk analytics generates ex-

pressed and predictive findings with full supporting evidence. These findings are sent to Cogynt's Analyst Workstation for further investigation used to create case files that enable case managers to document an assessment and recommendation. This workstation tool provides tagging, custom fields and filters, and participant assignment and notifications to facilitate team collaboration and action workflow. Cogynt's case management functionality also supports remote case submission, review, and status tracking. A Business Intelligence (BI) dashboard tool enables operational oversight and performance visualization. This results in highly automated and efficient insider threat detection, risk modeling refinement, case workflow, and program management.

Product Strategy

- Technology Roadmap: Cogility will continue to invest in its Cogynt platform. Cogility is currently implementing additional AI capabilities, particularly LLMs for integration within its HCEP engine to further enhance its assessment of unstructured data, its no-code Authoring Tool, and its Analyst Tool experiences with new UI designs.

- Strategic Roadmap: Cogility is focused on enhancing authoring, case management, reporting, and predefined threat indicator modeling capabilities to extend its advantage for insider risk predictability and workflow. It is also looking to further extend platform integration within Virtual Private Cloud infrastructure to obtain even more internal data access and security signals to enhance its whole person Insider Risk approach.

Market Strategy

- Geo-expansion Strategy: Cogility has a strong customer base in United States and is planning to expand its presence in Canada, the UK, and Australia.

- Industry Strategy: Cogility is currently focusing on government agencies.

- Use Case Support: Cogility supports various use cases, such as the identification of indicators of risk, implementing insider potential risk indicator decay, indicator to threat type mapping, whole-person risk profiling, analyst assessment, case workflow management, performance reporting, and C-InT program business intelligence.

Customer/ User Success Strategy

- Cogility offerings provide support for the Private Cloud owing to its ability to streamline deployment and management of its C-InT solution within a customer's virtual private cloud (VPC) – negating data privacy and secure deployment concerns while achieving cost-effective operation and elastic scalability.

- Cogility has established partnerships with technological partners, such as Confluent for Apache Kafka, Cambridge intelligence for Re-graph, Amazon Web Services, and Google Cloud Platform for Cloud Services.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics, and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- Cogility's Inside Risk management solution applies its Expert AI and evolving AI LLM technology within its platform to generate comprehensive risk insights and streamline decision-making processes with full traceability. The solution performs continuous technical and behavior data processing, through its Hierarchical Complex Event Processing (HCEP) engine - incorporating an organization's existing technical security and psychosocial-based data without disrupting operations or requiring the replacement of existing controls. The C-InT solution also offers extensive analyst case assessment and coordination workflow features.

Final Take

- Cogility's Counter-Insider Threat Intelligence solution leverages its Expert AI-powered Cogynt platform for real-time analysis of massive, diverse data streams. The no-code authoring enables analysts, data scientists, and security teams to more easily tailor insider risk patterns to support on-going analysis across a vast array of potential risk indicator sources. By providing a baseline framework for advanced behavioral and technical PRI processing informed by the SOFIT standard, Cogility C-InT offers a comprehensive, whole person solution for insider threat identification, assessment, and case workflow - yielding an overall a more effective, predictive insider risk management program.

- Government agencies looking for a whole person approach based Insider Risk Management solution with a proven, flexible deployment at significant scale should consider choosing the Cogility Insider Risk Management solution.

LogPoint

URL: https://www.logpoint.com/en/

Founded in 2001 and headquartered in Copenhagen, Denmark, LogPoint provides a converged cybersecurity platform equipped with Log Point UEBA and SIEM solutions that help organizations safeguard themselves from Insider threats primarily.

The comprehensive insider risk management solution, offered through Logpoint UEBA, allows users to perform improved investigations of unexpected behavioral patterns and minimizes the time spent on threat hunting, detecting advanced threats early, and mitigating risk, damage, and data loss. It helps accelerate detection and response to threats by spotting early signs of suspicious patterns and anomalous behavior.

LogPoint SIEM captures the event data generated by any device, application, or endpoint within the infrastructure and enhances visibility into network and IT architecture by centralizing data monitoring. It simplifies user behavior and event analysis by converting complex log data into a single language and mapping warnings to MITRE ATT&CK. The data is then intuitively visualized and contextualized, enabling rapid detection and investigation of problems.

LogPoint UEBA offers a wide range of features, including holistic monitoring, threat detection and investigation, compliance adherence, automated response, industry-leading analytics, visibility to action, built-in playbooks & guided decisions, automated triage, log & telemetry collection, and enrichment.

Analyst Perspective

Key Differentiators

- LogPoint UEBA platform offers a log and telemetry collection and enrichment feature, which helps users monitor system-level behaviors of event logs and flat files. The feature also obtains information from applications hosted on servers, performs forensic investigations and threat hunting on endpoints and applications, and retains alerts for regulatory requirements, thus saving time and resources during audits. It also easily detects PCI violations by enriching logs with compliance standards. MITRE ATT&CK enrichment aids in obtain-

ing a more comprehensive context of TTPs employed by actors and signals throughout the Converged SIEM platform.

- The platform also offers an automated triage feature enrichment, augments the threat warnings with contextual information, such as threat intelligence, to determine the visual indication and tactics to detect threats earlier, enabling better threat investigation.

- The unified platform ensures a direct flow of information from SIEM to SOAR. It enables quicker detection and resolution of cyber threat incidents by collecting and prioritizing security data and threat alarms. It helps increase the efficiency of security teams by utilizing automated structured workflows for day-to-day tasks. LogPoint SOAR automatically gathers all cyber incidents and supporting data in one place, uses playbooks to drive analysts to faster conclusions, and enables analysts to communicate with internal security and SOC teams.

Product Strategy

- Technology Roadmap: LogPoint has announced the release of new capabilities to its Converged SIEM platform to enhance its threat detection and security operations and streamline case management. LogPoint expects the new release to reduce the workload on operational tasks, empowering SOC teams to gain efficiency in threat detection, investigation, and response.

- Strategic Roadmap: LogPoint's strategic roadmap focuses on delivering a complete SOC service and enhanced threat detection capabilities. LogPoint has partnered with SecurValue and IT-TOTAL to deliver more robust threat detection and response, real-time data analysis, early detection of data breaches, and easy implementation of compliance requirements by strengthening itself in Europe.

Market Strategy

- Geo-expansion Strategy: LogPoint has a strong customer base in Europe, followed by North America. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: LogPoint is expanding its offering in Manufacturing, Health-

care and pharma, Education, Retail, Public Administration, Critical Infrastructure, Hospitality Services and Financial Services domains.

- Use Case Support: LogPoint supports various use cases, such as Detecting compromised user credentials, detecting unusual behavior on privileged accounts, tracking system changes, secure cloud-based applications, phishing detection, monitoring loads and uptimes, log management, and threat hunting.

Customer/ User Success Strategy

- LogPoint offerings offer on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- LogPoint provides support for clients' on-premises installations. It also supports real-time monitoring of security controls, providing real-time data analysis for early detection of possible data breaches, data collection, data storage, and accurate data reporting. The built-in log analysis engine is configured to automatically detect and notify of all critical events in the customer's system, including operation awareness, system breakdowns and user authentication issues.

- LogPoint has established partnerships with various system integrators, third-party integrations, and key technology partnerships, including SecurValue, a Managed Security Service Provider (MSSP) that offers more robust threat detection and response, and IT TOTAL, a secure and customized IT infrastructure provider, facilitating complete SOC service based on Logpoint Converged SIEM with real-time monitoring, detection, triage, analysis, and management of known and unknown threats.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics & AI integration, organizational agility & resilience, customization, and scalability, focus on user experience & interactivity.

- In these spaces, LogPoint is committed to continuous innovation in insider risk management by leveraging advanced analytics, machine learning, and

AI technologies to enhance its offering's threat detection capabilities and improve response efficiency.

Final Take

- LogPoint's UEBA is a robust Insider Risk Management solution emphasizing operational excellence, process design, and automation. With advanced features such as behavioral analytics and real-time monitoring, the platform facilitates digital transformation, delivering improved security outcomes and enhanced organizational resilience. Equipped with predictive analytics and AI capabilities, LogPoint's platform empowers organizations to proactively identify and mitigate insider threats, driving informed decision-making and effective risk management. The user-friendly interface ensures an intuitive experience, enabling organizations to optimize their security posture and adapt to evolving threats.

- Users looking for an easy-to-manage Insider Risk management solution with a strong customer base in EMEA and North America, and is rapidly expanding in the JAPAC region, offering various use cases in industry verticals such as manufacturing, healthcare, and BFSI can choose the LogPoint UEBA platform.

LogRhythm

URL: https://logrhythm.com/

Founded in 2003 and headquartered in Boulder, Colorado, US, LogRhythm provides cyber security through Security Information and Event Management (SIEM), log management, network and endpoint monitoring and forensics, and security analytics. The company offers SIEM, Log Management, Security Intelligence, Multi-Dimensional Behavioral Analytics, Compliance Assurance, SIEM, Event Management, Big Data Analytics, Artificial Intelligence, Machine Learning, Compliance, and Machine Data.

The company offers Insider Risk management solution through its LogRhythm UEBA platform, which helps organizations detect user-based anomalies through machine learning and prioritize the findings for investigation and response. It also helps monitor unknown threats and behavioral changes in user data, thus offering essential visibility into user-based threats that would otherwise go undiscovered. The solution's key capabilities include threat detection and analysis, advanced user behavior analytics, case management, guided workflows and task automation, real-time network monitoring, security orchestration and log management.

Analyst Perspective

Key Differentiators

- LogRhythm offers a comprehensive insider risk management solution through LogRhythm UEBA platform, which provides threat detection and analysis feature that helps organizations improve threat detection by applying self-evolving ML algorithms for security across enormous, cloud-based centralized datasets. It helps detect insider threats, as well as other threats like account compromise, privileged account abuse, and misuse.

- LogRhythm UEBA offers a real-time network monitoring feature that collects data from users, networks, and hosts inside the environment to offer useful, contextual information that streamlines investigations. It is agentless and collects data and logs to monitor operating system and workload behavior across environments. It integrates with SIEM, EDR, and other security systems via plug-and-play, enabling broader threat detection, and providing comprehensive visibility across the user environment.

- LogRhythm UEBA provides a case management feature that centralizes investigations and allows safe collaboration. It allows users to create, escalate, and prioritize cases easily and allows the addition of collaborators and tracking of remediation activities. LogRhythm UEBA also offers a guided workflows and task automation feature, which automates numerous operations, enhancing productivity and accelerating incident response.

Product Strategy

- Technology Roadmap: LogRhythm has unveiled advanced capabilities for its cloud-Native SIEM Platform and LogRhythm Axon to streamline auditing for compliance standards and enable greater efficiency with security analytics mapped to MITRE ATT&CK use cases.

- Strategic Roadmap: LogRhythm has partnered with SOC Prime, combining LogRhythm Axon's analytics and threat management with SOC Prime's cutting-edge capabilities, which enhance threat detection and response. LogRhythm Axon empowers security teams to create and test custom threat detection rules tailored to their unique environments. The joint solution also addresses the challenge of alert fatigue by enabling security teams to fine-tune detection rules and prioritize responses based on accurate threat intelligence. By enhancing the precision of alerts, organizations can focus their efforts on mitigating real threats rather than sifting through overwhelming volumes of false positives.

Market Strategy

- Geo-expansion Strategy: LogRhythm has a strong customer base in North America, followed by EMEA.

- Industry Strategy: LogRhythm is expanding its offering in financial services, healthcare, legal, manufacturing, government, and utilities.

- Use Case Support: LogRhythm supports on various use cases, such as telecommunication security, detecting and responding to ss7 attacks, cybersecurity for higher education, securing telehealth systems and patient data, securing electronic healthcare records (EHRs) and protecting patient privacy, monitoring and defending medical devices in real-time, preventing account compromise with user and entity behavior analytics, protect privileged ac-

counts with LogRhythm's UserXDR, detecting a phishing attack with (PIE), rapid forensics, protecting critical assets from data breaches, detecting advanced threats (APTs), and such others.

Customer/ User Success Strategy

- LogRhythm offerings support include on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- LogRhythm has established partnerships with various partners to expand solution services, and leverage opportunities for better customer solutions and business growth. The major technological partners of LogRhythm include AWS, BeyondTrust, BlackBerry, Checkpoint, Broadcom, code42, cisco, Forescout, Fortinet, Mimecast, Proofpoint, VMware, and Zscaler.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, LogRhythm positions its insider risk management solution as a powerful tool that leverages advanced data analytics and AI integration. The company's platform ingests data from various sources, including user activity logs, network traffic, and security events. This comprehensive data set is then analyzed using advanced analytics and machine learning algorithms to identify subtle behavioral anomalies and potential insider threats. Additionally, LogRhythm prioritizes customization and scalability to cater to a wide range of organizations. The solution offers modular components, allowing organizations to tailor the platform to their specific needs and threat landscape. This might involve focusing on specific user groups or integrating with existing security tools. Furthermore, LogRhythm leverages cloud deployment options, ensuring scalability and easier maintenance for evolving security needs.

Final Take

- LogRhythm's insider risk management solution offers a security intelligence platform that seamlessly integrates advanced data analytics and AI which em-

powers organizations to gain a holistic view of user activity and potential insider threats. LogRhythm's platform ingests data from diverse sources, including user behavior logs, network activity, and security events. By leveraging machine learning and advanced analytics on this comprehensive dataset, LogRhythm pinpoints subtle anomalies in user behavior that might signal insider threats. Furthermore, LogRhythm prioritizes scalability and customization to cater to a wide range of organizations. Its modular solution allows organizations to tailor their insider risk management strategy to their specific needs and threat landscape. Finally, LogRhythm prioritizes user experience with intuitive interfaces, interactive dashboards, and customizable views which empowers security analysts of all experience levels to efficiently investigate potential insider threats and make informed decisions for risk mitigation, ultimately safeguarding critical information.

- Users looking for an easy-to-use insider risk management solution with a strong customer base in North America, EMEA and rapidly expanding in the JAPAC region and supporting various use cases in industry verticals such as financial services, healthcare, legal, manufacturing, government, and utilities, can choose LogRhythm's Insider Risk Management platform.

Next DLP ("Next")

URL: https://www.nextdlp.com/

Founded in 2020 and headquartered in London, UK, Next DLP ("Next") is a global provider of insider risk and data loss prevention solutions. The company's solutions include various functionalities, including data protection, insider risk, data loss prevention, security education, compliance, privacy, and user behavior analytics.

Next offers an Insider Risk Management and Data Loss Prevention solution through its Reveal Platform. The solution helps organizations identify potential data breaches, risky user activities, and manage insider risks. Next's Insider Risk Management solution (Reveal) offers cloud-native, ML-powered functionalities that provide enhanced data loss prevention and threat prevention capabilities.

Analyst Perspective

Key Differentiators

- Next offers a comprehensive Insider Risk Management solution that offers policy-free user-activity visibility and policy-free agent deployment and helps in documenting activities including file, process, clipboard, network, browser, email (outbound), print and removable media activity. The resulting activity dataset and related insights help identify data exposure risks such as SaaS app usage, policy implementation, and assess policy efficacy. The solution also leverages ML models on the endpoint to baseline and identify changes in user behavior to flag and provide context around observed high-risk activity focused on sensitive data and IP.

- The Reveal Platform offers an end-to-end solution that helps secure corporate data across all devices (unmanaged and managed) by combining Insider Risk Management, Data Loss Prevention (DLP), and Cloud Data Security into a single, streamlined solution.

- Reveal's Insider Risk Management solution monitors and analyzes user behavior to proactively identify potential insider threats, ensuring that sensitive information is safeguarded against both unintentional and malicious internal breaches. For Data Loss Prevention, the Reveal Platform employs advanced

algorithms and machine learning techniques to prevent sensitive data from leaving the organization, protecting both in-motion and at-rest data across various endpoints. Reveal Beyond extends these protective measures to the cloud and unmanaged devices, enabling organizations to securely use cloud applications and protect data on personal devices.

- Next's Reveal Platform allows organizational IT systems to perform real-time, on-device content inspection, which enables organizations to analyze data when it is in active use. It also offers adaptive controls, which allow users to decide how to respond to any detected endpoint action that makes data vulnerable to breaches.

- Next's Reveal Platform enables contextual inspection by identifying sensitive data in both structured and unstructured formats without any predefined policies, which includes the location of data in the case of design documents, source code, and financial reports. Reveal collects telemetry data from system, user, and network events on the endpoint through Policy free deployment providing insights into how endpoints are being used.

Product Strategy

- Technology Roadmap: Next is implementing different product enhancements, such as the XTND AI (ML and LLM) model, which will help automatically sequence high-risk data loss activity, including novel and anomalous detections, into risk-scored incidents for prioritized investigations, SaaS Access Security integrated module which audits and risk scores SaaS and GenAI apps; tracks data and delivers insights into credential usage and associated account takeover risks and Reveal Beyond for O365 and Google Workspace cloud drive connectors which helps in gaining visibility and control over the movement, sharing and exfiltration of business data from corporate cloud drives across managed and unmanaged devices, including personal smartphones, tablets and PC devices.

