SOLUTION BRIEF

DataBahn for Heathcare and Pharma

Collect your clinical and lab telemetry without buying more SIEM capacity with DataBahn's Agentic Data Control Plane

DATABAHN

AGENTIC DATA CONTROL PLANE

Move. Detect. Search

Current Situation

Healthcare regulators everywhere are converging on the same ask: evidence, not promises. HIPAA in the US, NIS2 in the EU, and similar frameworks across the UK, Australia, and Asia all expect you to show what you monitor. Attackers know where the gap is. They're reaching patients through pathology, patient-record, and packaging suppliers, and a single supplier 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

Healthcare now sit alongside energy and finance as critical infrastructure in major markets. Rules differ by region, but all converge on the same ask: show what you monitor and show it fast after an incident.

Attackers are going through your suppliers

A pathology supplier, a patient-record vendor, and a drug-packaging manufacturer were each hit by ransomware within the last two years. Three different suppliers, the same gap each time.

Your clinical and lab telemetry never reaches a detection tool

Lab systems, PACS and imaging, infusion pumps, HL7 interface engines, and pharma line systems (DCS, MES, batch) run high volume in proprietary formats with no vendor connector.

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.

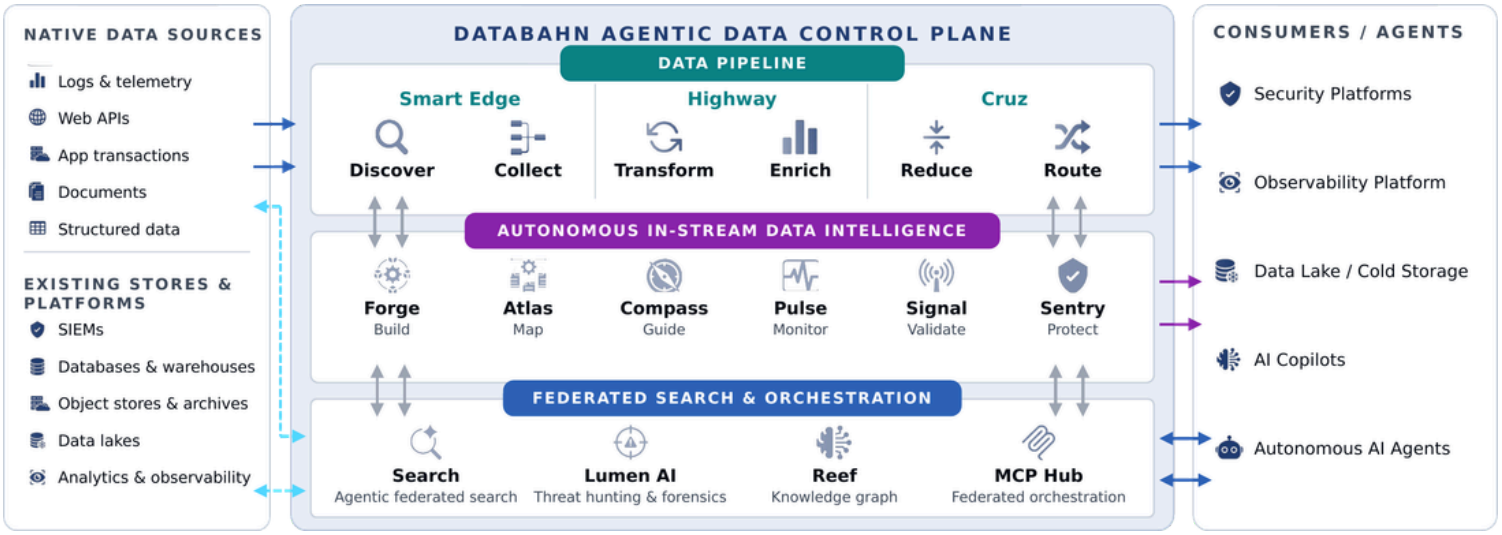
DataBahn for Healthcare and Pharma

Attackers are reaching patients through pathology, patient-record, and packaging 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 lab systems, medical devices, and pharma manufacturing lines 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 Healthcare and Pharma choose DataBahn

65%	5 Days	7 hours	4 months
Average SIEM cost reduction	Average time to deploy	Average time to implement	Average payback

- **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**