SOLUTION BRIEF

Elevate your Autonomous Security Operations using DataBahn's Security Data Fabric for your DEVO SIEM deployments

DataBahn + Devo

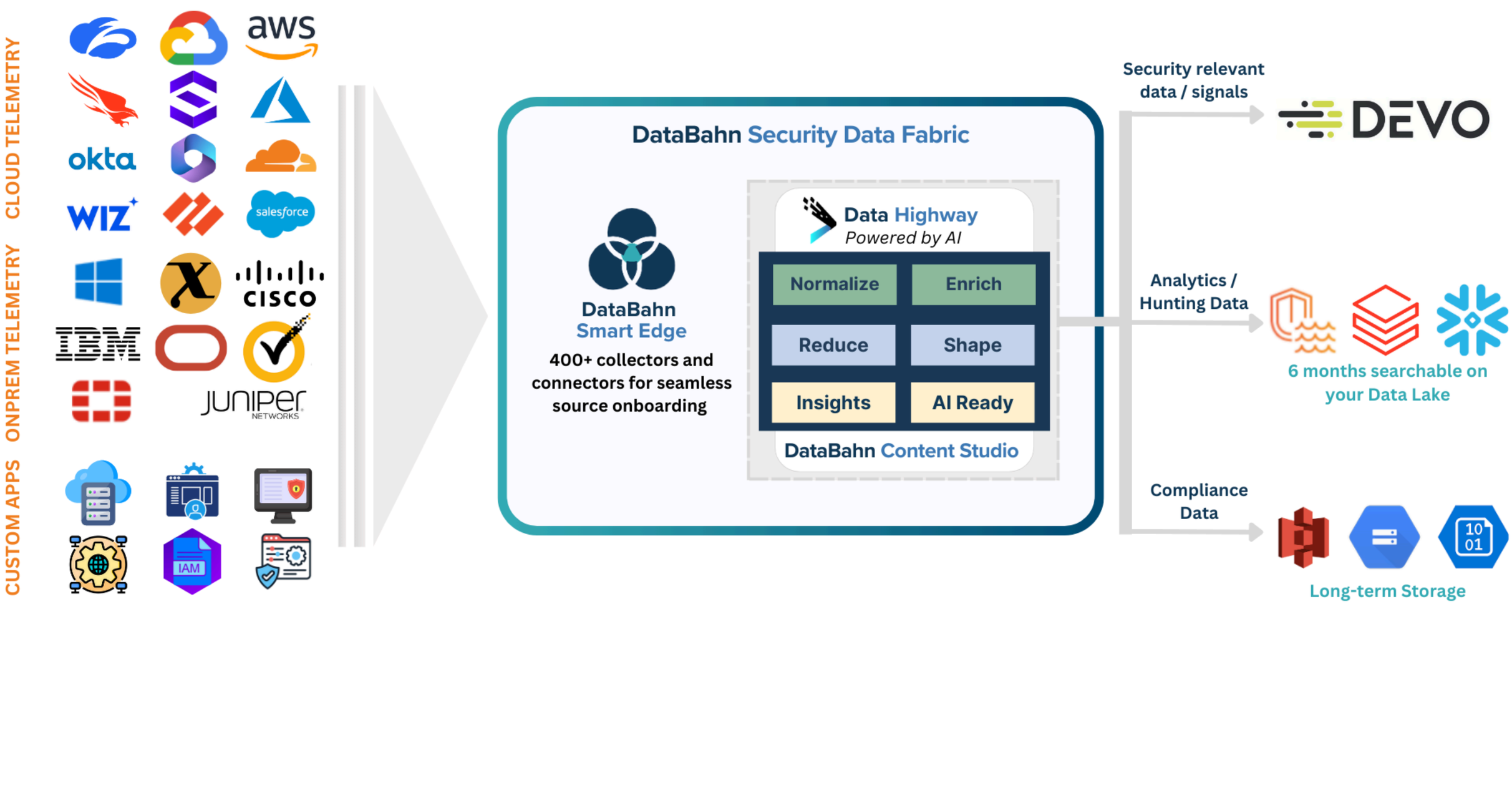
Security teams are increasingly opting for independent SIEM solutions like Devo due to their flexibility and specialized capabilities, rather than relying on an end-to-end platform for all security needs. Devo's platform is particularly appealing because it is cloud-agnostic and maintains the data in its raw form for comprehensive analysis. The platform's low-code / no-code UI empowers SOC analysts across all skill levels with automation capabilities that span multiple cloud environments and endpoints, ensuring that performance is optimized based on the volume of data ingested.

However, adopting independent SIEM solutions like Devo presents certain challenges. Starting with managing single-threaded log forwarders / relays, moving data from customer's cloud to Devo's cloud incurs additional data transfer charges, and the data volume-based pricing model can significantly impact the overall ROI for executives. This model may lead to increased costs, particularly when data volumes are large. Furthermore, customers often lack the flexibility to fork data based on its relevance to different downstream systems, which can affect the precision and effectiveness of security operations.