- Strategic Roadmap: Next's strategic roadmap for its Insider Risk Management product focuses on innovation within the solution space driven by a deep understanding of evolving challenges. Next's R&D is leveraging cutting-edge technologies like AI and machine learning with an emphasis on the development of proprietary algorithms and models, integration with existing security ecosystems, and the generation of actionable intelligence.

Market Strategy

- Geo-expansion Strategy: Next has a strong customer base in North America, followed by EMEA.

- Industry Strategy: Next is expanding its offering in BFSI, healthcare, computer hardware and software, manufacturing, retail, telecommunication, eCommerce, food and beverages, transportation, and entertainment sectors.

- Use Case Support: Next focuses on various use cases, such as detecting, responding and investigating deliberate data exfiltration, preventing data loss, educating users and changing behavior, capturing forensic data and SaaS application inventory, data flow mapping, and risk assessment.

Customer/ User Success Strategy

- Next's offerings provide cloud deployment. Its primary offering is cloud-based, but it also offers deployment flexibility for SaaS and hybrid deployments.

- Next has established partnerships with various technological vendors such as Splunk for more effective incident response and investigation, Microsoft {Microsoft Information Protection (MIP)} for enhancing data security and compliance, and Torq.io to combat insider risk through heightened detection and automated response actions.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, the Next Insider Risk Management solution leverages advanced algorithms and machine learning models to automatically identify and respond to potential data breaches and vulnerabilities in real time by integrating AI into Reveal. Additionally, AI capabilities in Reveal enhance the accuracy and efficiency of data classification and loss prevention strategies, ensuring sensitive information is accurately identified and adequately protected. Next Reveal also offers scalability, flexibility, and the ability to protect data across

multiple cloud services and platforms, addressing the unique challenges posed by cloud environments. Additionally, Reveal's Scoped Investigations empower organizations to meet employee privacy expectations and comply with information security regulations by limiting the information accessible to security analysts for forensic analysis by default. Scoped Investigations grants time-bound, revocable, and audited data access to allow comprehensive investigations by authorized personnel only.

Final Take

- Next Reveal is a robust Insider Risk Management solution. It leverages a unique combination of policy-free user activity monitoring, machine learning for behavior analysis, and real-time content inspection for proactive threat detection. This empowers organizations to identify and mitigate insider risks, protecting sensitive data from both intentional and unintentional breaches. Furthermore, Next Reveal's user-centric approach and focus on data privacy compliance solidifies its position as a technically robust and user-friendly solution.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA regions, and offering various use cases in industry verticals such as BFSI, healthcare, computer hardware and software, manufacturing, retail, telecommunication, eCommerce, food and beverages, transportation, and entertainment can choose Next's Reveal Platform.

Proofpoint

URL: https://www.proofpoint.com/us

Founded in 2002 and headquartered in Sunnyvale, CA, USA, Proofpoint offers software as a service-enabled products for email security, data loss prevention, electronic discovery, and email archiving that help users protect their digital assets and mitigate risks.

The company offers a comprehensive Insider Risk Management solution through its Proofpoint Insider Threat Management (ITM), which protects users against data loss and brand damage arising out of insiders acting maliciously, negligently, or unknowingly. The solution correlates activity and data movement, empowering security teams to identify user risk, detect insider-led breaches, and ensure accelerated security incident response.

Proofpoint's ITM solution offers a wide range of features, including people-centric user risk analysis, insider threat detection and analytics, accelerated insider threat response, an extensive cloud-native platform, user watchlists, a flexible rules engine, an alert library, content scanning and data classification, a unified console, point-and-click threat hunting, and alert triage.

Analyst Perspective

Key Differentiators

- Proofpoint Insider Threat Management (ITM) solution offers an accelerated insider threat response feature that creates workflows and evidence for user-driven events throughout the digital productivity stack. The feature simplifies the investigation process by providing contextual evidence of the incident, endpoint-specific remediation options, as well as automated alerts and responses with specific business units possessing SOAR and SIEM integrations.

- Proofpoint ITM's unified console platform collects data from endpoints, email, and the cloud to deliver multichannel visibility in a single location. This ability facilitates insider-led investigations and responses against cyberthreat intrusion into organizational IT systems. The console offers simple visualizations to aid in user activity monitoring activities, correlating alarms, managing investigations, hunting for risks, and coordinating incident response.

- Proofpoint ITM has an extensible cloud-native platform, which is equipped with API-driven modern architecture that is built for scalability, security, privacy, and flexibility in deployment. The platform helps comply with regional data mandates. In addition, it provides global deployment options as well as industry-leading granular access controls.

- Proofpoint ITM provides a user watch-lists feature that helps prioritize users based on risk tolerance and profile. These watch lists can be based on factors such as the user role's sensitivity and the data they access. They can also be based on the user's susceptibility to phishing and other forms of social engineering. Criteria can also be based on the user's location, changes in their position, and other employment and legal considerations.

Product Strategy

- Technology Roadmap: Proofpoint has launched many industry-first innovations over the last year. These innovations include Industry-first LLM-based Pre-delivery Threat Detection to prevent initial compromise; Generative AI-based Analysis for Powerful Threat Insights Across the Attack Chain through Proofpoint Security Assistant; and Defending Against Data Exfiltration through Misdirected Email to detect more attacks pre-delivery, quantify the impact of compromised identities, and improve the efficiency of defenders responding to data loss.

- Strategic Roadmap: Proofpoint has acquired Tessian, a leader in the use of advanced AI to automatically detect and guard against both accidental data loss and evolving email threats. The core focus of this acquisition is to drive added effectiveness against the full range of human-targeted threats, from social engineering to malware to credential phishing.

Market Strategy

- Geo-expansion Strategy: Proofpoint has a strong customer base in North America, followed by Europe. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: Proofpoint is expanding its offering in federal, state, and local government, higher education, financial services, healthcare, mobile operators, internet service providers, and small and medium businesses domains.

- Use Case Support: Proofpoint supports various use cases, such as combating email and cloud threats as well as data loss and insider risk, preventing loss from ransomware, defending remote workforces, protecting cloud-based apps, and managing insider risk.

Customer/ User Success Strategy

- Proofpoint offers multiple deployment options, including on-premises and cloud solutions. Its primary offering is cloud-based but offers flexibility for on-prem and hybrid deployments.

- Proofpoint has established partnerships with various system integrators and third-party integrations. The company's key technology partners include CrowdStrike, Palo Alto Networks, Okta, Sentinel One, AWS, Splunk, IBM, ServiceNow, and CyberArk. These partnerships allow easy integrations with the users' existing security solutions and allow accelerated o detection and response to insider risk with multi-layered protection, accurate, timely response to credential phishing attacks, coordinated detection and protection throughout network, endpoints, cloud, email, and social media platforms, a people-centric approach to protect privileged users, threat intelligence and multi-layered detection and response for malicious file from email to the endpoint, automating remediation tasks, enhancing customer protection against data loss, compliance outcomes, visibility and correlation of email, social, and network-based threats with additional data sources and mitigating the risks in internet email communications.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics & AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, Proofpoint's solutions stand out by leveraging advanced data analytics and AI integration to proactively address emerging trends. Proofpoint utilizes AI-driven algorithms to enhance its threat detection capabilities, enabling organizations to effectively identify and mitigate insider risks. Proofpoint offers customizable and scalable features that ensure adaptability and effectiveness in mitigating insider threats across different environments.

Proofpoint also provides enhanced collaboration features through cloud technology, facilitating seamless communication and coordination among security teams while offering cost efficiencies and streamlined updates. Moreover, Proofpoint prioritizes user experience by designing intuitive interfaces, interactive dashboards, and customizable views, allowing security professionals to navigate the platform effortlessly and leverage actionable insights for effective insider risk management.

Final Take

- Proofpoint's insider risk management solution integrates advanced features such as predictive analytics and Generative AI, enabling digital transformation and driving superior business outcomes with heightened customer value. Proofpoint ensures an intuitive experience, empowering informed decision-making and effective optimization of security protocols by offering user-friendly interfaces. In essence, Proofpoint's platform caters to advancing insider risk management, continuous improvement tailored to meet the evolving security needs of modern enterprises.

- Users looking for an Insider Risk Management solution that is easy to use and has a strong customer base in North America, EMEA and is rapidly expanding in the JAPAC region, offering various use cases in industry verticals such as federal, state, and local government, higher education, financial services, healthcare, mobile operators, internet service providers, and small and medium businesses.

Rapid7

URL: https://www.rapid7.com/

Founded in 2000 and headquartered in Boston, MA, USA, Rapid7 offers a range of information security solutions and services, including threat intelligence, managed services, detection and response, cloud security, and vulnerability management products.

The company offers an Insider risk management solution through its platform InsightIDR to detect, prioritize, and stop malicious cyber threats in real time.

Rapid7 InsightIDR enables organizational security teams to view insider data through customized dashboards. It also allows internal security and SOC teams to detect and prioritize the most critical Insider Risk Indicators (IRIs). InsightIDR helps organizations monitor high-risk events and other cyber threats in the same control plane and blocks the threats in real-time with its data collection source Incydr in the InsightIDR. Rapid7 InsightIDR validates important file modification events and suspicious user activity in real time, providing compliance and file integrity monitoring (FIM). It also detects unauthorized access from external and internal malicious threats and highlights abnormal activity to minimize the analysis of data streams.

Analyst Perspective

Key Differentiators

- InsightIDR leverages both internal and external threat intelligence to cover the whole post-perimeter attack surface for enhanced threat detection. InsightIDR is equipped with a threat detection library that contains threat data scenarios from Rapid7's open-source community, as well as proprietary machine learning to ensure enhanced attack surface mapping. The library also has Attacker Behavior Detection rules (ABA), which help users gain more knowledge about the alerts generated by User Behavior Analytics.

- InsightIDR offers easy-to-deploy deception technology that allows users to create more traps, including honeypots, honey users (fake users not associated with a real person within the organization), as well as honey credentials, and honey files, to identify malicious behavior earlier in the attack chain. It

helps deploy and manage intruder traps easily, catch the use of stolen credentials, and gain file-level visibility.

- Rapid7 InsightIDR offers comprehensive incident investigation and response capabilities which auto-enrich every log line with user and asset details and correlate security breach events across different data sources to form a pattern that will be used by algorithms in advanced threat detection. Every alert creates a detailed, intuitive, visual investigation timeline.

Product Strategy

- Technology Roadmap: Rapid7 has added a new capability titled cloud anomaly detection. This AI-powered, agentless detection capability is designed to detect and prioritize anomalous activity within an organization's cloud environment. The proprietary AI engine continuously learns and adapts to the customer's environment, surfacing suspicious behavior and automatically suppressing benign signals to reduce noise. This ability results in a significant reduction in false positives and enables teams to focus on investigating and responding to active threats. When such activity is identified, native automation within the Rapid7 platform can immediately adjust configurations, right-size permissions, and privileges, and integrate SOC, engineering, and IT teams into incident investigations.

- Strategic Roadmap: Rapid7's strategic roadmap focuses on enhancing threat exposure management through deeper threat intelligence integration and proactive mitigation strategies. The company is expanding its SOAR platform for automated incident response and investing in cloud security solutions. Additionally, the company will continue the development of its XDR solution with a focus on UEBA and user experience improvements through automation and AI/ML integration. Expansion into new security domains and industry verticals, along with strategic partnerships and adoption of emerging technologies like AI and blockchain, are also part of their roadmap.

Market Strategy

- Geo-expansion Strategy: Rapid7 has a strong customer base in North America, followed by EMEA. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: Rapid7 is expanding its offering in energy, financial services, government, education, retail, and healthcare.

- Use Case Support: Rapid7 focuses on various use cases, such as security data visualization, compromised user detection, monitoring remote workforce, investigations, and incident response, containing compromised users and assets, compliance regulations, and streamlining case management.

Customer/ User Success Strategy

- Rapid7 offerings support on-premises and cloud deployments. Its primary offering is cloud-based but offers flexibility for on-prem and hybrid deployments.

- Rapid7 InsightIDR offers integrations with SIEM and EDR to help organizations analyze the complex user log data and find insights quickly by natively-cloud data lake, diverse log collection capabilities, custom log parsing, and flexible search and reporting. It also uses a detection-first approach with the Insight Agent that drives reliable endpoint threat detection and spots attacks early.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, Rapid7 confronts insider threats by leveraging its security data lake and User Behavior Analytics (UBA) for deep analysis of user activity data, allowing security teams to pinpoint anomalies indicative of malicious intent. Rapid7's platform enables organizations to define risk profiles and user behavior baselines specific to roles, permissions, and access patterns, leading to more precise threat detection and fewer false positives. Additionally, cloud deployment empowers collaboration and information sharing across security teams, while Rapid7 prioritizes user experience through intuitive interfaces and interactive dashboards designed for efficient insider threat investigation and risk mitigation.

Final Take

- Leveraging its comprehensive security data lake and advanced User Behavior Analytics (UBA), Rapid7's powerful insider risk management platform empowers security teams to gain a deep understanding of user activity and identify potential threats with exceptional precision. Rapid7 also prioritizes customization, allowing organizations to tailor risk profiles and user behavior baselines to their specific environment. This meticulous approach minimizes false positives and streamlines threat detection. Furthermore, Rapid7 embraces cloud deployment, fostering seamless collaboration among security teams and ensuring automatic updates. By prioritizing user experience with intuitive interfaces and interactive dashboards, Rapid7 empowers security analysts to investigate and mitigate insider threats efficiently, safeguarding critical data and enhancing overall security posture.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA and rapidly expanding in JAPAC region offering various use cases in industry verticals such as security data visualization, compromised user detection, monitoring remote workforce, investigations, and incident response, containing compromised users and assets, compliance regulations, and streamlined case management can opt for Rapid7 Insider risk management solution.

SailPoint

URL: https://www.sailpoint.com/

Founded in 2005 and headquartered in Austin, Texas, USA, SailPoint is a global provider of identity security, insider risk, threat intelligence, data governance and solutions for corporations, financial institutions, and other industries. SailPoint acquired identity solutions startup SecZetta to provide comprehensive identity security solutions for non-employee identities. SailPoint offers third-party identity risk, access risk management, and identity security platform solutions to help organizations identify and mitigate security threats and insider risks.

SailPoint offers Insider Risk Management through its Identity Security Cloud platform and Non-Employee Risk Management which combinedly protects from insider risk from employees and secure access from "non-employees/third-party". Both the solutions help organizations mitigate cyber security risks by leveraging their AI and ML capabilities to automate access management and control, delivering the required access to the right identities and technology resources at the right time. Third-party identity risk solution help organizations execute risk-based identity access and security lifecycle strategies for diverse non-employee entities.

Analyst Perspective

Key Differentiators

- The SailPoint solution's governing and managing feature, equipped with AI and ML capabilities, helps users get actionable intelligence about insider threats. This intelligence, enriched with AI, helps provide access recommendations. It also helps analyze access controls and SOD (Segregation of Duties) risks by users, roles.

- SailPoint helps efficiently discover and manage user access with artificial intelligence (AI) through its identity security platform, which helps in user protection with the power of AI-Driven Identity Security composed of components such as Access Modeling, Identity Outlier Detection, and Access Recommendations. These capabilities help enable simplified role management, insightful identity intelligence, and informed access decision support for improved insider security.

- SailPoint identity security platform helps extend identity security to critical unstructured data and in governing cloud entitlements through its SaaS based data governance solution, Data Access Security. It helps organizations discover, visualize, manage, monitor, govern, and remediate access across different cloud entitlements such as Microsoft Azure, AWS, and Google Cloud Platform.

Product Strategy

- Technology Roadmap: SailPoint is focusing on integrating AI and machine learning for risk-based access control and data security. Additionally, it is developing improved SaaS connectivity and visualization tools to simplify identity governance and offer enhanced user experiences.

- Strategic Roadmap: SailPoint's strategic roadmap prioritizes a next-generation Identity Security platform that strengthens security and compliance across cloud and on-prem environments. This roadmap emphasizes user-centric design for simplified access management, including features like time-bound requests and flexible entitlements. By focusing on both security and user experience, SailPoint aims to accelerate adoption and maximize the value proposition of its IGA solutions.

Market Strategy

- Geo-expansion Strategy: SailPoint has a strong customer base in North America, followed by EMEA and Asia Pacific.

- Industry Strategy: SailPoint is expanding its offering in financial services, education, healthcare, education, manufacturing, and government & public sectors.

- Use Case Support: SailPoint focuses on various use cases, such as compliance, insider threat detection, mitigating cyber risk, embracing zero trust, as well as securing and enabling work from anywhere.

Customer/ User Success Strategy

- SailPoint offerings provide support for on-premises and cloud deployments. Its primary offering is SaaS-based but offers deployment flexibility for on-

prem and hybrid deployments.

- SailPoint has established partnerships with various technological partners, such as Accenture, AWS, Deloitte, Optiv, and PWC, to deliver the expertise, experience, and results its customers expect for identity security.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- SailPoint positions itself well within the evolving insider risk management landscape owing to the following factors. The company's focus aligns with key trends like AI and machine learning utilization. SailPoint's solutions leverage activity data to analyze user activity and data access patterns for risk-based access control, potentially identifying anomalous behaviors indicative of insider threats. Furthermore, SailPoint's Identity Security Cloud platform boasts scalability and a modular design. This allows organizations to customize access controls and risk management features to their specific needs and industry regulations. Additionally, SailPoint's SaaS-based platform, evidenced by its focus on SaaS integrations, fosters collaboration between security teams and simplifies security updates. SailPoint's solutions offer a user-friendly interface, interactive dashboards, and customizable views tailored for different security roles within an organization.

