exabeam™ | Google Cloud

Exabeam Solution Brief

Exabeam and Google Cloud

The Exabeam Security Operations Platform is built on Google Cloud

Introduction

Legacy SIEM technology often fails to detect modern threats. The lack of market innovation relative to data expansion, the sophistication of attacks, and a shift to the cloud have created a SIEM effectiveness gap. Security teams are overwhelmed with data and are unclear on what data to collect. Legacy tools don't provide a complete picture of a threat; they bury analysts with alerts and compel slow, ineffective, and manual investigations. Meanwhile, attacks are becoming increasingly sophisticated and hard to detect, and credential-based attacks are multiplying.

Whether it's phishing, ransomware, malware, or another external threat, valid credentials are now the adversaries' primary target. This demands a shift in investment from legacy on-premises, rule-based detection to cloud-native SIEM platforms designed to identify abnormal behavior and automate the entire threat detection, investigation, and response (TDIR) workflow.

To address these challenges, Exabeam built New-Scale SIEM™ — a cloud-native offering that leverages Google Cloud. Google Cloud provides scalability, security, and cost advantage for processing, storing, and searching security logs. Exabeam provides customers with the industry-leading user and entity behavior analytics (UEBA) solution, automation, and cloud-based storage to address today's SIEM effectiveness gap.

Benefits

- Limitless log ingestion and storage
- Quickly detect anomalous activity
- Easily built threat timelines
- Increased platform security

Exabeam's Cloud-scale Solution

Security operations success requires a new approach: New-Scale SIEM from Exabeam. New-Scale SIEM is a breakthrough combination of the capabilities security operations staff need 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 changes the way analysts do their jobs.

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

Why Exabeam and Google Cloud

Exabeam partnered with Google Cloud as the foundation on which we architected our hyperscale cloud-native Exabeam Security Operations Platform and product portfolio, providing customers with cloud-scale storage and compute to address the growing challenges of collecting the right data, increased alert noise, and the rising cost of data storage. By ingesting and parsing security log data from hundreds of different security tools, New-Scale SIEM provides cloud-scale security log management for storage and search, behavioral analytics to detect abnormal activity, and automated investigation for increased visibility and response.

Google Cloud is also a valued Exabeam technology partner that provides product integrations with Google Cloud and Workspace, Google's productivity and collaboration tools. By working together, end customers can better mitigate any security concerns across Google products, including phishing attacks, malware, and compromised credentials. In 2021, Exabeam extended the partnership beyond technology integrations by becoming a Google Cloud Marketplace member, simplifying the procurement of market-leading SIEM and security analytics solutions with Google Cloud customers.

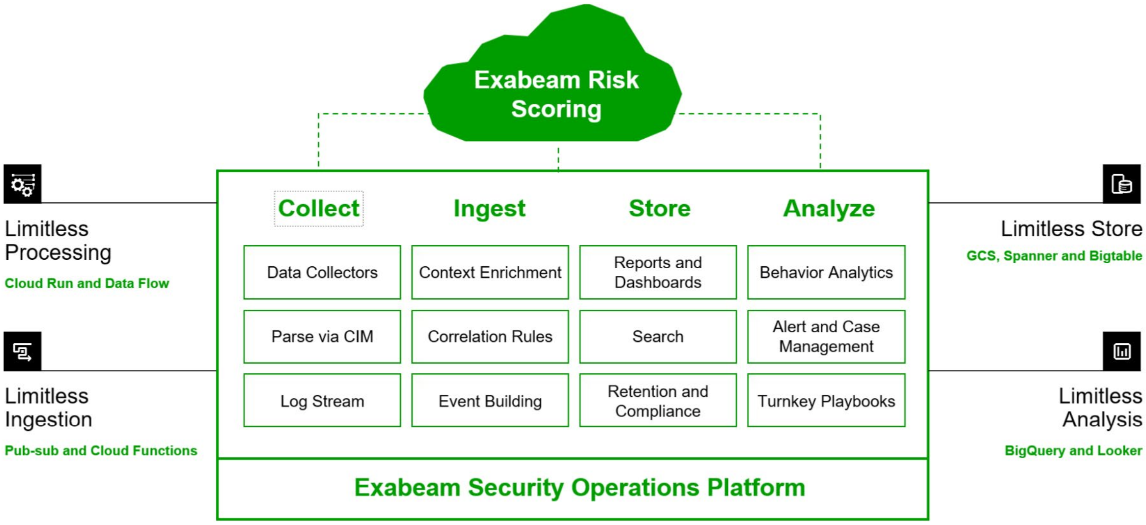

Figure 1. The cloud-native Exabeam Security Operations Platform is built on Google Cloud.

Google Cloud Capabilities leveraged by the Exabeam Security Operations Platform

Cloud Run and Dataflow — limitless data processing for parsing log streams

Pub-sub and Cloud Functions — scalable data ingestion

Google Cloud Storage, Spanner, and Bigtable — data storage for large analytical and operation workloads

BigQuery and Looker — scalable analysis with insightful visualizations

Key Benefits

Limitless log ingestion and storage — The Exabeam portfolio of products leverages Google Cloud Run and Dataflow to provide customers with scalable ingestion, parsing, storage, and intelligent search capabilities to substantially reduce mean time to resolution (MTTR).

Quickly detect anomalous activity — Security teams can detect, investigate, and respond to anomalous activity that often goes undetected by legacy SIEM products. With Google BigQuery and Looker, Exabeam customers are able to analyze anomalous user and device behaviors across 500+ IT and security vendor tools.

