Extend Google Security Operations with Exabeam Behavior Intelligence

Exabeam Behavior Intelligence strengthens Google Security Operations deployments by applying New-Scale Analytics through integrated data sharing, helping security teams surfacei nsider threats and risky activities across human and AI identitites.

Why Behavior Intelligence Elevates Google Security Operations Deployments

Security operations teams face a growing challenge: identifying insider threats and risky activity that look routine. Compromised users, insiders with valid access, and AI agents embedded in enterprise workflows often behave in ways that bypass rule-based detections. These behaviors blend into normal activity, especially in environments processing large volumes of security telemetry.

Google Security Operations gives organizations a cloud-scale foundation to centralize and correlate security telemetry, yet scale alone doesn't expose the subtle shifts that signal risk. As cloud adoption, remote work, and automated systems expand, these faint signals multiply. Teams must sort through large volumes of low-value alerts, which slows investigations and obscures meaningful activity. To reveal these threats, organizations need Behavior Intelligence applied directly to data already in Google Security Operations.

Exabeam and Google Security Operations

Google Security Operations gives organizations a powerful cloud-scale foundation to centralize and correlate security telemetry. Exabeam extends New-Scale Analytics to Google Security Operations through integrated data sharing between the two platforms, enabling security teams to apply advanced behavioral analytics without moving data or maintaining a separate analytics environment. Built on a shared Google Cloud foundation, the integration helps reduce cost, complexity, and operational overhead while giving teams deeper visibility into insider threats and risky activity across human and AI identities.

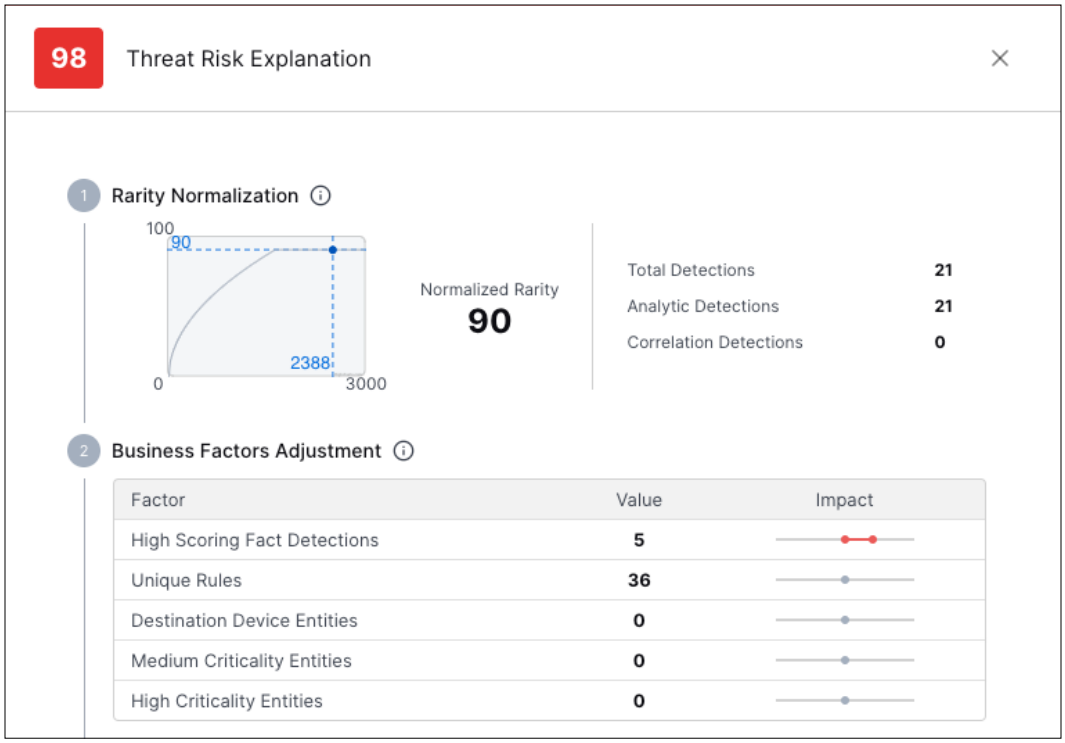

Figure1.

Dynamic risk scoring evaluates unusual behavior using normalized rarity and business context to help analysts identify meaningful activity in Google Security Operations data.

Key Capabilities

Challenge: Hidden Behavioral Threats

Subtle activity patterns blend into normal operations and evade static detections.

Solution

New-Scale Analytics evaluates Google Security Operations data through behavioral models that learn how each user, device, and AI agent typically behaves. Instead of relying only on correlation rules, Exabeam surfaces activities that fall outside these norms. Examples include a first-time login to a sensitive server, unusual command sequences, or access from an atypical location. The system also evaluates risk evidence from multiple signals, assigning dynamic risk scores linked to the behaviors observed. This makes it easier to distinguish genuine threats from noise and helps analysts zero in on the events that genuinely require action.

Benefit

You gain earlier detection of unusual activity, fewer distractions, and more confidence in the alerts you choose to investigate.

