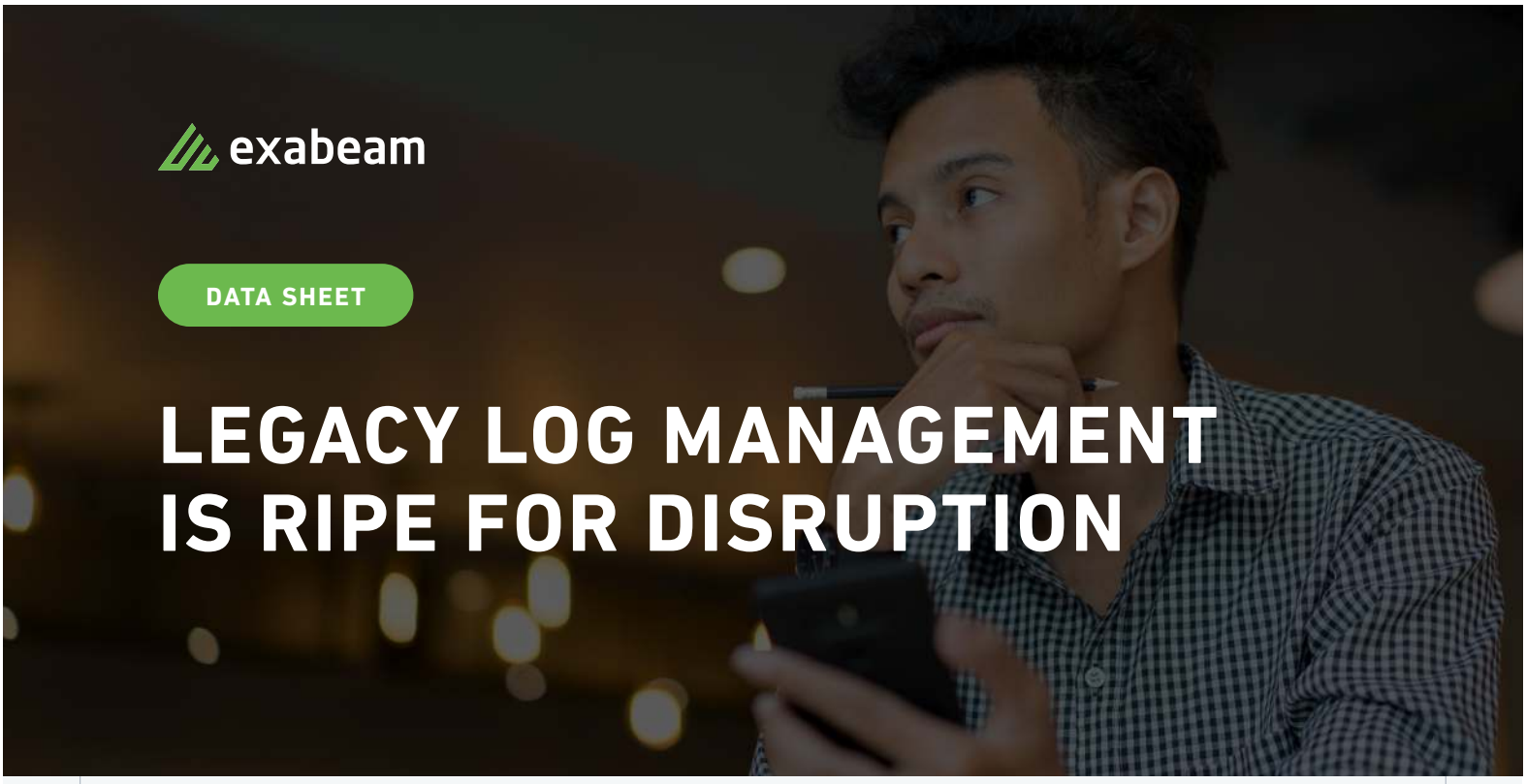

exabeam

DATA SHEET

LEGACY LOG MANAGEMENT IS RIPE FOR DISRUPTION

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. The bad news is that log management vendors have not kept pace with rapid changes in data growth, cloud architectures, and open source big data management. Log management systems are now measured in petabytes, with data streaming in from internal networks and the cloud. Legacy log management systems simply weren't designed for such an environment. Even worse, these systems are licensed "by the byte," becoming more expensive every year as data grows and requiring CISOs to plunk down 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 SEARCH SHOULDN'T BE PAINFUL

Exabeam Data Lake is built on a foundation of proven, scalable open source big data technology, including HDFS and Elastic- search. Many Web-scale companies rely on these technologies today to support the massive data volumes they generate.

HDFS is tailor-made for analytics and Elasticsearch is perfect for time series data management. Exabeam Data Lake integrates these technologies with others in the Elasticsearch stack to create a thoroughly modern log management solution.

Exabeam adds enterprise features such as remote collection agent management and security data enrichment to these technologies, and packages the solution for easy deployment and operations.

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 data management has become commoditized through the use of excellent open source technologies. Exabeam offers a petabyte-scale system that extends these proven building blocks.

KEY FEATURES

Exabeam provides world class threat detection, prioritizes analyst workloads, and greatly improves SOC productivity. Its key features include:

- Web-scale aggregation of log data
- Scale-out multi-node architecture
- Guaranteed at-least-once data delivery
- Search, dashboards and reporting
- Ability to enrich log events with unique security stateful context and Host-To-IP awareness
- Remote Management of agent based collectors, including update and stop/start
- User interface optimized for security analysis and reporting
- Ease of setup and use
- RESTful API
- Out of the box parsers for 750+ security and identity products
- Interoperability with any UEBA system
- Ability to deploy as a pre-sized physical appliances or as a cloud-ready VM

OPERATING INFORMATION

- Deployable as a physical appliance (in multiple sizes) or as a cloud-ready virtual machine
- Includes out of the box collection agents and parsers for over 500 security data sources
- Agents operate on Windows of Linux Platforms

EXABEAM SECURITY MANAGEMENT PLATFORM

Data Lake is a key component of the 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 platform includes:

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

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