securonix

SOLUTION BRIEF

Accelerate Security Operations with the Power of the Data Cloud

Built for Performance, Data Retention, and Innovation.

Traditional SIEMs Struggle with Modern Demands

As threats grow in complexity, organizations need to be able to collect data from everywhere and retain that data for longer time periods. The increased demand for capacity and higher performance overwhelms traditional SIEMs.

While tiered data storage models used to be sufficient, they no longer meet the requirements of modern security operations. The challenges in multi-tiered storage models becomes more obvious when searching large amounts of data across hot and cold stored data. In this tiered model users are provided with limited results, or they need to perform a time-consuming process of rehydrating cold data. Many security operation teams are forced to use workarounds to search vast sets of data to find the information they need. The workarounds yield inefficiency while increasing operational costs and threat mitigation times.

Introducing Securonix Unified Defense SIEM

Securonix Unified Defense SIEM leverages a single-tier storage approach that takes advantage of proven Snowflake Data Lake technology to collect massive volumes of data, in real-time. The single-tier, data cloud is purpose built to meet big data demands. Leveraging a virtually limitless data cloud delivers vast scalability, high performance, and extended data retention.

Having extensive data readily available fuels machine learning advanced threat analytics and provides pinpoint security incident response capabilities for fast remediation.

The data cloud is the backbone of the Securonix Unified Defense SIEM which gives your security team profound visibility, detection, and response at scale and integrates seamlessly with all the data sources, threat intelligence tools, and other technologies in your SOC that enable your analysts to stay on top of threats.

Using a single-tier data approach, threat hunters and security analysts can search larger sets of data without worrying if the data is within hot, warm, or cold storage. When data is stored in a centralized location, security analysts unlock faster search results across longer time periods to accelerate mean-time-to-respond (MTTR). This new architecture establishes the foundation to meet the needs of modern threat detection, investigation, and response (TDIR) for years to come!

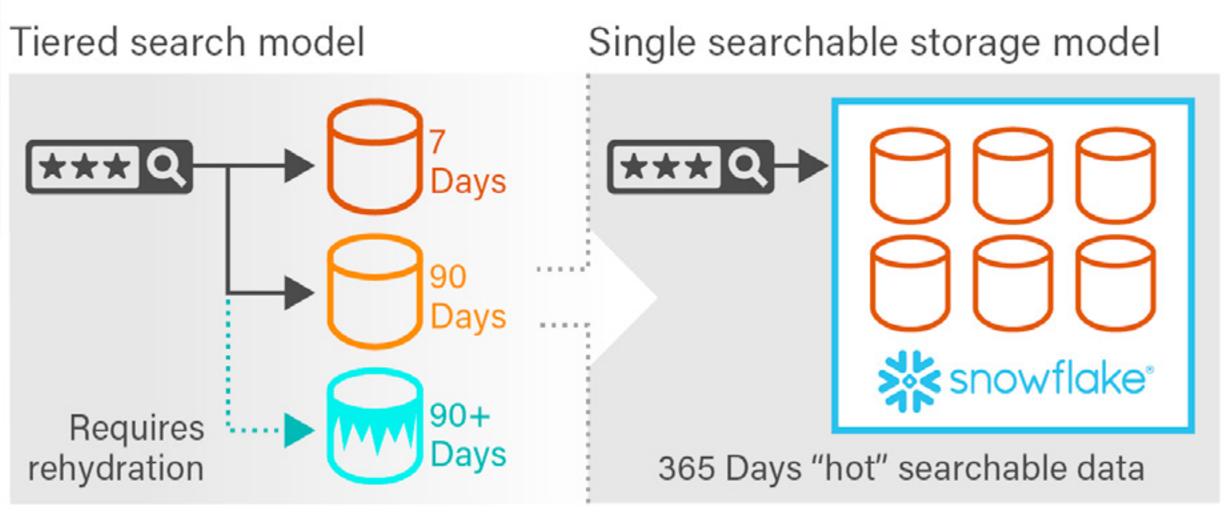


Figure 1: Securonix Unified Threat Defense SIEM improves efficiency with a single-tiered data storage model making data readily available with up to 365 days of "hot" searchable data.

How it Works

The Securonix Unified Defense SIEM consolidates data from the cloud and physical locations into the Snowflake Data Cloud. The Snowflake Data Cloud provides virtually unlimited scalability that is leveraged by Securonix industry-leading analytics and threat hunting workflows to improve the efficiency of your security operations. Snowflake Data Cloud establishes the foundation for future innovations, enabled by a simplified and robust data storage model.

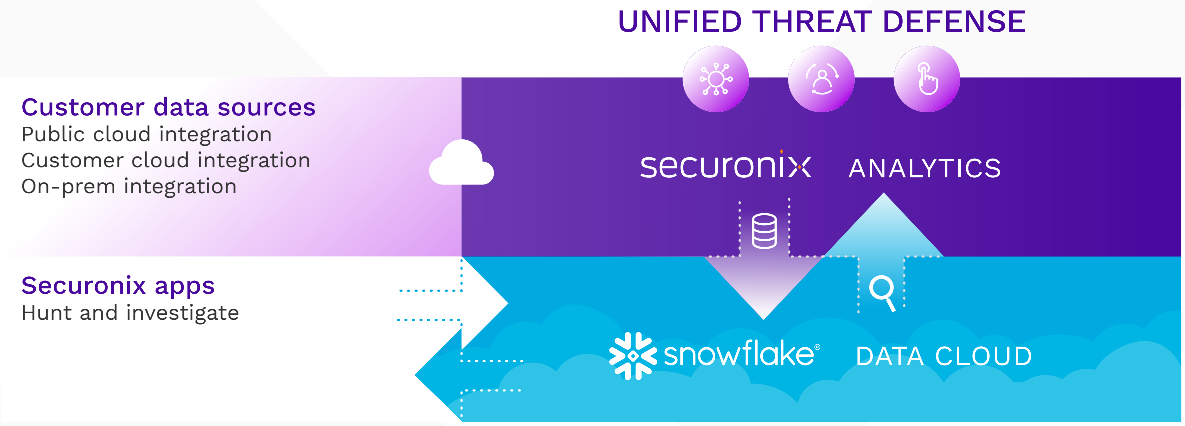


Figure 2: Securonix Unified Defense SIEM takes industry-leading analytics and threat hunting capabilities to the next level by leveraging the single data cloud from Snowflake.

