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. With its two-tier model — the **Analytics Tier** for hot, real-time security data and the **Data lake Tier** for cost-efficient long-term retention — Sentinel provides flexibility and scale across diverse security needs.

At the same time, organizations often need to bring in telemetry from hundreds of non-Microsoft sources, enrich it with business context, and manage ingestion costs effectively. Sentinel delivers the unified platform, and Databahn's **Security Data Fabric** strengthens adoption by enabling seamless onboarding, enrichment, and orchestration across diverse data sources and preparing data to be AI-ready for broader security and analytics initiatives.

As an **authorized Microsoft Sentinel partner**, Databahn works alongside Microsoft to help customers maximize the value of Sentinel. By streamlining ingestion from 500+ sources, normalizing and enriching telemetry, and orchestrating delivery into the right Sentinel tier, Databahn enables faster time-to-value, simplified onboarding, and operational efficiency at scale

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

- Leverage Sentinel's two-tier model, keeping hot data in the Analytics Tier for real-time detection while routing older logs into the native Data Lake Tier for cost-efficient long-term retention. External services like Blob or ADX can still be integrated when extended analytics is required.

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 into Sentinel's Data lake Tier for native long-term retention, while still allowing offloading to Blob or ADX if extended analytics or external archiving is desired.

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
Send high-value, security-relevant data to Sentinel's Analytics Tier, and move the rest into the Data lake Tier for cost-efficient retention. Blob or ADX remains available for specialized analytics or external storage needs.

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