Final Take

- SailPoint's insider risk management solution, Identity Security Cloud platform, leverages machine learning for access anomalies and combinations that do not match overall access to identify outliers to mitigate potential insider threats. The platform's scalability and modular design enable organizations to tailor access controls and risk management features to their specific industry regulations and needs. Furthermore, SailPoint's SaaS-based approach fosters collaboration between security teams and simplifies security updates. By prioritizing user experience through a user-friendly interface, interactive dashboards, and customizable views, SailPoint empowers security professionals with the tools they need to make informed decisions and optimize their organization's insider risk posture.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA, JAPAC region, offering various use cases in industry verticals such as financial services, education, healthcare, education, manufacturing, and government and public sectors can choose SailPoint Identity Security platform.

Splunk (a Cisco Company)

URL: https://www.splunk.com/

Founded in 2003 and headquartered in San Francisco, CA, USA, Splunk is a leading provider of cybersecurity solutions that enable organizations to record, index, and correlate real-time data in a searchable repository, from which graphs, reports, alarms, dashboards, and visualizations can be generated. Splunk's products utilize ML data to find data patterns, provide metrics, diagnose problems, and provide intelligence.

The company offers a comprehensive Insider risk management solution through its Splunk UBA product to help organizations identify and respond to security threats quickly and effectively. The solution enables organizations to protect themselves against unknown threats. It helps observe anomalous behavior to identify threats and prevent security incidents before they cause irrevocable damage through early and rapid behavior-based detection.

Splunk UBA offers various features, including advanced threat detection, accelerated threat hunting, risk-based alerting, and streaming analytics, a unified security operations platform, incident investigation and forensics, as well as enhanced visibility and detection.

Analyst Perspective

Key Differentiators

- Splunk's UBA solution is equipped with risk-based alerting and streaming analytics feature, which provides data-driven user insights for full breadth visibility and rapid detection. The feature minimizes data silos and absorbs data from multi-cloud and on-premises deployments to help users gain actionable threat intelligence. The solution also provides a risk index, which is prepared on the basis of risk score, MITRE ATT&CK, and outliers. It is observed by correlations and analytics to prepare risk incident rule alerting, which helps in the identification of risky users.

- Splunk UBA can integrate with Splunk SOAR and Splunk Enterprise security to automate repetitive tasks and get data-driven insights to gain full visibility into user activity.

- Splunk UBA's Incident investigation and forensics feature helps organizations combat threats at scale with the help of powerful analytics by leveraging automated investigation and response to data breach incidents. It detects harmful behavior as it occurs and quickly initiates an investigation to detect and prevent cyberthreat intrusion. It also has Data alarms from different sources to establish a contextual view of an incident and automate investigations for speedy insights and answers.

Product Strategy

- Technology Roadmap: Splunk is focusing on integrating AI capabilities and advance analytics, and simulation capabilities to accelerate detection, investigation and response across its security and observability offerings.

- Strategic Roadmap: Splunk has been acquired by Cisco to bring together global developer and partner communities with extensive experience extending security, observability, and data platform capabilities with pre-packaged applications and solutions. The company's collective partner ecosystem can create new profitable revenue streams through high-value services and by deploying innovative new applications and AI-powered solutions. The company intends to add a number of new product innovations across the portfolio over the next several months.

Market Strategy

- Geo-expansion Strategy: Splunk has a strong customer base in North America, followed by EMEA. The company is now planning to expand its presence in Asia Pacific.

- Industry Strategy: Splunk is expanding its offering in manufacturing, financial services, public sector, retail, online services, and communications.

- Use Case Support: Splunk supports various use cases such as advanced threat detection, application modernization, cloud migration, IT modernization, SOC automation, and orchestration.

Customer/ User Success Strategy

- Splunk's offerings include on-premises, private-cloud, and subscription-based

public-cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- Splunk has established partnerships with various system integrators and third-party integrations, such as Code42 Incydr, which delivers data exfiltration alerts and dashboards within Splunk. This collaboration enhances detection and response to insider threat events by correlating files, exfiltration destinations, and user risk indicators. Additionally, Splunk integrates with DTEX Systems, leveraging human telemetry and zero-trust principles to mitigate insider risks and account compromise. These partnerships strengthen Splunk's insider risk management capabilities and facilitate seamless collaboration across security channels.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, scalability, and focus on user experience and interactivity.

- In these spaces, Splunk's Insider Risk Management solution harnesses the power of AI and predictive analytics engines to delve deeper into risk insights and facilitate informed decision-making. The offerings are designed to be customizable and scalable to cater to diverse industries and organizations of varying sizes. Additionally, Splunk leverages cloud platforms to enhance collaboration capabilities, reduce maintenance costs, and streamline updates. The cloud-based approach ensures seamless access to critical risk data while maintaining robust security protocols. Furthermore, user experience remains at the forefront, with intuitive user interfaces, interactive dashboards, and customizable views tailored to different user roles. Splunk's commitment to enhancing insider risk management aligns with industry trends and empowers organizations to proactively address security challenges.

Final Take

- Splunk's robust insider risk management offering emphasizes operational excellence, risk mitigation, and proactive threat detection. It leverages advanced capabilities such as predictive analytics and seamless AI integration to drive digital transformation, resulting in improved business outcomes and

heightened customer value. It also offers user-friendly interfaces to empower informed decision-making and effective optimization of business processes. In summary, Splunk's innovative approach leads the way in advancing insider risk management, providing simplicity and continuous improvement tailored to evolving organizational needs.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA and is rapidly expanding in the JAPAC region, supporting various use cases in industry verticals such as manufacturing, financial services, public sector, retail, online services, and communications can choose Splunk UBA platform.

Teramind

URL: https://www.teramind.co/

Founded in 2014 and headquartered in Miami, Florida, USA, Teramind offers insider threat detection, data loss prevention, and business process engineering solutions.

Teramind's comprehensive insider risk management solution helps organizations mitigate insider threats with advanced behavioral analytics to detect suspicious activity, prevent data loss with real-time monitoring, and offer deep user insights for proactive risk mitigation, ensuring enterprise-grade security against both malicious and unintentional insider threats.

Analyst Perspective

Key Differentiators

- Teramind incorporates Optical Character Recognition (OCR) technology that allows it to extract text from screenshots, emails, and documents within applications, providing a more comprehensive view of user behavior. Additionally, Teramind's in-app field parsing capability analyzes data within specific fields of applications, potentially uncovering suspicious activities that might be missed by traditional monitoring methods. This granular level of insight empowers security teams to identify potential insider threats with greater accuracy.

- Teramind's scriptable rule logic empowers security teams to craft custom rules and threat detection scenarios specific to their organization. This level of customization allows them to tailor the system to identify user behaviors that deviate from established norms, potentially indicating malicious intent. Furthermore, Teramind's automated alerts ensure security teams are notified promptly about suspicious activities, enabling a swifter response to potential insider threats.

- Teramind offers a feature for productivity analysis. This feature provides valuable insights into user work patterns and potential deviations that might be linked to malicious intent. For instance, a sudden decrease in productivity coupled with a spike in unauthorized file transfers could raise a red flag. Ad-

ditionally, Teramind's live view functionality allows security teams to monitor user activity in real-time, enabling them to investigate suspicious actions immediately and potentially prevent a security incident.

Product Strategy

- Technology Roadmap: Teramind is focusing on integrating GenAI capabilities and ML Vision advancements into their product suite for improved Productivity understanding, NLP Text understanding, and Worker Digital Twin enhancement.

- Strategic Roadmap: Teramind's strategic roadmap involves active engagement with customers through the Teramind Wishlist section and regular platform updates to empower Business Process Optimization, helping customers become operationally sustainable.

Market Strategy

- Geo-expansion Strategy: Teramind has a strong customer base in North America, followed by EMEA. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: Teramind is catering its offering in finance, retail, manufacturing, energy, technology, healthcare, and government sectors.

- Use Case Support: Teramind supports various use cases such as employee monitoring, compliance management, User & Entity Behavior Analytics (UEBA), Behavioral Data Loss Prevention (DLP), insider fraud detection, workforce productivity optimization, business process optimization, and hybrid workforce management.

Customer/ User Success Strategy

- Teramind offerings provide support on-premises, private-cloud, and public-cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- Teramind has established partnerships with various system integrators and third-party integrations, with key technology partnerships including Splunk,

LogRhythm, Azure, Radar, Jira software, Zendesk, and Redmine, to facilitate enhanced insider threat detection and data loss prevention.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- Teramind is strategically aligning with these trends by integrating advanced AI capabilities (GenAI) and Machine Learning advancements (ML Vision) into its product suite. This strengthens its focus on data analytics and AI integration, enabling deeper insights into user behavior and activity patterns for improved insider threat detection. Additionally, Teramind's roadmap emphasizes customization and scalability, potentially offering modular solutions where clients can choose specific features relevant to their security needs and organizational size. This aligns with the market's demand for adaptable solutions. Furthermore, Teramind's cloud-based architecture is likely to contribute to organizational agility and resilience by enabling easier updates and enhanced collaboration between security teams. This focus on user-friendliness aligns with the market's growing emphasis on a positive user experience for security tools.

Final Take

- Teramind offers a comprehensive insider risk management solution that empowers organizations to proactively combat internal threats. Teramind goes beyond simple user monitoring to provide deep visibility into user behavior and identify potential threats before they cause significant damage by leveraging advanced AI and machine learning capabilities. This translates to improved security posture, reduced risk of data breaches, and a more secure work environment for all. Teramind's commitment to user experience ensures security teams have the tools they need to make informed decisions quickly and efficiently. As the insider threat landscape continues to evolve, Teramind remains at the forefront by offering a future-proof solution that adapts to meet the ever-changing needs of organizations.

- Users looking for an easy-to-use Insider Risk Management solution with a

strong customer base in North America, EMEA and rapidly expanding in JAPAC region offering various use cases in industry verticals such as finance, retail, manufacturing, energy, technology, healthcare, and government sectors can choose Teramind Insider Risk Management platform.

CounterCraft

URL: https://www.countercraftsec.com/

Founded in 1991 and headquartered in New York, New York, USA, CounterCraft offers a Cyber Deception platform that goes beyond simply identifying suspicious by generating high-confidence alerts that prioritize the most critical threats by leveraging deception technology and advanced analytics. This prioritization allows the security teams to focus their investigations on the at-risk users and potential insider threats. The platform also provides detailed user context and forensic data, allowing comprehensive investigations and informed decision-making.

Analyst Perspective

Key Differentiators

- CounterCraft The Platform™ offers Proactive Deception Technology for insider risk management. This unique approach avoids monitoring user activity and passively waiting for suspicious behavior by deploying deceptive environments like honeypots and honeytokens. These digital lures act as baits that attract bad actors, including malicious insiders, and reveal their malicious intent. This proactive strategy allows security teams to identify insider threats before they can cause harm.

- The CounterCraft Platform™ analyzes activity within deceptive environments and user behavior patterns to provide high-confidence alerts and enable prioritized Investigations. The platform generates high-confidence alerts that prioritize the most critical threats. This prioritization allows security teams to focus their investigations on the most at-risk users and potential insider threats. Additionally, the platform provides detailed user context and forensic data, allowing for comprehensive investigations and informed decision-making.

- The Platform entices potential insider threats to interact with deceptive environments. It identifies suspicious activity in real-time. This significantly reduces the dwelling time for insider threats within the network, minimizing the potential damage they can cause and allowing for a faster response.

Product Strategy

- Technology Roadmap: CounterCraft's technological roadmap includes a focus on proactive threat detection, cyber deception, and mission-critical performance enhancements. Its partnerships with government agencies and commitment to serving the mission underscore its impact in the field of cybersecurity.

- Strategic Roadmap: CounterCraft has entered into a strategic partnership agreement with S21sec, Cyber Solutions by Thales, to exponentially increase active defense globally to detect, reduce and prevent potential attacks that could compromise the security of organizations against the most advanced threats. This joint action will be carried out in the financial services, critical infrastructure, manufacturing, defense, and security sectors.

Market Strategy

- Geo-expansion Strategy: CounterCraft has a strong customer base in North America, followed by EMEA. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: CounterCraft caters its offering in financial services and banking, energy manufacturing and OT, retail, healthcare, and telecom domains.

- Use Case Support: CounterCraft focuses on various use cases, such as detecting and stopping lateral movement, protection from ransomware, external monitoring, active directory protection, and legacy systems protection.

Customer/ User Success Strategy

- CounterCraft offerings provide support on-prem and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- CounterCraft has established partnerships with various technological vendors to provide a comprehensive range of capabilities for tailoring cutting-edge cybersecurity solutions to cater to customers' needs.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, CounterCraft's Insider risk management platform leverages its deception technology through machine learning and analyzes interactions within deceptive environments, identifying subtle behavioral shifts indicative of insider threats. The modular platform scales with the user's needs, offering customization and cost-effectiveness. Its user-centric design with interactive dashboards empowers analysts to conduct efficient investigations.

Final Take

- CounterCraft The Platform™ offers a comprehensive deception-based solution that performs user monitoring and anomaly detection by deploying deceptive environments and leveraging advanced behavioral analytics. CounterCraft's The Platform™ proactively identifies malicious actors, including insider threats attempting to evade detection. This real-time threat intelligence empowers security teams to prioritize investigations and take swift action to mitigate potential security incidents. Furthermore, CounterCraft's The Platform™ prioritizes user experience with an intuitive interface and role-based functionalities. This empowers security analysts with the tools to conduct thorough investigations and make informed decisions. In essence, the CounterCraft The Platform™ offers a technically robust and user-centric solution.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA, and rapidly expanding in the JAPAC region, offering various use cases in industry verticals such as financial services & banking, energy manufacturing and OT, retail, healthcare, and telecom can choose the CounterCraft Insider Risk Management platform.

Resolver (Crisp)

URL: https://www.resolver.com/

Founded in 2005 and headquartered in Leeds, UK, Resolver is a global provider of risk intelligence and security solutions that cater to digital marketing, communications, trust & safety, security, HR, operations, and corporate customers' use cases. Resolver offers protection from insider threats through its Corporate Risk Intelligence and Platform Risk Intelligence solutions. The company was acquired by risk and financial advisory solutions provider Kroll in 2022 to expand its digital services capabilities.

Resolver's Insider Risk Management solution helps organizations mitigate cyber security insider risks by discovering and tracking risk signals through its AI and Human Intelligence Expert Teams.

Resolver's Corporate Risk Intelligence suite of solutions provides fast, actionable risk intelligence by leveraging different capabilities and differentiators, such as Crisis defense, Threat defense, VIP defense, Owned Social Defense, Paid social defense, and Intelligence Reports and Events Coverage.

Analyst Perspective

Key Differentiators

- Resolver offers a comprehensive Insider Risk management solution and corporate risk intelligence that helps organizations detect and respond to potential security threats in real time. Users can also leverage its artificial risk intelligence capabilities to minimize the risk of data breaches and other cyberattacks.

- Resolver Threat protection is equipped with threat defense capability, which enables organizations to receive timely actionable alerts about any threats. The capability leverages AI and ML algorithms to help identify risk signals embedded within the digital network.

- Resolver's Threat protection helps client organizations gain actionable insights into security threats through Intelligence Reports and Event coverage capabilities for advanced threat detection and response. It provides expert in-

sights into ongoing threat analysis or insider risk events and helps the clients receive fast, actionable risk intelligence in the development and execution stages of the response strategy against dealing with cyber threats.

Product Strategy

- Technology Roadmap: Resolver has released Resolver 23.3, which introduces a host of powerful customer-centric features designed to enhance data-driven decision-making and boost operational efficiency through enhancements to dashboards, document management, and mapping capabilities, and improved design and UX Enhancements.

- Strategic Roadmap: Resolver's strategic roadmap focuses on holistic approach to security, emphasizing complete visibility and risk management in the context of business objectives. Resolver is developing its platform to address the interconnectedness of security with business goals and overall organizational resilience.

Market Strategy

- Geo-expansion Strategy: Resolver has a strong customer base in North America, followed by EMEA. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: Resolver is catering its offering in financial services, life sciences, online platforms, fashion and luxury, technology and sports, media, and entertainment.

- Use Case Support: Resolver supports various use cases, such as threat detection and response, compliance monitoring, insider threat detection, identifying credible online threats, adverse event detection, and mitigating risk of adverse events.

Customer/ User Success Strategy

- Resolver offerings provide support on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- Resolver has established partnerships with Amazon Web Services, LexisNexis, Marketo, and Cloudflare to help its customers streamline their corporate security, IT, risk, and compliance processes through Resolver's platform.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, Resolver's insider risk management strategy leverages advanced data analytics and integrates AI to identify subtle behavioral patterns indicative of potential insider threats. Furthermore, its platform offers a modular and scalable design, allowing organizations of various sizes and industries to customize investigation workflows and risk management features to their specific needs. This focus on customization can involve modular components where clients choose features relevant to their operations. Additionally, Resolver's cloud-based platform fosters collaboration within security teams and simplifies security updates, minimizing maintenance costs. Finally, Resolver prioritizes user experience by designing intuitive interfaces, interactive dashboards, and customizable views tailored for different security roles, empowering security teams with the tools they need for efficient investigations and informed decision-making.