To mitigate these issues, integrating a security data fabric solution is crucial. It complements the autonomous SOC capabilities offered by Devo, allowing for the efficient management of data costs by filtering out unnecessary data. Moreover, it grants customers the flexibility to manage their data across any platform of their choice, enhancing both data autonomy and operational efficiency within the modern cybersecurity landscape.

The Solution

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



DataBahn helps Devo SIEM deployments by streamlining data collection and ingestion and removing the onus of your team having to manage log collection infrastructure, build out custom integrations and spend cloud data egress costs incurred by sending logs from your cloud sources and applications into your Devo SIEM.

Through DataBahn's native capabilities, Security teams can:

- **Simplify data collection and ingestion into Devo**
  - Using DataBahn's plug-and-play integrations and connectors with a wide array of products and devices
  - Using DataBahn's native streaming integration for a hassle-free, real-time data ingestion into your Devo SIEM, eliminating any additional log collection infrastructure in your network
  - By effectively normalizing and structuring complex data formats like nested JSON, multi-line logs using DataBahn's orchestration pipelines before the data is delivered to Devo
- **Send only security-relevant data to your Devo SIEM**
  - Use DataBahn's out-of-the-box library of context-aware volume reduction rule sets helping you achieve more than 45% data volume reduction
  - Use DataBahn's purpose-built micro-analyzers, reduce cloud data egress charges for any log sources onboarded into Devo from your cloud / multi-cloud environments
- **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 Amazon Security Lake reducing both the volume and the overall time for queries to execute
- **Increase overall data governance and data quality**
  - Identify and isolate sensitive data sets in transit thereby limiting exposure
- **Perform split-second threat hunting**
  - Use DataBahn's indicator index to extract insights such as Security Observables (IP addresses, Domains, URLs, Hashes), Entity Relationships (Processes, Network execution, Registry modifications), and Intel Context to compliment Devo's hyperstream technology
  - Use 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**
  - Leverage DataBahn's simplified data orchestration capabilities, Devo customers can use additional tools to implement a cyber mesh architecture without having to worry about locking your data within your vendor cloud
  - Taking advantage of DataBahn's multi-formal and multi-data model support for consistent query experience across different downstream systems
- **Get visibility into the health of telemetry generation**
  - By using the dynamic device inventory generated by DataBahn to keep track of devices to identify unexpected silences, log outages, and detecting any other upstream telemetry blind spots
- **Reduce overall costs of your Devo SIEM deployment**
  - 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 and keeping a copy of your logs using Data Highway to low-cost storage infrastructure such as your cloud storage (S3 / Blob / GCP storage) or your data lakes such as Snowflake, AWS while adhering to the same data models to access them only when the need arises.

Benefits of using DataBahn

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 ensures that your team doesn't have to worry about single points of failures or managing occasional data volume bursts - the data collection never stops.

Reduced Costs

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

Orchestrate data based on relevance

DataBahn helps tier data based on its relevance so you can put purpose to your data and send security relevant data to Devo while the rest can be sent to infrastructure or platforms of your choice for threat hunting or compliance

Enrichment against Multiple Contexts

Enrich data against various contexts including Threat Intelligence, User, Asset, and Geo-location, providing a contextualised view of the data for precise threat identification.

Flexibility to your data stores

Leverage the combined power of DataBahn and Amazon Security Lake to gain the freedom to choose from the OCSF enabled tools and services that meet their needs without having to reformat their own.

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 Devo and other services.

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 to augment your security operations

Schema drift

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

Sensitive Data Detection

Identify, isolate, and mask sensitive data to ensure data security, governance, and compliance.

Risk-free data sharing internally and externally

Use DataBahn to fork out data streams to different services beyond the Devo SIEM to provide the flexibility your teams need, so they can bring in any tool of their choice

With DataBahn and Devo, elevate your Autonomous SOC operations by unlocking the power of your data through selectively processing and retaining relevant data, reducing unnecessary data transfer and storage costs. By filtering out non-essential data, DataBahn's Security Data Fabric enhances Devo's performance, ensuring resources are used only for high-value operations. Moreover, this integration offers the flexibility to handle data across multiple platforms, improving the precision of security operations and empowering organizations to leverage Devo's robust SOC capabilities more effectively. This strategic approach not only controls costs but also significantly boosts the effectiveness of security measures, aligning with the needs of dynamic cybersecurity landscapes.

ABOUT DATABAHN

DataBahn.ai's Data Fabric empowers organizations to optimize data management, reduce costs, and enhance security and IT operations. By integrating AI readiness, addressing IT observability challenges, and offering flexible solutions, the platform delivers significant operational efficiencies and strategic benefits, setting a new benchmark for cybersecurity data management in the digital age.

Learn more at **databahn.ai**

DATABAHN