CONTRAST SECURITY

SOLUTION BRIEF

Moving beyond RASP

The evolution to Application Detection and Response (ADR)

The reality that 33% of all breaches[1] now begin with the exploitation of a software vulnerability has created an urgent demand for a new class of defense. Applications and APIs are under constant attack, absorbing an average of 14,250 hits every month.[2] While organizations struggle to manage this volume, the problem is compounded by a backlog that grows by 17 or more new vulnerabilities per application monthly.

This disparity creates a critical operational gap. AppSec teams are accountable for the application's defense but are not built for 24/7 incident response. Conversely, 24/7 SecOps teams are built for response but lack the deep application visibility and control required to distinguish noise from actual threats. Unless an organization is confident it produces perfect code and uses perfect libraries, a new approach is needed.

The evolution of application defense

To understand the path forward, we must look at how defense layers have evolved.

2000s WAF

The Web Application Firewall (WAF) remains a critical component today for mitigating volumetric threats like DDoS attacks. However, because it focuses on filtering HTTP traffic, it lacks visibility into application logic. It cannot see how code processes data, forcing teams to guess if an attack succeeded or failed.

2010s RASP

Runtime Application Self-Protection (RASP) represented a massive leap forward, embedding security inside the application to stop exploits at the source. However, RASP often operated as a silo—effective at blocking attacks, but leaving SecOps blind to the incident details and AppSec without a quick path to resolution.

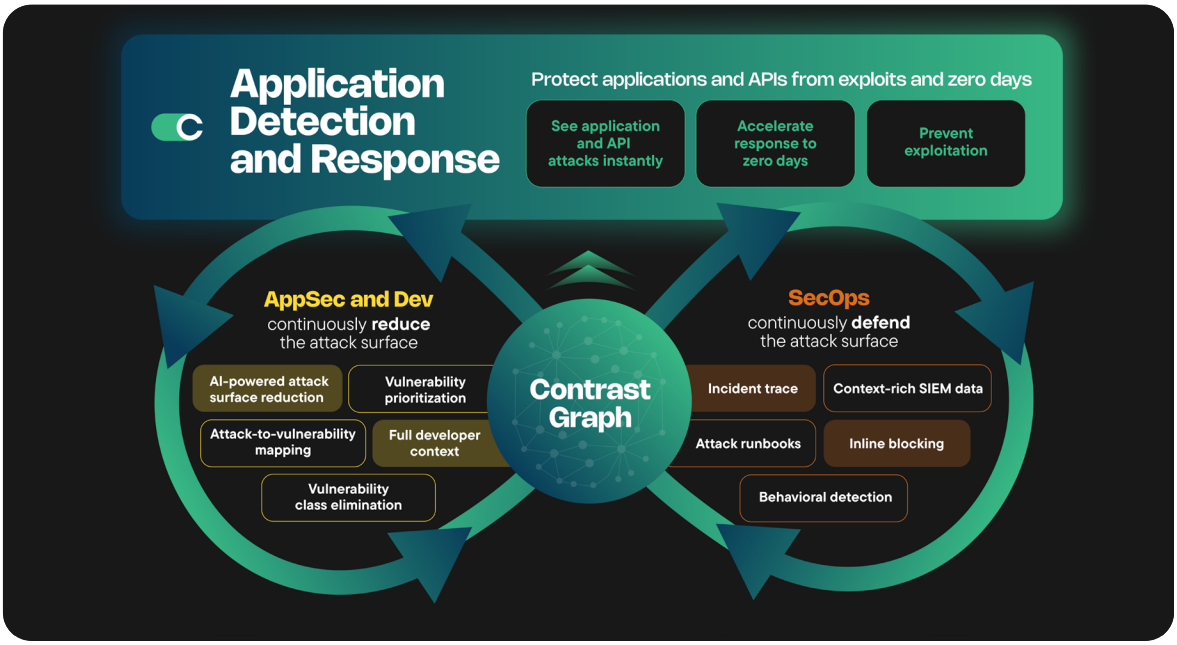
Now ADR

Application Detection and Response (ADR) fills the application-layer gap in the broader detection and response ecosystem. This shift acknowledges that applications will have vulnerabilities and that the focus needs to be on being ready to respond to incidents and issues.

The engine of context: The Contrast Graph

Contrast ADR is built from the ground up on a modern streaming architecture. While it delivers the same precise blocking outcome as RASP, it leverages the Contrast Graph to create a real-time digital twin of your application. This allows it to stream telemetry and correlate threats to vulnerabilities—transforming isolated blocking events into a complete detection and response workflow.

While other tools see isolated events, Contrast ADR leverages the Contrast Graph to continuously map the relationships between active attacks, underlying vulnerabilities, and the specific code paths being targeted. By observing software behavior from within running applications and APIs, this architecture delivers massive performance innovation and enables confirmed detection of attacks and continual monitoring of vulnerabilities in production.



Linking protection to response workflows

A mature cybersecurity program relies on two parallel missions: continuously defending the attack surface to stop breaches, and continuously reducing the attack surface to eliminate risk. Traditional tools force a trade-off between these goals, isolating the SOC's need for immediate response from AppSec's need for permanent remediation. Contrast ADR bridges this divide. It unifies these critical functions, empowering SecOps to neutralize active threats in real-time while simultaneously arming AppSec with the deep context needed to eliminate the underlying vulnerabilities for good.

Detection and response

- **Inline blocking:** Neutralize exploits inside the running code stopping attacks before full execution.
- **Native SIEM integration:** Integrate with the SOC by sending verified, code-level incidents—not just noise—via native SIEM integrations.
- **Incident trace:** Equip responders with a visual execution path of the attack, including stack traces and payloads.
- **Behavioral detection:** Identify and block novel and zero-day attacks that use known techniques, even without a specific CVE.

Risk prioritization and attack surface reduction

- **AI-powered attack surface reduction:** Leverage agentic Contrast AI SmartFix to automatically generate code fixes and pull requests for identified issues.
- **Attack-to-vulnerability mapping:** Know the exact vulnerability that is under attack to prioritize true risk over theoretical backlog.
- **Vulnerability class elimination:** Neutralize entire categories of vulnerabilities (e.g., deserialization) at the framework level.
- **Full developer context:** Provide the exact line of code and data flow to drive faster, permanent fixes.

Closing the loop on application risk

The goal of modern application security is to ensure the same attack can't happen twice. Contrast ADR facilitates a continuous loop: the attack is verified and blocked, the vulnerability is confirmed, and an AI SmartFix is generated.

Try Contrast

[1] M-Trends 2025 Report
[2] 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