securonix

Top 5 Reasons

the Data Cloud Improves Threat Detection, Investigation, and Response (TDIR)

Today's Reality:

Traditional SIEMs use a multi-tiered "Hot, Warm, Cold" data storage approach. When data demand grows, this model becomes overwhelmed and performance wanes.

SIEMs must rethink multi-tiered data storage and how that data is made accessible for security operations because data growth is not slowing down.

Securonix meets this challenge with our Unified Threat Defense SIEM that leverages a single-tiered data cloud to meet the data demands of today and tomorrow.

Here are 5 ways Securonix improves threat detection, investigation, and response (TDIR)!

1

Gain better efficiency when searching large data sets

Stop having to use 3rd party tools or run multiple searches across small time increments. Instead, access long-term data, without limitation, and streamline investigation and hunting workflows.

Up to 8x faster

2

Achieve faster search results

Accelerate investigations and hunting workflows by getting the data you need at lightning speed – even for complex queries.*

365 Days of "Hot" Searchable Data

3

Expand data retention

Make key data accessible for longer to detect threats that dwell in your environment. Be able to see what happened before, during and after a breach.

Realize complete TDIR in one platform

No need to move in and out of tools and interfaces. Get a seamless user experience and visibility to identify, analyze, and remediate complex and sophisticated threats in one platform.

4

Take advantage of advanced analytics innovations

Propel hunting and investigations by combining the latest threat content and models with extensive data. Continuously improve your security operations by more effectively leveraging and analyzing data.

5

*Based on internal testing using real-world data.

Visit the Securonix Unified Defense SIEM webpage to learn more.

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, SOAR, Security Data Lake, NDR, and vertical-specific applications as a pure SaaS solution with unlimited scalability and no infrastructure cost. Securonix reduces noise and prioritizes high fidelity alerts with behavioral analytics technology that pioneered the UEBA category.

For more information about Securonix, schedule a demo at: **www.securonix.com/request-a-demo**.

securonix

www.securonix.com

Follow us @securonix