KNOWLEDGE BRIEF

Gurucul Receives 2017 Product Performance Leadership Recognition in UEBA Market by Quadrant Knowledge Solutions

KNOWLEDGE BRIEF

BY

Quadrant
Knowledge Solutions

Gurucul Receives 2017 Product Performance Leadership Recognition in UEBA Market by Quadrant Knowledge Solutions

User and Entity Behavior Analytics (UEBA) solutions monitor user and entity behavior in corporate networks detecting anomalies indicating potential threats from behavior profiles and patterns by applying algorithms, statistical analysis, and machine learning techniques. UEBA technologies use a variety of data sources, such as access logs, endpoint security, threat intelligence, identity & access management (IAM), security information & event management (SIEM), and other security technologies, and correlates information about user access and activities to provide a unified and granular view of user risk scored anomalies across corporate networks, devices, and cloud applications. UEBA technologies help organizations in monitoring privileged user (super user) accounts, IP protection, information security, cyber fraud prevention, compliance to security policies, and such others.

Quadrant Knowledge Solutions' recent study of the "***User and Entity Behavior Analytics (UEBA) Global Market Outlook***" analyzes market dynamics, opportunities and the vendor ecosystem of the market. This study provides strategic analysis of the global UEBA market in terms of short-term and long-term growth opportunities. The study also provides detailed market forecast analysis of the global UEBA market in various geographical regions, industry segments, revenue type, and customer segments. The UEBA market outlook research helps companies formulate growth strategies by identifying growth prospects, market trends, market drivers, and challenges in the global market.

The research also provides detailed competitive positioning and supplier landscape analysis of major UEBA vendors, including Allure Security, Bay Dynamics, E8 Security, Exabeam, Gurucul, Niara, Securonix, Sqrrl Data, Veriato, and such others.

Gurucul Receives 2017 Product Performance Leadership Recognition in the Global UEBA Market

As part of the research on "User and Entity Behavior Analytics Global Market Outlook," Quadrant's competitive landscape analysis of the UEBA market compares the vendors' technological capabilities in providing different applications. Quadrant research analyzed vendors in terms of sophistication of technology, product capabilities, customer impact, ease of use, visionary innovation, and future roadmap.

According to research findings, Quadrant Knowledge Solutions recognizes Gurucul's product performance leadership position in the global UEBA market. Gurucul's leadership

recognition is driven by superior technology platform, comprehensive UEBA solution portfolio, high customer impact, and powerful algorithm based on machine learning, peer group modeling, and predictive analytics.

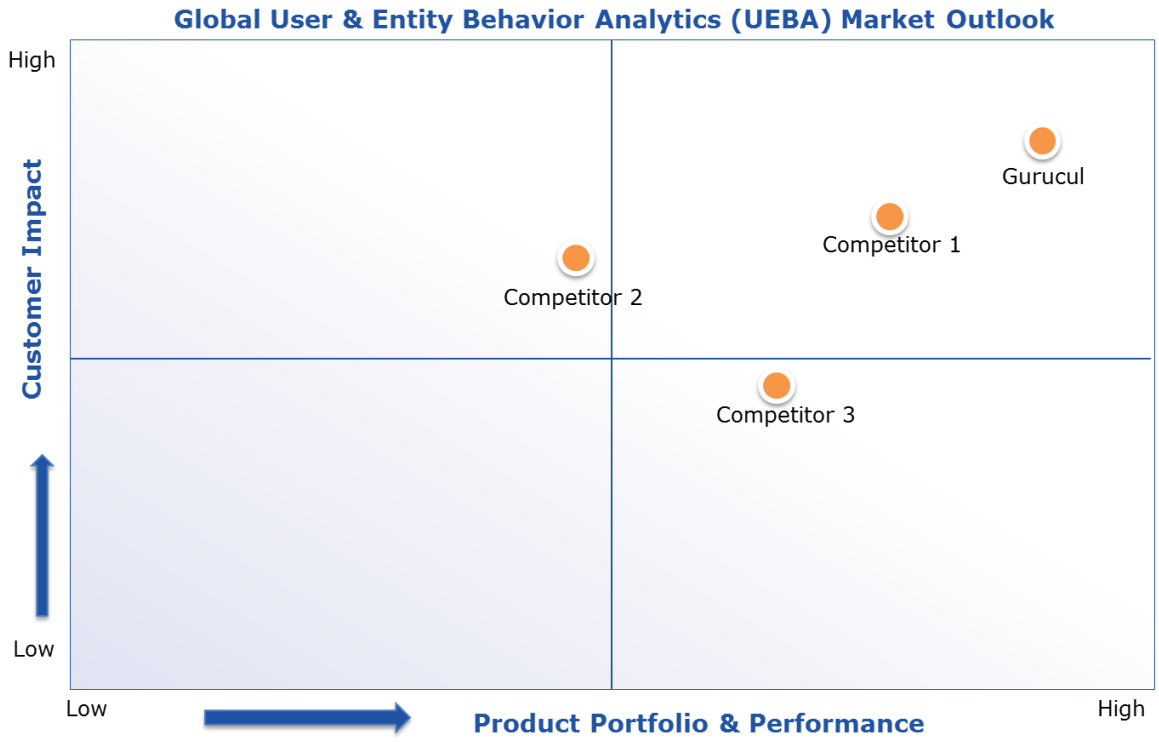
While organizations have invested in building robust security infrastructure for security against external threats, dealing with insidious threats are far more challenging. In addition, the insidious threats are on the rise and becoming more frequent. The employees with access to sensitive and valuable data can cause significant damage to the organization and disrupt the business as usual. According to Piyush Dewangan, Research Manager, Quadrant Knowledge Solutions "providing access with authentication and authorization is no longer effective especially in dealing with preventing misuse by high privileged user (or super user) accounts, reducing excess access, and detecting orphan and dormant accounts."

