snowflake®

CUSTOMER CASE STUDY

NETGEAR REPLACES ON-PREMISES SIEM WITH SNOWFLAKE AND XDR PLATFORM TO ACCELERATE CLOUD STRATEGY

TECHNOLOGY

NETGEAR

COMPANY	Netgear
LOCATION	San Jose, California

DATA SHARING · DATA SCIENCE · DATA APPLICATIONS · CYBERSECURITY · DATA WAREHOUSE · DATA LAKE · DATA ENGINEERING

Netgear is an American computer networking company based in San Jose, California, with offices in about 25 other countries. Netgear builds networking equipment to connect people and power businesses. Its products are widely used by consumers, businesses, and service providers.

STORY HIGHLIGHTS:

Supported cloud-first security strategy
Netgear's on-premises security stack could not support its cloud-first initiative. Snowflake was able to keep Netgear's business running without any security impact during its digital transformation journey.

Increased visibility and context
Near-unlimited data ingestion and retention of large, complex data sets in Snowflake enables Netgear to utilize data sets that it couldn't leverage previously to provide context in investigations.

Reduced noisy alerts and otherwise manual investigations
With access to data and context in Snowflake, Netgear's chosen Security Operations platform reduced the number of noisy alerts. Typically, these alerts would need to be manually investigated by analysts.

> **“We wanted to focus more on detection and response rather than just managing the tool itself.”**
>
> **—PALLAVI DAMLE,** Vice President of Enterprise Cybersecurity, Netgear

CHALLENGE:

Netgear had an established SOC team and a security information and event management (SIEM) solution for several years. Its previous SIEM worked for the company until it decided to implement a cloud-first strategy. With remote work on the rise and Netgear's massive growth, the security team knew they needed to move away from reactive security practices to more proactive and predictive approaches to security.

During the transition to the cloud, the security team experienced many challenges. They struggled to ingest cloud logs and other large, complex data sets into their prior SIEM. As a result, a lack of correlation and context led to an abundance of noisy alerts and false positives. SOC analysts were manually investigating noisy alerts that resulted in analyst fatigue. These challenges could lead to missed high-priority alerts and hamper incident response.

As Netgear's operations grew, the security team wanted to retain more data for extended periods. According to Pallavi Damle, Netgear's Vice President of Enterprise Cybersecurity, “While 90 days' retention was acceptable in the past, SOC requirements have evolved along with security threats, and it was important for Netgear to retain more data and for a longer duration to aid forensic analysis.”

Damle needed a new solution to remove the data management overhead that forced her team to pick and choose security data sets to ingest. She wanted access to all of the security data available for context and correlation. And she needed a solution that was easy to manage with out-of-the-box security capabilities. These requirements will enable her team to focus on adding more business value through threat detection and response, rather than manual work such as collecting data, investigating noisy alerts, or fine-tuning correlations searches.

SOLUTION:

Mobilizing all security data for investigations
Netgear was impressed by Snowflake's ability to help its team centralize and mobilize all of its security data across both on-premises and cloud environments for investigations. Using Snowflake as its security data lake, Netgear no longer faces budget constraints limiting data ingestion and retention.

Now, the company can utilize all of its traditional security logs with contextual data sets for threat detection and response. This enables the Netgear team to eliminate data silos for better visibility. Executives can receive security reports and SOC analysts have access to write queries.

> **“With access to all of the data sources in Snowflake as our security data lake, we have better correlations across multiple attack surfaces and analytics are automatically actionable. And as a result, it has led to faster incidence response from our side.”**
>
> **—PALLAVI DAMLE,** Vice President of Enterprise Cybersecurity, Netgear

RESULTS:

Leveraging automated detection and response capabilities on top of a security data lake
With Snowflake as its security data lake, Netgear was able to mobilize all its security data and logs for investigations. However, the team also needed off-the-shelf security capabilities, content, and workflows instead of building custom API integrations, detection searches, or event timelines.

The XDR Platform that Netgear leverages in conjunction with Snowflake for easy data access provided the user interface and the functionalities needed to get started right away. It helped Netgear's security team overcome their challenges with alert volume and false positives, apply threat hunting on historical data, triage alerts dynamically, and correlate security events for automatic investigations.

The key results of Snowflake and Netgear's XDR Platform include:

- **Greater incident clarity—**The ability to centralize data center logs with cloud logs and other business data was important for Netgear. This allowed the team to gain full visibility and dig into historical data across environments for forensic investigations.
- **Faster incident response—**More data means more context. Analysts were able to save time from manually gathering evidence across different sources to piece together an attack timeline.
- **Reduced manual processes—**No more manual data preparation, ingestion, parsing, and normalization. The team also does not need to manage different types of data on different platforms, causing data silos for cold, warm, and hot storage.

> **“Snowflake brings a lot of value to security space with its plug-and-play model. They have many native integrations with leading security solutions that allow us to build a more robust security program based on the tools that fit our needs.”**
>
> **—PALLAVI DAMLE,** Vice President of Enterprise Cybersecurity, Netgear

FUTURE:

Damle and her team want to do more advanced analytics across various data sources captured for effective cyber risk management. The goal is to create a cyber fusion center that integrates several different components of cybersecurity operations into one and provides complete visibility via real-time dashboards and KPI metrics. According to Damle, “All security leaders want to know how their security programs are performing at any point of time. For example, visualize the threat landscape, view real-time alerts with severity, get visibility into time taken for threat response, open vulnerabilities across the infrastructure, SLA's for remediation, trends, and much more. Our responsibility is to enable that effort to become more predictive, reducing manual effort across platforms and automating where we can. We look forward to continuing to send more data to Snowflake and building dashboards to increase our security program capabilities.”

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. Join Snowflake customers, partners, and data providers already taking their businesses to new frontiers in the Data Cloud. **snowflake.com**