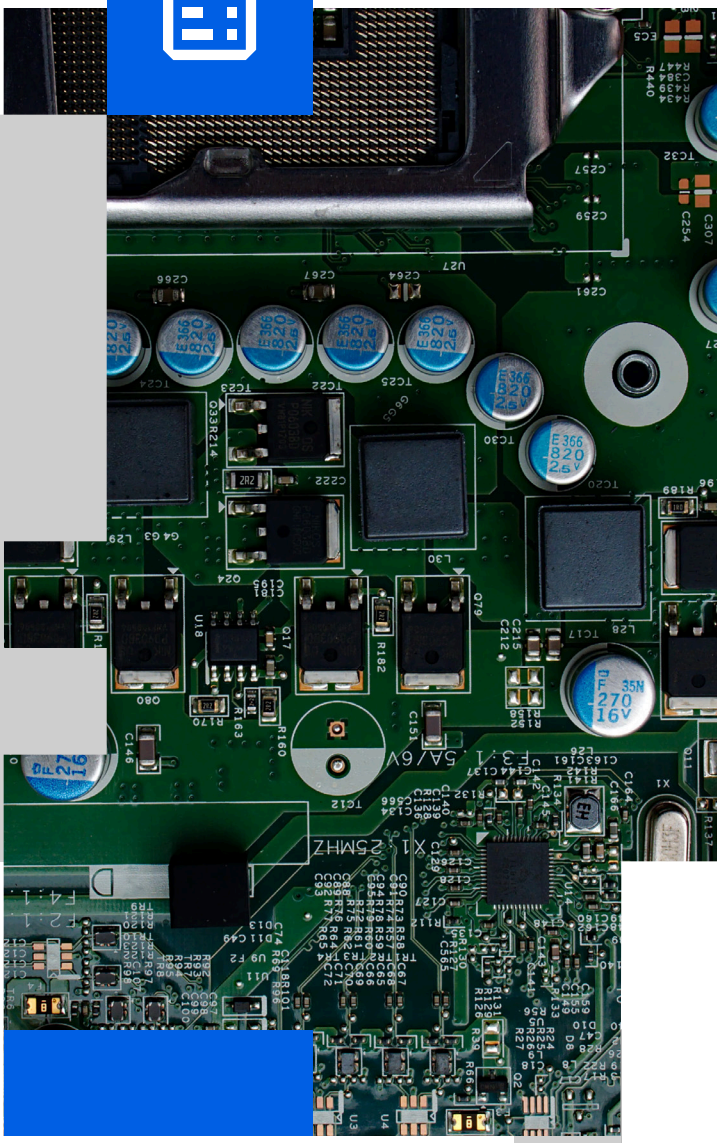
exabeam



Data Sheet

Exabeam Fusion Privacy

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

Fusion Summary

Fusion XDR and Fusion SIEM, both cloud-delivered solutions, take an outcome-based approach and offer prescriptive workflows and pre-packaged, threat-specific content to efficiently solve threat detection, investigation, and response (TDIR).

Pre-built integrations with hundreds of third party security tools and our market-leading behavior analytics combine weak signals from multiple products with an understanding of normal operating behavior to find complex threats missed by other tools.

Prescribed workflows and pre-packaged content focused on specific threat types enable SOCs to achieve more successful TDIR outcomes. Automation of triage, investigation, and response activities from a single, centralized control plane turbocharges analyst productivity and reduces response times.

Conventional SIEM capabilities include centralized log storage, powerful intelligent search, and data enrichment, plus hundreds of prefabricated audit and regulatory compliance reports.

What data does Fusion process?

Exabeam Fusion 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:

Exabeam Security Operations Platform has over 500 integrations with IT and security products, 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 Exabeam Fusion analyze your data?

Exabeam Fusion 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, Fusion builds a layer of intelligence, enabling SecOps teams to see the events within the attack chain to more effectively and quickly remediate the risk.

Where does Exabeam Fusion store your data and why?

Exabeam Fusion 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, your data will be permanently deleted. Supported GCP regions are listed in the table below.

Exabeam Fusion locations

Product	Data Stored
Exabeam Advanced Analytics Exabeam Data Lake Exabeam Incident Responders Exabeam Case Manager	Belgium, Finland, Germany, Hong Kong, England, Canada, India, Netherlands, Japan, Brazil, Singapore, Australia, Taiwan, United States, Switzerland
Exabeam Alert Triage Exabeam Cloud Archive	United States, Germany, Japan

Privacy option

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

Data masking

Data masking within Exabeam Fusion 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 Fusion. 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 Fusion 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. Exabeam Fusion issues 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 Fusion enforces TLS encryption when transferring data from site 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 Exabeam Fusion, 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 KMS.

How does Exabeam comply with data protection rules?

Exabeam compliance and certifications

Exabeam is SOC 2 Type II audited and is registered and certified with Privacy Shield. 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 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 Fusion will process in accordance with the agreement and the Customer's reasonable written instructions.

If Exabeam Fusion requires transfer or access to personal data outside of the EU, Exabeam will notify the customer first. Exabeam has the appropriate safeguards in place to satisfy **Article 46 of GDPR** which allows processors to transfer data outside of the EU.

Patriot Act and Fisa 702 E012333

As a US-based company, Exabeam is obligated to comply with all applicable laws and 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.

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.

exabeam

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