CONTRAST SECURITY

Three steps to block CVE attacks in real time

Stop exploitation before patches exist with Contrast CVE Shield

The three steps

STEP 1

Validate reachability with scope sensors

Pre-production scanners cannot tell you if a vulnerable method actually executes. Instrument scope sensors around vulnerable methods in each CVE definition to observe reachability continuously as a byproduct of live traffic.

DO THIS: Sort your CVE backlog by runtime reachability. Suppress unexecuted CVEs and escalate those with active sensors under production traffic.

STEP 2

Detect active exploit attempts

CVE Shield detects the instant a CVE is triggered in a live exploitation attempt, whether the payload is hand-crafted or AI-generated. Every detected trigger links directly to its specific CVE ID.

DO THIS: Review detection activity during Monitor mode. Prioritize CVEs showing live trigger activity for advancement to Block mode.

STEP 3

Enforce per-CVE micro-sandboxing

The per-CVE microsandbox enforces a targeted allowlist of system-level capabilities while execution is inside the vulnerable scope—blocking OS process execution, JNDI lookups, and remote class loading at the JDK call regardless of payload encoding.

DO THIS: Run Monitor mode for 1–2 weeks to baseline legitimate behavior. Advance to Block mode per CVE, starting with the highest-severity reachable CVEs.

THE NUMBERS THAT MATTER

28.3%
of CVEs exploited on or before day of disclosure

82%
false-positive rate in legacy scanning tools

30%
of CVEs in an application are active in production

Questions to ask before you buy or renew

- When a critical CVE drops on a Friday, how long before I know whether we are exposed — and what is the compensating control during that window?
- When a critical CVE drops on a Friday, how long before I know whether we are exposed — and what is the compensating control during that window?
- Does your runtime protection give me a per-CVE allow list, or a global behavioral policy?
- Can your tool show me a SOC incident for a blocked exploit — pre-enriched with CVE ID, CWE, and full call stack — without manual log correlation?
- How does your tool handle novel payload variants and AI-generated exploits that bypass signature-based detection?

Download the full guide

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.

© 2026 Contrast Security, Inc.

contrastsecurity.com

6800 Koll Center Parkway
Ste 235
Pleasanton, CA 94566
Phone: 888.371.1333