securonix

DATASHEET

Bring Your Own Snowflake

Threat Detection and Response at Cloud Scale

Big Data Security Challenges

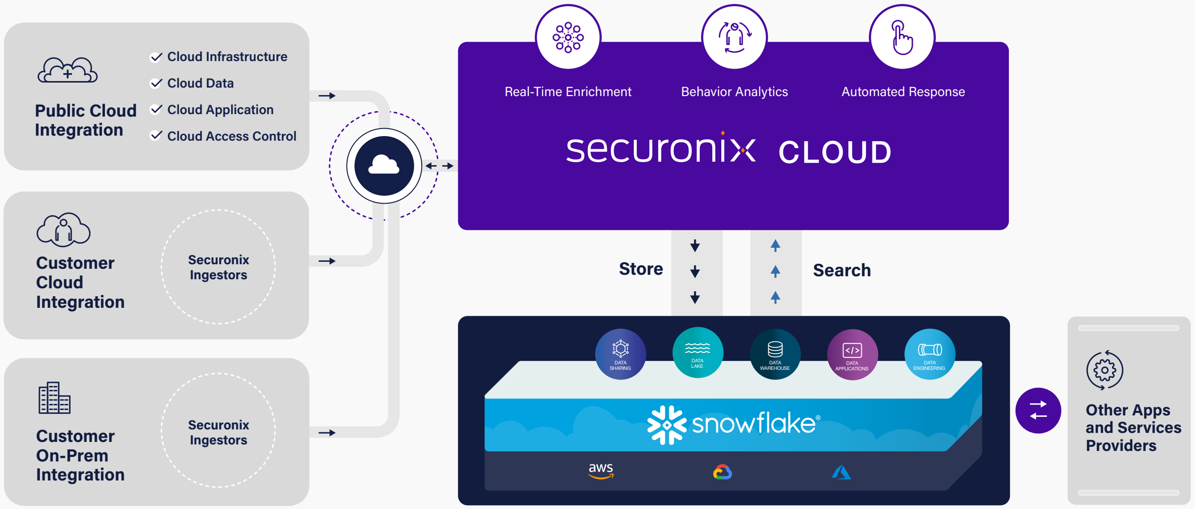
As enterprises move to the cloud, traditional SIEM solutions are unable to keep up with the scale and complexity of security data. The resulting limitations and visibility gaps make it difficult to effectively detect and respond to threats. Early attempts to solve this problem failed to ingest, enrich, and format the data into actionable use cases for analysts.

On the other hand, cloud data platforms are built for cost-effective analytics at a massive scale but lack the security integrations and out-of-the-box analytics that security teams need.

The Solution: Bring Your Own Snowflake

In an exciting new partnership, Securonix and Snowflake have created a split architecture solution that enables customers to use Securonix analytics on top of their existing Snowflake Data Cloud Platform. The joint solution allows Snowflake customers to keep their data within their Snowflake implementation while still leveraging Securonix Next-Gen SIEM for security visibility, analytics, and intelligence-based incident response.

Unlike traditional SIEM solutions that use a data consumption model, this hybrid approach enables data, services, and applications to be optimally deployed between the Snowflake Data Cloud and Securonix's cloud-native infrastructure. With the joint solution, organizations can consolidate their entire enterprise and security data into a single location and take advantage of advanced analytics for detection and response.



Solution Benefits

Gain a Single Source of Truth

All logs, assets, and configurations are analyzed together, removing silos and reducing complexity.

Transparent Pricing and Cost Savings

Affordable storage and per-second compute pricing cuts down on SIEM costs. Pay Snowflake directly to avoid spiraling data ingestion costs.

Faster Detection and Response to Threats

Centralized Securonix Next-Gen SIEM solution streamlines investigation and acts as an extension of the customer's Snowflake Data Cloud.

Customers can utilize Snowflake's single-tier architecture for cost-effective and bottomless cloud storage with a flexible retention policy that is controlled within the organization. Compute power is virtually unlimited and can be scaled as needed for rapid investigations across terabytes and petabytes of data. Additionally, Snowflake's consumption-based pricing means that you only pay for resources when used, which translates into significant cost savings overall.

Deployment Architecture Details

- Securonix hosts core SIEM application services, monitoring, microservices, and disaster recovery for the solution.
- The customer's existing Snowflake account receives normalized and enriched security data.
- Existing Snowflake Data Cloud resources are used for unlimited storage to power queries from the Securonix console.
- Business datasets from the customer's Snowflake account can be loaded independently and combined with security data for context enrichment.
- The customer owns all the collected log data and can leverage it for use cases beyond SIEM, such as operational observability, security metrics, and control validation.

Bring Your Own Snowflake for Detection and Response

Unlike traditional data consumption models, this shared deployment model delivers Securonix Next-Gen SIEM as a seamless extension of the customer's Snowflake cloud environment. All security logs are stored and analyzed in one place allowing for faster detection and response to threats in the customer's environment. Organizations can achieve complete visibility, actionable insights, better automation, and significant savings using Securonix with Snowflake.

For more information about Bring Your Own Snowflake,
schedule a demo at: www.securonix.com/request-a-demo