The Buyer's Guide to Modern Pentesting

Cobalt
Pentest as a Service

Table of Contents

Introduction

Managing cybersecurity is a complex operation. While balancing business interests with security needs, teams also have to handle growing attack surfaces, increasing numbers of cyber breaches, and rising scrutiny from leadership, stakeholders, and auditors.

No team can withstand these pressures without the help of external tools and services. But finding the most fitting solutions can feel like a challenge in itself — one that takes time away from impactful work on your security program. Vendor assessments can get particularly lengthy when reviewing services like manual pentesting, where teams search for a partner that will understand their workflows and align with them.

This guide aims to shorten that process and get you closer to finding, fixing, and preventing vulnerabilities. It explains how the pentesting market has evolved over the past 5-10 years and walks you through the following details:

- What scenarios call for a pentest
- What the market offers, pulled into three vendor groups
- What value each group brings to different stages of the pentest cycle
- Which option offers the best ROI for security programs as a whole
- What criteria you should consider when reviewing specific companies (with a checklist attached)

When You Need Pentests

Compliance

Compliance frameworks are the most common triggers for a third-party pentest. Nearly every industry has one. For example, consider how e-commerce revolves around PCI DSS, healthcare focuses onHIPAA, and SaaS vendors demonstrate good security with SOC 2 reports and ISO certifications. There are numerous other frameworks out there, and pentesting is a part of most of them. PCI DSS calls for a pentest at least once a year, while HIPAA, SOC 2, and ISO 27001 include it as a component of a wider requirement, typically regular security assessments.

→ LEARN MORE ABOUT COMPLIANCE DRIVEN-PENTESTING

Customer Requirements

If your auditor doesn't ask for a pentest, chances are your customers will. Digital services have created a complex network where one successful breach can impact multiple companies connected to the target, as evidenced by the FireEye and SolarWinds incidents in late 2020. As a result, businesses are increasingly concerned about their vendors' commitment to security and before they sign, they request documents such as a SOC 2 report or a pentest report issued in the past 6 months.

Mergers & Acquisitions

Whether getting acquired or acquiring another company, you will find that security assessments have become an integral part of the due diligence process. 100% of executives and advisors in a 2019 (ISC)[2] survey said security audits have become standard practice in M&As. Pentests are a common component of these audits, both as a point-in-time snapshot and as part of a continuous testing program.

Multi-Layered Security Testing

Clearly, the pressure is on for cybersecurity. To mitigate risk and mature their programs, teams are increasingly diversifying their approaches. One example is the combination of automated security tools and manual pentests. When configured correctly, scanners can capture malware signatures, coding errors, and suspicious behavior patterns. Pentests can act as an additional layer of defense, validating these tools' accuracy and searching for more complex flaws that require creative thinking: business logic flaws, authorization inconsistencies, chained exploits, and race conditions.

What's on the Market

The pentesting market can be broken down to three groups: crowdsourced software security testing platforms, traditional consultancies, and Pentest as a Service vendors. Each differs in how it sources, vets, and connects pentesters with customers. Pentesting operations also work differently with each group. Let's take a brief look before diving into a more detailed comparison.

Crowdsourced Software Security Testing Platforms

The first option is what Gartner describes as "Crowdsourced software security testing platforms," or CSSTPs. Vendors under this category offer a variety of testing services, including pentesting, bug bounties, and vulnerability disclosure programs. Tests are done by "the crowd" — global communities of hundreds, sometimes thousands of testers, grouped into tiers ranging from large and unvetted to small and highly vetted teams.

CSSTPs give you an unparalleled choice of testers. On the other hand, you have to spend more time scoping and scheduling tests, and may experience higher management overhead compared to the two options below.

Traditional Consultancies

Traditional consultancies are practices that bundle pentesting with wider security advisory services. They operate as a one-stop-shop, creating bespoke packages for each customer. Most maintain a large workforce of pentesters hired on a full-time basis.

