SOLUTION BRIEF

Enable value-driven data orchestration using DataBahn.ai's Security Data Fabric for your Google SecOps deployment

Google SecOps

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.

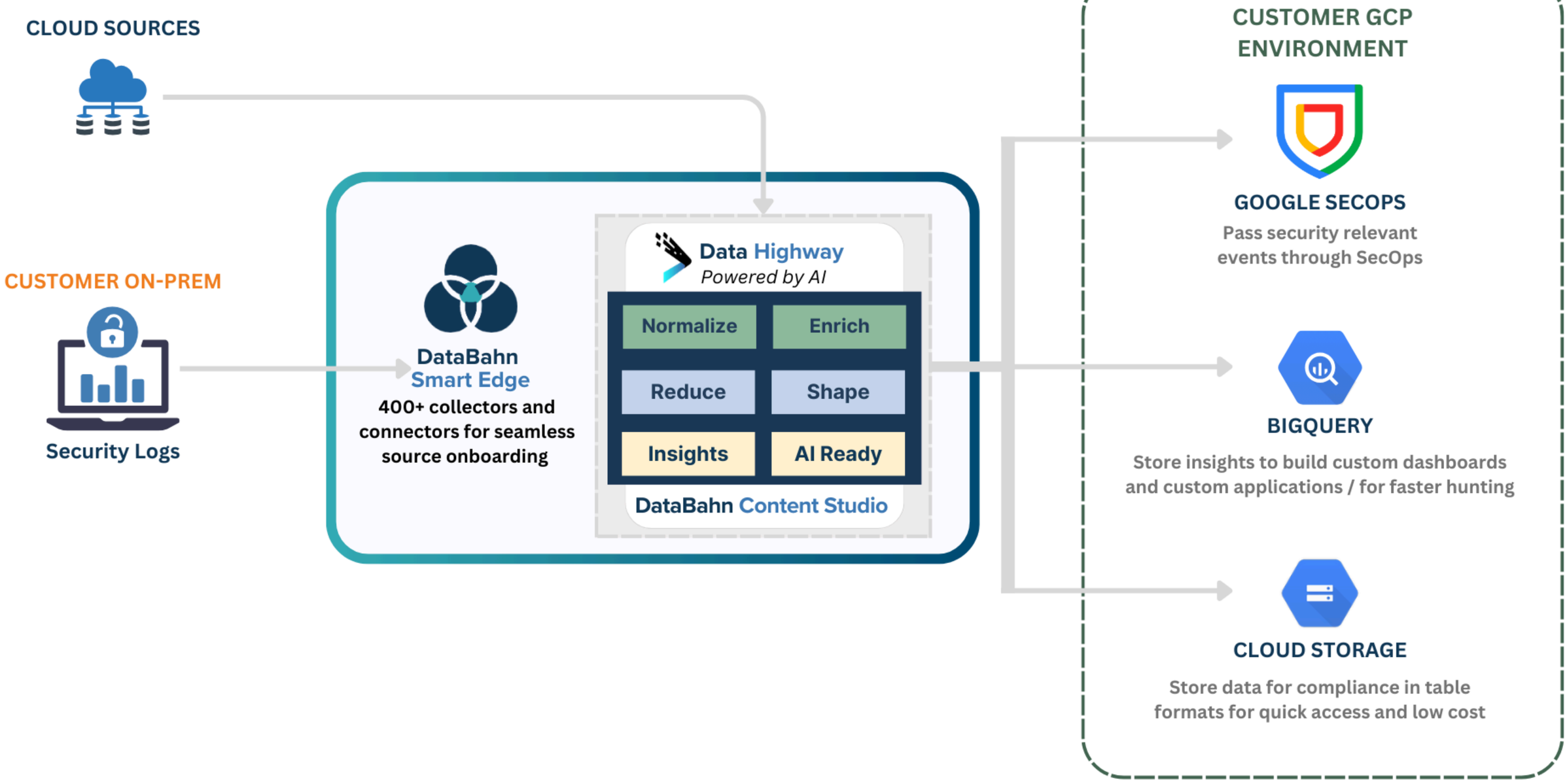
Data Utilization

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.



