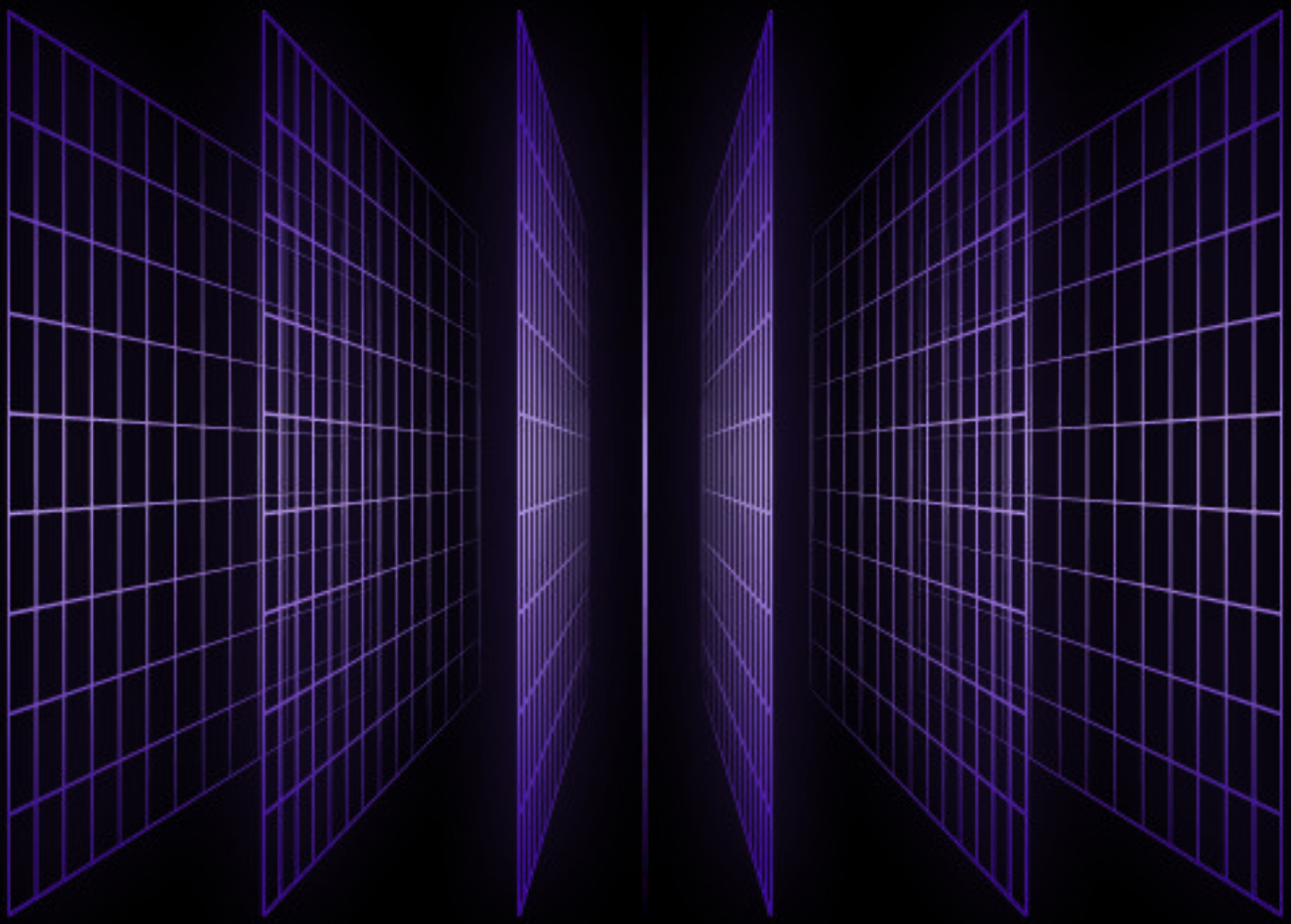
bugcrowd

# Penetration Testing 101



# Table of Contents


Everything you need to know about pen testing

03

The Basics of Pen Testing

04

Why Pen Test?

07

Penetration Testing Options

09

Problems with Traditional Pen Tests

12

What is Pen Testing as a Service (PTaaS)?

15

The Future of Pen Testing

17

Combining Pen Testing with Bug Bounty Programs

18

The Dawn of a New Era in Pen Testing

19

The Bugcrowd Platform

20

# Everything you need to know about pen testing

Penetration testing (AKA pen testing) has been an **indispensable tool in the security leader's toolbox** for over a decade. However, it's important to note that not all pen tests are created equal, and their effectiveness heavily relies on the details of their implementation.

Unfortunately, the industry has long relied on a cumbersome and consulting-heavy approach that does little to address underlying risks. As a result, traditional methods of pen testing have become more of a problem than a solution.



**In this guide you will learn...**

- Why pen testing is done today
- Current approaches to pen testing, with pros and cons
- Why the traditional approach comes up short
- The rise of Pen Testing as a Service (PTaaS)
- What crowdsourcing brings to pen testing
- How the Bugcrowd Platform enables crowdsourced PTaaS and other security testing strategies

# The Basics of Pen Testing

Pen testing, in one form or the other, has been with us for a long time, but adoption has been accelerating as of late, with Gartner estimating a **total market size of $4.5B by 2025** (and that's just for commercial tools; use of open source tools is also becoming increasingly significant).

