SECURONIX™
Security Analytics. Delivered.

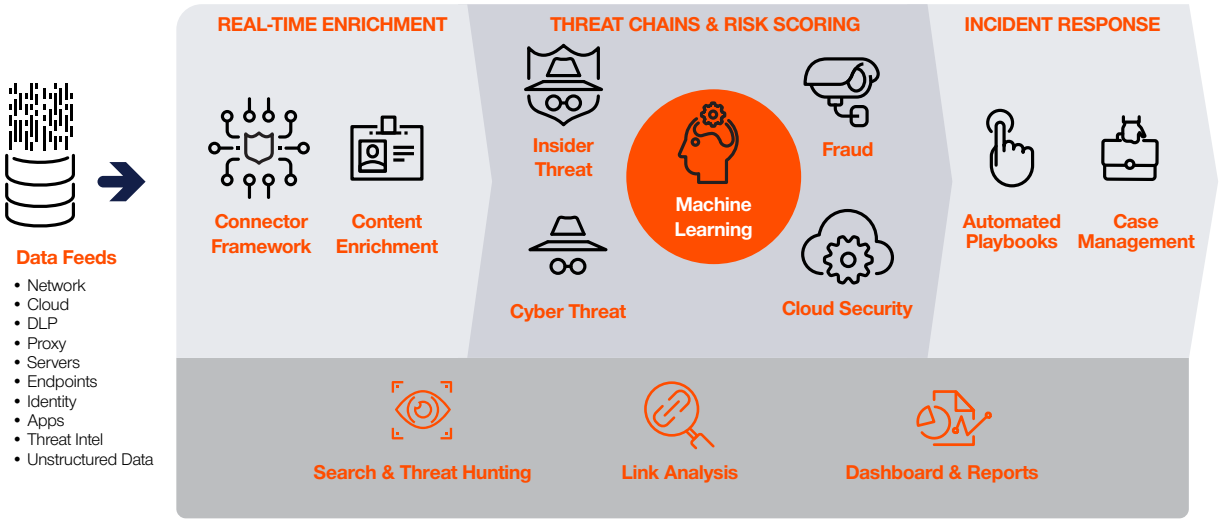
DATASHEET

Securonix Security Analytics Platform

Next-Generation SIEM, Simplified

The cybersecurity landscape is getting more complex. Hackers continue to innovate; business technologies generate increasing amounts of data; and obsolete perimeter defenses struggle with modern insider and cyber threats. Built on big data, Securonix Security Analytics Platform combines log management, security incident and event management (SIEM), and user and entity behavior analytics (UEBA) into a complete, end-to-end platform that can be deployed in its entirety or in flexible, modular components. It collects massive volumes of data in real-time, uses patented machine learning algorithms to detect advanced threats, and provides actionable security intelligence for quick response.

Collect, Detect, and Respond to Advanced Threats



Collect

Securonix Security Analytics Platform collects massive volumes of data, enriching raw events in real-time with meaningful identity, asset, network, geo-location, and threat intelligence context. Connectors support a variety of data sources, including cloud sources and non-technical data sources—such as badge readers and social media—that are not usually supported by log management solutions.

Detect

Unlike legacy SIEM solutions that rely on signatures, Securonix Security Analytics Platform applies sophisticated machine learning algorithms and threat chain modeling to event data in real-time to accurately detect advanced and insider threats. Every alert is automatically ranked so analysts can prioritize their response.

Respond

Comprehensive incident management workflow capabilities and an automated incident response framework enables you to automate remediation actions on select threats. Seamless API integration with third party solutions–including security orchestration, identity management, endpoint detection and response, and network access control systems–allows for a coordinated response.

Product Features

Avoid Vendor Lock-In with an Open Data Model

Unlike legacy security solutions, your data is not locked into a proprietary database. An open data format lets you to use, share, and manage your own data. This means you can maintain a single copy of data and make it available to other applications to use.

