hackerone

2022 Buyer's Guide to Pentesting

How to Choose and Assess the Ideal Pentest Solution for Your Organization's Needs

Table of Contents

Introduction

As IT infrastructure has grown in scope and complexity, vulnerability reports have soared. In 2020, the National Vulnerability Database (NVD) added 29,867 new vulnerabilities.

With more sophisticated infrastructure comes a rise in the complexity and visibility of vulnerabilities. Past issues that went unnoticed, at least for long periods, are discovered daily today.

Organizations need a mechanism to uncover vulnerabilities in their digital assets or risk damaging and costly security incidents. Basic controls like scanners help alleviate the problem by providing broad coverage for basic security issues, but there's no substitute for the testing depth and creativity offered by expert human testers.

What is a Pentest?

A pentest is a foundational requirement for any security program. Pentest engagements enlist human expertise to scrutinize digital assets—most commonly software—with the objective of uncovering and resolving security vulnerabilities before a malicious actor can exploit them. Despite their critical role, many organizations misunderstand pentests.

Traditional pentests are engagements delivered by a security services provider that attempt to find vulnerabilities in a specified asset or group of assets. In most cases, testing is delivered by on-staff security experts and follows a checklist-based approach. While this can help to ensure consistency and coverage between engagements—an important consideration, particularly for compliance-driven testing—it also limits the effectiveness of pentest engagements for finding non-standard vulnerabilities.

Today, pentests can go beyond these limited engagements to deliver comprehensive security and compliance benefits. The most important addition is diversity, both of testers and testing practices.

Where traditional penetration testing relies on a small pool of on-staff experts, organizations now have access to a huge pool of testers worldwide through the global hacker community. This introduces a far wider range of expertise, techniques, and tools to the pentest process, helping to uncover more exploitable and high-risk vulnerabilities—once again, before a malicious actor can exploit them.

Why Pentest?

Organizations need pentesting that supports key business objectives. These begin with basic regulatory and compliance obligations, but ultimately encompass a wider range of security, risk reduction, and business needs. The most common pentesting objectives include:

1. **Compliance** — Almost all regulatory and compliance frameworks like FedRAMP, NIST, and CISA require organizations to conduct pentests, usually on an annual basis.
2. **Meeting stakeholder requirements** — Many organizations will only work with partners or customers that uphold certain security standards.
3. **Protecting assets and preventing downtime** — Damage and disruption to digital assets can be costly. With the right visibility into application and system vulnerabilities, organizations minimize their risk.
4. **Protecting customer data** — Sensitive data is heavily regulated, and it's also an asset used to understand customers and improve products and service. Securing that data is both a business imperative and a regulatory requirement.
5. **Minimizing cyber risk** — Data breaches are a substantial risk and cause financial, operational, and reputational damage. The IBM 2021 Cost of a Data Breach report found breaches cost on average $5.52 million. Security testing like pentests help organizations understand and proactively manage risk with valuable vulnerability intelligence.
6. **Supporting software and product development** — Organizations need more frequent and thorough pentests that deliver timely information to support rapid development cycles and allow collaboration between security and development teams. Ideally, organizations choose a combination of external pentesting and internal controls that supports existing development workflows (e.g., DevOps or CI/CD pipelines) and reliably delivers secure code to production.

While improving security and reducing risk are top priorities, compliance has historically been the main driver for penetration testing. Failure to meet compliance requirements can result in multi-million dollar fines, and until recently the risk associated with these fines was often greater than the risk of a security breach.

Most penetration testing providers deliver a simple approach to meet testing requirements across various regulations and frameworks.

But organizations' needs go beyond passing audits and checking a box, and penetration testing engagements must evolve to support the more pressing need for proactive cyber risk management. The use of pentesting for additional risk management by finding vulnerabilities before exploitation extends an organization's security profile while still meeting compliance and regulatory requirements.

