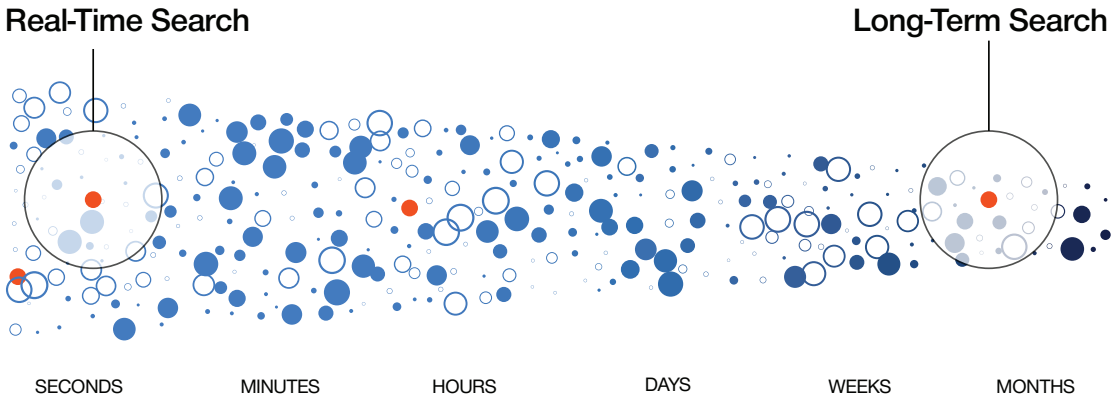
SECURONIX™

DATASHEET

Long-Term Search

Affordable Threat Hunting at Scale

Is the enemy already inside? With global dwell time averaging around 60 days, threat hunting continues to be an important part of cybersecurity resiliency. However, searching across historical data is costly and time consuming. Many legacy SIEM vendors aren't able to dynamically scale for fast search across archived data without throttling. However, Securonix empowers threat hunters with Long-Term Search at 1/3 of the cost and nearly unlimited scale. With Long-Term Search, organizations can reduce the time needed to investigate and find threats that are already in their environment.



Threat Hunting

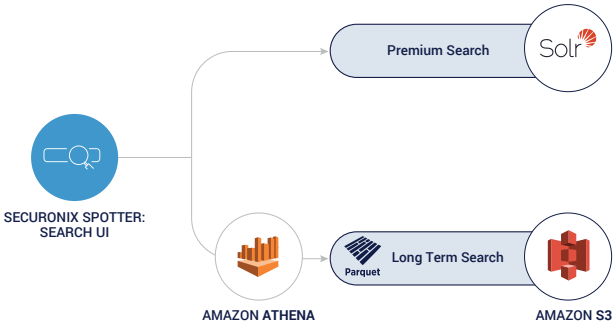
Security analysts need to continually ask new questions from their data in order to understand if threats already exist in their environment. For example, an analyst may learn from a reputable threat intelligence source that their industry is being targeted. They need to investigate a new indicator of compromise that was uncovered to see if an attacker is already inside. Securonix's cloud native SIEM allows threat hunters to be proactive, making search on historical data fast and affordable.

Benefits of Long-Term Search

- Decrease the dwell time of hidden threats persisting in your organization's environment.
- Reduce cost of searching on historical data by up to one-third.
- Empower threat hunters with fast, reliable, on-demand search on long-term data.

Product Features

Decouple Compute and Search for Better Search Performance

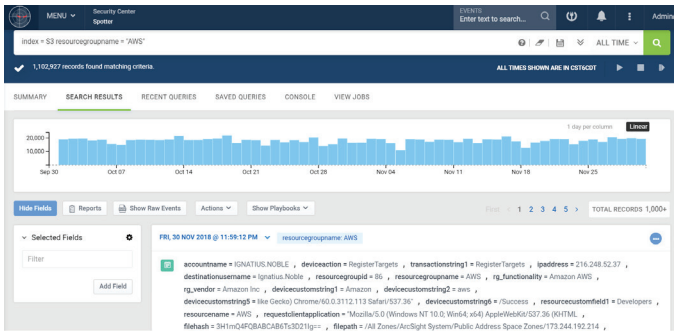


Search long-term data on-demand by decoupling search from compute resources, without impacting performance.

SIEM performance is not impacted because long-term search in AWS S3 doesn't use the same resources as premium search.

Long-term search is an on-demand capability.

Fast Search on AWS S3 Data



Fast search on historical data located in AWS S3 empowers threat hunters.

Threat hunters can query AWS S3 using Athena to bring rapid results.

Forget 'hot', 'warm,' and 'cold' data storage mathematics. Scale archived data with almost zero latency due to Securonix's cloud architecture leveraging AWS Athena.

Affordable Search

Affordable search is achievable due to a smaller data footprint resulting in a much lower cost.

An organization's long-term data is compressed using Parquet format and stored in AWS S3, resulting in a small data footprint.

When a threat hunter uses Securonix's cloud native SIEM for long-term search it costs you significantly less than other IT SIEM vendors charge.

Want to see how Securonix finds hidden threats and decreases detection and response times?
Contact us for a demo.

SECURONIX™

LEARN MORE
www.securonix.com

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