## What is Pen Testing?

According to the National Institute of Standards and Technology (NIST), pen testing is defined as "security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network."

In other words, pen testing is a **simulated cyberattack** carried out by an authorized third party (known as pen testers) who tests and evaluates the security vulnerabilities of a target organization's computer systems, networks, and application infrastructure.

Human pen testers attempt to find vulnerabilities and exploit them using various tools and manual procedures. Pen testers execute a variety of tests designed to exploit known vulnerabilities and leverage misconfigurations in software and security controls. Their goal is to identify **real-world security weaknesses** in an organization's security posture that an attacker can exploit.

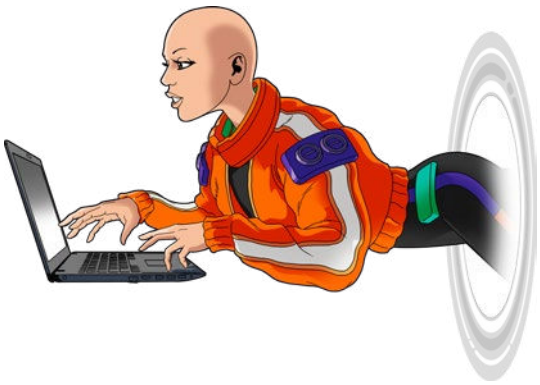
> **"Penetration testing is security testing in which assessors mimic real-world attacks to identify methods for circumventing the security features of an application, system, or network."**
>
> — NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY (NIST)

Pen testers often mimic the behaviors of real threat actors by using techniques such as social engineering. Once these security weaknesses are identified, they can be prioritized for remediation. Pen testing is an **iterative process,** and over time, it helps reduce the risk of a successful cyberattack.

## The Phases of a Pen Test

Pen testing is often broken down into several phases. The first phase is the **pre-engagement activity.** During this phase, the pen testing team reviews the goals and objectives that the target enterprise aims to achieve. Pen testers begin this process by looking for the best pen testing strategy for your organization.

The next phase is **reconnaissance and planning.** In this phase, pen testers gather as much information as possible about the targeted enterprise to learn more about potential vulnerabilities. This helps them plan their simulated attacks and define the mix of tools, both software and hardware, as well as the social engineering techniques they will use.



All of this information comes together in the **vulnerability mapping phase,** when the pen testers select the attack vectors and the techniques they will use. Vulnerability mapping depends on a good assessment of the vulnerabilities that may be targeted.

The fourth phase, **exploitation,** leverages the plans to find and use the exploits. In this phase, the ethical hacker seeks to penetrate the environment while avoiding detection.

When the testing is complete, the pen tester removes artifacts, including their testing tools, intermediate datasets, and special hardware modules. They will also remove anything else they have modified or used during the pen test. Everything in the environment will be returned to the original state before the test begins.

From there, the pen tester will provide a **written report** that details their findings. This report is often accompanied by a scheduled briefing to review the findings. The in-house teams, both purple and blue, as well as others, will then identify near-term areas that require improvement, assign priorities, and then build and **initiate a plan for implementation.** The same is done for longer-term areas requiring improvement. Correlating the results of pen testing with an organization's assessment of risk is essential, as pen testing results can provide important inputs and help to drive tool rationalization decisions.

Finally, the enterprise should schedule the pen test again to **validate that the vulnerabilities** identified were corrected and that the improved defenses now mitigate the pen tester techniques previously tested.

## Red vs. Blue vs. Purple Teams

Color teams refer to in-house teams that perform security exercises.

- **Red Teams**
  Red teams are composed of *offensive* security professionals. During the exercise, they will try to attack an organization's cybersecurity defenses.
- **Blue Teams**
  Blue teams are composed of *defensive* security professionals. During the exercise, they will defend against the red team attacks.
- **Purple Teams**
  When you mix blue and red, you get...purple! Purple teams are composed of both red and blue team members who work together to share insights, which can improve an organization's overall security.

## Pen Test Reports

Let's dive deeper into the written report submitted by the pen testing team. Pen test reports should include an **explanation of the test methodologies used** and how they were applied, technical findings, procedural findings, reproducibility, description of risks discovered, recommendations, and conclusions.

Reports can also be done with respect to compliance requirements to meet the needs of **ISO 27001, SOC2 Type 2, PCI, HITRUST, FISMA,** and other compliance regulations. These pen testing reports can often support risk assessments, such as those required to ensure HIPAA compliance.



## Pen Test Tools

You may be wondering more about the **types of tools** pen testers use during a pen testing engagement. Pen testing tools encompass a wide range of special tools developed by hackers and other software tools commonly found within the targeted enterprise. Many of the tools that ethical hackers use are available on an open source basis. Examples of widely used tools include Kali Linux, Metasploit, Wireshark, and MimiKatz.

The practice of using tools commonly found in the enterprise by both pen testers and threat actors is referred to as **"living off the land."** This enables threat actors to become part of the target enterprise's network and to hide among normal day-to-day activities. Even when malicious activity is detected, attribution becomes difficult or impossible, since everyone uses similar tools.

# Why Pen Test?

Up until recently, compliance (e.g., for PCI-DSS) was the dominant driver of pen testing. Today, according to industry research, **69% of adopters do pen tests to assess security posture, and 67% do them for compliance purposes.** This indicates a much more even split and signals that many organizations do pen tests for both reasons.

