DataBee
COMCAST TECHNOLOGY SOLUTIONS

Product Data Sheet

DataBee™ from Comcast Technology Solutions

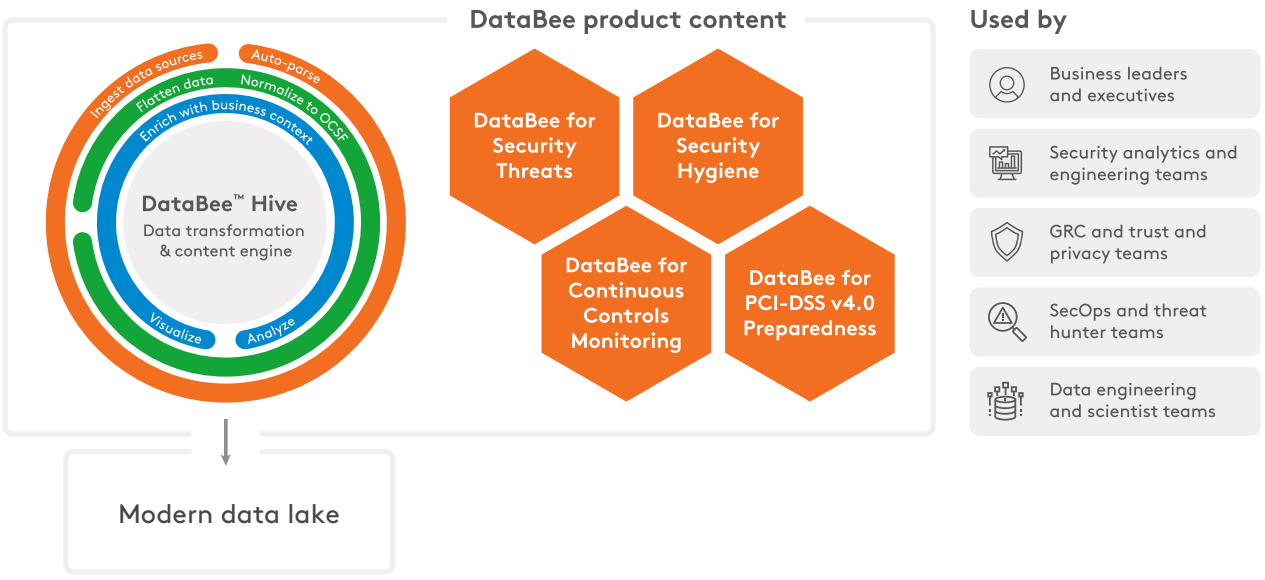
Get more from your security data with a security, risk, and compliance data fabric

Data-driven decisions are critical to driving every part of the business forward. Yet data silos persist that require costly and time-intensive data manipulation. As a result, inconsistent reporting and inaccurate insights cause poor communication between leaders and analysts — regardless of how much data is available to analyze.

Effective decision-making, rapid incident response, and real-time compliance reports and audit preparations need high-quality, complete data. Additionally, evolving data governance and privacy requirements are driving organizations to find modern, cost-effective methods for compliant and accessible data retention.

Introducing DataBee

DataBee™ creates connected security and compliance data and insights that can work for everyone. Inspired by a Fortune 20-scale internal data fabric implementation that resulted in significant cost savings and operational gains, DataBee, led by senior cybersecurity industry leaders, brings to market a commercially available security, risk, and compliance data fabric platform. Now, customers can unlock actionable and contextualized security insights with a unified source of truth for security analysis and reporting functions at scale.



Turning data into honey with the DataBee Hive

DataBee is engineered with an open architecture to help you avoid vendor lock-in with customizations targeted toward your unique and diverse use cases and self-generated reports and analytics. By streamlining access, enhancing data integrity, and preventing duplication in the data pipeline, DataBee delivers more complete and accurate data, whatever your use cases may be.

Data transformation engine

DataBee focuses on collecting and processing your data in a streamlined and low-cost way. Data from your security and IT logs and feeds, including non-traditional telemetry such as organizational hierarchy, is ingested via Application Programming Interfaces (APIs), on-premises log forwarders, AWS S3, or Azure Blob. This means less manual effort on your part to organize data to make it useful to your analysts. Data is automatically parsed and mapped to a DataBee-extended version of the Open Cybersecurity Schema Framework (OCSF) using a proprietary technology. Data source feed health can be monitored directly in the user interface.

The platform then enriches the dataset with your business policy context and applies patent-pending entity resolution technology to produce a unified, time-series dataset that is stored long term and cost-effectively in a modern data lake of your choice. The data transformation process breaks down data silos and technical barriers, giving analysts and data engineers faster and more valuable insights without manually organizing or manipulating data.

