What is Penetration Testing as a Service?

BY ANNA HAMMOND · OCTOBER 24, 2022 · LAST UPDATED ON SEPTEMBER 8, 2025

Penetration Testing as a Service (PTaaS), much like the other renditions of centrally hosted Software as a Service technologies (SaaS), is about providing a more flexible, continuous and scalable pentesting service. While remaining distinct from bug bounty programs, PTaaS is a modern approach to the traditional pentesting format.

How does Penetration Testing as a Service work?

Penetration Testing as a Service is about delivering pentests through a centrally hosted portal that takes care of backend overheads, provides real-time updates and is more adjustable depending on a client's needs.

Going back slightly, a pentest can be distinguished from a vulnerability scan in the sense it involves a cybersecurity expert actively searching and exploiting vulnerabilities. They provide a more rigorous testing method than preliminary vulnerability scanners. This is summarized by Gartner's definition as "*Penetration testing goes beyond vulnerability scanning to use multistep and multivector attack scenarios that first find vulnerabilities and then attempt to exploit them to move deeper into the enterprise infrastructure.*"

The main issue with the more traditional pentesting format is that results are available only at the end of the testing period, meaning they can be somewhat outdated. Determining which parts of security needs to be prioritized by small internal teams is also difficult, particularly since the speed of development cycles has vastly increased.

What are the benefits of PTaaS?

The agility of modern software development has been seen to benefit greatly from the PTaaS format. In no particular order of importance, we've outlined four key benefits of PTaaS below:

1. Continuous testing

Where pentesting begins and finishes at defined and isolated points, the automation involved with PTaaS can provide real-time updates. Say you develop a new release, this change is communicated to the pentesting platform automatically through the live dashboard, and testing on it can begin immediately. This ensuring that pentests can give a more continuous picture of overall security posture.

2. Hand-picked ethical hacker expertise

PTaaS can make use of wider hacking communities, who can use a greater variety of penetration methods. The hacking expertise possessed by white hat hackers is an unmatchable source of knowledge.

Today, accessing these skills is becoming easier than ever, with 66% of our community considering ethical hacking as a full-time job, according to our Ethical Hacking Insights 2022.

3. Reduced costs

The automation PTaaS provides also significantly reduces the time spent, and therefore budget spent, compared to traditional pentesting. This includes shortening the time taken to define the statement of work and other overhead administrative procedures.

4. Quick feedback and remediation

More automation enabling real-time updates also has an added benefit of accelerating the speed of remediation for any vulnerabilities, which can be dealt with swiftly. This is particularly pertinent given today's fast release cycles, where agility in development is becoming a standard.

How does PTaaS differ from bug bounties?

You'd be forgiven if you're wondering how exactly bug bounties fit into this picture. 'Continuous protection which can be viewed in real-time' sounds rather similar to how bug bounty platforms position themselves—particularly given the fact that the presence of actual human hackers and their expertise is also cited as a key benefit of both approaches.

