NetSPI™

How much does penetration testing cost?

How much does a pentest cost? Short answer: It depends.

At its core, **penetration testing services** enable IT and security teams to demonstrate the efficacy of existing security controls and improve the security of networks, applications, cloud, and even physical locations. This is done by simulating the actions of a skilled threat actor to discover key areas of insecurity.

The cost of a penetration test can differ based on several variables – from pentesting methodology to the complexity of the target.

Ultimately, it begins with the requirements of each organization and the key objectives you hope to get out of your pentesting results. **Common penetration testing goals and objectives include:**

- Compliance with security testing requirements from a third-party authority, such as the **HIPAA Security Rule**, **PCI Security Standards**, or industry regulators (e.g., OCC, FDIC, FRB, State Bank Regulators – NYDFS)
- Hardening application security prior to deployment
- Managing code change
- Validation and benchmarking of existing security controls
- Support internal IT, development, and security teams
- Reducing incidents and breaches

Knowing which variables impact the cost of a penetration test will allow you to strategically allocate budget based on your cybersecurity program objectives, your organization's risk tolerance, and compliance and regulatory requirements. Our goal is to help you better understand the cost components to ensure you're paying only for what you need.

Interested in learning how to optimize your penetration testing budget? **Read our guide.**

As you evaluate your cybersecurity budget for next year, keep these six core components in mind

1. **Complexity of the test**
2. **Regulartoy compliance**
3. **Penetration testing methodology**
4. **Pentest depth and breadth**
5. **Remediation testing**
6. **Quality and expertise of pentesters**

1 The complexity of the test

It's important to consider the criticality of the environment. One with a high level of risk or critical business impact (your "crown jewels") can cost more to test due to urgency, the number of people it affects, and its role in day-to-day business operations.

Will the test require overnight testing or extensive travel? Ensure you budget for these nuances.

Multiple types of penetration testing services exist, including **network pentesting**, **application pentesting**, and **cloud pentesting** to name a few. The time, effort, and resources required for each test may differ based on the complexity of the environment and the size of the attack surface. **Here are a few examples of how complexity can influence cost:**

Application pentesting

A two-page application with one user role is less expensive to test than an application with multiple user roles and varying levels of access. **Some components that contribute to the complexity of the app include:**

- Production vs. non-production applications
- Number of dynamic and static pages (or screens)
- Number of unique API requests serving content
- Number of endpoints
- Number of user roles, type of role, and their levels of access

Cloud pentesting

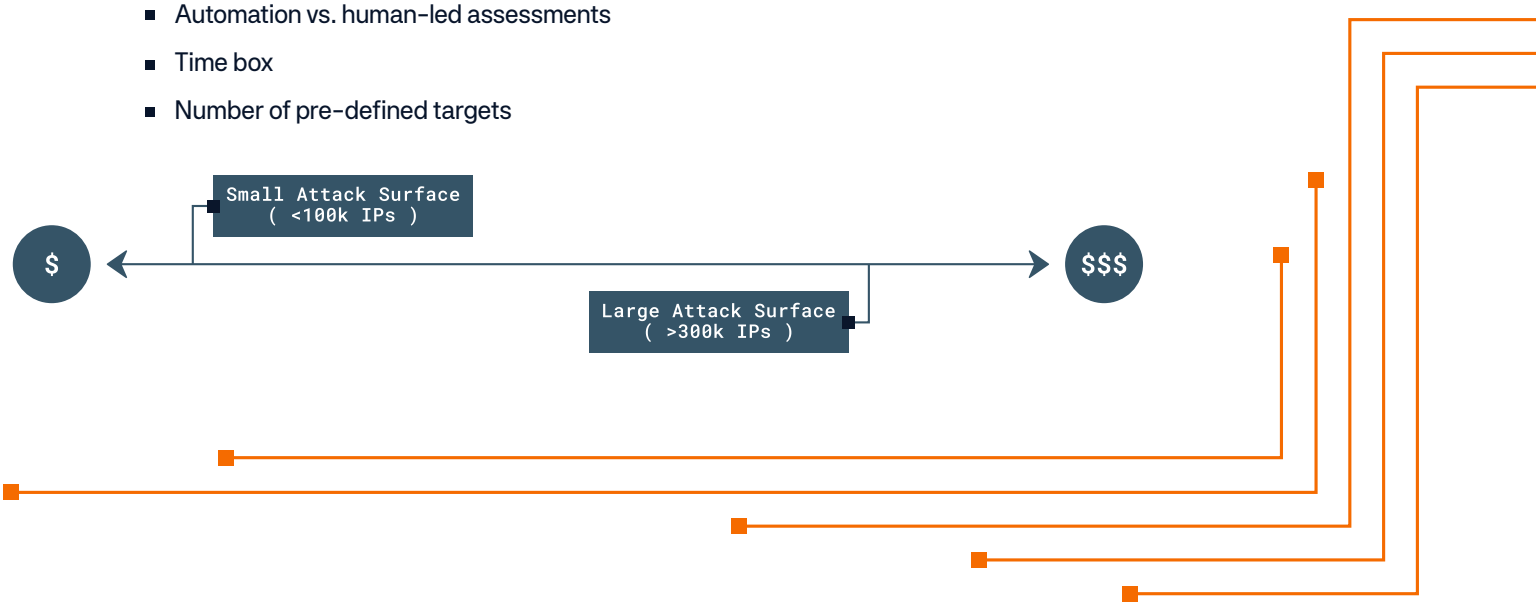
The complexity of a cloud pentest depends on how it's configured in your organization, the assets stored on the cloud, and the number of people who utilize it. **Other elements include:**

