securonix

snowflake

SOLUTION BRIEF

Take Advantage of Snowflake for Cybersecurity

Combine Securonix and Snowflake for Cost-Optimized Threat Detection and Response

Threat Visibility Should Not Consume Your Entire Security Budget

Security data is critical to identify sophisticated and aggressive threats. As organizations grow, they must bring in data from a wide range of sources to effectively gain visibility to threats. The byproduct of expanding this visibility is that the amount of data that is collected and stored also grows and therefore the cost associated and performance issues increase. This may leave you feeling like you are being forced to choose between paying higher costs associated with more data or restricting the amount of data stored, limiting threat detection capabilities. As you deal with strict budgets, neither approach is suitable to keep pace with today's complex and business impacting threats. To cost-efficiently deliver the storage capacity you need, Securonix and Snowflake have joined forces to deliver industry-leading analytics with virtually unlimited scale.

securonix | snowflake

Combining Forces to Deliver Threat Detection and Response at Cloud Scale

Securonix and Snowflake are partnered to provide a fully integrated solution delivering best-of-breed security analytics on top of a scalable cloud data lake.

Securonix + Snowflake combines leading technologies for better threat detection at cloud scale.

The Securonix + Snowflake solution allows you to own your data and store it in an open and highly accessible format in a single location.

Snowflake's data cloud delivers a modern security data lake with virtually unlimited storage and scalable compute. The ability to collect all data empowers rapid investigations across terabytes and petabytes of data. Organizations only pay for the use with Snowflake's consumption-based pricing. Snowflake's only pay for what you use pricing translates into significant cost savings.

Securonix delivers industry-leading threat detection and response and threat hunting capabilities that take advantage of best-in-class analytics and threat content. These analytics and threat hunting capabilities leverage a unified approach using identity context that reduces false positives and streamlines investigation workflows. Organizations such as Alberta Health Services have reported a 90% decrease in false positives using Securonix.

When combined, Securonix + Snowflake delivers the visibility you need to detect, investigate and respond to today's complex threats while delivering the cost-efficiency and scale needed to meet the demands of any organization.

Threat Mitigation at Scale without Compromise

Securonix + Snowflake resolves the need to limit security visibility to control cost. You can leverage industry-leading security analytics at scale without sacrificing speed or your budget.

Storing data within the Snowflake data lake allows you to take advantage of Snowflake's affordable consumption model. Snowflake leverages a per-second pricing model, which means that you only pay for the compute services that are being used which results in massive cost savings. These savings can be extended to your SIEM. The Snowflake consumption model allows you to avoid spiraling data ingestion costs. Organizations can be assured they are optimizing costs as their data requirements grow or they add more data sources.

Consolidate Your Security Data in One Place

Unify your logs and enterprise data in a single place and store virtually unlimited amounts of data for years.

Run Advanced Analytics Like Never Before

You can combine business and contextual data sets, not normally sent to a SIEM, with security data to achieve better fidelity and automation. Implement the latest threat content from Securonix ThreatLabs to identify new or emerging threats.

One Platform, Many Cyber Use Cases

Integrate Securonix content and visualizations for faster threat detection and response. You can take advantage of up-to-date content to identify the latest sophisticated attack techniques, tactics and procedures.

Elastic Compute Power and Instant Scalability

The Snowflake Data Cloud's separation of compute and storage allows investigations to run at breakneck speed. By automatically scaling compute resources up and down, you only pay for what you use. This allows you to focus on mission-critical activities without worrying about concurrency, resource contention, compute power, scalability, or cost.

Avoid Siloed Security Data

No longer maintain, manage, and govern separate enterprise and security data repositories.

