DataBee
A COMCAST COMPANY

SOLUTION BRIEF

DataBee® Defense Against AI-Accelerated Threats

Built for the AI-accelerated threat environment.

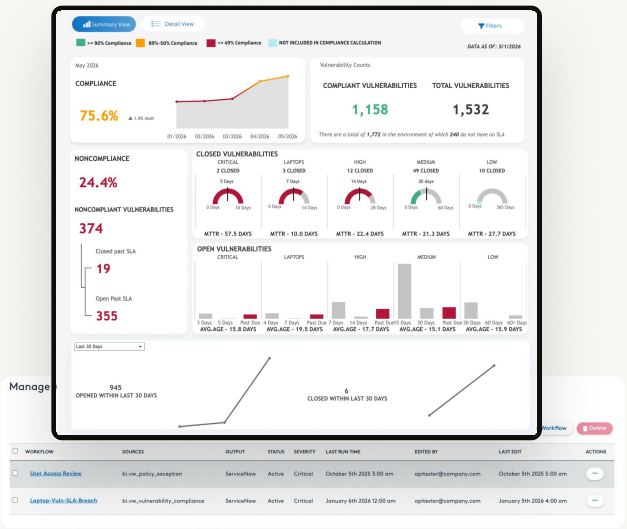
DataBee gives security operations, threat response, and vulnerability teams a normalized asset inventory, automatic ownership attribution, and continuous correlation of vulnerability findings to your assets, so when an AI-accelerated zero-day lands, you know in hours, not days, what's exposed, who owns it, and where to prioritize remediation.

VALUE PROPOSITION

When a high-impact CVE lands, most teams spend the first critical hours reconciling spreadsheets, chasing down owners, and separating real risk from noise — because asset inventory, ownership, and vulnerability context aren't pre-staged. In 2025, more than 48,000 new CVEs were disclosed, and attackers weaponize them within days. The DataBee platform changes that: continuously updated inventory, automatic ownership attribution, and vulnerability correlation mean the context teams need is already in place the moment a zero-day breaks.

KEY OUTCOMES

- **Know your exposure scope in minutes.** Every exposed asset surfaces across every connected source, normalized into a single trusted inventory — no inflated or fragmented counts.
- **Defensible from response through review.** Every scope, criticality, and ownership decision traces back to its source — the same numbers responders used are what leadership and audit see.
- **Focus response on what actually matters.** Findings combine scanner severity with asset criticality and business context, prioritizing real impact over raw CVE counts.
- **Know who owns every exposed asset on day one.** Ownership is attributed automatically from existing organizational data, including business application owners from your CMDB, without escalation.



HOW IT WORKS

01 Connect

DataBee aggregates data from 350+ sources across endpoint, identity, CMDB, cloud, vulnerability, network, and application systems — including assets your CMDB has never seen.

02 Resolve

Patent-pending entity resolution deduplicates records into a single trusted inventory, with business application owners and context pulled in from your CMDB and asset systems.

03 Respond

When a CVE lands, every exposed asset surfaces with owner and business context already attached. Ask follow-up questions in natural language using DataBee RiskFlow™.

KEY CAPABILITES

- **Patent-pending entity resolution.** One continuously updated record per real-world entity, deduplicated across every source — exposure counts aren't inflated by duplicates or fragmented across tools.
- **Prioritization by severity, asset context, and business impact.** Scanner severity combines with asset criticality and business application context, so teams focus on what actually matters in their environment.
- **Unified vulnerability and asset data.** Vulnerability findings are continuously correlated with the asset inventory. Every finding is linked to its owner and ready for assessment the moment a new CVE lands.
- **Explainable agentic AI for cyber risk.** DataBee RiskFlow™ analyzes asset and vulnerability data in natural language, summarizing exposure, surfacing owners, answering questions — every answer grounded in and traceable to source data.
- **Business application context.** Where your CMDB maps devices to business applications, DataBee pulls that mapping in — business impact and responsible owner travel with every asset and finding.
- **Remediation workflow orchestration.** Findings meeting defined criteria trigger ticket creation in your IT ticketing system, with full asset, application, and owner context attached and every submission recorded.

WHY DATABEE

One platform, many outcomes

From threat readiness 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, 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.

USE CASES & AUDIENCE

ROLE	WHAT DATABEE DELIVERS
CISO / BISO	A defensible answer to "are we exposed?" on day one of a zero-day disclosure, with scope, business impact, and accountable owners on hand for leadership and board conversations.
Vulnerability & Risk Manager	Continuously updated inventory with ownership attribution and vulnerability-to-asset correlation, so exposure assessment is fast and response prioritizes by severity and business impact.
SOC, IR & Threat Hunting	Instant exposure assessment with business context and ownership already attached to every affected asset — triage doesn't stall on inventory and owner lookups.
Security & IT Operations	Findings meeting your criteria flow into your IT ticketing system with full asset, application, and ownership context, so remediation starts without spreadsheet lookups or IP-only assignments.

RECOGNITIONS

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