bugcrowd

2020 ULTIMATE GUIDE TO

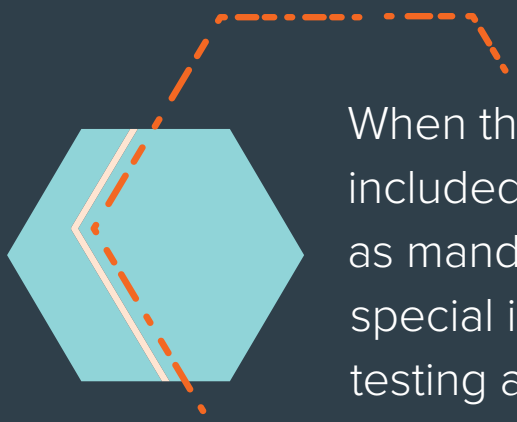
Penetration Testing

YOUR GUIDE TO CHANGES IN THE INDUSTRY,
AND WHAT'S COMING NEXT

TABLE OF CONTENTS

INTRODUCTION

Penetration testing started in the ’90s as adversary simulation. Its job wasn't to find every security flaw, it was to identify vulnerabilities that a malicious actor would likely be able to exploit. As a result, the practice was quickly adopted by a variety of compliance initiatives designed to assure regulators and other stakeholders that an organization took the ever-evolving threat landscape seriously.



When the PCI-DSS standard launched in 2006, it included penetration testing and vulnerability scanning as mandatory controls. In 2008, they published a special interest group paper that defined penetration testing as: "a vulnerability scan with manual confirmation of exploitability." This led to an explosion of scanner-assisted services where, due to strained resources, human testers played an incrementally smaller role. This over-reliance on technology was felt keenly, as testing services did an increasingly poor job of identifying new, complex threats, while margins rose significantly over time.

While the practical value of attack simulation hasn’t waned, deficiencies in the way these programs are deployed have caused many security leaders to view penetration tests as a ‘necessary evil’. They know serious vulnerabilities are often missed, but they also know that penetration testing addresses established business needs, such as compliance with PCI-DSS, HIPAA, SOC 2, and other frameworks.

WHEN RISK OVERTAKES COMPLIANCE

As recently as 2016, 34% of C-level executives were never updated about cybersecurity, while 23% were updated annually. Today, just four years later, cybersecurity is firmly established at the boardroom table.

Where previously many executives viewed the function purely as a cost center, cybersecurity's relatively recent ability to influence the financial decisions of customers, partners, and investors has elevated its status amongst the C-suite.

What changed? High-profile breaches like those of Target, Equifax, and Marriott made security tangible to even the least tech-savvy executives. And at the same time, increasingly large fines from regulators made it clear that simply complying with industry frameworks wasn't enough to keep an organization safe from cyber attacks.

Today's high regard for cybersecurity has placed traditional penetration testing in the crosshairs. Where previously these services were considered essential for a strong security program, the current method for resourcing and deploying them has failed to keep up with the evolution of the modern attack surface. After all, how could 1-2 penetration testers accurately mimic the activity of the entire global cybercriminal community in just a couple of weeks?

THIS REPORT EXAMINES

Why compliance is no longer the #1 reason for security testing, and what other factors play a role.

Eight major issues with traditional penetration testing, and what they mean for security teams.

The testing options available to modern organizations, plus their pros and cons.

What the results of a recent Bugcrowd survey tell us about the state of penetration testing in 2020.

How the next generation of penetration testing is addressing the shortcomings of traditional services.

1 Ponemon, 2016, The State of Malware Detection & Prevention.
2 DLA Piper Global Law Firm, 2020, GDPR Data Breach Survey

WHY PENETRATION TEST?

In the past, many organizations used penetration testing primarily as a tool to achieve compliance. However, as cybersecurity programs have evolved, they have become more risk-based.

Most industry professionals understand compliance is just one of many key security objectives. And that satisfying a compliance framework, while essential, does little to ensure the security of the organization. They know this, because while practically every organization can evidence compliance, a staggering proportion (as high as 61%) experience at least one compromise each year.

In 2020, there are five primary reasons why organizations continue to invest in penetration testing:

PROTECT THE ORGANIZATION AND ITS ASSETS

Cyber attacks pose a serious — even existential — threat, and any digital asset is a potential target. Penetration testing is used to identify vulnerabilities in websites, applications, and other digital systems before they can be exploited by an attacker.

