Extend Google Chronicle with Exabeam Behavioral Intelligence

Behavioral intelligence strengthens Google Chronicle deployments by surfacing subtle threats hidden in routine activity.

Why Behavioral Intelligence Elevates Chronicle Deployments

Security operations teams face a growing challenge: identifying threats that look routine. Compromised users, insiders with valid access, and AI agents embedded in everyday workflows often behave in ways that bypass rule-based detections. These behaviors blend into normal activity, especially in environments processing billions of events each day.

Google Chronicle delivers massive ingestion, normalization, and search capabilities, 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 behavioral intelligence and automated investigation layered on their Chronicle data.

Exabeam and Google Chronicle

Google Chronicle processes tens of millions of events per second and operates under a 99.99% uptime SLA. Exabeam adds behavioral intelligence and automated investigation to Chronicle telemetry to expose activity that static rule sets miss. You can deploy New-Scale Fusion for end-to-end threat management or extend Chronicle with New-Scale Analytics to increase detection fidelity without changing established workflows. This gives your team better visibility and earlier insight into unusual behavior.

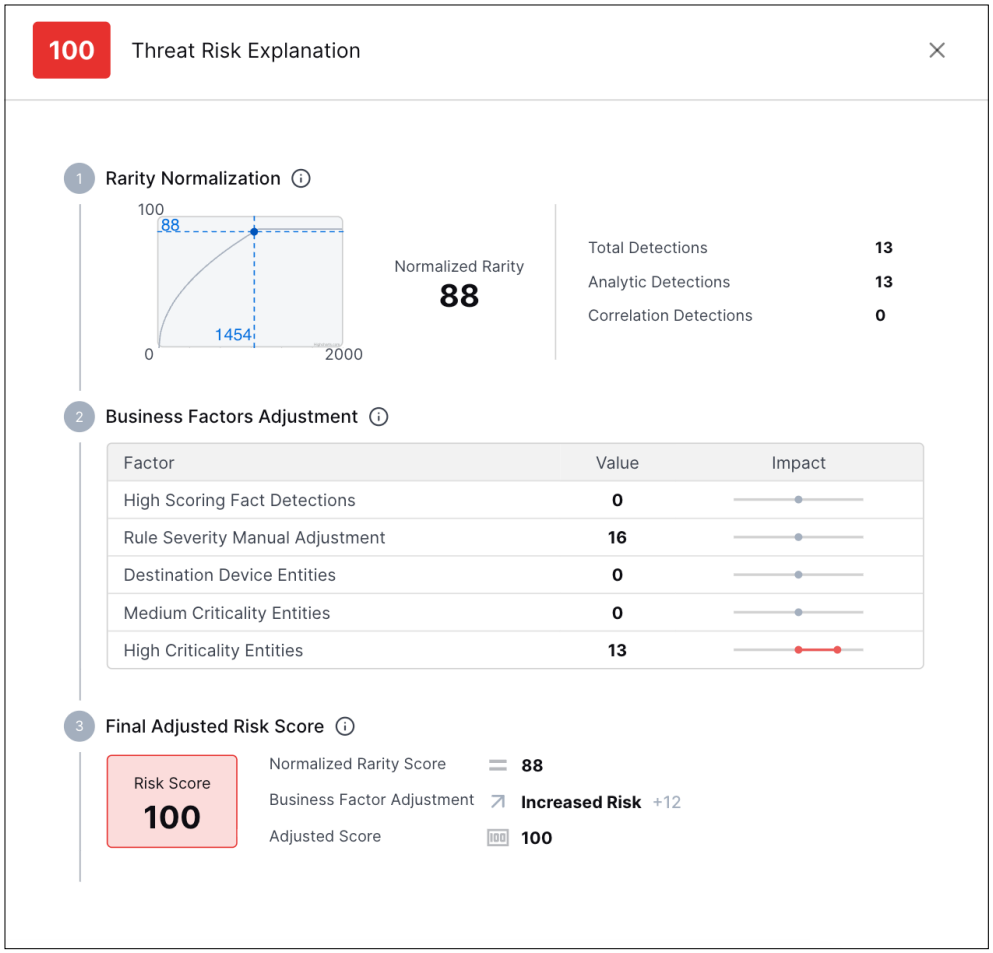

Figure 1.

Dynamic risk scoring evaluates unusual behavior using normalized rarity and business context to help analysts identify meaningful activity.

Key Capabilities

Challenge: Hidden Behavioral Threats

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

Solution

New-Scale Analytics evaluates Chronicle telemetry 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.

