KNOWLEDGE BRIEF

Securonix is Recognized as 2018 Technology Leader in the UEBA Market

KNOWLEDGE BRIEF

BY

Securonix is Recognized as 2018 Technology Leader in the UEBA Market

UEBA solution monitors users and entity behavior in the corporate network and detects anomalies indicating potential threats from behavior pattern by applying algorithms, statistical analysis, and machine learning techniques. The solutions enrich security events with user and entity context with feeds from HR systems, Active Directory, CMDB database, IAM solutions and others. UEBA technologies use a variety of data sources for security events, such as access logs, endpoint security, threat intelligence, SIEM, and other security technologies, and correlates information about user activities to provide a unified and granular view of user activities across the corporate network, devices, and cloud applications. UEBA solution help organizations in providing information security, IP protection, cloud security, fraud prevention, compliance to security policies, and such others.

Quadrant Knowledge Solutions' recent study "**Market Outlook: User and Entity Behavior Analytics (UEBA), 2018-2023, Worldwide**" analyses market dynamics, growth opportunities, emerging technology trends, and the vendor ecosystem of the global market. This research provides strategic information for technology vendors to better understand the market supporting their growth strategies and for users to evaluate different vendor capability, competitive differentiation, and its market position. According to the research findings, the UEBA market is expected to grow significantly in the next five to six years from the market size of $294.9 million in 2018 to over $2.33 billion by 2023. The market, which has grown by 60.5% in 2018 compared to 2017, is expected to grow at a compound annual growth rate (CAGR) of 51.3% from 2018-2023. UEBA market growth is primarily driven by increasing risk from insider threats, compromised accounts, growing complexities of regulatory compliance, increasing concern for data breaches and access management in cloud, intellectual property protection, scarcity of security professionals, and growing requirement for robust security intelligence by large enterprises.

Market Dynamics and Trends

A growing frequency of high-profile security and data breaches are driving significant investments in deploying various network and cyber security technologies. Though organizations have made appropriate investments in building robust security infrastructure for security against known external threats, dealing with unknown and insidious threats is 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.

Traditional security solutions are no longer effective in detecting advanced unknown and insider threats. Hence users are increasingly adopting advanced UEBA solution to detect advanced and unknown threats and enable protection against malicious insider, compromised accounts, cyber threats, frauds, and compliance to security policies.

The research includes detailed competitive analysis of the primary UEBA vendors, including Bay Dynamics, E8 Security (VMWare), Exabeam, Fortscale RSA, Gurucul, Haystex Technology, HPE Niara, LogRhythm, Palo Alto Networks, Securonix, Splunk, Zonefox, and others. Each of these vendors has comprehensive product offerings, strong value propositions to support diverse range of UEBA use cases, and market & technology strategies to support future market needs.

Majority of the UEBA vendors provide core functionalities and advanced analytics to detect advanced and insider threats. However, technology capabilities differ between different vendors offerings in terms of sophistication of analytics with data science-based machine learning capabilities, customization, robust integration, ease of deployment and use, time to value, and advanced threat detection and investigation capabilities.

According to the research findings, leading UEBA vendors such as Securonix and others are expanding their capabilities to offer next-generation SIEM solution. Driven by complexities of hybrid IT infrastructure and growing data volumes, the number of security alerts have grown significantly. The traditional SIEM solutions are not capable enough of detecting and responding to modern complex threats and preventing advanced insider attacks. Vendors are increasingly integrating their UEBA capabilities with big data, advanced analytics, enterprise log management, threat hunting, and security automation & orchestration capabilities to offer next-generation SIEM solution. Next-Gen SIEM solution enables end to end security monitoring to predict, detect, investigate, and respond to advanced and unknown threats.