Final Take

- Resolver's insider risk management is a comprehensive investigation and case management solution. By leveraging automation and advanced analytics, Resolver empowers security teams to streamline investigations, identify potential threats faster, and optimize their response procedures. The platform's focus on user experience through intuitive interfaces and customizable workflows ensures clear communication and collaboration within security teams. Resolver's commitment to continuous innovation positions them to address evolving insider threats and empowers organizations to proactively safeguard sensitive data and maintain a strong security posture.

- Users looking for an easy-to-use insider risk management solution with a strong customer base in North America, EMEA and rapidly expanding in

JAPAC region offering various use cases in industry verticals such as financial services, life sciences, online platforms, fashion and luxury, technology and sports, media, and entertainment can choose Resolver Insider risk management platform.

DTEX Systems

URL: https://www.dtexsystems.com/

Founded in 2002 and headquartered in Saratoga, California, USA, DTEX Systems offers DLP and Insider risk solutions. Its InTERCEPT platform consolidates the essential elements of DLP, UBA, and UAM in a single platform to detect and mitigate insider risks well before data loss occurs. Combining AI/ML with behavioral indicators, DTEX enables proactive insider risk management at scale without sacrificing employee privacy or network performance.

DTEX InTERCEPT empowers organizations to address insider threats proactively. This next-generation solution leverages advanced behavioral analytics and user entity behavior analytics (UEBA) to gain deep insights into user activity across diverse data sources. This allows security teams to intervene early and mitigate potential risks before they escalate into data breaches or other security incidents.

Analyst Perspective

Key Differentiators

- DTEX InTERCEPT leverages machine learning to offer comprehensive Entity Context and Peer Group Analysis, enabling the creation of user and entity profiles for every individual within the organization. These profiles consider factors like a user's roles, permissions, historical activity, and relationships with other users. DTEX InTERCEPT analyzes user behavior in context with this entity context to identify anomalous activities that might be missed by traditional user monitoring. Such activities include authorized users accessing highly sensitive data outside of their normal work hours or collaborating with unauthorized individuals on sensitive projects.

- DTEX InTERCEPT utilizes advanced User and Entity Behavior Analytics (UEBA) techniques combined with machine learning algorithms and the platform can learn from historical data and adapt to identify even subtle changes in user behavior that might indicate potential insider threats. Deviation from the typical behavior is flagged for further investigation.

- DTEX InTERCEPT prioritizes providing actionable insights to security teams. DTEX InTERCEPT utilizes risk scoring to prioritize investigations based on a

combination of factors. These factors include the severity of the detected anomaly, the user's access privileges, and the sensitivity of the data involved. By focusing on the highest-risk cases first, security teams can optimize their resources and efficiently address the most critical insider threats. Furthermore, DTEX InTERCEPT provides detailed user context and investigation tools to enable security teams to conduct thorough investigations and make informed decisions.

Product Strategy

- Technology Roadmap: DTEX Systems is focusing on integrating AI capabilities and advance analytics through the addition of an AI risk assistant to its InTERCEPT™ platform to guide and fast-track insider investigations and decision-making. The DTEX Ai³ Risk Assistant feature of the InTERCEPT™ platform processes natural language to provide quick and comprehensive insight into the nuances of insider risk and intent, and it bypasses complex database searches and data wrangling to provide actionable insights that address the complexity of human behavior in real-time.

- Strategic Roadmap: DTEX Systems closed $50M in Series E funding, leading to total funding being raised to $138M. The funding will be used to expand the company's U.S. engineering team and grow its go-to-market (GTM) operations globally, accelerating its mission to proactively protect global organizations from insider threats. These new funds will continue to fuel significant company momentum and accelerate DTEX's application of large language models (LLMs) and behavioral science research to disrupt the insider risk management market.

Market Strategy

- Geo-expansion Strategy: DTEX Systems has a strong customer base in North America, followed by Australia. The company plans to expand its presence in EMEA.

- Industry Strategy: DTEX Systems is catering its offering in manufacturing, healthcare, financial services, Pharma, media, technology, and the public sector.

- Use Case Support: DTEX Systems focuses on various use cases, such as

User Behavior Analytics, User Access Management, and Data Loss prevention.

Customer/ User Success Strategy

- DTEX Systems' offerings support on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- DTEX Systems has established partnerships with various technological vendors such as Microsoft, crowdstrike, IBM, Exabeam, Securonix, and Trellix to provide a comprehensive insider risk management solution.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- DTEX InTERCEPT aligns with these trends by offering a next-generation cloud-native platform built on advanced UEBA (User and Entity Behavior Analytics) and machine learning. This empowers organizations to gain deep contextual insights into user behavior. DTEX leverages machine learning algorithms to create comprehensive user and entity profiles, incorporating factors like roles, permissions, and peer group interactions. This allows for the identification of subtle deviations that might indicate malicious intent, even when users attempt to evade traditional detection methods. Additionally, DTEX leverages the cloud to deliver a user-centric experience with an intuitive interface, interactive dashboards, and role-based views.

Final Take

- DTEX InTERCEPT leads in Insider Risk Management with its cloud native UEBA platform leveraging unsupervised machine learning. It analyzes user behavior and entity interactions, building context-rich profiles with roles, permissions, and peer group activity. This unveils subtle deviations that traditional methods might miss, identifying potential insider threats attempting to evade detection. DTEX prioritizes user experience with a modular design and risk scoring tailored to specific workflows.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, Australia, and rapidly expanding in EMEA region, offering various use cases in industry verticals such as manufacturing, healthcare, financial services, Pharma, media, technology, and public sector can choose DTEX Systems Insider Risk management platform.

Ekran System

URL: https://www.ekransystem.com/

Founded in 2013 and headquartered in Newport Beach, California, USA, Ekran System provides insider threat detection platform offering Insider threat management, user-based risk detection, enterprise security, employee monitoring, contractor monitoring, and internal visibility and helps to deter, detect, and disrupt insider threats.

The company's Insider risk management (IRM) platform helps users detect threats by combining robust insider threat detection tools, including comprehensive activity monitoring, alerting functionality, advanced access management and identity control toolset, manual and automated incident response, and powerful reporting.

Analyst Perspective

Key Differentiators

- Ekran System's insider risk management (IRM) platform offers a monitoring and activity investigation feature that provides key episode search, client protection, and session video recording capabilities. The feature helps record all user sessions on target endpoints based on both IP-based and username-based record filtering. Additionally, it has a smart combination of watchdog and driver-level process protection mechanisms, which help prevent disruptions in monitoring, ensuring enhanced user and entity monitoring.

- The platform offers predefined custom alerts that enable rule-based incident flagging. The solution's library of alarm templates covers the most typical insider threat indicators and aids in system enhancement by employing several activity factors such as process names, opened websites, connected USB devices, typed keystrokes, and performed Linux commands.

- Ekran System's USB management device control platform identifies, tracks, and generates alarms when various sorts of USB devices are connected. It also includes a collection of tools for blocking unauthorized devices and risky devices. It also provides manual approval for specific USB devices for guest and third-party clients.

Product Strategy

- Technology Roadmap: Ekran System's technology roadmap is centered on continuous improvement in its core functionalities: advanced UAM, threat detection, and user behavior analytics. The company is focusing on these areas to provide users with a comprehensive and future-proof solution for insider risk management.

- Strategic Roadmap: Ekran System is partnering with Hideez to enhance the authentication process and improve user experience. As an alternative to two-factor authentication, customers can now use a straightforward passwordless authentication method for enhanced authentication.

Market Strategy

- Geo-expansion Strategy: Ekran System has a strong customer base in North America, followed by EMEA. The company is now planning to expand its presence in Asia Pacific.

- Industry Strategy: Ekran System is catering its offering in telecommunications, finance & insurance, healthcare, energy, public administration, government and military, manufacturing, education, IT services, and automotive segments.

- Use Case Support: Ekran System focuses on various use cases, such as insider threat prevention, security incident investigation, employee monitoring, third-party vendor monitoring, privileged user monitoring, IT Compliance, and user Privacy.

Customer/ User Success Strategy

- Ekran System offerings provide support on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- Ekran System has established partnerships with various system integrators and third-party integrations. These include AWS, Citrix, VMware, Microsoft and UBX Cloud.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- Ekran System capitalizes on these trends by integrating advanced data analytics and machine learning into its platform. This integration empowers security teams with deeper user behavior insights and facilitates proactive risk identification. Ekran System also recognizes the importance of customization and scalability. Its platform accommodates a wide range of organizations with modular designs, allowing clients to tailor features based on their specific needs. Additionally, Ekran System leverages cloud deployment to offer enhanced collaboration, streamlined maintenance, and automatic updates. Ekran System also prioritizes user experience with intuitive interfaces, interactive dashboards, and customizable views that cater to different security analyst roles, ensuring efficient threat investigation and mitigation.

Final Take

- Ekran System offers robust Insider Risk Management capabilities with its comprehensive security intelligence platform. This platform empowers organizations to gain a holistic view of user activity and identify potential insider threats. The platform leverages advanced analytics and machine learning to detect subtle behavioral anomalies that might signal malicious intent. Furthermore, Ekran System prioritizes user experience with intuitive interfaces and customizable dashboards, enabling security analysts to make swift and informed decisions for risk mitigation. By continuously innovating and integrating cutting-edge technologies, Ekran System safeguards critical information and ensures business continuity for organizations of all sizes.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA and rapidly expanding in the JAPAC region offering various use cases in industry verticals such as Telecommunications, Finance and insurance, healthcare, energy, public administration, governmentand& military, manufacturing, education, IT services and automotive can choose the Ekran System platform.

Elevate Security (a mimecast company)

URL: https://elevatesecurity.com/

Founded in 2017 and headquartered in San Francisco, California, USA, Elevate Security offers a cloud-based security risk management platform that helps identify risky users and automatically orchestrates additional security measures to minimize the likelihood of such an incident.

Elevate Security offers a comprehensive suite of solutions to address insider threats by empowering organizations to proactively manage user risk. It integrates with existing security tools to continuously monitor user behavior and identify potential threats. By leveraging machine learning and risk scoring, Elevate Control prioritizes high-risk individuals, enabling security teams to focus their efforts on the most critical cases.

Elevate Engage complements Elevate Control by fostering a culture of security awareness. It provides targeted training and education based on the users' risk profiles. This personalized approach helps mitigate unintentional insider threats and empowers employees to make informed security decisions.

Analyst Perspective

Key Differentiators

- Elevate Security utilizes continuous user behavior monitoring, unlike traditional solutions that rely on static rules. This divergence allows Elevate Control to capture a comprehensive picture of user activity and identify subtle changes indicating potential threats. Additionally, Elevate Control generates dynamic risk scores for each user based on their behavior and context. This scoring prioritizes critical cases and empowers security teams to efficiently allocate resources.

- Elevate Security's risk scoring goes beyond basic user activity monitoring by incorporating behavioral biometrics into its analysis. This process involves analyzing user interaction patterns, keystroke dynamics, and mouse movements to establish a unique behavioral profile for each user. Elevate Control

considers these factors alongside traditional activity data to generate more nuanced and context-aware risk scores, allowing security teams to prioritize investigations based on a user's typical behavior and potential for malicious intent.

- Elevate Security's Elevate control utilizes adaptive user profiling to continuously update individual baselines as user activity patterns change. This updation ensures the platform remains sensitive to subtle deviations indicating a shift towards malicious intent. Furthermore, Elevate Security empowers security analysts with advanced threat-hunting capabilities. These functionalities enable investigators to explore user activity data beyond pre-defined alerts, allowing them to proactively identify potential insider threats that might not trigger traditional alarms.

Product Strategy

- Technology Roadmap: Elevate Security is focusing on workforce cyber risk quantification. It has introduced new SaaS-based offerings that provide rapid risk assessments, deep visibility into company-wide internal cyber risk, and instant risk-adjusted security controls at the individual worker level. The company's adaptive trust solution can unite with Microsoft's security suite to automatically protect users by considering their unique risk characteristics.

- Strategic Roadmap: Elevate Security's strategic roadmap includes international expansion plans to address the growing demand for insider risk management solutions. The company is also investing in enhancing the platform's scalability and user experience to cater to a wider range of organizations and security teams. This enhancement involves developing features for easier customization and streamlined workflows to offer a more comprehensive insider risk management ecosystem.

Market Strategy

- Geo-expansion Strategy: Elevate Security has a strong customer base in North America, followed by EMEA. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: Elevate Security caters its offering in pharmaceuticals, energy and utilities, financial services, healthcare, and consumer and packaged goods.

- Use Case Support: Elevate Security focuses on various use cases such as Security Awareness and Human Risk Management, Security Operations and Case Management, as well as Identity and User Risk Authentication.

Customer/ User Success Strategy

- Elevate Security' offerings provide support on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- Elevate Security has established partnerships with various technological vendors, including Microsoft, Cisco, SailPoint, Zscaler, and Crowdstrike, and ingests inbound risk data signals to different integrations for connecting with email, web, IAM, SIEM, Endpoint, Device, DLP, and HR, platforms, and uses powerful analytics to identify riskiest users, Clear dashboards and automated playbooks to identify high-risk users and automate business workflows.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- Elevate Security aligns with these trends by offering a next-generation Insider Risk Management Platform that is built on the foundation of advanced machine learning and behavioral analytics. This goes beyond simple anomaly detection by incorporating unsupervised machine learning to identify subtle deviations in user behavior that might indicate potential insider threats. Furthermore, Elevate Security prioritizes scalability and customization through a modular platform design.

Final Take

- Elevate Security offers a robust Insider Risk Management solution, which leverages unsupervised machine learning algorithms to continuously monitor user behavior and identify anomalies indicating malicious intent. Unlike traditional solutions relying on pre-defined threat models, Elevate Security utilizes behavioral biometrics to establish a unique baseline for each user. By

focusing on unsupervised machine learning, behavioral biometrics, and user-centric design, Elevate Security delivers a technically robust solution that proactively identifies and mitigates insider threats in today's dynamic security landscape.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA, and rapidly expanding in the JAPAC region, and offering various use cases in industry verticals such as pharmaceuticals, energy and utilities, financial services, healthcare and consumer and packaged goods, can choose elevate security insider risk management platform.

Everfox (Forcepoint)

URL: https://www.everfox.com/

Founded in 1994 and headquartered in Austin, Texas, USA, Forcepoint is a data security company offering computer security software and data protection, cloud access security broker, firewall, and cross-domain solutions. Forcepoint's Everfox, formerly Forcepoint Federal, defends critical organizational data and networks against complex cyber threats.

Forcepoint offers Insider Threats and Risk Adaptive Protection through the Forcepoint Data Loss Prevention (DLP) system. The solution gathers user behavior and DLP incidents before calculating the user's risk with Forcepoint's Indicator of Behavior (IOB) analytic models. This risk score is actively transmitted to DLP so that policy enforcement can be automated based on the risk level.

Analyst Perspective

Key Differentiators

- Forcepoint Risk adaptive protection's Autopilot comes with risk assessment that detects suspicious behavior by continuously collecting, enhancing, and connecting events. It provides the appropriate context to events without the requirement for configuration to recognize Indicators of Behavior and generate alerts that raise the user's risk score. It consists of activity monitoring, a policy engine, anomaly detection, and risk calculation features.

- Forcepoint Risk adaptive protection couples an alert with a specific risk impact, longevity factor, and reduction function that evaluates the user's risk score depending on the severity of the behavior. When an alarm is generated, the risk is influenced based on the severity, resulting in a score ranging from 0 to 100. This risk score is calculated by considering numerous associated indications of behavior, allowing for an exponential increase in the implementation of risk-adaptive data security strategies. Risk impact, longevity, and reduction function are the core parameters that influence risk.

- Forcepoint offers Insider Risk Solution through its User Activity Monitoring (UAM) and Analytics platform that gives analysts and investigators comprehensive access to all user endpoint activity for effective detection and resolu-

tion of aberrant behavior. Robust endpoint sensors for policy-driven data collection and Secure UAM solution with end-to-end encryption of data features help provide deep visibility and identify the riskiest users, protect workforce, organization, and customers, simplify exploration and analysis, optimize workflows, customize the program accordingly and safeguard all investigations.

Product Strategy

- Technology Roadmap: Forcepoint is focusing on accelerating investment into industry-leading solutions, threat protection, and insider risk technologies by deepening its relationships with global government, critical infrastructure, and regulated industries.

- Strategic Roadmap: Forcepoint's strategic roadmap for Insider Risk Management solution focuses on developing and delivering defense-grade cybersecurity technology. With its recently announced partnership with Microsoft, Everfox will integrate its industry-leading cross-domain solution technology into Azure's cloud services offering for the U.S. Government. Through this partnership, Everfox and Microsoft will develop and deploy new cloud offerings for federal agencies that deliver on-demand multi-level cloud desktop services.

Market Strategy

- Geo-expansion Strategy: Forcepoint has a strong customer base in North America, followed by EMEA. The company is now planning to expand its presence in Asia Pacific.

- Industry Strategy: Forcepoint is catering its offerings in critical infrastructure, financial, healthcare, energy, and government segments.