- Type of testing required (internal testing, external testing, or configuration review)
- Cloud architecture (AWS, Azure, Google Cloud)
- Number of systems and services on the cloud
- Number of tenants or business units

Social engineering pentesting

These security exercises assess a company's ability to identify and respond to real-world attack and breach scenarios in real-time. The level of complexity varies based on the type of assessment. With social engineering, assessments can range from an email phishing campaign to a full-blown on-site **physical pentest**. **Other considerations include:**

- Automation vs. human-led assessments
- Time box
- Number of pre-defined targets



2 Regulatory compliance

Compliance requirements vary across industries, geographies, and more.

The pentest requirements in the payment card industry differ from healthcare and financial institutions, governed by well-known standards such as PCI DSS, HIPAA, and FINRA, respectively. Highly regulated industries such as banks and healthcare require more in-depth and frequent pentests, while industries such as technology, higher education, and nonprofits need less extensive pentests due to fewer regulatory requirements. Geography can also influence the depth of security activities required by your local, state, and federal laws.

Additionally, customized reporting for your compliance requirements warrants more time and dedication from your team, which can also increase the cost of a pentest.

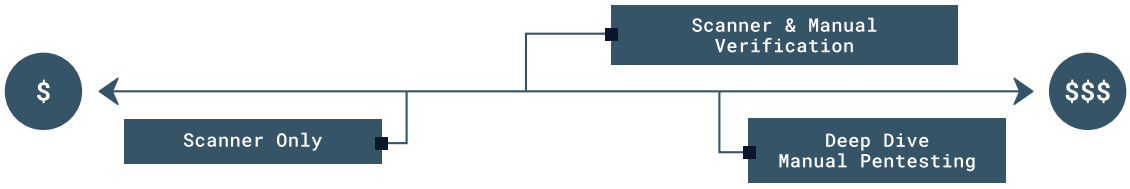
3 Penetration testing methodology

Pentesting companies and internal teams develop their own penetration testing methodology, but many are derived from the top four globally recognized frameworks: **OWASP**, **NIST**, and **MITRE ATT&CK**. These frameworks serve as a great resource due to their adaptability and level of standardization over the years.

With these frameworks as a baseline, some vendors rely entirely on automated pentesting, others manual. Others take a hybrid approach. Automated pentests yield results quickly and are typically inexpensive, but they cannot detect all vulnerabilities or chain together low-risk vulnerabilities to identify areas of weakness. They simply aggregate surface-level data, which can check the box for some organizations.

A manual pentest on the other hand can yield detailed, critical-level results and explanations but is lengthy and relies heavily on the tester assigned to your project. Each has its pros and cons, but the most strategic and cost-effective pentests utilize both.

NetSPI uses a team-based approach supported by our Proactive Security Platform. We combine automated and manual pentesting to deliver the highest quality vulnerability findings efficiently and consistently.



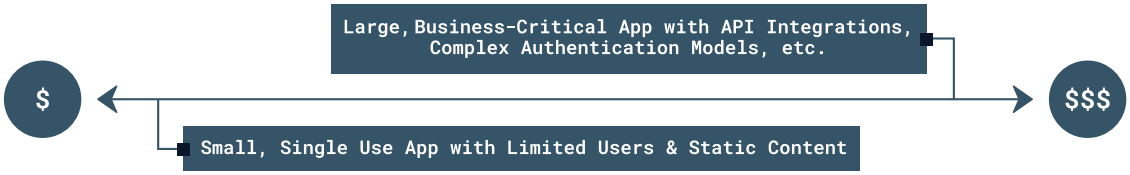
4 Pentest depth and breadth

Manual pentesting can drive up costs but provides the greatest value: uncovering business critical vulnerabilities that tools cannot. If a vendor quotes you lower than the average pentest cost of other vendors, we recommend exploring their methodology deeper to understand the depth and breadth of the pentest.

It all comes down to the depth and breadth of the checklist, methodology, and tenure of the pentester – the insights and perspectives that have been brought into that methodology and approach. A word of advice? Any pentest on a medium-sized application with multiple user roles listed at $4,000 is probably not a true penetration test.

