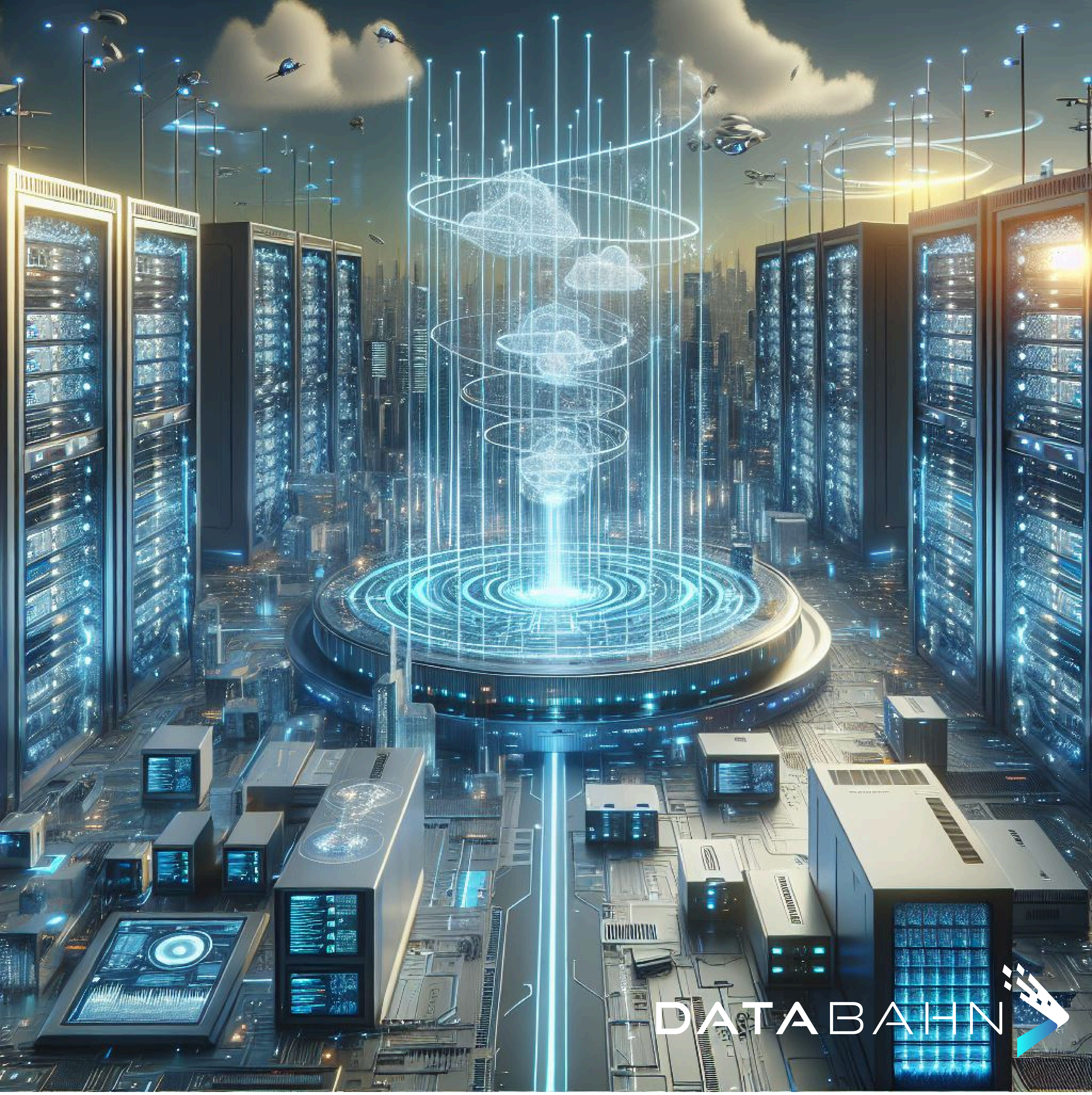


SOLUTION BRIEF

Centralize your Security Data in Amazon Security Data Lake using DataBahn's Security Data Fabric

