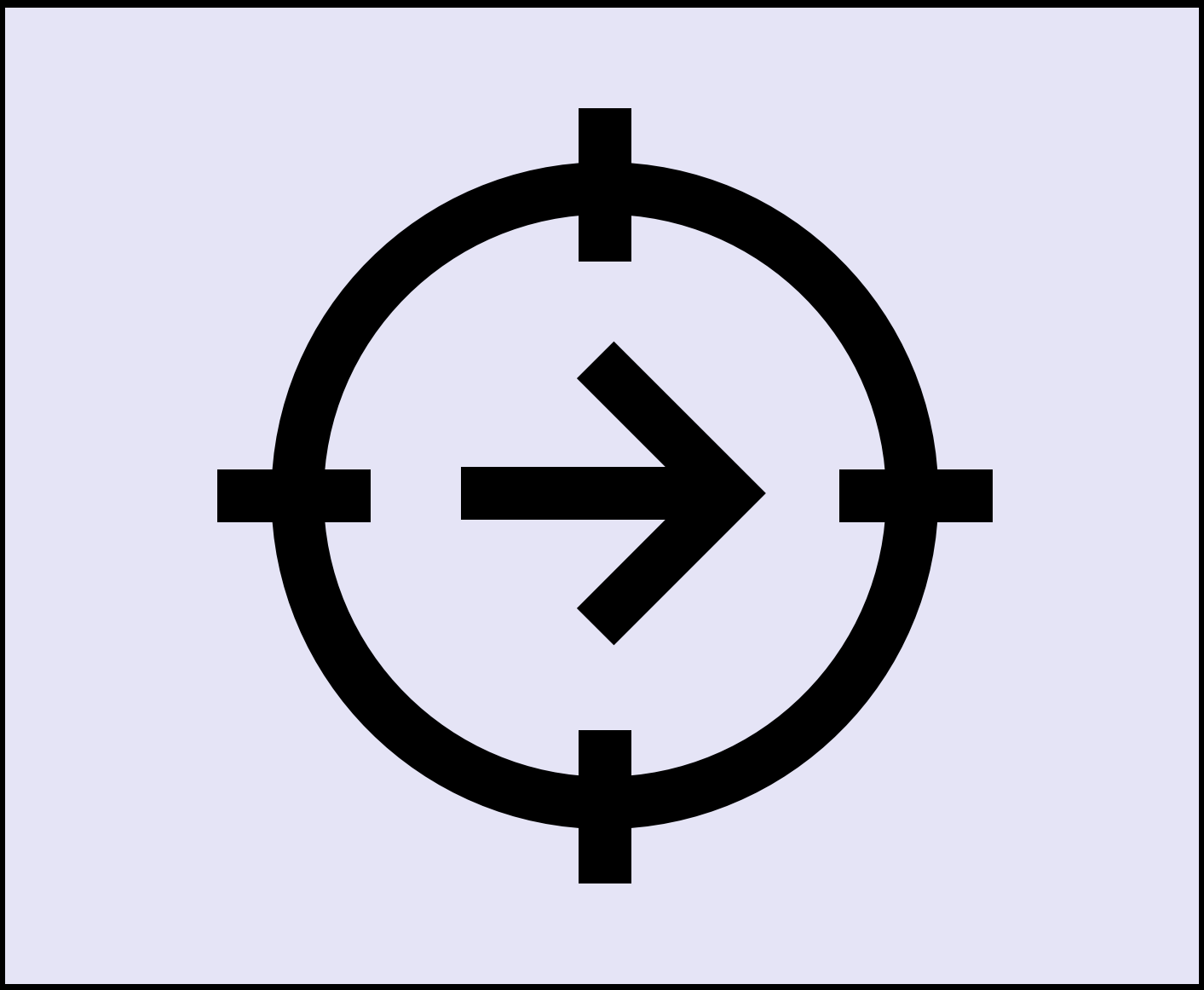


BUG BOUNTY, SIMPLIFIED

How Security Teams Can Get Better Coverage and Predictable Costs

Inspectiv

Inspectiv

Bug Bounty Doesn't Have to be Loud or Unpredictable

CUT THROUGH THE NOISE. STAY AHEAD OF RISK.

