SECURONIX
Security Analytics. Delivered.

DATASHEET

Securonix Security Apps

Extended Use Cases. Delivered.

Securonix is revolutionizing security with an advanced analytic platform that leverages machine learning and behavior analysis to rapidly detect any threat, anywhere. Securonix platform comes packaged with out-of-the-box applications specifically designed for insider threat, cyber threat, fraud, cloud security and compliance, delivered in the form of threat models and built-in connectors that enable rapid deployment and quick time-to-value. Threat models are fully customizable from the user interface, providing flexible tuning to fit unique needs. Some of the key packaged applications are:

Data Security Analytics

Ingests data from sources such as email, DLP, proxy, cloud applications and printers to baseline normal behavior patterns and detect sudden spikes in data egress attempts coming from inside or outside the organization and potential compromises to critical data. The application also applies predictive behavior analytics that identify, profile and monitor users whose behaviors indicate an elevated risk for data theft; for example, a flight-risk employee with plans to leave the company.

Privileged Account Analytics

Identifies and monitors privileged user and service accounts and detects misuse of credentials, account compromise and credential sharing. Securonix ingests data from sources such as Active Directory, UNIX, databases, and PIM/PAM solutions to baseline privileged account behavior and look for anomalous events such as rare suspicious transactions, login anomalies and more.

Cyber Threat Analytics

Monitors security logs and network flows to detect malware infections (e.g. zero day attacks and ransomware,) system compromise, lateral movement, pass-the-hash, pass-the-ticket and other advanced threats. Securonix ingests data from sources such as firewalls, proxy, VPN, IDS, DNS, endpoints and Netflow devices to baseline normal behavior and detect malicious patterns such as beaconing, connections to digitally-generated domains, robotic behavior, rare executables and programs, lateral connections and unusual web activity.

Identity and Access Analytics

Analyzes access privileges of users to identify rogue access and support risk-based access management and review. Securonix ingests entitlement data from authentication sources such as Active Directory, enterprise applications (e.g. SAP) and IAM solutions and analyzes it using peer comparisons, fuzzy logic and SOD libraries to detect high-risk outlier access. The solution also integrates with authentication systems (e.g. IAM devices) to decommission or block access, or step up authentication for high risk users.

Application Security Analytics

Monitors transaction and security logs from enterprise applications to detect and prevent data snooping, data exfiltration, privilege misuse, login anomalies and sabotage. Securonix ingests transaction logs, security logs and entitlements from enterprise applications (e.g. SAP, EPIC and custom apps) to baseline normal activity patterns and identify anomalous behavior.

Cloud Security Analytics

Monitors cloud infrastructure platforms and applications for data exfiltration attempts, privilege misuse, advanced external attacks and access anomalies. Securonix also has the ability to perform data discovery and classification in cloud applications and manage dynamic permissions to critical infrastructure. Securonix supports integration with several cloud services including O365, Google Apps, Box, Salesforce, Workday, Hightail, Netskope, Okta, Ping, AWS, Azure and many more.

Fraud Analytics

Monitors transaction data over a period of time, profiling normal entity-data-time relationships to detect fraudulent behavior patterns. Baselines of normal transaction behavior are based on actor, target, location, time, frequency and sequence to detect rogue events such as spikes in transactions, misuse of discount or promotional codes, suspicious refunds, fraudulent prescriptions, rogue orders, suspicious shipping request. The application provides packaged use cases for many types of fraud including healthcare, ATM, online banking, retail, customer and customer service reps, among others.

Patient Data Analytics

Monitors the activity of users accessing electronic medical records in clinical applications and detects attempts at data snooping and data exfiltration. Securonix has specific algorithms to detect different types of snooping events including family snooping, co-worker snooping, VIP snooping, self-examination, age-based anomalies and location-based anomalies. Securonix has out-of-the-box integration with several Clinical applications including EPIC, Cerner, Medicity Allscripts and many others. Securonix provides use cases, built-in reports and dash-boarding capabilities for compliance requirements such as HIPAA and HITECH.

EXCLUSIVE FEATURES

Threat Models

Behavior anomalies, when looked at in isolation, may seem innocuous. However, a combination of these anomalies over a period of time or in a particular sequence could be an indicator of a sophisticated cyberattack. Securonix threat models are built to predict and detect the kill-chains of events that could be part of an advanced attack. For each of the analytic applications, Securonix provides out-of-the-box threat models that can rapidly scan through historical or real-time data to predict and detect advanced threats. Customers can view and edit the logic built into threat models or change the risk scoring multipliers to suit their unique business needs.

Cloud-Based Threat Model Exchange

The Securonix Threat Model Exchange is an online library where customers access and share the latest threat models. The cyber security experts and data scientists who make up The Securonix Cyber Research Team continuously update and vet the threat models against the latest cyberattacks. The Securonix Threat Model Exchange is available exclusively to Securonix customers and is fully integrated into the Securonix security platforms. Customers access the online library from their Securonix application interface. The latest threat models can be downloaded and deployed with a few clicks.

Build Your Own App

The Securonix SNYPR solutions provide an open-data model enabling customers to use raw or enriched data for analytics on their own analytics applications. You can also add your own custom analytics apps that you build, or from third parties that can be easily plugged into the SNYPR open data platform.