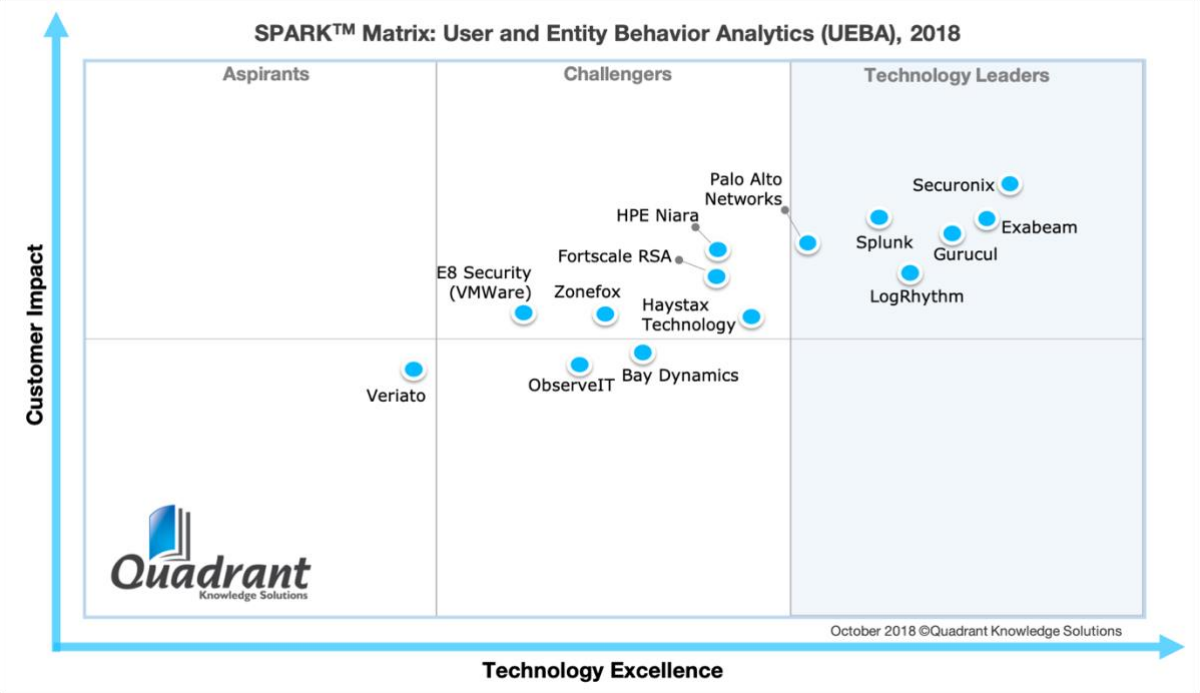
Competition Landscape & Analysis of the Global UEBA Market

Securonix is Recognized as 2018 Technology Leader

Quadrant Knowledge Solutions conducted an in-depth analysis of major User & Entity Behavior Analytics vendors by evaluating their product portfolio, market presence, and value proposition. The evaluation is based on the primary research with expert interviews, analysis of use cases, and Quadrant's internal analysis of the overall UEBA market. Quadrant's competitive landscape analysis compares vendors' technological capabilities in providing UEBA in terms of technology excellence performance and customer impact. Performance in technology excellence is measured by parameters, including sophistication of technology, technology application diversity, scalability,

competitive differentiation, and industry impact. Customer impact includes parameters, such as addressing unmet needs, product performance, proven records, ease of deployment, and customer service excellence. According to research findings, Securonix, with the comprehensive UEBA solution, has received the highest overall ratings and is positioned as the 2018 technology leader in the global UEBA market.

Founded in 2008, Securonix is amongst the most innovative provider of UEBA solution and next-generation security analytics platform. Given it's built on an open big data platform, Securonix platform combines patented machine learning, behavior analytics, log management, advanced threat detection, and intelligent incident response on a single platform to predict, detect, investigate, and respond to the most advanced,



insider, and unknown threats. Securonix also provides investigation workbench to perform visual link analysis and help SOC analyst to explore data relationship with complete contexts of identity, activity, access, and the DLP violations.

Securonix Capabilities in the Global UEBA Market

Securonix provides comprehensive UEBA solution with its big data platform, identity enrichment, behavior analytics capabilities, packaged security application content, and incident response automation. Securonix supports deployments via software licensing, appliance, virtual appliance, and SaaS. The company offers flexible and predictable pricing based on the number of identities in the customer organizations.