Additionally, as dependence on software and non-traditional network architecture grows, the need to maximize security has overtaken compliance as the most important consideration for many organizations. Organizations now need additional pentest options that go beyond compliance coverage to proactively reduce cyber risk by uncovering vulnerabilities throughout the attack surface—including cloud and hybrid infrastructure. These options must combine more advanced testing for security weaknesses with the flexibility to support regular updates to business-critical software assets.

What Pentesting Options Are Available?

When people hear the word "pentest," some may immediately think of security service providers. However, there are three types of pentest engagement, each with its objectives, benefits, and drawbacks.

Option 1

Traditional

Delivered by:
A security service provider

Duration:
Usually 1–2 weeks

Designed to:
Uncover common security weaknesses

Characteristics:
Checklist-driven, compliance-focused

Advantages

- Established budget engagement
- Schedule to support product releases
- Supports compliance needs

Drawbacks

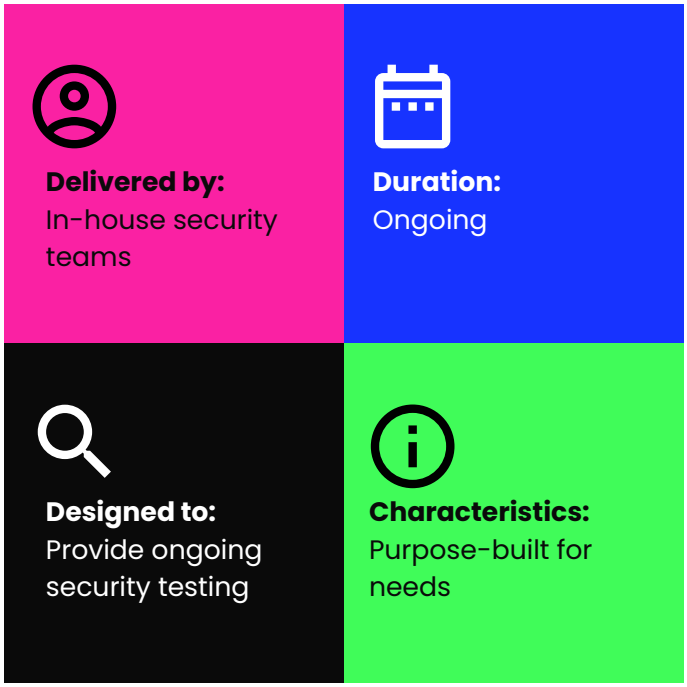
- Limited pool of testers and expertise
- Testing model doesn't encourage creativity
- Results often limited to common vulnerabilities
- Long lead times can cause delays
- Minimal prioritization of results

Traditional penetration tests might be for you if you need to:

- Meet regulatory and compliance obligations
- Find common vulnerability classes
- Test non-critical software 1-2 times per year
- Test assets that require rare skills, e.g., unusual hardware

Option 2

Internal



Advantages

- Highly-flexible and supports internal needs
- Instant, ongoing access to security testing
- Suitable for testing that requires a high level of system access
- Zero Trust model

Drawbacks

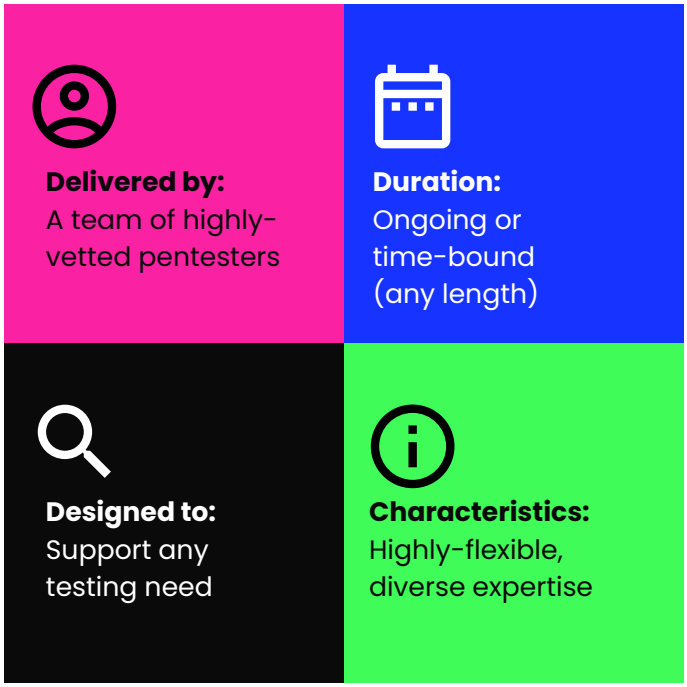
- Limited pool of testers and expertise
- Hard to find and retain suitable skills
- Unlikely to address short-term needs
- Not suitable for most compliance needs