- Use Case Support: Forcepoint supports on various use cases such as protecting data in the cloud and office 365 solutions, zero trust security, cloud app security and SASE networking and security solutions, network security by remote worker security, connecting and securing remote offices and branches, cross-domain security by continuous diagnostics and mitigation.

Customer/ User Success Strategy

- Forcepoint offers on-premises, private-cloud, and subscription-based public-cloud deployments. Its primary offering is cloud-based but offers flexibility for on-prem and hybrid deployments.

- Forcepoint has established partnerships with various system integrators and third-party integrations. These include AWS, Ping Identity, Microsoft, VMware, Okta, Ericom, Splunk, and Kiteworks. Their focus on partnerships and integrations aims to ensure comprehensive solutions for safeguarding critical data and mitigating risks from within.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization and scalability, as well as focus on user experience and interactivity.

- In these spaces, Forcepoint's strategic approach aligns seamlessly with prevailing technological trends, harnessing advanced data analytics and AI integration to empower organizations. The solution provides unparalleled visibility into user behavior, safeguarding critical data and detecting insider threats through key capabilities such as a robust endpoint sensor, in-depth analytics, and enterprise readiness. Investigative tools, such as comprehensive video replay and native integrations, enhance threat detection and flexible UAM data inspection, which ensures persistent monitoring and privacy governance.

Final Take

- Forcepoint delivers a comprehensive suite of capabilities through its platform that combines visibility and analytics to understand how users interact with critical data, enabling proactive risk mitigation. The platform leverages advanced features, including predictive analytics and Generative AI, to empower organizations to make informed decisions and drive digital transformation. The platform's intuitive interfaces enhance user experience by ensuring that security professionals and decision-makers can confidently navigate the system. Forcepoint enables effective business process optimization by combining robust analytics with user-friendly design.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA and rapidly expanding in JAPAC region offering various use cases in industry verticals such as critical infrastructure, financial, healthcare, energy, and government can choose Forcepoint Insider Risk Management platform.

Exabeam

URL: https://www.exabeam.com/

Founded in 2013 and headquartered in Foster City, CA, USA, Exabeam is a security analytics and automation company that provides a cloud platform to simplify security operations. Exabeam offers an Insider Risk Management Solution through its Fusion SIEM, which integrates SIEM with XDR to create a cutting-edge SecOps solution. The Fusion SIEM solution detects, investigates, and responds to external threats, compromised users, and malevolent adversaries in real-time. The solution includes a centralized, highly scalable data storage that provides comprehensive visibility into the entire organizational IT ecosystem. Exabeam also offers guided search and enhanced results to highlight critical facts for quick review. The solution also offers a rapid search capability to enhance the analyst performance and productivity and in-built compliance reports and dashboards to minimize the need for cumbersome spreadsheets needed for auditing purposes. Exabeam Fusion SIEM maximizes the productivity of organizational IT systems by minimizing false positives.

Analyst Perspective

Key Differentiators

- Exabeam offers a comprehensive Insider risk management solution through Exabeam Fusion SIEM which offers Automated investigation and response to help organizations in incident detection, triage, and investigation. It is equipped with machine learning-based Smart Timelines that automatically collect information, apply risk grading, and compile it into a cohesive narrative that may be utilized to conduct an initial inquiry.

- Exabeam Fusion enables organizations to detect and prioritize anomalies by using behavioral model histograms to detect sophisticated threats like credential-based assaults, insider threats, and ransomware activities that other technologies miss. It offers Smart Timelines that depict the whole history of an incident while emphasizing the risk associated with each event. Exabeam Fusion's Anomaly Search provides a streamlined search experience with quick query returns. A single interface allows analysts to search across their data repository for Exabeam-triggered events, combining behavior-based TTP detection with known IoCs to improve threat-hunting skills.

- Exabeam SIEM offers a cloud-scale security log management feature that speeds up data ingestion, parsing, storing, and searching. It also offers a single interface that allows searching across various sorts of data at the same pace and enables accelerated construction of visualizations from parsed log data and build a dashboard with many pre-built chart kinds.

Product Strategy

- Technology Roadmap: Exabeam's roadmap prioritizes advanced security analytics with AI and machine learning for threat detection, anomaly identification, and threat prediction through Transformative Unified Workbench to improve user experience with a centralized platform for security operations. Additionally, the emphasis on ingesting data from various sources aligns with the XDR approach for a more comprehensive security view with a focus on addressing specific security challenges like insider threats and financial fraud, indicating the potential tailoring of their solutions for different industries.

- Strategic Roadmap: Exabeam's strategic roadmap for its Insider Risk Management solution focuses on AI-driven security operations. The roadmap prioritizes advanced security analytics along with patented anomaly detection and generative AI assistance for precise threat detection, investigation, and even potential prediction.

Market Strategy

- Geo-expansion Strategy: Exabeam has a strong customer base in North America, followed by EMEA. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: Exabeam is catering its offering in financial services, healthcare, higher education, manufacturing, and government.

- Use Case Support: Exabeam focuses on various use cases such as compliance, isolating compromised and malicious insiders, and mitigating external threats.

Customer/ User Success Strategy

- Exabeam offerings provide support on-premises and cloud deployments. Its primary offering is cloud-based but offers flexibility for on-prem and hybrid deployments.

- Exabeam has established technology partnerships through Integrations with various security vendors, such as AWS, Cisco, Code42, Google, Mimecast, Sail Point, VMware, and Zscaler to power greater visibility and efficiency. Customers can leverage these integrations between Exabeam's industry-leading security analytics platform and over 2,500 unique data sources and APIs to automate operations in the SOC.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, Exabeam's insider risk management solution seamlessly integrates advanced data analytics and AI capabilities, enabling organizations to proactively address insider threats. With a focus on organizational agility and resilience, Exabeam's platform adapts swiftly to dynamic risk scenarios. It offers customizable and scalable solutions that cater to diverse industries and organizational sizes. Clients can opt for modular designs, selecting features relevant to their specific operations. Moreover, Exabeam leverages the cloud platform to enhance collaboration, reduce maintenance costs, and streamline updates. The user experience remains paramount, with intuitive UI, interactive dashboards, and customizable views tailored to different user roles.

Final Take

- Exabeam's insider risk management solution addresses the challenges posed by insider threats, particularly in the context of hybrid or remote workforces. As organizations increasingly rely on third-party integrations, Exabeam's platform provides robust monitoring capabilities to safeguard against data breaches and malicious activities. Leveraging advanced data science, behavioral analytics, and automation, Exabeam empowers security and risk man-

agement leaders to proactively manage insider risks. By fostering a secure work environment and protecting sensitive data, Exabeam contributes significantly to enhancing users' overall security posture.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA, and rapidly expanding in JAPAC region offering various use cases in industry verticals such as manufacturing, healthcare, BFSI can choose Exabeam Insider risk management platform.

Fortinet

URL: https://www.fortinet.com/

Founded in 2000 and headquartered in Sunnyvale, CA, USA, Fortinet is a major provider of network security solutions. The company offers a comprehensive Insider Risk Management (IRM) solution through its FortiInsight. The solution leverages machine learning analytics to monitor endpoints, data movement, and user activities to spot abnormal, malicious behavior and policy violations.

Fortinet's IRM solution safeguards organizations against insider threats by continually monitoring users and endpoints and providing automated detection and response capabilities. FortiInsight uses machine learning and advanced analytics to detect non-compliant, suspicious, or abnormal behavior and quickly alerts to any compromised user accounts.

Analyst Perspective

Key Differentiators

- The FortiInsight solution enables rapid threat detection by optimizing machine learning at each stage of the investigation pipeline and identifying emerging threats. It learns usual user behavior to recognize unfamiliar behavior and warns about it in real time. The lightweight agent securely transmits t data about user interactions with the monitored endpoints or cloud services to the ML engine, where an anomaly-detection mechanism detects out-of-place occurrences. These anomalies are then verified for known risk variables and assigned a risk score. Any acts that may pose a risk trigger an immediate alert, allowing the users' SOC teams to take appropriate action.

- FortiInsight offers Visual Threat Hunting Through Link Analysis, which combines visibility, correlation, automated reaction, and remediation into a single, scalable system. This combination decreases the complexity of managing network and security operations to effectively liberate resources, increase breach detection, and even prevent breaches. FortiSIEM also contains new link graph technology, which enables easy visualization of relationships between users, devices, and incidents.

- FortiInsight offers next-generation SOC automation, which analyzes the most recent risks and develops mitigation measures quickly. The solution can be paired with the most recent AI-driven behavior anomaly detection capabilities, such as UEBA, to guard against both known and new attacks. Statistical models are used to detect unexpected and improbable deviations, such as logins from different geographical locations.

Product Strategy

- Technology Roadmap: Fortinet has added a generative AI (GenAI) assistant titled Fortinet Advisor to its product portfolio. The implementation of GenAI will allow the products to protect customers and keep business operations online. The assistant will support and guide security operations (SecOps) teams to investigate and remediate threats faster. Fortinet also plans to implement enhancements across its security operations portfolio to introduce tighter integration and improve its ability to automate detection and response, accelerating discovery and remediation. Significant updates included new AI and machine learning capabilities and additional real-time response and automation capabilities to improve efficacy, increase effectiveness, and accelerate time to resolution of sophisticated attacks.

- Strategic Roadmap: Fortinet's strategic roadmap for its insider risk management solution focuses on public-private partnerships to strengthen cyber resiliency in the United States, on how organizations can implement secure-by-design recommendations, and work to close the cybersecurity workforce gap. The company has also joined the Operational Technology Cybersecurity Coalition to help enhance the resiliency of US-based critical infrastructure and businesses' Industrial Control Systems (ICS).

Market Strategy

- Geo-expansion Strategy: Fortinet has a strong customer base in North America, followed by Europe. The company now plans to expand its presence in Asia Pacific.

- Industry Strategy: Fortinet is expanding its offering in Operational Technology, Manufacturing, SCADA/ICS, Oil & Gas, Power Utilities, Healthcare, Pharmaceutical, Financial Services, Retail and Hospitality.

- Use Case Support: Fortinet focuses on various use cases such as SOC Optimization, Alert Triage Automation, Unified Incident Response Management, SOC Collaboration, Threat Intelligence MGT, Custom Process Mapping, and NOC/SOC Convergence.

Customer/ User Success Strategy

- Fortinet offers include on-premises, private cloud, and public cloud-based solutions based on a subscription basis. Its primary offering is cloud-based but possesses deployment flexibility for on-prem and hybrid deployments.

- Fortinet's open ecosystem consists of partnerships with Fabric-Ready technology alliances, cooperation with threat-sharing groups, and more Fabric integrations. Customers can achieve enhanced end-to-end protection across their digital infrastructure by utilizing its integrated security solutions with the protection Fabric.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- Fortinet recognizes the growing focus on AI-powered user behavior analysis, modular security for scalability, cloud-based deployment for agility, and user-friendly interfaces. Fortinet addresses the insider risk management market through its Security Fabric. This integrated platform leverages advanced analytics and AI to identify suspicious user activity. The platform also offers a modular design to customize security features for specific needs. In addition, the platform utilizes a cloud-based architecture for centralized management and simplified updates and prioritizes user experience with intuitive interfaces and role-based dashboards, empowering security teams to proactively mitigate insider threats and safeguard sensitive data.

Final Take

- Fortinet's FortiInsight stands as a comprehensive insider risk management solution. It leverages advanced analytics and machine learning to detect sub-

tle anomalies in user behavior indicative of potential threats. The solution's scalable, modular architecture allows organizations to tailor security features to their specific needs. Fortinet's cloud-based approach ensures centralized threat visibility, simplified deployment, and automatic updates for enhanced organizational agility. Finally, the solution's user-friendly interface with intuitive dashboards empowers security teams to efficiently investigate and mitigate insider risks, safeguarding sensitive data and fostering a proactive security posture.

- Users looking for an Insider Risk Management solution that is easy to use and has a strong customer base in North America, EMEA and rapidly expanding in the Asia Pacific region, as well as supporting various use cases in industry verticals such as Operational Technology, Manufacturing, SCADA/ICS, Oil & Gas, Power Utilities, Healthcare, Pharmaceutical, Financial Services, Retail and Hospitality can choose the FortiInsight platform.

Gurucul

URL: https://gurucul.com/

Founded in 2010 and headquartered in El Segundo, CA, USA, Gurucul provides a real-time, cloud-native next-gen security analytics and operations platform that offers a Next-Generation SIEM, UEBA, Open XDR, and Identity & Access Analytics. Gurucul integrates machine learning behavior profiling with predictive risk-scoring algorithms to forecast, detect, and prevent data breaches, fraud, and insider threats. It also reduces the attack surface for accounts and removes unneeded access rights and privileges to improve data security.

The platform monitors organization's environment, natively ingests data from many data sources, including applications, and analyzes it to detect unauthorized and malicious privilege access, lateral movement and external communications, and data exfiltration.

Gurucul's Next-Gen SIEM offers various features, which include identity-centric risk modeling, a flexible entity model, user behavior baselining, analytics and monitoring, peer-group analytics, sentiment analysis, dashboards and reporting, risk-response workflow, alerting and case management and UEBA.

Analyst Perspective

Key Differentiators

- Gurucul offers a comprehensive IRM solution through its Next Gen SIEM that offers Identity-centric risk modeling, which tracks every user, account, and entitlement and connects them to create a complete picture of every user. The solution then connects this human-centric behavioral data with information security data to identify unusual conduct, which will be used in advanced threat detection.

- The Gurucul SIEM offers peer-group analytics feature that allows both static and dynamic peer-group definition and analytics. It automatically organizes users to produce baselines based on regular user behavior and detects unexpected changes from peer group baselines. It also enables advanced dynamic peer groups, which are generated on the need-to-know basis at runtime, depending on feature data analysis and data cardinality.

- The Gurucul SIEM also offers sentiment analysis, which helps organizations to combine data streams from HR apps, social media, emails, website visits, and other sources to profile a user to identify symptoms of dissatisfaction before leaving the organization or attempting to steal data or intellectual property.

- Gurucul Risk Analytics provides alerting and case management and UEBA features, comprehensive case management capabilities and alerting techniques. UEBA helps in behavior-based risk scoring, incident response and management, data masking, and intelligent threat hunting.

Product Strategy

- Technology Roadmap: Gurucul is focusing on integrating GenAI, AI capabilities, advance analytics, and simulation capabilities through its new generative AI capability called SME (Subject Matter Expert) to accelerate threat detection, supercharge security investigations, and automate responses. The capability empowers Security Operations Center (SOC) analysts with insights into a rich, correlated dataset across identity, security, network, enterprise, and cloud platforms. It will improve SOC team efficiency and help counter the ongoing challenges of limited resources and skill sets, overwhelming alert fatigue, false positives, and mis- or unprioritized alerts.

- Strategic Roadmap: Gurucul's strategic roadmap for focuses on predictive analytics and risk scoring to anticipate insider threats, implement Zero Trust security models, and automating data access requests to ensure compliance with evolving data privacy regulations. Gurucul aims to transform to a platform that empowers organizations to proactively manage risk and navigate the complexities of the modern security landscape.

Market Strategy

- Geo-expansion Strategy: Gurucul has a strong customer base in North America, followed by EMEA. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: Gurucul is expanding its offering in financial services, healthcare, manufacturing, retail, federal government, and energy & utilities.

- Use Case Support: Gurucul focuses on various use cases, including Insid-

er threat management, SOC transformation, cloud security monitoring, fraud detection and prevention, privileged access management, and compliance.

Customer/ User Success Strategy

- Gurucul's offerings support on-premises, and public-cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- Gurucul has established partnerships with various technological vendors like AWS, Checkpoint, Cisco, Microsoft, Google, Okta, Proofpoint, SentinelOne, Tenable, and Zscaler to deliver integrated and optimized solutions to solve customers' complex business needs by leveraging the Gurucul Security Analytics and Operations Platform in order to maximize value and efficiency of the SOC.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, Gurucul leverages its Security Analytics and Operations Platform by integrating machine learning and advanced anomaly detection to provide deep insights into user behavior. Gurucul's approach emphasizes predictive risk scoring, enabling organizations to proactively identify and mitigate potential insider threats. Furthermore, Gurucul offers a scalable solution with modular features. Clients can tailor the platform to their specific needs, focusing on the most relevant functionalities for their industry and size. Gurucul also embraces the cloud, ensuring easy updates, lower maintenance costs, and enhanced collaboration.

Final Take

- Gurucul's Insider Risk Management platform is a robust solution that emphasizes proactive protection through continuous user behavior monitoring and advanced threat detection powered by machine learning and anomaly scoring. This ability empowers organizations to identify and prevent potential in-

sider incidents before they escalate. It emphasizes continuous risk mitigation through a unique approach combining User and Entity Behavior Analytics (UEBA) with Identity and Access Management (IAM). This convergence allows users to monitor user behavior for anomalies, analyze access privileges, and contextualize activities within the organization. Gurucul utilizes machine learning models to generate risk scores to further strengthen its solution and enable security teams to prioritize investigations based on potential threat severity.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA, and rapidly expanding in JAPAC region, offering various use cases in industry verticals such as financial services, healthcare, manufacturing, retail, federal government, and energy & utilities can choose Gurucul Insider Risk Management platform.

Human Security

URL: https://www.humansecurity.com/

Founded in 2012 and headquartered in New York, New York, USA, Human Security offers cybersecurity solutions that protect organizations by disrupting bot attacks, digital fraud, and abuse.