Traditional bug bounty programs - where trusted ethical hackers find and report security vulnerabilities - promised continuous security at scale, but for many teams, they've delivered complexity, unpredictability, and a whole lot of noise.

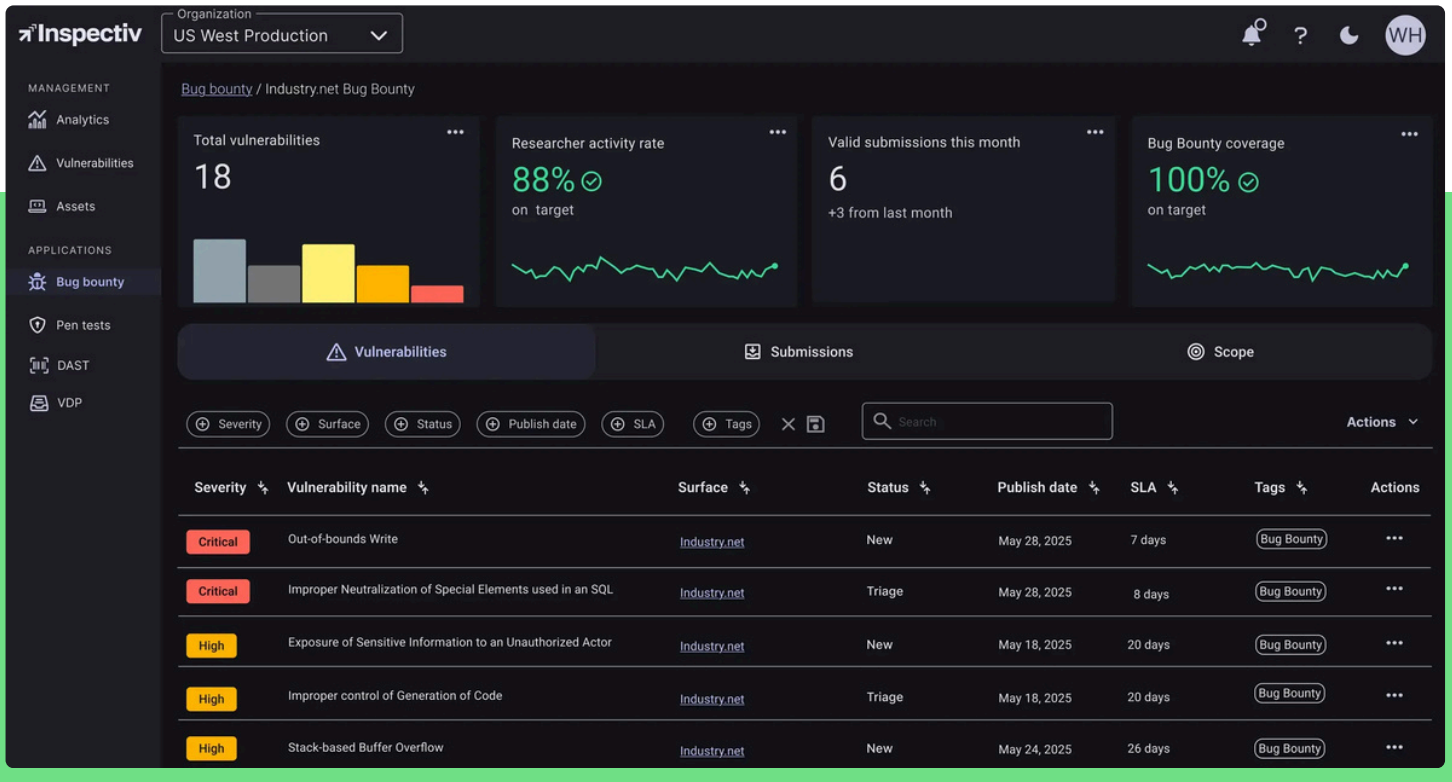
When a report is submitted, it may or may not be valid - historically less than half are. That validity check - triage - takes time and effort. Some bug bounty platforms cut costs by making the software owner part of the triaging workforce. It is a hidden cost of time, reputation, and risking researcher unhappiness when evaluating vulnerabilities to see if they will pay out or not.

