DataBee™ | COMCAST TECHNOLOGY SOLUTIONS

Solution Brief

Continuous controls monitoring (CCM) from DataBee™

As more corporations become digital first and the threat landscape continues to expand, executives and business leaders are leaning in and placing more importance on cybersecurity programs. Despite the need for communication and collaboration, security and risk management teams face challenges arising from disconnected, disparate security data sources, culminating in ineffective cybersecurity measurements that fail to deliver the insights business leaders need to make informed decisions.

When auditors request documentation, teams struggle with time-intensive manual collection and analysis processes as they gather data from so many disparate security controls. Just as their data is fractured across disparate security tools, geographic regions, and schemas, their collaboration is fractured, making it difficult to identify the process owners or operational managers responsible for compliance. This disconnection between people and data creates confusion and delays remediation activities. The point-in-time nature of these audits means that the limited controls tested can fall out of compliance, leaving organizations with no visibility into their current state.

Instead of collaborating across operational managers, risk management, and internal audit functions for a proactive compliance and audit process, security teams are in perpetual "reactive" mode and disconnected from business operations. A consistent dataset that creates trust and operational efficiencies could be a game changer.

Introducing the DataBee™ Platform for continuous controls monitoring

DataBee provides core continuous controls monitoring (CCM) capabilities, delivering consistent and accurate compliance dashboards and reports for data-centric risk measurement and security controls effectiveness measurements. DataBee automatically identifies and connects data so governance, risk, and compliance (GRC) leaders and analysts can assess compliance controls, save time on audit preparedness, and achieve fast compliance answers and resolutions.

By weaving and enriching multiple data sources into security data fabric, DataBee enables operational managers, risk management, and internal audit functions to collaborate and report on the same contextualized insights derived from data they trust. DataBee normalizes and maps security data to the Open Cybersecurity Schema Framework (OCSF) schema using patented entity correlation logic and asset owner discovery tools. The enriched dataset is sent to your data lake of choice where it can be easily tapped for insights and enabled for data sharing.

By putting data at the center of your CCM program using DataBee, you can create a culture of compliance accountability with robust and data-driven actionable reports based on management structure, reducing confusion about who in the organization is responsible for improving compliance. Predefined dashboard views and reports focus on your business's policies and standards for quick and proactive delivery of measurable and accurate metrics.

DataBee automatically identifies and connects data empowering all three lines of defense with access to real-time, year-round, proven-at-scale CCM dashboards for visibility into compliance trends and actionable insights using industry-leading visualization tools — Tableau and Power BI.

DataBee's data-centric CCM features

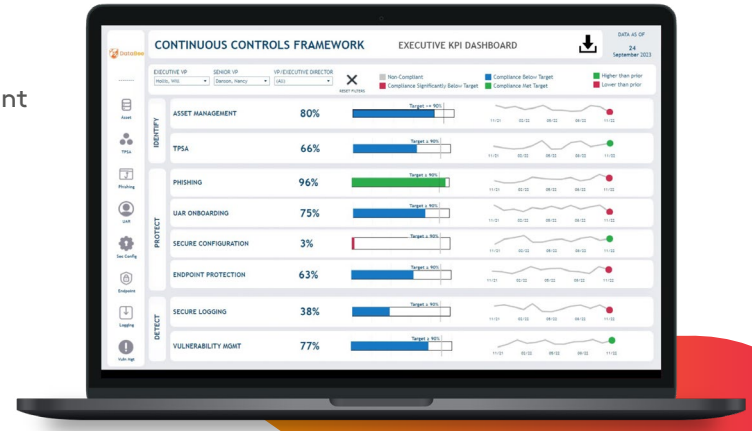
- Single pane of glass with dashboards and reports for operational managers, risk management, and internal audit functions
- Prebuilt and customizable CCM dashboards that automatically identify and connect data required to assess compliance and controls aligned to your business policies and standards
- Layered dashboards and real-time reports based on management structure enhancing communication and collaboration by identifying process owners and business managers
- Access insights year-round for real-time and historical controls and compliance trends
- Robust and actionable reporting that eliminates point-in-time compliance and spreadsheets
- Accelerate your security data maturity journey with Comcast GRC consulting services
- Enhanced communication throughout the compliance lifecycle — from defining controls objectives, to evaluating controls implementation, ensuring accountability, and monitoring controls effectiveness

Use case example:

Supporting NIST Cybersecurity Framework risk identification, compliance monitoring, and assessment

In addition to sustaining compliance programs, DataBee CCM enables organizations with compliance monitoring requirements from frameworks such as NIST 800-53, NIST 800.171, PCI 4.0, or ISO27001.

Security assessments are labor-intensive and time-consuming, especially when large amounts of data are in scope for sampling, analysis, or monitoring. DataBee can help your compliance analysts and your independent assessors with identifying risk, monitoring controls, and sustaining compliance across the Identify, Protect, and Detect pillars. Instead of spending the effort on gathering and analyzing large amounts of data for point-in-time testing, they can rely on auditable CCM dashboards and focus on the quality of the controls.



PCI DSS requirement	DataBee report
Apply secure configurations to all system components (#2)	Secure configuration
Protect all systems and networks from malicious software (#5)	Endpoint protection Vulnerability management
Develop and maintain secure systems and software (#6)	Vulnerability management
Restrict access to system components and cardholder data by business need to know (#7)	User access reviews
Identify users and authenticate access to system components (#8)	Policy exceptions
Log and monitor all access to system components and cardholder data (#10)	Security logging and monitoring, and log retention and normalization
Test security systems and networks regularly (#11)	Vulnerability management
Support information security with organizational policies and programs (#12)	Asset management Resiliency Training and phishing

Table 1: Sample of data and telemetry DataBee gathers and combines to show PCI DSS requirements

Get started with DataBee for CCM

The power of the DataBee security data fabric platform for CCM allows you to spend less time searching for the right data for controls and compliance reporting and more time on the quality and sustainability of controls and gaps remediation. Comcast has firsthand experience with implementing a CCM program at scale, and DataBee brings this experience along with proven feeds, dashboards, and visualizations to your organization. With DataBee, you will quickly be able to:

- **Proactively understand and monitor compliance posture in accordance with internal policies, regulations, and industry standards.**
- **Continuously identify control gaps and refine metrics.**
  Establish controls baselines and continuously test and measure against targets to prioritize critical remediations.
- **Create a culture of compliance accountability through data transparency and trust.**
  Automatically score and rescore your leaders and departments against controls standards, and consistently track their performance trends over time.
- **Save time on audit preparedness.**
  Provide fast compliance answers with evidence of adherence to security controls, policies, and procedures.
- **Improve security operational efficiency and save money.**
  Eliminate the need for labor-intensive manual security data mapping and maintenance efforts.
- **Provide actionable remediation insights and prescriptive resolutions to address gaps and guard against threats.**
  Instruct leaders exactly where there are gaps and recommend how to close those controls gaps.

Find out more

Are you ready to take advantage of an enterprise-scale security data fabric with continuous controls monitoring capabilities? Let's talk.
Request a custom DataBee demo | comca.st/databee

DataBee | COMCAST TECHNOLOGY SOLUTIONS