- **Securonix Security Analytics Platform**: Securonix security analytics platform is built on Hadoop and combines log management, SIEM, advanced analytics, UEBA, and security automation & orchestration capabilities to offer an end-to-end solution with next-generation SIEM capabilities. Securonix unified platform uses non-proprietary data stores and provides enterprise-class scalability for security monitoring and response. Securonix provides over 1000 out of the box use cases with threat models for multiple industry-specific and business use cases. The content is automatically delivered to the customers with Securonix Threat Library and Threat Exchange. The platform uses patented machine learning and statistical analytics model to detect advanced and insider threats. The threat model capability integrates a series of events using threat chains to prioritize risks and support SOC analysts in effectively responding to threats based on their risk scores. The platform enables faster threat hunting using natural language search to facilitate investigation, visualization, and reporting on threats. The platform provides comprehensive incident management, workflow, and case management capabilities to facilitate collaboration among multiple teams for threat investigation. Securonix platform is integrated with a third-party solution to enable automatic threat response to mitigate and neutralize threats.

- **Securonix User and Entity Behavior Analytics**: Securonix UEBA solution uses entity enrichment, patented machine learning and behavior analytics to build a comprehensive risk profile of users based on the correlation between user identity and interaction with systems, applications, and access to corporate resources. The solution compares user activities to their individual baseline, peer group baseline, and various known threat indicators to provide a unified view of user risk scorecard and identify risk across corporate networks, devices, and cloud applications. Securonix UEBA is a proven solution to detect advanced insider threats, cyber threats, fraud, cloud data compromise, and non-compliance. Security analyst can use built-in automated incident response capability to respond to threats quickly and efficiently.

- **Securonix Security Data Lake**: Built on Hadoop, a fault-tolerant and open data platform, Securonix Security Data Lake collects significant amounts of data and supports long-term data retention. The data is enriched with contextual information about a user, asset, IP address, geo-location, and network intelligence. Securonix Spotter capability offers faster threat hunting with natural language search and visualization to transform raw log data into meaningful security insights. With open data format, it enables users to maintain a single source of log data and the same is available to other applications. It also provides built-in dashboard and reporting packages for

major security mandates, including PCI DSS, SOX, HIPPA, FISMA, and ISO 27001, to manage regulation and demonstrate compliance.

- **Securonix Security Applications**: Securonix provides packaged out-of-the-box applications for identity analytics, insider threat, cyber threat, fraud, and cloud security use cases. These applications are delivered as a threat model and built-in connectors for rapid deployment and time to value. The threat models can rapidly scan real-time or historical data to predict and detect advanced threats. The Securonix Threat Model Exchange, a library of threat models, facilitate collaboration with customers, partners, and security leaders. Users can access the library, download, and deploy the latest threat model with a single click. These threat models can be customized to suit users-specific unique needs. Users can also use their in-house or third-party security analytics applications and plug them into the Securonix Security Analytics platform. Securonix offers insider threat application bundle including data security analytics application and privileged account analytics application. In addition, Securonix also offers identity and access analytics, cyber threat analytics application, cloud security analytics application, patient data analytics application, and fraud analytics application.

The Last Word

Organizations are increasingly facing challenges due to growing complexity and frequency of security breaches leveraging compromised accounts and credentials. Information security professionals are looking at next generation of security intelligence and analytics tools to predict, identify, and prevent the advanced and unknown threats. Traditional rules and signature-based platforms are not effective in handling these modern threat vectors. The insider threats are considered far more risky than external malware threats. This can significantly damage an organization in terms of money and brand image. Securonix is well recognized for delivering a comprehensive UEBA and next-generation SIEM solution to predict, detect, and respond to advanced insider and unknown threats. Driven by its sophisticated technology capabilities and strong customer value proposition, Securonix has received the highest overall ratings and is recognized as the technology leader in the global UEBA market.