SOLUTION BRIEF

DataBahn for Retail Services

Lower your SIEM and compliance costs while keeping full visibility across every store and channel, with DataBahn's Agentic Data Control Plane

DATABAHN

AGENTIC DATA CONTROL PLANE

Move. Detect. Search

Current Situation

Retail regulators and card networks everywhere are converging on the same ask: evidence, not promises. PCI DSS 4.0, state breach-notification laws, and GDPR all expect you to show what you monitor across every store and channel. Attackers know where the gap is. They're increasingly targeting point-of-sale systems and eCommerce platforms directly, since a breach during peak season costs more by the hour than almost any other kind of incident, and a single breach can run into the tens of millions. It comes back to one question: which telemetry actually reaches your SIEM. DataBahn built the Agentic Data Control Plane to answer that, so your SOC gets the right data, in the right format, with the noise removed, and no manual data engineering behind it.

Regulators already expect this

Retail now sits alongside finance and healthcare as a top target for data-driven attacks. Rules differ by card network and region, but PCI DSS 4.0 and similar frameworks all converge on the same ask: show what you monitor, and show it fast after an incident.

Your POS and eCommerce telemetry never reaches a detection tool

POS terminals, payment gateways, inventory systems, and eCommerce platforms run high volume in proprietary or vendor-specific formats with no native connector.

Attackers are targeting checkout and inventory systems

Ransomware and payment-skimming groups target retailers more than almost any other sector, because a breach during a peak sales event costs more by the hour than most other kinds of incidents. A single breach can run into the tens of millions and take weeks to fully contain.

Your daily ingest cap is making your coverage decisions

When ingest hits the licence cap, someone picks which sources to stop collecting, on cost, not risk. Teams hold back EDR, DNS, WAF, and OT, the sources they need most.

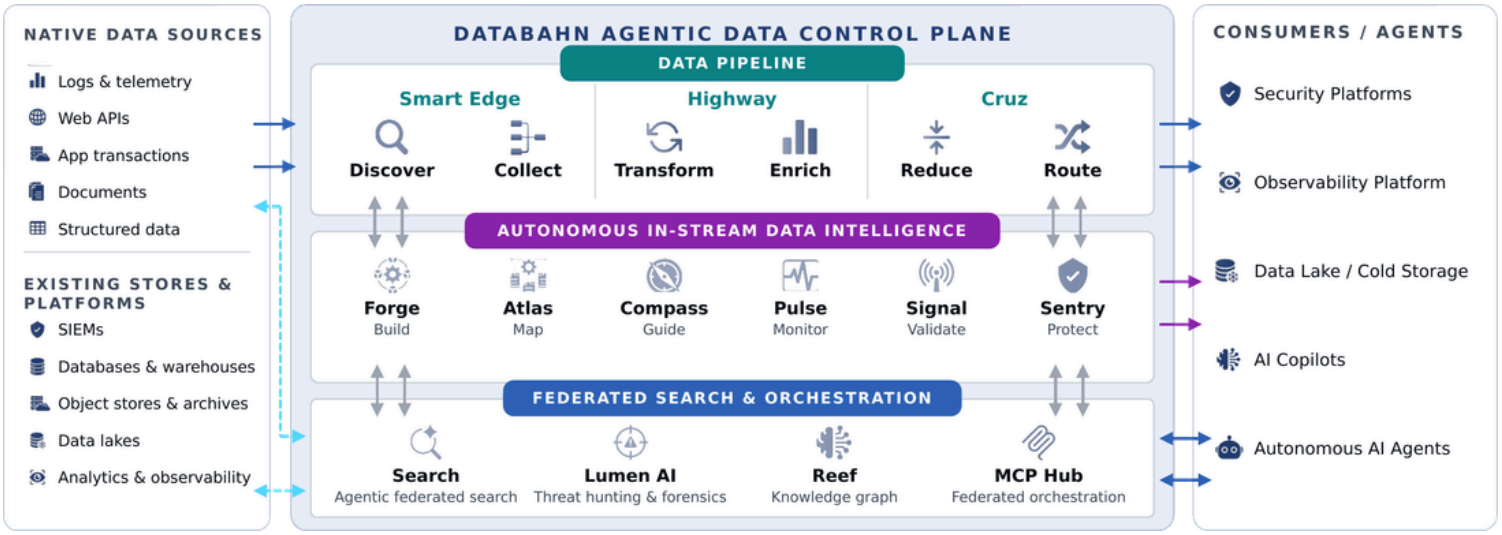
DataBahn for Retail Services

Attackers are reaching shoppers through payment processors, POS vendors, and eCommerce platform suppliers. Each breach comes back to the same question: which telemetry reaches your SIEM. DataBahn sits between your sources and your SIEM, data lake, and compliance archive.

Data Pipeline collects from POS terminals, payment gateways, and eCommerce platforms while AIDI parses and normalizes that telemetry, masks sensitive fields, and maps every source to MITRE ATT&CK.

Federated Search & Orchestration also lets you query everything else, wherever it lives, without moving it first. With these capabilities, your team stops guessing which sources to drop when the ingest cap hits, and stops losing coverage to a supplier's silent format change.

Architecture



DataBahn Key Features

1. Faster onboarding, less engineering
Draw on 700+ prebuilt connectors and auto-generated parsers to bring a new application or data source online in hours, not months.

2. Lower costs without losing coverage
980+ context-aware reduction rules, tuned by purpose-built data engineering agents that cut ingestion as much as 70% within weeks while keeping the fields your detections and auditors actually need.

3. Compliance built into the pipeline
Databahn agents find and mask PII, PHI, and cardholder data in motion. That satisfies SOX, PCI-DSS, and GDPR before the data reaches a downstream system.

4. Full visibility and lineage
Databahn agents auto-discover every data source and flag the ones that go silent or drift. Auditors get a traceable record from source to destination.

5. An architecture that survives change
Data Pipeline keeps collecting through outages and traffic spikes. Swap or add a SIEM, lake, or archive later without rebuilding anything upstream.

6. Investigations across every store
Search, Lumen AI, and Reef query the SIEM, data lake, and cold storage together, in plain language without any delay or rehydration job.

Why Retail services choose DataBahn

- **80% faster onboarding.** 700+ prebuilt integrations and AI-generated parsers connect security, observability, and IoT/OT sources with no custom development.
- **Up to 70% volume reduction.** Events are restructured, not dropped, so coverage stays intact. Proven in a no-risk POC on your own data.
- **40% faster investigations.** One query spans SIEM, lake, and cold storage, with no tool pivoting or manual rehydration.
- **Automatic schema drift remediation.** Source schema changes are detected and mappings fixed before a detection goes dark.
- **Up to 90% faster MTTD.** Quick Signals generate alerts in the stream, cutting up to 40 minutes detection time while SIEM waits to index and correlate data.
- **80-90% of detections caught pre-index.** Detections run in the stream, catching issues before data ever lands in the SIEM.
- **100% of configured PII masked in-stream.** Hashing, tokenization, or redaction at the source keeps raw PII away from downstream tools and models.

See it with your own data

Schedule a personalized demo and we'll walk through your pipeline's health score, live, so you can see exactly how Pulse surfaces failures in your environment.

DataBahn is the agentic data control plane for the enterprise. Its platform ingests, normalizes, enriches, governs and routes telemetry from 700+ sources with complete data and AI neutrality: any source, any destination, any model, no vendor lock-in, at Fortune 100 scale. DataBahn is headquartered in Dallas and serves Fortune 500 enterprises.

Learn more at **databahn.ai**