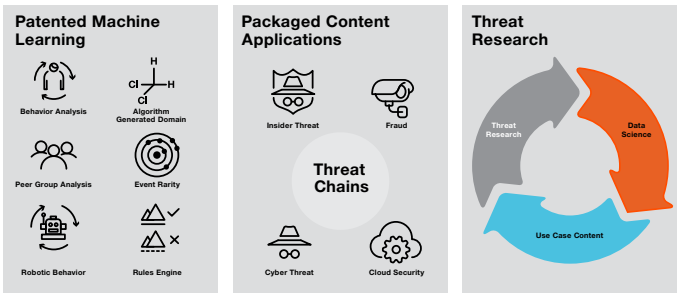
Contextual Awareness Gives You the Big Picture

Securonix Security Analytics Platform enriches security data with contextual information at the time it is ingested. Contextual enrichment adds user identity, asset metadata, network information, geo-location, and threat context to an event. This transforms raw events into meaningful information that is easy to understand, search, and investigate.

Secure, Reliable Long-term Data Storage

Enriched events are stored in a Hadoop distributed file system (HDFS) and can be used for long-term analysis, search, and reporting. Raw events are also maintained in HDFS for legal and compliance purposes. Securonix Security Analytics Platform supports transparent disk encryption for security and privacy reasons. It also supports the archival of data to external storage as needed. The data in HDFS is accessible to any external applications as needed.

Advanced Analytics Find Events with Minimal Noise



Securonix Security Analytics Platform detects threats using a combination of patented machine learning and statistical analytic models. Using threat chains, it stiches together a chain of events over time in order to surface the highest risk events.

Clear Visibility into Your Cloud

Extend your security monitoring to your cloud environment. Securonix Security Analytics Platform has built-in APIs for all major cloud infrastructure and application technologies. This allows you to analyze user entitlements and events to look for malicious activity. Correlate cloud data and on-premises data to analyze end-to-end activities and detect actionable threat patterns.

Straightforward Threat Hunting

Securonix Spotter enables blazing-fast threat hunting using natural language search. Searching for threat actors or indicators of compromise (IOC) is simplified with visual pivoting available on any entity in order to develop valuable threat context. Visualized data can be saved as dashboards or exported in standard data formats.

Built-In Applications

Out-of-the-box content in the form of packaged applications enable rapid deployment and quick time to value. Applications include threat models and built-in connectors that are specially designed for insider threat, cyber threat, fraud, and cloud security use cases. Elegant visualizations allow you to view the threats in context and take intuitive, easy-click actions to mitigate.

Discover the Securonix Threat Library

The Securonix Threat Library is a collection of threat models created by the Securonix cyber research team in collaboration with customers, partners, and national security leaders. The library enables you to access, download, and deploy with a single click.

Faster Investigations & Automated Incident Response

The Securonix Investigation Workbench allows you to rapidly investigate incidents by pivoting on anomalous entities and tracing associated activities and events. Comprehensive incident management and workflow capabilities allow multiple teams to collaborate on an investigation. Incident response frameworks enable you to automate remediation actions on select threats.

Simplify Your Compliance Efforts

Securonix Security Analytics Platform simplifies your compliance process by allowing you to consolidate multiple different control sets while still allowing for specific compliance use cases such as anti-money laundering, trade surveillance, and internal and external fraud. Advanced analytics allow you to easily detect access violations; analyze rogue, orphaned, or terminated accounts; drive user self-service access reviews; and support risk based access reviews.

Convenient Cloud-Based SaaS

With Securonix Cloud you can enjoy all the capabilities of Securonix Security Analytics Platform, with the convenience of a software-as-a-service (SaaS) solution. It provides security that spans across your cloud infrastructure, data, applications, and access control solutions. Benefit from the quick deployment, easy scalability, and shorter time to value of Securonix Cloud.

For more information about Securonix Cloud visit www.securonix.com/securonix-cloud/

For more information about Securonix Security Analytics Platform visit www.securonix.com/security-analytics-platform/

SECURONIX
Security Analytics. Delivered.

LEARN MORE
www.securonix.com

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

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