How much does it cost for a penetration testing service?

What is the cost of a Pentest?
Short answer : It depends

The cost of a penetration test can vary depending on several factors, including the methodology used, the complexity of the target, and the organization's specific goals and objectives. Some common reasons for conducting a penetration test include

- Compliance with security testing requirements from a third-party authority, such as HIPAA Security Rule, PCI Security Standards, or industry regulators.
- Hardening application security prior to deployment,
- Validating and benchmarking existing security controls,
- Reducing incidents and breaches.
- Support internal IT, development, and security teams.

It is important to understand that the cost of a penetration test can be influenced by the specific needs and requirements of the organization. For example, a large enterprise with complex logic and systems to test may require a more extensive and complex penetration test than a small business with a single network.

Additionally, the cost may also be affected by the type of pentesting methodology used, such as black box, white box, or grey box testing. These different approaches have varying degrees of access to the target system and therefore can have an impact on the cost of the test.

Ultimately, when determining the cost of a penetration test, it is important to consider the organization's cyber security program objectives, risk tolerance, and compliance and regulatory requirements. By understanding these factors and the cost components involved, organizations can better allocate their budget and ensure they are only paying for what they need.

1 The Complexity of the Test

When assessing the cost of penetration testing, it's essential to factor in the level of risk or criticality of the environment being tested. This includes considering the urgency, number of people impacted, and its importance to day-to-day operations. Additional expenses such as overnight testing or travel should also be budgeted for. There are various types of penetration testing services available, such as application and cloud testing, and the cost can vary depending on the complexity of the environment and the size of the attack surface. Factors that can influence the cost include the complexity of the environment and the size of the attack surface.

• Application Pentesting

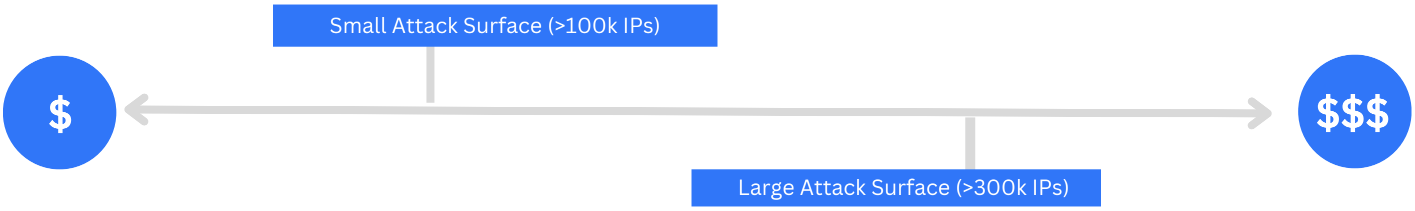
Testing the security of an application can vary in cost depending on its complexity. A simple application with a limited number of user roles and access levels is typically less expensive to test than a more complex application with multiple user roles, access levels, and various other components. Factors that can influence the cost include: whether the application is in

- production or development,
- the number of pages or screens,
- the number of API requests, the number of endpoints, and
- the number of user roles and their respective access levels.

• Cloud Pentesting

The cost of a cloud penetration test can depend on various factors such as the configuration of the cloud within an organization, the assets stored on it, and the number of users who access it. Other elements that can impact the cost include

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

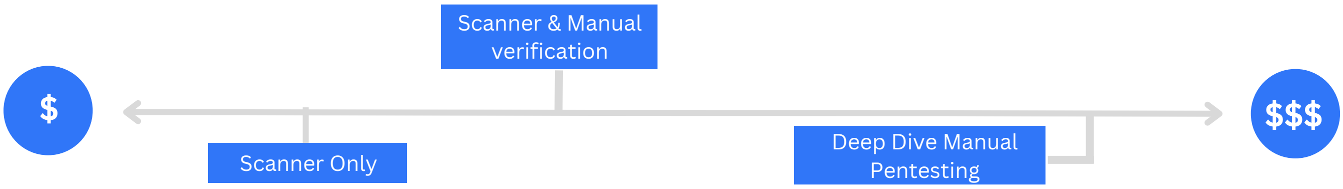

Small Attack Surface (>100k IPs)
$
$$$
Large Attack Surface (>300k IPs)

2 Regulatory Compliance

The requirements for penetration testing can vary depending on the industry, location, and other factors. Different industries have different compliance standards such as PCI DSS for the payment card industry, HIPAA for healthcare, and FINRA for financial institutions. Industries that are heavily regulated such as banking and healthcare may require more comprehensive and frequent penetration tests, while others like technology, higher education, and non-profits may require less extensive testing due to fewer regulatory requirements. The laws and regulations of a specific location can also affect the level of security activities required. Additionally, meeting custom reporting requirements for compliance can add extra time and effort to the penetration testing process, resulting in an increased cost.