Through DataBahn's Orchestration capabilities, SOCs and Security Teams can:

- **Simplify data collection and ingestion into Google SecOps**
  - Using DataBahn's plug-and-play integrations and connectors with a wide array of products and devices including and beyond the Google ecosystem
  - Using DataBahn's native streaming integration for a hassle-free, real-time data ingestion into Google SecOps
  - Normalizing and structuring data to adhere to both native and Google's UDM formats
- **Send only security-relevant data to your Google SecOps by**
  - Using DataBahn's out-of-the-box library of context-aware volume reduction rule sets helps you achieve a >35% data volume reduction in 2-4 weeks
- **Convert logs into insights and perform split-second threat hunting**
  - Use volume reduction functions like aggregation and suppression to convert noisy logs like network traffic / flow into manageable insights that can be loaded in Google SecOps reducing both the volume and the overall time for queries to execute
- **Increase overall data governance and data quality by**
  - Identifying and isolating sensitive data sets in transit thereby limiting exposure
- **Perform split-second threat hunting**
  - Use DataBahn's Indicator Index to extract insights such as Security Observables (IP addresses, Domains, URLs, Hashes), Entity Relationships (Processes, Network execution, Registry modifications), Intel Context
  - By using additionally derived context such as first observed / last observed time / frequency of observation to speed up data exploration and hunting
- **Bring best of breed services and technologies**
  - Leverage DataBahn's simplified data orchestration capabilities, SecOps customers can use additional Google services such as BigQuery and Cloud Storage to implement both a cost-effective and future-ready security architecture

- **Get visibility into the health of telemetry generation by**
  - Using the dynamic device inventory generated by DataBahn to keep track of devices to identify unexpected silences, log outages, and detecting any other upstream telemetry blind spots
- **Reduce overall costs of your Google SecOps deployment by**
  - Removing the need for any staging locations or custom integrations by taking advantage of DataBahn's library of integrations and connectors
  - Routing less-frequently accessed data sets or less security-relevant data sets using Data Highway to low-cost cloud native storage while adhering to the same data models to access them only when the need arises, while still owning your data

Benefits of using DataBahn

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.

Reduced Costs

DataBahn enables your team to manage the overall costs of your SecOps deployment by providing a library of purpose-built volume reduction rules that can weed out redundant and less relevant logs.

Resilient data collection

DataBahn's highly resilient Smart Edge ensures that your team doesn't have to worry about single points of failures or managing occasional data volume bursts - the data collection never stops.

Relevance-based data orchestration

Tier and segment data based on relevance and send security-relevant data to SecOps while send the rest to your data lake or storage for threat hunting and compliance cases

Enrichment against Multiple Contexts

Enrich data against various contexts including Threat Intelligence, User, Asset, and Geo-location, providing a contextualised view of the data for precise threat identification

Format Conversion and Schema Monitoring

The platform supports seamless conversion into the UDM data model, native to SecOps, additionally facilitating flexible and faster downstream onboarding in Google SecOps

Risk-free data sharing

Use DataBahn to fork out data streams beyond SecOps in your Google Cloud Environments such as BigQuery or Cloud Storage for continuous compliance and to external destinations

Get your data AI-ready

DataBahn's AI-ready framework gets your data cleansed, enriched, feature extracted, and with embeddings generated to build AI-powered apps on top of your Google Cloud environment

Sensitive Data Detection

Identify, isolate, and mask sensitive data to ensure data security, governance, and compliance

Schema drift

Detect changes to log schema intelligently for proactive adaptability and to avoid downstream detection impact

DataBahn's Security Data Fabric empowers organizations to overcome the challenges of managing Google SecOps, optimizing both operational efficiency and cost-effectiveness. By focusing on the critical aspects of data collection and orchestration, our solution ensures that businesses can leverage SecOps' powerful capabilities while maintaining control over their cybersecurity expenditures and data management processes.

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