snowflake®

CUSTOMER CASE STUDY

CYBERSECURITY AT COMCAST INTEGRATES SNOWFLAKE INTO SECURITY DATA FABRIC

MEDIA

COMCAST TECHNOLOGY SOLUTIONS

COMPANY Comcast Technology Solutions

LOCATION Philadelphia, PA

SNOWFLAKE WORKLOADS USED

Comcast Technology Solutions (CTS), a division of one of the world's leading media and technology companies, brings Comcast Corporation's proven technologies to an evolving list of industries worldwide. CTS believes in continuous innovation, always looking for new and better ways to connect with their customers, and aggregate, distribute, and secure their own content, advertising, and data. They invest in and test these solutions — freeing customers up to focus on their business, not their tech stack. CTS brings these innovations to the global marketplace, enabling their partners to think big, go beyond, and lead the way in media and technology.

STORY HIGHLIGHTS:

Better visibility without ingest-based pricing
With Snowflake's virtually limitless low-cost storage, Comcast can collect security data at cloud scale.

Powerful analytics for hunting at petabyte scale
Snowflake's queries execute quickly on Comcast's largest data sources for advanced detection and investigation.

Security metrics and compliance use cases
Self-service dashboards built on Snowflake allow business, compliance, and audit teams to work on shared security data sets.

CHALLENGE:

Security tools are unable to elastically scale and meet enterprise needs
Standard cybersecurity analysis tools failed to accommodate the needs of Comcast cybersecurity teams, one of the reasons was that they could not elastically scale. In the past, Comcast threat hunters had to rely on multiple security analytics tools. According to Amish Amin, Executive Director of Security Development and Analytics at Comcast, "There are numerous tools available in the cybersecurity industry, each of them fulfilling a specific purpose. The challenge is that most of these tools work within their own ecosystems, creating data silos." For example, compliance teams need access to security data, as do other teams such as threat hunting and cybersecurity data science. Many functions work best if they rely on common systems of record and sources of truth for cybersecurity data.

Comcast set out to address this need by building a modern, cloud-native security data fabric. Amin said, "Today, it's not only threat hunters and SOC analysts that use security data, audit functions and others do as well. We needed a foundational security data lake, built in the cloud, to evolve our security program."

SOLUTION:

Data-driven security at scale with Snowflake
Snowflake's security data lake is an integral component of Comcast's security data fabric. Instead of employees managing on-premises infrastructure, the Comcast security data lake built on Snowflake's elastic engine in the cloud stores over 10 PBs of data with hot retention for over a year. "The ability to push this level of detail into one system and quickly query against it has really changed the way we do security," said Amin.

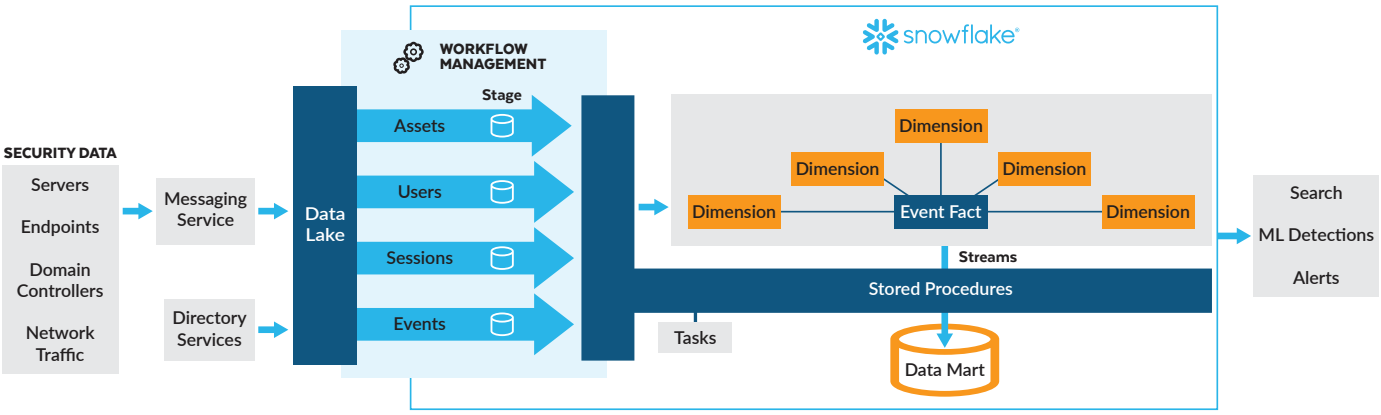

Figure 1: Comcast's reference architecture for their security program

Across a large organization like Comcast, a strong security program needs to support multiple stakeholders—from executives, to security analysts, to data scientists, to compliance teams. Multiple parties need to be empowered from the same data fabric. As a strategic partner, Snowflake is helping Comcast meet its needs. Data scientists supporting the threat detection team can now easily build a machine learning model using time-series analytics in the security data fabric. Compliance teams can support continuous controls assurance. Threat hunters can conduct deep searches. And executives can understand the cyber risk posture of their business units.

RESULTS:

Robust inhouse threat hunting

By incorporating Snowflake's elastic and cloud-native engine into their security data fabric, Comcast's security program has been able to extend threat hunts to large-scale data sets, returning more actionable results while reducing false positive findings. "For threat hunting and running analysis, the result of the query is only as good as the data available. Our security team has built a security data fabric incorporating Snowflake that enables them to join and combine data sets, clean them, and deposit them into a single, common schema within Snowflake. And as a result, analysis can be done in a way that yields much cleaner results," said Nicole Bucala, VP and General Manager of the Cybersecurity Suite at Comcast.

For Comcast's threat hunters and SOC analysts, the Comcast security data fabric enables access to a full year's worth of history.

Compliance insights across business units

In the past, business units often lacked visibility into their compliance posture and had to rely on compliance teams. The data they had access to was often stale, creating a negative feedback loop of delayed action and compliance gaps. This would in turn lead to negative audit results—creating a lot of unnecessary noise in the system. To address this, the Comcast team has built dashboards on top of the security data fabric to monitor controls assurance, as well as key performance indicators and key risk indicators. Business units now have near real-time visibility into their compliance and risk posture and can be much more proactive. For example, one business unit saw a gap in their endpoint detection and response coverage, and within three days increased their coverage to 95%—all without prompting from other oversight groups. With these self-service dashboards, Comcast is building a culture of proactive security compliance.

Search performance in Snowflake also improved compliance with threat intelligence findings. Automated sweeps of over 50,000 indicators of compromise (IOCs) across the 10-petabyte security data lake can now be completed in under 30 minutes.

FUTURE:

Continuing to leverage new Snowflake features and functions

New use cases that are able take advantage of the capabilities provided by a robust security data fabric continue to emerge at Comcast. Comcast cybersecurity teams will continue to support these new use cases and will look to the strategic partnership with Snowflake to take advantage of new features and functions available from Snowflake.