Founded in 2009, and headquartered in Los Angeles, USA, Gurucul provides advanced UEBA technology to detect anomalous behavior across users, accounts, applications, and device by using predictive security analytics, machine learning, and peer group modeling. Gurucul uses Predictive Identity Based Behavior Anomaly Engine™ (PIBAE™) architecture that combines user behavior intelligence, big data analytics, and leverages identity as an access risk and threat surface to provide actionable risk intelligence. PIBAE enables building a behavior baseline for a user or entity based on multiple attributes and compares it with peer groups to detect anomalous behavior. These patterns can be evaluated using risk-modeling algorithms to generate a user or entity's risk score. This approach to security intelligence helps organization to detect and respond to cyber-criminal activities and protect against insider threats, prevent data exfiltration, and privilege access misuse.

Gurucul's UEBA platform uses identity as an access risk and threat plane to determine the risk of a user's identity. Gurucul collects relevant datasets from a variety of internal and external sources including identity management system, privileged account management systems, directories, log sources, and defense in depth systems including DLP, anti-malware, IDS, IPS, firewalls, SIEM, and such others. It also takes information from external sources that track broad scope of threat patterns. Gurucul's behavioral machine learning algorithms analyzes up to 254 different attributes to create a user or entity identity profile, behavior base lines and within peer group analysis.

Gurucul's UEBA solution methodology for insider threat detection and prevention includes three key components: a) identity analytics (IdA) to risk-rank access risks and to reduce excess access and outliers b) user and entity behavior analytics (UEBA) based on dynamic peer groups and machine learning algorithms to reduce false positives and c) bringing users

into a collaborative relationship with IT security to protect their identities via self-audits to review risk-ranked anomalous behavior and access analytics.



Gurucul's Capability in Global UEBA Market

Gurucul's product portfolio includes Gurucul Risk Analytics (GRA), Access Analytics Platform (AAP), Cloud Analytics Platform (CAP), and Threat Analytics Platform (TAP). These products are built on PIBAE architecture that identifies anomalous behavior across users, accounts, applications, and devices by leveraging behavior analytics, machine learning and peer group modeling with context from an open choice of big data. Gurucul provides Hybrid Behavior Analytics (HBA) architecture for on-premise and cloud applications in one platform.

- **Gurucul Risk Analytics (GRA)**: Gurucul Risk Analytics incorporates "identity as a threat vector" into organization's cyber-defense system and by applying advanced predictive security analytics to predict and detect unknown threats and reduce access risk. GRA uses machine learning models with context from big data for on-premises, cloud and hybrid environments. Gurucul STUDIO enables custom machine learning models in a step-by-step process with no coding and a minimal knowledge of data science. GRA includes a Self-Audit feature leveraging user context to detect and verify anomalies beyond the knowledge and awareness of SOC analysts.
- **Access Analytics Platform (AAP):** Access Analytics Platform enables organizations to predict and prevent access risks by providing a near real-time contextual view of

identities, their access and activities across enterprise applications, systems, and resources. AAP provides identity analytics for an effective risk-based compliance and provisioning for identity and access management to reduce excess access, access outliers, plus orphan and dormant accounts. Risk-based certifications, requests and approvals increase revocations to reduce access risk, remove rubber-stamping and access cloning, while intelligent roles replace legacy rules and roles.

- **Cloud Analytics Platform (CAP):** Gurucul's CAP is an API-based CASB (Cloud Access Security Broker) to predict and detect unknown threats and access risks within cloud applications (SaaS), infrastructure (IaaS/PaaS) and access (IDaaS) providing risk-scored contextual views of an identity, its access, and activities. CAP helps companies track behavioral anomalies and identify insider threats, compromised accounts, compliance violations, data leakage and assist in investigation forensics. CAP provides both identity analytics and user and entity behavior analytics to reduce the attack surface for cloud-based accounts, unnecessary access rights, and privileges, and identify, predict and prevent breaches.
- **Threat Analytics Platform (TAP):** Gurucul's Threat Analytics Platform helps organizations predict, detect, and deter insider threats, compromised accounts, data exfiltration and cyber-fraud. TAP helps in protecting an organization's intellectual property, sensitive information, and preventing IP theft leveraging bi-directional API integrations with security solutions for automated risk response. Examples include step-up authentication based on risk score, closed-loop DLP risk scored alerting, access privilege removal and self-audits.

Last Word

According to industry estimates, over 90% of the breaches involved compromised accounts and over 80% of all data loss were due to compromised credentials. This can significantly damage organization in terms of money and brand image. As insider threats are becoming more frequent, internal users are considered more risky than external malware or hackers. Driven by growing frequency of security breaches including several high-profile incidents, information security professionals are looking for next generation of security analytics and intelligence tools to predict, identify, and prevent the most sophisticated threats beyond rules, patterns and signatures. Gurucul, with its comprehensive UEBA product portfolio and superior technology platform, is well positioned to help organizations in early detection of potential access risks and threats, plus protect against insider threats, advanced threats, and cyber fraud. With strong overall performance and solution scale, Quadrant Knowledge Solutions recognize Gurucul's Product Performance Leadership position in the global UEBA market.