Hybrid Pentesting: The Smart Approach to Securing your Assets

BY INTIGRITI · FEBRUARY 5, 2025 · LAST UPDATED ON SEPTEMBER 8, 2025

Pentesting-as-a-Service is your next crucial layer of security

For businesses dedicated to their security, they'll know that truly mature infrastructure doesn't involve just one kind of protection. Vulnerability scanners, firewalls, periodic penetration tests, and bug bounties are all independent layers of an onion of well-rounded cybersecurity. They each serve different purposes and ensure every kind of potential cyber-attack is taken into consideration.

While beginning as primarily a bug bounty platform, at Intigriti we've expanded our offering over the years to service our customers' evolving cybersecurity requirements. With 125,000+ highly skilled ethical hackers on hand, it's a no-brainer that this unique knowledge base should be leveraged to its full potential.

What is a penetration test?

Traditionally, a penetration test – or 'pentest' – is a controlled, simulated attack on a computer network or application. A pentest is similar to a bug bounty in that it involves the use of ethical hackers to test your systems. However, there are some key differences between a pentest and a bug bounty.

First, a pentest uses a time-boxed approach, meaning it tests the security at a particular time. Bug bounties provide a method of continuous assessment, as security researchers can test the target for as long as the program is in place. Secondly, penetration tests tend to be more targeted, with a tighter scope that can be used to demonstrate specific compliance. Bug bounties on the other hand tend to have a wider target that can capture a variety of different vulnerabilities.

Hybrid Pentesting is a time-boxed test using your desired methodology. With a short lead time and simple setup, we provide real-time updates on the tests that can be completed within a tight deadline.

What are the benefits of Hybrid Pentesting?

Hybrid Pentesting is a faster, more scalable and more cost-efficient method of pentesting, where you can access the unique knowledge base of Intigriti's hacking community. It follows the loose format of what's become known as 'Pentesting-as-a-Service' (PTaaS).

Our Pentest Manager, Pascal Schulz, says the key benefits of Hybrid Pentesting revolve around scalability and cost-efficiency, while providing customer with access to the expert skills of our hacking community.

"Hybrid Pentests can be set up quickly and to your exact specifications, regardless of your company's development stage," Pascal said. "They can expand or retract as your needs do."

"Hybrid Pentesting also takes care of the backend overheads typical of traditional pentests to reduce costs. And most importantly, it is pay-for-impact. That means the cost of your Hybrid Pentest is capped

and linked to the vulnerabilities that are found."

He added: "The researchers used in our Hybrid Pentests are expert members of our global community. They have a proven track record and are hand-picked for their knowledge."

How Hybrid Pentesting works

A Hybrid Pentest occurs through five simple steps:

1. We help you to define your project and scope.
2. We list the program on our platform where researchers can apply to take part.
3. We then review the applications, assisting you in your choice of researchers to ensure the best ones are chosen for the job.
4. As the test happens, you receive live updates on its progress through our platform.
5. After completion, you receive a full report that can be used to support any specific compliances required.

Interested in learning more? Pascal takes you through our Hybrid Pentest in more detail in the video below:

Why Hybrid Pentesting is the leading iteration of pentesting-as-a-service

But just what is it exactly that distinguishes Hybrid Pentesting from other Pentesting-as-a-Service offerings?

How you reward researchers is a key part of this approach, and Hybrid Pentesting addresses this to maximize interest in your program. Our combination of a 'bounty pool' and 'base bounty' is unique and ensures that even if security vulnerabilities are not found, researchers are still rewarded for their time.

This unique pay-for-impact model means that you only pay the bonus of bounty if any new vulnerabilities are discovered. Additionally, Hybrid Pentests reduce the number of backend requirements typically involved in pentesting, which further helps to reducing costs while delivering results.

Visit Intigriti's Hybrid Pentest page for more information.