SECURONIX™

SOLUTION BRIEF

Threat Hunting with Securonix

Live Channel | Long-Term Search | Community-Powered Threat Hunting

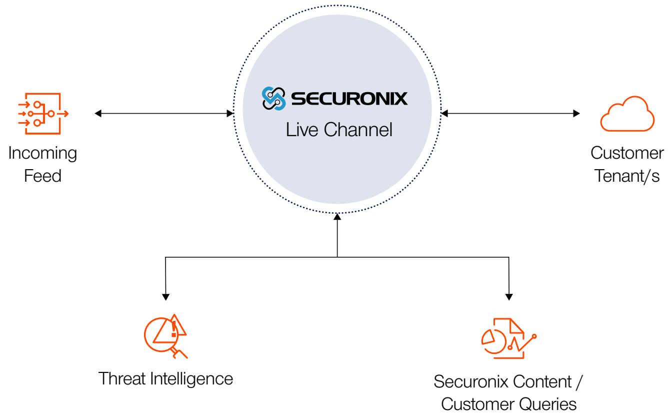
Threat Hunting is Essential

Attackers are constantly trying to bypass an organization's existing security controls. Any delays in detection can cause significant damage as attackers quietly remain in the network for months, collecting data, confidential material, or even login credentials that allow them to move laterally into connected systems.

Unlock Your Hidden Potential

Securonix Next-Gen SIEM allows you to more quickly detect advanced and sophisticated threats that would otherwise remain in your network, undetected. It improves your threat detection and response capabilities, giving you the ability to:

- Multiply your threat hunting strength by 10x with the security industry's first Community-Powered Threat Hunting capability.
- Discover sophisticated threats by leveraging the ability to search and act on real-time, streaming data with Live Channel.
- Find threats hidden in historical data with Long-Term Search at 1/3 the cost of competing solutions.



Real-Time Search on a Live Channel of Streaming Data

Typically, security teams must wait until data is ingested and indexed before they can search. This increases the time required to detect and respond to threats. Also, it can mean that users are not always aware when there is a disruption in the ingestion pipeline. Live Channel addresses both challenges, giving customers complete visibility into — and allowing security teams to search for active threats on — live, streaming data even before data is parsed or indexed.

- **Reduce Detection Time for Active or Hidden Threats:** Security teams can hunt for active threats in raw data — before indexing occurs — with virtually zero latency.
- **Test for Data Disruptions:** Securonix Live Channel can be used to troubleshoot data pipeline issues and confirm that data sources are being ingested correctly.
- **Save and Share Searches:** So that security teams can work together to find anomalies and compare them against their own hypotheses.

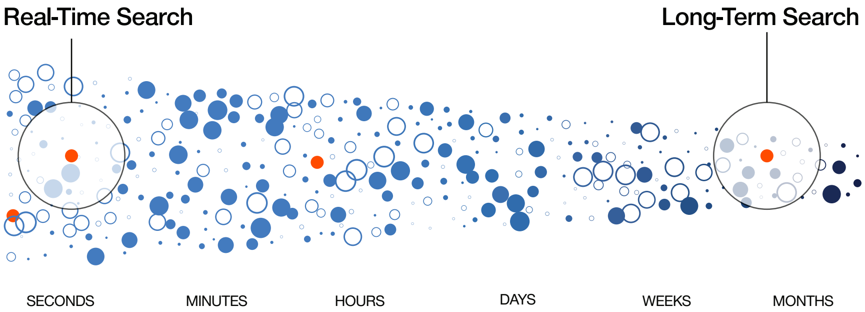
Solution Benefits

- Find active threats that may have bypassed existing detection solutions.
- Discover hidden threats using the ability to easily search on historical data.
- Multiply your threat hunting strength 10x with proactive community-powered threat content.
- Reduce the cost of searching long-term data by up to one-third, as compared to similar solutions.

Hunt for Threats Across Historical Data Using Long-Term Search

Finding hidden threats that already exist in your environment requires the ability to investigate historical data. While some SIEM solutions may allow you to search across historical data, the search negatively impacts the performance of their SIEM because they lack scalability, impeding existing ingestion and detection. Historic search is also costly because most vendors are forced to pass the cost of their non-effective scalability on to their customers.

Securonix addresses this challenge through innovation. Leveraging its cloud native, big data architecture, the Securonix platform decouples search and compute resources so that it can scale on demand to deliver high-performance searches on long-term data at an affordable rate. It provides this capability at one-third of the cost of comparable solutions.



Leverage Community-Powered Threat Hunting

Security operations center (SOC) teams are at a disadvantage when it comes to detecting today's continuously evolving threats if they rely solely on their own threat hunting content. Using a community-driven approach, Securonix creates collaborative threat hunting playbooks for customers to leverage. Your team can strengthen their threat hunting efforts with contributions from Securonix Threat Labs, commercial threat intelligence, and global user communities such as MITRE ATT&CK and Sigma.

Uncover and Detect Hidden Threats with Securonix

Securonix Next-Gen SIEM provides effective threat hunting for unknown and sophisticated threats, whether they are new or if they are already hidden deep in your environment. With Securonix threat hunting you are able to detect threats in real-time, on live streaming data, as well as uncover hidden threats concealed in your environment by performing scalable search on stored historical data without negatively impacting your SIEM's performance. Securonix also empowers your team with the latest security content so they can detect evolving and active threats.

For more information about how Securonix can improve your search and threat hunting capabilities visit us at www.securonix.com or schedule a demo www.securonix.com/request-a-demo.

Solution Features

- Live Channel enables real-time threat hunting on live, streaming data.
- Long-Term Search supports search across historical data for rare events, sequence, and log anomalies.
- Community-Powered Threat Hunting allows seamless collaboration and the ability to share security intelligence with your peers and global community, leveraging MITRE ATT&CK and Sigma.

About Securonix

The Securonix platform delivers positive security outcomes with zero infrastructure to manage. It provides analytics-driven next-generation SIEM, UEBA, and security data lake capabilities as a pure cloud solution, without needing to compromise. For more information visit www.securonix.com.

SECURONIX™

LEARN MORE
www.securonix.com

©2021 Securonix

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