securonix | snowflake®

Global Infrastructure Leader Selects Securonix + Snowflake for Cloud & Data Security

CASE STUDY

Global Infrastructure Leader Selects Securonix + Snowflake for Cloud & Data Security

About Snowflake

Snowflake enables every organization to mobilize their data with Snowflake's Data Cloud. Customers use the Data Cloud to unite siloed data, discover and securely share data, and execute diverse analytic workloads. Wherever data or users live, Snowflake delivers a single data experience that spans multiple clouds and geographies. Thousands of customers across many industries, including 223 of the 2021 Fortune 500 as of July 31, 2021, use Snowflake Data Cloud to power their businesses.

Learn more at snowflake.com

The Challenge: Limited Insights and Lack of Visibility Into Multi-Cloud Environments and Security Events

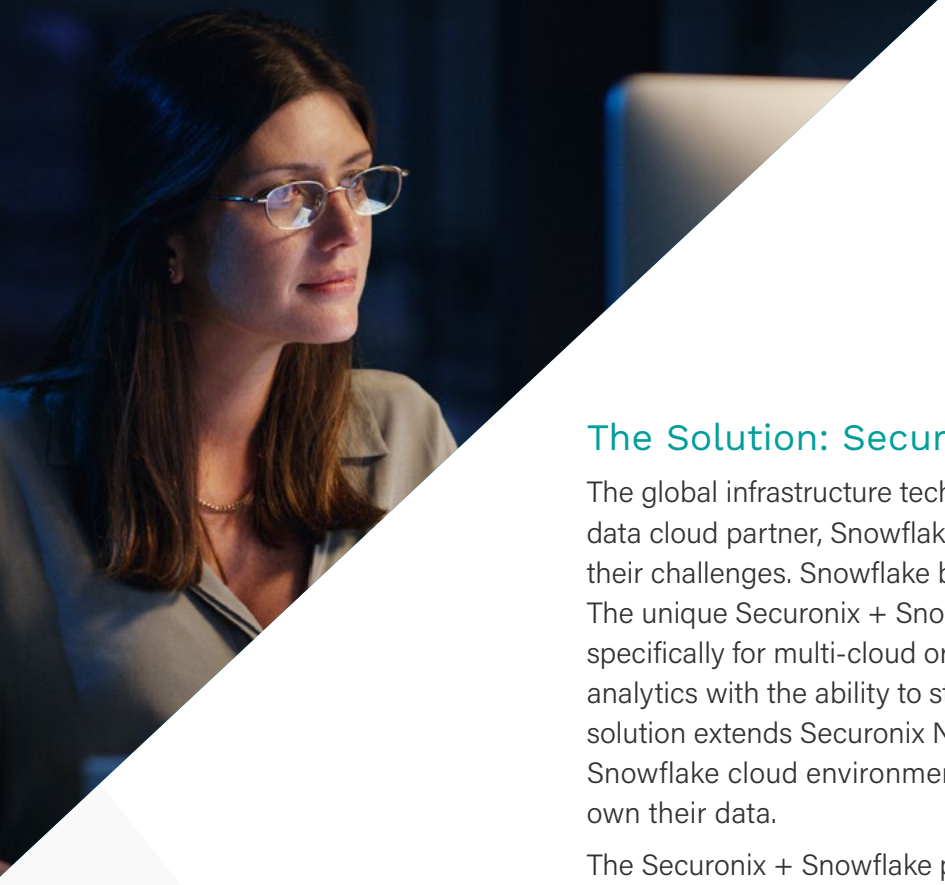
A leading global infrastructure technology company faced increasing challenges as they continued to acquire companies to expand their portfolio of services. Their previous SIEM solution was unable to meet a growing need for advanced analytics, active reporting, and agility in adapting to evolving multi-cloud environments.

With data stored in silos from the acquisitions, it was challenging to gain actionable insights into the activity in their networks. The security team recognized the constraints of its existing solution to scale and, coupled with the growing costs of operations, started a search to find a new solution that could provide contextual data insights, improve visibility into potential security events, and scale as they acquired additional companies.

During their assessment of new solutions, their main requirements included having their new SIEM integrate with Snowflake, offer predictable pricing, and leverage more cloud data. In addition, migrating to a multi-cloud security analytics platform was an added benefit.

Key Challenges

- Legacy SIEM issues included a lack of reporting, difficulty to use in an evolving hybrid environment, and lack of advanced analytics
- Data silos and quality issues for security were increasing
- As the company grew and increased acquisitions, the legacy SIEM was unable to scale to meet their business needs
- Rising cost as the data volume continued to grow



The Solution: Securonix + Snowflake

The global infrastructure technology company worked with their modern data cloud partner, Snowflake, to find a security partner to help overcome their challenges. Snowflake brought in Securonix and their joint solution. The unique Securonix + Snowflake deployment model is designed specifically for multi-cloud organizations that are looking for best-of-breed analytics with the ability to store long-term data in Snowflake. This joint solution extends Securonix NextGen SIEM seamlessly in a customer's Snowflake cloud environment to simplify cost and allow customers to own their data.

The Securonix + Snowflake product removes data silos and complexity because data is stored in a customer's Snowflake environment while allowing for faster detection and response to potential security events. Securonix is a unified security operations and analytics platform providing NextGen SIEM, UEBA, and SOAR capabilities as a cloud solution with unlimited scalability. By providing updated security content-as-a-service and sophisticated advanced analytics, the NextGen SIEM drives down false positives and scales for very large and complex organizations.

The Business Impact: Analytics-driven, Scalable Cloud Security

The company chose the Securonix NextGen SIEM to meet its security analytics needs which included having immediate access to its vast stores of data. As the company continues to grow and add more data, they needed a cloud-native security platform that could be flexible and scale as their operational needs increase. The team saw the immediate benefits of keeping all their data in one place by bringing their Snowflake instance and leveraging Securonix NextGen SIEM to detect and respond to security threats.

Securonix + Snowflake met the company's current and future security goals. With an optimized cost model and the ability to access data on demand, Securonix + Snowflake offer multi-cloud flexibility and industry-leading security. Customers achieve complete security visibility, actionable insights, security metrics, and better automation with significant cost savings.

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