SECURONIX™

DATASHEET

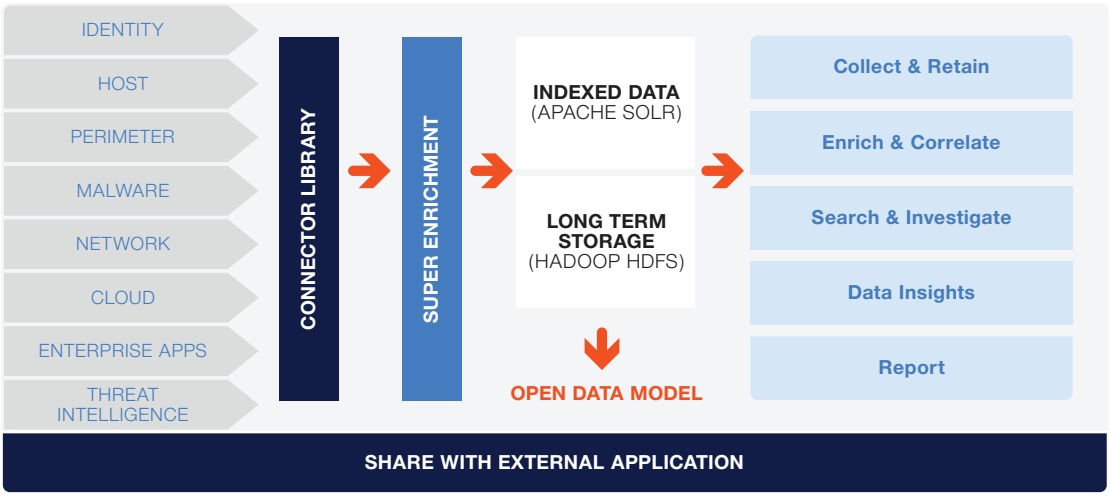
Securonix Security Data Lake

Unlimited Scalability with Rapid Search

Today's digital world generates a vast amount of data. The three Vs of big data — volume, velocity, and variety — have made security log management a big data problem. Securonix Security Data Lake, powered by Hadoop, is a highly scalable, fault tolerant, open data platform that ingests massive amounts of data and supports reliable and economical long-term data retention.

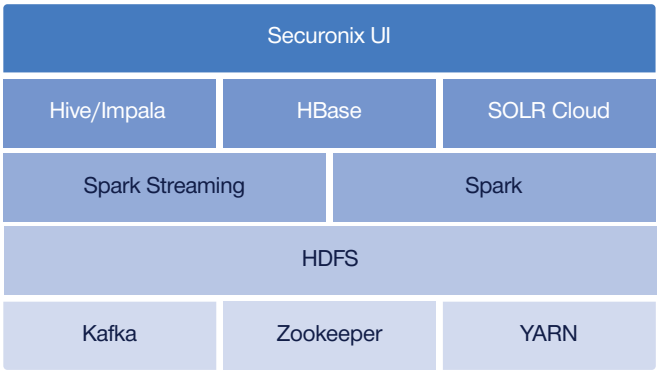
At the time it is collected, data is super enriched with contextual information including user, asset, IP address, geolocation, and network intelligence. This transforms raw log data into meaningful security insights that can be accessed using Securonix Spotter's blazing-fast search. Additionally, the open data format lets you keep a single source of log data and make it available for visualization, analysis, and reporting by other applications.

