SECURONIX

Security Intelligence Platform

Product Brief

Security Intelligence. **Delivered.**

Securonix Security Intelligence Platform

From Data to Actionable Security Intelligence

Highlights

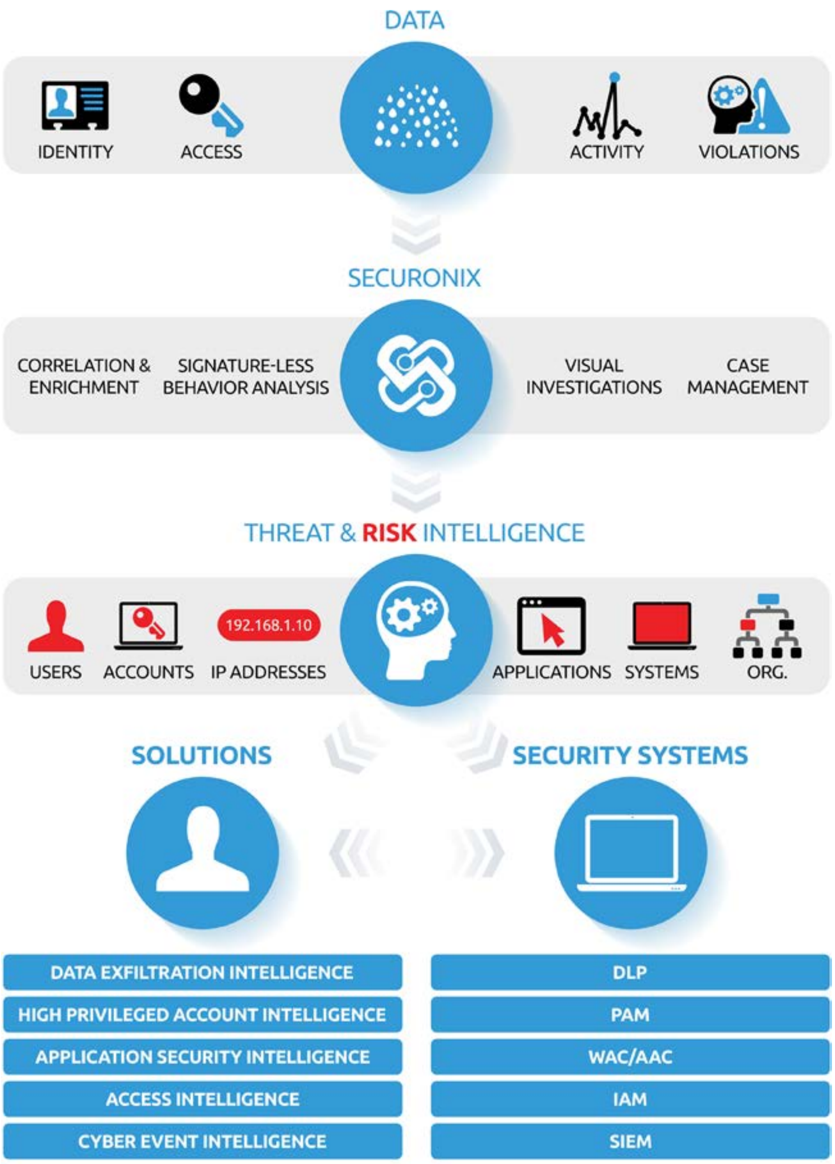
- **Delivers real-time security intelligence to security, IT, business and key security systems**
- **Detects insider threats and APTs through signature-less behavior and outlier analysis**
- **Immediate ROI in risk and cost reduction for security programs across DLP, SIEM, IAM, PAM, DAM, and Enterprise or Cloud Application Security Management**

Product Overview

Securonix is the industry-leading platform for security analytics and intelligence. Security analytics is one of the fastest growing, and most important areas of information security today and is a must have in the fight against insider and external cyber security threats.

Where current event monitoring technologies are focused on data collection, retention and compliance reporting at the perimeter, Securonix focuses on detecting advanced threat patterns and even insider threats. Securonix continuously analyzes the billions of events generated on your network, systems and applications and pin points the suspicious events that require further investigation. The Securonix risk engine automatically risk ranks threats and actors enabling organizations to prioritize their investigations. Securonix provides a versatile investigation workbench and integrated incident response system that provides security analysts the ability to perform visual link analysis of events, accounts, users, access, activities, systems and even network addresses.