Combined, these features make consultancies attractive for large enterprises, but put their pricing out of reach for small and mid-sized companies. With a larger portfolio of services to maintain, consultancies can also be slower to innovate their pentesting workflows. Often needing weeks to set up a test, they can miss the mark for more agile-minded teams.

Pentest as a Service

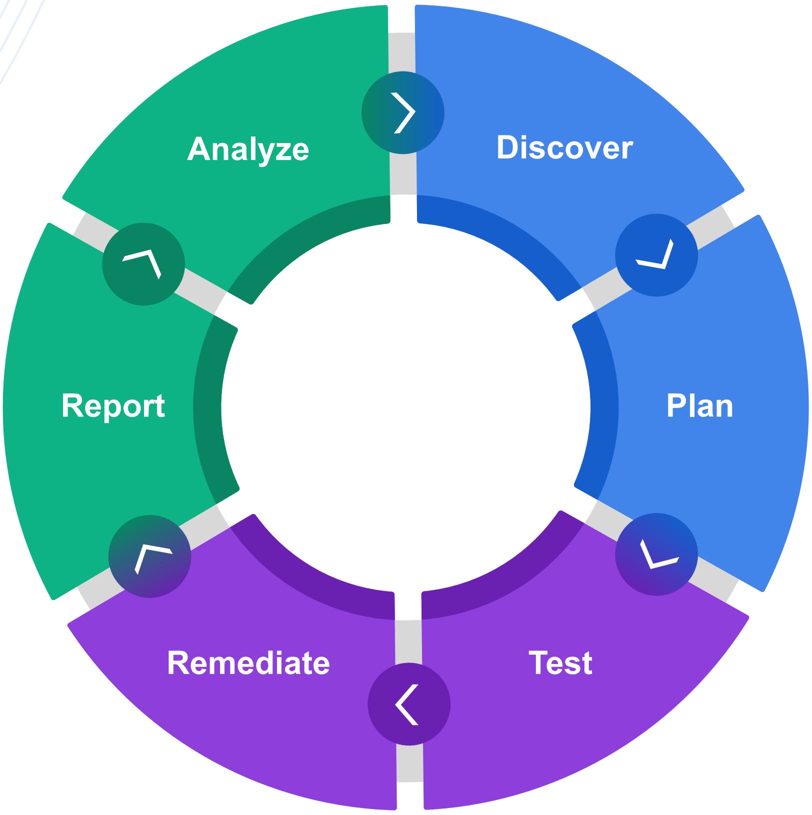
Pentest as a Service (PtaaS) is a relatively new model. Similar to CSSTPs, vendors in this category build and maintain a pentester community, but often have more rigorous vetting processes. They also offer customers SaaS-like platforms to scope, schedule, and manage their tests in the cloud.

Vendors in this category concentrate on innovating the pentesting process. While this limits their selection of additional security services, their pentests tend to be more efficient and collaborative. Testers work closely with your security and development teams, while integrations automate numerous tasks. As a result, their pricing is more affordable and tests can start faster, sometimes within 24-48 hours.

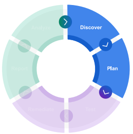
Comparing Each Option

Pentesting is a multi-step process. CSSTPs, consultancies, and PtaaS vendors approach it differently, with important details that distinguish them at every stage. To highlight these nuances, this guide will break down the pentest cycle into 3 components: **Discover & Plan**, **Test & Remediate**, and **Report & Analyze**.

You'll learn what should happen as a baseline for each stage, and see what the three vendor groups bring to the table. You'll also see what additional features each offers to further elevate your pentests' impact. Towards the end, you'll have a full view of how CSSTPs, consultancies, and PtaaS vendors stack up against each other with their technology, people, and processes.



01 Discover & Plan



Laying the groundwork for a productive pentest.

