DataBee
A COMCAST COMPANY

SOLUTION BRIEF

DataBee® Faster Vulnerability Remediation

Know what you have, who owns it, and what needs to close first.

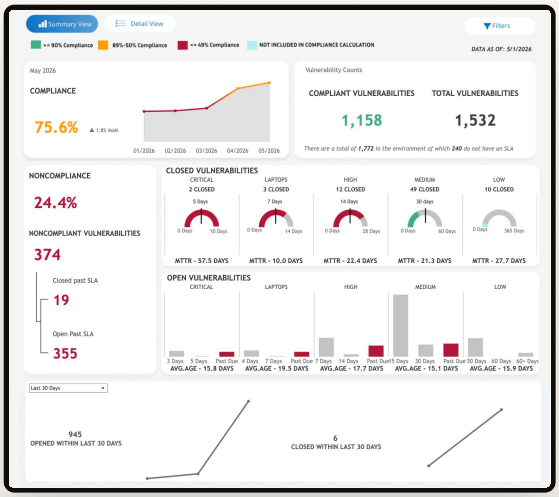
DataBee gives vulnerability and security teams a vulnerability compliance dashboard, accurate asset inventory, and automatic ownership attribution, so findings route to the right people on day one and SLAs don't slip silently.

VALUE PROPOSITION

Vulnerability programs rarely fail at scanning. They fail at everything after. Most scanners stop at "this IP has 14 criticals," but the real question is who owns that device and whether the SLA has been breached. In 2025, over 48,000 vulnerabilities were disclosed and attackers exploit them within days. DataBee Faster Vulnerability Remediation addresses the gap with continuously updated asset inventory, automatic ownership attribution, and a compliance dashboard that tracks SLAs and surfaces breaches.

KEY OUTCOMES

- **Route every finding to a real owner.** Ownership is attributed automatically from existing organizational data. Rremediation starts immediately instead of stalling in escalation loops.
- **Track SLAs before they slip.** The vulnerability compliance dashboard monitors Critical, High, and Medium findings against defined targets — overdue and at-risk findings surface before the auditor asks.
- **Prioritize by context, not just score.** Severity combines with asset criticality and business impact, so teams focus on real-world risk rather than raw CVE numbers.
- **Automate the handoff to remediation.** DataBee automatically creates tickets in your IT ticketing system for findings meeting your criteria, with full asset and owner context attached.



HOW IT WORKS

01 Connect

DataBee ingests findings from your existing scanners — correlating each to a continuously updated asset inventory so every finding is tied to a real device and a real owner, not an IP address.

02 Priortize

Vulnerability compliance dashboard applies your SLA targets to every finding, combining scanner severity with asset criticality and compliance requirements — overdue and at-risk findings surface without manual triage.

03 Act

DataBee automatically creates a ticket for every finding meeting your criteria, with full asset and owner context attached and every submission recorded alongside the original finding.

KEY CAPABILITES

- **Continous updated asset and application inventory.** Vulnerabilities are correlated to a current, accurate inventory — tied to real, active assets rather than stale or incomplete records.
- **Automatic ownership attribution.** DataBee identifies the most likely owner for every asset using existing organizational data, routing findings to the right person on day one.
- **Vulnerability compliance dashboard.** Tracks overall compliance percentage and mean-time-to-remediate by severity, surfaces ownerless findings, and flags what's overdue before the auditor asks.
- **Priortized based on severity, asset context, and business impact.** Scanner severity combines with asset criticality and compliance requirements — teams focus on what actually matters, not raw CVE scores.
- **Remediation workflow orchestration.** Findings meeting your criteria automatically trigger ticket creation with full asset and owner context — every submission recorded for reporting and accountability.
- **Explainable agentic AI for cyber risk.** DataBee RiskFlow™ analyzes vulnerability data in natural language, summarizing SLA compliance, exploring findings, answering questions — every answer grounded in source data.

WHY DATABEE

One platform, many outcomes

From vulnerability compliance to control monitoring 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, not last quarter's snapshot. Every result is grounded in its source data, so teams across security, risk, and operations work from the same trusted numbers.

RECOGNITIONS

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