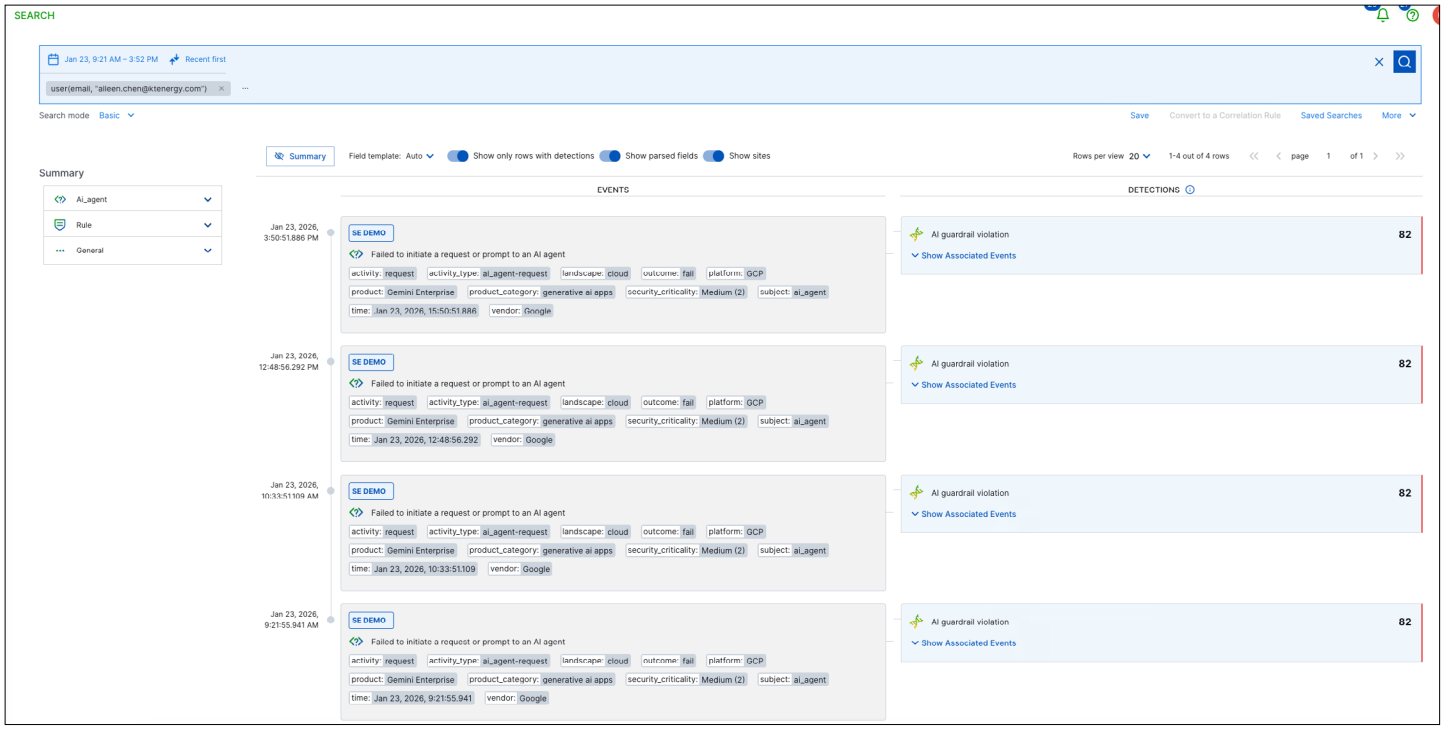

Figure 2.

Investigation Timelines connect related events from Chronicle 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. The platform assembles related events from Chronicle telemetry into a single behavioral Investigation 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. Automation across detection, correlation, and investigation reduces threat detection, investigation, and response (TDIR) workload by up to 80%, which lets your team redirect energy toward higher-value work.

Benefit

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

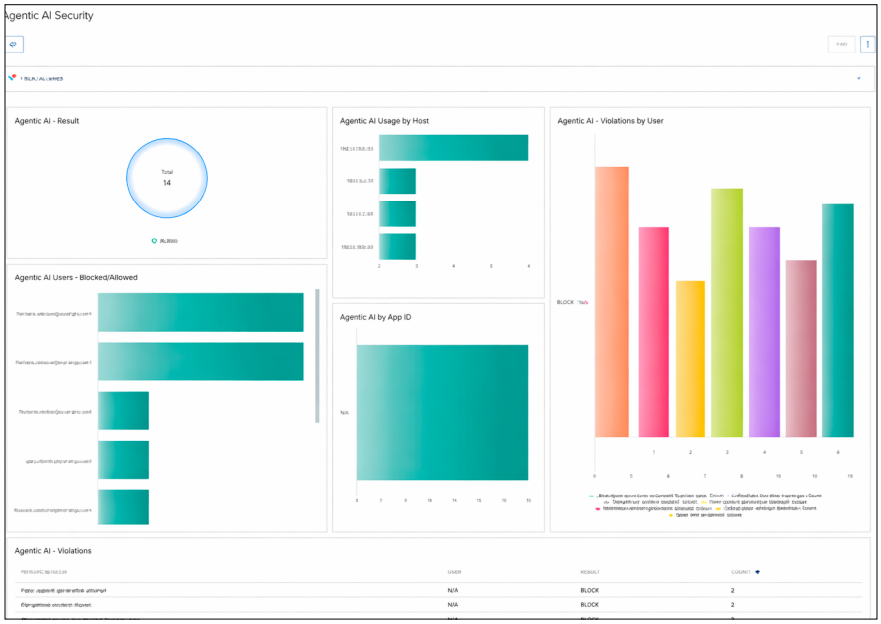

Figure 3.

The Agentic AI Security dashboard highlights usage patterns and violations to reveal unexpected or risky actions in Google Cloud environments.

Challenge: AI Agent Activity Visibility

AI agents introduce new, opaque behaviors with limited monitoring.

Solution

As organizations adopt AI agents, Exabeam extends behavioral intelligence to monitor their activity alongside human users. Detection models evaluate agent workflows, interactions, and execution patterns to identify actions that fall outside typical usage. Integrations with Google Cloud, including Gemini Enterprise, bring added context to agent behavior and potential misuse. 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

Onboard AI agents securely, monitor their behavior, and detect misuse before it creates a business risk.

Conclusion

By adding behavioral intelligence and automation to Chronicle data, your team gains stronger insight into unusual behavior, faster investigation paths, and a dependable way to act earlier in the attack chain. This approach gives your security operations team the context and automation needed to move from reactive alert handling to more efficient threat management.

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).

exabeam™

Learn more at
www.exabeam.com →