Internal penetration tests might be for you if you need to:

- Continuously test specific assets
- Test assets too sensitive to share with an external provider

Option 3

Pentesting with Hackers



Advantages

- Uncovers complex, high-risk vulnerabilities
- Highly-flexible engagements and costs
- Access almost any testing skills needed
- Ideal for fast-moving environments and needs
- Real-time communication with pentesters
- Rapid retesting for fixed vulnerabilities
- Managed programs deliver verified vulnerabilities

Drawbacks

- May require a new business case
- Not suitable for internal assets
- May not be practical for hardware testing

Penetration tests with hackers might be for you if you need to:

- Maximize security outcomes and cyber risk reduction
- Uncover high-risk vulnerabilities of any complexity
- Support fast-moving development or digital transformation
- Tailor engagements to meet shifting security and IT objectives

On-demand pentests give organizations access to expert, vetted testers, including those with skill sets in specific asset classes. This ensures a more thorough pentest that uncovers critical vulnerabilities a less specialized tester might miss.

The HackerOne community talent pool supports continuous pentesting that runs 24/7/365, highlighting vulnerabilities the moment a hacker uncovers them. Continuous pentests mean that critical vulnerabilities are uncovered as quickly as possible, substantially reducing the risk of a cybercriminal exploit.

Example: HackerOne's Application Pentests for AWS

Thoroughly testing AWS applications requires specific capabilities and AWS Certified hackers. HackerOne offers on-demand pentests specifically for AWS applications. AWS Certified hackers uncover critical vulnerabilities specific to AWS applications protecting them from data leaks, subdomain takeovers, and cloud misconfigurations.

Continuous pentests

HackerOne's large talent pool supports continuous pentesting that runs 24/7/365. This ensures that critical vulnerabilities are uncovered as quickly as possible, substantially reducing the risk of a cybercriminal exploit.

Continuous pentests allow the same level of customization and specialized testing offered by hacker-powered pentests and security assessments.

HackerOne Invests in Hackers

HackerOne is the only platform with a dedicated team focused on hacker education initiatives. From CTFs, to live hacking mentorship programs, conference sponsorships, regional community days, twitch live streaming, and an active Discord server, we invest thousands of hours and well over $500K per year. We're committed to helping hackers broaden skill sets and grow their expertise.

Our HackerOne pentester community includes a global group of highly skilled pentesters who meet specific requirements including three years of professional pentesting experience and certifications in OSCP, OSCE, OSWE, and CREST. For in-platform hackers, these certifications can be replaced by in-platform statistics.

Our pentesters have many training opportunities like HackerOne-sponsored AWS Certification scholarships. AWS Certifications ensure pentesting-experienced hackers have the requisite understanding of AWS environments to more effectively pentest and quickly identify AWS application vulnerabilities. Hacker certification ultimately expands the expertise of HackerOne's community and offers a broader range of skill sets for AWS customers seeking to enhance their cloud security.

Which Pentest is Right for Your Organization?

Many organizations have a variety of security and compliance objectives that require pentesting. Organizations can combine various pentests to achieve these objectives and support security, IT, and development workflows.