Copyright © 2024, **Databahn**. All rights reserved

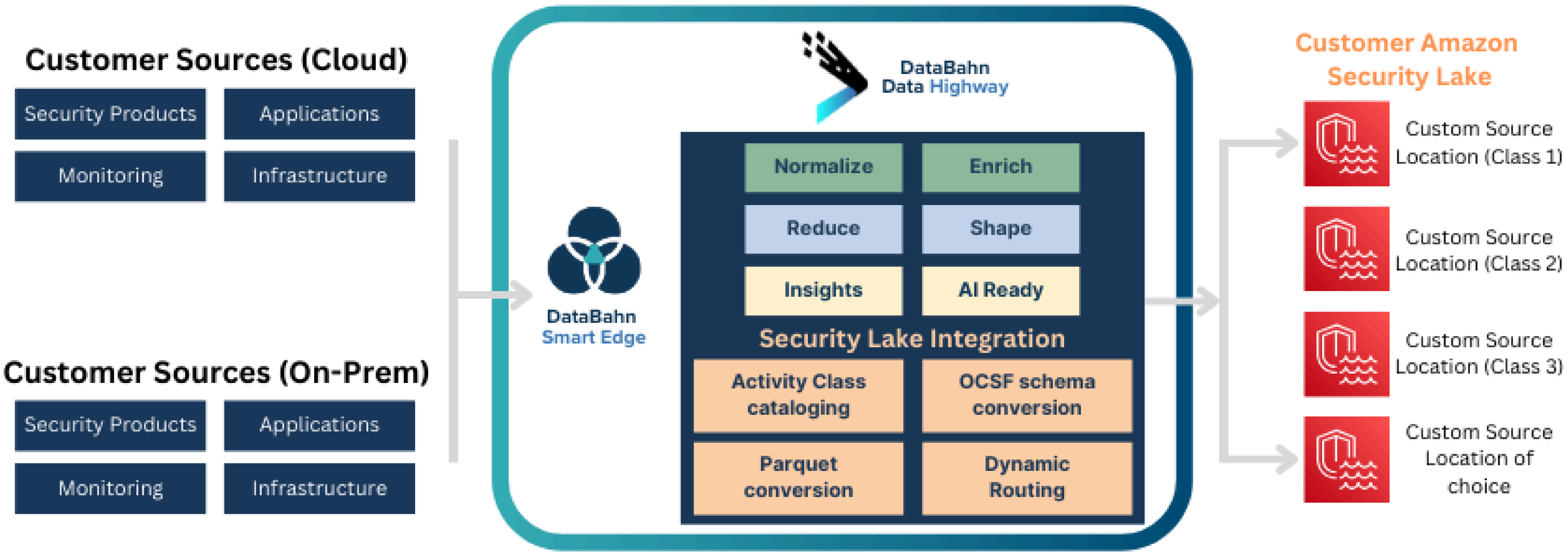
DataBahn + Amazon Security Data Lake

Many security teams are opting to build their own data lakes using Amazon Security Lake, a decision driven by the need for greater control and flexibility over their security data. This trend addresses key challenges that enterprises face with cloud SIEM vendors, notably the issues of data lock-in and limited tool integration flexibility.

Amazon Security Lake serves as a centralized hub for security data from a variety of sources, including AWS environments, SaaS providers, on-premises data centers, and other cloud platforms. By aggregating data into a single, purpose-built data lake stored within the user's own AWS account, it facilitates a more comprehensive understanding of security data across the entire organization. The adoption of the Open Cybersecurity Schema Framework (OCSF) by Security Lake allows for the normalization and amalgamation of security data, which is crucial for consistent analysis and monitoring.

One of the primary benefits of using Amazon Security Lake is its ability to centralize petabytes of data from diverse sources directly into Amazon S3 buckets. This capability allows security teams to utilize their preferred tools for security analytics, ensuring that they are not restricted to the tools provided by traditional SIEM vendors. By hosting their own data lake on AWS, organizations avoid the pitfalls of vendor lock-in and gain the ability to introduce or change analytical tools as their security needs evolve or as better technologies emerge. The flexibility to control and analyze security data without being tied to the limitations of specific vendor ecosystems makes Amazon Security Lake a compelling choice for organizations aiming to enhance their security posture while maintaining the agility to adapt to new threats and technologies. This approach not only streamlines security operations but also empowers teams to focus on more strategic security initiatives.

AWS Partners and customers can leverage DataBahn's Security Data Fabric to accelerate the onboarding of data from various third-party sources. This rapid integration enhances visibility across security and operational environments, helping to safeguard workloads, applications, and data more effectively.



The Solution

DataBahn's purpose-built Smart Edge along with the Data Highway platform provides AWS customers with the flexibility to select from an array of OCSF-enabled tools and services that best meet their needs, without the hassle of manually reformatting data. This capability enables teams to analyze security data from endpoints, networks, applications, and cloud sources in a standardized format. Quick identification and response to security events are facilitated, empowering organizations with enhanced access controls, cost-efficient data storage, and regulatory compliance.

DataBahn simplifies the process of enriching and shaping raw data from third-party sources to meet the specifications of Amazon Security Lake's Parquet Schema. This transformation is facilitated by a repeatable process that minimizes the need for modifications, making data integration seamless and efficient.

Through DataBahn's Orchestration capabilities, customers using AWS security lake can:

- **Simplify data collection and ingestion into Snowflake**
    - Using DataBahn's plug-and-play integrations and connectors with a wide array of products and devices, both cloud and non-cloud
    - Using DataBahn's native streaming integration for a hassle-free, real-time data ingestion into AWS Security Lake without the need of any manual reformatting or code
    - By effectively normalizing and structuring data using DataBahn's orchestration pipelines before the data is loaded into Amazon Security Lake tables
- **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 set in transit thereby limiting exposure
- **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

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.

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.

WIZ
okta
salesforce
JUNIPER NETWORKS
IBM

Automated OCSF Conversion

DataBahn's Security Fabric supports automated conversion of security logs into OCSF, formatting and partitioning the data according to the requirements of Amazon Security Lake in parquet schema.

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.

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.

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.

Security teams routinely contend with the issue of handling increasingly large data volumes trapped in a variety of vendor-specific formats, complicating the processes of data integration and transformation for use with appropriate security tools. With DataBahn and Amazon Security Lake, unlock the power of your security data by maximizing the value while reducing the overhead effort it takes to collect, ingest, process, store, and make the data available for any consumer. DataBahn's purpose-built data collection and orchestration platform enables your teams to worry less about data acquisition into Amazon Security Lake.

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