The company offers comprehensive insider risk management capabilities through its Human Defense Platform, which tackles insider threats by constantly monitoring login attempts and user activity to identify anomalies that could signal malicious insider intent. These anomalies include unauthorized access attempts, suspicious data downloads, and unusual activity patterns. The Human Defense Platform detects such red flags and empowers organizations to take swift action and prevent insider threats before they escalate.

Analyst Perspective

Key Differentiators

- The Human Defense Platform continuously monitors user activity, even after successful logins, unlike traditional security measures that focus on perimeter defense. This ability enables the detection of suspicious behaviors that might indicate malicious intent, such as unauthorized data access attempts or unusual file downloads.

- The platform goes beyond simply monitoring activity logs by utilizing advanced analytics to identify anomalies in user behavior. The anomalies can include factors such as login attempts from unusual locations or times, access attempts to unauthorized files or systems, and significant deviations from a user's typical activity patterns.

- The platform leverages machine learning algorithms to continuously learn and adapt to evolving threats. This ability allows the platform to identify even the most sophisticated insider attacks, including those that attempt to bypass traditional security rules.

Product Strategy

- Technology Roadmap: Human Security is focusing on leveraging stronger AI and machine learning for deeper user behavior analysis, integrating with security ecosystems like UEBA and DLP tools, and offering enhanced user behavior analysis features to identify subtle anomalies indicative of insider threats.

- Strategic Roadmap: Human Security's strategic roadmap focuses on extending digital fraud management capability across the entire digital user journey, from the top of the marketing funnel to account creation, login, and transactions. This approach will allow the company to design the HUMAN Defense Platform to tackle diverse digital fraud use cases, increase its serviceable market, and leverage a larger data footprint in a domain where data is crucial.

Market Strategy

- Geo-expansion Strategy: Human Security has a strong customer base in North America, followed by EMEA. The company now plans to expand its presence in Asia Pacific.

- Industry Strategy: Human Security is catering to the digital advertising, finance, healthcare and insurance, public sector, retail and eCommerce, streaming and media, technology platforms, travel and entertainment, and FinTech domains.

- Use Case Support: Human Security supports various use cases, such as protection against threats like account takeover, account fraud, transaction abuse, scraping, client-side attacks and malvertising.

Customer/ User Success Strategy

- Human Security's offerings provide support on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- Human Security has established partnerships with various technological vendors, such as Ping Identity and Okta, as well as cloud platforms such as AWS, Google Cloud and Snowflake to provide deep integrations between custom-

er's existing solutions and the Human Defense Platform and to strengthen the capabilities to safeguard user organizations against digital attacks.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- Aligning with market trends, Human Security's Human Defense Platform leverages AI to analyze user activity and identify insider threats. It empowers organizations with real-time detection and potential customization for scalability, while its cloud-based nature ensures easy updates and potentially lower costs.

Final Take

- Human Defense platform is a robust Insider risk management solution that performs continuous user monitoring and anomaly detection, powered by machine learning, and can identify suspicious activity within an organization. This ability allows for early intervention and potential mitigation of insider threats. The platform can integrate with other security tools and complementary solutions to provide features like data loss prevention and user behavior analysis, offering a more holistic approach to insider risk mitigation.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA and rapidly expanding in the JAPAC region, and offering various use cases across industry verticals such as digital advertising, finance, healthcare and insurance, public sector, retail and eCommerce, streaming and media, technology platforms, travel and entertainment and FinTech can choose Human's Insider Risk management platform.

IBM

URL: https://www.ibm.com

Founded in 1991 and headquartered in Armonk, New York, USA, IBM is a leading provider of hardware, infrastructure, and solutions that cater to various segments. The company offers an insider risk management solution through its IBM Security QRadar suite. The solution helps user organizations identify and respond to security threats quickly and effectively. The IBM Security QRadar suite incorporates enterprise-grade AI and automation to significantly boost productivity, allowing resource-constrained security teams to work more efficiently across core technologies. It provides integrated solutions for endpoint security (EDR, XDR, MDR), log management, SIEM, and SOAR, all with a unified user interface, shared insights, and linked processes.

Analyst Perspective

Key Differentiators

- IBM Security QRadar provides Security QRadar UBA, which helps organizations create a baseline of behavior patterns that is vital for detecting threats within the organization's perimeter. It uses existing QRadar SIEM data to generate new insights about users and risk. It creates risk profiles for network users that help in providing accelerated response to suspect activity, including identity theft, hacking, phishing, or malware.

- IBM Security QRadar's Security QRadar EDR enables organizations to secure endpoints from cyberattacks, detect anomalous behavior, and remediate it in near real-time. It uses simple intelligent automation to remediate known and undiscovered endpoint threats in real- time using the support of advanced continuous learning AI capabilities and a user-friendly interface, it assists in making rapid and educated decisions using attack visualization storyboards and uses automatic alert management to focus on significant threats.

- IBM Security QRadar offers integration with Security QRadar SIEM which provides insights and workflows with broader security operations toolkits. It employs artificial intelligence and network and user behavior analytics, as well as built-in threat intelligence, federated search, and case management, to deliver more accurate, contextualized, and prioritized warnings. It provides enhanced

visibility through network behavior collection devices, event log sources, and AWS integrations, enhanced detection through network threat analytics, user behavior analytics and threat intelligence, as well as enhanced alerts through offense prioritization and high-risk users.

Product Strategy

- Technology Roadmap: IBM has introduced new AI-enhanced versions of IBM Storage Defender software to help organizations detect and respond to ransomware and other cyberattacks that threaten their data. This move aims to address the growing risks posed by insider threats such as data exfiltration and hardware failures. The technology leverages machine learning models to identify anomalies like ransomware and enable early detection of threats in the data stream.

- Strategic Roadmap: IBM plans to bring security and management across decentralized computing/digital environments with identity and digital assets which aims to enhance protection and trust to IT deployments and sovereign clouds. IBM's early breach notification driven by generative AI is planned to solve the security challenges posed by the expanded attack surface of decentralized IT deployments like sovereign clouds and virtual worlds.

Market Strategy

- Geo-expansion Strategy: IBM has a strong customer base in North America, followed by EMEA and the Asia Pacific region.

- Industry Strategy: IBM is catering its offering in automotive, banking, consumer goods, energy and utilities, government, health care, life sciences, insurance, manufacturing, retail, telecommunications, and travel domains.

- Use Case Support: IBM focuses on various use cases such as advanced threat detection, compliance, protection from ransomware, and threat hunting.

Customer/ User Success Strategy

- IBM offerings provide on-premises, private-cloud, and subscription-based public-cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- IBM has established partnerships with various system integrators and third-party integrations with key technology partnerships, including anomaly, CrowdStrike, and Cisco for threat intelligence, Proofpoint, Splunk, and Tenable for security analytics, and Varonis, NNT, and Security Scorecard For data security.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, IBM's proprietary AI algorithms and predictive analytics engine delve deep into data streams, identifying patterns and anomalies that might indicate potential risks. By analyzing historical data and real-time events, IBM provides actionable insights to decision-makers, enabling them to take timely preventive measures. Their customizable and scalable solutions cater to diverse industries and organizational sizes. The cloud platform enhances collaboration, reduces costs, and ensures seamless updates. IBM empowers users to navigate the complexities of insider risk management effectively with its intuitive UI and interactive dashboards.

Final Take

- IBM's cutting-edge insider risk management solution stands at the forefront of safeguarding organizations against internal threats. With a focus on proactive risk mitigation, IBM leverages advanced features such as AI-driven predictive analytics and real-time monitoring and empowers security teams and decision-makers with actionable insights, enabling timely intervention to mitigate insider risks. IBM's user-friendly interfaces ensure intuitive navigation, facilitating informed decision-making. In essence, IBM's innovative approach leads the way in addressing the multifaceted challenges of insider risk management, aligning seamlessly with evolving organizational needs.

- Users looking for an easy-to-use insider risk management solution with a strong customer base in North America, EMEA, and JAPAC region and offering support to various use cases across multiple industry verticals such as automotive, banking, consumer goods, energy and utilities, government,

health care, life sciences, insurance, manufacturing, retail, telecommunications, travel can choose IBM's Insider risk management platform.

Microsoft

URL: https://www.microsoft.com/en-in

Founded in 1975 and headquartered in Redmond, Washington, US, Microsoft is a global provider of computer software, hardware, mobile and gaming systems, and cloud services.

The Microsoft 365 Purview Insider Risk Management solution helps identify potential insider risks in a network. It also helps mitigate any insider risk by detecting it in advance, investigating it efficiently, and taking timely responsive action.

The solution includes policies that help define the types of risks that must be identified and detected. It helps in ensuring that all network users are under the compliance threshold and takes appropriate action in the event of a breach. It also offers role-based access controls and audit logs to protect user privacy.

Analyst Perspective

Key Differentiators

- The Microsoft 365 Purview Insider Risk Management solution enables policy creation using a machine learning playbooks feature that helps create policies using configurable machine learning templates that do not require the deployment of scripting or endpoint agents. It enables the creation of security policies that apply to all users in an organization and defines individuals or groups for management.

- The solution also offers an Insider Risk Management Adaptive protection feature, which leverages machine learning to analyze how users interact with data, identify dangerous behaviors likely to result in data security events, and then automatically implement Data Loss Prevention (DLP) safeguards based on the risk recognized. The feature enables the creation of dynamic DLP policies, guaranteeing that the most effective policy—such as banning data sharing—is applied exclusively to high-risk users while low-risk users can continue to work productively. It combines the variety of intelligence in Insider Risk Management with the extent of protection in DLP, allowing security teams to focus on developing strategic data security initiatives and completing their data security programs. Machine learning enables Adaptive Protection con-

trols to adjust automatically, allowing your organization to protect more (while using less) while maintaining workplace efficiency.

- The solution's case management feature assists in deep investigation and action on the issues reported by risk indicators defined by policies. Cases are manually created from alerts when more action is required to address a compliance-related concern for a user. Each case is assigned to a single user, and the user can have many alarms added to an existing or new case. Once the investigation is completed, further action can be initiated by sending the user a notice for it, resolving the case as benign, sharing the case with the email recipient, or escalating it for further investigation.

Product Strategy

- Technology Roadmap: Microsoft is focusing on integrating GenAI, AI capabilities, and advanced analytics into its insider risk management offerings through technological partnerships with Vodafone, Adobe, and NVIDIA.

- Strategic Roadmap: Microsoft's strategic roadmap for Insider Risk Management solutions focuses on leveraging the latest NVIDIA generative AI and Omniverse™ technologies across Microsoft Azure, Azure AI services, Microsoft Fabric, and Microsoft 365 to accelerate customer and first-party AI offerings through new integrations with NVIDIA.

Market Strategy

- Geo-expansion Strategy: Microsoft has a strong customer base in North America, followed by EMEA and Asia Pacific.

- Industry Strategy: Microsoft is expanding its offering in different operating segments such as productivity and business processes (Office Commercial, Office Consumer, LinkedIn, Dynamic Business Solutions), intelligent cloud, and personal computing.

- Use Case Support: Microsoft supports on various use cases such as prevention of various types of insider threats, including data exfiltration by departing employees, data leakage (malicious and inadvertent), security violations, regulatory compliance violations, fraud, and insider trading.

Customer/ User Success Strategy

- Microsoft offerings include on-premises, private-cloud, and subscription-based public-cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- Microsoft prioritizes collaboration to bolster its insider risk management solution. The solution can integrate with leading Security Information and Event Management (SIEM) providers like Splunk and Sumo Logic, enabling seamless data ingestion and analysis of security events alongside user behavior data. Additionally, Microsoft partners with UEBA specialists like Palo Alto Networks and McAfee, allowing for advanced user and entity behavior analysis within the Microsoft 365 environment. This focus on established security partners empowers organizations to leverage existing security investments and gain a comprehensive view of potential insider threats.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, Microsoft Insider Risk Management solution prioritizes tight integration with industry-leading Security Information and Event Management (SIEM) and User Entity Behavior Analytics (UEBA) tools. This enables organizations to seamlessly ingest and analyze security event data alongside user behavior information within the Microsoft 365 environment. This holistic view empowers security teams to correlate seemingly disparate events and identify potential insider threats with greater accuracy. Secondly, Microsoft emphasizes automation across the entire insider threat management lifecycle. This includes automating alert generation based on pre-defined behavioral baselines, streamlining investigation workflows with pre-built playbooks, and even automating remediation actions in specific scenarios. By automating these processes, Microsoft empowers security teams to focus on complex investigations and incident response, ultimately improving overall efficiency and reducing the time to identify and mitigate insider threats.

Final Take

- Microsoft Purview Insider Risk Management is a robust solution that addresses the evolving landscape of insider risk management. It identifies potential malicious or inadvertent insider risks by correlating various signals, such as IP theft, data leakage, and security violations. Customers can create policies to manage security and compliance effectively. Built with privacy in mind, the solution employs role-based access controls and maintains audit logs to ensure user-level privacy. This compliance solution enables organizations to detect, investigate, and act on insider threats, allowing risk analysts to swiftly enforce compliance standards. The solution analyzes real-time native signals across Microsoft 365 and third-party applications, including file activity, communications sentiment, abnormal user behaviors, and HR events. Furthermore, Microsoft empowers data security teams to proactively manage insider risks across cloud services, addressing challenges posed by the extensive use of public cloud services.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA, and JAPAC region and offering various use cases in industry verticals, such as protection from insider threats like data exfiltration by departing employees, data leakage (malicious and inadvertent), security violations, regulatory compliance violations, fraud, and insider trading can opt for Microsoft Insider Risk Management solution.

OpenText (Microfocus)

URL: https://www.opentext.com/

Founded in 1976 and headquartered in Waterloo, Ontario, Canada, OpenText is a provider of advanced analytics-based business and IT security transformative products. OpenText offers an insider risk management solution through ArcSight Intelligence solution that protects organizational IT systems by exposing and analyzing cyber threats by integrating with CrowdStrike Falcon endpoint detection.

The company leverages ArcSight Intelligence's behavioral analytics, which adds contextualization to help organizations analyze cyber threats. It allows organizations to identify abnormal login patterns, sudden or unusual file or system activity, user impersonation, internal recon, or low and slow attacks. When these threats are identified, threat leads are automatically passed on to organizational security teams or the CrowdStrike Falcon OverWatch™ service for further investigation.

Analyst Perspective

Key Differentiators

- OpenText offers an Insider Threat Mitigation solution that leverages unsupervised machine learning, advanced models, and a threat-hunting user interface to detect risky and anomalous insider behavior in real-time. The solution also helps detect other threats like fraud, data breaches, IP theft, abuse, as well as advanced threats and optimize analyst productivity. MicroFocus ArcSight Intelligence allows intuitive, contextualized detection and investigation and provides downloadable reports that describe current threats.

- MicroFocus ArcSight Intelligence provides insights into the lifecycle of cyber threats. These insights help users to react rapidly and remediate cyber threats successfully. MicroFocus leverages ArcSight Intelligence AI algorithms to allow organizations to have deep insights about the detection of abnormal behavior. Its automated intelligent risk scoring mechanism allows organizations to prioritize the cyber threats that have to be investigated for strengthening the cybersecurity ecosystem of organizations.

- Micro Focus ArcSight Intelligence provides emphasis in investigational process with prioritized threat leads by combining unsupervised machine learn-

ing with mathematical probability for calculating risk scores that portrays which entities are suspicious and cause damage to sensitive IT assets, this allows ArcSight Intelligence in enabling organization to deconstruct numerous IT events into productive threat leads, eliminates alert fatigue and allows organizational IT systems to focus on investigating the cyber threats which are in high priority to be dealt with.

Product Strategy

- Technology Roadmap: OpenText focuses on integrating GenAI, AI capabilities and advanced analytics across its entire product portfolio.

- Strategic Roadmap: OpenText's strategic roadmap for its Insider Risk Management solutions focuses on its new unified OpenText Partner Network. The OpenText Partner Network unifies OpenText's and recently acquired Micro Focus' partner ecosystems to offer cohesive support and greater opportunities to the entire network consisting of more than 30,000 partners. It is now aligned under a standardized program framework, where partners will have access to OpenText's information management that will equip them with best-in-class solutions to deliver exceptional value to enterprise customers.

Market Strategy

- Geo-expansion Strategy: Open Text has a strong customer base in North America, followed by EMEA. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: OpenText is catering its offering in automotive, banking, insurance, healthcare, life sciences, oil and gas, industrial manufacturing, public sector, and utilities.

- Use Case Support: OpenText supports various use cases such as advanced threat detection, user activity history and alert investigation, process case resolution, and enhanced security and compliance.

Customer/ User Success Strategy

- OpenText's offerings include on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- OpenText has established partnerships with various system integrators and third-party integrations with key strategic technology partnerships, including public cloud partners such as AWS, Google Cloud, and Azure, as well as enterprise application partners such as Microsoft, Salesforce and SAP, and global system integrators, such as Accenture, Capgemini, Cognizant, Deloitte, and TCS.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, the OpenText Insider Risk Management solution addresses the evolving landscape of insider risk management by combining endpoint and network visibility with cutting-edge enterprise investigation technology. This synergy enables organizations to detect and mitigate insider threats more effectively. OpenText's approach empowers businesses to increase visibility into threat landscape, enhance threat detection capabilities, and expand off-network collection.