In a recent survey of security professionals around the globe, we found that **91% said that they'd like to raise their expectations of what a pen test could achieve.** This demonstrates a desire for elevated pen tests that don't just check the compliance box.

Compliance can be an opportunity for organizations with less mature cybersecurity practices to secure investments for pen testing. However, annual or biannual compliance-driven testing alone is just table stakes for most companies; there are many other important reasons to invest in pen testing.

For example, the continuous development cycles typical of cloud-based environments have highlighted the need for more frequent, if not continuous, testing. And the turmoil created by mergers and acquisitions, particularly in regulated industries, is a common reason for more rigorous testing than what checking a compliance checkbox will provide.

With the **increasing complexity of the attack surface,** which has expanded well beyond web apps, networks, and databases to include APIs, cloud infrastructure, and even physical devices, the reasons for conducting deep pen testing are certain to multiply.



## Satisfy Stakeholder Requirements with Pen Testing

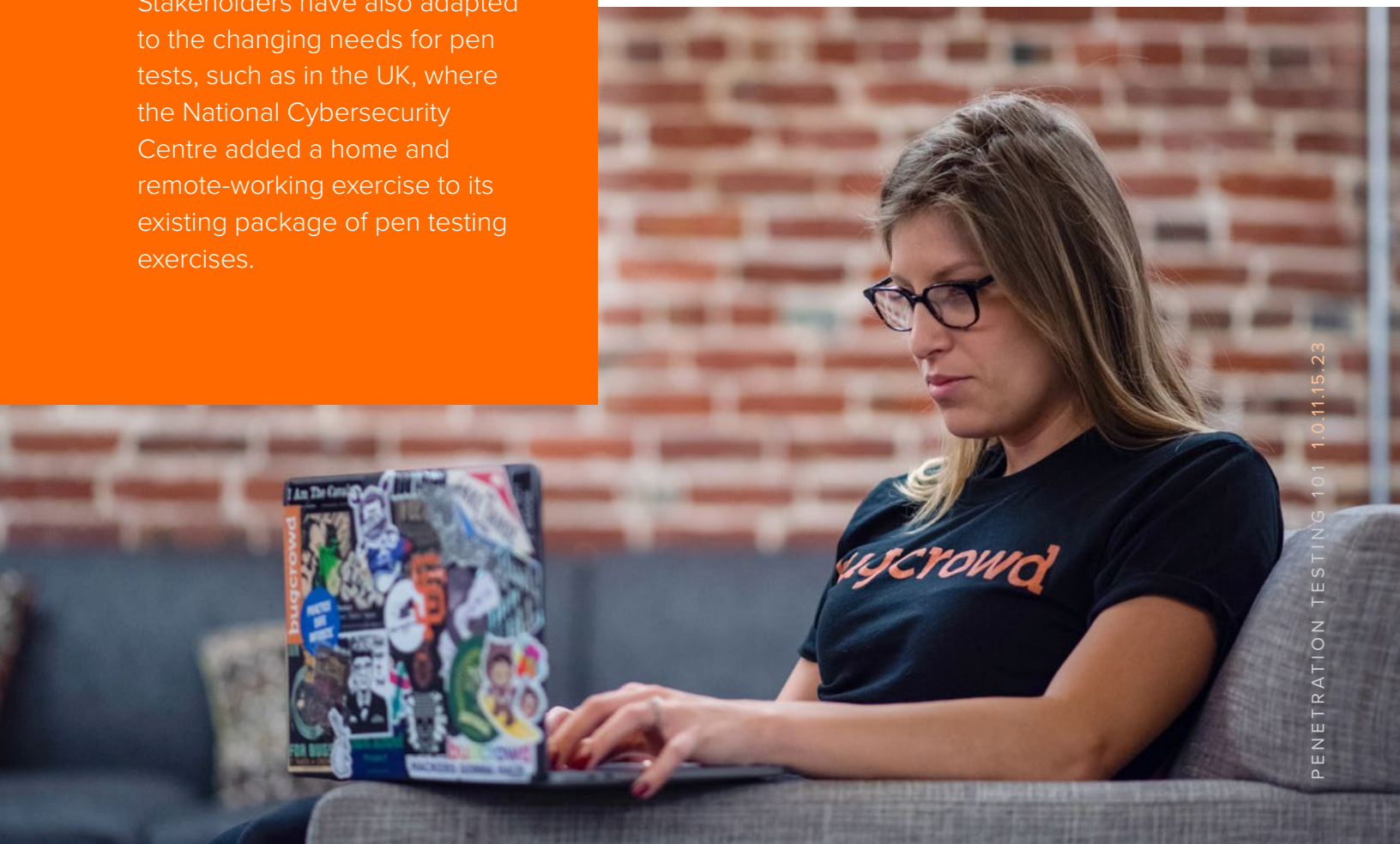
Stakeholders, such as customers, suppliers, investors, and regulators, play a considerable role in an organization's decision-making. The most obvious place where this occurs is in supply chain risk, where key stakeholders need to be reassured that a supply chain is sustainable, secure, and free of criminality. During the pandemic, supply chains were put under considerable pressure, and pen testing played a pivotal role in helping organizations adapt to these challenges and protect customer and partner data.