The "Discover" phase is where you map out your attack surface. This gives you a clear vision of your applications, APIs, networks, cloud instances, and other assets you might be managing. It is best to categorize items according to a set of criteria, for example how important they are to business function, whether they hold sensitive data, and how likely they are to be attacked. These factors determine assets' criticality, which guides your decisions on what gets tested and how often.

The "Plan" phase is where you define the upcoming test's scope, describing details such as:

- **Targets**: What assets need to be tested, and should the pentesters focus on specific features?
- **Objectives:** What do you hope to achieve with the test, e.g. a routine check versus zeroing in on user authorization?
- **Instructions**: Are there any technical details you want the testers to be careful about, or aware of?
- **Timing**: Do you want the test to start as soon as possible, or schedule it for a later date?

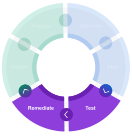
Vendor Comparison

	CSSTPs	Consultancies	PtaaS
Scoping the test	Collect scoping details via questionnaires and publish info to their tester community	Scope tests with customers as part of a wider security service package, usually via calls, meetings, or emails	Provide step-by-step scoping instructions and detailed templates for self service in a cloud platform Support teams are available for scoping calls if preferred
Sourcing talent	Offer a range of options, from unvetted to highly vetted hackers across the globe	Pick out testers from local in-house teams, depending on their customers' location and testing scope	Match customers with highly vetted testers across the globe, based on test and asset requirements
Scheduling the test	Can start tests within 3-7 days after confirming scope	Can start tests within 4-6 weeks after confirming scope	Can start tests within 1-2 days after confirming scope

Ask the Vendor

"How do you help us set up a successful pentest? How quickly can we get the test started?" Planning and scheduling are critical first steps, and your chosen vendor should make them as seamless as possible.

02 Test & Remediate



Addressing vulnerabilities quickly and effectively.

Once staffed, the pentest moves to **the "Test" stage.** Pentesters use the information provided in "Plan" and begin their inspection, recording their findings as they go. Some vendors will notify you in real time and continue testing, others will wait until the test is complete. Whatever the scenario, findings need to be clear and descriptive, with proof of concept, notes on perceived criticality and impact, and recommended fixes.

Once this information reaches your team, you can start **the "Remediation" phase**. Typically, the more detailed pentesters' findings are, the more effective your fixes will be. An important differentiator is how involved vendors are at this stage — some don't participate, while others have pentesters work together with your teams to clear up questions and validate fixes. Retesting is another important factor: some vendors charge a premium for retests, others include it as part of their base package for a limited time.

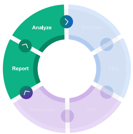
Vendor Comparison

	CSSTPs	Consultancies	PtaaS
Accessing test findings	Testers record findings in the platform, customers get a notification Customers can manage findings in the platform or send them to their internal tools	Results are available once test is complete and the final report has been written, edited, and approved Findings are collected in encrypted PDFs	Findings appear in the platform in real time, customers get notifications Findings are available as individual tickets that can integrate with Dev tools
Collaboration between testers and internal teams	Testers assist in triaging and remediation for an additional fee	Testers assist remediation for a fee, customers typically have to wait for their availability	Pentesters work with developers and security in dedicated workspaces, e.g. Slack, as part of the basic package
Coordinating remediation efforts	Platform integrations with Dev tools enable remediation teams to automatically share findings' status	Remediation process is managed across emails, messages, phone calls, and meetings — possible communication overhead	Platform reflects comments and actions stored in customers' internal tools with the help of native integrations

Ask the Vendor

"What information will your findings include, and how fast do you send them? Any integrations that could make remediation more efficient?" Select a vendor who will give you critical information as quickly as possible for a swift response.

03 Report & Analyze



Learning from tests and improving your security program

The "Report" stage has two sides to it:

1. The vendor provides a document listing all discovered vulnerabilities, participating pentesters, used methodologies, and the actions you've taken during "Remediation."
2. You share this documentation with auditors, customers, and internal stakeholders.

