CONTRAST SECURITY

Three steps to use runtime truth to harden AI-generated code

AI amplifies old bugs; runtime truth catches them.

The three steps

STEP 1

Establish runtime truth across the portfolio

Pre-production scanners cannot tell you which code paths actually run. Instrument the application runtime so exploitability, runtime SBOM and data flow are observed continuously as a byproduct of normal execution.

DO THIS: Capture a runtime baseline per app: exercised endpoints, loaded libraries, observed taint paths.

STEP 2

Protect in-process, prioritize by exploitability

Unpatched AI-introduced flaws receive structural protection at the sink while remediation is underway. Re-sort the open backlog on exploitability so the queue engineering actively works and shrinks sharply.

DO THIS: Re-baseline SLAs on exploitability, not CVSS. Accelerated SLA for exploitable code, sprint cadence for not.

STEP 3

Close the loop with runtime-guided remediation

AI-assisted fixes without runtime grounding are guesses. With the taint path, stack, and request attached, every fix is anchored in how the code actually behaves, and re-validated as traffic exercises it.

DO THIS: Pipe runtime evidence into IDE, PR review and any AI-assisted remediation in use.

THE NUMBERS THAT MATTER

Seconds
Median time to exploit after CVE disclosure

74 days
Average MTTR for critical app vulnerabilities

62%
Of libraries in apps never used at runtime

Questions to ask before you buy or renew

- Can you show me exploitability per finding, not just a theoretical CVSS score?
- Is your SBOM observed from the running process, or read from the manifest?
- For a detected vulnerability, can you deliver the taint path, stack and triggering request to the developer's IDE?
- Is the same agent used across dev, QA, CI/CD and production, or is it separate tools glued together?

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.

contrastsecurity.com

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