SOLUTION BRIEF

# Contrast and Splunk integration

## Executive summary of the integration

Contrast seamlessly integrates with Splunk, delivering deep application insights that empower SOC teams to identify and respond to sophisticated attacks faster. This integration seamlessly blends Contrast's deep application-layer insights with Splunk's powerful SIEM capabilities, enriching Splunk dashboards and searches with crucial application context.

## The application security blindspot

The application layer is a primary target for cyberattacks and one of the last refuges for attackers to hide. Traditional security tools struggle to provide adequate protection of web applications and APIs. Web Application Firewalls (WAFs) offer no protection to zero days and generate a high volume of alerts with limited context, many of which are false positives. If teams actively try to ingest and triage the resulting flood of alerts, the SOC is overwhelmed, with no choice but to disregard or disable these application alerts. This creates a gap in the company's defenses. Even when some application alerts are accurate, SOC teams often lack the application-specific context and expertise needed to effectively investigate and respond to these security incidents. This combination of alert fatigue, lack of context and limited visibility hinders an organization's ability to defend its critical applications and data.

## Application security with a unified solution

Contrast Application Detection and Response (ADR) and Splunk are a powerful combination for organizations seeking to elevate their security posture. Contrast ADR instruments applications from within, providing deep and continuous visibility into application behavior and identifying attacks with high accuracy. This real-time security telemetry is seamlessly integrated into Splunk, enriching security events with crucial application context. This empowers security teams to identify sophisticated attacks that bypass traditional tools, accelerate investigations and remediate with correlated data.

By combining high-confidence application security insights with broader security context, SOC teams can achieve a unified view of their security landscape to significantly reduce MTTD and MTTR for application attacks.

This real-time data is seamlessly integrated into Splunk, enriching security events with crucial application context and enabling the SOC to:

### Detect application threats

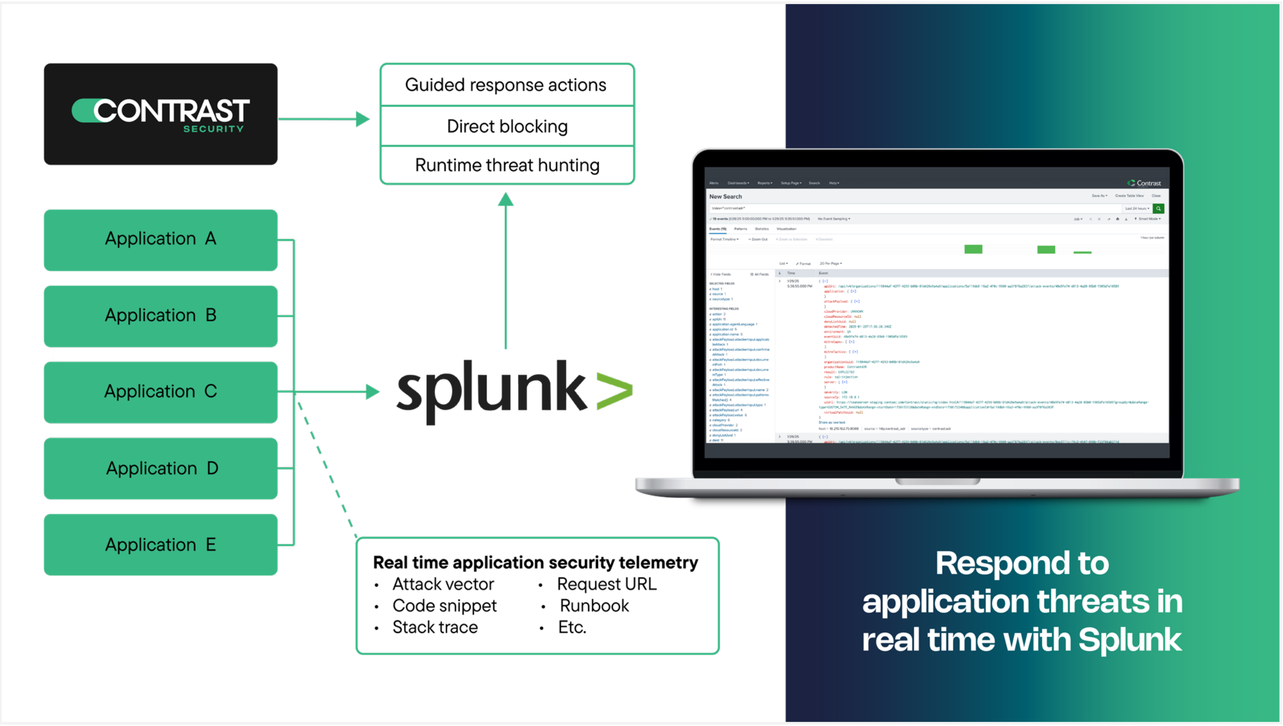
Gain actionable insights into application attacks by correlating security events with real-time application behavior.

### Investigate with context

Enrich Splunk security investigations with deep application context for faster threat analysis and response.

### Eliminate the noise

Focus on actual application threats with precise, actionable alerts within Splunk.



Respond to application threats in real time with Splunk

# Solving application security challenges

## Gain deep application visibility and control

### Challenge

Traditional tools miss attacks hidden within the application layer.

### Solution

Contrast ADR instruments applications for continuous visibility. Integrated with Splunk, SOC teams gain real-time context — down to the specific code exploited — to identify sophisticated attacks and guide faster, consistent incident response using runbooks.

## Detect and respond to zero-day attacks

### Challenge

Signature-reliant tools like WAFs are blind to unknown, zero-day exploits.

### Solution

Contrast ADR detects attacks based on actual malicious behavior, not just signatures. This real-time behavioral telemetry feeds Splunk, enabling rapid identification and response to novel threats targeting your applications.

## Uncover hidden threats and data exfiltration

### Challenge

Attackers exploit the internal application blindspot to conceal activity.

### Solution

Contrast ADR provides deep runtime visibility inside applications. Accurate telemetry in Splunk empowers SOC teams to hunt for Indicators of Compromise (IOCs), expose hidden threats and identify suspicious data exfiltration patterns.

## Get started today

Visit our website or request a demo today to learn how Contrast Security can empower your Splunk environment with deep application security insights.

Try Contrast