Stakeholders have also adapted to the changing needs for pen tests, such as in the UK, where the National Cybersecurity Centre added a home and remote-working exercise to its existing package of pen testing exercises.

## Preserve the Organization's Image and Reputation

Cyber incidents cause **fundamental harm** to an organization's reputation, particularly when they put customer data at risk and result in prolonged legal proceedings. Breaches and attacks are becoming more prevalent in business reporting, and consumers are now more wary about their data and privacy. Pen tests represent a **crucial part of the cybersecurity stack** and help prevent these attacks and the resultant harm to reputation.

According to IBM, the average cost of a breach for U.S. companies is $4.24 million. A huge portion of this cost comes from the impact breaches have on reputation.



# Penetration Testing Options

## PROS AND CONS

Although the tools and tactics used by pen testers don't vary much, the testing frameworks within which pen testers operate have **significant differences.** The framework you choose will have a major impact on the testing experience for everyone involved (e.g., testers and testing consumers alike).

### Traditional ("Status Quo") Penetration Testing

In the next section, we'll go into more detail about how the most common approach to pen testing has led to low expectations for pen testing, but at a high level, the pros and cons include the following:

**PROS**

- Established budget line item
- A known quantity
- Usually low cost

**CONS**

- Slow, cumbersome, and consulting-heavy service delivery
- Inflexible with questionable skill fit
- Low-intensity testing with low-impact results
- Multiple providers often required

## Crowdsourced Pen Testing

The crowdsourced model implies the involvement of a bench of trusted pay-per-project testers who are crowdsourced from the massive hacker community. Crowdsourced testing is quickly becoming the top choice for organizations seeking more impact from pen testing.

### PROS

- Offers access to the massively diverse skillsets of a global community
- Option to “pay for impact” instead of time to incentivize better results
- Enables easy tester rotation

### CONS

- Still unfamiliar to many AppSec decision makers
- New business case may be required

## Internal Security Testing

While often infeasible for smaller organizations, some enterprises prefer to build and maintain in-house teams ("red teams") of security testing. This approach allows the organization to set its own schedule and may reduce barriers in some areas (e.g., the provision of credentials).

### PROS

- Best for extremely sensitive work
- Can be run as frequently as needed
- Low marginal cost

### CONS

- Labor intensive to set up and maintain
- Impossible to retain all testing skills
- Hard to acquire new skills when needed

## A Mixed-Testing Approach

Some organizations use a combination of traditional, crowdsourced, and internal testing to meet the specific needs of each project.

### PROS

- Includes the best aspects of each method
- Potential for thorough security coverage
- Testing depth for each project is on an ad hoc basis

### CONS

- Includes the worst aspects of each method
- Complex to arrange and maintain
- It can be extremely costly



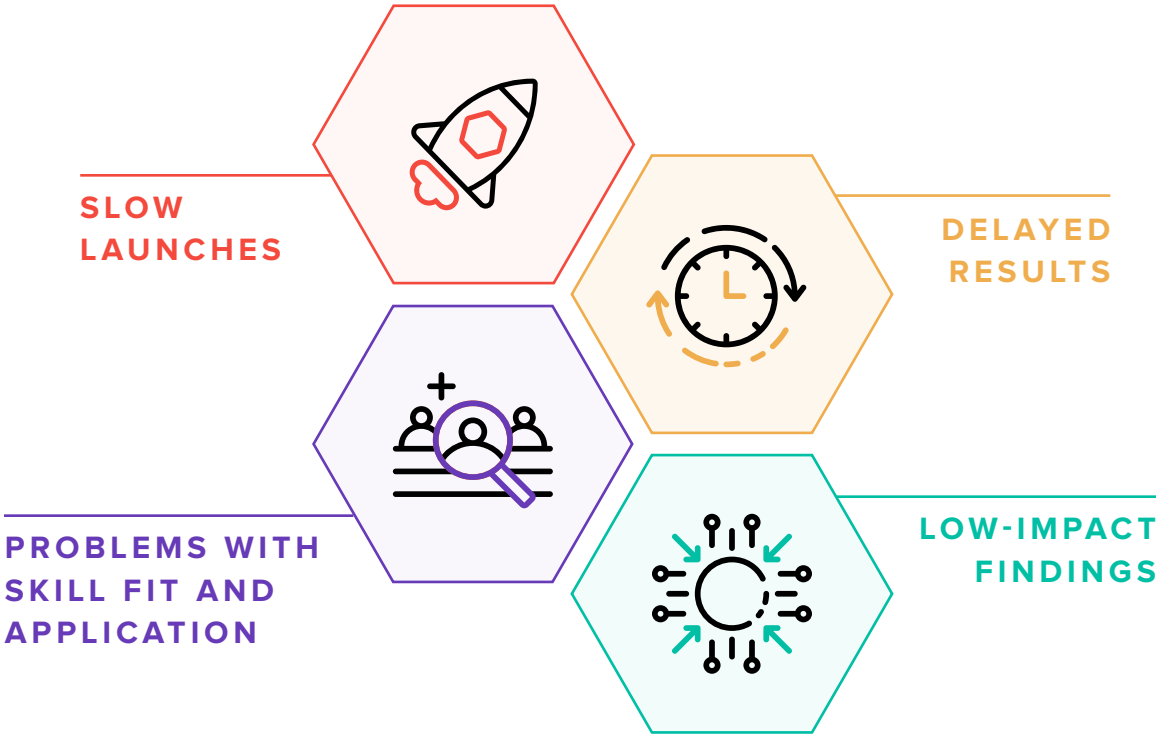
# Problems with Traditional Pen Tests

Over the past five years, there has been a growing consensus that the most traditional approaches to testing have become dated, if not obsolete. These traditional pen tests adopt a **"one-size-fits-all"** approach; simulated attacks are carried out by one to two testers who offer box-ticking results according to narrowly defined compliance-based methodologies.

