DATABAHN

SOLUTION BRIEF

Enabling an AI-driven SOC of tomorrow with DataBahn.ai’s Security Data Fabric for your XSIAM

paloalto NETWORKS | CORTEX XSIAM™

DataBahn + Palo Alto XSIAM

Customers are choosing Palo Alto XSIAM for their SIEM and SOC needs due to its comprehensive and centralized platform that unites XDR, SOAR, ASM, and SIEM capabilities. This eliminates the inefficiencies of console switching and streamlines security operations. By automating security tasks, XSIAM reduces the manual work while accelerating incident response, and enhance remediation efforts before analysts even engage. As a cloud-delivered, integrated SOC platform, Cortex XSIAM consolidates key functions such as EDR, XDR, SOAR, ASM, UEBA, TIP, and SIEM into a single, cost-effective solution. This not only improves operations and increases analyst productivity but also provides an intelligent data foundation that easily integrates telemetry from any source, ensuring unified security operations across hybrid IT architectures.

That said, while Palo Alto XSIAM offers many promising benefits, there are also some challenges to consider.

Third-Party Coverage and Parsing

Coverage for connecting and parsing third-party log sources, i.e., sources non-native to Palo Alto, is limited. This leads to significant additional time and effort from the security team to integrate such sources.

Infrastructure Management

Customers of XSIAM are responsible for setting up servers, syslog forwarders, and working with Palo Alto Networks (“PANW”) to set up collectors for each non-PANW native source (i.e., 3rd party log source) integrated. Managing this infrastructure also includes 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 XSIAM versus stored in cloud storage, leading to inefficiencies and higher costs in data management.

Cost Control

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

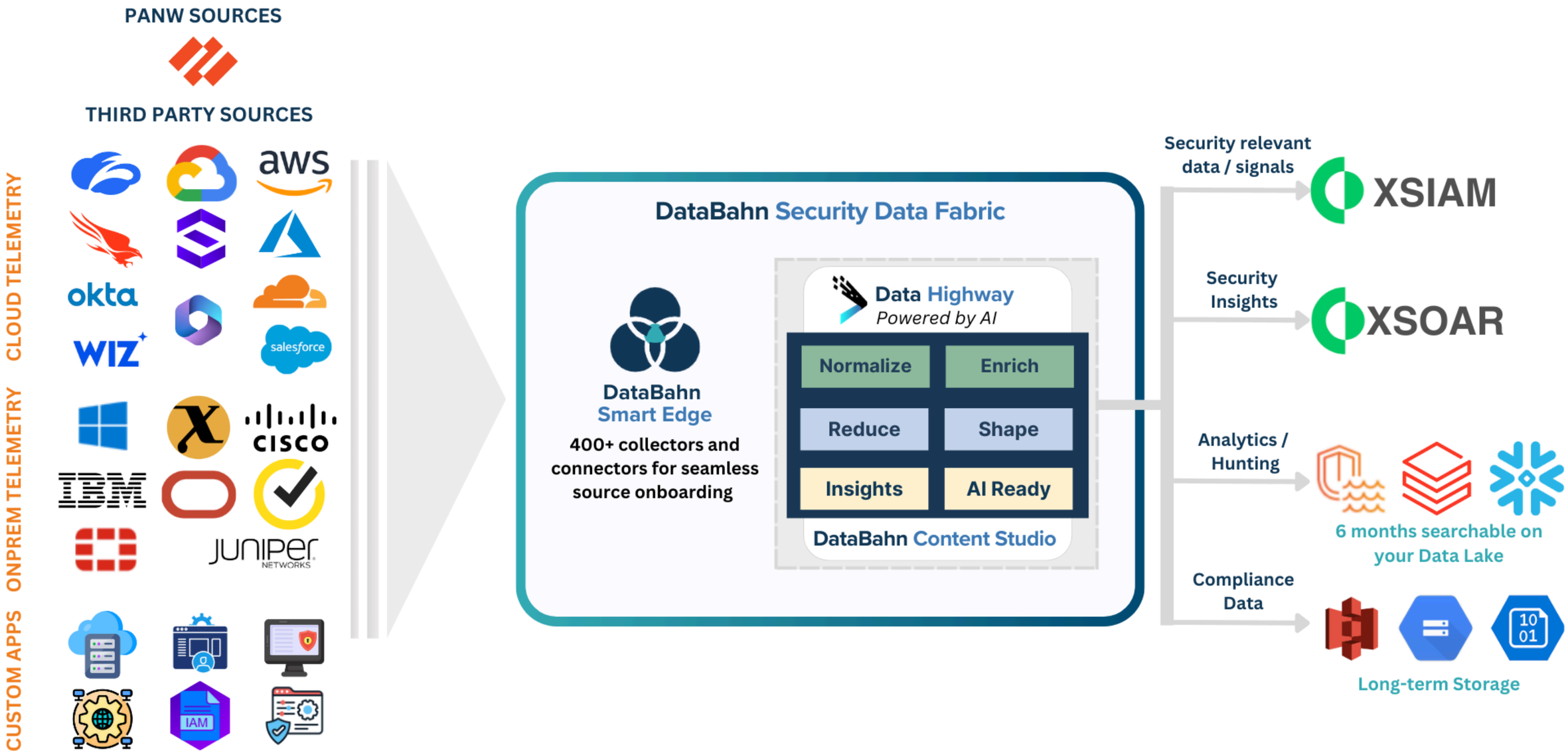
Data Utilization

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 and Data Highway solutions can:

- Seamlessly ingest data from a wide range of sources (native and non-PANW sources such as on-premise and cloud infrastructure, security products and applications)
- Normalize and enrich this data with internal and external contextual data sources
- Orchestrate the data to extract meaningful insights, and
- Deliver security-relevant data and insights into your XSIAM platform for optimal querying, analytics, and search



DataBahn's Security Data Fabric helps XSIAM deployments by streamlining data collection and ingestion while removing the onus of your team to have to build custom integrations or deploy staging locations to publish data from third party products and services into the XSIAM SIEM.

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

- **Simplify data collection and ingestion into XSIAM by**
  - Using DataBahn's plug-and-play integrations and connectors with a wide array of products and devices including and beyond the PANW ecosystem
  - Using DataBahn's native streaming integration for a hassle-free, real-time data ingestion into XSIAM
- **Send only security-relevant data to your XSIAM SIEM 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 XSIAM reducing both the volume and the overall time for queries to execute.
  - 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
  - Using additionally derived context such as first observed / last observed time / frequency of observation to speed up data exploration and hunting
- **Increase overall data governance and data quality by**
  - Identifying and isolating sensitive data sets in transit thereby limiting exposure
  - Create metrics from logs without introducing code changes

    - Aggregate metrics on critical tags
    - Time-bound proliferation and suppression for emergency situations
    - Maintain raw data for past insights
- **Get visibility into the health of telemetry generation by**
    - Using the dynamic device inventory generated by DataBahn to keep track of devices and endpoints to identify devices that have gone silent, log outages, and detecting any other upstream telemetry blind spots
- **Reduce overall costs of your XSIAM SIEM 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 XSIAM 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 XSIAM while sending 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 any data model of your choice, facilitating flexible and faster downstream onboarding in XSIAM

Schema drift

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

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

Sensitive Data Detection

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

Risk-free data sharing

Use DataBahn to fork out data streams beyond XSIAM in your cloud and to external destinations

DataBahn's Security Data Fabric empowers organizations to overcome the challenges of managing PANW XSIAM SIEM, 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 XSIAM's powerful capabilities while maintaining control over their cybersecurity expenditures.

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