Meanwhile, vulnerabilities don't wait. As your environment grows more complex, the stakes only get higher.

IS YOUR BUG BOUNTY PROGRAM ACTUALLY MAKING YOU MORE SECURE OR JUST MORE BUSY?

There's a better way.

Inspectiv's Bug Bounty Program helps you cut through the noise, get the results you want, take control, and fix what matters — fast.



Inspectiv

When Your Bug Bounty Vendor Makes You the Worker

Bug bounty programs were supposed to make security easier. But for most teams, they've only added more noise, more busywork, and more budget headaches. Here's what's really getting in the way:

YOU'RE NOT AN ETHICAL HACKING EXPERT

You're flooded with findings and many of them duplicates or low impact. Triage becomes a chore, pulling time away from real security work. You don't know the market price for a bounty.

THE COST ROLLERCOASTER

Variable payouts. "Escrow accounts." Unpredictable burn. Try explaining that to your CFO or planning a budget around it.

ONE SIZE DOESN'T FIT ALL

Your environment isn't generic. Your bug bounty program shouldn't be either. Traditional platforms expect you to manage scope, researcher quality, and coordination all on your own. Now, you don't have to.

YOU'RE STILL DOING THE HEAVY LIFTING

Access to researchers doesn't mean less work. You're still approving bounties, chasing down unclear reports, and managing communication between teams.

THE BOTTOM LINE?

You're spending more time managing your bug bounty program than benefiting from it. Inspectiv was built to fix that by removing the worst problems of earlier bug bounty platforms. That means we do the triage, offer fixed rates, show you signal without noise, and deliver the AppSec and Security Testing that you can't buy.

Inspectiv

Finally, a Way to Cut Through the Chaos

Bug Bounty as a Service (BBaaS) does what traditional programs never could: It gives you the power of the world's best researchers, without the chaos. No noisy inbox. No endless triage. No surprise invoices. Inspectiv's BBaaS model was built for lean security teams that need results, not distractions.

HERE'S WHAT THAT LOOKS LIKE:

FOCUSED, HIGH-SIGNAL FINDINGS

We scope your program around your environment, not a generic template. The result? Less noise, more signal. Plus, vulnerabilities that are worth your time.

WE HANDLE THE TRIAGE

Forget chasing down unclear reports or managing researcher DMs. Our team vets and prioritizes every submission before it ever hits your queue.

GUIDANCE FROM PEOPLE WHO GET IT

We don't just throw findings over the wall. You get expert-backed remediation support, including walkthroughs, when you need them.

CUSTOMIZED PROGRAMS

Each Inspectiv program is customized; there's no rules (for bounty, scope, etc.) that are company-wide whether you like it or not.

PREDICTABLE PRICING

Flat-fee simplicity replaces the unpredictable economics of traditional bounty programs. No escrow. No spikes. No surprises at budget time.

Inspectiv

Traditional Bug Bounty vs. Inspectiv Bug Bounty as a Service

With Inspectiv, you get all the upside of bug bounty, minus the noise, overhead, and burnout. It's security that works like your team does: lean, focused, and fast.

	Traditional Bug Bounty	Inspectiv Bug Bounty as a Service
Crowd-sourced expertise	✓	✓
Integrated program management	✗	✓
Predictable costs	✗	✓
Precise coverage scope	✗	✓
Actionable, prioritized findings	✗	✓

Inspectiv

You Shouldn't Need Google's Budget to Feel Secure

Big names like Google have paid out $59 million in bug bounties since 2010 with single rewards topping $113,000. That's great for them. But most security teams don't have Google's scale, staffing, or spend. The great majority of readers will not get access to those researchers' time. But you can still close your security vulnerabilities. You can still secure increasingly complex environments, respond faster, and stay compliant, all without burning out your team or your budget.