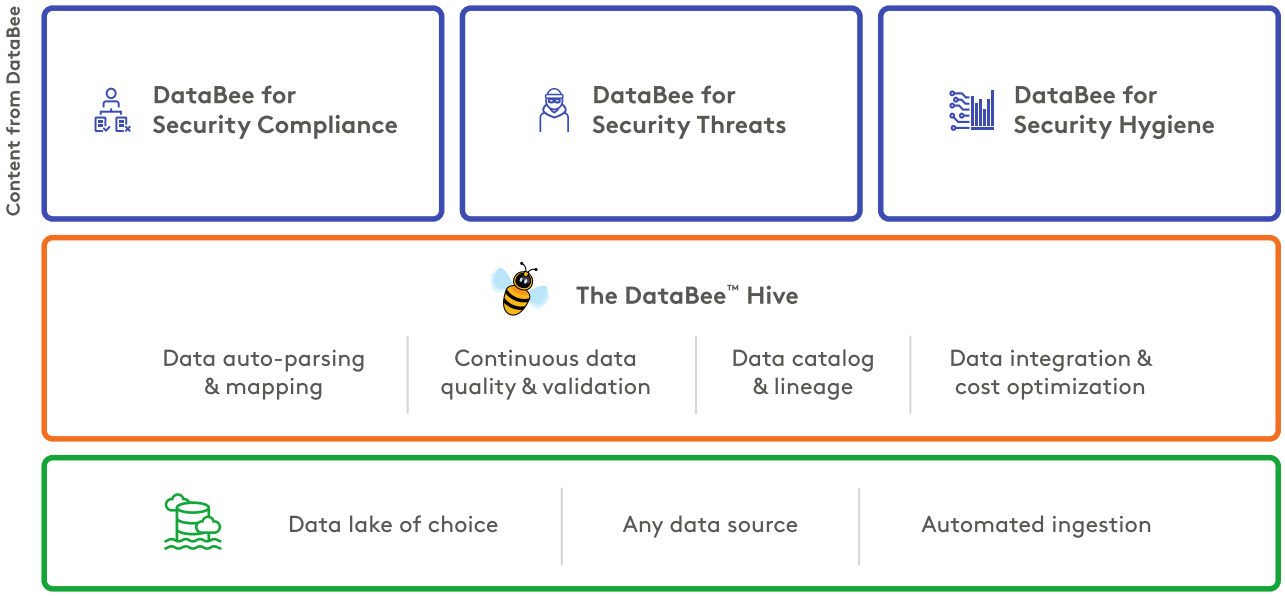
Content and use cases

Once data is joined and enriched, your business can start using enterprise-ready content provided by DataBee to report on insights for key initiatives.

Executives can make well-informed business decisions even with less manual work for data engineering and data science teams. They can also gain back control of data ownership and prevent runaway data ingestion and storage costs. Security teams will have a more complete view of user activity with higher fidelity alerts when responding to incidents. Threat hunters can conduct multiple investigative queries when searching for insider threats or stealthy attackers on the network. Governance, risk management, and compliance (GRC) can validate levels of privacy policy compliance. They can also provide security controls compliance evidence, while staying ahead of internal and external audits using data they can trust.

The benefits of the DataBee Hive

DataBee can be customized based on your business needs. The DataBee Hive is the core security, risk, and compliance data fabric platform that transforms your data and primes it for your data lake. Maximize your data by adding on DataBee use case content across security compliance, security threats, and security hygiene.



Mature your security data as you retain and optimize costs with the DataBee Hive

- Prepare data for advanced analytics and reporting without manual data manipulation.
- Process and analyze data in memory with DataBee, refining ownership and classification with the data producer of each system.
- Achieve business-focused security by weaving asset owner information and security logs with IT data, business policies, and organizational hierarchy details.
- Gain end-to-end visibility into data consumption and data source health.
- Accelerate AI initiatives and operations using cleaner, optimized data.
- Apply optional machine learning customized to your organization's patterns and relationships for enhanced predictive analytics and data modeling.

Mitigate risks, improve compliance, and better protect the business with DataBee for Security Compliance

- Create business leader accountability with dynamic, auditable reports and metrics.
- Verify data ingestion to ensure data quality and integrity for compliance audits.
- See trending metrics and self-defined KPI values for continuous security and controls reporting.
- Proactively manage risks and compliance gaps, including noncompliant users, devices, and services.
- Be more prepared for compliance audits or security assessments such as PCI-DSS v4.0.
- Get faster answers and limitless flexibility working with DataBee logic and reporting delivered in tools that analysts everywhere know and love, such as Tableau and Power BI.

Optimize your security analytics tech stack and operations with DataBee for Security Threats

- Reduce security information and event management (SIEM) spend by diverting high-volume and underutilized logs to the DataBee transformation engine and into your modern data lake.
- Decouple storage and compute from your SIEM, enhancing your indexing experience, improving your query results, and reducing costs.
- Create an accessible, time-series user dataset using patent-pending entity resolution technology for insider threat monitoring.
- Conduct multiple threat hunting queries simultaneously without planning for outward scaling.
- Apply active detection streams using sigma rules to detect anomalies and indicators of compromise (IoCs) in datasets as they stream to their destinations.
- Cleaner data results in enhanced SIEM and security orchestration, automation, and response (SOAR) workflows with high-fidelity alerts and threat signals.

Discover relationships between data across dispersed environments with DataBee for Security Hygiene

- Progress your security data estate to be more complete, answering the "who, what, where, and when" questions about assets and their owners using patent-pending entity resolution technology.
- Augment your configuration management database (CMDB) or alternative asset inventory source by enriching it with directory services, vulnerability scanner, and other information.
- Identify unknown or orphaned assets to prevent potential entry point for bad actors, insider threats, and unintentional compliance violations.

DataBee team

Led by dedicated engineering, product & sales leaders from leading SaaS companies

Customer profile

US Fortune 1000 & large, regulated industries

Partner ecosystem

EY | Guidepoint | Databricks | Snowflake | Accenture | AWS

DataBee | COMCAST TECHNOLOGY SOLUTIONS