CONTRAST SECURITY | sumo logic

SOLUTION BRIEF

Contrast Application Detection and Response (ADR) and Sumo Logic Cloud SIEM

Enrich Sumo Logic insights with application runtime intelligence

Sumo Logic's Cloud SIEM has established a new standard for modern Security Operations Centers (SOCs), delivering the AI-driven intelligence and unified visibility needed to modernize SecOps workflows. By unifying security and observability data, Sumo Logic empowers teams to defend complex multi-cloud environments. However, as security teams ingest data from across the enterprise, the application layer remains a critical intelligence gap. Telemetry from application security tools like Web Application Firewalls (WAFs) and static scanners is notoriously noisy, lacks exploit confirmation and ultimately pollutes the SIEM with low-quality data that hinders the ability to identify real application attacks quickly.

Contrast Application Detection and Response (ADR) enriches Sumo Logic Cloud SIEM by streaming high-fidelity, real-time security signals from deep within running applications and Application Programming Interfaces (APIs). This synergy provides the missing fidelity needed, allowing security teams to extend Sumo Logic's powerful analytics to the application layer and create definitive, context-rich Insights that unify the security narrative from the infrastructure to the code.

The application-layer intelligence gap

Effectively monitoring the application layer is a persistent challenge for security operations. Traditional tools like WAFs and scanners flood the SOC with low-context alerts based on pattern matching, contributing directly to the alert fatigue that modern Security Information and Event Management (SIEMs) tools are designed to solve. Recent research shows that fewer than 0.25%[1] of WAF alerts correlate to a real exploit; the rest are benign probes or noise. Without the ability to confirm if a vulnerability was actually exploited, analysts are forced to investigate low-context alerts, wasting valuable time and preventing the SIEM's correlation engine from accurately identifying and prioritizing genuine threats. This intelligence gap means that even a modern SIEM can be limited by the poor quality of the data it ingests.

Connecting runtime behavior to SIEM analytics

The Contrast ADR integration solves the application intelligence gap by embedding a threat sensor directly within running applications and APIs to observe their real-time behavior. Instead of guessing from the perimeter, Contrast confirms — by observing behavioral anomalies within the application — whether an attack was successful or blocked, or if it was just a probe. This unique runtime visibility generates a stream of high-fidelity Application Security (AppSec) records and signals — the foundational elements of Sumo Logic's analytics.

This stream of verified threat data acts as a supercharger for Sumo Logic's intelligence engine. The platform's adaptive signal clustering engine correlates Contrast's precise application attack signals with events from endpoints and cloud infrastructure to create definitive insights. These enriched Insights provide analysts with a single, correlated view of an attack chain, including details of threats that Contrast proactively blocked at runtime to prevent exploitation. To accelerate resolution, Contrast's agentic AI remediation identifies the root cause and provides code-level fixes straight to the developer, allowing SOC teams to focus their own efforts on containment and investigation.

This deep integration empowers security teams using Sumo Logic Cloud SIEM

Pinpoint the attacker's entry point

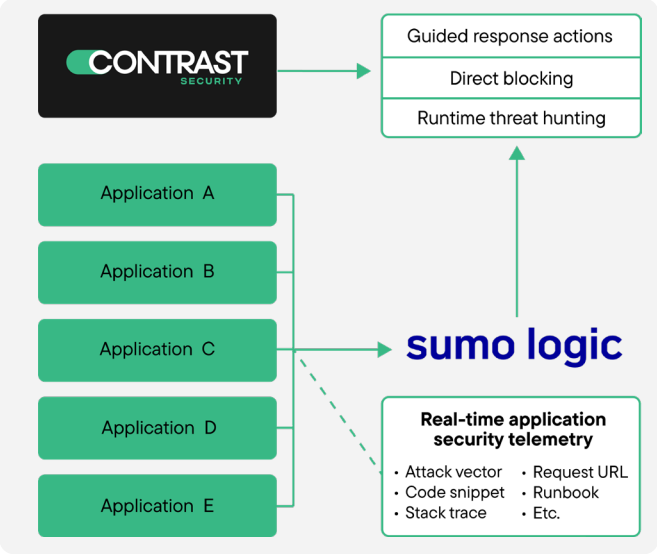
Immediately understand how an attacker compromised an application with runtime data inside of Sumo Logic.

Proactively stop breaches

Prevent application and API breaches by identifying and blocking attacks at runtime.

Reduce the attack surface

Close the loop on application incidents faster as an AI agent generates the code fix, permanently stopping the threat.



Sumo Logic SIEM application security use cases

Focus SOC teams on confirmed threats

Challenge: Noisy, low-context alerts from perimeter tools overwhelm analysts and prevent them from identifying real threats.

Solution: Contrast provides a stream of verified alerts on genuine runtime attacks. Sumo Logic correlates this accurate data to create prioritized incidents, allowing analysts to focus on investigating confirmed threats, not false positives.

Accelerate incident investigation

Challenge: When an application is breached, analysts waste critical time trying to determine the attack's entry point and the underlying vulnerability.

Solution: Contrast enriches security incidents with the specific attack vector and the vulnerable line of code. This allows analysts to immediately understand the root cause, shortening the investigation phase and allowing them to focus on impact analysis and containment.

Enable full-stack threat hunting

Challenge: Threat hunters often lack the application-level data needed to investigate sophisticated attacks, leaving a critical blindspot.

Solution: Contrast streams rich application security data into Sumo Logic. Analysts can then use Sumo Logic's powerful query capabilities to hunt for subtle indicators of compromise across their full technology stack.

Ready to see Contrast in action?

Ready to enrich your Sumo Logic Cloud SIEM deployment with deep application and API security intelligence? Visit our website or request a demo today to discover how Contrast Security can help you achieve a more comprehensive and actionable view of your application risk.

Try Contrast

[1] ADR vs EDR and WAF | Application Security Tool Comparison

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