DataBahn for Microsoft Sentinel

Enable value-driven orchestration using
DataBahn's Security Data Fabric
for your Microsoft Security Deployments

DATABAHN

DataBahn + Microsoft Sentinel

Many enterprises and security teams are increasingly choosing Microsoft Sentinel for its comprehensive service stack, advanced threat intelligence, and automation capabilities, which facilitate faster investigations. Most notably, it offers native support for seamless integration with other Microsoft services, infrastructure, and applications. However, these choices often present two distinct challenges:

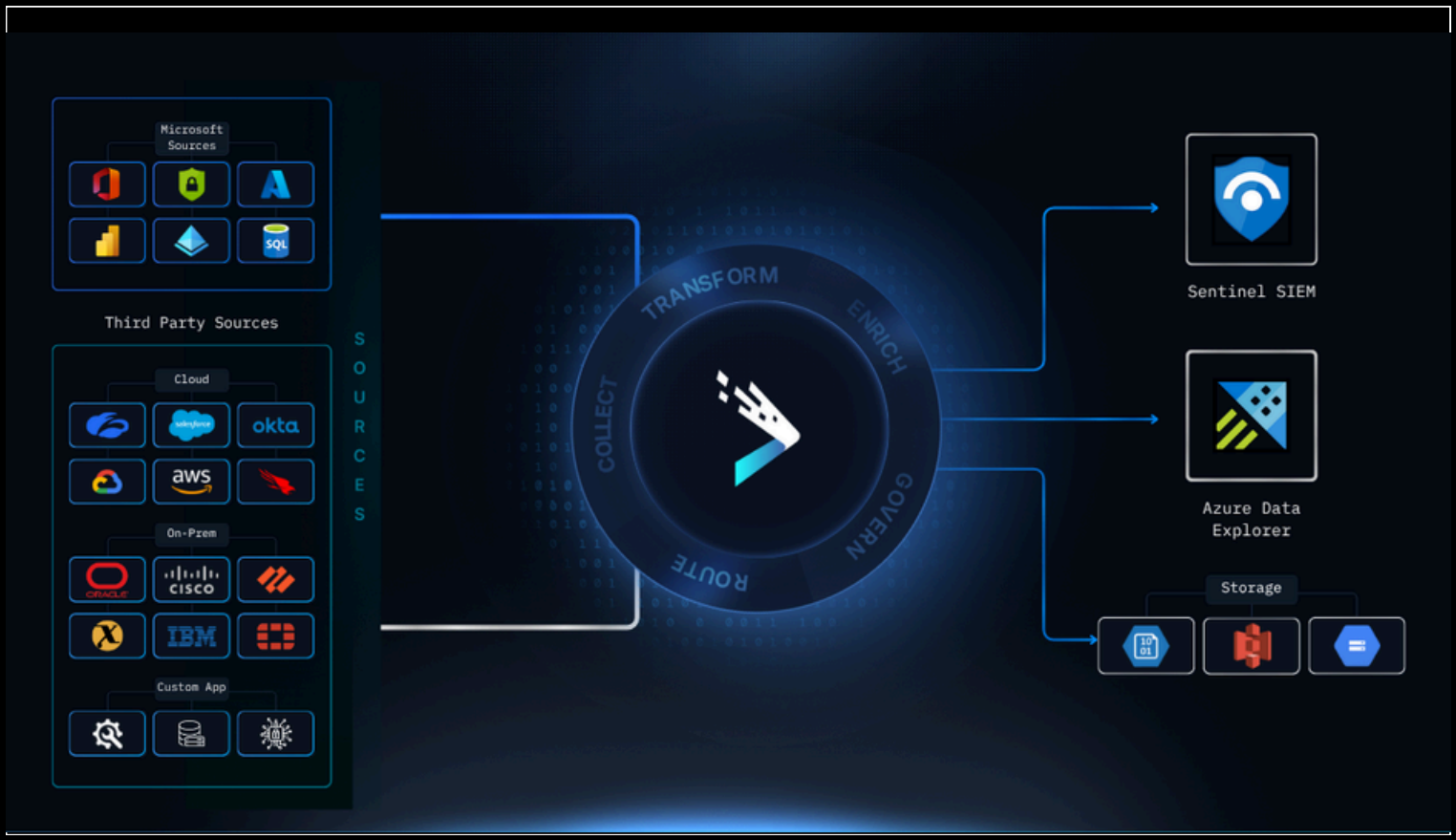
First, Microsoft offers a wide range of security features, with many integrated into their premium Microsoft 365 subscription packages. This can lead some budget-conscious executives to consider Microsoft's offerings as potential cost-effective alternatives for their security needs. However, it's essential to recognize that Microsoft Sentinel, unlike most of their security solutions, is not included in any specific Microsoft 365 plan, not even the highest-tier subscriptions. Instead, it adheres to the typical pricing model of SIEM/Data Lake products, where costs are determined by data usage.