Easily built threat timelines — Exabeam Fusion leverages Google BigQuery and Looker to help security teams triage events by combining weak signals across multiple tools to build timelines with prescriptive use case guidance.

Increased Platform Security — Google Cloud products provide Exabeam with robust security governance and reliability controls that offer high availability and a 99.99% uptime SLA. Customers can trust in the security of their log data and analytics.

Key Features

Collectors — The Exabeam Security Operations Platform provides extensive data collection capabilities and coverage. A single interface is used to securely configure, manage, and monitor the transport of data into the Exabeam service from on-premises, cloud, and context sources. The platform provides collection from 200+ on-premises products and supports 34 cloud-delivered security products, 11 SaaS productivity applications, and 21 cloud infrastructure products.

Log Stream — Delivers rapid log ingestion processing at a sustained rate of more than 1M EPS. A central console enables you to visualize, create, deploy, and monitor parsers within a unified ingestion pipeline for all Exabeam products and features. As it is ingested, data is parsed using 7,937 pre-built log parsers, and enriched using three context collectors from open source and commercial threat intelligence feeds.

Search — Simplified search experience with faster query and instant results over petabytes and years of data; search hot and cold data at the same speed.

Advanced Analytics — Offers UEBA with more than 1,800 rules, including cloud threat detection, and more than 750 behavioral models to automatically baseline normal behavior of users and devices with histograms to detect, prioritize, and respond to anomalies based on risk. Advanced Analytics automatically visualizes these events in Smart Timelines™ that show full event flows and activities to inform the next right action.

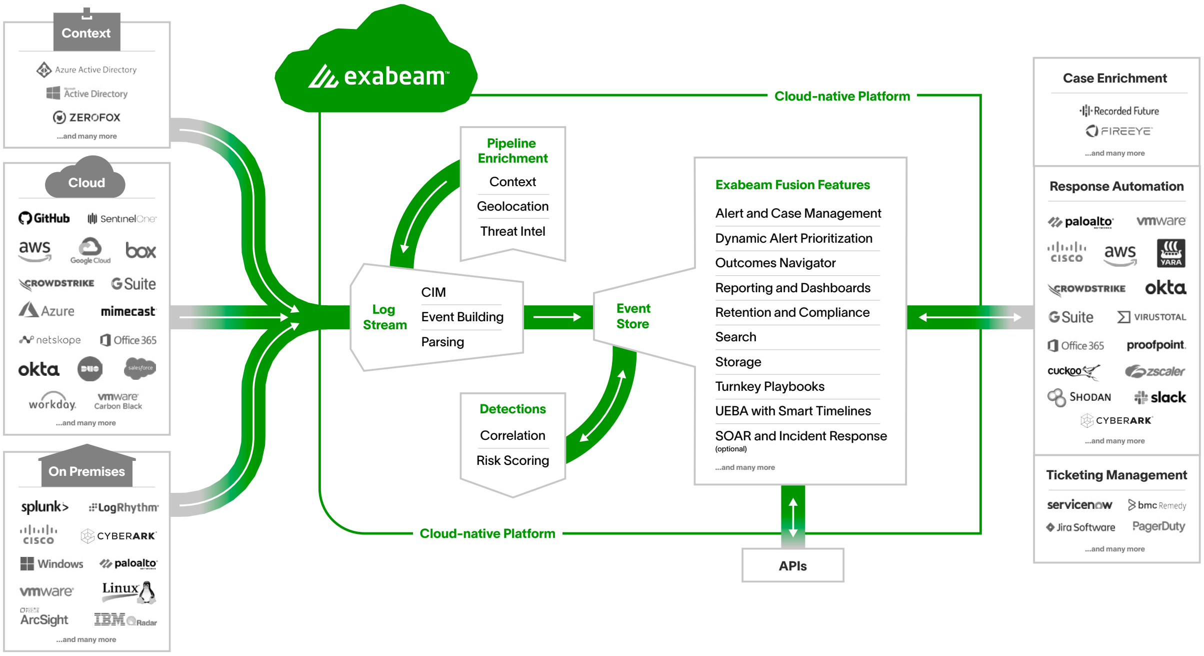

Figure 2. Exabeam Fusion: New-Scale SIEM, powered by modern, scalable security log management, powerful behavioral analytics, and automated TDIR — including integrations with Google Cloud products.

About Google Cloud

Google Cloud accelerates organizations' ability to digitally transform their business with the best infrastructure, platform, industry solutions and expertise. We deliver enterprise-grade solutions that leverage Google's cutting-edge technology – all on the cleanest cloud in the industry. Customers in more than 200 countries and territories turn to Google Cloud as their trusted partner to enable growth and solve their most critical business problems. For more information, visit **cloud.google.com.**

Why did Exabeam select Google Cloud?

"After looking at several cloud players in the market, we selected Google Cloud, specifically the Data Analytics family of products including BigQuery, Dataflow, and Looker, because of its hyperscale, speed, and ability to support the type of technically advanced products we build at Exabeam," said Adam Geller, Chief Product Officer, Exabeam. "Google Cloud has enabled us to greatly accelerate our own security platform and product innovation, resulting in state-of-the-art features and capabilities that can finally overcome the data proliferation and TDIR challenges faced by security operations teams today."

- Adam Geller, Chief Product Officer, Exabeam

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