3 Penetration Testing Methodology

Penetration testing companies and teams may use different methodologies, but many are based on globally recognized frameworks such as OWASP, NIST, and MITRE ATT&CK. These frameworks provide a standard level of adaptability and consistency over time. Some companies may use only automated testing, while others use manual testing, and some use a combination of both. Automated testing can produce results quickly and at a lower cost, but it may not detect all vulnerabilities or identify areas of weakness by combining low-risk vulnerabilities. Manual testing, on the other hand, can provide detailed, high-level results and explanations but is time-consuming and heavily dependent on the tester. A combination of both automated and manual testing can be the most effective and cost-efficient approach. Qualysec uses a process-based approach for Penetration testing as a service, combining automated and manual testing to provide efficient and consistent vulnerability findings.



4 Pentest Depth and Breadth

Manual penetration testing can be costly, but it provides the most comprehensive results. Identifying vulnerabilities that automated tools cannot find is crucial for protecting your business. If a vendor quotes a price that is significantly lower than others, it is important to investigate their methods to ensure they are thorough and comprehensive.

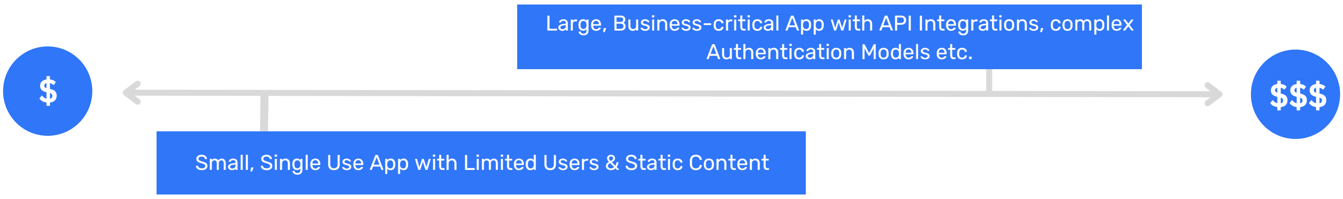
The experience and expertise of the pentester, as well as the methodology and approach used, are key factors in determining the value of a penetration test.

Keep in mind that a penetration test on a medium-sized application with multiple user roles should not be offered at a very low cost.

Instead of a traditional manual penetration test, you may want to consider a source code-assisted penetration test. This approach offers many advantages, including:

- More in-depth results
- Comprehensive testing
- Identification of more vulnerabilities
- No additional cost
- Detailed recommendations for addressing identified vulnerabilities.

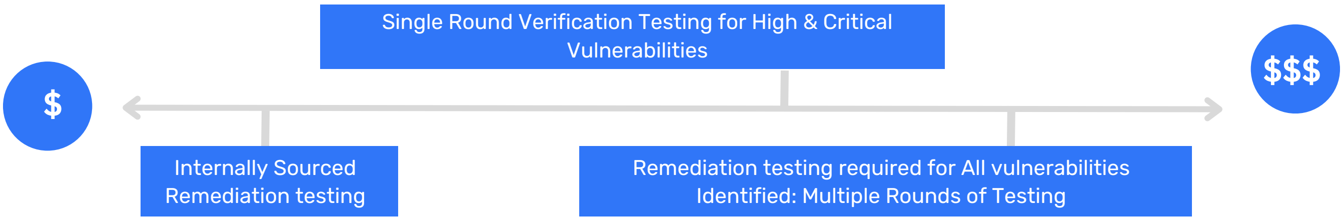
It is worth noting that a source code-assisted penetration test requires access to the source code of the application to be tested, and its results are limited to the areas of the code that are analyzed.