PROTECT CUSTOMER DATA

Customer data is among the most important assets an organization has. Its possession is heavily regulated. Any breach of customer data is potentially devastating, as it can lead to heavy fines from industry regulators — not to mention a loss of customer trust. Penetration testing is used to find and close vulnerabilities that could otherwise be used to gain unauthorized access to customer data.

REDUCE CYBER RISK

Once a vague concept, cyber risk is now a clearly calculable factor. Using tools like the Threat Category Risk framework , it can be clearly articulated as a dollar value. For organizations with a mature cybersecurity function, managing cyber risk is the #1 priority in cyber defense, and penetration testing is a critical component.

SATISFY STAKEHOLDER REQUIREMENTS

Customers, suppliers, shareholders, and other stakeholders have a huge influence on the decisions an organization makes. As concepts like supply chain risk have become more widely understood, key stakeholders have increasingly demanded close attention to cyber risk management. Penetration testing plays a crucial role in this area.

PRESERVE THE ORGANIZATION'S IMAGE AND REPUTATION

Cyber incidents can fundamentally harm an organization's ability to operate by undermining customer trust in its products, services, and brands. A major motivation for investment in penetration testing is to preserve customer trust by avoiding high-profile incidents.

3 Hiscox, 2019, Cyber Readiness Report 2019.
4 Hubbard Research, 2019, How To Measure Anything in Cybersecurity Risk.

WHY TRADITIONAL PENETRATION TESTS AREN'T FIT FOR PURPOSE

To be clear, there is a huge distinction between penetration testers — the experts who use their skills to identify security vulnerabilities — and the model through which they are deployed.

Penetration testers are an incredible resource. If they could, every organization would have dozens of penetration testers working full-time to identify vulnerabilities in its digital assets. However, this approach is cost-prohibitive and logistically impossible. There simply aren't enough penetration testers in the industry, leaving the market to 'make do' with a method for resourcing talent that seriously constrains outcomes.

Traditional penetration tests are based on standard industry guidance produced by organizations like OWASP and CIS, and are heavily influenced by the major compliance frameworks. As a result, while they can be relied on to find vulnerabilities that fall into standard categories, they are likely to miss more complex and potentially damaging issues.

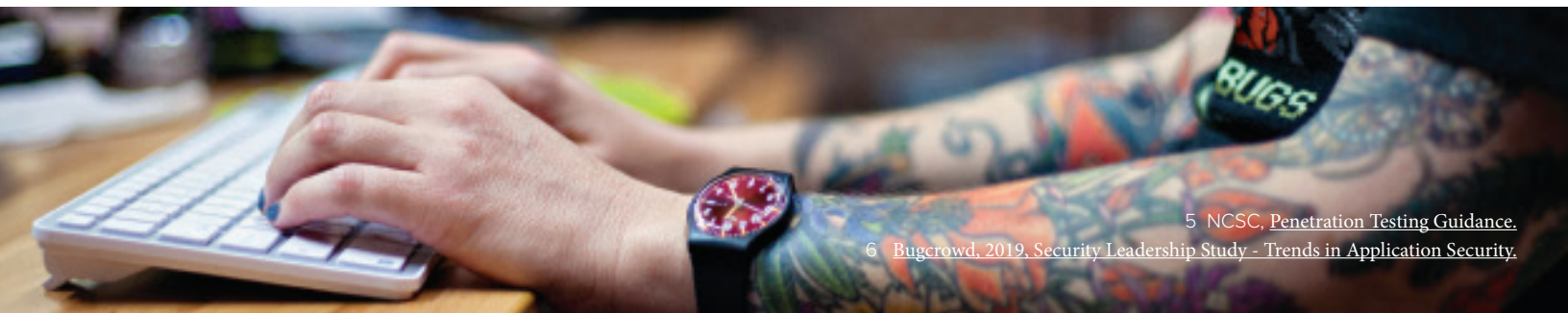
In recognition of this, the UK's National Cyber Security Centre actually advises organizations that:

> "You should know what the penetration testers are going to find, before they find it. [...] use third-party tests to verify your own expectations. Highly experienced penetration testers may find subtle issues which your internal processes have not picked up, but this should be the exception, not the rule."