That's where Inspectiv's Bug Bounty changes the game.

WHAT GROWING TEAMS ACTUALLY NEED:

- Adaptive bug bounty that moves faster than attackers
- Relevant findings that don't waste time
- Triage and validation baked in
- Not competing for researcher attention against much larger companies
- A pricing model that makes sense in front of leadership
- Support that scales with your environment

Bug bounty doesn't have to be expensive. Or messy. You just need a model that's built for the way you work.

$59M

THE HIGH COST OF BUG BOUNTIES

Google has paid out $59M in bug bounties but most companies need a smarter, more manageable approach. **Inspectiv delivers high-signal security without high-stakes chaos.**

Inspectiv

This is What Bug Bounty Looks Like When it Works

With Inspectiv, you don't just get a platform, you get a partner. Our Bug Bounty programs are built to reduce the chaos and deliver the kind of security outcomes your team can trust and act on.

HERE'S WHAT BETTER LOOKS LIKE:

ADAPTIVE PROGRAMS BUILT AROUND YOU

We tailor every program to your environment and priorities so every result is relevant, actionable, and built for your team. You have the option to run both private and public programs that fit your organization's needs.

TOP RESEARCHERS, ZERO BABYSITTING

You get access to trusted, high-performing researchers with Inspectiv's help managing the relationship. Inspectiv handles the communication, triage, and bounty decisions so your team doesn't have to. We also plug straight into your existing workflows through integrations with tools like JIRA, Slack, APIs and webhooks so findings flow where your team already works.

COMPLIANCE WITHOUT THE FIRE DRILL

Whether you're prepping for SOC 2, ISO, or GDPR, Inspectiv helps simplify your audit process. With consolidated reporting, validated findings, and remediation tracking, your team stays ready.

FINDINGS YOU CAN TRUST

Every report is reviewed, validated, and prioritized by our team before it ever reaches yours. No noise. No spam. Just clear insights, often with step-by-step guidance or videos to speed remediation. Plus, you get the option to retest any vulnerabilities as many times as you need to for up to a year.

PRICING YOU CAN PLAN FOR

Flat-fee pricing means no surprises when it's time to plan your budget.

ServiceTitan

"We run multiple bug bounty programs with Inspectiv across different parts of our business. The quality of the findings has made a real difference in how we manage risk. Inspectiv's team consistently uncovers impactful vulnerabilities and provides clear, detailed insights that help us respond quickly and strengthen our security posture."

Paul Intrarakha
Senior Principal
Application Security Architect

Inspectiv

Let's Make Security Quieter

Security teams don't need more alerts, more tools, or more to manage. They need clarity, control, and confidence that their bug bounty program is actually working.

INSPECTIV'S BUG BOUNTY GIVES YOU:

- High-signal findings, not alert fatigue
- A fully managed researcher network
- Straightforward pricing that scales with your team
- Continuous coverage that grows with your software
- Readable, curated reports that get to the point
- Flexible test scoping that can change with your needs

Ready to Cut Through the Noise?

Let's talk about how Inspectiv can help your team fix what matters.

→ **Book a demo** or learn more at **inspectiv.com**.

Inspectiv

Inspectiv is an all-in-one AppSec testing platform that simplifies the process of discovering, validating, and remediating vulnerabilities. By offering Bug Bounty, Pentesting, Dynamic Application Security Testing (DAST), and Vulnerability Disclosure (VDP) in a single solution, organizations can reduce risk, maintain compliance, and strengthen their security posture. With streamlined management, minimal operational overhead, and predictable pricing, Inspectiv delivers impactful results that make security testing more efficient and effective.