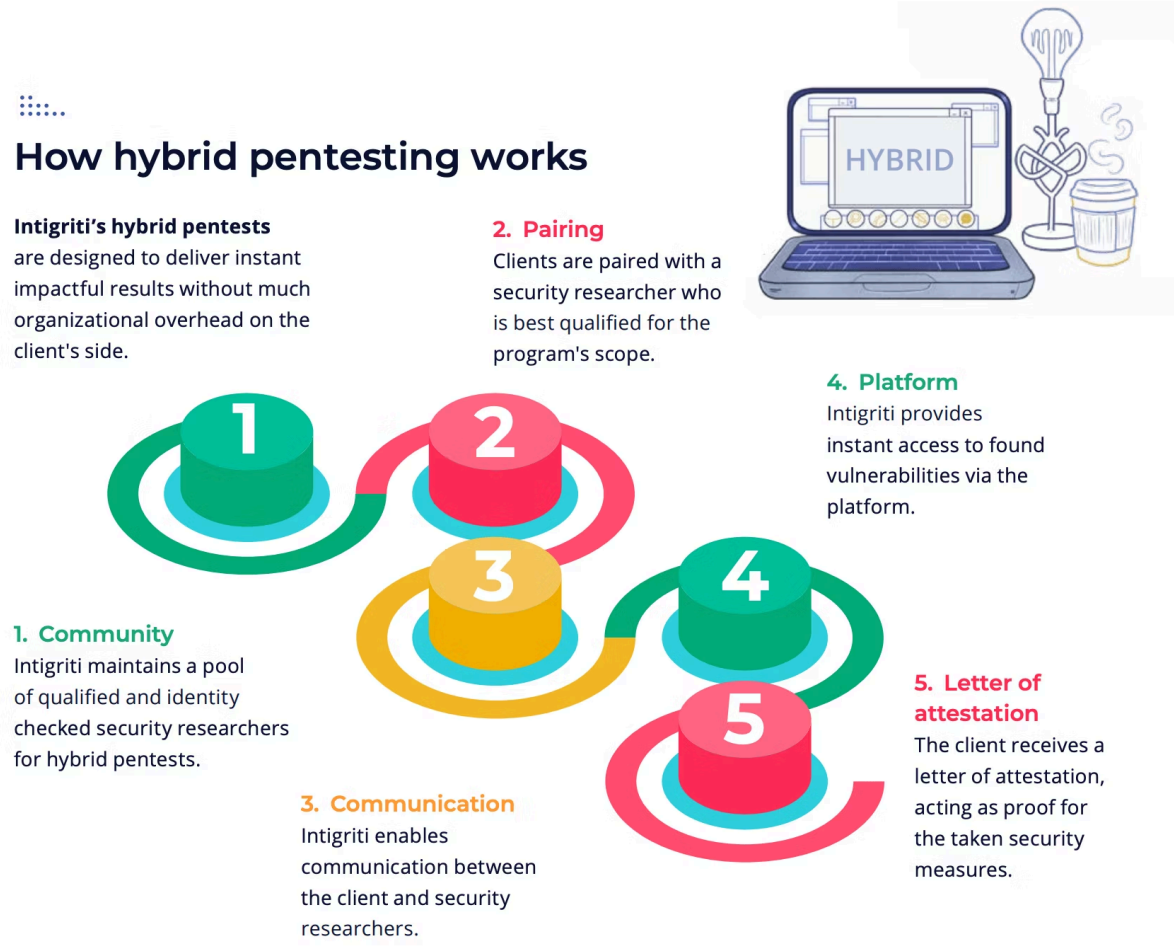
However, there is a key difference that distinguishes the two. Primarily, it is a question of the needs of a customer. PTaaS, despite it supporting a more 'continuous' approach, remains a more controlled form of security testing compared to bug bounty programs, and maintains the time-boxed nature of traditional pentesting. It usually has a more specific scope than bug bounty programs too. This is essential for a number of scenarios. You might be checking the posture of a product or new feature before release, or perhaps only need to check for a specific compliance.

Penetration Testing (PTaaS) at Intigriti

At Intigriti, our Penetration Testing as a Service is known as Pentest as a Service. Through a simple framework, it is an impact-focused approach to PTaaS.

It begins with our continuous community management, where we nurture and maintain the pool of skilled white-hat hackers ready to be picked for their techniques. Next, after hearing your needs, we pair the researcher profiles best qualified for your project.

We then open communication between you and the researchers so they can get to grips with the requirements. As they begin work, you can monitor their progress as it happens through our platform. Finally, you receive a letter of attestation confirming proof of the security compliance you've carried out.



Refining PTaaS

Controlled penetration testing continues to hold a vital role in our security infrastructure. However, as our software development has become more agile, the need for real-time updates and lower security costs has become crucial. Intigriti's PTaaS is a cost-efficient and impact-focused approach to PTaaS.

REQUEST A DEMO

intigriti.com/demo

VISIT THE WEBSITE

intigriti.com

GET IN TOUCH

hello@intigriti.com