Virtually Unlimited Capacity, Improved Performance, and Longer Data Retention

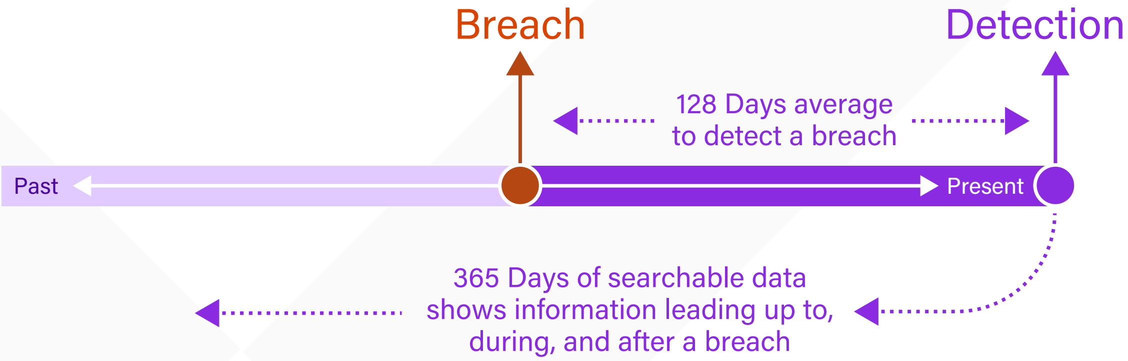
Securonix Unified Threat Defense SIEM reimagines threat detection, investigation, and response with 365 days of searchable data and faster search performance. The Securonix Solution is a unified platform for data storage, management, and analytics, with the ability to access and analyze data in real-time. It supports a wide range of data types and formats, enabling quick ingestion. This new architectural approach establishes the foundation to develop powerful Securonix applications and advanced threat models.

Fast Access to Data During Hunts and Investigations

Removing the tiers for data storage simplifies operations by eliminating the need to understand if the data you are looking for is stored within “hot, warm, or cold” repositories when running searches and performing threat hunting. The no-tier approach delivers a single data store perfect for large scale searches, while maintaining high performance. This is because all searchable data is “hot” and serviced from a single tier.

Leverage 365 Days of "Hot" Searchable Data

Take advantage of one year of searchable data for threat investigations and hunting. According to a Thoughtlab's report titled, "Cybersecurity Solutions for a Riskier World",* cyber breaches take 128 days to detect. A single data store allows for more effective analytics and threat hunting workflows. With long-term data readily available security practitioners can perform searches and hunts across longer time frames to understand today's most complex threats. Having one year of data available provides insight into activities leading up to, during and after an event. This expanded storage reduces the need to rehydrate data from cold storage during investigations across longer time frames.


Breach
Detection
128 Days average to detect a breach
Past
Present
365 Days of searchable data shows information leading up to, during, and after a breach

Amplifying Your Securonix Unified Defense Capabilities

Leveraging a data cloud to deliver a modern, single-tiered, and highly scalable data storage model establishes the foundation to improve virtually all Securonix threat detection, investigation, and response capabilities.

Advanced Analytics

Designed with advanced analytics at its core, our Unified Defense SIEM solution leverages machine learning algorithms, contextualized enrichment, and user-based risk scoring to help you uncover complex threats with minimal noise. The threat content leveraged by these analytics is continuously delivered as-a-service. With threat chain analytics you can reduce the volume of alerts using threat models that map to both MITRE ATT&CK and US-CERT frameworks.

*Source: Thoughlabs, "Cybersecurity for a Risker World.";2022

These threat chains tie seemingly insufficient alerts together to deliver a combined risk score. This risk score delivers the confidence to know where to spend your time and resources. The single-tier data model supercharges these advanced analytics with readily available data that delivers faster results.

Autonomous Threat Sweeper (ATS)

ATS automatically and retroactively hunts for new and emerging threats in current and long-term historical data based on the latest, up-to-date threat intelligence. ATS automates the process of assessing your exposure to emerging threats with the ability to detect low and slow threats through post-hoc detection of both IOCs and TTPs, extracted and codified by Securonix Threat Lab. Leveraging a single-tier data cloud accelerates this capability by reducing the number of data sets that must be searched.

Security Orchestration, Automation, and Response (SOAR)

Securonix SOAR helps security operations teams accelerate incident response by streamlining workflows between detection and investigation to response. Securonix improves the efficiency of these workflows by leveraging the same set of data with the data cloud. Unlike other SIEMs with bolted-on SOAR that need to move, duplicate, and correlate data between the functions. This allows you to simplify the threat detection, investigation and response process and reduce mean-time-to-respond.

securonix

About Securonix

Securonix is leading the evolution of SIEM for today's hybrid cloud, data-driven enterprises. Securonix Unified Defense SIEM provides organizations with the first and only content-driven threat detection, investigation and response (TDIR) solution built with a highly scalable data cloud and a unified experience from the analyst to the CISO. The innovative cloud-native solution enables organizations to scale up their security operations and keep up with evolving threats. For more information visit securonix.com