SOLUTION BRIEF

The future of runtime security

How Application Detection and Response redefines application security

With one in three intrusions starting with vulnerability exploitation,[1] a layered application defense is essential. Many security teams pair a Web Application Firewall (WAF) with a Runtime Application Self-Protection (RASP) tool. The goal is for the RASP to provide the deep, internal visibility the WAF lacks and to reduce the noise from the perimeter.

This noise reduction is critical, as WAFs generate a high volume of low-context alerts with signals showing less than a 0.25% correlation to real exploits.[2] However, this strategy often falls short due to the architectural limitations of non-behavioral RASP solutions, such as those from vendors like Imperva, Rapid7 and Datadog. This pattern-matching approach often isn't the definitive source of ground truth. It can miss modern, context-aware attacks and, crucially, it does not connect a blocked threat to the specific vulnerability in the code.

The result is that even with two layers of defense, the application security backlog still grows by an average of 11 vulnerabilities per month.[3] This predictable and persistent state of vulnerability is precisely why the application layer has become the primary front for initiating a breach.

The operational challenges of non-behavioral RASP

Complex deployment and management

Non-behavioral RASP solutions are known for creating significant operational hurdles. Customers consistently report challenges with complex installation, configuration, and ongoing management, especially at an enterprise scale. The specific agent-management and constant tuning introduce performance overhead and operational friction. This often leads to mass deployment across the enterprise portfolio rarely being achieved, forcing teams to leave large parts of their application portfolio exposed.

Stagnant and unsupported

Oftentimes, RASP solutions are a secondary feature within a larger vendor portfolio without a core runtime focus. This frequently results in slower product evolution and less dedicated technical support, leaving customers with a solution that struggles to keep pace with modern application threats and development practices.

CAN YOU STOP THESE ATTACKS?

According to the 2025 Software Under Siege Report, these are the top 5 most prevalent and successful attack techniques targeting applications.[3]

1. Insecure Deserialization (31%)
2. Business Logic Abuse (22%)
3. Broken Access Control (14%)
4. SQL Injection (9%)
5. OS Command Injection (7%)

A "WAF-on-a-server" approach that impacts workflows

Operationally, these tools often function like an on-the-server WAF. Their pattern-matching methods are typically restricted to surface-level request inspection and do not discover vulnerabilities in the code. This lack of deep intelligence translates to limited workflow support. It creates a disconnect for development teams by failing to provide vulnerability context and, for the SOC, it generates alert fatigue instead of providing actionable intelligence.

The ADR advantage: Combining protection, remediation and response

The objective of a modern runtime platform is not merely to block attacks but to function as the source of ground truth for application risk. This requires a fundamental paradigm shift from shallow, input-aware protection to deep, behavior-aware security instrumentation. This is Application Detection and Response (ADR), and it works at the speed of threat actors, ensuring you are always protected.

Core capabilities of an ADR platform

At the core of the platform is the Contrast Graph, a real-time model of the entire application layer built from runtime telemetry. It maps the architecture, data flows and dependencies across all monitored applications and services.

Achieve full visibility with behavioral analysis

A modern runtime security solution uses behavioral analysis to monitor an application's execution and data flow. By understanding the application's intended logic, it accurately identifies true threats with low false positives, eliminating the noisy alerts that plague legacy tools.

Accelerate remediation with precise vulnerability findings

When an active threat or test payload exercises an exploitable vulnerability, ADR provides a complete, high-fidelity issue report directly from the production environment. It delivers the exact line of vulnerable code, the full stack trace and AI-powered suggested fixes, focusing developer effort on vulnerabilities that present the most immediate danger.

Unify security with native SOC integration

ADR enriches the SOC's incident workflow with high-fidelity, application-layer telemetry. By feeding contextual alerts directly into SIEM platforms, it allows incident responders to correlate application-layer attacks with events from across the enterprise kill chain, reducing Mean Time To Resolution (MTTR).

Traditional defenses (WAF + non-behavioral RASP) vs. modern ADR

Attribute	Traditional defenses (WAF + non-behavioral RASP)	Contrast ADR
Detection method	**Input-focused:** Analyzes request structure and grammar, creating blind spots for context-aware attacks.	**Behavior-based:** Analyzes runtime execution and data flow, providing high-fidelity protection against entire vulnerability classes.
Developer output	**Disconnected, high-level alerts:** Might confirm a block but provides no automated link to the specific vulnerability.	**Code-level context:** Delivers the exact line of code and automatically reprioritizes the associated vulnerability.
SOC integration	**Siloed data:** Owned by AppSec, limited ownership within SecOps.	**Integrated telemetry:** Feeds rich, contextual intelligence directly into the AppSec and SecOps workflow, unifying security visibility.

Learn more

[1] Mandiant M-Trends 2025 Google Cloud

[2] Contrast Labs Research uncovers: EDR's blindness to application exploits, WAF's inability to cut through the noise

[3] Contrast Security 2025 Software Under Siege Report

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