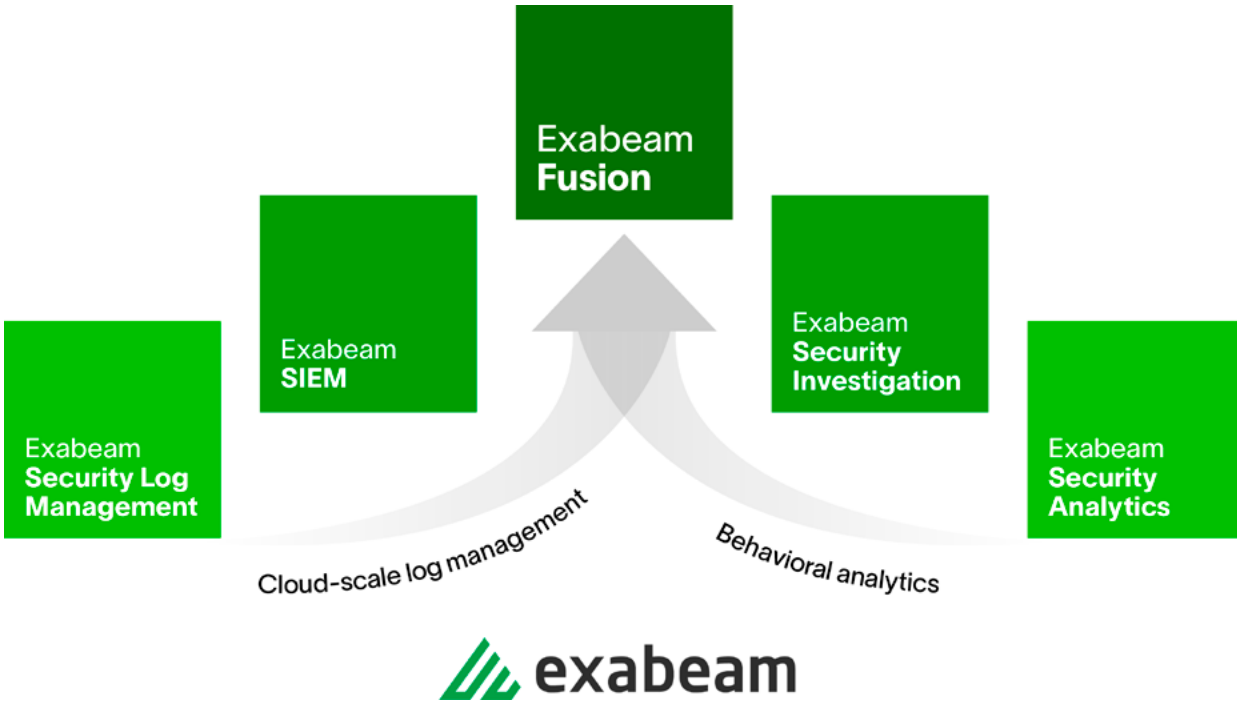
Exabeam Security Operations Platform Privacy

This document provides the information you need to understand how the Exabeam Security Operations Platform gathers, analyzes, and stores sensitive data, so you can assess the impact on your overall privacy posture.

The Exabeam Security Operations Platform Summary

Exabeam, the New-Scale SIEM™ for advancing security operations, offers a powerful combination of cloud-scale security log management, behavioral analytics, and an automated investigation experience. New-Scale SIEM™ is a breakthrough combination of capabilities security operations needs in products they want to use. These capabilities include: rapid data ingestion, a cloud-native data lake, hyper quick query performance, powerful behavioral analytics for next-level insights that other tools miss, and automation that streamlines the way analysts do their jobs.

Security log management leverages a cloud-scale architecture to ingest, parse, store, and search data at lightning speed. Behavioral analytics baseline "normal" behavior of users, devices with histograms, to detect, prioritize and respond to anomalies based on risk. An automated investigation experience across the threat detection, investigation and response (TDIR) workflow provides a complete picture of a threat, automating manual routines and simplifying complex work.



The Five Exabeam Security Operations Platform Products

Exabeam Security Log Management

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

Exabeam SIEM

Cloud-native SIEM at hyperscale with fast, modern search, and powerful correlation, reporting, dashboarding, and case management

Exabeam Fusion

New-Scale SIEM™, powered by modern, scalable security log management, powerful behavioral analytics, and automated threat detection, investigation, and response

Exabeam Security Investigation

Threat detection, investigation, and response powered by user and entity behavioral analytics, correlation rules, and threat intelligence, supported by alerting, incident management, automated triage, and response workflows

Exabeam Security Analytics

Automated threat detection powered by user and entity behavioral analytics with correlation and threat intelligence

What data does the Exabeam Security Operations Platform process?

Exabeam will only process data that you share with us. At Exabeam, data privacy is very important, especially when it comes to processing personally identifiable information (PII). Exabeam believes in the confidentiality of your information and complies with the requirements of the contract with the parties.

Data sources for log ingestion include:

The Exabeam Security Operations Platform has over 500 integrations with IT and security products and over 7,900 log parsers, providing a myriad of inbound data sources, including cloud applications; as well as, response integrations with third party vendors to help you automate and orchestrate your security response. A complete list of data sources for log ingestion can be found here.

Why does the Exabeam Security Operations Platform analyze your data?

The Exabeam Security Operations Platform provides end-to-end detection, user and entity behavior analytics, and security orchestration automation and response. From the data and logs collected in an environment either through a SIEM platform, cloud connectors or directly ingested via Syslog, Exabeam builds a layer of intelligence, helping security analysts see the events within the attack chain to more effectively and quickly remediate the risk.

Where does the Exabeam Security Operations Platform store your data and why?

The Exabeam Security Operations Platform is hosted on Google Cloud Platform (GCP) which enables you to run historic searches and set retention policies.

