DataBahn for Google SecOps

Enable value-driven orchestration using DataBahn’s Security Data Fabric for your Google SecOps deployment

DATABAHN

DataBahn + Google SecOps

As organizations seek to fortify their cybersecurity defenses, the integration of Security Information and Event Management (SIEM) systems like Google SecOps (formerly known as Chronicle) becomes critical. Customers prefer Google SecOps for its powerful analytics and AI capabilities, which enhance threat detection and response. Its integration with Google Cloud Platform offers unparalleled scalability and data processing speeds. Additionally, its ability to handle massive volumes of data efficiently and provide real-time security insights helps organizations stay ahead of evolving cybersecurity threats, making Google SecOps a preferred solution for companies seeking robust and a scalable SIEM. While SecOps' previous pricing model, based on user-based pricing rather than data volume, made it an attractive choice for businesses of all sizes, the recent shift to the data volume-based model has made the overall ROI on the SIEM less attractive. Managing SecOps can present numerous challenges, particularly in data collection, orchestration, and cost management.

Organizations leveraging Google SecOps encounter several operational challenges:

Infrastructure Management

Customers are responsible for setting up servers, syslog forwarders, and to set up collectors for each non-Google source integrated, along with securing these logs staging machines and managing their volume and scalability.

Data Segregation

There is no native capability to define what data is sent to Google SecOps versus stored in cloud storage, leading to inefficiencies in data management.

