SECURONIX
Security Analytics. Delivered.

DATASHEET

Security Data Lake

Infinite Scalability At A Fraction Of The Cost.

Organizations collect and store massive volumes of data; the challenge is deriving meaningful value from it. Securonix Security Data Lake® is able to process and store petabytes of data in an open data format, and make it available for visualization, analysis, and reporting by any application. The data is super enriched with contextual user, asset, IP address, geo-location and network intelligence that transforms raw big data into meaningful security insights with blazing-fast search and elegant visualization.

Securonix Security Data Lake is powered by Hadoop, a massively scalable, fault tolerant, open-data platform that ingests hundreds of terabytes per day and supports reliable, economical, long-term data retention. The open data model is key. It provides a single source of data that extends to SNYPR's packaged use cases: insider threat, cyber threat, fraud and compliance, as well as any other custom use cases or applications the enterprise needs. The possibilities are endless.

Uncover actionable intelligence through super enrichment, search and visualization. The SNYPR Security Data Lake delivers a **SMARTER, FASTER** and **MORE ECONOMICAL** way to reveal comprehensive, actionable insights into an organization's security posture.

SMARTER

- Super enrichment adds identity, asset and geo-location context plus threat intelligence correlation, transforming raw events into meaningful insights that are easy to understand, search and investigate. Data is indexed to provide search and visualization capabilities enabling investigators to tie dynamic context to data, understand the context of an anomalous event, and take corrective action without time consuming manual work.
- Delivered with a library of out-of-the-box connectors that integrate with structured and unstructured data sources including traditional network and server log sources, plus a wide selection of additional connectors for enterprise applications, cloud services, identity stores, IAM systems, and non-technical feeds such as badge readers, social media events, travel logs and background checks. More data means more accurate profiling and analysis of entities and events for use cases that are most relevant to today's advanced insider and cyber threat scenarios.

FASTER

- Securonix Spotter® provides powerful search capabilities and enables rapid threat hunting using natural-language search. Searches can be visualized by pivoting on any entity to analyze events quickly and efficiently.
- Automated, time-based data distribution and tracking enables a consistent query response time, irrespective of the amount of data indexed.
- Automatically generates elegant visualizations and charts that can be saved as dashboards or exported via standard data formats. Securonix provides a library of built-in visualizations based by type of data source, type of threat and compliance requirements, plus custom dashboards for ad-hoc threat investigation or periodic threat and compliance monitoring.

MORE ECONOMICAL

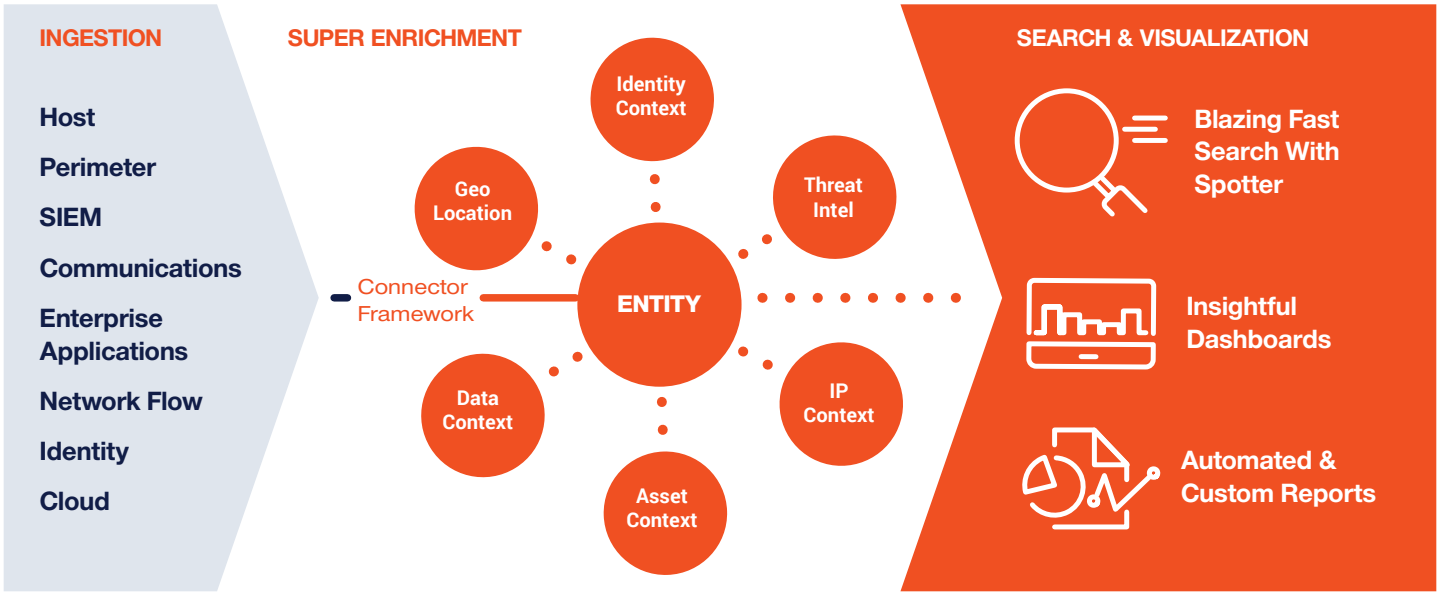
- Legacy data collection and log management tools create expensive overhead because they typically charge by the byte. SNYPR Security Data Lake delivers incredible cost efficiency through unlimited ingestion and storage.
- Open data model means raw and enriched events are available to any application for analytics, eliminating the need to create multiple data stores and the cost associated with licensing and maintaining them.
- Uses commodity hardware making it much more cost efficient compared to legacy log management products.

LEARN MORE
www.securonix.com

LET'S TALK
+1 (310) 641-1000

14665 Midway Rd. Suite #100, Addison, TX 75001 | ©2017 Securonix

UNCOVER ACTIONABLE DATA THROUGH SUPER-ENRICHMENT, SEARCH & VISUALIZATION



KEY FEATURES

Open Data Model

Securonix open data model uses a common data format for all security events in the Security Data Lake. This enables organizations to maintain a single copy of data in the Security data lake and make it available to any number of applications to run their own custom analytics. Unlike traditional log management your data is not locked into a proprietary data store, enabling you to use, share, manage and own your data without dependencies on the vendor platform.

Data Retention

Context aware enriched events are stored in HDFS and can be used for long term analysis, search and reporting. Raw event also maintained in HDFS for legal and compliance purposes. Securonix supports transparent disk encryption for security and privacy reasons. The solution also supports archival of data to external storage as needed. The data is HDFS is easily accessible to any external applications.

Connector Library

350+ out-of-the-box connectors integrate with a variety of structured and unstructured data sources including enterprise applications, identity systems and non-technical data sources such as badge readers and social media that are not supported by typical log management solutions. Rest API with fully published schema supports bi-directional integration with any target system.

Super Enrichment

Super enrichment of security data with contextual information at the time of ingestion helps transform raw events into meaningful information that is easy to understand, search and investigate. Contextual enrichment adds user identity, asset metadata, network information, geo-location and threat context to an event.

Threat Hunting

Securonix Spotter threat hunting product enables blazing-fast hunting using natural language search. Searching for threat actors and IOCs is simplified with visual pivoting on any entity to develop valuable threat context. Visualized data can be saved as dashboards or exported via standard data formats.

Visualization & Reporting

Securonix data insights provides built-in dashboards that are fully customizable. The solution has reporting capabilities to build your own scheduled and ad-hoc reports. Several user friendly formatting formats are supported out of the box.