CASE STUDY

When traditional AppSec reaches its limit

Beyond the AppSec blind spot

Brian Vlootman had done what the industry recommended.

As CISO of Backbase, an AI-powered digital banking platform serving 100+ financial institutions, Vlootman had implemented developer training, SAST, SCA, threat modeling and secure architecture principles.

"But the realization came that yes, you can do everything perfectly with these tools, but it is not enough," says Vlootman.

Traditional AppSec stops at deployment. Once code shipped to production, Backbase had no visibility into what was actually executing, how it was being attacked, or which vulnerabilities actually mattered.

Vlootman needed a different approach.

BACKBASE

Industry: Financial services

Location: Amsterdam

Challenges: Securing customized SaaS at scale, legacy risk, zero-day exposure

Contrast solutions: Contrast Application Detection and Response (ADR)

Benefits: ~66% less CVE triage, real-time attack blocking, higher developer trust

The challenge

Backbase faced what most maturing SaaS companies face:

- **Production was a black box:** Security teams had no insight into which code paths executed, which libraries loaded or how attackers probed applications once deployed.
- **CVE overload:** Every new open-source vulnerability triggered time-consuming triage with no data on actual risk. *"You cannot simply patch all the CVEs,"* Vlootman notes. *"That's just wasted effort."*
- **Legacy systems couldn't be patched:** Some customer deployments were years behind. *"They're so far left behind that deploying security patches was impossible,"* says Vlootman.
- **False positives destroyed developer trust:** *"Developers would see tons of findings. Because there were so many false positives, they didn't feel there was a good use of their time. It erodes the trust they have in the security tool."*
- **Exploit windows kept shrinking:** Zero-days and newly disclosed vulnerabilities were being weaponized faster than teams could test and deploy patches.

Vlootman realized Backbase needed to do more than chase vulnerabilities; they needed to start managing production risk.

Introducing Application Detection and Response

"You should not stop at the SDLC," Vlootman says. *"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?"*

Vlootman selected Contrast Security's Application Detection and Response (ADR) platform to close the gap between development-time security and production-time risk.

Introducing Application Detection and Response (cont.)

Because ADR instruments applications at runtime, it could be introduced without requiring application code changes, a critical factor for a platform with hundreds of customer-specific deployments.

Unlike traditional AppSec tools that analyze code statically, ADR instruments applications at runtime, revealing which code paths and libraries actually execute in production, which vulnerabilities are reachable and exploitable, how attackers are probing applications and provides real-time blocking of exploitation attempts.

During the proof of concept, Contrast's ADR found a SQL injection vulnerability that had been in production for years and missed by three prior security vendors.

"The first reaction was, wow, this is really something else," Vlootman recalls. *"This can find stuff that we would've otherwise missed."*

It wasn't just another tool. It was a different category of security.

What Application Detection and Response delivered

- **Developers got their time back:** By identifying which vulnerable components were actually executed in production, Backbase eliminated roughly two-thirds of CVEs from triage queues.

"The insight you get from ADR gives you an excellent data point to ignore some CVEs," says Vlootman. *"You can eliminate a lot of waste."*

- **Legacy systems became defensible:** ADR reduced risk for customer environments that couldn't be patched or upgraded. *"You get instant risk reduction and also the insight into what attackers are doing with your legacy systems that you otherwise would just have to treat as a black box."*

- **Zero-day exposure dropped:** *"There are a lot of CVEs that are just waiting to be found,"* Vlootman notes. *"Even if you do everything perfectly, it takes time to deliver the patch and roll it out. Having ADR there as another layer of defense is really, really valuable."*

When the next Log4j-scale event hits, Backbase will know immediately whether they're affected, and attackers will be blocked while patches are prepared.

- **Leadership gained confidence:** *"It's nice to know there's something monitoring production and blocking attacks,"* says Vlootman. *"The insight into what is actually running versus what we think is running gives you the confirmation you're looking at the right things."*

Making ADR the default

Vlootman made a critical decision: Application Detection and Response would be deployed by default across all platform environments, not offered as an opt-in.

Crucially, ADR can be deployed without requiring code changes or redevelopment, eliminating the friction that typically slows security adoption.

"We believed that having ADR in place for our production workloads helps reduce risk on our side, not just the customer side," Vlootman explains.

If it had been optional or required development effort, adoption would have been slow. Teams would only enable it after an incident, when it was too late. By making it default, every new project experiences ADR from development through production, building confidence across teams and eliminating deployment friction.

"Not just with the security team looking at Contrast, but also involving the project teams who need to make the change," Vlootman says. Teams see it work in dev and test before it reaches production, eliminating anxiety about introducing something into the critical path.

Looking forward

As AI accelerates both software development and attack velocity, Vlootman views Application Detection and Response as increasingly non-negotiable.

"If developers do not pay close attention, AI-generated code contains a lot of vulnerabilities," warns Vlootman. *"Instead of 1x vulnerable code you get 2x or 5x. Traditional SDLC tools cannot cope."*

Meanwhile, attackers using AI are exploiting vulnerabilities faster than ever. *"Because AI continues to drive and accelerate the exploitation of these vulnerabilities, the necessity to have ADR to protect your production workloads increases."*

Today, Backbase runs Application Detection and Response across its entire platform. *"Number one for me would be insight into production,"* Vlootman says. *"The second, especially as a CISO, is the peace of mind that even if you've missed something, you still have another layer of defense. And the third would be the fact that you can leverage ADR at scale, from one to 10 to 100 to a thousand applications."*

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