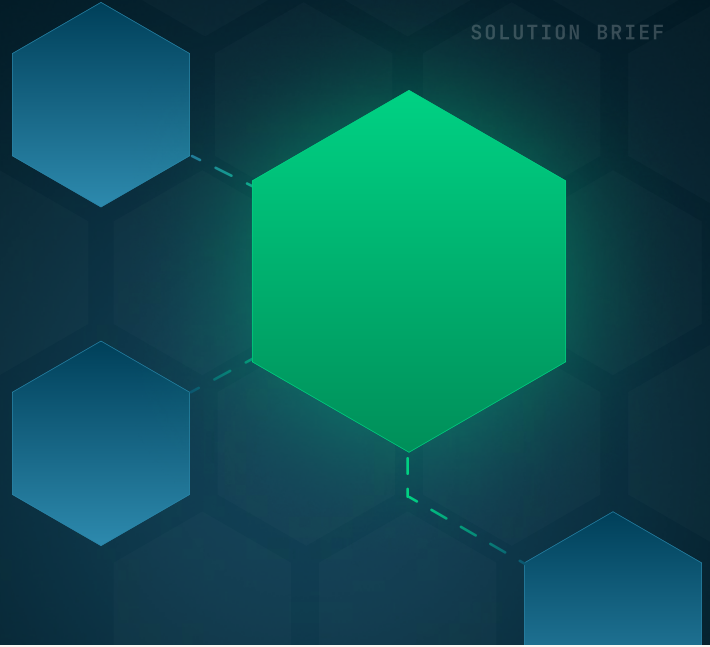


DataBee® Complete Asset Inventory

See every asset,
know who owns it, and keep it current.

DataBee gives GRC and security teams continuous inventory, discovery, and context across every device, person, account, and application, with ownership attributed and unowned assets, missing records, and incomplete attributes surfaced in one place.

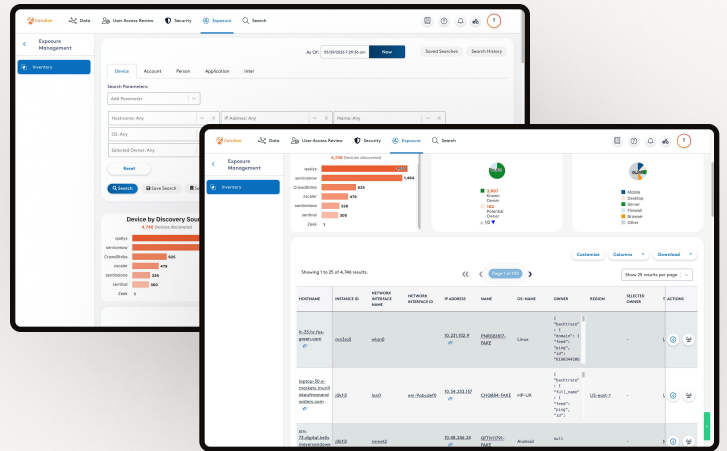


VALUE PROPOSITION

Most organizations can't reliably say what they own or who's accountable. CMDB records fall behind, ownership gaps linger, and unknown assets keep surfacing. DataBee Complete Asset Inventory solves this. The DataBee platform continuously pulls from every source referencing a device, person, account, or application, merges duplicates into single records, and assigns ownership. You get a defensible, continuously updated view of what you own and who's responsible, every entry traceable to its source.

KEY OUTCOMES

- **Faster remediation.** When CCM flags a gap, ownership is already assigned — findings reach the right team immediately, no manual lookup required.
- **Complete, current inventory.** Every device, person, account, and application resolves to a single deduplicated record, continuously getting updated.
- **Ownership for every asset.** Ownership is attributed automatically, with machine learning filling gaps — every asset has a named owner and org chain visible.
- **Surface assets your CMDB misses.** New and orphaned assets surface the moment they appear in any data stream, not just what your CMDB tracks.



HOW IT WORKS

01 Connect

DataBee aggregates data from 350+ sources across endpoint, identity, CMDB, cloud, vulnerability, network, and application systems — continuously discovering every asset in any event stream.

02 Resolve

Patent-pending entity resolution deduplicates records, assigns a unique ID to every device, person, account, and application, and suggests likely owners where none exist. Configurable source priority resolves conflicts.


03 Track

A searchable, filterable, exportable inventory with views aligned to NIST, CIS, and PCI. Unowned assets and incomplete records surface automatically — and the same inventory feeds every other DataBee solution.

KEY CAPABILITES


- **Patent-pending entity resolution.** One continuously updated record per real-world entity, deduplicated and aggregated across every source — inventory reflects what’s actually in the environment.
- **ML-driven owner discovery.** For devices with no confirmed owner, DataBee analyzes authentication patterns and suggests the three most likely owners, ranked by confidence, for review and confirmation.
- **Device inventory compliance dashboard.** Tracks owner, criticality, and authorization status against leading security frameworks — gaps and missing attributes surface automatically.
- **Data source prioritization.** When sources report conflicting attributes, configurable priority determines which is authoritative, preventing stale or lower-fidelity data from overwriting reliable records.
- **Explainable agentic AI for cyber risk.** DataBee RiskFlow™ analyzes your asset data in natural language, summarizing inventory coverage and ownership, exploring assets and gaps, and answering questions, with every answer explainable and grounded in the source data.

WHY DATABEE




One platform, many outcomes

CCM, vulnerability remediation, and access reviews all depend on accurate inventory and ownership. Complete Asset Inventory is the foundation every DataBee solution builds on.




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 ASSET INVENTORY DELIVERS
BISO / CISO	A single, defensible answer to what the organization owns and who is responsible — across every business unit and data source, without a separate asset management tool.
GRC / Security Risk Leader	A complete, ownership-attributed inventory aligned to leading security frameworks, so controls can be measured accurately and risk programs start from a trusted foundation.
Security & IT Operations	Continuous discovery of new and orphaned assets across every data stream, with ground-truth inventory reconciled automatically against your CMDB — gaps, unowned assets, and conflicting attributes surface without manual effort.

RECOGNITIONS



Gartner® Sample Vendor



Gartner® Example Vendor



IDC MarketScape, A Major Player



Omdia “Vendor to Watch”

GARTNER is a trademark of Gartner, Inc. and its affiliates. Gartner does not endorse any company, vendor, product or service depicted in its publications, and does not advise technology users to select only those vendors with the highest ratings or other designation. Gartner publications consist of the opinions of Gartner’s business and technology insights organization and should not be construed as statements of fact. Gartner disclaims all warranties, expressed or implied, with respect to this publication, including any warranties of merchantability or fitness for a particular purpose. Hype Cycle is a registered trademark of Gartner, Inc. and/or its affiliates and is used herein with permission. All rights reserved.