Final Take

- OpenText empowers organizations to gain a holistic view of user activity and data access by leveraging its expertise in content management and security, and through potential partnerships with SIEM, UEBA, and DLP vendors, OpenText's platform facilitates the correlation of security events with user behavior, enabling the identification of subtle anomalies that might indicate insider threats. Additionally, OpenText's focus on content security features like data classification and access controls strengthens organizations' ability to safeguard sensitive information. This combined approach empowers security teams with the tools and insights needed to proactively detect, investigate, and mitigate insider threats, ultimately safeguarding critical information.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA and is rapidly expanding in JAPAC region and supporting various use cases in industry verticals such as Automotive, banking, insurance, healthcare, life sciences, oil and gas, indus-

trial manufacturing, public sector and utilities can choose Open Text's Insider risk management platform.

RSA Security

URL: https://www.rsa.com/

Founded in 1982 and headquartered in Burlington, MA, USA, RSA Security is a provider of cybersecurity and digital risk management solutions.

RSA offers insider risk management capabilities through its RSA NetWitness platform, which acts as a central hub, collecting and analyzing data from diverse sources across the network, applications, and endpoints. The platform helps ingest security logs, network traffic, endpoint activity, user behavior, and threat intelligence feeds. This comprehensive data pool provides a unified view for threat detection and provides security teams with a complete picture of their security landscape.

Analyst Perspective

Key Differentiators

- RSA Insider Risk Management leverages user behavior analytics (UBA) to collect and analyze vast amounts of security data from diverse sources, including user activity logs, endpoint data, and application usage across the users' networks. This rich data pool empowers RSA's UBA engine to identify subtle anomalies in user behavior that might deviate from established baselines. These deviations could signal potential malicious intent, allowing security teams to proactively address insider threats before they escalate into major security incidents.

- RSA Insider Risk Management goes beyond basic anomaly detection by integrating sophisticated risk scoring algorithms within the UBA framework. These algorithms analyze not only the type of anomaly but also factors like the user's role, access privileges, and historical behavior. This risk-based approach prioritizes the most critical threats based on their potential impact. Security teams can then focus their investigations on high-risk individuals, maximizing efficiency and ensuring swift response to the most concerning insider threats.

- RSA Insider Risk Management provides a dedicated toolkit for investigating potential insider threats. This comprehensive set of tools includes detailed user profiles, encompassing historical activity data, access privileges, and

role information. The solution also offers in-depth activity logs that capture user actions, file transfers, and application usage over time. Finally, its advanced reporting capabilities allow security teams to analyze trends, identify patterns, and gather the necessary contextual evidence to make informed decisions about mitigation strategies. This focus on providing a comprehensive view of potential insider threats empowers security teams to take decisive action and safeguard critical data.

Product Strategy

- Technology Roadmap: RSA Security's roadmap prioritizes a future-proof security posture by emphasizing Extended Detection and Response (XDR) for providing a holistic threat view across diverse security tools by leveraging AI-powered threat detection and integrating Machine Learning (ML) and Artificial Intelligence (AI) across their product suite.

- Strategic Roadmap: RSA's strategic roadmap revolves around security and trust through investments in Identity as a Service (IDaaS) growth in Japan, Canadian SaaS market, support for Zero Trust initiatives through open standards, AI-driven identity security insights, and strategic partnerships. As RSA continues to innovate, their focus remains on safeguarding identities and data in an ever-evolving threat landscape.

Market Strategy

- Geo-expansion Strategy: RSA Security has a strong customer base in North America, followed by EMEA. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: RSA Security is catering its offering in manufacturing, healthcare, banking & investment services, and the insurance sector.

- Use Case Support: RSA Security supports various use cases such as Moving IAM To the cloud, passwordless authentication, risk-based authentication, and zero trust access.

Customer/ User Success Strategy

- RSA Security's offerings provide support on-premises and cloud deploy-

ments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- RSA Security has established partnerships with different advisory firms, systems integrators, outsources, and other firms that do not resell while offering benefits such as deal registration and sales and product training.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- In these spaces, RSA Security tackles evolving insider threats with AI-powered UBA, offering deeper insights for proactive mitigation. Recognizing the need for flexibility, they provide a customizable and scalable solution that adapts to diverse industry needs and organizational growth. Furthermore, RSA prioritizes user experience with intuitive dashboards and customizable views, empowering security teams to efficiently analyze data, make informed decisions, and maximize the platform's potential.

Final Take

- Leveraging the power of RSA NetWitness, its core security platform, RSA Insider Risk Management goes beyond basic anomaly detection. By integrating sophisticated User Behavior Analytics (UBA) with advanced risk scoring and contextual investigation tools, this solution empowers security teams to identify and prioritize the most critical insider threats. This user-centric approach, with intuitive dashboards and detailed user profiles, facilitates informed decision-making and swift action. By mitigating insider risk efficiently, RSA empowers organizations to safeguard sensitive data, build trust within their workforce, and fortify their digital environment for a more secure future.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA and rapidly expanding in JAPAC region offering various use cases in industry verticals such as manufacturing, healthcare, BFSI can choose RSA insider risk management solution.

Securonix

URL: https://www.securonix.com/

Founded in 2008 and headquartered in Addison, Texas, USA, Securonix offers a suite of next-generation security analytics and operations management platform for big data threats and advanced cyber threats.

Securonix offers Insider Risk Management solution through the Securonix Security Analytics and Operations Platform. Securonix IRM continuously monitors user activity across diverse data sources, including network traffic, system logs, and application access logs. This monitoring allows the creation of user baselines and identification of the deviations that might indicate malicious insider intent. By analyzing these deviations alongside context-rich security data, Securonix IRM identifies potential insider threats such as unauthorized data exfiltration attempts, privilege abuse, or violations of security policies.

Analyst Perspective

Key Differentiators

- Securonix Insider risk management solution offers Entity Context and Peer Group Analysis, which leverages its Security Data Lake to create a comprehensive identity and risk profile for every user and entity within the user organization. Furthermore, the platform utilizes Peer Group Analysis, which compares the actions of one user against their peers within similar roles or departments. This comparison allows the identification of outliers and potential insider threats that might not be apparent through individual user monitoring.

- Securonix Insider risk management solution utilizes advanced UEBA (User and Entity Behavior Analytics) capabilities to go beyond simple anomaly detection. It integrates machine learning algorithms to identify subtle behavioral changes that might indicate malicious intent. These algorithms learn from historical data and adapt to evolving insider threat tactics. This adaption allows Securonix IRM to detect even the most sophisticated insider threats that attempt to evade traditional detection methods.

- Securnoix Insider risk management, through its threat detection with risk

scoring and prioritization utilizes risk scoring based on a combination of factors, such as the severity of the detected anomaly, the user's access privileges, and the sensitivity of the data involved. This scoring empowers security teams to focus their resources on the most critical cases, allowing for faster response times and mitigation of high-risk insider threats.

Product Strategy

- Technology Roadmap: Securonix is focusing on integrating GenAI, AI capabilities, advanced analytics, and simulation capabilities to enhance its product. The company's product roadmap includes innovative initiatives like the Unified Defense SIEM, which provides 365 days of 'Hot' data powered by Snowflake, enabling faster response times and proactive defense.

- Strategic Roadmap: Securonix's strategic roadmap is focused on adapting to the evolving threat landscape by embracing trends such as increased data needs, generative AI, and integrated automation. Their integration with ChatGPT enhances threat resolution using artificial intelligence.

Market Strategy

- Geo-expansion Strategy: Securnoix has a strong customer base in North America, followed by Asia Pacific and Europe.

- Industry Strategy: Securonix caters its offering in manufacturing, financial services, healthcare, banking & investment services, and the insurance sector.

- Use Case Support: Securonix supports various use cases, such as monitoring compliance violations, investigating unusual file transfers, identifying disgruntled employees, detecting data exfiltration attempts, and monitoring privileged users.

Customer/ User Success Strategy

- Securonix offerings provide support on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- Securonix has established partnerships with various technological vendors such as AWS, Cloudera, Netskope, Okta, and ServiceNow through the Secu-

ronix fusion program to provide a robust integrated solution.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- Securonix aligns with these trends by offering a next-generation Security Analytics and Operations Platform that integrates UEBA (User and Entity Behavior Analytics) with advanced machine learning. This powerful combination enables organizations to gain deep insights into user behavior and entity relationships, allowing for a more comprehensive understanding of potential insider threats.

Final Take

- Securonix offers a cutting-edge solution for insider threat detection and response through its security analytics and operations management suite. Their platform leverages industry-leading Next-Gen SIEM and behavior analytics to uncover elusive threats originating from within an organization. With a focus on predictive analytics and Generative AI, Securonix's Insider Threat Detection & Response solution ensures operational excellence, process design, and automation. The platform empowers informed decision-making through user-friendly interfaces, enabling effective business process optimization. In essence, Securonix's innovative approach advances insider risk management, providing simplicity and continuous improvement aligned with evolving organizational needs.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA, and JAPAC region offering various use cases in industry verticals such as manufacturing, financial services, healthcare, BFSI can choose Securonix Insider Risk Management platform.

Veriato

URL: https://veriato.com/

Founded in 1998 and headquartered in West Palm Beach, Florida, USA, Veriato offers solutions for Insider Risk Management (IRM), behavioral analytics, user activity monitoring (UAM), and data loss prevention (DLP) in a single platform using AI-based user behavior analytics to help companies prevent risks and increase productivity in their remote, hybrid and in-office environments.

Veriato Insider Risk Management (IRM) strengthens the user organization's cybersecurity posture by proactively identifying potential insider threats through its AI-powered solution, which leverages advanced user behavior analytics (UEBA) and machine learning to analyze user activity across various platforms.

Analyst Perspective

Key Differentiators

- The solution utilizes Generative AI to analyze user behavior and interpret complex signals like tone, sentiment, and use of sensitive data (PII/PHI) alongside traditional activity data. This comprehensive analysis creates a more nuanced risk profile for each user.

- Veriato Insider Risk Management solution boasts a user-friendly interface that simplifies threat detection and investigation. Additionally, the platform offers customization options that allow the security teams to tailor risk scoring and monitoring parameters to their specific needs and organizational context.

- Veriato IRM goes beyond basic user activity monitoring (UAM) by incorporating UEBA. It also analyses the context surrounding the actions, like login times, file access patterns, and communication trends. This deeper analysis helps identify subtle behavioral deviations that could indicate potential threats.

Product Strategy

- Technology Roadmap: Veriato is focusing on integrating GenAI, AI capabilities, advanced analytics, and simulation capabilities to enhance user experience and make better business decisions by predicting future outcomes.

Additionally, the platform could integrate with behavioral science models to refine risk scoring based on user psychology.

- Strategic Roadmap: Veriato's strategic roadmap for Insider Risk Management solution is to prioritize deeper user context analysis by integrating Insider risk management with communication platforms to analyze email tone and sentiment alongside behavioral patterns. This, combined with potential user psychology models, could predict and prevent insider threats before they escalate.

Market Strategy

- Geo-expansion Strategy: Veriato has a strong customer base in North America, followed by EMEA. The company plans to expand its presence in Asia Pacific.

- Industry Strategy: Veriato is catering to the financial services, healthcare, government, and higher education segments.

- Use Case Support: Veriato supports various use cases, such as insider risk management, user activity monitoring, employee productivity, workplace investigations, and audits and compliance.

Customer/ User Success Strategy

- Veriato offerings provide support for on-premises and cloud deployments. Its primary offering is cloud-based but offers flexibility for on-prem and hybrid deployments.

- Veriato has established partnerships with various system integrators and third-party integrations to offer an enhanced insider risk management solution.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- Veriato aligns with the insider risk management market's tech trends by leveraging advanced data analytics and AI. Its Generative AI analyzes user behavior beyond actions, including tone and data usage, for a comprehensive risk profile. Veriato IRM offers a user-friendly interface and customization options, allowing organizations to tailor threat detection to their specific needs. This focus on user experience empowers security teams to act swiftly and effectively.

Final Take

- By prioritizing cutting-edge AI and user behavior analytics, Veriato IRM positions itself ahead in proactive insider threat detection. Its ability to analyze user intent and sentiment alongside traditional activity data empowers security teams to identify potential threats before they cause harm. This focus on user context, combined with a user-friendly interface, allows organizations to make informed decisions and safeguard sensitive data, ultimately fostering a more secure and resilient business environment.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA and rapidly expanding in the JAPAC region, offering various use cases in industry verticals such as Financial Services, Healthcare, Government and Higher Education can choose Veriato Insider risk management platform.

CyberHaven

URL: https://www.cyberhaven.com/

Founded in 2016 and headquartered in Palo Alto, California, USA, CyberHaven offers DLP, data protection, insider threat, data tracing, and data lineage solutions. Cyberhaven's Data Detection and Response (DDR) solution goes beyond traditional data loss prevention (DLP) tools by employing a unique approach to insider threat management by focusing on the data itself. The solution utilizes advanced data lineage tracking to follow sensitive information wherever it goes. From original creation to user access attempts, Cyberhaven's DDR continuously monitors data movement, providing real-time insights into potential insider risks.

This focus on data lineage empowers organizations to identify and stop unauthorized access or exfiltration attempts before they occur. By prioritizing data protection throughout its lifecycle, Cyberhaven's DDR solution offers a comprehensive approach to mitigating insider threats and safeguarding sensitive information.

Analyst Perspective

Key Differentiators

- Unlike traditional security solutions that focus on user activity, CyberHaven's DDR prioritizes data itself. This means the platform continuously tracks the lineage of sensitive information, identifying its origin, movement, and access attempts. This data-centric approach provides a more comprehensive view of potential insider threats compared to just monitoring user behavior.

- With its focus on data movement, CyberHaven's DDR offers real-time insights into potential insider risks. The platform can detect suspicious access attempts, data exfiltration efforts, or unauthorized modifications as they happen. This allows security teams to intervene immediately and prevent significant data breaches or leaks.

- CyberHaven DDR utilizes advanced analytics and AI to analyze data movement patterns and user access attempts. This allows the platform to differentiate between authorized and suspicious activity, considering the user's role, access needs, and typical data interactions. This contextual understanding reduces false positives and empowers security teams to focus on genuine insider threats.

Product Strategy

- Technology Roadmap: CyberHaven has launched the Linea AI platform designed to combat critical insider risks and safeguard vital corporate data. Linea AI applies human-like insight across billions of workflows to understand an organization's data, when it's at risk, and what's needed to protect it—with precision.

- Strategic Roadmap: CyberHaven's DDR roadmap prioritizes expanding its focus beyond data movement with the integration of user behavior analytics tools to create a more holistic risk profile. Additionally, automation features for incident response and remediation could be implemented, allowing for faster and more efficient mitigation of insider threats.

Market Strategy

- Geo-expansion Strategy: CyberHaven has a strong customer base in North America, followed by EMEA. The company now plans to expand its presence in Asia Pacific.

- Industry Strategy: CyberHaven caters to technology, manufacturing, law firms, investment management, and healthcare.

- Use Case Support: CyberHaven focuses on various use cases, such as understanding data flows, stopping data exfiltration anywhere, accelerating internal investigations, and detecting and stopping risky behavior.

Customer/ User Success Strategy

- CyberHaven's offerings provide support for on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- CyberHaven has established partnerships with various system integrators and third-party integrations such as Optiv, EVOTEK, ignition and Presidio to safeguard customer data in a comprehensive manner.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- Cyberhaven aligns with the insider risk management market trends through its Data Detection and Response (DDR) solution. It leverages advanced data analytics and AI to track data lineage, providing real-time insights into user access and potential exfiltration attempts. While Cyberhaven doesn't directly offer user behavior monitoring or customization options, its focus on data movement aligns with organizational agility and resilience by allowing for proactive threat detection and prevention.

Final Take

- Cyberhaven's Data Detection and Response (DDR) solution stands out in insider risk management by prioritizing the data itself. Using advanced data lineage tracking and AI, it offers real-time insights and proactive threat prevention. While customization options might be limited, this data-centric approach aligns with the market's emphasis on agility and resilience. Ultimately, Cyberhaven's DDR empowers organizations to safeguard sensitive information and make informed decisions, fostering a more secure and data-protected environment.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA and rapidly expanding in the JAPAC region, offering various use cases in industry verticals such as technology, manufacturing, law firms, investment management, and healthcare can choose CyberHaven Insider risk management platform.

Dasera

URL: https://www.dasera.com/

Founded in 2019 and headquartered in Mountain View, California, USA, Dasera offers a Data Security Posture Management (DSPM) platform providing automated security and governance controls for structured and unstructured data across cloud and on-prem environments.

The company offers a comprehensive Data Security Posture Management (DSPM) platform which plays a crucial role in mitigating such threats. The platform focuses on data security throughout its lifecycle – from creation to storage and access. The continuous monitoring and analysis of activity data analysis enables organizations to identify anomalies and suspicious behavior patterns indicating potential insider threats.

This proactive approach allows security teams to address risks before they escalate. Dasera's platform provides valuable insights into user activity and data access attempts. By analyzing these insights, security teams can identify individuals who might be misusing data or exhibiting behavior indicative of malicious intent.

