databahn.ai

DATA SHEET

DATABAHN DATA FABRIC *NextGen Security Data Fabric*

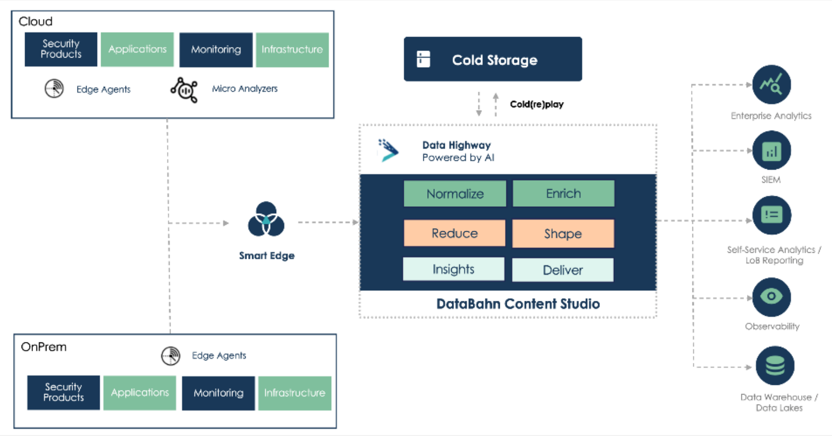
Simplify Ingestion | Reduce Cost | Get Insights and Preventive Controls | Make Data AI Ready

Join the Security Data Revolution!

The ever-evolving realm of cybersecurity presents a pressing challenge: the exponentially growing "cybersecurity haystack" (i.e data) overshadowing the search for needles (i.e threats). Traditional SIEM tools, designed for a different era, grapple with scalability, soaring data storage costs, and data silos. As new solutions continue to identify threats effectively, the root issue remains unaddressed – the ever-expanding haystack.

The challenge of efficiently integrating a myriad of products and devices continues to increase every SOC team's dependency on the SIEM. Though, Data warehouses are more tailor-made to solve the Volume, Velocity, Variety challenges, they expect organizations to bring the data into their platforms which is a distraction to many SOC teams.

Introducing DataBahn, a cutting-edge platform that revolutionizes security data ingestion. DataBahn seamlessly ingests data from multiple feeds, aggregates, compresses, reduces, and intelligently routes it. With advanced capabilities, it standardizes, enriches, correlates, and normalizes the data before transferring a comprehensive time-series dataset to your data lake, SIEM, UEBA, AI/ML, or any downstream platform. DataBahn empowers organizations to efficiently manage their data pipeline with enhanced efficiency and accuracy.



Why DataBahn?

Highly Scalable to meet Modern Day Data Demands

Simplify data management complexities using Purpose built data collection nodes to natively handle data volume spikes guaranteeing uninterrupted processing and continuous resilience.

Reduce your platform costs

Unlock value from your cyber data by revamping your traditional data architecture by efficiently collecting, normalizing, and enriching data from diverse sources, ensuring that only relevant and purposeful data is sent to your SIEM keeping the costs in check.

Get your data AI ready for the future

Harness the power of AI by transforming your data to be ready for AI . Revolutionize SOC operations by enhancing threat detection, speeding up incident response, and optimizing resource utilization, ultimately fortifying cybersecurity measures.

For more information about the DataBahn platform, request a demo at https://databahn.ai/

Security Data Management

- 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.
- Threat Research Enabled Filtering Rules
  Pre-configured filtering rules, underpinned by comprehensive threat research, guarantee a minimum volume reduction of 35%, enhancing data relevance for analysis.
- 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 popular data formats like CIM, OCSF, CEF, and others, facilitating faster downstream onboarding. It intelligently monitors log schema changes for proactive adaptability.

Security Data Governance

- Schema Drift
  Detect changes to log schema intelligently for proactive adaptability.
- Sensitive data detection
  Identify, isolate and mask sensitive data ensuring data security and compliance.
- Continuous Support for New Event Types
  DataBahn provides continuous support for new and unparsed event types, ensuring consistent data processing and adaptability to evolving data sources.

Security Data Insights

DataBahn offers continuous ML and AI powered insights and recommendations on the data collected to unlock maximum visibility and ROI.

Indicator Index

DataBahn accelerates threat hunting, allowing SOC teams to swiftly detect and respond to potential threats by extracting insights from key attributes. Drastically reduces time, enabling SOC teams to respond swiftly to potential threats and vulnerabilities.

Device Inventory

DataBahn creates a comprehensive inventory of devices, highlighting silent devices, non-compliant devices for your teams to quickly identify and isolate devices that have gone silent

Security Posture Management

DataBahn offers a unified view of logs collected powered by ML/AI-powered insights on telemetry blind spots for effective threat detection and hunting and increasing your overall threat detection

BYO-Security Data Lake

- Data Engine to power your data lakes to consolidate telemetry from cloud/on-prem sources
- Cloud agnostic deployment design, data planes can be hosted on any cloud or on-premise
- Destination agnostic – Supports any data lake of your choice
- Native data segregation pipelines to route security relevant, compliance, observables and insights into different tables
- Design pipelines to support use cases for AI – generate embeddings, insights, mask/redact sensitive information