Layered security in action: How VDP, Bug Bounty, and PTaaS combine to protect your business

BY ELEANOR BARLOW · OCTOBER 8, 2025 · LAST UPDATED ON JANUARY 2, 2026

What you will learn

- **How different security strategies (VDP, bug bounty, and PTaaS) uniquely identify and uncover vulnerabilities**, and how to combine them for modern defence.
- **How combining these approaches creates continuous visibility, deeper testing, and structured assurance** across your digital assets.
- **How to evaluate and demonstrate the value (ROI) and maturity of your security programme** by integrating broad reporting, incentivised testing, and formal assessments.

You asked, and we answered.

At Intigriti, we've been paying close attention to the questions most frequently asked by those with a bug bounty program in place. That's why we've launched this blog series dedicated to answering the most asked questions, diving into hot topics, and sharing practical and expert-backed strategies to help you maximize your bug bounty success.

So far in this series, we have answered:

- How to attract security researchers to test on my bug bounty program?
- How should I scope third-party assets in my bug bounty program?
- What is the pattern that can be expected after going public with a bug bounty program?
- How can I get more bug bounty submissions and higher severity findings?
- How do I know I'm paying the right amount of bug bounty?

Today, we discuss the differences between a VDP, BBP, and PTaaS and how a combination might benefit your cybersecurity strategy.

No single security measure is enough. The most resilient organizations rely on a layered security strategy. While scanners and Static Application Security Testing (SAST) and Dynamic Application Security Testing (DAST) have their place, companies are turning to a combination of Vulnerability Disclosure Programs (VDP), Bug Bounty Programs (BBP), and Penetration Testing as a Service (PTaaS).

Each offers a unique approach to identifying and managing vulnerabilities. Together, they deliver continuous, structured, and scalable protection across your digital assets.

Different tools for different jobs

A Vulnerability Disclosure Program (VDP) gives anyone, including researchers, users, or partners, a safe and legal way to report security issues they discover. These are often low to medium-risk findings reported incidentally. There's typically no financial reward; instead, recognition or small gestures like swag may be offered. The focus is on transparency, risk reduction, and encouraging responsible disclosure.

A Bug Bounty Program (BBP), on the other hand, ensures ethical hackers are financially rewarded for finding high-impact vulnerabilities. These researchers are given a defined scope and are incentivized to look deeper and push harder than typical testing would allow. Bug bounty programs tap into diverse security expertise worldwide, delivering continuous testing on your assets. So, an internal skills shortage? Consider it solved.

While VDPs offer broad coverage with minimal cost, BBPs provide targeted, high-value testing by security researchers.

Managing scope and access

VDPs are public and open to anyone. Their scope is intentionally broad to encourage general issue reporting. Bug Bounty Programs, on the other hand, may be public or invite-only and focus on high-priority areas. Findings outside the defined scope are generally not rewarded.

VDPs require clear policy and response workflows. Bug bounty programs through a platform like Intigriti add value by providing benefits from more hands-on management, including triage, researcher vetting, engagement, and payout processing.

Each program is designed to meet different needs: VDPs catch what's found by chance; BBPs uncover what only deep, deliberate testing will reveal.

Take a look at the features of both a BB and a VDP in this brochure.

PTaaS for methodical testing

Penetration Testing as a Service (PTaaS) provides scheduled, methodical testing. Unlike VDPs and BBPs, which rely on external communities, PTaaS follows formal testing methodologies and aligns with compliance requirements and internal timelines.

As David Andersson, the Security Engineering Manager at Grafana Labs, puts it:

> **"If you look at a pentest, it's more of a mile wide and an inch deep, whereas a bug bounty initiative is an inch wide and a mile deep."**

PTaaS delivers structured, in-depth assessments of key systems, often used for product launches, infrastructure changes, or regulatory audits. PTaaS offers clear documentation, threat modelling, and remediation guidance crucial for meeting frameworks like ISO 27001, PCI DSS, and NIST.

How all three work together

These programs are most effective when combined:

- VDPs serve as an open door for low-risk issue reporting.
- Bug Bounty Programs drive high-skill, continuous real-world testing for critical systems.
- PTaaS ensures regular, in-depth assessments with defined outcomes.

Together, they create continuous visibility, targeted testing, and structured assurance. A bug found through a bounty program may inform future PTaaS testing. A VDP report could uncover trends that shape bounty scope. PTaaS findings may expose systemic gaps that open new testing needs for both VDP and BB.

This interplay strengthens your overall security posture, not through redundancy, but through coverage at every level.

Proving ROI and maturity

Bug Bounty Programs are cost-effective: you only pay for valid vulnerabilities submitted. VDPs offer early insights at little to no cost. PTaaS provides reliable, auditable reports for internal risk management and compliance.

Combined, they signal security maturity. You're not just ticking boxes, you're proactively identifying, managing, and reducing risk across your environment.

A stronger defense through layers

Used individually, VDP, Bug Bounty, and PTaaS provide value. Used together, they provide defense in depth: VDP for broad visibility, Bug Bounty for targeted depth, and PTaaS for structured assurance.

A layered approach gives you wider coverage, deeper testing, and stronger control, protecting your business against both common and advanced threats.

Next steps to enhance your bug bounty journey

For more information on any of the points made in this article, contact the team today. And keep an eye out for our next blog, where we dissect another popular question posed to our team!

Interested in a particular topic? Send us the questions you'd love answers to by emailing pr@intigriti.com

AUTHOR

Eleanor Barlow

Eleanor Barlow is a London-based Senior Cyber Security Technical Writer at Intigriti, with 9+ years' experience reporting on and writing for the cyber and tech sector. She specializes in data-driven content on cybersecurity and bug bounty intelligence, helping organizations benefit from the latest trends and insights.