DataBee
A COMCAST COMPANY

SOLUTION BRIEF

DataBee® Continuous Controls Monitoring (CCM)

Continuous controls visibility.
Continuous confidence.

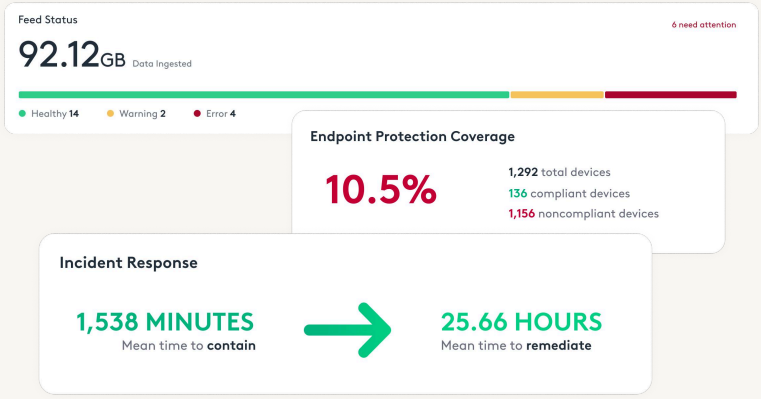
DataBee CCM provides BISOs and GRC teams with continuous controls monitoring that surfaces coverage gaps and ties them to accountable leaders and the owners of the underlying applications or devices, so control posture stays current without manual effort.

VALUE PROPOSITION

Most control validation still happens periodically, which means gaps can grow between assessments. DataBee CCM changes that. Built on the DataBee platform, CCM continuously measures control performance and provides framework cross-mapping to the standards and policies against which you report. The result is a dependable, ongoing view of control coverage and effectiveness, with every number grounded in the data behind it.

KEY OUTCOMES

- **Control performance reported with business context**, tied to the business unit, owner, and asset behind every metric.
- **Security control scores roll up** by business unit and accountable leader, with trends tracked over time for accountability.
- **Manual data gathering replaced** with continuous monitoring, freeing teams for higher-value work.
- **Coverage gaps surface continuously**, attributed to the responsible business unit, leader, and owner of the underlying device or application.



HOW IT WORKS

01 Connect

CCM runs on the DataBee platform's broad connector ecosystem, with 350+ integrations across your security, IT, and business systems. There's no separate data copy and no new ingest project to set up.

02 Measure

Controls are continuously monitored against near real-time operational data, with framework cross-mapping to NIST, CIS, PCI, custom frameworks, and more.

03 Act

When a control starts to slip, the gap shows up early, with the specific devices, users, or systems behind it. Ask follow-up questions in natural language using DataBee RiskFlow™, without leaving the platform.

KEY CAPABILITES

- **Continuous control monitoring.** Measure control effectiveness across your systems using real operational data, not periodic checklists or manual spot checks.
- **Stand behind every number.** Every control measurement is grounded in source data, so the metrics you report are the ones you can defend.
- **Detect drift and breakdowns early.** Identify changes in control effectiveness as environments evolve, before gaps require urgent attention.
- **Explainable agentic AI for cyber risk.** DataBee RiskFlow analyzes your controls data in natural language, summarizing control performance and KPIs, exploring gaps, and answering questions, with every answer explainable and grounded in the source data.
- **Ground in patent-pending entity resolution.** Measure the right number of users, devices, and applications in a unified, continuously updated view, not double-counted across tools.
- **Framework cross-mapping.** Cross-maps control results to NIST, CIS, PCI, custom frameworks, and other regulatory frameworks without duplicative effort.

WHY DATABEE

One platform, many outcomes

From control monitoring to vulnerability remediation to executive reporting, every DataBee solution runs on the same connected data foundation, so investment in the platform compounds across your program.

Works with what you already have

DataBee connects to your existing security, IT, and business systems, bringing fragmented data together without disrupting the platforms your teams rely on.

Your data, your storage, no lock-in

DataBee normalizes and processes data, then places it in your existing data lake or cloud storage, giving you a flexible, cost-effective storage model. Your data stays yours, with no vendor lock-in.

Current and defensible

What you see reflects your environment today. Every result is grounded in its source data, so teams across security, risk, and operations work from the same trusted numbers.

USE CASES & AUDIENCE

ROLE	WHAT CCM DELIVERS
BISO / GRC Leader	Continuous control validation across the frameworks you report to, with less manual data gathering. GRC and operations work from the same dashboards.
CISO / Security Risk Leader	Continuous insight into control performance, fewer blind spots, and stronger, more defensible cyber risk reporting to the board and leadership.
Security & IT Operations	Early visibility into control gaps and drift, with clear lines back to the systems behind each gap, so the team can prioritize what to fix first.

RECOGNITIONS

- Gartner® Sample Vendor
- Gartner® Example Vendor
- IDC MarketScape, A Major Player
- Omdia “Vendor to Watch”