snowflake®

CUSTOMER CASE STUDY

FIGMA BUILDS A SCALABLE SECURITY OPERATIONS PROGRAM WITH SNOWFLAKE

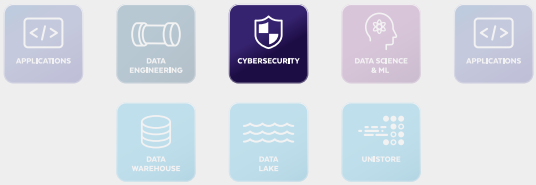
TECHNOLOGY & DESIGN

Figma

COMPANY Figma

LOCATION San Francisco, California

SNOWFLAKE WORKLOADS USED



Figma is a cloud-based design platform that helps teams brainstorm, design, and build better products together — from start to finish.

STORY HIGHLIGHTS:

Enabling fearless logging

Using Snowflake as a security data lake enabled the Figma team to store and analyze years of security data without worrying about the cost and retention limits. The team is able to leverage high-volume data sets such as Okta System Logs and AWS CloudTrail logs for better enrichment and higher-fidelity alerts.

Achieving faster time to value with connected applications

Figma's security engineers prefer utilizing Snowflake-connected applications such as Panther to run on top of their security data lake instead of building and maintaining custom applications. With Panther as a search engine, Figma can write custom detections using SQL and Python to analyze data and correlate events across all of Figma's security data.

Unlocking data science expertise

Security and data teams have historically worked in silos. With a modern security architecture, Figma enjoys working within the same data platform as the rest of the company. Security teams can benefit from data science expertise for customized data visualizations to drive prioritization and focus.

> **"Snowflake's ecosystem of modern security tools and programming languages enables us to do really novel, creative investigations that were previously impossible."**
>
> **—DEVDATTA AKHAWE,** Head of Security, Figma

CHALLENGE:

Keeping pace with exponential growth in data volumes and attack surfaces

Figma's success has been fueled by multiple factors, including its commitment to data security and protecting the organization from cyber threats. "Figma aims to be the core tool for many designers, thinkers, and project managers, and so people need to trust us to keep their data safe and available," Figma's Staff Security Engineer, Max Burkhardt, said.

Sustained growth at Figma led to the rapid expansion of customers, users, employees, and security data. Security teams need proper context from a variety of security logs and business contextual data to obtain high-fidelity alerts and effectively investigate security events. However, security data is often fragmented, with data coming from identity platforms, cloud providers, SaaS applications, and more.

Additionally, the costs of ingesting and retaining data in traditional security information event management (SIEM) solutions across the industry force security teams to silo security data in cold storage. This siloed data architecture ultimately limits the visibility a security analyst should have. And as a result, adversaries are often identified months to a year after they have already infiltrated the organization's systems.

While fragmented logs and disjointed data lakes make it hard for teams to combine data and collaborate, for Figma's Head of Security, Devdatta Akhawe, staying ahead of security risks required a single, unified view of data. "Teams need to be able to use security tools at scale and quickly respond to security incidents," Akhawe said.

SOLUTION:

Building a modern security data program

Seeking to build a modern security data program, the security team discovered their data science teams at Figma had already been using Snowflake. By connecting Panther, a cloud-native SIEM tool, with Snowflake as their security data lake, Figma can store high-volume data sets from multiple sources and easily query the data for further automated detections and alerts.

Snowflake empowers the security team's philosophy of "fearless logging." According to Akhawe, "Most legacy security tools would not be able to handle the growth we experienced in a way that scales reliably. Snowflake as the core of our security data program allows us to ingest all the disparate logs without worrying about scale or cost."

The key ingredients for a modern security data program include a scalable architecture to consolidate security data and an ecosystem of best-of-breed security applications to run on top of that data. Snowflake provides an all-in-one solution to help security teams focus on what really matters.

> **"By unifying our security data in Snowflake, we've achieved faster investigations, a lower false positive rate for alerts, and greater confidence in our ability to respond to security incidents."**
>
> **—MAX BURKHARDT,** Staff Security Engineer, Figma

RESULTS:

Faster investigations with greater confidence

Snowflake as the central repository of Figma's security data enables automation. "Our team's approach to security is to build automated workflows and tools that allow us to solve security problems a lot more effectively. Instead of combing through endless alerts, we build automated workflows and efficient pipelines and, at the core, Snowflake supports all of that," Burkhardt said.

For example, if an employee logs in to Figma's internal systems from an unusual IP address, previously that might have been a tedious, manual investigation that involves correlating employee information with security logs. Now, with business data, contextual data, and security data all in one place within Snowflake, security engineers at Figma can write a simple query to combine HR employee data with endpoint and login data to determine whether or not this is a malicious attack or an employee authenticating from a new place. A simple query within Snowflake can make event correlations easily and quickly, helping remove false positive alerts.

Greater collaboration with the data team

"Snowflake allows us to take advantage of standard industrywide tools like SQL and Python," Akhawe said. "Many security tools can be really troublesome because there is only a small niche of security practitioners who are using it globally." Instead, Figma's security engineers and data scientists can take advantage of the ecosystem of advanced BI tools and create data visualizations that keep security analysts informed about the security posture of the organization.

With Snowflake, the security team collaborates closely with other teams across Figma. "Being able to use the same tools they use, the same languages they use, allows us to collaborate more effectively. What's more, the engineers and data scientists can be effective from day one as we are leveraging a common skill set," Akhawe said.

> **"Snowflake Data Cloud enables us to build a unique security program because we're able to leverage the whole world of data science tools and expertise for our security investigations."**
>
> **—MAX BURKHARDT,** Staff Security Engineer, Figma

FUTURE:

Maximizing the impact of security data

As Figma's security team grows, the team can focus on mission-critical alerts rather than on false positives. They are also more efficient with their time by implementing automated workflows and out-of-the-box detections from partner solutions such as Panther. According to Akhawe, "With Snowflake, we're able to focus on creative problem-solving with the business and the unique value security can bring to the table."

Supporting additional users, data, and workloads with Snowflake will accelerate Figma's ability to enhance its security program and, ultimately, maintain high levels of trust with customers. According to Akhawe, "As we foster deeper collaboration across Figma, we welcome talent and input across different backgrounds. I'm excited for Snowflake to help enable that and drive a more robust security program at Figma."