Enable value driven Data Orchestration using databahn.ai's Security Data Fabric for your Microsoft Security Deployments

SOLUTION BRIEF

DataBahn + Microsoft

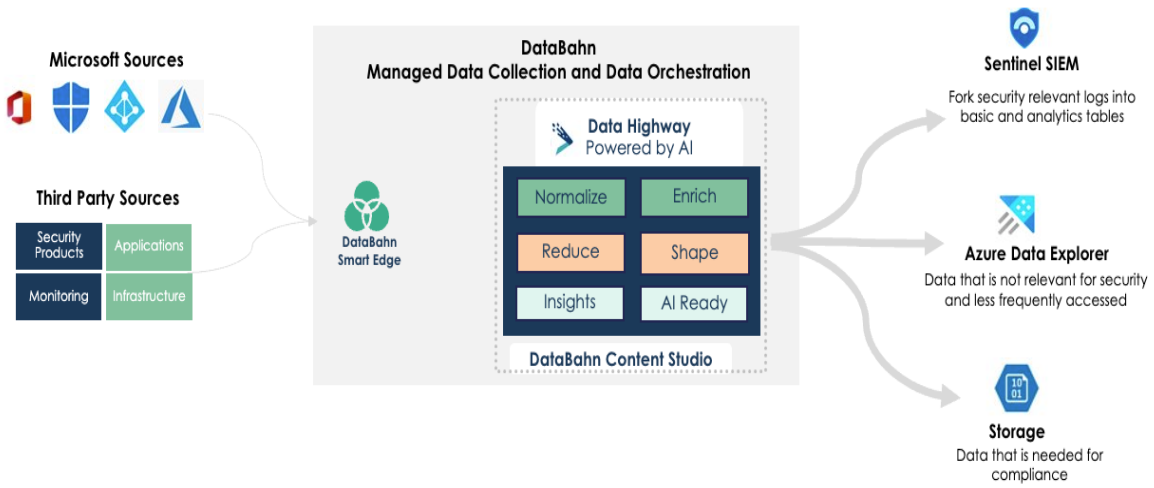
Many enterprises and security teams are increasingly choosing Microsoft Sentinel for its comprehensive service stack, advanced threat intelligence, and automation capabilities, which facilitate faster investigations. Most notably, it offers native support for seamless integration with other Microsoft 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.

Through DataBahn's Orchestration capabilities, Security teams can:

- Simplify data collection and ingestion into Sentinel
    - By using DataBahn's plug-and-play integrations and connectors with a wide array of products and devices including and beyond the Microsoft ecosystem
    - By using DataBahn's native streaming integration for a hassle-free, real time data ingestion into Sentinel, eliminating any additional log collection infrastructure
    - By effectively normalizing and structuring data using DataBahn's orchestration pipelines before the data is delivered to your destinations
- Send only security relevant data to your Sentinel SIEM
    - By using DataBahn's out of the box library of context-aware volume reduction rule sets helping you achieve more than 35% data volume reduction
- Convert logs into insights by
    - Using volume reduction functions like aggregation and suppression to convert noisy logs like network traffic/flow into manageable insights that can be loaded in Sentinel reducing both the volume and the overall time for queries to execute
- Increase overall data governance and data quality
    - By identifying and isolating sensitive data set in transit thereby limiting exposure
- Perform split second threat hunting
    - By using the DataBahn's Indicator Index to extract insights such as Security Observables (IP addresses, Domains, URLs, Hashes), Entity Relationships (Processes, Network execution, Registry modifications), Intel Context
    - By using additionally derived context such as first observed / last observed time / frequency of observation to speed up data exploration and hunting
- Bring best of breed services and technologies
    - By leveraging DataBahn's simplified data orchestration capabilities, Microsoft customers can use additional Azure services like Azure Data Explorer, Blob Storage to implement both a cost effective and future ready security architecture
- Get visibility into the health of telemetry generation
    - By using the dynamic device inventory generated by DataBahn to identify devices that have gone silent, log outages and detecting any other upstream telemetry blind spots
- Reduce overall costs of your Microsoft Sentinel deployment
    - By removing the need for any staging locations or custom integrations by taking advantage of DataBahn's library of integrations and connectors

- By routing less frequently accessed data sets using Data Highway to low-cost services like Sentinel basic tables or Azure Data Explorer or storage solutions like Blob storage while adhering to the same data models to access them only when the need arises

Benefits of using DataBahn with Sentinel

Out-of-the-box connectors and integrations
DataBahn offers effortless integration and plug-and-play connectivity with a wide array of products and devices, allowing SOCs to swiftly adapt to new data sources.

Resilient data collection
DataBahn's highly resilient Smart Edge enables your team to not worry about single points of failures or managing occasional data volume bursts.

Enrichment against Multiple Contexts
DataBahn enriches data against various contexts including Threat Intelligence, User, Asset, and Geo-location, providing a contextualized view of the data for precise threat identification.

Format Conversion and Schema Monitoring
The platform supports seamless conversion into any data model of your choosing, additionally facilitating flexible and faster downstream onboarding in Sentinel and other services.

Schema Drift
Detect changes to log schema intelligently for proactive adaptability and to avoid downstream detection impact

Reduced Costs
DataBahn enables your team to manage the overall costs of your Sentinel deployment by providing a library of purpose-built volume reduction rules that can weed out redundant and less relevant logs keeping your Sentinel SIEM costs optimal.

Sensitive data detection
Identify, isolate and mask sensitive data ensuring data security, governance and compliance.

Orchestrate data into different Microsoft destinations based on relevance
DataBahn's orchestration platform helps tier data based on its relevance so you can put purpose to your data and send security relevant data to Sentinel while the rest can be sent to Azure Data Explorer or Azure Blob Storage for threat hunting and compliance use cases.

Get your data AI ready
Use the DataBahn AI Ready framework to get your data cleansed, enriched, features extracted, and embeddings generated to build AI powered apps on top of your Azure environment.

Risk free data sharing internally and externally
Use DataBahn to fork out data streams to different services beyond the Sentinel SIEM in your Microsoft environment such as Azure Data Explorer or Blob storage for compliance and to external destinations.

With DataBahn and Microsoft Sentinel, unlock the power of your data by maximizing the value while reducing the overhead it takes to collect and ingest data for Azure and non-Azure sources and the overall operating costs.