DATA SHEET

DATABAHN SECURITY DATA FABRIC

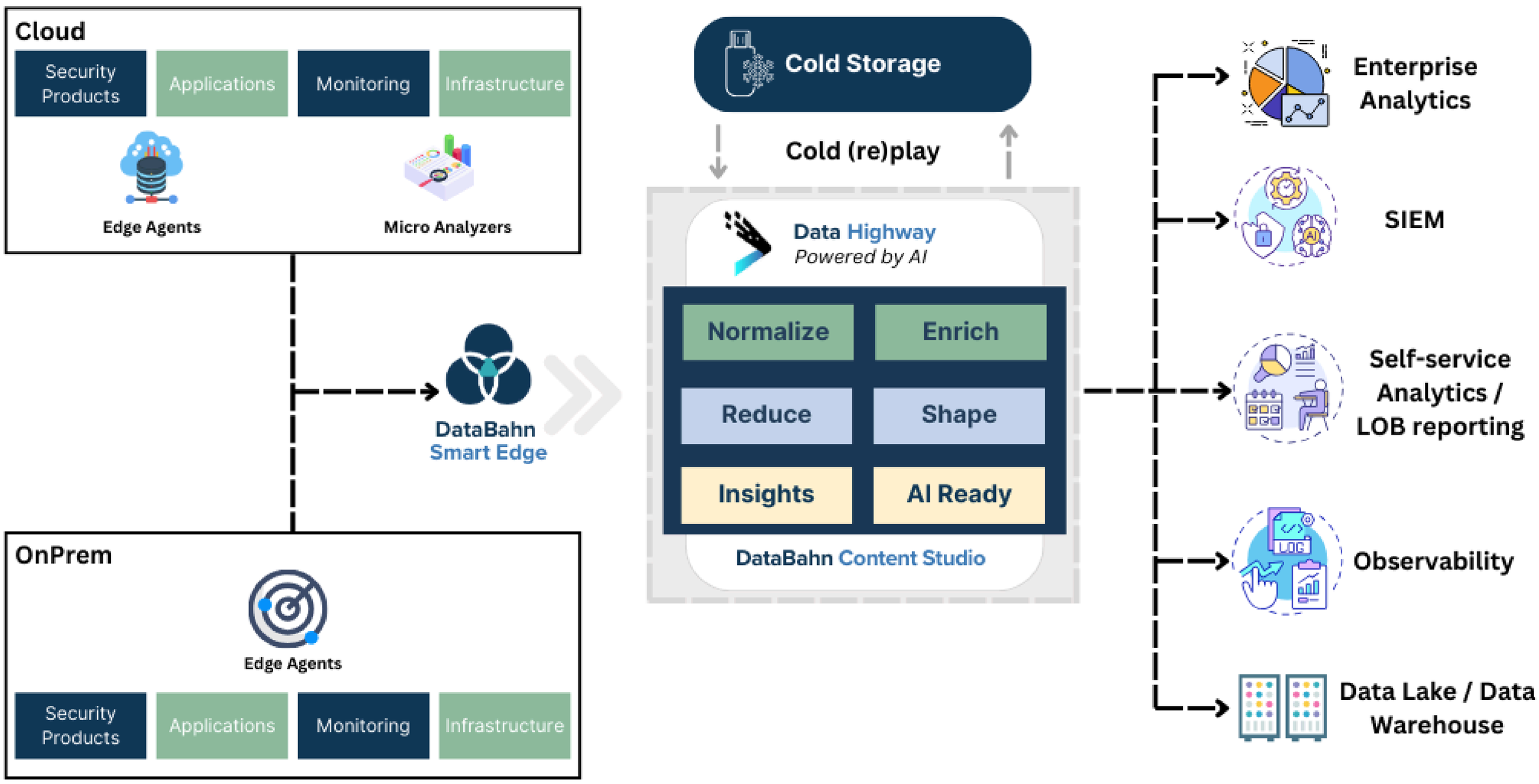
Simplify Ingestion | Reduce Cost | Get Insights & Preventive Controls | Make data AI ready

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 growth in security data volume, cybersecurity’s 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. While Data Warehouses are better suited to solve the Volume, Velocity, and Variety challenges of security data, SOCs are expected to bring the data into their platforms which is a distraction and takes up considerable bandwidth.

Introducing **DataBahn**, a cutting-edge platform which revolutionizes security data ingestion. DataBahn seamlessly ingests data from multiple feeds and then 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 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.

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. It drastically reduces time to detect threats, enabling SOC teams to respond swiftly to potential 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 AI / ML-powered insights on telemetry blindspots 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-generated embeddings, insights, mask / redact sensitive information

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