DataBee COMCAST TECHNOLOGY SOLUTIONS | snowflake®

Unlock the power of a security data fabric

Partner brief

Modern enterprise environments and cybersecurity tools generate data at an exponential speed and volume, yet available security data remains largely inaccessible and underutilized for analysis and decision-making. This is compounded by changing data privacy regulations and mandates, leading data owners to grapple with the dual challenge of maintaining governance over their data and meeting retention requirements.

Existing logging and security monitoring tools like SIEMs leave even the organizations with the most mature cybersecurity data programs with siloed views — and exorbitant ingestion costs — while requiring extensive data engineering and manipulation before value and insights can be derived. Passing data from one security tool to another reduces downstream data's accuracy and quality, leading to inconsistent analytics and undermining efforts for cross-functional collaboration.

Stitching together insights with DataBee™, a security, risk, and compliance data fabric platform

By shifting transformation to the data life cycle's early stages, you gain control of all data relevant to security and compliance initiatives while ensuring sharable real-time insights for the entire organization. The DataBee Hive™ weaves together disparate security and IT data from across your technology stack into a security data fabric where it is enhanced with business intelligence and logic. With this enriched data, you can use best-of-breed business intelligence and data analytics tools for analyses, monitoring, and reporting, then send it to Snowflake for cost-effective, near-unlimited storage.

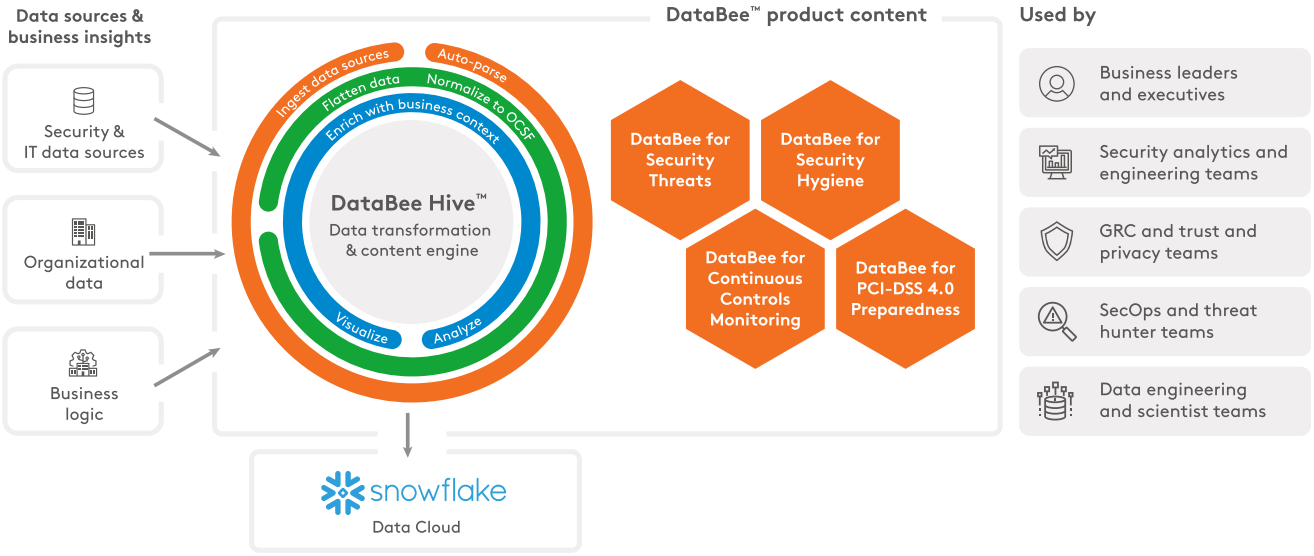
Separating storage and compute significantly drives down costs while simultaneously ensuring high performance and robust analytics. When used together, DataBee™ from Comcast Technology Solutions and Snowflake give your business the near-limitless, cost-optimized capacity to store cleaned and integrated security telemetry for extensive retention periods while benefiting from Snowflake's scale for swift correlation and search capabilities.

As a connected Snowflake application, DataBee provides you with the flexibility and connected intelligence of a data fabric while using Snowflake as your security data lake. Now your security data is correlated with your business data for a single source of truth while remaining under your data ownership and control. The same cleaned data is exportable to security operations or business intelligence (BI) and visualization tools for enhanced analytics and reporting.

Better together: Benefits of DataBee and Snowflake

Integrated data management

DataBee transforms and standardizes data to a DataBee-extended Open Cybersecurity Schema Framework (OCSF), so you can correlate traditionally difficult-to-merge data as a single standardized dataset. With early and constant engagement in the data pipeline process, DataBee parses, flattens, and normalizes data that sources and feeds generate as they are being created before sending to Snowflake for storage and querying. Dashboards and metrics from DataBee can be configured to connect directly to Snowflake, and users can combine a variety of datasets from the Snowflake Marketplace with security data from DataBee to derive additional insights.



Continuous controls monitoring (CCM)

DataBee ensures that data consumers have access to the same available, usable, and quality data as executives. Your governance, risk, and compliance (GRC) team can implement and monitor data-centric risk measurement and security controls, delivering consistent, accurate, near-real-time compliance dashboards by coupling controls data and user activity with business context. For holistic visibility into system and network activity, you can use DataBee's patented technology that creates a single static entity ID for every user and device connected to your environment, helping quickly validate endpoint detection and response (EDR) coverage, asset management, vulnerability management, and more. Using actionable reports and metrics exported to BI tools, like Tableau or Power BI, GRC leaders and analysts save time on audit preparedness and provide fast answers and resolutions to compliance questions.

Data-centric threat hunting

DataBee speeds up threat detection and mitigates risks with automated, concurrent threat hunting queries. When integrated with Snowflake, DataBee can perform investigations without needing to plan for outward scaling by performing queries on cluster compute. Since DataBee creates a unified view after aggregating and correlating data, threat hunters can automate traditionally time-consuming manual processes using signals from disparate tools, helping them trace threats faster while reducing the number of pivots between screens. Analysts will find enhanced capabilities when connecting their favorite tools, like Jupyter Notebooks, directly to Snowflake and using the enhanced data for queries and analysis.

Together, DataBee and Snowflake provide a robust and powerful security data fabric for organizations looking to augment their data management process, ensure continuous controls monitoring, and leverage accurate, consistent analytics for threat hunting.

Find out more

Are you ready to take advantage of an enterprise-scale data fabric? Let's talk.
CTS-Cyber@comcast.com | comca.st/databee

DataBee | COMCAST TECHNOLOGY SOLUTIONS