"Analyze" is taking that documentation and drawing actionable insights from it. Does most of what the pentesters discovered concentrate around a particular issue, say Broken Access Control? Could that suggest a wider design flaw in how your application handles user authorization? If you have done multiple pentests, are you seeing issues re-emerge at a later date? Do you get fewer or more findings with each report?

These are all questions you can explore, not just with one pentest, but across multiple tests if you set up a continuous pentest program. The goal is to prevent vulnerabilities earlier in your SDLC by extracting learnings from each engagement.

Vendor Comparison

	CSSTPs	Consultancies	PtaaS
Reporting test results	Final report is available in different formats for multiple stakeholder groups	Final report comes with limited options to customize or adjust its structure	Similar to CSSTPs, final report can be further customized with editable layout templates
Analyzing progress over time	Platform displays data on discovered vulnerabilities and test coverage, comparing customer performance against global stats	Long-term analytics are an additional advisory service	Dashboards track vulnerability and remediation data from multiple tests and benchmark against global stats
Options to scale pentest program	Platform stores data from different testing services	Longer admin time spent manually redoing test scopes	Platform stores asset and findings data for analysis and easy transfer to upcoming tests

Ask the Vendor

"How do you help customers improve their security posture over time?" Select a vendor that makes it easy to retain and analyze insightful data that can inform your next steps.

At a Glance

✓ offer the feature as part of their basic package

✗ do not offer the feature

! only some vendors in the category offer the feature, or include it for an additional fee

	CSSTPs	Consultancies	PtaaS
Discover & Plan			
Self service* and planning assistance	✓	✗	✓
Highly vetted testers	!	✓	✓
Test up and running in less than a week	!	✗	✓
Test & Remediate			
Real-time notifications of findings throughout the test	✓	✗	✓
Collaboration between pentesters and customers' teams	!	✗	✓
Pentesters assist remediation and validate fixes	!	!	✓
Report & Analyze			
Customizable reports	✓	✗	!
Continuous analytics	!	!	✓
Tests easy to replicate, can scale to a larger program	!	✗	✓

*Self service is the option to get your pentest started without having to attend calls and/or meetings with the vendor, even if it's your first time working with them. This is a benefit cloud platforms with intuitive onboarding can offer.

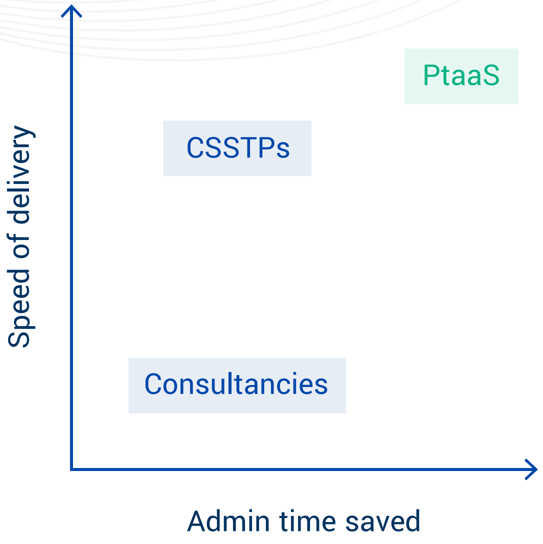
ROI Comparison

Aside from comparing the features each group offers, it's also important to consider their impact on your security. We measure impact based on two factors: time (both admin time and how quickly you get test results) and remediation effectiveness.

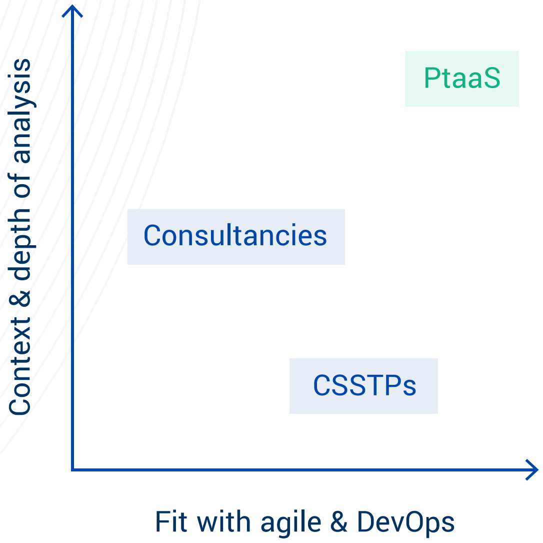
Time

Consider time from two perspectives: how much time your team spends on admin — planning, managing, and supporting a pentest project; and how quickly pentest findings reach you.

