DataBahn for Exabeam

Optimize data management for threat detection, investigation, and response.

DATABAHN

Unlocking Exabeam's Full Potential Starts with the Pipeline

In the dynamic world of cybersecurity, threats and attack vectors adapt and change every second – and for SOCs to stay ahead, they need to be empowered with advanced threat detection, investigation, and response capabilities. The growing number of threats and alerts stretch understaffed security teams that need consistent and reliable data collection and automated response capabilities.

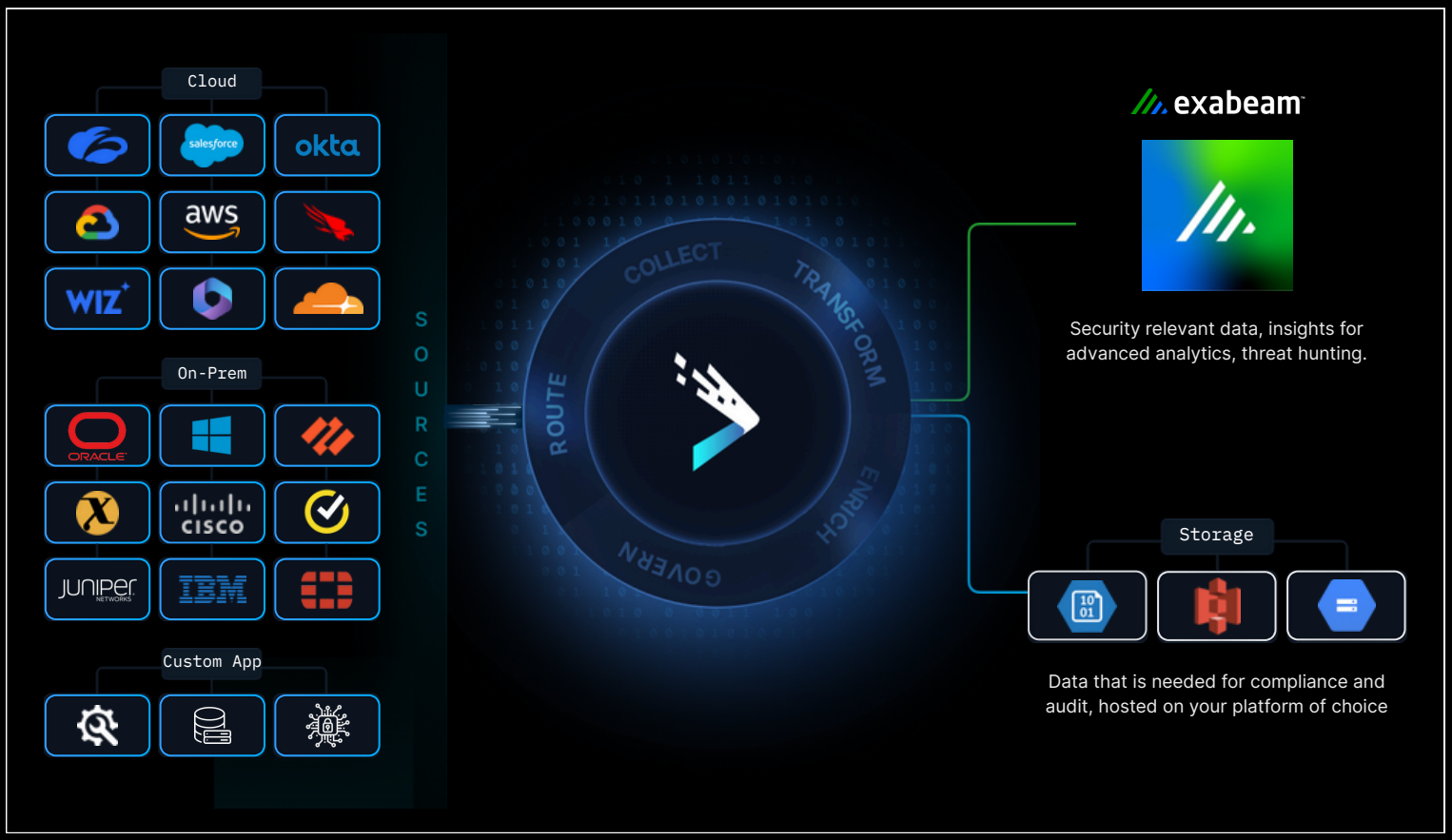
Exabeam is a leading, next-generation, cloud-native SIEM platform designed to empower SOCs. Built on a foundation of behavioral analytics and automation, Exabeam SIEM addresses the evolving challenges of modern security teams by delivering speed, accuracy, and efficiency at scale. Enterprises use Exabeam to gather analytics-driven insights to uncover, investigate, and resolve security threats and vulnerabilities that other SIEMs and tools might miss.

