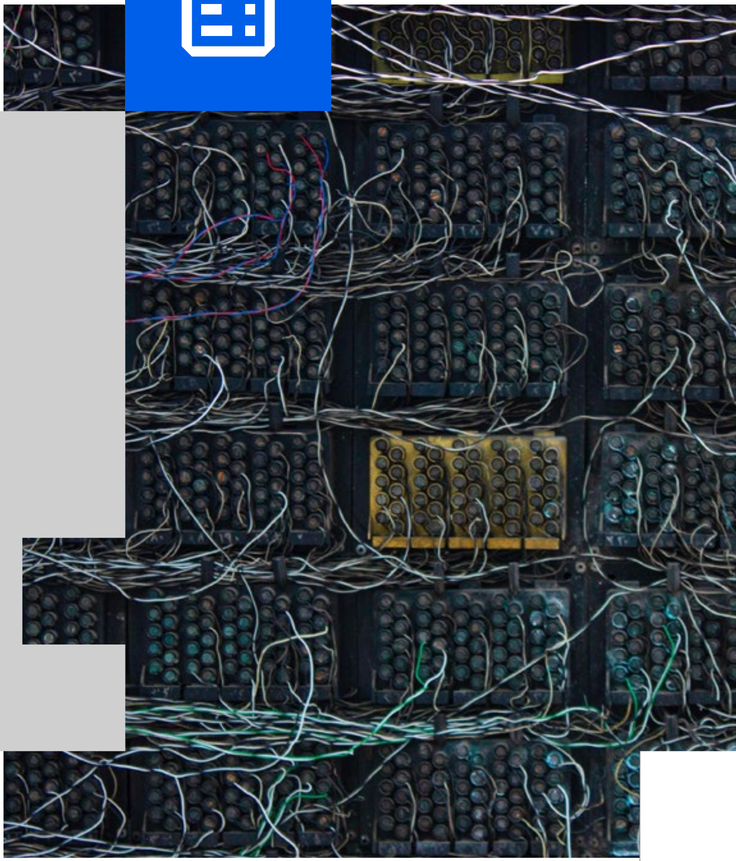
exabeam

Data Sheet

Exabeam Data Lake

Lightning-Fast Search for Security Data



Log Management for the Modern Network

Log management is a fundamental component of a strong enterprise security architecture. It supports security intelligence and analytics, as well as compliance and forensics reporting. The good news is that the log management process is mature and well-understood. Yet legacy vendors have not kept pace with rapid changes in data growth, cloud architectures, and open source big data management.

Log Search Shouldn't be Painful

Exabeam Data Lake is built on top of Elasticsearch, a foundation of proven, scalable open source big data technology. Exabeam adds enterprise features such as remote collection agent management and security data enrichment, and packages the solution for easy deployment and operations. Creating a thoroughly modern log management solution.

Additionally, Data Lake natively integrates with the entire suite of analytics and automation solutions available from Exabeam to ensure your team is as efficient and effective as possible.

Key Benefits

- Natural language querying, with context enhanced parsing and data presentation to improve analyst productivity
- Compliance reporting utilizing hundreds of prebuilt templates help easily display adherence with regulatory requirements
- Guided search enables SOC analysts of all levels to easily find the right answers to their security, risk, and compliance questions
- Rapid search times make SOC analysts more productive in their day-to-day activities

How it Works

Exabeam Data Lake involves three main processes:

01 Log collection

02 Log parsing, enrichment, ingestion, and indexing

03 Data presentation (searching, visualizing, reporting, dashboards, etc)

It allows for large scale aggregation and storage of logs from the servers, applications, databases, network devices and virtual machines that make up your IT infrastructure and provides access to those logs via a web interface. Additionally Exabeam Data Lake enriches log events with contextual information. As data travels from the source, Exabeam Data Lake parses each event, identifies named fields to build structure, and transforms them to converge on a common format for easier, accelerated analysis and business value.

Exabeam Security Management Platform

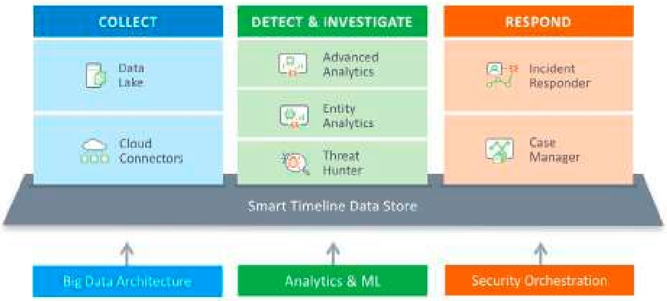
Exabeam's modular offerings can be mix-and-matched according to your organization's specific needs. Whether you're looking for a full SIEM replacement, or to enhance your current setup incrementally by augmenting it with improved threat detection, more cost effective logging, and improved productivity, we can help. The Exabeam platform includes:

- Data Lake
- Cloud Connectors
- Advanced Analytics
- Entity Analytics
- Threat Hunter
- Case Manager
- Incident Responder

Key Features

Exabeam provides world class threat detection, prioritizes analyst workloads, and greatly improves SOC productivity. Key features of Exabeam Data Lake include:

- Out-of-the-box (OOTB) parsers for 500+ security and identity products Full indexing of logs at point of ingestion, ensures results returned faster than many competitive solutions
- Context-Aware log parsing and presentation
- Highly scalable, centralized, log storage
- Federated Search, allows for searches across highly distributed global enterprise environments using a single query
- Guided Search, eliminates the need to learn any additional coding languages
- Natural Language-Based Rule Builder, enables even the most junior analyst to craft complex and effective rules
- Hundreds of OOTB compliance reports to fulfill audit and regulatory requirements



To learn more about how Exabeam can help you visit exabeam.com today.