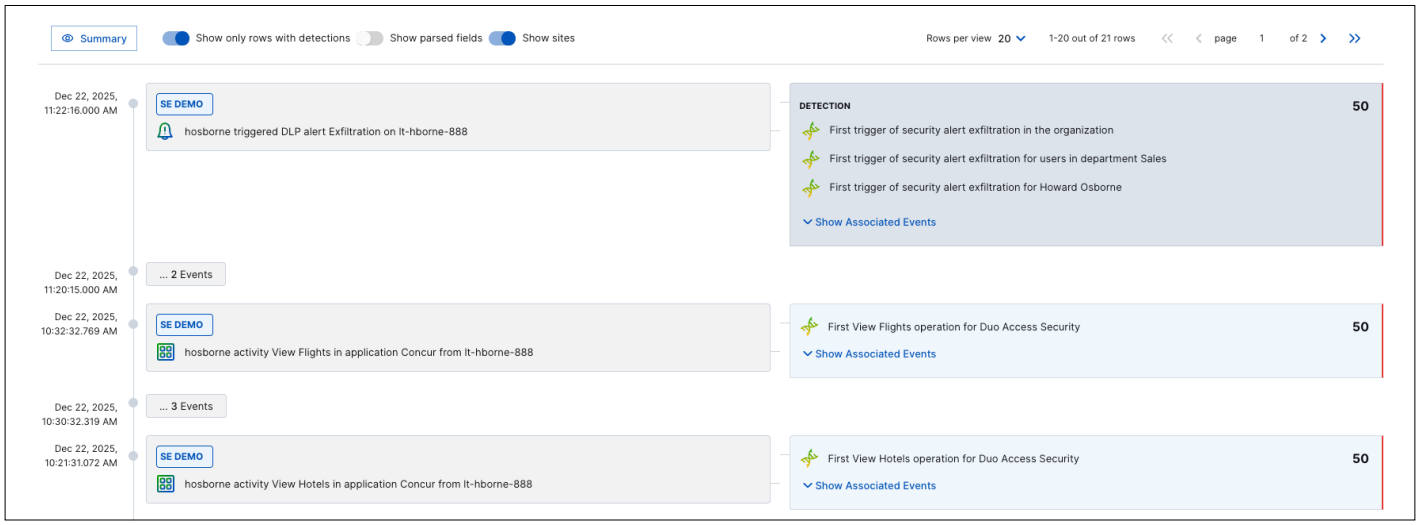

Figure 2.

Threat Timelines connect related events from Google Security Operations telemetry to show the full sequence of activity.

Challenge: Slow, Manual Investigations

Analysts lose time stitching data across tools and building timelines.

Solution

Exabeam automates the investigative steps that typically consume hours of manual effort. New-Scale Analytics assembles related events from Google Security Operations telemetry into a single behavioral Threat Timeline that shows the full sequence of actions. It enriches each event with user roles, device attributes, and threat intelligence. Analysts no longer need to craft complex queries or switch between tools to understand what happened. According to Exabeam validation testing, organizations accelerated threat detection, investigation, and response (TDIR) workflows by up to 80%, helping teams redirect energy toward higher-value work.

Benefit

Your team investigates faster and responds sooner without losing time to manual data gathering.

Challenge: AI Agent Activity Visibility

AI agents introduce a new category of insider risk, with non-human identities accessing systems, invoking tools, executing workflows, and making decisions with increasing autonomy.

Solution

As organizations adopt AI agents, Exabeam extends Behavior Intelligence to monitor non-human identities alongside human users. Detection models evaluate agent workflows, interactions, and execution patterns to identify actions that fall outside typical usage. Applied directly to Google Security Operations data, New-Scale analytics helps security teams analyze behavior across every identity in the environment and act before threats escalate. The Agentic AI Security use case in Outcomes Navigator provides guidance to improve monitoring and reduce risk. This closes visibility gaps without requiring additional point tools.

Benefit

Secure and govern AI agents alongside human users, monitor behavior across identities, and detect misuse before it creates a business risk.

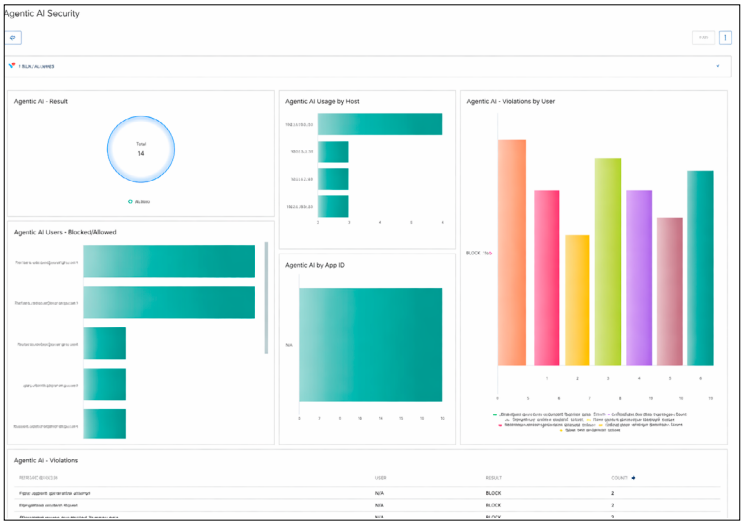

Figure 3.

The Agentic AI Security dashboard highlights usage patterns and violations to reveal unexpected or risky actions across human and AI identities.

Conclusion

By applying Behavior Intelligence directly to Google Security Operations data, your team gains stronger insight into unusual behavior, faster investigation paths, and a dependable way to act earlier in the attack chain. Available through Google Cloud Marketplace, New-Scale Analytics helps Google Security Operations customers improve threat detection and investigation while reducing the cost and complexity of maintaining a separate analytics environment.

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.

exabeam™

Learn more at
www.exabeam.com →