snowflake®

CUSTOMER CASE STUDY

FORBES 1000 MEDIA COMPANY TRACKS ACTIONABLE SECURITY METRICS USING SNOWFLAKE SECURITY DATA LAKE

SECURITY

Forbes 1000
MEDIA COMPANY

COMPANY Forbes 1000 Media Company
LOCATION Global

SNOWFLAKE WORKLOADS USED

Ranked within the Forbes Global 1000, this media company provides news and information-based tools to help professionals answer complex questions about law, tax, compliance, government, and media. To improve visibility, reduce cyber risk, and ensure compliance with security policies, it transforms large amounts of machine data into cybersecurity key performance indicators (KPIs) for leadership, infrastructure, and application teams.

STORY HIGHLIGHTS:

Data-driven decision making
All relevant log, scan, inventory, and configuration data is centralized in a security data lake enabling the CISO to base decisions on quantitative metrics.

Single source of truth to validate
Each team involved with audits, infrastructure configurations, and application development can access security compliance reports, knowing which priority issues to address.

Reduced security risk with automation
With analytics that accurately identify risks such as cloud misconfigurations or invalid user permissions, automation tools enable immediate action.

CHALLENGE:

Getting timely insights from an outdated system
Every security program has several security policies designed to reduce the likelihood and impact of a security breach. However, security leaders struggle to apply these security policies to the real world. And although policies may set clear expectations, applying them across large and fast-changing environments is hard.

This media company had siloed data housed in multiple security and compliance platforms prevented the CSO and other C-level executives from quantitatively measuring key risk indicators (KRIs). Compliance analysts often had to sample systems and users to identify policy violations before external audits, with results determined manually in spreadsheet tools or written reports.

This approach had questionable reliability and didn't scale well, with insights being delayed by weeks or months. As a result, security leadership often had to make strategic decisions without the benefit of data, while weaknesses in the security program remained undiscovered until a breach occurred.

To address these security challenges, the media company initiated a security program, built upon a security data lake, that would define, analyze, and reduce cyber risk. However, its previous data platform could not support the semi-structured security data. In addition, compute and storage were not separated, leading to additional administration and data storage expenses.

SOLUTION:

Snowflake's single source of truth
The media company turned to Snowflake on AWS as its single source of truth. Snowflake's easy-to-navigate interface, native SQL support, and in-depth documentation enabled the team to consolidate POC testing into one week and begin ingesting data to identify security gaps, detect vulnerabilities, and report findings as security metrics.

Snowflake's extensive network of connectors, drivers, programming languages, and utilities enabled the team to build a nimble data pipeline that automatically loaded JSON and other data types from Amazon S3. Snowflake Tasks and Streams simplified data capture and enabled the team to aggregate and enrich raw security data for actionable insights. Snowflake's fully-managed platform scaled to become the media conglmerate's security data lake.

> **"Everything that you need for a modern security data platform resides within Snowflake."**
>
> **—DIRECTOR OF SOFTWARE ENGINEERING,**
> Forbes Global 1000 Media Company

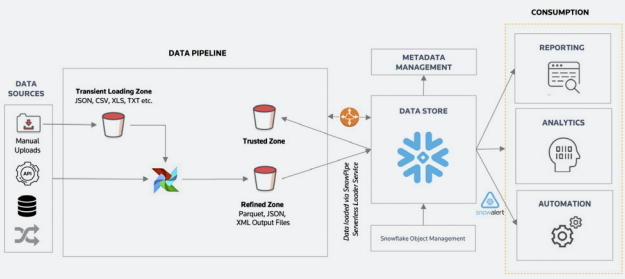

Figure 1: Snowflake supports multiple use cases for the media company's security program.

Snowflake supports data management and maintains data quality and integrity while the security organization constantly collects new data sources. Centralized role-based access control enables the media company to granularly manage data access.

RESULTS:

Increased security insights and reduced risk

By architecting the **security data lake** on Snowflake Data Cloud, the media company security organization can rapidly develop self-service reports to inform executives about security and compliance trends across the business. The CISO relies on data from Snowflake to focus on strategy and drive change with confidence.

"For example, Snowflake powers dashboards that display key risk indicators and trends in real time. If there is data pointing towards upwards risk for cloud compliance, the CISO can immediately issue a new policy to mitigate it. And by the end of the day, the CISO should be able to see the risk trend decrease."

Security remediation results are collected back into Snowflake, giving the media company a single dashboard that shows a holistic picture of its security findings, priority issues, and latest status.

> **"Our CISO recently expressed his amazement at all of the data-driven insights that we've surfaced in such a short period of time with the Snowflake Data Cloud, which is a big deal for our team."**
>
> **—DIRECTOR OF SOFTWARE ENGINEERING,**
> Forbes Global 1000 Media Company

Data-driven security across all teams

The media company's security program enables teams across the company, including DevOps and IT, to leverage Snowflake as the source of truth for identifying risk-reducing activities.

In comparison to traditional organizations that only allow security teams access to operational dashboards, all teams can access security data that's relevant to their work. "With Snowflake, teams can use their BI tool of choice to see if they're in compliance", said the director of software engineering.

Near real-time data in Snowflake eliminates the need to log into servers and check maintenance schedules. Enriched security data helps IT and developers prioritize security patches across thousands of servers, simplifying audit reports and streaming remediation results to the security team and CISO in near real time.

High-fidelity findings enable security automation

Combining accurate analytics about security events, infrastructure, and users in Snowflake creates automated insights that power tools across the remediation and reporting process.

Creating alerts with the open source SnowAlert project allows the media company to use data in Snowflake to proactively detect anomalies and reduce risk. "Having alerts was only part of the equation," said the director of software engineering. "It's only as effective as the quality of the data." Accurate and reliable data through Snowflake, paired with SnowAlert and other security automation tools, enabled the lean security team to build a powerful security program that scales.

FUTURE:

Snowflake Data Sharing to accelerate data availability

Enabling real-time data ingestion is a top priority for this Forbes Global 1000 media company. According to the director of software engineering, "We currently rely on timely data feeds, but our goal is to ingest data into Snowflake as close to real time as possible."

Snowflake Secure Data Sharing represents another opportunity to accelerate data availability. "My vision is to connect Snowflake to all of my data shares, and the data just shows up without worrying about data pipelines," the director of software engineering said.