cloudera

SOLUTION BRIEF

SECURONIX

Securonix

Industry

Software

Website

www.securonix.com

Platform Overview

The Securonix Platform is a purpose-built advanced security analytics technology that mines, enriches, analyzes, scores and visualizes security data into actionable intelligence on the highest risk threats from within and outside an enterprise. Using signature-less anomaly detection techniques that track users, account, and system behavior, Securonix is able to automatically and accurately detect the most advanced data breach attempts.

Securonix + Cloudera Solution Highlights

- Over 90 percent reduction in security events warranting investigations
- Signature-less, behavior based and peer based analytics for detecting insider and targeted cyber attacks
- User and entity centric monitoring across hosts, network and applications
- Privileged account monitoring and misuse detection
- Leverage the full power of your data to achieve pervasive analytics, increase business visibility and reduce costs
- Bring diverse users and application workloads to a single, unified pool of data on common infrastructure; no data movement required
- Best-in-class holistic interface that provides end-to-end system management
- Zero-downtime rolling upgrades
- Easy integration with existing systems
- Open source to achieve stability, continuous innovation, and portability

Securonix + Cloudera = Security Intelligence. Redefined.

Security event monitoring products were built for data collection, retention and compliance reporting, with limited threat detection capabilities. These tools tend to overwhelm security teams with alerts and do a poor job of detecting real threats. The volume of security alerts they generate is unmanageable and ineffective. Enterprises need real-time analytics that mine large volumes of data to automatically identify threats and provide context-rich visibility into the data. Organizations are realizing that the value of Big Data for security is not just in the collection of data, but the parallel analytics that can be run on this data to identify real threats without hiring an army of data scientists with a flair for predicting the future.

Securonix is the industry's top security analytics platform that packages sophisticated data science, behavior based anomaly detection, peer analysis and other machine learning techniques into out-of-the-box threat models that detect both known and unknown threats. Securonix is used by the largest organizations to detect insider threats, privilege abuse, data exfiltration, advanced persistent threats, and "hard-to-see" breaches involving sophisticated malware. Securonix and Cloudera partnered to harness the power of big data and put actionable intelligence into the hands of security leaders, enabling them to combat cyber threats and reduce risk to their organization with fewer resources and lower costs.

Big Data Intelligence. Delivered.

The Securonix-Cloudera joint solution delivers on the promise of Big Data for security by detecting the most complex, unknown, and impactful internal and external threats with a data-driven approach that is purpose built for security analytics. It delivers the full-context security monitoring and automated signature-less threat detection Securonix is known for, plus the enterprise data management, visibility and storage of Cloudera's Enterprise Data Hub. The result is a groundbreaking new threat detection capability that harnesses the power of Big Data environments. Use the Securonix-Cloudera solution for:

- User Behavior Analytics
- Network Flow Analytics
- Endpoint Analytics
- Data Exfiltration Analytics
- Cloud Security Analytics
- Application Analytics
- Fraud Analytics

360 Degree Visibility

With a powerful, context-enriched anomaly detection and visualization engine, Securonix analyzes events, identity, access, and transaction data to detect advanced threats and risk-ranks events for proactive security management. The Securonix high-risk dashboard provides one place to store, analyze and derive new value from enterprise data that delivers real-time visibility of the highest risks to an organization.

Advanced Security Analytics

Securonix integrates directly with sources of event information the enterprise already has in place. In addition to leveraging existing event data, it provides aggregation and enrichment with other relevant sources of information including identity, access, third party intelligence and geolocation information.

Cloudera Benefits

Stores and Analyzes Any Type of Data

- Leverage the full power of your data to achieve pervasive analytics, increase business visibility, and reduce costs
- Bring diverse users and application workloads to a single, unified pool of data on common infrastructure; no data movement required

Enterprise Approach

- Compliance-ready perimeter security, authentication, granular authorization, and data protection through encryption and key management
- Enterprise-grade data auditing, data lineage, and data discovery

Industry-Leading Management and Support

- Best-in-class holistic interface that provides end-to-end system management and zero-downtime rolling upgrades
- Open platform ensures easy integration with existing systems
- Open source to achieve stability, continuous innovation, and portability

Access to historical data from high volume data feeds is essential to providing advanced security analytics capabilities. The Securonix integration with Cloudera Enterprise (Impala, Solr, Spark, Kafka) is designed to target emerging or suspected security threats by:

- Going beyond two-tier analytics to provide n-tier and on-demand analytics that span the enterprise
- Leveraging time boxed analytics and dynamic user behavior analytics to identify threats
- Virtualizing and analyzing massive quantities of event data by leveraging event streams

Forensic Security Event Enrichment and Analysis

Correlation of event feeds is critical for security analytics. Securonix paired with Cloudera enables historical analytics as well as advanced storage of all relevant information associated with security event data. Securonix takes this process of event enrichment to the next level by providing forensic security enrichment of events with point-in-time non-repudiation of the complete enriched event. This enables:

- Analytics based on point-in-time snapshots of the event and related details (user, access, devices, versions, patch levels, threat indicators, etc.) that were present at that time the event happened
- Analytics based on the volatility of enriched information associated with each event

Enterprise Security

Securonix provides advanced security features for encryption and masking of relevant information. The integrated solution with Cloudera also enables advanced protection of the entire solution in an enterprise environment by providing:

- Strong Authentication and authorization with Kerberos and Cloudera Sentry
- Encryption of sensitive data when storing in a shared environment

Use Case Examples

- Privileged Account Misuse - Analyze every activity performed using privileged accounts for misuse including creation of shadow accounts, initiation of suspicious services, suspicious connections to external IP addresses, changes to critical system files and even critical customer data access.
- Endpoint Protection - Analyze all endpoint generated data to detect suspicious process execution, abnormal network flows, rare file Md5 hashes detected, and suspicious lateral movements
- Insider Threat Protection - Correlate all events to a user identity and analyze all user generated events to detect misuse of data access privileges and data exfiltration attempts
- Patient Record Protection - Automated correlation of all PHR access attempts to appropriate staff members and analyses of all PHR data access attempts to detect unauthorized PHR access, VIP snooping, neighbor snooping and family snooping

About Securonix

Securonix radically transforms data security with actionable intelligence. Our purpose-built security analytics technology mines, enriches, analyzes, scores and visualizes data into actionable intelligence on the highest risk threats to organizations. Using signature-less anomaly detection techniques, Securonix detects the most advanced data security, insider threat and fraud attacks automatically and accurately. www.securonix.com

About Cloudera

Cloudera delivers the modern platform for data management and analytics. The world's leading organizations trust Cloudera to help solve their most challenging business problems with Cloudera Enterprise, the fastest, easiest, and most secure data platform built on Apache Hadoop. Our customers can efficiently capture, store, process, and analyze vast amounts of data, empowering them to use advanced analytics to drive business decisions quickly, flexibly, and at lower cost than has been possible before. To ensure our customers are successful, we offer comprehensive support, training, and professional services.
Learn more at cloudera.com.

cloudera.com

1-888-789-1488 or 1-650-362-0488
Cloudera, Inc. 1001 Page Mill Road, Palo Alto, CA 94304, USA

© 2015 Cloudera, Inc. All rights reserved. Cloudera and the Cloudera logo are trademarks or registered trademarks of Cloudera Inc. in the USA and other countries. All other trademarks are the property of their respective companies. Information is subject to change without notice.

cloudera-solutionbrief-securonix-101_A4