These tests can be useful for confirming hypotheses or concerns within the organization, but they do not meaningfully reduce risks or address unknowns.

Since then, gaps and failings in the strict and narrow approach to pen testing have resulted in even lower expectations for pen testing from its adopters. Below are the most pressing concerns.

### Gaps in the Traditional Pen Testing Model





## SLOW LAUNCHES

Tests can take months to schedule due to resource constraints on the part of testing providers and their desire to reduce time on the “bench” for salaried employees.

This might seem fine to companies that consider these tests to be the equivalent of a routine dental check-up but not for the many organizations that worry that they may need an emergency root canal.

Many of these tests also come with strictly limited time windows for delivering a testing schedule. These can cause the exclusion of some crucial testing methods—for example, it is impossible to carry out a 10-day scan as part of an assignment where five days have been allocated for testing. Putting artificial time constraints on pen testing reduces the extent to which it can reduce risk.

## DELAYED RESULTS

Another way timing is a problem is the delay in receiving results. With a standard pen test, the customer doesn’t receive results until the engagement is concluded, often 14–24 days after testing begins. This leaves assets vulnerable for an unnecessarily long time, which can be a real issue when the pen test is being carried out to address a newly identified risk as quickly as possible.

Most digital assets are only pen tested a maximum of one to two times per year. With modern agile development lifecycles, new codebase versions are released much more frequently. While an asset may be secure immediately following a test, new code releases could leave it vulnerable to attacks until the next scheduled test.



## PROBLEMS WITH SKILL FIT AND APPLICATION

A traditional pen test is carried out by one to two testers over a period of two weeks. Regardless of how experienced the testers are, they can't be versed in every possible attack technique, and their skillsets may not be appropriate for the asset being tested. Furthermore, in these situations, customers don't have the option of selecting which testers are assigned to their projects. Paying for these tests "off the shelf" adds a randomized element around what testers the organization has access to, which can have a profound effect on the results.

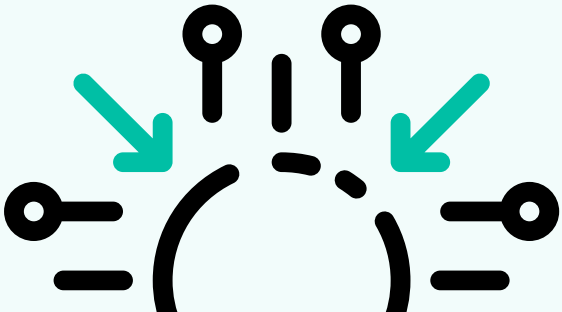
There is also an issue of skills being applied too narrowly, with most pen tests being based on checklists. These provide minimal time or few incentives for testers to use their initiative or "dig deeper" to find complex vulnerabilities. This issue is exacerbated by a "pay-for-time" business model, where buyers pay for a certain number of tester hours and the testers are only required to finish the methodology within that time. The number and severity of vulnerabilities that surface during this time are irrelevant to the tester's final pay.

## LOW-IMPACT FINDINGS

All the above-mentioned limitations contribute to the central problem of relying solely on traditional pen tests. The narrow nature of the timing, skillsets, compliance focus, and selection of participants reduces the effectiveness of a traditional pen test engagement in relation to alternatives.

**Due to poor results, high costs, and time delays, traditional pen testing services are not a cost-effective security measure. Worse, because skill fit is likely to be suboptimal and testers aren't incentivized to "go deep," it's more likely that high-risk vulnerabilities will be missed.**

Given this, the traditional pen testing model is simply not suited to the needs and goals of most adopters today.