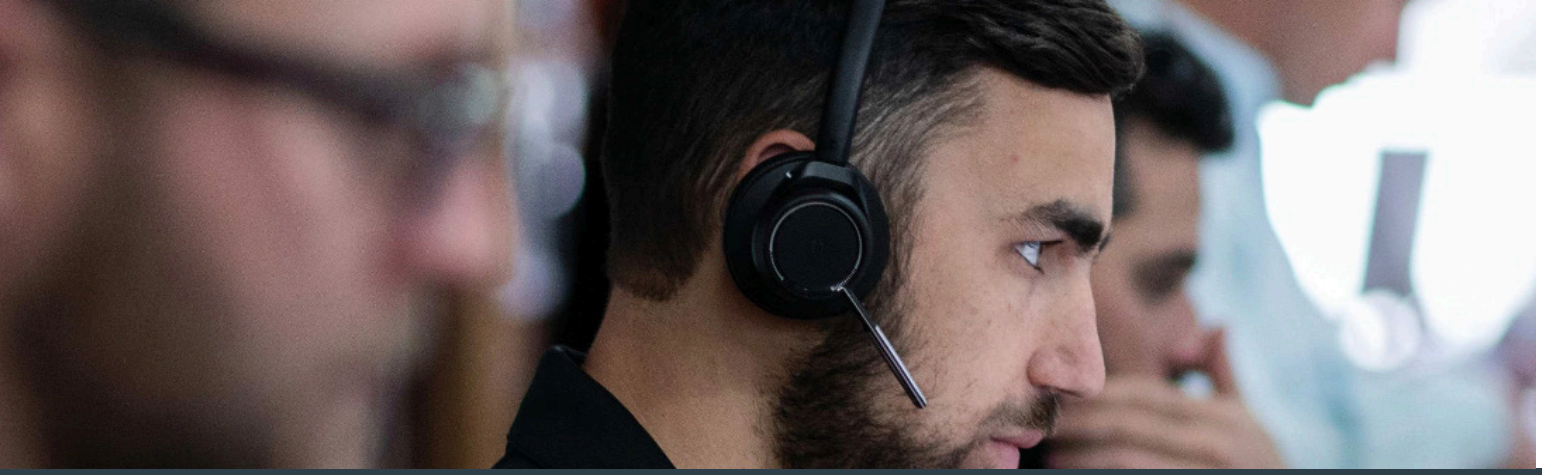
Clearly, this doesn't suggest high confidence in the effectiveness of traditional penetration testing.

Even (and especially) penetration tests conducted by industry leaders and global consulting providers leave much to be desired from a security perspective. Utilization targets often lead to a skills mismatch, as testers are assigned to a project based purely on availability. This inevitably leads to over-reliance on automated scanners, and a dogmatic adherence to standard methodologies.

It's hardly surprising, then, that a 2018 Bugcrowd survey of 200 cybersecurity leaders found 56% were dissatisfied with their current penetration tests. Since then, the traditional penetration testing model has only become less effective as a tool for promoting security and managing cyber risk. And here's why:



5 NCSC, Penetration Testing Guidance.
6 Bugcrowd, 2019, Security Leadership Study - Trends in Application Security.



GAPS IN THE CURRENT PENTESTING MODEL

SCHEDULING DELAYS

Organizations are frequently forced to accept long wait times (up to months) for each testing period. As penetration testing providers aim to reduce time on the 'bench' for salaried employees, getting resources where and when needed is a constant challenge.

TESTS ARE DIFFICULT TO EXTEND

In theory, a testing window can be extended if early findings indicate a need to dig deeper. However, this is often logistically impossible as penetration testing providers are routinely booked for back-to-back engagements.

INCOMPATIBLE INCENTIVES

The provider's need to reduce overheads can lead to the assignment of testers who aren't suited to the engagement at hand. Often, the only thing protecting customers from the 'caveat emptor' nature of this model is the provider's desire to win the renewal the following year.

SPEED OF RESULTS

With a standard penetration test, the customer doesn't receive results until the engagement is concluded, often 14-24 days after testing begins. This leaves tested assets vulnerable for an unnecessarily long time.

QUESTIONABLE SKILL FIT

A typical penetration test is carried out by 1-2 testers over a period of two weeks. Regardless of how experienced the testers are, they can't be versed in every possible attack technique, and their skill sets may not be appropriate to the asset being tested. Equally, customers don't have the option to select which testers are assigned to their projects.

