

SOLUTION BRIEF

Contrast Application Detection and Response (ADR)

Protect applications and APIs from exploits and zero days.

Exploitation is outpacing security. Vulnerabilities are now exploited before patches exist, and attackers can move from initial access to impact in seconds. The mean time to exploit a vulnerability has dropped to an estimated -7 days, meaning exploitation now occurs, on average, before a patch even exists.¹ Once an attacker gains initial access, the hand-off to a ransomware operator takes a median of 22 seconds.¹ Traditional application security defenses and manual triage cannot operate at this speed.

The average application faces 81 confirmed, viable attacks every month that reach vulnerable code, while nearly 30 serious vulnerabilities sit in every production application.² AI is accelerating code production beyond human review capacity and at runtime, it doesn't matter who wrote a function if it's exploitable. Most security stacks can detect active attacks and, separately, vulnerabilities. They cannot tell whether an attack on an application is successful, what line of code is being exploited, or how those two facts are connected.

The closest most organizations get to application-layer defense is a WAF, which correlates fewer than 0.25% of alerts to actual exploits.³ Determining whether an active attack is reaching a real vulnerability in third-party or custom code requires visibility from inside the application. No perimeter, endpoint, or aggregation tool is architecturally capable of providing it.

See and stop application and API exploits

Contrast Application Detection and Response (ADR) provides the attack detection and blocking that security teams need to secure the application layer. By embedding lightweight sensors into the application runtime, Contrast observes code execution, data flow and request handling to confirm what's actually happening.

Instead of inferring threats from external traffic patterns, Contrast ADR confirms them from inside the application. When a payload reaches and executes against vulnerable code, Contrast detects it, distinguishing a harmless probe from a genuine exploit without relying on signatures or rules. This inside-out approach delivers two fundamental advantages:

- **Verified detection:** Contrast ADR triggers an alert only when a payload has actually reached and executed against vulnerable code, not when traffic looks suspicious. That's the difference between inferring a threat and confirming one.
- **Precision blocking:** With execution-level visibility, Contrast ADR identifies and blocks entire classes of vulnerabilities — including complex injection attacks, unsafe deserialization, and zero-day exploits — without a CVE or signature to match against.

Most tools can't see the execution — and therefore can't stop these attacks.

According to the 2025 Software Under Siege Report, these are the top five most prevalent and successful attack techniques targeting applications.²

1. Untrusted Deserialization (31%)
2. Method Tampering (22%)
3. OGNL Injection (16%)
4. Path Traversal (13%)
5. Bot Blocker (7%)

See application and API attacks instantly

Detailed alerts on attacks to prevent exploits from succeeding

Accelerate response to zero days

Stop malicious activity in real-time and respond with guided runbooks

Prevent exploitation

Continuously monitor for vulnerabilities in production

Every verified incident feeds directly into the Contrast Graph, the intelligence engine powering the broader Contrast platform. The Graph correlates live attack telemetry with known vulnerabilities to answer the question that matters most: which flaws are attackers actually reaching right now? When an attack successfully targets a vulnerability previously scored as medium severity, the Graph automatically elevates its priority based on observed production behavior rather than theoretical risk scores. That signal doesn't stop at the security operations team. When the Contrast Security platform confirms that a vulnerability is critical, it drives prioritization across development and AppSec workflows and powers AI-assisted remediation that closes the gap between what's being exploited today and what gets fixed tomorrow.

Security teams stop triaging based on assumptions and start acting on evidence.

Architectural defense built for the modern security stack

Because Contrast operates from within the application, it requires no network configuration changes, decryption, or rule tuning. The lightweight, instrumentation-based agents are built for production environments, ensuring minimal performance overhead measured in less than a millisecond. This approach supports all major languages across cloud, container, and server environments without disrupting existing deployment pipelines.

Key integrations

Splunk, Microsoft Sentinel, IBM QRadar, CrowdStrike Falcon, Datadog, Google SecOps, Sumo Logic, plus any SIEM via the Universal ADR Forwarder.

From detection to action

In an environment where AI is accelerating both code creation and attack execution, theoretical risk scores are no longer enough. Contrast ADR confirms which attacks are actively reaching vulnerable code, blocks them in real time, and generates runtime evidence that enables faster, more precise downstream decisions. Organizations that wait for patch cycles and perimeter alerts to tell the story will always be a step behind. Runtime visibility is not an upgrade; it is an absolute necessity.

[Learn more](#)

¹ Mandiant M-Trends 2026 Report

² Contrast Security, 2025 Software Under Siege Report

³ Contrast Labs, 2025