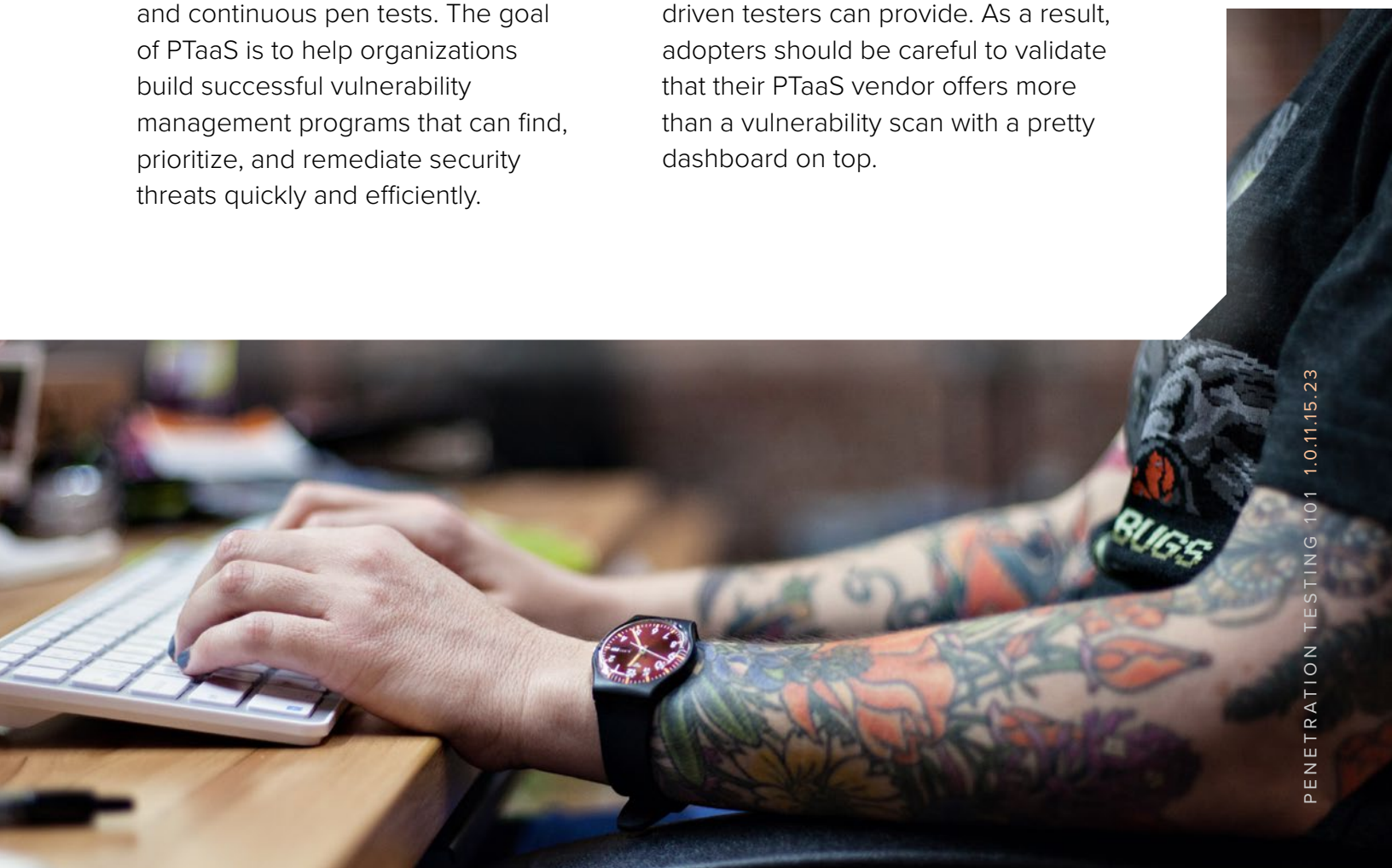


# What is Pen Testing as a Service (PTaaS)?

With the new dominance of the cloud in IT, recently, we've seen the emergence of **Penetration Testing as a Service (PTaaS)** options that have modernized pen testing by incorporating the agility, scale, and user experience of SaaS. This is a welcome development for buyers accustomed to the cumbersome, consulting-heavy approaches of traditional vendors.

TechTarget defines PTaaS as a cloud service that provides IT professionals with the resources they need to conduct and act upon point-in-time and continuous pen tests. The goal of PTaaS is to help organizations build successful vulnerability management programs that can find, prioritize, and remediate security threats quickly and efficiently.

That being said, because most PTaaS options rely heavily on automation to achieve scale, such tools lack the depth and intensity that only human-driven testers can provide. As a result, adopters should be careful to validate that their PTaaS vendor offers more than a vulnerability scan with a pretty dashboard on top.



# Benefits of PtaaS

PTaaS delivers high-velocity, high-impact results to ensure both compliance and risk reduction at the speed of digital business. Some of the benefits are as follows:

Brings modern SaaS sensibilities to pen testing, such as self-service dashboards, repeatability/scale, and a good user experience for pen testers and adopters alike

Enables much faster launches (days instead of weeks) and report delivery than traditional approaches

Integrates findings directly with DevSec workflows so remediation can begin quickly

# Watch out for...

Many old-fashioned or traditional pen testing firms use language that indicates they provide PTaaS solutions. However, this is often not true. When evaluating vendors, organizations should watch out for the following:

Excessive reliance on automation that leads to shallow/checkbox results

Limited choice of target types

Manual scoping

Narrow, siloed solutions that don't integrate with other programs

"Crowd washing" or old-fashioned pen tester sourcing masquerading as crowdsourcing

**The existence of one or more of these indicators may mean that the firm you're speaking to doesn't actually provide PTaaS.**

# The Future of Pen Testing

The most effective and convenient way to do pen testing is to bring the value of crowdsourcing to PTaaS.

## Crowd-Powered PTaaS

While many organizations share a need for compliance, not all have the same testing requirements or capacity. Some seek continuous coverage to match increasingly rapid development cycles. Others need shorter testing windows throughout the year, as dictated by engineering workflows or budgetary and procurement cycles. Furthermore, an organization's ability to provide tester incentives may be shaped by its bandwidth for addressing vulnerabilities and its ability to maintain an elastic pool of monetary rewards.

