WHITEPAPER

Beyond signatures and system calls

Unmatched application protection with Contrast ADR

See real attacks inside of applications and APIs

A 34% surge in vulnerability exploitation marked a significant shift in how breaches began last year, with this method now accounting for 20% of initial access, according to Verizon's 2025 Data Breach Investigations[1] report. This surge puts immense pressure on security operations teams tasked with protecting vital applications and Application Programming Interfaces (APIs). Yet, these teams often find themselves battling tool limitations. Traditional Web Application Firewalls (WAFs) operating outside the application generate a flood of alerts based on simplistic traffic patterns, burying real threats in a sea of false positives.

Meanwhile, newer OS-level visibility tools, often leveraging technologies like eBPF, offer deep insights into kernel activity and system calls. While valuable for infrastructure monitoring, they fundamentally lack application context. They can't see inside the application's code, logic or data flows, making it difficult to accurately identify application-specific threats or understand their true risk, let alone respond effectively without disrupting the business. SecOps needs a better way to both detect and respond with precision.

Shining a light inside of applications with behavioral detection

Contrast Application Detection and Response (ADR) provides unparalleled visibility, accuracy and response capability by working from inside each application. Using threat sensors that integrate seamlessly and safely within the application runtime, Contrast gains continuous, deep runtime context — seeing actual code execution, data flow, library usage, configuration, backend connections and more, precisely as the application experiences them.

Contrast ADR leverages this deep context to perform behavioral detection, tracking data flow and analyzing code logic as it executes within the runtime. Unlike tools relying on signatures or system calls, runtime analysis identifies behavioral anomalies and malicious patterns based on their actual runtime interactions, pinpointing only genuine threats.

Accuracy, depth and response that other technology can't match

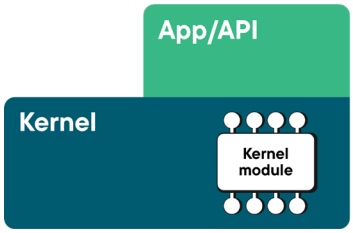
Operating from inside the application provides advantages unattainable by other methods:

True application context vs. OS-level view

While OS-level tools see system calls originating from various sources, Contrast ADR understands the specific application logic initiating many of those calls, providing crucial context. External tools often have to guess how the application will interpret complex payloads, leading to misinterpretations or missed attacks. Because Contrast ADR operates inside the runtime, it sees data after it's been processed by the application's frameworks, exactly as the application logic handles it, ensuring analysis is based on ground truth. Furthermore, this deep context enables precise response. Contrast ADR can prevent specific exploits attempts from causing damage while allowing legitimate users to continue using the app/API. By comparison, eBPF-based tools generally operate asynchronously, limiting their response options for application logic attacks primarily to reporting for external/delayed action (like packet filtering or sending notifications) rather than direct, inline prevention within the application flow. True ADR requires deep application context for both accurate detection and precise response.

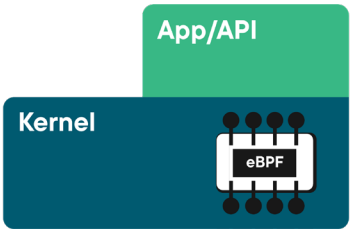
Cut through the WAF noise and protect against zero days

By analyzing actual application behavior and verifying risk within the runtime context, Contrast ADR distinguishes attempted exploits from legitimate software behavior. This accuracy not only stops the flood of false positives but also gives teams the confidence to enable active blocking, knowing that legitimate activity won't be impacted. Furthermore, unlike signature-based WAFs that require constant updates for new threats, Contrast ADR's behavioral detection focuses on the underlying techniques (the classes of attack). This allows it to detect and block novel variants and even zero-day attacks that exploit vulnerabilities within known classes (like SQLi, path traversal, etc.) without requiring specific signatures. Essentially, Contrast ADR takes critical tools out of the attacker's toolbox by preventing the core behaviors required to exploit applications.



Kernel module

- Runs directly in kernel
- Can see app/API interaction with kernel



eBPF program

- Runs in kernel with restrictions
- Can see app/API interaction with kernel

Software instrumentation

- Runs in user space without privilege
- Can see all app/API behavior with kernel

How Contrast detects and stops malicious behavior

Contrast's behavioral detection works through advanced analysis powered by unique runtime context. Contrast confirms active threats by observing their direct impact and identifying key behavioral anomalies across different dimensions:

- **Unsafe data flow during attack:** Contrast ADR traces malicious data seen during runtime from source to destination to verify if an active attack payload reaches a point where it can cause harm. This focus on reachability is key to eliminating alerts on theoretical attacks that have no real chance of succeeding.
- **Malicious intent/logic manipulation:** Contrast ADR analyzes the structure and logic of interpreted commands (like SQL queries) as they execute. Detecting if malicious input fundamentally changes a query's meaning or targets restricted system resources confirms an active attack's intent.
- **Applying targeted controls:** Contrast ADR applies targeted controls and sandboxing during high-risk operations (like deserialization or expression evaluation) to prevent known exploit paths from executing, effectively neutralizing attacks tailored to these risky functions.
- **Evasion resistance:** We handle common obfuscation techniques to ensure malicious attack payloads attempting to hide their anomalous behavior are still detected.

