Exabeam and Google Cloud

How Exabeam and Google Security Operations Detect Insider Threats, Credential Misuse, and Agentic AI Risk

Joint Value Summary

As organizations expand cloud operations and deploy autonomous AI agents, they face critical visibility gaps and a surge in sophisticated insider threats that traditional rule- and signature-based approaches struggle to detect. This joint solution combines the hyperscale data lake and cloud-scale security operations capabilities of Google Security Operations with Behavior Intelligence from Exabeam to establish behavioral baselines across human, machine, and AI identities. Together, the platforms deliver an end-to-end threat detection, investigation, and response (TDIR) workflow that scales with modern cloud environments, simplifies operations, and streamlines procurement through Google Cloud Marketplace.

Why Organizations Use the Exabeam and Google Security Operations Joint Solution

Organizations adopt the combined Google Security Operations and Exabeam solution to achieve complete behavioral visibility and accelerate TDIR across modern hybrid and cloud environments. By streaming raw security telemetry from Google Security Operations into New-Scale Analytics, the joint solution applies Behavior Intelligence to establish precise behavioral baselines for human users, machine accounts, service identities, and autonomous AI agents.

Through a native, co-engineered integration, organizations can analyze massive volumes of security data without complex middleware, secondary data pipelines, duplicate storage fees, or moving data outside Google Cloud infrastructure. Exabeam behavioral analytics, dynamic risk scoring, and chronological timelines surface complex attack chains, account compromise, privilege misuse, and anomalous insider activity that traditional security tools often miss.

The result is a unified TDIR workflow that reduces analyst burnout, improves operational efficiency, and provides predictable procurement and pricing through Google Cloud Marketplace.

The Market Challenge

Traditional security methods rely on static rules and signatures that struggle to detect legitimate identities behaving maliciously. This challenge extends beyond human users to service accounts, machine identities, and AI agents operating with trusted access to sensitive systems, internal APIs, and production environments. Without behavioral context, security teams cannot reliably distinguish authorized activity from account takeover, insider threats, data exfiltration, and malicious agent behavior, leaving organizations vulnerable to slow-moving attacks operating within trusted environments.

How Exabeam and Google Security Operations Work Together

A Unified Defense at Cloud Scale

Google Security Operations and Exabeam deliver a co-engineered integration that bridges hyperscale data ingestion with advanced behavioral analytics. Through a native Google Security Operations collector, raw security telemetry streams directly from Google Security Operations to New-Scale Analytics. This direct pipeline allows organizations to store massive volumes of raw security logs in Google Security Operations while automatically applying advanced behavioral threat modeling in Exabeam without complex middleware, secondary data pipelines, additional storage costs, duplicate storage fees, or moving data outside Google Cloud infrastructure.

Google Security Operations provides the telemetry foundation, cloud-scale security operations platform, and hyperscale data lake, while Exabeam applies user and entity behavior analytics (UEBA), Agent Behavior Analytics (ABA), and dynamic risk scoring to establish expected behavior patterns across human, machine, and AI identities. By comparing activity against established behavioral patterns, the solution automatically identifies credential abuse, insider threats, privilege misuse, lateral movement, and anomalous agent behavior that may not be apparent through rules and signatures alone.

Security teams can investigate prioritized threats through automatically generated chronological investigation timelines that unify activity into a single view, expose complete attack chains, and provide rich behavioral context. Together, the platforms deliver an end-to-end TDIR workflow that scales with modern cloud environments while simplifying operations and procurement through Google Cloud Marketplace.

Key Integration Benefits

- **Stop Compromised Digital Insiders:** Detect anomalous activity across human identities, machine accounts, and autonomous AI agents by applying UEBA, ABA, and dynamic risk scoring to identify deviations from normal behavior.
- **Eliminate Costly Visibility Gaps:** Stream raw telemetry directly from Google Security Operations to New-Scale Analytics without extra middleware, duplication of storage fees, additional storage costs, or leaving Google Cloud infrastructure while applying advanced behavioral analytics to large-scale security telemetry.
- **Accelerate Incident Response by 80%:** Improve TDIR efficiency by 80% using automatically generated behavioral timelines that replace manual log searches and instantly expose the entire attack path.
- **Reduce Investigation Time With Behavioral Context:** Replace manual raw log analysis with automatically generated investigation timelines that expose attack chains, correlate related activity, and provide clear, plain-language context that helps analysts understand the scope and impact of what happened.
- **Maximize Security Value and ROI:** Use existing Google Cloud spend commitments directly through Google Cloud Marketplace to achieve predictable pricing, streamlined procurement, lower total cost of ownership, and greater value from existing Google Cloud investments.

Primary Use Case: Autonomous AI Agent and Digital Insider Threat Detection

Definition

Monitoring and securing human identities, machine accounts, service identities, and autonomous AI agent networks that operate as highly privileged digital insiders with access to corporate data, internal APIs, and production workflows.

Challenge

Traditional rule-based security systems cannot reliably detect compromised credentials, insider threats, privilege misuse, or malicious AI agent activity because these actions often mimic authorized, legitimate behavior. As a result, organizations remain vulnerable to data exfiltration, lateral movement, prompt injection attacks, and other identity-based threats operating within trusted environments.

Solution

Apply UEBA, ABA, dynamic risk scoring, and behavioral threat modeling to telemetry from Google Security Operations to identify, prioritize, and isolate anomalous activity. Security teams gain unified visibility into human, machine, and AI identities, enabling earlier detection of credential abuse, insider threats, lateral movement, and anomalous agent behavior before significant damage occurs.

About Exabeam

Exabeam is the leader in behavior intelligence for the agentic enterprise. As organizations deploy digital workers and confront machine-speed adversaries, Exabeam delivers flexible, industry-proven solutions for insider threat coverage of humans and agents and faster, more accurate threat detection, investigation, and response (TDIR). Learn more at www.exabeam.com.

Learn more at
www.exabeam.com →