Earlier in this guide, we listed seven common objectives for pentesting, beginning with the most basic:

1. Compliance
2. Stakeholder requirements
3. Protecting assets and preventing downtime
4. Protecting customer data
5. Minimizing cyber risk
6. Protecting reputation
7. Supporting internal software and product development

Compliance and Stakeholder Requirements

These needs are the most rigid in their criteria. Since stakeholder requirements are often linked to compliance frameworks, this section will address both objectives together.

To ensure compliance, your organization must determine what its obligations are, legal and otherwise. However, most compliance frameworks lack specific guidance.

For example, the Cybersecurity Maturity Model Certification (CMMC) requires U.S. Department of Defense (DoD) contractors to: *"Conduct penetration testing periodically, leveraging automated scanning tools and ad hoc tests using human experts."*

Other examples of vague requirements include:

- ISO 27001: *"[...] information about technical vulnerabilities of information systems being used shall be obtained in a timely fashion, the organization's exposure to such vulnerabilities evaluated and appropriate measures taken to address the associated risk."*
- NIST 800-53: *"Employ an independent penetration testing agent or team to perform penetration testing on the system or system components. [...] Independent penetration testing agents or teams are individuals or groups who conduct impartial penetration testing of organizational systems."*

Your organization can choose any pentest for compliance and stakeholder requirements—as long as it meets these criteria. This leaves your organization free to select pentests that support internal security and risk reduction objectives rather than choosing a pentest purely to satisfy a compliance checkbox.

Security and Risk Reduction

Depending on your organization's objectives, you should choose a pentest (or combination of pentests) accordingly. For example:

- **Protecting assets, preventing downtime, and protecting customer data** require your organization to maximize security. You can achieve this with a continuous hacker-powered pentest which exposes assets to a wide range of techniques.
- **Minimizing cyber risk** requires pentests that combine broad asset coverage with exposure to real-world cybercriminal tactics, techniques, and procedures (TTPs). Continuous and one-off hacker-powered pentests are ideal for **protecting reputation,** as this is one component of cyber risk.
- **Supporting internal software and product development** requires a pentest that can be arranged quickly with no wait time. It should also provide immediate communication with pentesters, allowing developers to clarify issues and request prompt retesting of patched vulnerabilities. Hacker-powered pentests are ideal because they provide real-time access to ethical hackers with diverse expertise and skill sets.

"Being able to have issues retested during the same engagement is a game-changer. That's something that hasn't been available in the past because traditionally, you didn't receive the results of a penetration test until after the engagement was over."

Rich Kellen, VP and CISO Wind River

Your organization should combine pentest options as needed to support current and ongoing needs. For example, you may use a continuous hacker-powered program for ongoing security coverage, hacker-powered pentests to support development roadmaps and most compliance objectives, and a traditional penetration test for PCI-DSS compliance.

"Being able to have issues retested during the same engagement is a game-changer. That's something that hasn't been available in the past because traditionally, you didn't receive the results of a penetration test until after the engagement was over."

Rich Kellen
VP & CHIEF INFORMATION SECURITY OFFICER, WIND RIVER

Why Choose Hackers over Traditional Penetration Tests?

While valuable for some use cases, traditional penetration tests have several drawbacks that make them unsuitable for current security objectives. Organizations need flexible pentests to build into existing development workflows and expose assets to a broad range of testing skills and expertise.

HackerOne pentests follow a structured testing methodology with hackers who are matched to your specific needs and in-scope software.

Working with vetted, proven hackers for pentests fulfills both requirements, making them ideal for supporting the needs of rapid-pace development teams and their security team counterparts. The table below compares traditional penetration tests with hacker-powered pentests to demonstrate some of the key differences:

