# Exabeam Security Log Management

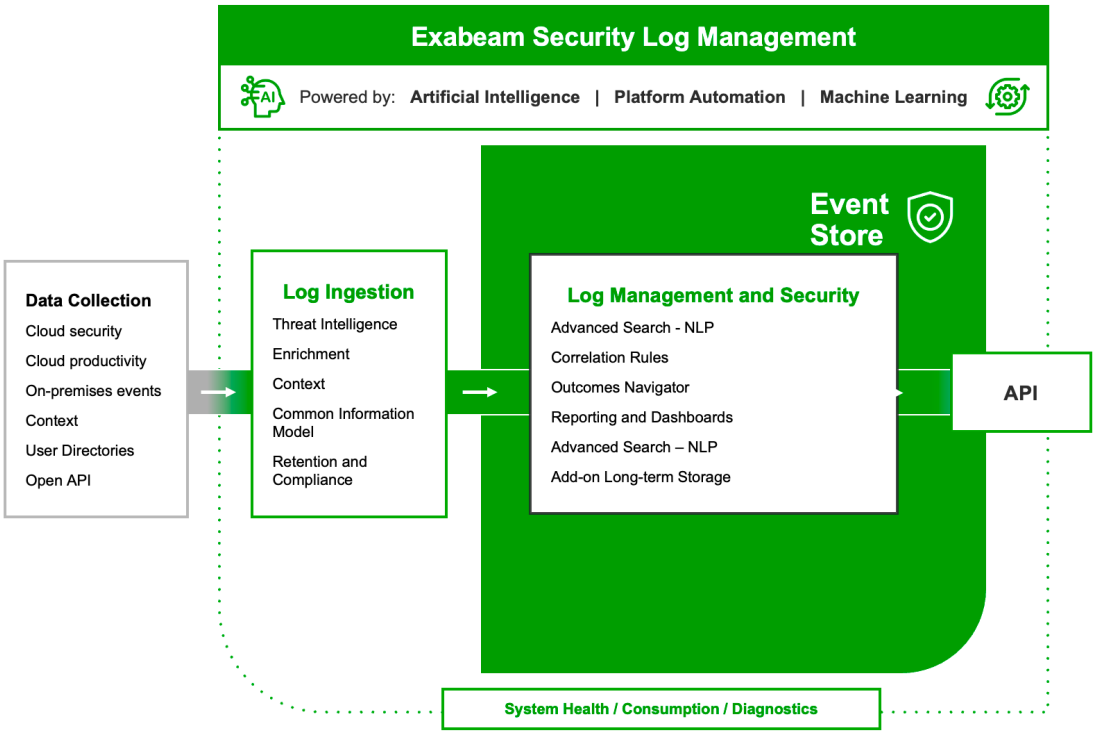
Cloud-scale log management to ingest, parse, store, and search log data with powerful dashboarding and event correlation

Critical to every enterprise strategy is the ability to record and search security events that occur within an IT environment. Detailed records of events or log files provide security teams with an audit trail to monitor activity within an IT environment that may signal issues like policy violations, abnormal activity, or security incidents. Logged data must be monitored and analyzed, and critical events investigated. Searching, analyzing, and storing these logs is critical, but not without its challenges; the flow of data is continuous and voluminous, often impacting system performance.

Security logs are generated by a wide variety of vendors, devices, and applications, from firewalls to servers and intrusion detection and prevention systems — which lack a uniform format to easily search and read. Consequently, modern log management solutions must make it easy to deploy, ingest, store, and process logs from multiple sources, whether on-premises or in the cloud. These solutions must parse and retrieve data quickly from terabytes or petabytes of data and return search results rapidly.

## Cloud-scale security log management

Exabeam Security Log Management is a cloud-native solution for log collection, storage, and analysis. Built to support security use cases, Security Log Management is the entry point to ingest, store, report, and analyze security data for your organization in one place, providing a fast, modern search and dashboarding experience across multi-year data. Deployed quickly and easily, Exabeam Security Log Management has the flexibility to scale with your needs.




## Cloud-native architecture to ingest, parse, enrich, store, and search on more data, everywhere

From endpoint to cloud and everything in between, your organization's data is everywhere. Exabeam Security Log Management provides highly scalable, centralized storage and rapid, intelligent search capabilities for complete visibility across your entire ecosystem. Exabeam Security Log Management also enriches ingested data and events with its pre-built threat OEM and open source intelligence feeds, enabling high-fidelity TDIR. If your organization requires additional log storage or extended storage time, Exabeam Security Log Management offers cloud-native scale and open architecture to meet those needs. Through fast, modern search and visualization, security analysts of all levels can quickly derive answers to their security questions, reducing the learning curve for new analysts and immediately adding to their expertise and understanding of threats. And, the results are instantaneous without having to reload or move data. Experience faster investigations, higher productivity, reduced risk, and improved metrics.

## Flexible data sourcing indexed to a CIM

An average enterprise security stack can consist of 45 or more security solutions, each having its own logs and structures. Typically, different sources have different styles of storing and sending log information; it's important to normalize this data before it can be ingested and analyzed. In addition, event types like app activity have become a catch-all bucket with little detail, creating confusion about what they represent.

Exabeam built a CIM to provide a foundational way to parse, store, and view security information from any vendor. The Exabeam CIM supports a standard process to create new log parsers which adhere to this model, are easier to maintain, and are less prone to errors and misconfiguration. This standardization also defines extensibility to future-proof new log sources and use cases.

## Built on the Exabeam Security Operations Platform

Bringing a cloud-native experience built to scale with your organization, the Exabeam Security Operations Platform allows you to collect and search log data, leverage behavioral analytics to detect attacks, and automate incident response. Visualize the health of your security log feed for every service, log, and application with dashboards showing uptime, health, and data flows. The Exabeam Security Operations Platform supports measurable, continuous, outcomes-focused security posture improvement by recommending information, event stream, and parsing configuration changes to close any common security use case gaps.

### Exabeam Security Log Management helps security teams:

- **Collect, store, and search security event logs and context for threat detection, investigation, and response (TDIR).** Gain visibility across your entire ecosystem with highly scalable, centralized storage and rapid natural language processing (NLP) search capability, without requiring advanced query skills.
- **Simplify the normalization, categorization, and transformation of raw log data.** A common information model (CIM) supports swift threat detection and response, and establishes a standard process to efficiently create and modify log parsers.
- **Threat hunt.** Search on third-party events, known indicators of compromise (IoCs), and correlated events mapped to the most common use cases and the MITRE ATT&CK® framework.
- **Report on compliance standards.** Gain and export visibility into events required by common compliance standards like PCI, HIPAA, and many more with pre-built dashboards.
- **Close security gaps.** Outcomes Navigator maps data sources against security use cases, along with associated correlation rules and dashboards.
- **Visualize your service health and data consumption.** Monitor the uptime and health of all your log parsers, applications, data flows, and connections, as well as your total license consumption.



## About Exabeam

Exabeam is a global cybersecurity leader that delivers AI-driven security operations. The company was the first to put AI and machine learning in its products to deliver behavioral analytics on top of security information and event management (SIEM). Today, the Exabeam Security Operations Platform includes cloud-scale security log management and SIEM, powerful behavioral analytics, and automated threat detection, investigation, and response (TDIR). Its cloud-native product portfolio helps organizations detect threats, defend against cyberattacks, and defeat adversaries. Exabeam learns normal behavior and automatically detects risky or suspicious activity so security teams can take action for faster, more complete response and repeatable security outcomes.

exabeam

**Detect**
**Defend**
**Defeat™**

Get a demo →

Speak with an Expert →

Join a CTF →