These are just some examples that show some of the essential detection techniques; Contrast ADR also recognizes other behavioral irregularities to ensure complete security. High-fidelity detection of runtime behavioral anomalies directly powers precise, optional in-application blocking of attacks. Contrast ADR can be configured to intervene exactly where needed, halting the specific malicious operation or request within the runtime, offering effective protection with minimal disruption.

Furthermore, when an attack is detected, the Contrast platform provides developers with rich diagnostic details about the underlying vulnerability, including the exact line of code, stack traces, data flow analysis and remediation advice, accelerating permanent fixes and improving the application's security posture.

Beyond individual CVEs: Protect against entire vulnerability classes

Contrast ADR's behavioral detection understands attack techniques, not just known patterns found in signatures. This provides inherent protection against many zero-day threats that exploit known vulnerability classes, closing the critical gap left by signature-based tools.

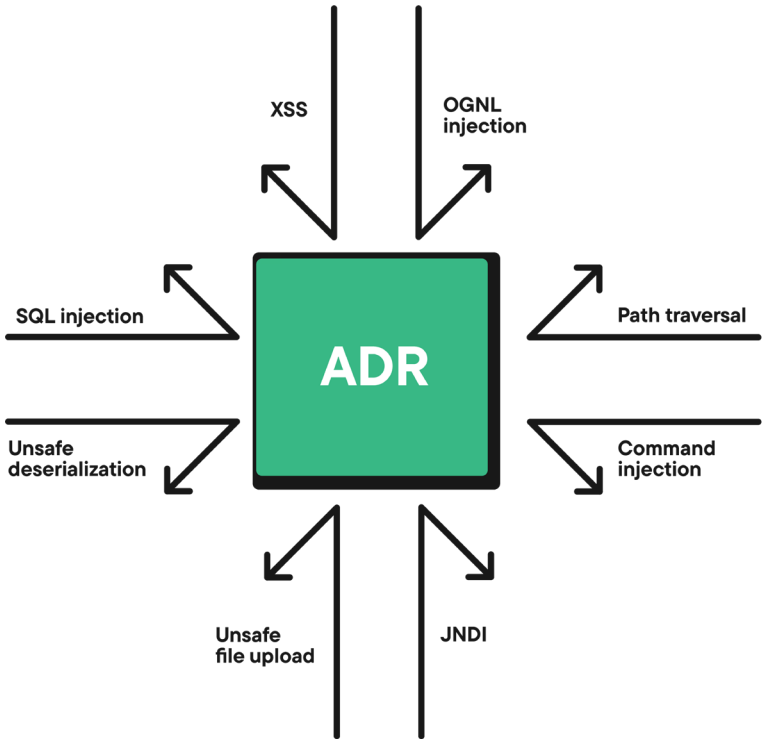
Detect and block the threats that matter most

Contrast's behavioral detection and response capabilities protect applications and APIs against a wide array of critical attack patterns. Contrast coverage includes crucial OWASP Top 10 risks and other sophisticated techniques attackers use to compromise applications from within.

- SQL injection/NoSQL injection
- Cross-Site Scripting (XSS)
- Command injection
- Path traversal
- Unsafe deserialization
- XML External Entities (XXE)
- OGNL injection
- ...and many more.

EFFORTLESS DEPLOYMENT, POWERFUL PROTECTION

Contrast ADR deploys easily via lightweight threat sensors with minimal performance overhead. Get accurate runtime protection without complex tuning or disruptive changes.



Actionable intelligence that accelerates and informs response

Detecting and blocking a threat is critical, but seamless integration into existing security operations is just as important. Contrast ADR provides rich, actionable intelligence that integrates seamlessly with leading SIEM platforms and ticketing systems. This allows SecOps teams to correlate Contrast's deep application insights with data from across their security stack, incorporating accurate application threats into their existing workflows.

Every alert includes precise context — exact code location, full data details, environmental specifics and more — slashing Mean Time To Detect (MTTD) and Mean Time To Identify (MTTI) and informing developers for faster Mean Time To Respond/Remediate (MTTR), all within the tools operations teams use every day.

Empower the SOC with true application visibility and control

With Contrast ADR, security operations teams can finally gain control over application risk. Empower the security operations center (SOC) to:

Focus on actual application threats	Prioritize high-fidelity alerts originating from deep within each application.
Gain full application visibility	See attacks unfolding inside the runtime where other tools are blind.
Detect critical threats	Ensure comprehensive coverage against sophisticated application-layer attacks.
Protect against zero days	Proactively block novel attacks exploiting entire vulnerability classes.
Respond with precision	Benefit from accurate, in-application blocking that stops attacks, not the business.
Accelerate incident response and remediation	Leverage rich, actionable context integrated into existing SOC workflows.
Secure applications and APIs	Effectively protect the complex applications and APIs that drive the business.

Ready to gain unparalleled visibility and control over application security?

Request a personalized demo

[1]2025 Data Breach Investigations Report, 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