

What is Penetration Testing as a Service (PTaaS)?

Did you know that you can get regular penetration tests without spending too much? That's possible with Penetration Testing as a Service (PTaaS), which provides access to leading cybersecurity services on a budget.

Conducting penetration testing seems easy in theory, but the task requires high-level cybersecurity expertise. Hiring a professional doesn't come cheap, especially when you have a limited budget.

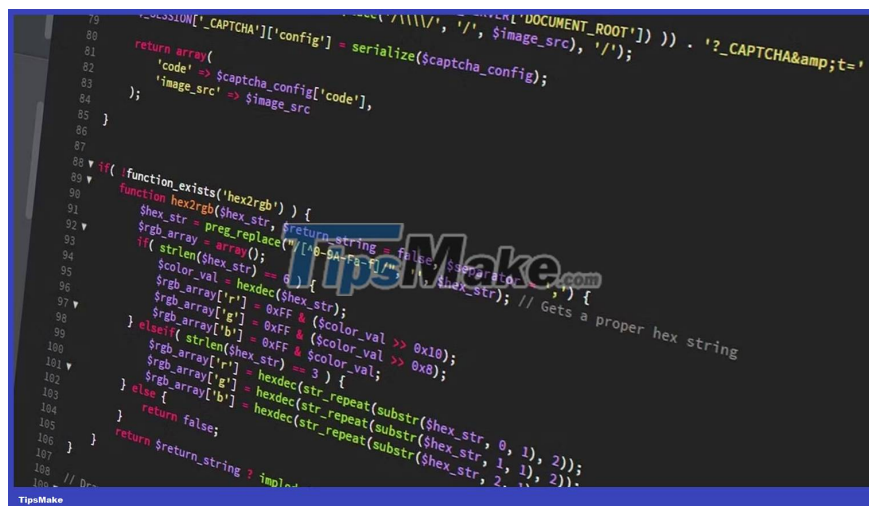
Did you know that you can get regular penetration tests without spending too much? That's possible with Penetration Testing as a Service (PTaaS), which provides access to leading cybersecurity services on a budget. Check out how PTaaS works and how you can maximize it to your benefit.

What is Penetration Testing as a Service?

Penetration Testing as a Service (PTaaS) is a subscription-based model that provides hacking simulation services to identify and fix vulnerabilities in your system.

The frequency of pentests is important in detecting and stopping threats early, but conducting regular checks can be expensive. PTaaS makes penetration testing affordable and accessible. You work with certified white hat hackers who monitor the system if you have an active subscription.

How does Penetration Testing as a Service work?



Penetration Testing as a Service uses the SaaS model, a cloud-based system where software application service providers solve operational problems for customers upon registration. As a member of a PTaaS provider, you have on-demand access to quality inspection and maintenance services.

Professionals perform traditional penetration craft. This is often time consuming as they have to check every detail on their own. PTaaS implements automated penetration testing along with human input. The software regularly scans your connected device for vulnerabilities, and then the network security experts from the service provider perform an assessment. They expand on the data that the software generates and take a closer look at the small details that the scan might have missed.

As a network owner or administrator, a typical penetration test does not allow you to participate in this process. Experts do their job and provide feedback on their findings, but PTaaS is more holistic. You have access to the reporting data the app generates on the dashboard, so you know nothing about the security context of the system. Data gives you more control over your cybersecurity aspect.

What are the benefits of PTaaS?

A flexible and specialized cybersecurity platform, Penetration as a Service offers the following benefits.

Professional testing capacity

Penetration testing is most effective when thorough testers are like a brutal hacker. Failure to detect vulnerabilities in the test is not a good sign, as it indicates that the white hat hacker is not skilled enough.

PTaaS provides you white hat hackers with years of experience in the job. Their expertise is just as high as that of seasoned cyber attackers, if not better. A threat is less likely to go unnoticed. Asking them to check your system regularly will ensure there is no room for vulnerabilities to develop.

Action-driven reporting data



Cyber threats escalate due to lack of visibility. If you keep an eye on all areas of your network to detect and remediate emerging threats, they shouldn't pose a problem. Traditional penetration testing typically can take place after intruders have exploited a vulnerability and caused damage.

PTaaS has automated sensors to select and report threats. The application dashboard shows threat activities in the system. This data prompts you to make informed decisions and take the necessary actions. However, for this information, you may have to wait for your next routine check, while a cybercriminal is opportunistically compromising your system.

Feedback on the vulnerability of the update

You can prevent some security holes in your system by checking the safety of the design or encryption updates before launching them. New updates you make can enhance the user experience but open the door for intruders.

PTaaS is compatible with software development security. It checks for updates for connected devices in the context of cybersecurity and highlights inputs that fail the validation check. You can change them early enough and prevent future attacks.

Flexible payment plan

PTaaS providers cater to many users with different network capacities. They offer flexible payment options to strike a balance among their clients. If you are an individual who wants to secure your network, you can choose a more affordable subscription plan because your needs are less than the needs of organizations with larger networks.

Payment flexibility helps you secure your system even when you are on a tight budget. This is not a typical penetration test case. You have to arrange all the expenses before the tester does the work.

You finished reading the article "**What is Penetration Testing as a Service (PTaaS)?**" edited by the [TipsMake](#) team. We hope this article has provided you with many useful tech tips and tricks. You can search for similar articles on tips and guides. Thank you for reading and for following us regularly.