These enterprises also use DataBahn for an intelligent data pipeline that guarantees consistent and reliable log collection and aggregation, data normalization, and seamless orchestration from source to destination with full visibility and improved governance.

Together, Exabeam and DataBahn offer a solution that enables enterprise SOCs to accelerate and optimize their security operations, while enhancing data management and governance.

How It Works: Intelligent control across the pipeline

To help visualize how DataBahn supports Exabeam end-to-end, the following diagram maps the key stages of the pipeline:



Smart Edge: Resilient Log Collection at Scale
Smart Edge supports both agentless and agent-based collection, built on a mesh architecture that scales horizontally and vertically. This ensures continuous ingestion—even during bursts—while simplifying deployment across on-prem, cloud, or hybrid environments.

Transform, Enrich, and Optimize in Real Time
As logs enter the pipeline, DataBahn applies a suite of enrichment and optimization steps:

- Normalize to standard formats such as OTEL, OCSF, or Exabeam-native schemas
- Enrich with geolocation, business context, CMDB data, or application metadata
- Suppress or reduce noise using prebuilt or custom rules
- Aggregate or convert logs into lightweight summary signals or metrics, where appropriate

These operations can be performed at the edge, in transit, or centrally, giving teams maximum flexibility.

Smart Routing and Replay
With built-in routing controls, only security-relevant data is sent to Exabeam. Additional

telemetry can be streamed to alternate destinations, such as cloud-based cold storage (e.g., S3, Azure Blob), data lakes, or observability platforms. Replay functionality enables teams to pull older data back into Exabeam or any other tool when needed, without reprocessing through the full pipeline or duplicating ingestion.

Control Plane: Unified Visibility and Management
Fleet management, volume analytics, destination configuration, and billing are managed through a single interface. Schema drift is continuously monitored and flagged proactively, ensuring ingestion compatibility as source formats evolve. This ensures that security teams can scale confidently while maintaining control and compliance across their telemetry stack.

DataBahn: A smarter, more scalable pipeline for Exabeam

DataBahn's Security Data Fabric was built to help security teams regain control of their telemetry, starting at the edge and continuing all the way through to their SIEM and beyond. When deployed with Exabeam, it enables clean, reliable, and cost-efficient delivery of security-relevant data while providing flexible routing, visibility, and governance across the pipeline.

Key Benefits

- Reduce telemetry volume to Exabeam by 60%+ through built-in log control rules, summarization, and filtering.
- Eliminate fragile collectors using Smart Edge, a resilient, mesh-based ingestion layer with horizontal and vertical scaling.
- Accelerate onboarding with a library of 500+ prebuilt connectors and agentless collection support.
- Route only what's relevant to Exabeam while streaming full-fidelity data to cold storage, data lakes, or observability platforms.
- Replay logs on demand from compliant cold storage without reprocessing through Exabeam.
- Detect schema drift automatically, ensuring ongoing compatibility and ingestion success.
- Manage the pipeline centrally, with complete visibility into fleet status, volume usage, and destination health.

Why DataBahn + Exabeam Are Better Together

Exabeam delivers advanced analytics and timeline-based investigations. But to function effectively, it needs clean, timely, security-relevant telemetry. DataBahn ensures that's exactly what it gets, while reducing operational complexity and cost. Together, they enable faster detection, smarter investigation, and a more efficient SOC.

DataBahn.ai is a leader in AI-driven Data Pipeline Management and Data Fabric solutions, helping organizations transform their data operations with innovative engineering and advanced analytics technologies. With its Data Fabric platform and cutting-edge AI capabilities, DagtaBahn.ai is committed to empowering organizations to harness the full potential of their data for a smarter, more connected future.

Learn more at **databahn.ai**

DATABAHN