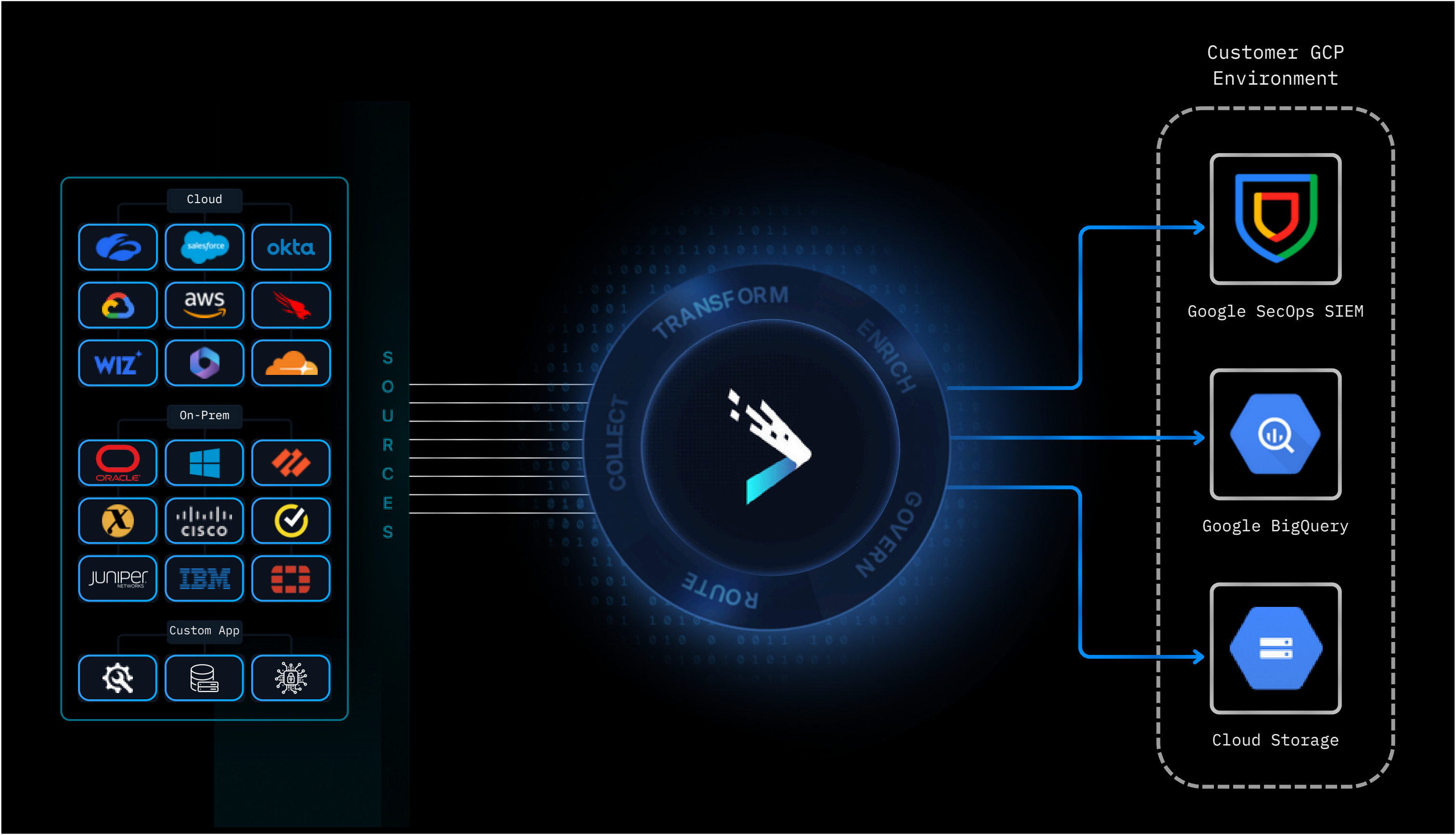
Cost Control

The absence of mechanisms to enforce spending limits, particularly with non-Google sources, can lead to unexpected expenses. The shift from user to ingest-based pricing exacerbates this, potentially making Google SecOps deployments less cost-effective over time.

Data Utilization

Customers lack the flexibility to fork data based on its relevance to different downstream systems, affecting the precision of security operations.

The Solution



DataBahn's Security Data Fabric with its purpose-built Smart Edge along with the Data Highway products can take data from a wide range of sources (both Google and non-Google sources), parse and structure them into the native Google UDM format, enrich data with any meaningful context (internal and external context), orchestrate the data to extract meaningful insights and deliver security relevant data and insights into your Google SecOps for optimal querying, analytics, and search.

DataBahn's Security Data Fabric helps Google SecOps deployments by streamlining data collection and ingestion and removing the onus of your team having to build custom integrations, deploying your staging locations to publish data from third party products and services into your Google SecOps.

DataBahn's orchestration engine gives SOC and SecOps teams full control over their data, from ingestion to enrichment to storage, without the overhead of custom builds.

1. Simplify Data Ingestion
Ingest telemetry from hundreds of products and devices, including non-Google sources, using DataBahn's plug-and-play connectors. Native streaming integration enables real-time ingestion into Google SecOps with zero added infrastructure. All data is automatically normalized and structured to match native and UDM schemas for seamless downstream use.

2. Send Only What Matters
DataBahn's prebuilt, context-aware reduction rules help reduce more than 35% data volume in just weeks. This lowers cost while ensuring that security-relevant logs continue to flow to your SIEM.

3. Turn Logs into Insights
Noisy telemetry, such as NetFlow and network traffic, is automatically aggregated and suppressed to extract actionable insights. These compact records improve query performance in Google SecOps and reduce storage overhead.

4. Hunt Faster, Respond Smarter
DataBahn's Indicator Index extracts key observables like IPs, domains, and hashes, along with entity relationships across processes, registry activity, and network behavior. Enriched metadata such as first seen, last seen, and frequency supports faster threat exploration and investigation.

5. Improve Data Governance
Sensitive data in transit is identified and isolated to minimize exposure and enforce security controls early in the pipeline.

6. Build a Future-Ready Stack
DataBahn integrates cleanly with Google services such as BigQuery and Cloud Storage to support scalable, cost-efficient, and AI-ready security operations.

7. Monitor Telemetry Health in Real Time
A dynamic device inventory gives you visibility into upstream data generation. It flags silent endpoints, telemetry outages, and blind spots before they impact detection or coverage.

8. Reduce Total Cost of Ownership
Remove the need for staging infrastructure or custom connectors by using DataBahn's built-in integrations. Route low-priority or infrequently accessed data to lower-cost cloud-native storage like Google Cloud Storage, while maintaining schema consistency and full access when needed.

Why Security Teams Choose DataBahn

Plug-and-Play Integrations

Connect to 500+ tools and data sources instantly with out-of-the-box connectors—no custom engineering required.

Lower Costs, Higher ROI

Cut Sentinel costs by filtering out redundant and low-value logs using built-in volume reduction rules.

Always-On Data Collection

Smart Edge ensures uninterrupted collection, even during traffic spikes or outages, so your data never stops flowing.

Context-Rich Enrichment

Enrich logs with threat intel, user, asset, and geo-data to boost the precision of detections and investigations.

Targeted Data Delivery

Route only high-value, security-relevant data to Sentinel, and offload the rest to Azure Blob or ADX, reducing cost while preserving access.

Seamless Format + Schema Handling

Auto-adapt to schema changes and format variations to ensure consistent data quality with minimal overhead.

Sensitive Data Protection

Detect and isolate sensitive data in transit to strengthen compliance and reduce exposure risk.

DataBahn.ai is a leader in AI-driven Data Pipeline Management and Data Fabric solutions, helping organizations transform their data operations with innovative engineering and advanced analytics technologies. With its Data Fabric platform and cutting-edge AI capabilities, DagtaBahn.ai is committed to empowering organizations to harness the full potential of their data for a smarter, more connected future.

Learn more at **databahn.ai** | Check out our **LinkedIn**

DATABAHN