Massively Scalable Security Log Management



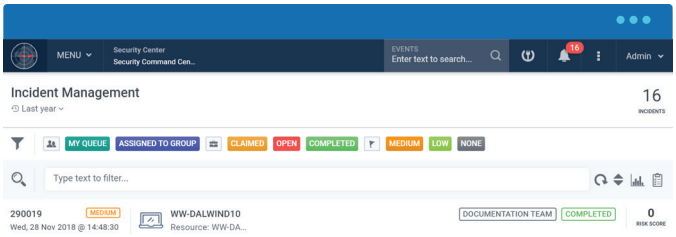
Product Features

Scalable Big Data Architecture



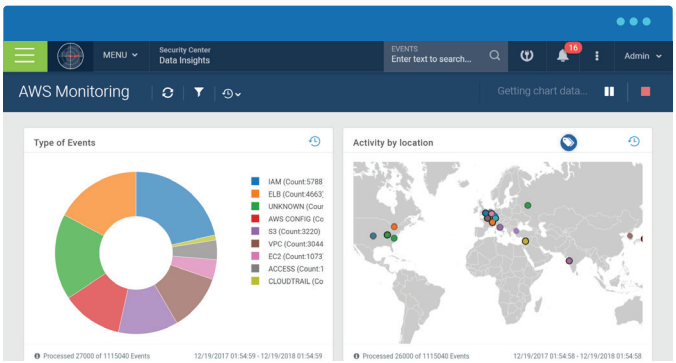
- Powered by Hadoop, a massively scalable, fault-tolerant open data platform that ingests hundreds of terabytes per day and supports economical long-term data retention.
- An open data model means you can maintain a single copy of your data in an open data format and make it available to other applications as needed.
- Unlimited long-term retention with over 90% compression.
- 100% native Hadoop components certified on Cloudera and Hortonworks.

Threat Hunting and Search



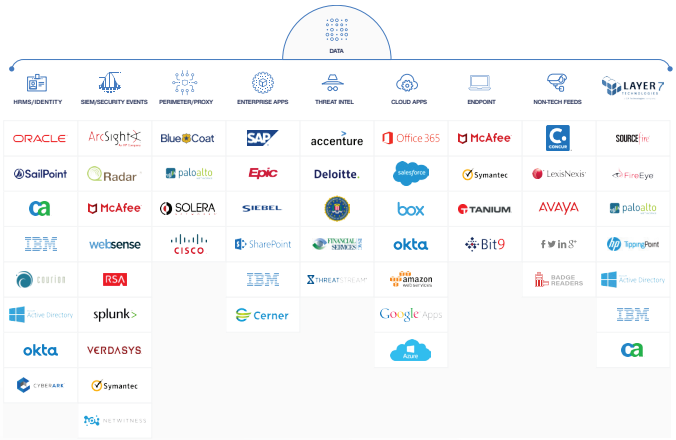
- Securonix Spotter enables blazing-fast threat hunting using natural language search.
- Searching for threat actors and IOCs is simplified with visual pivoting on any entity to develop valuable threat context.
- Visualized data can be saved as dashboards or exported in a standard data format.

Data Insights and Reporting



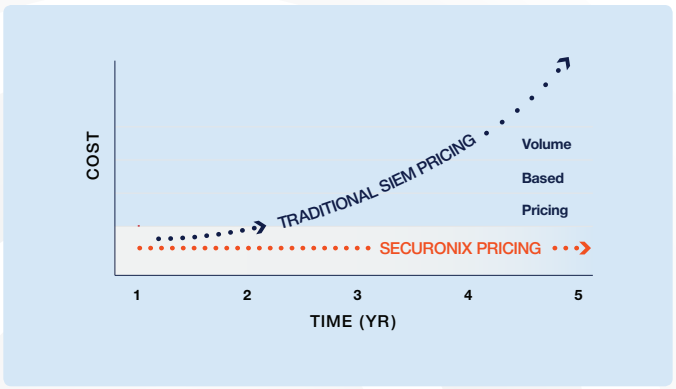
- Data insights with built-in shareable dashboards.
- Use out-of-the-box reports or create ad-hoc reports as needed.
- Includes compliance management reports with built-in packages that cover all major mandates, including PCI DSS, SOX, HIPAA, FISMA, and ISO 27001.

Connector Library and Context Enrichment



- Built-in connector framework with support for cloud applications, cloud infrastructure, enterprise applications, identity and HR data, and non-technical data feeds.
- Unstructured data parsing with REGEX.
- Simple parsing rules defined through UI.
- Real-time enrichment of data with identity, asset, geolocation, threat intelligence and data from lookup tables.

Predictable Identity-Based Pricing



- Cost is based primarily on identity instead of by events per second or gigabytes, so costs are predictable, even as your data requirements increase.
- Deploy on commodity hardware, which is much more cost efficient compared to legacy log management products with proprietary hardware requirements.
- With optional Securonix Threat Monitoring Services, Securonix will also manage your threat monitoring for you, giving you time back to focus on your core business.

For more information about Securonix Security Data Lake visit www.securonix.com/security-data-lake/

SECURONIX™

LEARN MORE
www.securonix.com

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

14665 Midway Rd. Suite #100, Addison, TX 75001 | ©2018 Securonix