CONTRAST SECURITY | Google Cloud Security

SOLUTION BRIEF

Contrast Application Detection and Response (ADR) and Google Security Operations

The agentic SOC requires runtime reality, not just more logs.

Vulnerability exploitation is the leading initial intrusion vector for the sixth consecutive year, accounting for 32% of all intrusions.[1] The Contrast Application Detection and Response (ADR) integration addresses this by instrumenting applications at runtime. By observing real code execution, Contrast provides Google SecOps with verified, high-fidelity evidence of exploitation that network traffic analysis simply cannot see.

The visibility and noise crisis

Modern security teams are fighting an asymmetry of information where traditional tools like Web Application Firewalls (WAFs) guess at threats based on traffic patterns, generating massive volumes of noise and false positives. Because these perimeter tools cannot see inside the application to verify if code is actually vulnerable, they force analysts to waste cycles on harmless probes rather than real risks. In an era of AI-speed attacks, this lack of runtime context creates a critical visibility gap that leaves organizations exposed.

Runtime precision fuels the agentic SOC

Contrast Security and Google Cloud have partnered to bring runtime reality to the SOC. Unlike traditional tools that scan from the outside, Contrast's technology operates from within the running application. It observes every request, analyzes code execution in real time and confirms whether an attack was successful or blocked based on behavioral abnormalities within the runtime. This inside-out telemetry acts as a force multiplier for Google Security Operations.

By feeding incident data from the real-time Contrast Graph directly into Google SecOps, the integration provides the high-fidelity intelligence required for accurate triage and response. Purpose-built detection rules automatically surface confirmed application exploits as cases within Google SecOps, and correlate application-layer findings with signals from WAFs, EDR tools and database security sensors — giving analysts a complete picture of an attack chain without writing custom logic. Because Contrast telemetry arrives pre-structured in Google's Unified Data Model (UDM), it is immediately available to Google SecOps' Gemini-powered AI features, providing the verified, high-fidelity data that AI-driven investigation and triage requires.

Verified attack data drives prioritization across the security organization. The broader Contrast platform — including AI-assisted remediation through SmartFix — gives engineering teams the precise runtime context required to close the gap between what is being exploited today and what gets fixed tomorrow.

Redefining application defense for the agentic SOC

The integration between Contrast Security and Google Security Operations represents a fundamental shift in how enterprises defend the application layer. By replacing probabilistic alerts with verified runtime intelligence, security teams can finally operate with the confidence required for an Agentic SOC. This integration fills the critical visibility gap, enabling faster, more autonomous responses to the threats that matter most.

The road ahead connects the SOC, the application runtime and the development team into a single, continuous defense loop where every confirmed exploit drives both an immediate operational response and a permanent fix in code.

Ready to see Contrast in action?

Visit our website or request a demo today to learn how Contrast Security can empower your can empower your Google Security Operations with verified, runtime application intelligence.

Try Contrast

[1] Google Cloud Mandiant M-Trends 2026

Contrast Security is the world's leader in Runtime Application Security, embedding code analysis and attack prevention directly into software. Contrast's patented security instrumentation enables powerful Application Security Testing and Application Detection and Response, allowing developers, AppSec teams and SecOps teams to better protect and defend their applications against the ever-evolving threat landscape.

contrastsecurity.com

6800 Koll Center Parkway
Ste 235
Pleasanton, CA 94566
Phone: 888.371.1333