Second, challenges arise when security teams adopt Sentinel as their central hub for aggregating data from third-party sources (non-Microsoft sources) and maintaining threat detection and response capabilities. In this scenario, integrations are usually custom-developed or managed by the security teams themselves, often lacking mechanisms to enforce spending limits within the Sentinel framework.

The Solution

DataBahn's Security Data Fabric with its purpose built Smart Edge along with the Data Highway products can take data from a wide range of sources (both Microsoft and Non-Microsoft sources), parse and structure them into any format or data model of your choosing, enrich data with any meaningful context (internal and external context), orchestrate the data to extract meaningful insights and deliver security relevant data and insights into your Sentinel SIEM for optimal querying, analytics and search.

DataBahn helps Sentinel deployments by streamlining data collection and ingestion and removing the onus of your team having to build custom integrations, defining what data goes into basic/analytics tables, deploying your staging locations to publish data from third party products and services into your Sentinel SIEM.



With DataBahn's orchestration engine, security teams can optimize data pipelines and control costs without compromising visibility.

1. Simplify Ingestion into Microsoft Sentinel

- Ingest telemetry in real time using DataBahn's native streaming integration, no additional infrastructure is needed.
- Tap into 500+ plug-and-play connectors spanning the Microsoft ecosystem and beyond.
- Auto-parse, normalize, and structure data on the fly before forwarding to Sentinel.

2. Reduce Volume Without Losing Signal

- Apply context-aware, out-of-the-box volume reduction rules to cut noisy, low-value logs.
- Achieve a 50%+ reduction in ingestion volume, lowering cost while preserving the context needed for detection and investigation.

3. Turn Logs into Insight

- Use smart orchestration features such as aggregation and suppression to reshape high-volume telemetry (e.g. NetFlow) into compact, query-ready records.

Accelerate investigations with leaner, faster data in Sentinel.

- DataBahn gives security teams deep control over data quality, cost, and performance, without adding complexity.

4. Enforce Stronger Data Governance

- Automatically detect and isolate sensitive data in motion, minimizing exposure and tightening compliance.

5. Accelerate Threat Hunting

- Leverage DataBahn's Indicator Index to extract key observables (IPs, domains, hashes) and entity relationships (processes, network activity, registry changes).
- Enrich context with first/last seen timestamps and frequency patterns to drive faster, more targeted investigations.

6. Adopt a Future-Ready Architecture

- Use orchestration to integrate seamlessly with Azure services like Blob Storage and Azure Data Explorer, enabling cost-effective long-term storage and analysis.

7. Track Telemetry Health in Real Time

- Use DataBahn's dynamic device inventory to detect silent endpoints, upstream outages, and blind spots before they impact your SOC.

8. Cut Sentinel Ingestion Costs

- Eliminate staging infrastructure with plug-and-play integrations.
- Route cold or low-priority data to cost-efficient storage (e.g. Azure Basic Tables, ADX, Blob) while retaining access through the same data models, no compromises on visibility.

Why Security Teams Choose DataBahn

Plug-and-Play Integrations

Connect to 500+ tools and data sources instantly with out-of-the-box connectors—no custom engineering required.

Lower Costs, Higher ROI

Cut Sentinel costs by filtering out redundant and low-value logs using built-in volume reduction rules.

Always-On Data Collection

Smart Edge ensures uninterrupted collection, even during traffic spikes or outages, so your data never stops flowing.

Context-Rich Enrichment
Enrich logs with threat intel, user, asset, and geo-data to boost the precision of detections and investigations.

Targeted Data Delivery
Route only high-value, security-relevant data to Sentinel, and offload the rest to Azure Blob or ADX, reducing cost while preserving access.

Seamless Format + Schema Handling
Auto-adapt to schema changes and format variations to ensure consistent data quality with minimal overhead.

Sensitive Data Protection
Detect and isolate sensitive data in transit to strengthen compliance and reduce exposure risk.

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, DataBahn.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