

DATA SHEET

BLUSAPPHIRE: SECURE DATA LAKE

CHALLENGES

In the current cybersecurity landscape, a stark reality becomes evident: an astounding 70% of data ingested by Security Information and Event Management (SIEM) systems is virtually redundant. This goes beyond mere inefficiency and poses a critical flaw in the cybersecurity strategies of many organisations. It resembles an oversized, sluggish entity overwhelmed with unnecessary information, depleting resources and burdening organizations with exorbitant licensing costs.

Instead of vigilant guardians, SIEM systems often transform into bloated, expensive data repositories with limited practical value. The ever-increasing complexity of cybersecurity threats presents a significant challenge for security teams. Therefore, organisation's ability to effectively manage and analyse the growing volume of alerts, events, and data is being put to the ultimate test.

Organizations face the complex challenge of balancing their data requirements for robust protection against cyber threats with their budget constraints. Historically, data lakes have been difficult to manage and maintain, often requiring dedicated teams. The intricacy of working with data lakes has discouraged their adoption. However, the need for advanced data analytics to extract actionable insights for proactive measures conflicts with financial limitations, resulting in a critical dilemma.

The exponential growth in data generated from various sources, coupled with the expanding attack surface, has amplified the strain on security infrastructures. Teams are under immense pressure to streamline processes and implement efficient big data management methodologies to effectively harness this wealth of information without exceeding financial constraints and disrupting existing security operational procedures.

SOLUTION

BluSapphire's Revolutionary Security Data Lake solution represents a game-changing leap towards cost-effective yet robust cybersecurity data infrastructure for businesses. By seamlessly integrating Smart Data Ingestion capabilities, it offers an holistic shield against emerging threats while significantly trimming expenses.

The Security Data Lake's core functionality lies in its ingenious ability to intelligently filter, condense, and eliminate duplicate data, effectively slashing storage and processing overheads. Its Scalable Architecture stands as a testament to long-term viability, accommodating an organisation's security growth trajectory without incurring exorbitant expenses and also not disturbing your current business processes aligned with your SIEM.

Harnessing the power of BluSapphire's Security Data Lake empowers organisations to streamline their security data management, resulting in substantial cost reductions associated with SIEM Ops, cloud services, and data storage. This streamlined approach not only cuts expenses but also supercharges overall operational efficiency, making it an indispensable asset in the cybersecurity arsenal of any forward-thinking enterprise.

KEY BENEFITS

Organisations reported an average cost savings of 62% upon adopting a Secure Data Lake.

Seamless plug-and-play solution that enhances your existing cybersecurity infrastructure without causing disruption. No impact on existing business processes, no retraining of current SOC staff.

Improved Security Observability; Speed up cross-domain threat analysis, investigation, and hunting tasks with lightning fast unlimited storage & analytics.

Improve response times for sophisticated cyber-attacks by utilizing precise insights into an attacker's operational patterns.

Achieve regulatory compliance while minimizing costs and future-proofing your organization.

BUSINESS OUTCOMES LIKE NEVER BEFORE!

Transition seamlessly into optimized security data management with the integration of BluSapphire's Secure Data Lake. This cutting-edge solution eliminates the disruption to existing tools such as SIEM deployed and the need for retraining of your Security Operations Center (SOC) staff, while ensuring there is no compromise on business processes. With our plug-and-play approach, your existing cybersecurity infrastructure is now enhanced.

BluSapphire's Secure Data Lake offers a transformative approach by diverting surplus data before it enters your SIEM systems, resulting in a dramatic reduction in SIEM licensing costs and associated operational expenses.

Now, Leverage the power of Secure Data Analytics coupled with AI-driven BluSapphire Threat Detection, Response automation, say goodbye to limitations and embrace the ability to address complex use cases enabling mitigation of complex malicious signals early and prevent sophisticated breaches.

SEAMLESS INTEGRATION, EFFICIENT OPERATIONS

Bridge data silos by utilizing open and common data schemas to effectively aggregate and normalize information. This enables seamless decision-making and facilitates quicker incident response.

When it comes to third-party integration, it's important to remember that there's more to it than just log ingestion. To achieve high efficiency and effectiveness with your data, it's crucial to consider aspects around data transformation, analytics, visualization, and more. By taking a comprehensive Secure Data Lake approach, you can generate amazing outcomes for your business in terms of cost saving, seamless analytics, robust threat detection.

BluSapphire utilizes Secure Data lake which operates on common data schemas, making it easy to integrate with third-party components and bridge siloes. This means that only a minimal amount of integration is required to ensure that all components are operating at full effectiveness. By streamlining processes and improving data flow, BluSapphire offers considerable operational efficiency benefits for your organization.

LIGHTNING FAST QUERIES, HASSLE FREE DATA MANAGEMENT

Unlimited Hot Storage

Data retention policies often involve the simple aging out of older data. However, BluSapphire stands out with its unique compaction algorithm that applies aging based on data importance. This allows for the aggregation of data and prioritizes context over fidelity, resulting in reduced data size while ensuring the ability to address key questions. Say goodbye to concerns about data retention and extraction costs. Safely store and retain your data in your Amazon S3 or Azure Blob instances should you decide to archive a data set.

Robust Observability: Threat Hunt, Detection, Analytics, Incident Response

Enriching data with user, asset, and threat intelligence context is a widely adopted practice that is commonly implemented across various solutions. Similarly, the execution of detection content, such as sigma rules, is frequently performed multiple times. By shifting the execution of detection content to the data lake, data can be processed in a cost-effective manner, ensuring consistently available enriched real-time data analytics for workloads. With an innovative data architecture, the ability to query petabytes of data and achieve desired outcomes within seconds becomes a reality. Threat hunting on large data sets with complex queries becomes a definite possibility. Expedite the triage of complex malicious signals, empowering Incident Response teams with precise data-driven context to effectively mitigate breaches.

Compliance & Reporting

Numerous industries adhere to rigorous regulatory mandates concerning data security and privacy. A security data lake can effectively address these compliance reporting requirements by offering robust data governance capabilities.

OPERATIONAL BENEFITS

Optimized Data Ingestion:

Enhance data channel efficiency, reduce data duplication to save costs, and unlock the full potential of previously constrained SIEM use cases.

Unlimited Hot Storage:

Say goodbye to storage limitations and data archival constraints.

Harness the potential of unlimited queries and analytics to empower security teams. Strengthen threat hunting capabilities and effectively counter sophisticated attackers with powerful analytics and precise queries.

Optimize incident response efficiency:

Enhance context through data-driven decision-making, facilitating precise and targeted incident response.