To address these varied needs, Bugcrowd provides crowd-powered PTaaS through our multi-solution platform—matching skillsets from the global hacker community (called the Crowd) to ensure high-velocity, high-impact results, while providing methodology-based coverage and compliance reporting.

### Only Bugcrowd PTaaS Offers...

- ✓ A trusted and expert team of pen testers selected for your specific needs.
- ✓ 24/7 visibility into timelines, analytics, prioritized findings, and pen tester progress through the methodology.
- ✓ Ability to "clone" pen tests at scale for repeatability and manage them all as a group.
- ✓ Easy rotation of the pen tester bench as needed.
- ✓ A choice of "pay-for-time" or "pay-for-impact" incentives.
- ✓ Crowd-powered pen tests to identify on average 7X more high-priority vulnerabilities than traditional pen tests.



# Combining Pen Testing with Bug Bounty Programs

Bug bounty programs engage with specialized hackers to help organizations find vulnerabilities at scale. They use a pay-for-results model, which incentivizes impactful results. For example, P1 and P2 vulnerabilities, which are more critical, get paid out more reward money than P4 or P5 vulnerabilities.

Both bug bounty programs and pen testing take a focused, strategic approach to the discovery and assessment of vulnerabilities and greater security risks.

Both solutions also rely on attacker tools, techniques, and mindsets for vulnerability discovery under a predefined scope. Although both solutions have similar goals, they differ with respect to the intensity of the assessments. For this reason, many organizations find that a **layered strategy** of using both provides the best results.

By using both pen testing and bug bounty programs for compliance and risk reduction, organizations can build a strategy that combines the following:

**1**



**Ongoing vulnerability discovery and assessment**

When the exploitability of vulnerabilities is confirmed, this is what some might consider a “basic” pen test.

**2**



**Periodic, human-driven pen testing to find common flaws**

This is what some might consider a “standard” pen test.

**3**



**A continuous bug bounty running “over the top”**

This picks up emerging vulnerabilities that are not yet detectable using the prior two methodologies.

# The Dawn of a New Era in Pen Testing

Some security leaders get nostalgic about the traditional approach to pen testing—it's comfortable and familiar. But the adoption of Bugcrowd's crowdsourced PTaaS shows that the trend is leaning toward the adoption of more modern, distributed testing that creates access to diverse skillsets and away from cumbersome, consulting-heavy approaches that depend on scanning or plain vanilla human testing.

Even for organizations that prioritize compliance over risk reduction in pen testing, crowdsourcing can be just as good, or better, at meeting compliance requirements than a small team.

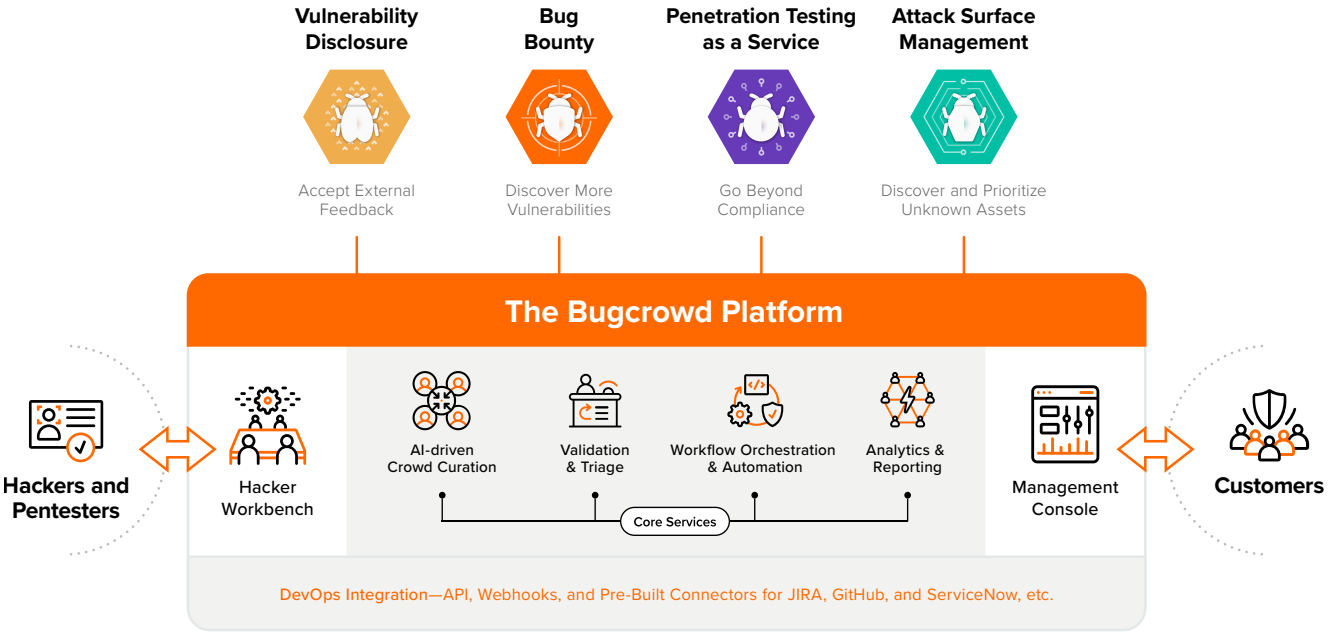
Ultimately, pen testing is another piece of the security puzzle. Organizations should incorporate it into their arsenal of security tools and processes to find and remediate vulnerabilities in the software development lifecycle (SDLC).

