SOLUTION BRIEF

Contrast Application Detection and Response (ADR) and Datadog Cloud SIEM

Building the application SIEM for real-time threat response

Datadog has set the standard for unifying observability and security, enabling Dev, Sec and Ops teams to collaborate and move faster. By aggregating data from across the enterprise, Datadog provides powerful tools to detect and investigate threats. However, as organizations ingest logs from hundreds of sources, security teams still face a significant challenge: isolating verified application attacks from the noise of performance metrics and low-context perimeter alerts.

The Contrast Security Application Detection and Response (ADR) integration solves this by enriching Datadog Cloud SIEM with a stream of verified, context-rich security intelligence from deep inside running applications. This synergy delivers the missing application security context needed to transform how teams detect, triage and respond to threats targeting their applications and APIs.

The application security context gap

Datadog Cloud SIEM excels at unifying security and operational data, allowing teams to detect and investigate anomalies across dynamic environments at scale. However, even with this powerful foundation, security teams face a universal challenge when securing custom applications: distinguishing a genuine attack from the noise of benign traffic and low-context perimeter alerts. The problem is often the data itself. Perimeter tools like WAFs can flood the platform with alerts that have less than a 0.25% correlation to real exploits[1]. This is because perimeter tools only see traffic coming into an application; they are fundamentally blind to what happens within the application's code and logic. This forces SOC analysts to spend valuable time manually validating threats, searching for a needle in a haystack and slowing down incident response.

Runtime behavioral detection in Datadog

The Contrast ADR integration solves the context gap by delivering intelligence derived from behavioral anomaly detection from inside the application. By analyzing actual code execution and data flow from inside the application, Contrast moves beyond signatures to identify legitimate application-level threats with unparalleled accuracy. This high-fidelity approach becomes the foundation for confident automation and incident response, providing the validation and verification that Security Operations teams need to move from time-consuming manual investigation to automated security incident response and orchestration.

This method provides comprehensive coverage against critical attack techniques, from various forms of Injection (SQL, Command, XXE) to Server Side Request Forgery, techniques that network appliances and endpoint detection systems both typically miss It also offers deep visibility into sophisticated threats like Untrusted Deserialization, which accounts for 31% of viable attacks, according toContrast research[2]. Each verified threat becomes a high-confidence security signal in Datadog, serving as the perfect trigger to kick off an automated workflow.

Ultimately, this stream of verified intelligence unleashes the full potential of Datadog's platform. It allows security teams to build automated pipelines that triage incidents, create detailed work tickets, and notify on-call teams without manual intervention, dramatically reducing the time to respond to an ongoing incident. Instead of adding to the noise, Contrast Security delivers the clarity needed to automate triage and response for alerts from the application layer, transforming Datadog into the definitive Application SIEM for the modern SOC.

Gain comprehensive attack coverage

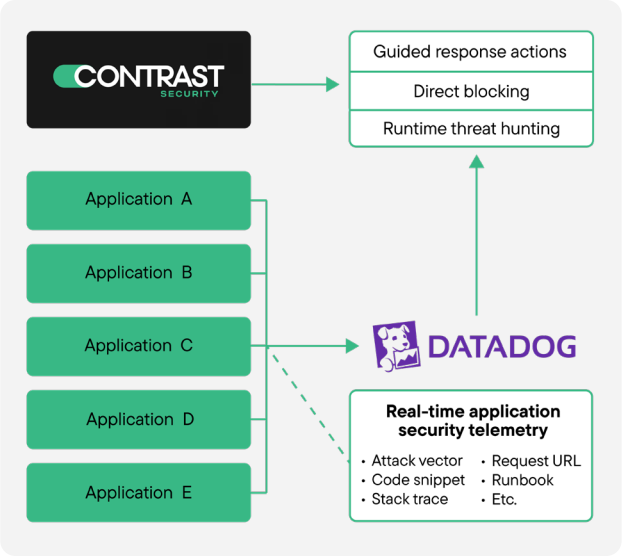
Use behavior-based detection to protect against entire classes of attacks—from SQLi and SSRF to unsafe deserialization—without relying on flawed signatures.

Responding to verified threats

Use accurate context-rich alerts from Contrast to safely trigger Datadog workflows and accelerate incident response.

Accelerate remediation

Deliver high-fidelity alerts to the SOC and code-level diagnostics to developers from a single data source in Datadog.



Datadog Cloud SIEM application security use cases

Confident response to zero-day exploits on entire classes of vulnerabilities (CWEs)

Challenge: Signature-based tools are blind to novel attacks, while SOC teams are hesitant to automate actions based on noisy alerts.

Solution: Contrast's behavioral analysis detects sophisticated attacks like untrusted deserialization without relying on signatures. Contrast can be configured to block the exploit attempt within the application, preventing any impact. The verified alert in Datadog then serves as a trigger for a workflow to add a malicious IP to a blocklist, page the on-call team, open an issue for tracking and automatically run an incident response runbook—all before a human even touches a keyboard.

Automated incident triage

Challenge: A generic alert from a perimeter tool forces a SOC analyst to spend valuable time manually investigating, gathering context from different systems and creating a ticket before they can escalate to the right team.

Solution: A verified and specific application security signal from Contrast ADR triggers a Datadog workflow. The workflow automatically creates a high-priority work ticket, populates it with the exact line of code and stack trace from Contrast, notifies the application owner, and runs security orchestration to mitigate the immediate risk, drastically reducing the time to respond to an ongoing application security incident.

Ready to see Contrast Security + Datadog in action?

The Contrast Security integration for Datadog Cloud SIEM delivers the accurate, application runtime intelligence you need to stop hunting for threats in logs and start automating your response. Transform your SOC's efficiency and gain a comprehensive view of application risk, all within the Datadog platform you already use.

Request a demo today to see how you can use Contrast and Datadog to automate triage, respond with confidence and unify your security and development teams.

Try Contrast

[1] ADR vs EDR and WAF | Application Security Tool Comparison
[2] Software Under Siege 2025

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