# Exabeam and DataBahn

How Exabeam and DataBahn Work Together to Control Security Data Volume

## Joint Value Summary

Security operations teams face rising telemetry volumes that strain budgets and slow investigations. The Exabeam and DataBahn joint solution separates data control from detection, allowing teams to reduce ingestion volume while maintaining detection quality and retaining full-fidelity data in customer-owned storage for long-term search, investigation, and compliance. The result is cleaner detection inputs, controlled data costs, and flexible long-term retention of full-fidelity telemetry in customer-owned storage.

## Why Organizations Use the Exabeam and DataBahn Joint Solution

Most security teams ingest far more data than they can effectively analyze. High-volume sources drive up security data costs without a reciprocal increase in security value, reduce signal quality, and limit flexibility during architecture changes or migrations. At the same time, teams still need access to historical telemetry to meet regulatory requirements or other IT requirements.

This joint solution allows organizations to control where data goes and why, so detection systems focus on high-value signals while other data remains available for long-term use in a cost-efficient manner. Teams can retain historical telemetry in customer-owned object storage or data lakes, keeping data accessible for investigations and audits optimizing data retention costs.

## Market Challenge

Detection platforms often require teams to decide what data to ingest up front, tying cost, retention, and investigative access to a single system. As environments evolve, organizations need greater flexibility to manage data flow and retention without disrupting detection workflows or losing access to important historical telemetry.

Without an upstream data fabric and independent archival layer, organizations struggle to balance detection performance, cost control, and long-term access to full-fidelity telemetry stored in systems they own and manage.

## How Exabeam and DataBahn Work Together

DataBahn operates upstream as a security data fabric that collects, filters, enriches, and routes telemetry based on purpose. It normalizes data to common security schemas and uses AI-assisted parsing to handle custom and legacy log formats without manual engineering. Security-relevant data is routed to Exabeam for detection and investigation, while full-fidelity data is archived in customer-owned storage or data lakes managed through DataBahn. A collect-once, route-anywhere architecture means telemetry can flow to multiple platforms simultaneously, preserving data ownership and avoiding vendor lock-in. This approach helps organizations more effectively manage SIEM data storage requirements while preserving long-term access to historical telemetry for investigation and compliance.

New-Scale Fusion applies behavioral analytics, correlation, and dynamic risk scoring to the curated detection data stream. Analysts investigate detections in Threat Center using high-value signals, while historical data retained through DataBahn remains available through its own interface and tools when deeper investigation or audit support is required.

## Key Integration Benefits

- Increase visibility into data flow and detection readiness: Provide visibility into what data is collected, how it is processed, and where it is routed. This helps security operations teams identify coverage gaps, detect data quality issues, and maintain readiness as environments and data sources change.
- Support investigations and compliance with low-cost data retention: Retain enriched telemetry in customer-owned storage outside the primary detection path to support investigations and audit requirements without increasing SIEM storage costs.
- Ensure reliable telemetry delivery at enterprise scale: Persistent buffering, automatic failover, and burst handling keep data flowing to Exabeam even during downstream interruptions or traffic spikes, across hybrid and multi-cloud environments.

## Primary Use Case: Reduced Security Data Costs Without Detection Tradeoffs

**Definition:** Reduce the volume of data sent to the SIEM while maintaining detection coverage and access to historical telemetry.

**Challenge:** Security teams ingest large volumes of low-signal data that increase costs and slow investigations. Attempts to reduce ingestion often risk losing visibility or investigative depth.

**Solution:** DataBahn filters and routes telemetry upstream, sending only high-value data to Exabeam for detection while retaining full-fidelity data for long-term search and compliance. Exabeam applies behavioral analytics and investigation workflows to a cleaner dataset, improving efficiency without reducing coverage.

## Integration Overview

Integrated Product: New-Scale Fusion

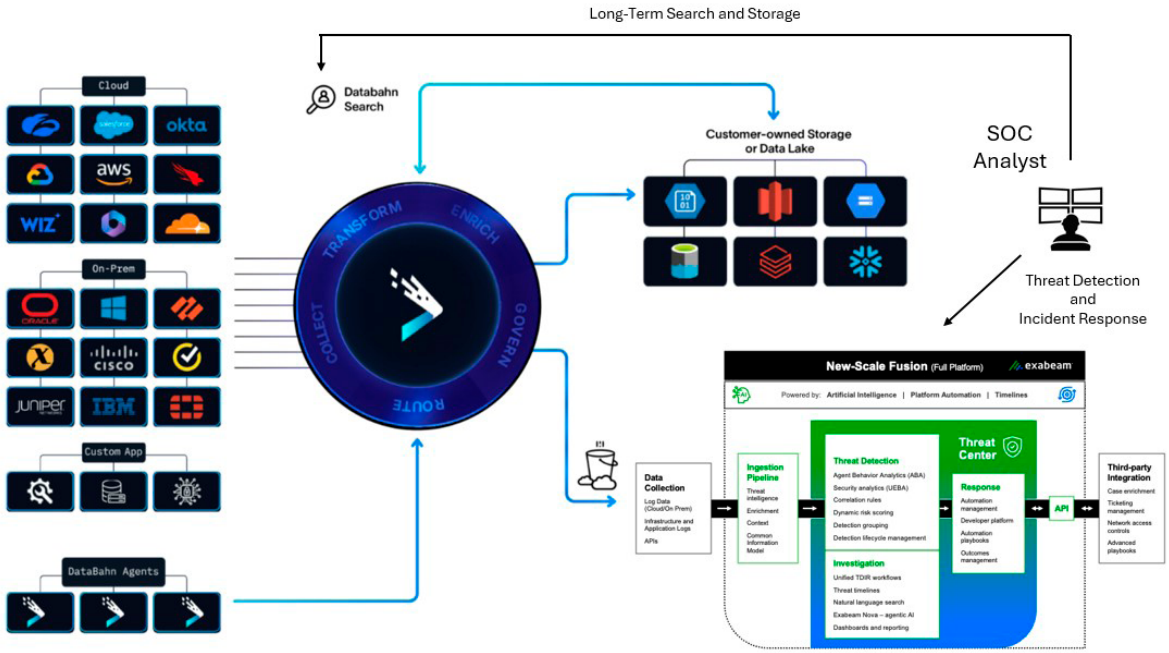


Figure 1.

**Route security-relevant telemetry to Exabeam** for detection while retaining full-fidelity data in customer-owned storage through DataBahn for long-term search, investigation, and compliance.

## About Exabeam

Exabeam is the leader in behavior intelligence for the agentic enterprise. As organizations deploy digital workers and confront machine-speed adversaries, Exabeam delivers flexible, industry-proven solutions for insider threat coverage of humans and agents and faster, more accurate threat detection, investigation, and response (TDIR). Learn more at www.exabeam.com.

**Learn more at**
**www.exabeam.com →**