SOLUTION BRIEF

Empowering an AI-driven SOC of tomorrow with DataBahn.ai's Security Data Fabric for QRadar Deployments

DataBahn + QRadar

QRadar, a legacy Security Incident and Event Management (SIEM) solution, has been trusted by a wide range of enterprises and SMBs since its on-premise days for its comprehensive threat detection, threat hunting, and alerting capabilities. Over time, QRadar has evolved to include QRadar on Cloud (WROC), extending its trusted SIEM functionalities to cloud. While QRadar has offered many promising benefits, there are some challenges to consider.

Data Volume Management and License Constraints

QRadar SIEM, like many legacy systems, uses an events per second (EPS) licensing model. This licensing approach makes it challenging to scale the platform and manage data volume as customers approach their license limits. Additionally, QRadar often struggles with data bursts, a common issue with cybersecurity logs. When license limits are exceeded, QRadar collectors may drop events which lead to gaps in data coverage.

Rigid Onboarding Options

QRadar administrators frequently need to navigate various protocols and develop or customize Device Support Modules (DSMs) for unsupported products or custom application logs. This process is time-consuming and complex, particularly when onboarding new or non-standard data sources. Incoming data must conform to a predefined schema based on the LEEF format. Any attempt to reformat events or reduce their size could disrupt the correlation rules within the QRadar Event Processor

(In)Flexible Security Stack

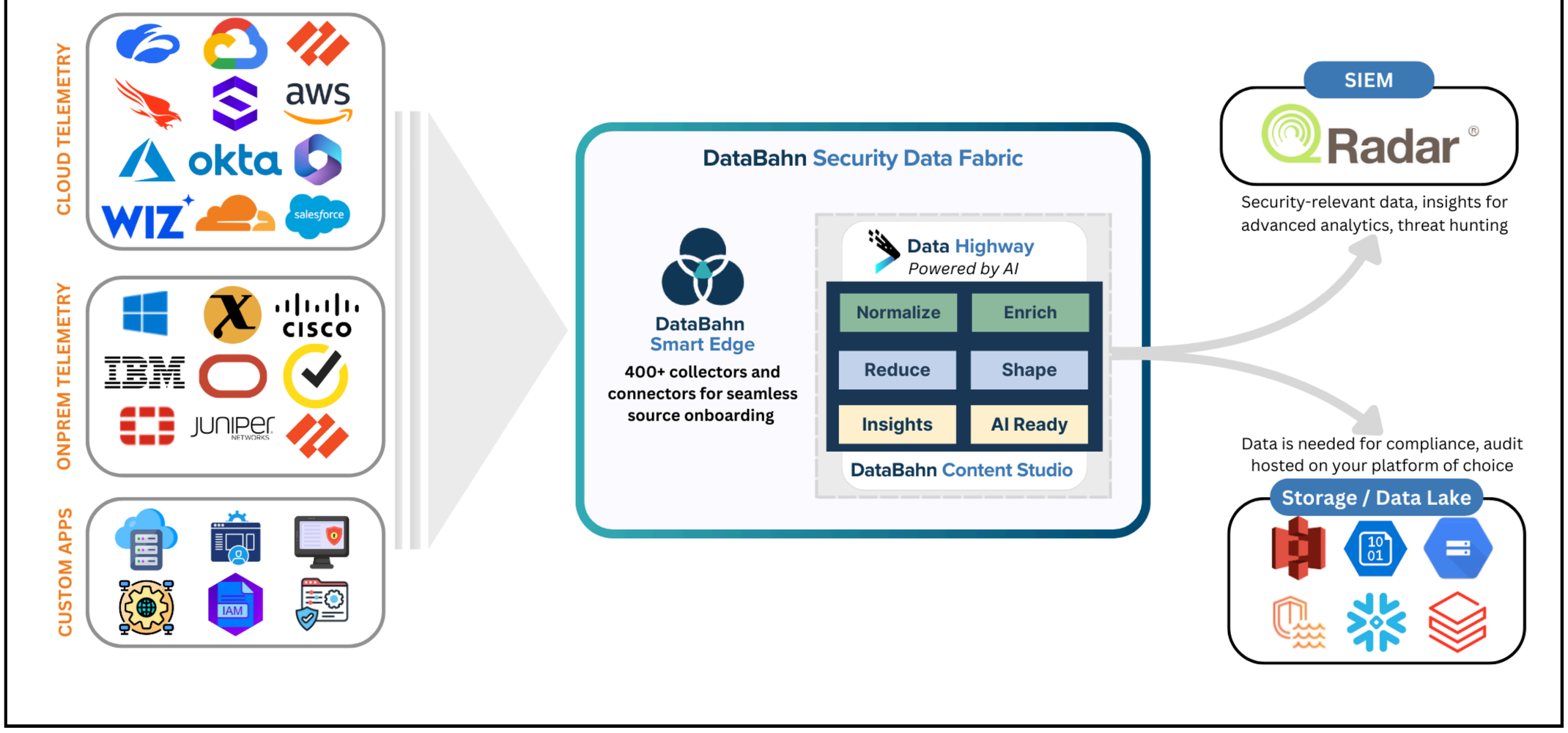
Organizations using QRadar face limitations when integrating the platform with non-native tools. For those with a flexible security stack that includes data lakes, cold storage for retention, and custom analytics, balancing those solutions can complicate integration efforts. Ensuring seamless operation and comprehensive security coverage requires meticulous coordination.

Historical Data Access

Accessing or restoring archived data in QRadar can be slow and cumbersome. This can significantly hinder compliance efforts and investigations, especially when dealing with threats that extend back several months.

The Solution

DataBahn's Security Data Fabric with its purpose-built Smart Edge along with Data Highway solutions can take data from a wide range of sources, such as on-premise and cloud infrastructure, security products and applications, normalize and enrich data with any meaningful context (internal and external), orchestrate the data to extract meaningful insights and deliver security relevant data and insights into your QRadar platform for optimal querying, analytics and search. DataBahn's Security Data Fabric helps QRadar deployments by streamlining data collection and ingestion and removing the onus of your team having to build custom integrations, write or manage DSMs from your QRadar SIEM.



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

- **Simplify data collection and ingestion into QRadar by**
  - Using DataBahn's plug-and-play integrations and connectors with a wide array of products and devices including and beyond the QRadar supported ecosystem
  - Using DataBahn's native streaming integration with LEEF schema support for a hassle-free, real-time data ingestion into QRadar without needing to update existing parsers or rewriting new DSMs
- **Send only security-relevant data to your QRadar 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
- **Flexibly manage data volume by**
  - Using volume reduction functions like aggregation and suppression to convert noisy logs like network traffic / flow into manageable insights that can be loaded in QRadar 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 set in transit thereby limiting exposure
  - Quickly identifying changes to data schema or data formats for log feeds to provide the necessary corrections needed to avoid security coverage or posture impact for your security teams in QRadar
- **Perform split-second threat hunting by**
  - Using 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
- **Get visibility into the health of telemetry generation by**
  - Using the dynamic device inventory generated by DataBahn to keep track of devices to identify devices that have gone silent, log outages, and detecting any other upstream telemetry blind spots
- **Reduce overall costs of your QRadar SIEM deployment by**
  - 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 QRadar 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 QRadar while send the rest to your data lake or storage for threat hunting and compliance cases

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 QRadar in your cloud and to external destinations

DataBahn's Security Data Fabric empowers organizations to overcome the challenges of managing QRadar 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 QRadar'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