DataBee
A COMCAST COMPANY

SOLUTION BRIEF

DataBee® User Access Reviews (UAR)

Know who has access.
Prove you reviewed it.

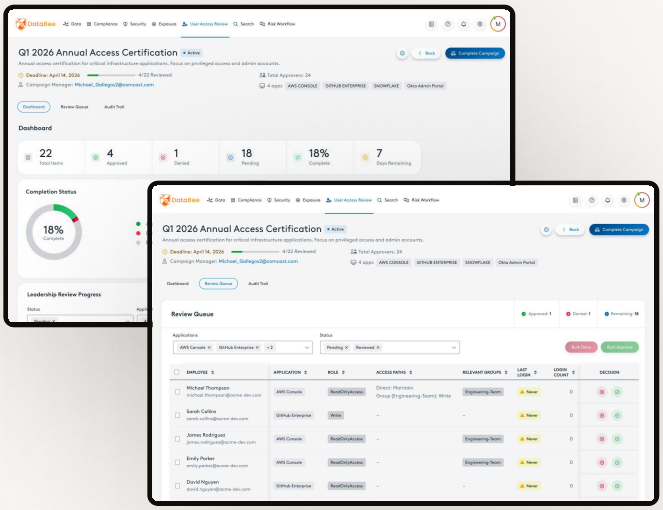
DataBee UAR gives GRC and identity teams a purpose-built, lightweight access review capability built for large, complex organizations, designed to scope, route, and close periodic reviews quickly with a clear audit trail.

VALUE PROPOSITION

Large organizations run access reviews as a required compliance control, but existing tools often add unnecessary complexity or overhead. DataBee UAR changes that. Built on the DataBee platform, UAR provides a lightweight, purpose-built way to connect to existing identity sources—from Microsoft Entra ID and Okta to legacy systems—and launch campaigns quickly without a full IGA implementation. The result is a fast, reliable way to route decisions, maintain a clear audit trail, and leverage identity data already in DataBee to eliminate additional integration or setup effort.

KEY OUTCOMES

- **Lightweight to operate.** Scope, route, and close access reviews inside the DataBee console, without spreadsheets, manual exports, or full identity lifecycle platform overhead.
- **Decisions made on evidence, not names.** Every review item includes last login, MFA status, and access context so managers act on facts rather than rote approvals
- **Close the loop automatically.** When a campaign closes, denied access is grouped by application and dispatched as remediation workflows.
- **Audit ready evidence with full traceability**. Every decision is logged with full access context, traceable to source identity data, and exportable for audit obligations.



HOW IT WORKS

01 Connect

DataBee connects to your identity providers and assembles the campaign population automatically. Every in-scope user-application pair is included, deduplicated regardless of how access was granted. No manual export, no data migration required.

02 Review

Access decisions route to each user's direct manager via their existing SSO. Managers see last login, MFA status, and access context on every item. Admins track completion across the full organizational and dispatch bulk reminders from a single dashboard.

03 Remediate

On campaign close, denied access is grouped by application and orchestrated as remediation workflows. The full decision record, including every approval, denial, escalation, and notification, is retained and exportable for compliance reporting.

© 2026 DataBee® All Rights Reserved

KEY CAPABILITES

- **Campaign management with audit export.** Create, schedule, and run access review campaigns at any cadence — every decision logged, traceable to source identity data, and exportable for audit requests.
- **One review per access relationship.** Each user-application pair is reviewed exactly one, regardless of weather access was granted directly or through a group. Single denial remove every access path.
- **Grouped remediation workflows.** On campaign close, denied access is grouped by application and orchestrated as workflows aligned with how IT teams actually remediate.
- **Explainable agentic AI for cyber risk.** DataBee RiskFlow™ analyzes access data in natural language, summarizing review status, exploring access patterns, answering questions — every answer grounded in source data.
- **Risk-informed review queue.** Everyitem surfaces last login, MFA status, role, and access paths so managers can bulk-approve healthy access and investigate anomalies with full context.
- **Automatic manager routing.** Access decisions go to each user's direct manager via their existing SSO. No training required, no IT ticket to get started.

WHY DATABEE

One platform, many outcomes

From access governance 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 identity 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 UAR DELIVERS
GRC / Risk Leader	Repeatable access reviews aligned to SOX, SOC 2, and other audit obligations, with a clear decision record for reporting and no implementation project to get started.
Identity & Access Management Team	Lightweight reviews against modern identity providers and legacy systems alike, with a clean decision record that feeds back into your identity governance program.
CISO / BISO	A purpose-built UAR capability inside the same platform used for risk monitoring and executive reporting, at the scale large organizations require.
Security & IT Administrator	Scope and launch campaigns against your identity data sources, track completion across the org hierarchy, and dispatch remediation workflows without leaving the console.

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.