exabeam

Solution Brief

Exabeam Answers 10 Questions to Ask About a Cloud SIEM

Security teams demand better visibility into their environments that now support distributed teams and extend to the cloud. As organizations provide more access to data and collaboration tools, securing and making services available around the clock are critical priorities for security operations centers (SOCs) and their teams.

Digital transformation has accelerated and will continue to advance making it necessary for organizations to adopt cloud solutions. This landscape increases the attack surface for external and internal threats putting SOC teams under pressure to detect potential threats from an overwhelming number of alerts.

In this guide we'll share how **Exabeam Fusion XDR** and **Exabeam Fusion SIEM**, two powerful cloud-delivered solutions, answer the 10 questions **Gartner** recommends asking when assessing a cloud-delivered solutions vendor.

1. Where is the solution delivered from, and where is my data stored?

Exabeam Fusion is cloud-delivered from Google Cloud Platform (GCP). We leverage GCP to store data securely and leverage many of their data centers across the globe. The exact location and country used in your deployment will be determined at the time of purchase as we continuously keep adding new locations. Customers may choose where their Fusion service is hosted from a list of available, global locations.

We use every care to protect our customers' data. As part of our commitment to making data private, each customer's data is isolated and not visible to other tenants.

2. How is my data protected?

All your data is protected through an end-to-end encryption data flow pipeline. We start by ingesting logs and data from APIs like Cloud Connectors into Exabeam Site Collector using secure communication channels (Syslog, agents, Kafka sources using SSL/TLS) in your environment and then upload them through TLS-secured channels onto the cloud-delivered Exabeam Security Management Platform (SMP). In addition, Exabeam Cloud encrypts data at rest to ensure the highest level of security for your data.

Exabeam Fusion is SOC2 Type II certified. To meet the requirements for certification we have developed and follow strict information security procedures and policies for the security, availability, processing, integrity, confidentiality, and privacy of customer data. This aligns with Exabeam's ongoing commitment to create and maintain a secure operating environment for our clients' data.

3. Does the solution provide the scaling and ease of management benefits of a true SaaS model?

Yes. As customer demand increases either due to a temporary spike in usage or normal customer growth over time, we leverage the elasticity of the cloud to add the necessary, incremental resources to meet that demand through auto-provisioning. In addition, we monitor hundreds of metrics for every service location to ensure availability.

4. How is my data collected and transported to the SIEM?

We use a combination of Site Collectors, Cloud Connectors, log forwarding, as well as log fetching options directly from other SIEMs like QRadar or Splunk (on-prem or Splunk Cloud) using their APIs, to securely transport customer data to our cloud-hosted solution. Site Collectors are virtual machines running Exabeam software on your premises. They are secured behind your firewalls and use SSL to forward encrypted data to Exabeam Fusion. Cloud Connectors are similar to Site Collectors as they bring your data from public clouds such as AWS, Azure, and GCP and SaaS applications, including Microsoft Office 365 and Salesforce.

5. What is the expected impact on network or internet links?

The Exabeam cloud-delivered solutions receive data from Site Collectors over the network or internet link through approved ports/protocols documented **here**.

The Site Collectors minimize the impact on the network through compression, batching, and local buffering to gracefully work in congested networks.

6. How does the vendor balance the cadence of feature and function upgrades with adequate testing to ensure availability and quality?

With our Fusion solutions, Exabeam delivers updates and feature rollouts continuously on our cloud platform. Updates are immediately available to Fusion XDR and Fusion SIEM customers.

We ensure the highest quality of all our feature rollouts by implementing proactive controls including:

- Early access and beta customer program — Our beta program allows customers to try pre-release features. If you are interested in accessing a beta release, please contact **program@exabeam.com**.
- Secure code development training — Regular security and code development training and rigorous process requirements arm our employees with the knowledge and support they need to keep all of our sensitive customer data safe.
- Static code analysis — We have facilitated security hardening during development by implementing processes to identify, triage and remediate vulnerabilities.
- Internal penetration testing — We conduct regular internal pen tests to gauge network vulnerability and incident response.
- Third-party external penetration testing — We also conduct unscheduled pen tests by third-party organizations to review common techniques, tools and procedures used by external threat actors.

7. How does the vendor support security technologies that are part of their platform?

At Exabeam, security is at the core of everything we do. Our Fusion products offer multiple capabilities including data collection, threat detection, incident investigation, and response automation to achieve outcomes through prescriptive workflows and guided checklists that help quickly operationalize your Exabeam deployment. The components of our Fusion products are built with the highest standard of security considerations.

Feature and content upgrades are available to all Fusion customers through our cloud-delivered platform.

With Fusion SIEM and Fusion XDR, all ingested logs, events and sessions are stored and available for search, visualization, and investigations for one year. Your subscription is designed to meet your business and compliance needs so you can expand your business without concern for scaling infrastructure, versions, or patches.

8. Is the licensing and pricing model consumption based?

Yes. Our Fusion solutions are cloud-delivered and licensed accordingly. These solutions are priced by the volume of data ingested by your organization. As your security organization matures and brings in a wider variety and higher volume of data to support expanded requirements, Exabeam Fusion offerings can scale to meet your growing needs.

9. How does the vendor ensure availability of the SIEM solution?

The Exabeam Security Management Platform is built on GCP which has a 99.5% uptime service level agreement (SLA). Uptime is further enhanced with application-level resiliency and redundancy. Lastly, Exabeam has a global team of cloud operations experts who monitor dozens of health signals around the clock to proactively detect and remediate concerns before they become issues.

Customers can access their unique status page at any time to check the availability of Exabeam cloud-delivered solutions.

10. What happens at the end of the agreement?

You own your data and it is available to you at all times. With Fusion XDR and Fusion SIEM, you have access to all log data sent to Exabeam which you can analyze or copy for retention regulations and other log management needs. If you choose to transition from a Fusion solution, you can arrange for access to extract your data for 30 days after the end of the contract. You can do this on your own or optionally engage our professional services team for assistance with this process.

About Exabeam

Exabeam is a global cybersecurity leader that adds intelligence to every IT and security stack. We are reinventing the way security teams use analytics and automation to solve threat detection, investigation, and response (TDIR), from common security threats to the most critical that are difficult to identify. The Exabeam Security Management Platform is a comprehensive cloud-delivered solution that leverages machine learning and automation using a prescriptive, outcomes-based approach to TDIR. It is designed and built to help security teams detect external threats, compromised users, and malicious adversaries, minimize false positives and make security success the norm. For more information, visit **www.exabeam.com**.

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

exabeam