SOLUTION BRIEF

Contrast Application Detection and Response (ADR) + SIEM

Integrated runtime protection and confirmed exploit data into the SIEM

With one in four attacks targeting public-facing applications,[1] the application layer has become a primary battleground for enterprise security. For Security Operations Centers (SOCs), this creates a significant challenge for their primary data source: the Security Information and Event Management (SIEM) platform. Most SIEMs rely on data from perimeter tools that are blind to the application's internal runtime, leading to a flood of low-context, noisy alerts. This data overload is why 83% of SOC professionals report being overwhelmed by alert volume,[2] a problem that directly impacts their ability to distinguish real threats from noise.

Contrast Application Detection and Response (ADR) solves this by fundamentally changing the quality of application data the SIEM ingests. By moving from noisy perimeter guesswork to confirmed findings from within the application runtime, Contrast enables SOC teams to eliminate ambiguity, block attacks at the source and use the SIEM for what it does best: correlating high-fidelity threat intelligence.

The application data quality issue

For a SOC, the effectiveness of its SIEM is entirely dependent on the quality of the data it receives. The application layer, a primary target for attackers, is notoriously difficult to monitor accurately with traditional tools. Perimeter defenses like Web Application Firewalls (WAFs) lack insight into application execution and are prone to false positives, flooding the SIEM with alerts that are not actual exploits. One study found that fewer than 0.25% of WAF alerts correlate to a real attack.[3]

This data quality gap creates significant operational challenges. Analysts spend valuable resources investigating alerts that pose no real threat, driving up costs and leading to burnout. This constant noise not only masks genuine threats but also has major financial implications. With the average cost of a data breach hitting a record $4.88 million, the ability to eliminate false positives and focus on credible threats becomes a critical operational and financial imperative.

Connecting runtime behavior to SIEM analytics

Contrast ADR embeds instrumentation directly within running applications and APIs, providing a definitive, inside-out view of application behavior. Instead of inferring threats from the outside, Contrast observes them from within the code as they execute. This unique position allows it to not only detect malicious activity with high accuracy but also to actively block exploits before they can succeed.

This stream of verified, high-fidelity threat data transforms your SIEM operations. Every alert sent to the SIEM is a real, confirmed threat with 100% correlation to an exploit,[4] limiting false positives and allowing your team to focus on what matters. These incidents are enriched with the exact attack vector, vulnerable line of code and full payload — the ground-truth data analysts need for immediate root cause analysis. Most importantly, Contrast provides the ability to neutralize attacks as they happen, preventing breaches at the application layer and reducing the number of incidents the SOC needs to manage downstream.

This deep integration empowers security teams integrating ADR into their SIEM to:

Prevent breaches at runtime

Actively block and neutralize exploits in real time, including zero-day attacks, preventing them from ever becoming a security incident that requires a full-blown response.

Reduce false negatives

Drastically reduce noise by feeding the SIEM a stream of accurate threats, allowing analysts to focus their expertise on high-impact investigation and threat hunting.

Accerlerate incident response

Equip analysts with definitive context within their SIEM, enabling them to understand the root cause of an attack in minutes, not hours, and measurably reduce Mean Time to Remediation (MTTR).

Streamlining incident response: A workflow comparison

The integration of Contrast ADR into a SIEM fundamentally redefines the response to application-centric threats. The table below compares the inefficient, perimeter-based approach with the decisive, runtime-powered workflow enabled by Contrast.

	Traditional workflow (Perimeter-based alerts)	Modern workflow (Contrast ADR-powered)
Initial alert	Receives a low-context, ambiguous alert from a WAF, requiring manual validation.	Receives a high-fidelity alert for a confirmed exploit, with full context.
Triage and validation	Analyst manually sifts through disparate logs to determine if the threat is real.	Analyst instantly verifies the threat was blocked at runtime; no validation needed.
Action and escalation	Wastes hours escalating a likely false positive to senior analysts or application owners.	Focus immediately shifts to permanent remediation as the threat is already neutralized.
Remediation	Concludes with a manual ticket for a potential issue, often after significant time has been wasted.	Contrast's agentic AI generates a code fix and pull request; the dev team simply reviews and approves.
Outcome	High MTTR, wasted resources and significant risk of analyst fatigue.	Incident contained in minutes, risk eliminated at the source, and an efficient, confident SOC.

Ready to empower your security operations?

Stop chasing ghosts and start blocking real attacks. Learn how Contrast Security can transform your SIEM's effectiveness with definitive, actionable intelligence from the application runtime.

Learn more

[1] IBM X-Force Threat Intelligence Index 2025

[2] Devo, The Evolution Toward an Alertless SOC, 2025

[3] Contrast Security, ADR vs EDR and WAF | Application Security Tool Comparison

[4] Internal Contrast Security Data

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