You are given the option to select the desired GCP region at provisioning. All logs ingested into the selected region will remain within that region for the lifetime of the contracted service. At contract conclusion, you can request access to retrieve your data. After 90 days or by request, your data will be permanently deleted. **Supported GCP regions are listed in the table below:**

Feature	Data Stored
Collectors **Log Stream** **Search** **Dashboard** **Correlation Rules** **Outcomes Navigator** **Service Health and Consumption** **Threat Intelligence Service** **Alert Triage** **Alert and Case Management** **Turnkey Playbooks**	US (East and West), Canada, Germany, Japan, Singapore, Australia
Advanced Analytics **Case Management** **Incident Responder**	Belgium, Finland, Germany, Hong Kong, England, Canada, India, Netherlands, Japan, Brazil, Singapore, Australia, Taiwan, United States, Switzerland

Privacy options

Exabeam provides you with privacy options that you can configure at any time.

Data masking

Data masking within the Exabeam Security Operations Platform user interface anonymizes users and assets and ensures that personal data cannot be read, copied, modified, or removed without authorization during processing or use. Data masking helps preserve individual employee privacy, and with data masking enabled, only users granted viewing permission will be able to see personal information.

Role-based access controls

Role-based access controls allow you to manage the responsibilities and activities of your security team. Each user can be assigned one or more roles to create an aggregate set of permissions within the Platform. You can also create custom roles to fine tune permissions that best align with your organization's security structure.

Data retention

Data Retention policies enable you to choose when data is automatically transferred to an archive destination. Data retention can be set by day, time, or storage space used. For auditing purposes, Exabeam keeps an audit trail of all deletions.

Data security

Exabeam has implemented mechanisms to ensure the secure operation of the environment that stores and processes your data. Among them, a defense in depth methodology, zero trust policy and vulnerability management program coupled with industry standard security tools and techniques. Personnel security is also a key focus. Exabeam performs background checks on all employees and mandates annual security awareness training. The Exabeam Security Operations platform has ISO 27001 certification, certified by a SOC 2 Type II report, and is certified with Privacy Shield.

Customer data is encrypted both in transit and at rest. For data in transit, Exabeam enforces TLS encryption when transferring data from all collectors to the cloud. TLS encryption is configured with TLS 1.2 or 1.3 versions with minimum 128-bit ciphers suites. For all data stored in the Exabeam Security Operations Platform, Exabeam leverages GCP native encryption capabilities using AES-256 algorithm to encrypt data at rest. Each customer environment has dedicated encryption keys, and the keys are stored and are automatically managed through Google Cloud Key Management Service (KMS).

How does Exabeam comply with data protection rules?

Exabeam compliance and certifications

Exabeam has ISO 27001 certification, along with 27017 and 27018, is SOC 2 Type II audited, and is registered and certified with Privacy Shield. ISO 27001 is an internationally recognized standard that specifies requirements for establishing, implementing, maintaining and continually improving an information security management system (ISMS). SOC 2, developed by the American Institute of CPAs, reports on the effectiveness of controls as it relates to security, availability, and processing integrity of the systems, and confidentiality and privacy of the information processed by the systems. Exabeam's Data Security Policy identifies its controls and practices in detail.

Exabeam and GDPR

GDPR is the General Data Protection Regulation enacted by the European Union to establish requirements and standards for companies that may have access to data from EU citizens or residents. Exabeam has appropriate technical and organizational measures in place for GDPR and is considered a processor (as defined under Article 4(2)) which includes essentially any use, disclosure, storage, organization, or destruction of the personal data. Exabeam will process in accordance with the agreement.

If Exabeam transfers or accesses personal data outside of the EU, Exabeam will ensure all appropriate safeguards required by Article 46 of GDPR are in place, which allows processors to transfer data outside of the EU. See 'Transfers to Subprocessors' for additional detail.

If Exabeam transfers or accesses personal data outside of the EU, Exabeam will ensure all appropriate safeguards required by Article 46 of GDPR are in place, which allows processors to transfer data outside of the EU. See 'Transfers to Subprocessors' for additional detail.

Patriot Act and Fisa 702 E012333

As a US-based company, Exabeam is obligated to comply with all applicable laws and valid government requests. Exabeam's standard confidentiality provision in Section 9.5.3 of the EULA specifically states that, if permitted under applicable law, Exabeam will notify customers if a government body has requested or required access to customer's confidential information (including customer data), and allow the customer to take protective measures. Exabeam further agrees to comply with the Standard Contractual Clauses, including Clause 15 as relating to obligations in case of access by public authorities, to the extent applicable.

Transfers to Subprocessors

Exabeam engages Subprocessors who may have access to the Personal Data uploaded to the Cloud environment. Such Subprocessors may process such data outside of the GCP region selected upon provisioning. A list of Exabeam's current Subprocessors is incorporated in its Data Security Policy and available at **https://community.exabeam.com/s/subprocessors**. Exabeam complies with all applicable laws as relating to the transfer of Personal Data to such subprocessors, including GDPR, using appropriate transfer mechanisms such as Standard Contractual Clauses, where applicable.

Trust Exabeam

At Exabeam, trust is the cornerstone of how we conduct our business–everything from how we build our products to how we run our operations. We understand that one of your most valuable assets is your data, and we focus on ensuring your data is secure, data privacy rules are followed, and the platform has a high uptime. For more information, visit **exabeam.com/trust.**

About Exabeam

Exabeam is a global cybersecurity leader that created the New-Scale SIEM™ for advancing security operations. We Detect the Undetectable™ by understanding normal behavior, even as normal keeps changing – giving security operations teams a holistic view of incidents for faster, more complete response.

Learn more about Exabeam today

Get a Demo Now