	Conventional Pentest	Hacker-Powered Pentest
Scheduling	Typically a four to six week lead time to get started.	Get started in days.
Time-Frame	Point-in-time.	Point-in-time.
Talent	One to two testers are usually assigned to different engagements	Diverse and vetted pentester community with three to five testers assigned to different engagements. Tap into a vast rotating talent pool.
Tester Communication	Interact with project manager(s) but communications with pentesters may vary.	Communicate directly with pentesters to discuss issues and drive engagement via HackerOne platform.
Testing Process	Little to no interfacing with the security team throughout the testing process. The focus is on the final report.	Transparency of your pentest progress across kick-off, testing, retesting, and remediation phases.
Vulnerability Notifications	Critical or severe vulnerabilities aren't disclosed until the final report at the end of the engagement.	Act on vulnerabilities as they are surfaced and reduce remediation lag time. Always aware of vulnerabilities.
Vulnerability Management	Tests are purely transactional with each engagement independent from the other.	End-to-end vulnerability lifecycle management beyond initial reporting.
Integrations	No integrations with customer workflows.	Integrations with Jira, GitHub, Slack, etc.
Reporting	Final PDF report consolidates findings, but it's not organized to make important findings accessible, understood, and actionable.	Summarized, actionable report for both executive stakeholders and auditors. Detailed recommendations highlighted.
Pricing	Pentesters paid hourly, regardless of results.	Pentesters paid for coverage and effort.

Our On-Demand SaaS Platform Integrates with the SDLC Process

The HackerOne platform provides pentest management through a dedicated platform, giving your organization a single location to manage every aspect of the security testing program, including one-off and continuous pentests.

This has several benefits, including:

- Arranging new pentests is easy and fast.
- Provides easy vulnerability tracking from report through remediation.
- Delivers real-time, two-way communication between organizations and hackers.
- Allows organizations to easily request retesting for fixed vulnerabilities (this can take weeks with traditional penetration tests).
- Provides management-ready reporting on program status and costs.
- Gives the option to outsource program management, including human verification of all reported vulnerabilities.
- Supports the SDLC by feeding vulnerabilities directly into development workflows.

Combined with the flexibility and broad expertise of working with hackers, the platform gives organizations full control, making it easy to tailor pentests to their objectives.

Tracking Pentest ROI

Ideally, organizations would measure pentest return on investment (ROI) using a metric such as a dollar value or measurable risk reduction. However, this is challenging because pentests are preventative measures. It's impossible to know which vulnerabilities, if not reported, would have led to a security incident or breach.

While most organizations can't measure pentest ROI in these concrete terms, there are several metrics organizations can use to track their pentest value or compare the effectiveness of different pentests. While cyber risk reduction can be difficult to quantify, the metrics below are useful guidelines for organizations without a mature risk management program.

- **Reduction in cyber incidents related to vulnerability exploits** — Completely avoiding incidents related to malicious hacking isn't possible — but a combination of pentest engagements should lead to incident reduction.
- **Number of vulnerabilities reported over time** — A mature pentest should expose assets to a broad and evolving range of TTPs, so vulnerabilities should continue to be reported over time, particularly for regularly updated assets.
- **Number of critical vulnerabilities reported** — A pentest that consistently finds critical vulnerabilities demonstrates a high ROI because it limits security breach risk.
- **Breadth of program coverage** — An ideal combination of pentest engagements provides coverage (and vulnerability reports) for all assets.
- **Internal effort required to manage the program** — Traditional penetration tests often require an internal coordinator. A platform avoids this resource cost by allowing direct communication between security practitioners, developers, and the testing team.
- **Ability to support development without delaying roadmaps** — Speed and flexibility are critical. Pentests that support release schedules have a high ROI, as they support business profitability.

Tracking these metrics will help organizations understand how their investment in pentesting correlates with results and see how different pentests compare.

It's Easier with a Platform

Tracking pentest metrics manually can be difficult and prone to error. HackerOne makes it easy to track metrics, export data to security tools, and correlate pentest results with other activities, e.g., product releases and updates, program scope changes, external events, etc.

Tracking pentest metrics manually can be difficult and prone to error. HackerOne makes it easy to track metrics, export data to security tools, and correlate pentest results with other activities, e.g., product releases and updates, program scope changes, and external events.

Pentesting Beyond Compliance

When working with hackers, organizations have many new pentest options. Instead of being constrained by traditional penetration tests, organizations can easily access a range of pentests to support their security and compliance needs.