Consultancies are the least time-efficient of the three options. In fact, a recent study into the ROI of modern pentesting found that consultancies need twice as much time as PtaaS vendors to produce test results. As for admin time, PtaaS vendors require 25% fewer days because of their platforms' capacity to automate tasks and retain data for later re-use.



When pulling these ROI metrics together with the features listed in previous sections, PtaaS vendors stand out as the most modern pentesting solution.



Remediation Effectiveness

To successfully patch discovered vulnerabilities, you need to be assured that findings are based on a thorough analysis. While findings need to be clear and descriptive, it's also important how this information reaches your teams: the less aligned the reporting process is with DevOps workflows, the more complicated it becomes for developers to fix issues.

CSSTPs & PtaaS platforms integrate with a variety of Dev tools and send findings where the remediation team works, pulling them ahead of consultancies. What puts PtaaS vendors on top is that their basic packages consistently include tests done by highly vetted, skilled, and experienced professionals — CSSTPs typically apply an additional fee for vetted testers.

Cobalt's Take on PtaaS

Start Testing Faster

Launch pentests in **days, not weeks** with our intuitive platform and team of **on-demand security experts**

Remediate Risk Smarter

Accelerate find-to-fix cycles through technology integrations and **real-time collaboration** with pentesters

Make Security Stronger

Mature your security program through a **scalable, data-driven** approach to pentesting

50%

Faster to execute a pentest than traditional consultancies

300+

Highly vetted pentesters around the world

24 hours

To get a pentest up and running

> "The main benefits that we get from Cobalt are speed, scalability, and repeatability. We're able to quickly launch and execute pentests; and beyond that, we're able to see individual findings in real time and relay them to the engineering team so they can start triaging immediately."
> **Eric Galis - VP of Compliance and Security at Cengage**

Cobalt Integrations

Connect Cobalt to the tools & platforms you're already using to gain more insights, increase findings visibility, and streamline the SDLC.

Jira

Slack

Tugboat Logic

Kenna Security

ThreadFix

GitHub

JupiterOne

DefectDojo

Asana

ANNEX: Vendor Criteria Checklist

	Vendor offers in base package:
- People	
Global and diverse selection of pentesting talent available on demand	
Thorough vetting processes to ensure skilled and comprehensive analysis	
Matches with pentesters whose skill sets align with pentest’s requirements	
Pentest team is managed by an experienced lead who sets SLAs, verifies findings, and acts as a liaison with the customer	
Dedicated customer success team available throughout the pentesting process	
- Process	
Options to pentest multiple types of assets: mobile, API, web app, networks, and cloud instances	
Intuitive setup with descriptive templates for independent planning and scheduling	
Tests can begin within 24-48 hours	
Testers follow industry-recommended methodologies	
Visibility into progress over time without having to check in with vendor’s customer support team	
Descriptive findings with proof of concept, criticality level, recommended fixes	
Real-time notifications of findings during the pentest	
Pentesters collaborate with security and development teams during testing and remediation	
Free, unlimited retesting to validate fixes	
Thorough, customizable reports	
Option to re-use prior pentests’ scope and results to launch new tests more quickly	
- Tools	
Cloud-based platform to plan, schedule, track, and manage multiple pentests	
Integrations with wide variety of tools for DevOps, compliance, vulnerability management, and business intelligence	
Open API	
Analytics dashboards tracking multiple metrics over time and against a global average	