CONTRAST SECURITY

SOLUTION BRIEF

The application production gap

Security that follows your code into production

Traditional application security stops at deployment, leaving organizations with a fundamental blind spot precisely where attacks actually happen: in production. Meanwhile, perimeter defenses attempt to infer threats from network traffic, burying teams in alerts that lack context and have almost zero correlation to actual exploits.

Contrast takes a different approach. By embedding lightweight sensors directly into running applications, Contrast provides the visibility, attack data and prioritization signals that can only be captured from inside the code.

The runtime advantage

Day 1
Production attack visibility

~66%
Reduction in vulnerability triage workload[1]

< 1ms
Per-request latency impacy in production

The path to production

Contrast is designed for a frictionless, phased rollout — built to instrument your running applications without disrupting them.

1 Staging

Validate in staging first.
Run existing test suite.
Confirm performance.
No surprises
in production.

2 Monitor mode

Both outputs unlock immediately — before a single request is blocked.

- **Attack visibility**
  Confirmed attacks from inside the code.
- **Vulnerability prioritization**
  Stop triaging theoretical risk, fix what's under fire.

3 Blocking

Activate blocking incrementally, on your timeline.

From attack signal to fixed vulnerability — in real time

Runtime sensors continuously build the Contrast Graph: a live data model of every code path, library and dependency actually executing in production.

When an attack occurs, it is instantly correlated to the specific, exploitable vulnerability in the backlog. This is not a theoretical match — it is a confirmed link between the active threat and the required fix.

WITHOUT PRODUCTION CONTEXT

Perimeter noise: 10,000+ weekly WAF alerts completely disconnected from application code.

The blind spot: No visibility into application-layer attacks — for example, the single unsafe deserialization payload that slipped past the perimeter. This class of attack is just one of many that perimeter tools cannot confirm.

Static prioritization: An accurate backlog of possible vulnerabilities from staging, but zero intelligence on which ones are actively being exploited..

The reality: Remediation is prioritized by theoretical CVSS scores, not real-world attack activity.

WITH PRODUCTION CONTEXT

Attack confirmed: Contrast ADR flags a malicious unsafe deserialization payload executing in production.

Linked vulnerability: The attack is instantly mapped to the known vulnerability (*queue-processor.jar*) in the existing backlog.

Dynamic prioritization: The exact vulnerability under fire is immediately escalated to *critical* priority.

The reality: Live production attack data acts as the ultimate signal, telling teams exactly what to fix first.

Verified intelligence proves which vulnerability to fix first

Adding runtime security empowers AppSec teams to scale their impact without slowing down engineering workflows.

Definitive proof for developers

Because sensors observe actual code execution, every flagged vulnerability is a verified event. AppSec can prove exact exploitability, eliminating debates with engineering over what needs to be fixed.

Zero-day breathing room

Behavioral detection inside the runtime neutralizes novel attacks without requiring new signatures. This gives AppSec and engineering teams the time to properly test and deploy patches without emergency fire drills.

Developer-native remediation

Rich context — including stack traces and exact lines of code — flows directly into existing tracking tools. Contrast's SmartFix can even generate verified pull requests to propose the fix directly in the developer's workflow.

Zero engineering friction

The agent instruments at runtime. There is no redevelopment, no refactoring, and no code changes required to deploy protection.

Proven at scale: Backbase

Backbase, an AI-powered digital banking platform serving over 100 financial institutions, deployed Contrast across all environments by default.

> "You need to consider the fact that you will end up with vulnerabilities in your production environment anyway. So how are you going to deal with those?"
>
> *— Brian Vlootman, CISO, Backbase*

By catching threats from inside the application, Backbase identified critical vulnerabilities missed by other vendors and reduced the vulnerability triage workload by approximately 66%.[2]

Close the gap

As engineering velocity accelerates and the volume of code in production continues to grow, vulnerability triage becomes an unwinnable math problem. True prioritization requires more than just knowing what is exploitable — it requires knowing what is actively under attack. By correlating known vulnerabilities with live threat intelligence, Contrast provides the ground truth needed to identify exactly what is being weaponized right now.

Modern runtime protection automatically neutralizes attacks, decoupling immediate risk from the remediation lifecycle. Instead of disrupting engineering with emergency fire drills, AppSec can provide the breathing room needed to systematically test and deploy fixes on a standard schedule.

Ready to see what is actually running in production?

Talk to the Contrast account team today.

Try Contrast

[1,2] Backbase case study: When traditional AppSec reaches its limit

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