Google Cloud exabeam

Exabeam Fusion on Google Cloud

New-Scale SIEM™ powers end-to-end threat management with unprecedented speed, security, and cost advantage.

As cyberattacks become increasingly frequent, sophisticated, and hard to detect, security operations teams are struggling with the limitations of legacy security information and event management (SIEM) and traditional perimeter security. Traditional platforms haven't kept pace with the growth of data, the sophistication of attacks, or the shift to the cloud. Nor can it handle the increasing volume of data that remote computing, new SaaS solutions, and complex infrastructure bring. Legacy tools fail to provide a complete picture of a threat, and they bury analysts with alerts.

Rather than focusing on the amount of data, organizations need to collect more of the right data and know what they're looking for to uncover threats buried in a sea of noise. Simply put, manual investigations take too much time and resources and often lead to an incomplete outcome that leaves your organization at greater risk.

93%

of security breaches are the result of credential-based attacks.

Support your security use cases with a cloud-native solution

Seismic changes require an innovative, robust approach to data access as well as to the threat detection, investigation, and response (TDIR) workflow. Together, Google Cloud and Exabeam close the loop on cybersecurity. Exabeam brings New-Scale SIEM™ via Exabeam Fusion, a cloud-native security operations platform that uses Google Cloud to offer a new level of scalability, security, and cost advantage to process, store, and search security logs. The solution provides customers with industry-leading user and entity behavior analytics (UEBA) capabilities, automation, and cloud-based storage to address today's SIEM effectiveness gap. The Exabeam suite of solutions complement and augment Google's shared-fate approach to cybersecurity, which includes security by design and by default, as well as robust zero-trust solutions for data access.

Cloud security is about more than just solving your short-term problems. It's about achieving your strategic goals. With the right security capabilities in place, you can secure your entire digital transformation journey. Exabeam products on Google Cloud can meet your security analysts where they are today — providing the event definitions, context, and associated risk, and suggesting next steps for mitigation or resolution.

Google Cloud

exabeam

- ✓ Lightning-fast search and dashboarding experience with all security data in one place
- ✓ More than 100 pre-built Correlation Rules with processing speeds exceeding 1M EPS sustained
- ✓ Prescribed workflows for ransomware, phishing, malware, and other threats

+

- ✓ Secure-by-design infrastructure with legendary scalability and encryption
- ✓ Zero-trust framework with context-aware controls to automate policy enforcement
- ✓ Compliance without compromise, with data residency options

→

- ✓ Improve your security maturity with solutions designed to integrate seamlessly.
- ✓ Upgrade your defenses and detect sophisticated and credential-based attacks.
- ✓ Work faster thanks to automation and advanced analytics.

Manage security logs at cloud scale

Built from the ground up to take advantage of Google Cloud's flexible and resilient architecture, the Exabeam Security Operations Platform lets you securely ingest, parse, store, and search security data at scale from any location. Integrate with more than 500 products supporting over 9,000 pre-built parsers for on-premises and cloud data sources, and process more than 1 million events per second (EPS), sustainable for each tenant.

Take advantage of Google Cloud's robust security governance and reliability controls, and gain fast, modern search and visualization with instant results over exabytes and years of information without having to move data.

Detect anomalies with behavioral analytics

The Exabeam Security Operations Platform provides lightning-fast search and analytics powered by Google Cloud so you can detect, investigate, and respond to anomalous activity that often goes undetected by legacy SIEM products.

Analyze anomalous user and device behaviors across 500+ IT and security vendor tools including Google BigQuery and Looker. Automatically assign risk scores to events with machine learning, and detect intruders with built-in awareness of adversarial tactics and techniques including 101 MITRE ATT&CK® framework tactics, techniques and procedures (TTPs), and 180 sub-techniques.

Automate security investigations

No more searching through a sea of alerts! Exabeam provides an automated experience across the TDIR workflow to reduce manual routines. Build events along a common information model (CIM) with automatic context enrichment via threat intelligence feeds, group information, and other fingerprinting.

You can quickly see and act on meaningful alerts with automated case enrichment providing relevant context, followed by scripted response actions. Improve productivity, scale operations, and focus on meaningful work by recapturing two-thirds of analyst time on detection, triage, and investigation. (Ponemon)

The Exabeam suite of solutions is designed to complement and augment Google's shared-fate approach to cybersecurity, as well as its robust zero-trust solution for data access.

→ **Learn more at exabeam.com**