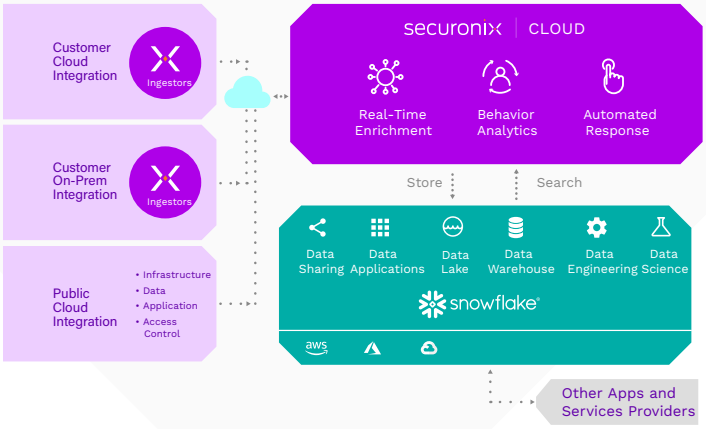
The Securonix + Snowflake Joint Solution

Securonix and Snowflake have created a split architecture solution that consolidates data within Snowflake implementations while leveraging Securonix security visibility, analytics, and intelligence-based incident response. Data, services, and applications are optimally deployed between the Snowflake Data Cloud and Securonix's cloud-native infrastructure. You can now consolidate your entire enterprise and security data into a single location and take advantage of advanced analytics for detection and response.

The shared deployment models deliver Next-Gen SIEM functionality as a seamless extension of your Snowflake cloud environment:

- Securonix collects and formats data to maximize value.
- Store and analyze all security logs in one place allowing for faster detection and response to threats.
- Perform searches via the - Securonix UI for powerful investigation capabilities that leverage the Snowflake back-end
- Eliminate the need to archive data in cold storage or use unreliable data rehydration procedures with data that is always ready for searching.

Gain complete visibility, actionable insights, better automation, and significant savings using Securonix with Snowflake.



The Securonix + Snowflake Architecture Works in Unison to Deliver Better Threat Detection and Response

securonix

Benefit from Snowflake's Scale and Cost Control

Snowflake is not bound by the limitations of a legacy on-premises solution. The shared data architecture enables you to scale, even on the fly, as your data storage demands increase.

The Securonix Solution capitalizes on the data, architecture and features inherent to the data cloud. Securonix + Snowflake delivers a single source of truth that removes silos and reduces complexity by analyzing all logs, assets, and configurations in one place. Layering Securonix on top of the data lake you get a consolidated user interface with the ability to seamlessly search, hunt, and visualize data in the Snowflake. These abilities are available at scale and without performance compromise.

Meet Modern Operational Use Cases

Securonix + Snowflake work together to deliver modern cybersecurity operation capabilities and use cases.

- Enable faster detection and response by streamlining investigation with real-time enrichment and advanced analytics.
- Aggregate data from all clouds to support multi-cloud environments.
- Take advantage of up-to-date threat content created by Securonix ThreatLabs to stay ahead of new and emerging threat Techniques, Tactics, and Procedures (TTPs)
- Leverage native user and entity behavior analytics (UEBA) to identify insider threats quickly and easily.
- Simplify your data security and governance with consistent implementation of security and privacy controls for data protection with a single copy of data.
- Retain your data within your dedicated environment to meet regulatory compliance such as GDPR.

About Snowflake

Snowflake delivers the Data Cloud — a global network where thousands of organizations mobilize data with near-unlimited scale, concurrency, and performance. Inside the Data Cloud, organizations unite their siloed data, easily discover, and securely share governed data, and execute diverse analytic workloads. Wherever data or users live, Snowflake delivers a single and seamless experience across multiple public clouds. Snowflake's platform is the engine that powers and provides access to the Data Cloud, creating a solution for data warehousing, data lakes, data engineering, data science, data application development and data sharing. Join Snowflake customers, partners and data providers already taking their businesses to new frontiers in the Data Cloud.

About Securonix

Securonix is redefining SIEM for today's hybrid cloud, data-driven enterprise. Built on big data architecture, Securonix delivers SIEM, UEBA, XDR, 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 visit securonix.com