

Penetration testing

Pros and cons of five common methods

1 Traditional penetration testing

The ‘traditional’ model comprises one or two testers working against a set methodology for a defined period, usually anywhere from three days to two weeks. This format is a mainstay of the security industry, and executives and business leaders are pre-sold on the need for it.

Pros

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

Cons

- ✗ Delays to scheduling and results
- ✗ Inflexible with questionable skill fit
- ✗ Not optimized to incentivize true risk reduction

2 Penetration testing as a service

Crowdsourced options utilize a large pool of remote, pay-per-project testers. Often combined with an incentivized ‘pay for results’ approach to billing, crowdsourced testing is quickly becoming the top choice for organizations seeking more from their security testing services.

Pros

- ✓ Rapid setup and time to value
- ✓ Real-time results and SDLC integration
- ✓ Option to ‘pay for results’ instead of time

Cons

- ✗ Not optimized for highly sensitive or physical targets too big to ship
- ✗ ‘Bounty’ approach may not fit buying cycles
- ✗ New business case may be required

3 Internal security testing

While often not feasible for smaller organizations, some enterprises prefer to build and maintain in-house teams of security testers. This approach allows the organization to set its own testing schedule and may reduce barriers in some areas (e.g., provision of credentials).

Pros

- ✓ Best for extremely sensitive work (e.g., Secret, NOFORN)
- ✓ Tests can be run as frequently as needed
- ✓ Little marginal cost to testing

Cons

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

4 Agentic pen testing

Agentic pen testing uses AI agents to autonomously simulate attacks against web applications and APIs. Where a vulnerability scanner tells you something might be wrong, agentic testing confirms whether it’s actually exploitable.

Pros

- ✓ Tests entire attack surfaces at a fraction of the cost of manual testing
- ✓ Delivers results in minutes or hours rather than days or weeks
- ✓ Provides evidence of exploitability, not just potential vulnerability flags
- ✓ Runs on demand with no scheduling lag
- ✓ Consistent and repeatable coverage across all assets

Cons

- ✗ Not suited for complex business logic flaws, exploit chaining, or zero-days
- ✗ May not meet auditor requirements for some controls (e.g., PCI-DSS) on their own
- ✗ Requires human-led testing for high-stakes, regulated, or sensitive targets
- ✗ A newer category with evolving methodology and compliance recognition
- ✗ Effectiveness depends on scope quality and asset inventory accuracy

5 A mixed testing approach

Some organizations use a combination of all methods to meet the specific needs of each project.

Pros

- ✓ Includes the best aspects of each method
- ✓ Potential for thorough security coverage
- ✓ Testing depth is as-needed for each project

Cons

- ✗ Includes the worst aspects of each method
- ✗ Complex to arrange and maintain
- ✗ (Potentially) extremely high-cos

Making the best decision

Wherever you’re at in your pen testing journey, Bugcrowd can help. Check out the *Ultimate Guide to Penetration Testing: The Rise of Agentic AI* to learn more.