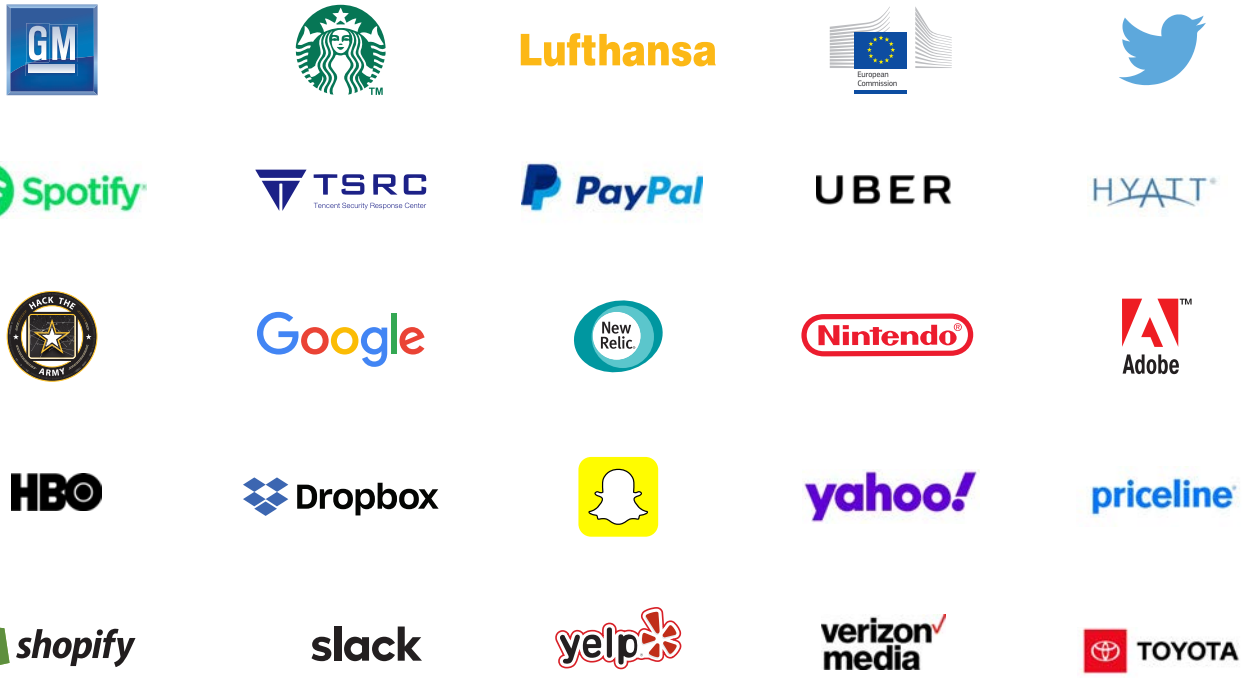
Key learning points from this buyer's guide include:

- Compliance is essential, but security and risk reduction objectives are equally important considerations when choosing a pentest provider.
- Organizations should choose a pentest provider based on their ability to support internal security, risk reduction, development, and compliance objectives.
- Some requirements may require a specific pentesting approach—but this doesn't mean all pentesting must follow the same approach.
- Due to their flexibility, speed, and breadth of testing, hacker-powered pentests can fulfill almost all pentesting use cases while providing many other benefits.
- For best results, organizations can combine different pentest engagements to achieve their full range of security objectives.
- The security and risk reduction benefits of using hackers for pentest engagements go far beyond the capabilities of traditional penetration testing.
- To maximize ROI, organizations can manage hacker-powered testing engagements through a platform like HackerOne (or outsource management to the provider).

For more information on improving pentest results and security outcomes working with hackers on security engagements, visit the HackerOne Assessments webpage.

hackerone

HackerOne has vetted hackers for hundreds of organizations including:



With over 2,000 customer programs, more companies trust HackerOne than any other vendor

Contact Us