Large, Business-critical App with API Integrations, complex Authentication Models etc.
$
$$$
Small, Single Use App with Limited Users & Static Content

5 Remediation Testing

Hiring a third-party for retesting after remediation can be more costly, but the benefits often justify the expense. Retesting gives you confidence that the vulnerabilities have been effectively addressed and that your systems are secure. Additional tasks that may increase costs include extensive remediation support and guidance.

The cost of retesting will depend on the number of vulnerabilities that need to be re-evaluated. Some vendors may include remediation testing in their pricing for all vulnerabilities, but this may not be necessary for all organizations and can add unnecessary costs. It's important to select a vendor who offers a flexible pricing model that allows you to pay only for the retesting that you need. Qualysec and other firms offer this type of "pay-as-you-go" service which can significantly reduce costs and ensure that you are not overcharged for retesting. If you have an in-house team that can validate vulnerabilities, you can avoid paying for additional retesting that may not be needed. You can also choose to focus on retesting only the vulnerabilities that pose the greatest risk to your organization, which is a cost-effective way of ensuring that your systems are secure.

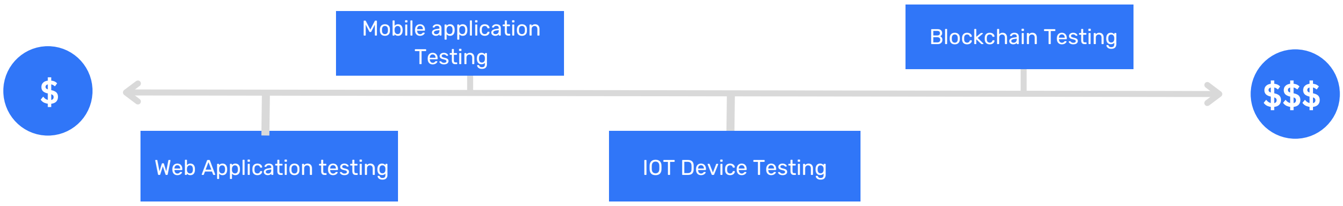

Single Round Verification Testing for High & Critical Vulnerabilities
$
$$$
Internally Sourced Remediation testing
Remediation testing required for All vulnerabilities Identified: Multiple Rounds of Testing

6 Quality and Expertise of Pentesters

When paying for a penetration test, you are paying for the skill and expertise of the testers. It is a good idea to work with teams that hold industry-standard certifications, such as

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

However, it is important to remember that certifications alone are not enough. The hands-on experience of the testers is also crucial. An experienced testing partner should be familiar with the scope and type of assessment and should have experience testing similar-sized organizations and industries. Less experienced or new partners may charge less but may not have the knowledge and experience to identify all the vulnerabilities. The complexity of the environment being tested also plays a role in this. Complex systems such as mainframes and IoT devices require more experienced testers. In the long run, choosing a well-established and experienced penetration testing partner with the right tools can save you money by identifying vulnerabilities that others might miss.



One Size Pentest Does Not Fit All

The cost of a penetration test can vary widely depending on a variety of factors such as the size and complexity of the organization, the scope of the test, and the level of expertise of the testers. To determine the right solution and partner for your organization, it's important to take into account the factors that influence the average cost of a pentest and align them with your organizational priorities and cybersecurity budget. When evaluating different providers, there are four key criteria to consider to help you choose the right penetration testing partner:

- Choose an agile team that is constantly improving its processes to meet the evolving needs of the business.
- Look for consistency in terms of methodology and delivery of quality, service, and results.
- Select a team that focuses more on the actual testing and less on administrative tasks. This allows them to use creative approaches to find business logic vulnerabilities.
- Decide how much external support you need or want for remediation.
- Ask about the pentester's processes, technology, and culture to ensure that they align with your objectives.

It's worth noting that it's important to evaluate the provider and ensure they have a good reputation and experience in the industry. Also, try to have a clear understanding of their process and the deliverables they will provide.

The cost of a penetration test can vary based on factors like organization size, the scope of the test, and tester expertise. When selecting a partner, look for a provider like Qualysec that considers your priorities and budget while also assessing risk.