

DataBee® Entity Correlation & Normalization

One trusted inventory,
built from everything you already have.

DataBee normalizes, deduplicates, and aggregates security data from your existing tools, correlating records that refer to the same user, device, or application, giving GRC and security teams a consistent data foundation for controls monitoring, reporting, and investigations.

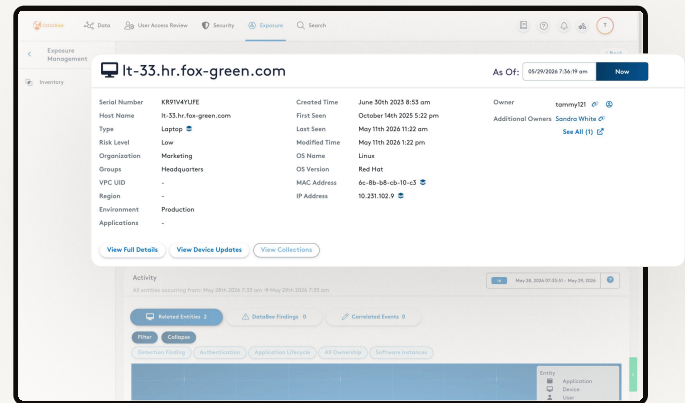


VALUE PROPOSITION

Most organizations that try to build a trusted security data foundation themselves find schemas drift, identifiers don't match, and programs end up running on inconsistent data. The DataBee platform delivers that foundation: every connected source is normalized, then deduplicated and aggregated by patent-pending entity resolution into a single record per real-world entity — giving every team a continuously updated, trusted data layer to work from.

KEY OUTCOMES

- Normalized data across every connected source.** Every security and IT tool transforms into a consistent schema — analytics, dashboards, and downstream programs work from common structures, not vendor-specific formats.
- One record per entity, deduplicated across every source.** Every user, device, and application resolves to a single continuously updated record. CCM dashboards, executive reports, and vulnerability management all work from the same defensible data..
- Investigate faster with full entity context.** Every entity has a single correlated view across all sources — authentications, vulnerability scans, threat signals, and ownership changes — no manual stitching across consoles.



HOW IT WORKS

01 Connect

DataBee connects to 350+ sources across identity providers, CMDBs, endpoint tools, cloud environments, and SaaS applications, continuously aggregating security and business data as it is produced.

02 Resolve

Patent-pending entity resolution assigns a unique ID to every user, device, and application, linking and deduplicating records across sources. Configurable priority determines which source is authoritative.


03 Correlate

Every incoming event is enriched with entity context and appended to that entity's activity timeline — feeding CCM dashboards, executive reporting, access reviews, and vulnerability management from a single source of truth.

KEY CAPABILITIES


- Patent-pending entity resolution engine.** Assigns a unique ID to every user, device, and application — linking records across sources even when identifiers change, are missing, or appear inconsistently.
- Cross-source deduplication and aggregation.** Detects and merges duplicate records across tools, preventing inflated counts and contradictory data in downstream analytics and dashboards.
- Configurable source priority.** Define which system is authoritative when sources disagree — works across single or multiple CMDBs, with conflicts and discrepancies surfaced as they're discovered.
- Entity activity timeline.** A single console view per entity showing the full correlated history of what occurred across every source: authentications, vulnerability scans, threat signals, ownership changes, and more.
- Continuously updated inventory.** Correlations refine in near real time as new data arrives, keeping entity records current without manual reconciliation or scheduled refresh cycles.
- Explainable agentic AI for cyber risk.** DataBee RiskFlow™ analyzes entity data in natural language, summarizing data foundation status, exploring relationships, answering questions — every answer grounded in source data.

WHY DATABEE




One platform, many outcomes

Entity correlation is the foundation every other DataBee solution depends on. Accurate CCM metrics, defensible executive reports, and reliable access reviews all start with a trusted entity layer.




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 ENTITY CORRELATION DELIVERS
GRC & Security Analytics Teams	A consistent, deduplicated foundation of user, device, and application data, ready for controls monitoring, reporting, and analytics without manual reconciliation or custom pipelines.
CISO / BISO	Confidence that every control dashboard, vulnerability count, and executive report reflects the actual environment, not inflated counts from duplicate or fragmented records.
Data Engineering / Security Architect	A purpose-built foundation for security data programs in your existing data fabric or data lake, replacing custom entity resolution logic that's hard to build and harder to maintain.
Security Operations	A per-entity activity timeline showing the full history of what occurred across every source, so investigations start from a complete picture rather than manually stitched logs.

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.