Securonix Security Intelligence Platform



DATA

IDENTITY · ACCESS · ACTIVITY · VIOLATIONS

SECURONIX

CORRELATION & ENRICHMENT · SIGNATURE-LESS BEHAVIOR ANALYSIS · VISUAL INVESTIGATIONS · CASE MANAGEMENT

THREAT & **RISK** INTELLIGENCE

USERS · ACCOUNTS · IP ADDRESSES · APPLICATIONS · SYSTEMS · ORG.

SOLUTIONS

- DATA EXFILTRATION INTELLIGENCE
- HIGH PRIVILEGED ACCOUNT INTELLIGENCE
- APPLICATION SECURITY INTELLIGENCE
- ACCESS INTELLIGENCE
- CYBER EVENT INTELLIGENCE

SECURITY SYSTEMS

- DLP
- PAM
- WAC/AAC
- IAM
- SIEM

Delivering Plug 'n Play Security Analytics Across the Enterprise

Source Specific Security Analytics

Perform purpose build security analytics on virtually any data source, system, application, and device in real time. Securonix knows what behavioral models and analytics must be applied to each source to detect the threats. In addition, you can even build your own analytical models and save it for the source type.

Full-Context Monitoring with Real-time Entity Correlation As identity, account, activity and security event information flows into Securonix it continuously is correlated back to an "entity" (i.e. a user, account, system, device, or an organizational unit). This provides a single console view and the full context on any security event, user, account, or systems for better detection and faster response.

Real Time Event Enrichment

As the events flow into Securonix, you can perform operations to embed intelligence in each event. With over 40 operations to choose from and a custom computation engine, you can now perform operations on the event attributes prior to the analytics.

Behavior-based Anomaly Detection

What sets the Securonix Security Intelligence Platform apart from other solutions is the use of our proprietary signature-less threat detection algorithms that continuously scan your data to pinpoint rogue activities, abnormal security events, and access privileges. The Securonix technology utilizes intelligent behavior-based analytics and peer group analysis techniques to detect unseen attacks launched from within or outside the perimeter of your organization.

Personalized and Prioritized Threat and Risk Dashboards

Organizations face different types of threats and have dedicated teams to investigate and manage each threat category. Securonix provides the capability to set up different threat categories and associate threat indicators with each threat category. More importantly, Securonix risk ranks users, systems and applications based on the different threat categories. Security professionals can now easily see the top users in their threat category and investigate them.

Data Driven Link Analysis & Investigation

Investigate any identified threat, security event, user, account, or system using Securonix's Investigation Workbench that provides data-driven link analysis and visualization allowing a user to link users, accounts, systems, activity, and violations together for rapid "single pane" investigations.

Data Level Security and Privacy Controls

Built to gather and generate sensitive information on users and other sources, Securonix provides the complete capability to secure, mask, encrypt and enable the controlled authorized access to this information that is inline with the most stringent data security and privacy requirements in the industry.

Out-of-the-Box Security Intelligence Solutions

Data Exfiltration Intelligence

Using purpose built data parsers and standard APIs, the Data Exfiltration Intelligence application mines DLP events and/or raw monitoring activities from major DLP products such as Symantec DLP, McAfee DLP, and Verdasys Digital Guardian. The application performs automated analytics on events such as identity correlation, recipient analysis, sentiment analysis, behavior analysis, peer group analysis and additional techniques aimed at identifying data exfiltration threats tied to specific or multiple events.

High Privileged Account Intelligence

HPAs are a primary source of insider misuse and a platform for cyber attacks. Securonix automatically identifies HPAs such as administrator, service, and shared accounts, then monitors them for abnormal behavior associated with an attack. High-risk behavior is linked back to a real user and their risk profile to give the potential threat full context.

Application Security Intelligence

The application Security Intelligence application monitors enterprise and cloud-based applications such as SAP, EPIC, SharePoint, Office 365, Box, and custom applications for anomalous behavior and known threats associated with data theft, fraud, and data snooping.

Access Intelligence

The Access Intelligence application is purpose built to automatically detect all types of high risk access from privileged service and shared accounts, to orphaned accounts, and rogue access. This means you do not need to know anything about account types, access entitlements, user identities, orphaned accounts or business rules in order to generate a prioritized list of high risk access for cleanup or review by the business.

Cyber Event Intelligence

The Cyber Event Intelligence application performs real-time analytics on events from such security products as HP ArcSight, Splunk, McAfee ESM, IBM QRadar, FireEye, and others automatically identifying undetected threats while providing full context monitoring, risk ranking, and link analysis investigations.

Security Intelligence. Delivered.