CASE STUDY

How a Fortune 500 firm prioritizes AppSec risk with runtime evidence

The problem: Millions of findings, no clear way to prioritize

The application security team supports more than 2,300 applications across retirement planning, investment management, and internal platforms. Like most large enterprises, they had invested in standard AppSec tooling — SAST in CI pipelines and DAST for testing.

What they didn't have was confidence.

"DAST had a lot of false positives," said Bob, who leads application security at the organization. *"SAST had noise as well. Cyber was often seen as telling teams what was wrong and to go fix it, without enough context on why it mattered."*

With many potential findings across tools, discovery wasn't the challenge. **Prioritization was.**

"If an application has too many vulnerabilities, what do you actually focus on?" Bob said. *"It's impossible to know."*

A 0.2% false-positive rate with IAST focuses developer effort on what matters.

Organization: Fortune 500 retirement and investment services provider

Challenges: SAST/DAST noise, limited context, friction with developers

Scale: 2,300+ applications, ~4,000 developers

Approach: Deploy Contrast Assess broadly and use runtime evidence as the prioritization arbiter

Validation: In an internal AppSec quality review, 0.2% of ~21,000 Assess (IAST) findings required follow-up, meaning nearly zero false positives.

Leadership identified the core gap: without runtime evidence, the team had no reliable way to separate real risk from background noise — or to credibly explain prioritization decisions to developers.

Why IAST: Runtime evidence as the deciding factor

The Log4j incident in late 2021 reinforced that gap.

"Infrastructure tools could tell us a library existed," Bob said. *"They couldn't tell us whether it was actually exploitable."*

What stood out about IAST was its ability to observe application behavior during testing and confirm whether vulnerabilities were reachable — not just theoretically present.

The team positioned Contrast Assess (IAST) as a validation layer across their AppSec stack. Rather than replacing SAST or DAST, Assess became the system for determining which findings warranted attention.

Deployment: Coverage first, confidence second

Given the organization's size and governance requirements, the AppSec team made a deliberate decision to establish broad coverage before driving remediation workflows.

"Our first mission was adoption," Bob said. *"Leadership wanted something that was simple and easy to deploy."*

Agent rollout is typically a multi-team effort. With Assess, deployment was centralized and managed by AppSec.

"Originally there were four or five touchpoints just to roll out the agent," said Priya, Application Security Specialist. *"We simplified it so AppSec manages the entire process. AppDev doesn't have to get involved."*

That approach enabled **security by default** — Assess running broadly across applications and microservices in monitoring mode, without adding developer friction.

Validation: 0.2% false-positive rate

Before using Assess to influence prioritization decisions, the AppSec team conducted its own internal quality review.

The team analyzed approximately **21,000 vulnerabilities** identified by Contrast Assess across severity categories and application types.

According to that internal analysis, only **~0.2% of findings required follow-up** for missing details, feature requests or product bugs.

"Everything else had solid evidence," Priya said. *"Across misconfigurations, injection issues, and other categories."*

For the team, the result mattered more than any external benchmark.

"We trust what it finds," Bob said. *"That confidence is critical when you're deciding what deserves developer time."*

How it works: Contrast as the prioritization arbiter

Rather than flooding developers with raw findings, the AppSec team uses runtime evidence to guide decisions.

Findings from SAST, DAST, and penetration testing are evaluated against Assess data.

- **If runtime evidence exists, the issue is escalated.**
- **If it doesn't, the issue is deprioritized.**

"If another tool flags something as high but we don't see runtime evidence in Assess, that changes the conversation," Bob said. *"Contrast becomes the decider."*

"At our scale, 100% is too much," Bob added. *"We need a way to decide what actually deserves attention."*

This approach reduces noise, limits unnecessary remediation work, and gives security and development teams a shared basis for decision-making.

Partnership that matters

For the AppSec team, Contrast stood out not just for the technology but for how the company engaged.

"I've worked with many vendors," Bob said. *"Contrast is at the top when it comes to how they engage. It's a real partnership. When we raise an issue, we know it's being tracked, documented, and taken seriously."*

That accountability reinforced trust in both the platform and the relationship.

"When you're building something that has to work at our scale," Bob said, *"that kind of partnership matters."*

The bigger picture: Prioritization that scales

For this organization, IAST isn't about discovering more vulnerabilities or generating more reports.

It's about focus.

"Contrast tells us when risk is real," Bob said. *"That's what allows us to prioritize."*

By using runtime evidence to validate findings, the AppSec team has built a durable foundation for prioritization — one that scales across thousands of applications and thousands of developers.

Identify vulnerabilities and stop attacks in real-time with Contrast Security

Try Contrast

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