Analyst Perspective

Key Differentiators

- Unlike traditional security solutions that focus on specific points in time, Dasera offers a continuous approach to data security. The platform constantly monitors and analyzes data activity across its lifecycle, providing a comprehensive view of potential insider threats. This view allows for early detection of suspicious behavior compared to solutions that only analyze data at specific points.

- Dasera's platform goes beyond simply monitoring user activity by analyzing user behavior alongside contexts like data type, access attempts, and historical activity patterns. This contextual analysis allows for a more nuanced understanding of user intent and helps identify suspicious behavior that might otherwise be overlooked. For example, a user accessing a highly sensitive file for the first time outside of regular working hours could be flagged for further investigation.

- Dasera excels in data lineage tracking. Its platform tracks data movement from its origin to wherever it goes, regardless of its form. This ability allows security teams to identify potential insider attempts at data exfiltration or unauthorized access. By understanding how data is being used and accessed, organizations can proactively mitigate risks associated with insider threats.

Product Strategy

- Technology Roadmap: Dasera has added data security and governance scores to its comprehensive dashboard, giving customers a clear view of their data's security posture. This feature highlights potential security risks, allowing businesses to address them proactively. The dashboard also reveals the extent of sensitive data exposure and identifies infrastructure, data, users, and applications risks while monitoring data usage through query analysis. This enables administrators to detect and resolve issues swiftly, ensuring robust protection for the organization's data.

- Strategic Roadmap: Dasera's strategic roadmap focuses on integrating with a wider range of cloud storage platforms, allowing them to track data movement even after it leaves the organization's primary environment. This would provide a more comprehensive view of potential insider attempts at data exfiltration, especially with the rise of Shadow IT.

Market Strategy

- Geo-expansion Strategy: Dasera has a strong customer base in North America, followed by EMEA. The company now plans to expand its presence in Asia Pacific.

- Industry Strategy: Dasera caters to manufacturing, healthcare, banking & investment services, and insurance sectors.

- Use Case Support: Dasera supports various use cases, such as contextualized visibility, Data Security Posture Management (DSPM), Data Access Governance (DAG), data usage risk management, compliance monitoring, and Data Detection & Response (DDR).

Customer/ User Success Strategy

- Dasera offerings provide support for on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- Dasera has established partnerships with various system integrators and third-party integrations, such as Snowflake, Google Cloud, Splunk, Sumo Logic, Datadog, LogRhythm, slack, Okta, Ping Identity, and One login to integrate with customers' existing data architecture to operationalize their data governance.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- Dasera aligns with the insider risk management market trends through its Data Security Posture Management (DSPM) platform. While customization options might be limited, Dasera leverages advanced data analytics and AI to continuously monitor data activity. This provides real-time insights into user behavior and potential insider threats. Furthermore, Dasera's data lineage tracking offers a comprehensive view of data movement, fostering organizational agility and resilience in addressing insider risks.

Final Take

- By adopting a data-centric approach, Dasera's DSPM platform transcends traditional insider risk management solutions. The platform's continuous data monitoring and contextual user activity analysis empower organizations to proactively identify and mitigate potential threats. This focus on data lineage and comprehensive security posture management fosters organizational resilience against insider risks. Ultimately, Dasera empowers security teams with actionable insights, allowing them to safeguard sensitive data and navigate the evolving threat landscape.

- Users looking for an easy-to-use Insider Risk Management solution with a

strong customer base in North America, EMEA and rapidly expanding in the JAPAC region, offering various use cases in industry verticals such as manufacturing, healthcare, BFSI can choose Dasera Insider risk management platform.

Do Control

URL: https://www.docontrol.io/

Founded in 2020 and headquartered in New York, USA, Do Control offers a SaaS Security Platform (SSP) that recognizes the evolving threat landscape and places a strong emphasis on mitigating insider threats within cloud applications. The platform leverages AI-powered threat detection and automation to continuously monitor user activity across various SaaS applications. By analyzing user behavior specific to each platform, Do Control can identify suspicious actions that might otherwise go unnoticed.

This comprehensive approach empowers security teams to proactively address potential insider risks. Do Control helps minimize the risk of data breaches and security incidents by providing real-time insights into user activity. The platform's focus on automation further streamlines threat detection and response. When suspicious activity is detected, the platform can automatically trigger pre-defined workflows, allowing security teams to react quickly and efficiently. These workflows can include actions like account suspension, data exfiltration prevention, or user access restriction.

Analyst Perspective

Key Differentiators

- The Do Control platform integrates seamlessly with a wide range of SaaS applications, providing deeper visibility into user activity within these critical platforms. This visibility allows the analysis of user behavior specific to each application to identify suspicious actions that might not be readily apparent in traditional security solutions.

- The Do Control platform prioritizes real-time analysis of user activity. This prioritization allows the platform to identify and respond to potential insider threats as they happen, minimizing the risk of data breaches or other security incidents.

- Do Control emphasizes automation to streamline threat detection and response. The platform can automatically trigger pre-defined workflows based on suspicious activity, allowing security teams to react swiftly and efficiently. This automation can also involve actions like account suspension, data exfil-

tration prevention, or user access restriction.

Product Strategy

- Technology Roadmap: Do Control is focusing on integrating GenAI, AI capabilities, advanced analytics, and simulation capabilities into its products to enhance user experience and make better business decisions by predicting future outcome.

- Strategic Roadmap: Do Control's strategic roadmap prioritizes expanding its platform's capabilities beyond real-time threat detection with features like user risk scoring based on behavioral trends and machine learning. Additionally, integration with user behavior analytics (UEBA) tools will provide a more holistic view of user activity, potentially identifying insider threats even before suspicious actions occur.

Market Strategy

- Geo-expansion Strategy: Do Control has a strong customer base in North America, followed by EMEA. The company now plans to expand its presence in Asia Pacific.

- Industry Strategy: Do Control caters to manufacturing, healthcare, banking & investment services, and insurance sectors.

- Use Case Support: Do Control supports various use cases such as CASB, SaaS to SaaS, cloud-native DLP and insider risk management.

Customer/ User Success Strategy

- Do Control offerings provide support for on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.

- Do Control has established partnerships with various technological vendors, such as Datadog, Github, AWS, Google, Slack, Zoom, and Okta, to provide a differentiated SaaS Security Solution for today's cloud security challenges for its customers.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- Do Control aligns with the insider risk management market trends through its SaaS security platform. It leverages AI for threat detection, analyzing user activity across various cloud applications. This focus on user behavior provides real-time insights and allows for proactive risk mitigation. Its focus on SaaS applications directly addresses the need for agility and resilience by enabling organizations to secure their specific cloud environment.

Final Take

- By offering a platform specifically designed for SaaS security, Do Control empowers organizations to address potential insider threats proactively. Real-time analysis, automation of workflows, and deep integration with SaaS applications combine to provide a comprehensive solution for mitigating insider risks. This allows organizations to protect sensitive data, ensure regulatory compliance, and foster a more secure cloud environment.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA and rapidly expanding in the JAPAC region, offering various use cases in industry verticals such as manufacturing, healthcare, BFSI can choose Do Control Insider risk management platform.

Secure Passage (Formerly Haystax)

URL: https://securepassage.com/

Founded in 2012 and headquartered in Kansas City, Missouri, USA, Secure Passage (Formerly Haystax) offers cybersecurity solutions for enterprise threat management, public safety risk management, security analytics, situational awareness, school safety management, secure cloud applications, physical security, and assessments.

The company offers a comprehensive insider risk management (IRM) solution to mitigate insider threats by focusing on user behavior and activity within the organization. SecurePassage IRM leverages advanced analytics and machine learning to continuously monitor user activity across various systems and applications. By analyzing these actions and identifying anomalies, the platform empowers security teams to proactively address potential insider risks before they escalate into significant security incidents.

SecurePassage IRM provides valuable insights into user behavior patterns. By analyzing these insights, security teams can identify individuals who might be exhibiting suspicious behavior or attempting unauthorized access to sensitive information. This allows for early intervention and mitigation strategies to be implemented before any damage occurs.

Analyst Perspective

Key Differentiators

- Secure Passage IRM goes beyond simply monitoring user activity and identifying anomalies within that activity. The platform utilizes advanced machine learning models to analyze user behavior patterns and flag deviations from established baselines. This allows security teams to focus on users whose actions deviate significantly from their typical patterns, potentially indicating malicious intent.

- The platform analyzes user activity alongside various contextual factors, such as time of day, location, access attempts to specific data types, and recent changes in job roles or access privileges. This comprehensive analysis provides a more nuanced understanding of potential insider threats and helps prioritize investigation efforts.
- Secure Passage IRM empowers security teams with actionable insights. The

platform identifies anomalies and assigns risk scores to users based on the severity of their suspicious activity and the context surrounding it. This scoring allows security teams to prioritize their investigations and focus on the users posing the most significant insider threat risk.

Product Strategy

- Technology Roadmap: Secure Passage is focusing on integrating with threat intelligence platforms for enriched risk assessments and exploring advanced AI techniques. This involves unsupervised anomaly detection to identify novel suspicious behavior and even predict future insider threats through advanced machine learning algorithms, ultimately evolving SecurePassage IRM into a more comprehensive and predictive solution for mitigating insider threats.

- Strategic Roadmap: Haystax announces a name change to Secure Passage and a renewed focus on converged security with an objective to provide a secure passage for our customers by architecting security into all products we. This change further aligns with focus on delivering converged security products and services.

Market Strategy

- Geo-expansion Strategy: Secure Passage has a strong customer base in North America, followed by EMEA. The company now plans to expand its presence in Asia Pacific.

- Industry Strategy: Secure Passage is catering its offering in manufacturing, healthcare, banking & investment services, and insurance sectors.

- Use Case Support: Secure Passage supports various use cases, such as data loss prevention and insider risk management.

Customer/ User Success Strategy

- Secure Pasage offerings provide support for on-premises and cloud deployments. Its primary offering is cloud-based but offers deployment flexibility for on-prem and hybrid deployments.
- Secure Passage has established partnerships with various system integrators

and third-party integrations, for enhanced capabilities and integrations.

Trend Analysis

- The Insider Risk Management market is moving towards technological trends, which include advanced data analytics and AI integration, organizational agility and resilience, customization, and scalability, as well as focus on user experience and interactivity.

- SecurePassage IRM aligns with the insider risk management market trends through its use of advanced data analytics and AI. Their platform continuously monitors user activity and leverages machine learning to detect anomalies in user behavior. This focus on user activity analysis allows for proactive threat detection and mitigation. While SecurePassage IRM might not offer extensive customization options, its contextual threat assessment fosters organizational resilience by prioritizing investigation efforts based on relevant factors.

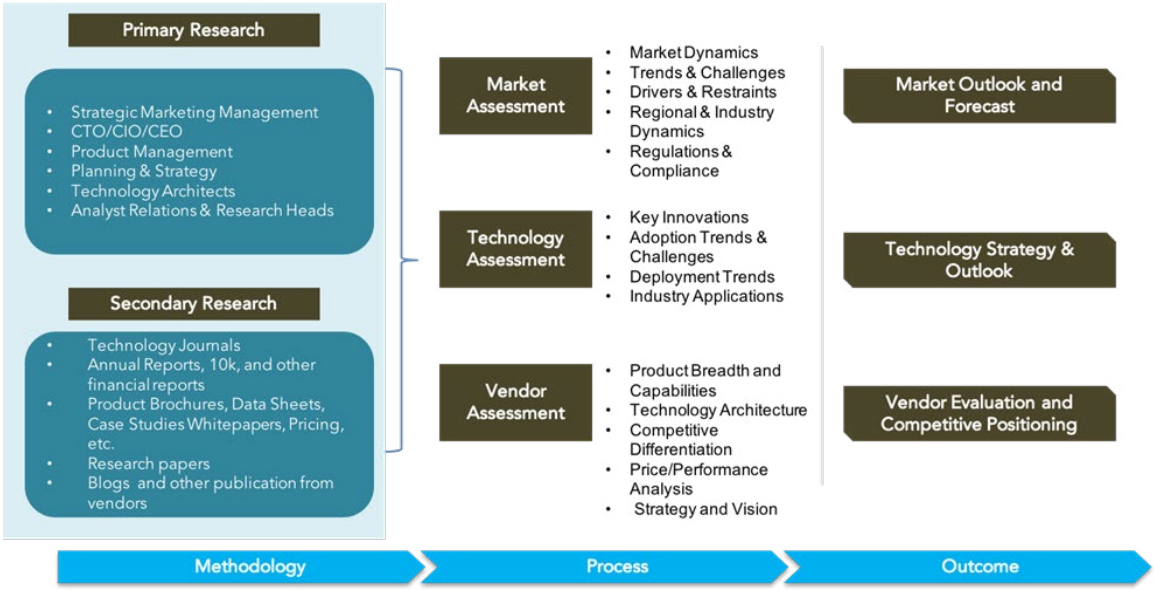
Final Take

- Secure Passage IRM positions itself as a leader in proactive insider risk management by prioritizing user behavior analysis and context-rich threat assessments. Its AI-powered anomaly detection and risk scoring empower security teams to identify and prioritize potential threats before they escalate. Despite limitations in customization options, Secure Passage IRM fosters organizational agility through its focus on actionable insights. Ultimately, the platform provides a comprehensive solution for mitigating insider risks and safeguarding sensitive data within a user-friendly and informative interface.

- Users looking for an easy-to-use Insider Risk Management solution with a strong customer base in North America, EMEA and rapidly expanding in the JAPAC region, offering various use cases in industry verticals such as manufacturing, healthcare, BFSI can choose Secure Passage Insider risk management platform.

Research Methodologies

Quadrant Knowledge Solutions uses a comprehensive approach to conduct global market outlook research for various technologies. Quadrant's research approach provides our analysts with the most effective framework to identify market and technology trends and helps in formulating meaningful growth strategies for our clients. All the sections of our research report are prepared with a considerable amount of time and thought process before moving on to the next step. Following is the brief description of the major sections of our research methodologies.



Secondary Research

Following are the major sources of information for conducting secondary research:

Quadrant's Internal Database

Quadrant Knowledge Solutions maintains a proprietary database in several technology marketplaces. This database provides our analyst with an adequate foundation to kick-start the research project. This database includes information from the following sources:

- Annual reports and other financial reports
- Industry participant lists
- Published secondary data on companies and their products
- Major market and technology trends

Literature Research

Quadrant Knowledge Solutions leverages on several magazine subscriptions and other publications that cover a wide range of subjects related to technology research. We also use the extensive library of directories and Journals on various technology domains. Our analysts use blog posts, whitepapers, case studies, and other literature published by major technology vendors, online experts, and industry news publications.

Inputs from Industry Participants

Quadrant analysts collect relevant documents such as whitepaper, brochures, case studies, price lists, datasheet, and other reports from all major industry participants.

Primary Research

Quadrant analysts use a two-step process for conducting primary research that helps us in capturing meaningful and most accurate market information. Below is the two-step process of our primary research:

Market Estimation: Based on the top-down and bottom-up approach, our analyst analyses all industry participants to estimate their business in the technology market for various market segments. We also seek information and verification of client business performance as part of our primary research interviews or through a detailed market questionnaire. The Quadrant research team conducts a detailed analysis of the comments and inputs provided by the industry participants.

Client Interview: Quadrant analyst team conducts a detailed telephonic interview of all major industry participants to get their perspectives of the current and future market dynamics. Our analyst also gets their first-hand experience with the vendor's product demo to understand their technology capabilities, user experience, product features, and other aspects. Based on the requirements, Quadrant analysts interview with more than one person from each of the market participants to verify the accuracy of the information provided. We typically engage with client personnel in one of the following functions:

- Strategic Marketing Management
- Product Management
- Product Planning
- Planning & Strategy

Feedback from Channel Partners and End Users

Quadrant research team researches with various sales channel partners, including distributors, system integrators, and consultants to understand the detailed perspective of the market. Our analysts also get feedback from end-users from multiple industries and geographical regions to understand key issues, technology trends, and supplier capabilities in the technology market.

Data Analysis: Market Forecast & Competition Analysis

Quadrant's analysts' team gathers all the necessary information from secondary research and primary research to a computer database. These databases are then analyzed, verified, and cross-tabulated in numerous ways to get the right picture of the overall market and its segments. After analyzing all the market data, industry trends, market trends, technology trends, and key issues, we prepare preliminary market forecasts. This preliminary market forecast is tested against several market scenarios, economic most accurate forecast scenario for the overall market and its segments.

In addition to market forecasts, our team conducts a detailed review of industry participants to prepare competitive landscape and market positioning analysis for the overall market as well as for various market segments.

SPARK Matrix: Strategic Performance Assessment and Ranking

Quadrant Knowledge Solutions' SPARK Matrix provides a snapshot of the market positioning of the key market participants. SPARK Matrix representation provides a visual representation of market participants and provides strategic insights on how each supplier ranks in comparison to their competitors, concerning various performance parameters based on the category of technology excellence and customer impact.

Final Report Preparation

After finalization of market analysis, our analyst prepares necessary graphs, charts, and table to get further insights and preparation of the final research report. Our final research report includes information including competitive analysis; major market & technology trends; market drivers; vendor profiles, and such others.

Client Support

For information on hard-copy or electronic reprints, please contact Client Support at

ajinkya@quadrant-solutions.com | www.quadrant-solutions.com