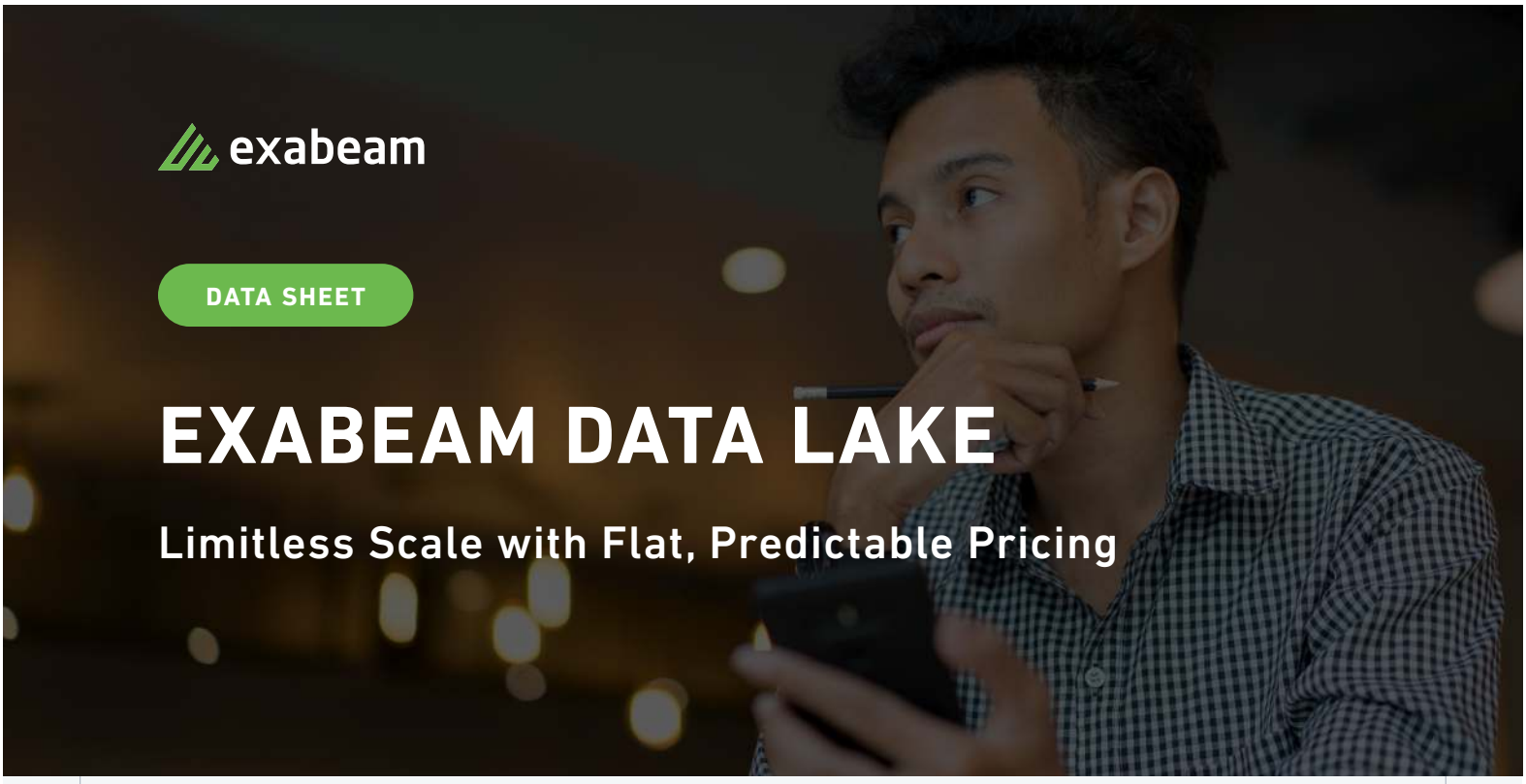

exabeam

DATA SHEET

# EXABEAM DATA LAKE

## Limitless Scale with Flat, Predictable Pricing

**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. Even worse, these systems are licensed "by the byte," becoming more expensive every year as data grows, requiring CISOs to dispense more of their budget for no associated gain.

Exabeam Data Lake is different. It's designed for the modern world, with a scale-out architecture that can support any volume of data, and for a predictable price.

**LOG STORAGE SHOULD BE PREDICTABLE**

Unlike other log management products, Exabeam Data Lake is licensed in a predictable, per-user model so that you can capture as much data as you need for reporting and analytics. Want to add your EDR or DLP data into your log system? How about your network data? If you tried that with another product, the additional bills would quickly drain your budget. With Exabeam Data Lake, there is no charge for extra data, so you can finally log and analyze anything necessary to detect and respond to modern threats.

**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.

## HOW IT WORKS

Exabeam Data Lake involves three main processes:

1. Log collection
2. Log parsing, enrichment, ingestion, and indexing
3. 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.

## KEY FEATURES

Exabeam provides world class threat detection, prioritizes analyst workloads, and greatly improves SOC productivity.

Key features of Exabeam Data Lake include:

- Pricing based per user. Not per byte
- Out-of-the-box (OOTB) parsers for 750+ 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
- Over 70 OOTB compliance reports to fulfill audit and regulatory requirements.

## KEY BENEFITS

- Unlimited logging at a predictable price, enabling organizations to log all of their security data without exhausting their budgets
- Natural language querying, with context enhanced parsing and data presentation to improve analyst productivity
- Competent compliance reporting utilizing hundreds of prebuilt templates

## 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


**TO LEARN MORE ABOUT HOW EXABEAM CAN HELP YOU, VISIT EXABEAM.COM TODAY.**