Crowdsourced pen testers are a crucial piece of this **dynamic security puzzle.** As they continue to build out this industry, expect it to continue to grow in importance and adoption.



# The Bugcrowd Platform

PTaaS isn't the only way to leverage the power of the Crowd. The multi-solution Bugcrowd Platform brings the right crowd into all your workflows at the right time, allowing you to run bug bounties, pen tests, vulnerability disclosure programs, and more at scale and in an integrated, coordinated way.




### ✓ Best Security ROI from The Crowd

We match you with the right trusted security researchers for your needs and environment across hundreds of dimensions using AI.

### ✓ Instant Focus on Critical Issues

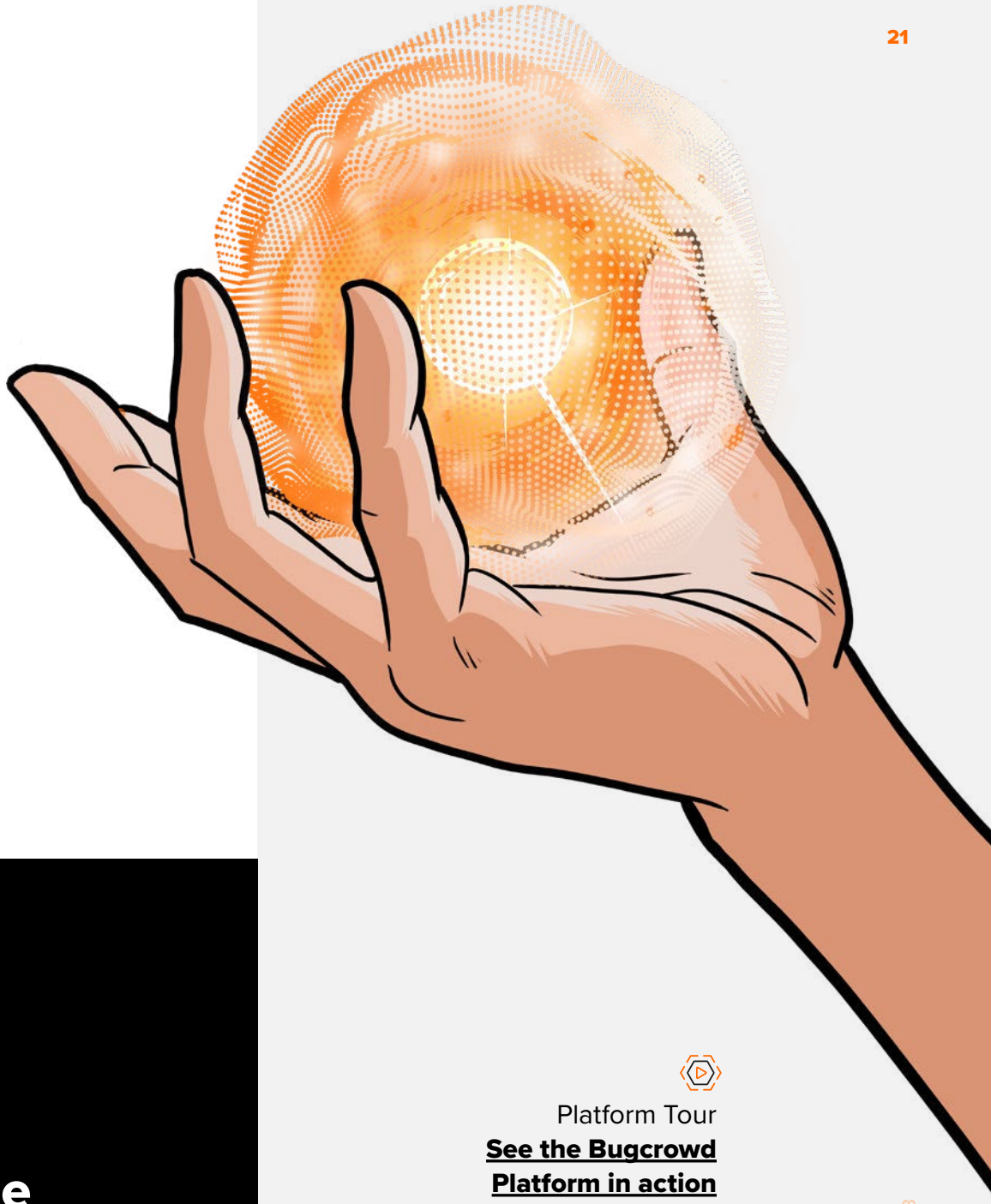
Working as an extension of the platform, our global security engineer team rapidly validates and triages submissions, with P1s (critical vulnerabilities) often handled within hours.

### ✓ Continuous, Resilient Security for DevOps

The platform integrates workflows with your existing tools and processes to ensure that applications and APIs are continuously tested before they ship.

### ✓ Contextual Intelligence for Best Results

We apply accumulated knowledge from over a decade of experience crafting thousands of customer solutions to your goals for better outcomes.



# Unleash the ingenuity of the global hacking community now

Try Bugcrowd

Platform Tour
**See the Bugcrowd Platform in action**

Data Sheet
**Bugcrowd PTaaS**

bugcrowd