Alternatively, consider a **source code assisted penetration test**. **A source code assisted penetration test offers many benefits:**

- More thorough results
- More comprehensive testing
- More vulnerabilities discovered
- No added cost
- Much more specific remediation guidance for identified vulnerabilities

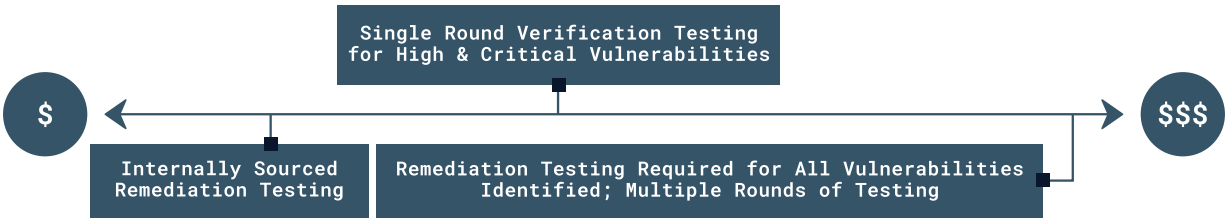


5 Remediation testing

Paying a third-party for remediation testing will cost more, but the value of retesting typically outweighs the cost. With it, you gain peace of mind that the remediation steps taken were effective and that the vulnerability does not persist. Additional remediation-related tasks that may drive costs up include in-depth remediation support and guidance.

The number of vulnerabilities being retested following remediation directly affects the penetration test cost. A word of caution: some vendors automatically bundle remediation into their pricing model for all vulnerabilities. Often, this level of remediation testing is unnecessary, given many organizations balance testing between internal and external teams. You shouldn't be charged for something you don't need.

Some firms, like **NetSPI**, have transitioned to a "pay for only what you need" a la carte approach which significantly reduces costs and ensures you do not overpay for remediation testing. You only pay for the number of vulnerabilities you need retested. If you have an in-house team validating vulnerabilities, you won't get charged for this extra step. Or if you have only a few critical vulnerabilities that surface after a pentest, you can choose to only retest and validate that the issues that pose the greatest risk to your business were resolved.



6 Quality and expertise of pentesters

When you pay for a penetration test, you pay for the quality and expertise of your pentesters.

Consider working with teams that hold industry standard certifications. For example, NetSPI is a **CREST-certified** company, known for demonstrating competency and consistency in our services. You can learn about other valuable certifications in this CSO article, **8 top penetration testing certifications employers value, including:**

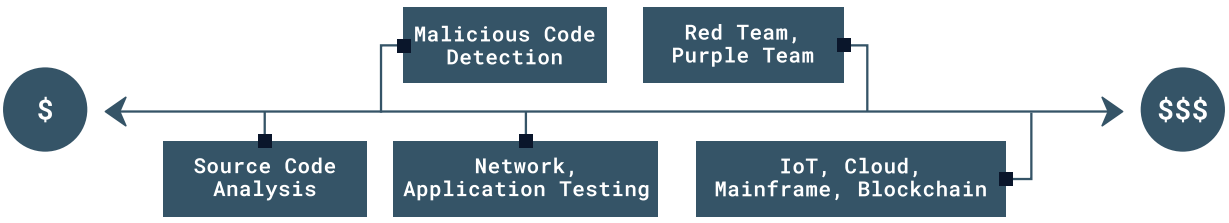
- Offensive Security Certified Professional (OSCP)
- Offensive Security Wireless Professional (OSWP)
- EC-Council Certified Ethical Hacker (CEH)
- SANS offensive security courses

Certifications alone are not enough. Like in any field, proven, hands-on experience is invaluable. An experienced partner should be familiar with the scope and type of assessment and should have experience testing similar sized organizations and industries. Less experienced or established partners may charge less.

This factor also directly correlates with the complexity of the environment being tested. Complex environments such as mainframe, IoT, etc. require more experienced pentesters.

It's important to note that choosing a penetration testing partner backed by years of experience and equipped with the necessary tools for the engagement can save you money in the long run. Experienced, quality pentesters can identify critical vulnerabilities that others miss.

Quality of pentesters, based on environment



One size pentest does not fit all

So, how much does a penetration cost? It depends.

The six factors above play a critical role in how your costs and the results you receive can change. Use these as a baseline to help you identify a solution and partner that fits your organizational priorities and cybersecurity budget.

As you evaluate your testing program and budget, you'll quickly find many providers in the space. Beyond the factors that influence the average cost of a pentest, **here are four criteria to help you choose a penetration testing partner:**

- Select an agile team. They're always improving their processes to meet the ever-changing needs of the business.
- Look for consistency: They should also have a consistent and standardized methodology built around the delivery of quality, service, and results. Your test shouldn't only be as good as the latest tester assigned.
- Select a team that spends more time on the actual testing versus the administrative tasks. Enable your pentesting team to use creative approaches to find business logic vulnerabilities.
- Decide how much external support you want or need from a remediation standpoint.
- Ask about their pentesting talent, processes, technology, and culture to ensure you're working with a team that meets your objectives.

Many factors determine the cost of a penetration test. When looking for a penetration testing partner, consider a team like NetSPI that will look out for your best interest both from a financial and risk perspective.

You deserve The NetSPI Advantage

250+ in-house security experts

Intelligent process

Advanced technology

Your proactive security partner

NetSPI is the proactive security solution used to discover, prioritize, and remediate security vulnerabilities of the highest importance. NetSPI helps its customers protect what matters most by leveraging dedicated security experts and advanced technology, including Penetration Testing as a Service (PTaaS), Attack Surface Management (ASM), and Breach and Attack Simulation (BAS).