SOLUTION BRIEF

Application Detection and Response (ADR) + WAF

Defense-in-depth for modern applications

The initial access point for one-third of all breaches is the exploitation of a software vulnerability. This is the reality of the current threat landscape, where attackers have shifted their focus from the network perimeter to the application layer itself. The rise of generative AI is accelerating this trend, enabling adversaries to create sophisticated and novel attacks at an unprecedented scale.

This new reality requires a security strategy that extends beyond traditional perimeter defenses. While Web Application Firewalls (WAFs) remain a foundational component of security, a defense-in-depth approach that provides visibility from the network edge to the application's code is now essential.

The necessary first line of defense

A WAF is a critical component for any organization's security posture. It provides an essential first pass on all incoming traffic, acting as a frontline defense against a high volume of known threats. WAFs are effective at mitigating DDoS and other volumetric attacks, filtering out malicious bots and scanners, and blocking common attack patterns that match predefined signatures and rules. By handling this high-volume, low-complexity traffic at the network edge, WAFs provide a valuable layer of protection.

However, the operational model of a WAF is to analyze traffic from the outside-in. It makes decisions based on traffic patterns and signatures without having insight into how the application is actually processing a request. This architectural reality means that WAFs can be bypassed by sophisticated attacks that use novel or obfuscated techniques to appear as legitimate traffic. This creates a security gap between the perimeter and the application runtime.

The application-layer blind spot

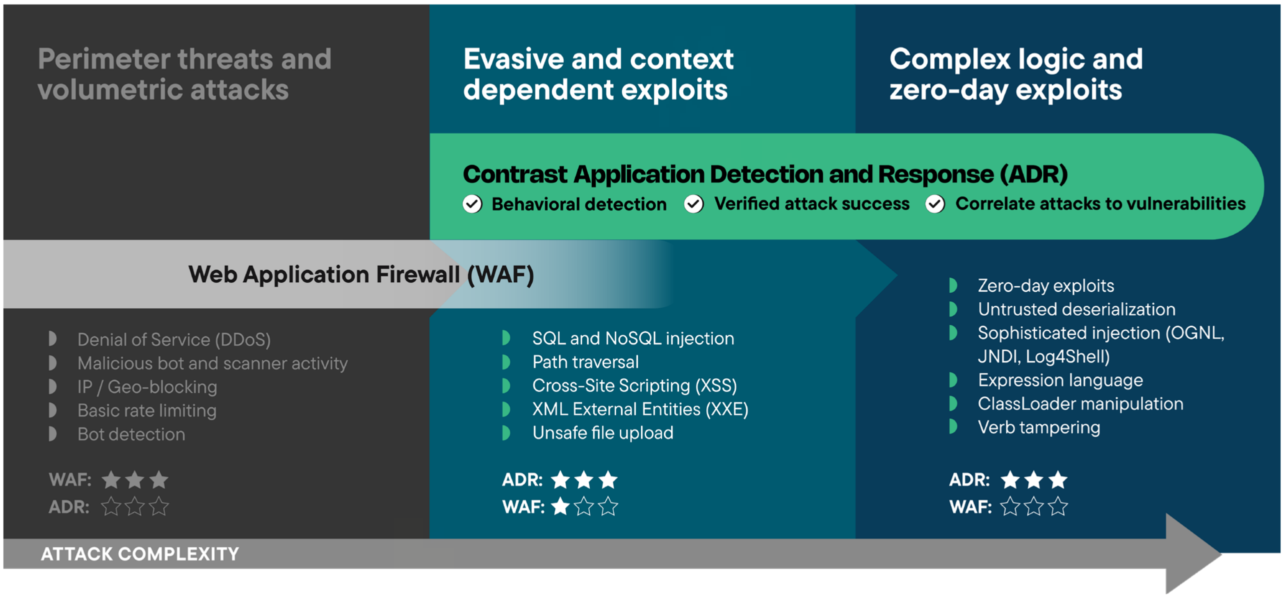
Attackers are increasingly bypassing perimeter defenses, with our research indicating that over half of all successful application attacks utilize such evasion techniques. A significant portion of these, 31% of viable attacks,[2] leverage insecure deserialization. These attacks are particularly challenging for Web Application Firewalls (WAFs) to detect, as the malicious payload is frequently concealed within data streams that appear legitimate.

This creates a significant challenge for security teams. They are often faced with a high volume of low-fidelity alerts from their WAFs, with less than 0.25%[3] of these alerts correlating to actual exploits. This flood of false positives consumes valuable time and resources, while the real, sophisticated attacks slip past the perimeter undetected.

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.[1]

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



Perimeter threats and volumetric attacks

- Denial of Service (DDoS)
- Malicious bot and scanner activity
- IP / Geo-blocking
- Basic rate limiting
- Bot detection

WAF: ★★★
ADR: ☆☆☆

Evasive and context dependent exploits

- SQL and NoSQL injection
- Path traversal
- Cross-Site Scripting (XSS)
- XML External Entities (XXE)
- Unsafe file upload

ADR: ★★★
WAF: ★☆☆

Complex logic and zero-day exploits

- Zero-day exploits
- Untrusted deserialization
- Sophisticated injection (OGNL, JNDI, Log4Shell)
- Expression language
- ClassLoader manipulation
- Verb tampering

ADR: ★★★
WAF: ☆☆☆

Contrast Application Detection and Response (ADR)
✓ Behavioral detection ✓ Verified attack success ✓ Correlate attacks to vulnerabilities

Web Application Firewall (WAF)

ATTACK COMPLEXITY

Closing the gap with runtime security

To close this gap, security teams need to see what is happening inside the application. Contrast Application Detection and Response (ADR) provides this crucial runtime security. By using lightweight instrumentation that operates from within the application's runtime, ADR can observe the actual behavior of the code as it executes.

This approach provides two fundamental advantages:

- **Certainty:** Contrast ADR verifies every alert against the application's actual execution. This allows it to differentiate between a harmless probe and a genuine exploit with perfect accuracy, delivering alerts with a 100% correlation to real attacks.
- **Precision:** With deep visibility into the application's code, ADR can identify and block entire classes of vulnerabilities, including complex injection attacks and zero-day exploits that do not have a known signature.

A complete defense: From the network to the code

Pairing a WAF with Contrast ADR creates a comprehensive, multi-layered defense that protects the entire application stack. In this model, the WAF continues to perform its critical function of filtering high-volume traffic and known threats at the perimeter. Contrast ADR then provides the critical security for modern attacks on applications.

This complementary approach provides security operations teams with:

- Confirmed breach prevention by stopping novel and zero-day attacks within the application.
- Accelerated incident response with precise, code-level detail for every confirmed attack.

Try Contrast

[1, 2] Contrast Security 2025 Software Under Siege Report

[3] Research uncovers: EDR's blindness to application exploits, WAF's inability to cut through the noise, Contrast Labs, 2025

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