CHECKLIST FOCUSED

Most penetration tests are checklist-based, with minimal time or incentive for testers to use their initiative or 'dig deeper' to find complex vulnerabilities.

POINT-IN-TIME TESTING

Most digital assets are penetration tested a maximum of 1-2 times per year. With modern, agile development lifecycles, new codebase versions are released much more frequently. While an asset may be secure immediately following a test, new code releases could leave it vulnerable to attack until the next scheduled test.

LACK OF INCENTIVE

Traditional penetration testing providers operate a 'pay for time' business model, where customers pay for a certain number of hours, and the assigned tester is only required to finish the methodology in that time. Number and severity of vulnerabilities surfaced during this time is irrelevant to the tester's final pay.

LACK OF SDLC INTEGRATION

Traditional penetration tests aren't constructed in a way that actively integrates security and development teams. Developers must manually migrate vulnerabilities to their preferred workspace (e.g., JIRA or ServiceNow) before 'sifting through' a long report lacking context, priority, and guidance on how to resolve vulnerabilities safely.

POOR RESULTS

In a typical report from a traditional penetration test provider, valid findings are interspersed with false positives and no-risk issues, making them hard to identify and resolve. Worse, due to a compliance-centric focus and reliance on automated scanners, many genuine high-risk vulnerabilities are simply not identified.

Due to poor results, high cost, and time delays, traditional penetration testing services are **not a cost effective security control.** Worse, because skill fit for a project is likely sub-optimal and testers aren't incentivized to 'go deep,' it's likely that genuine, high-risk vulnerabilities will be missed.

Given this, the traditional penetration testing model is simply **ineffective for Cyber Risk Management.**

PENETRATION TESTING: WHAT ARE THE OPTIONS?

While there are a number of different penetration testing methodologies that vary by target type, compliance initiative, and more, there are **four** primary methods for deploying services generally.

TRADITIONAL PENETRATION TESTING

Many organizations still rely on traditional penetration testing services, often as a result of budgetary or procurement constraints. 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
- Best suited to targets that require physical presence to access/test

CONS

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

CROWDSOURCED SECURITY PENETRATION TESTING

The crowdsourced penetration test is a comparatively new method of testing. 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

INTERNAL SECURITY TESTING

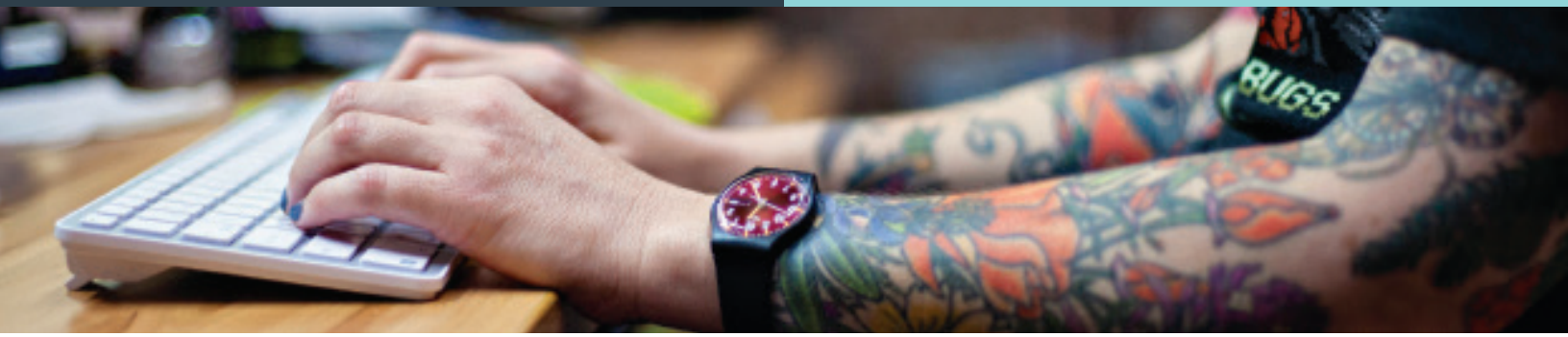
While often not feasible for smaller organizations, some enterprises prefer to build and maintain in-house teams of security testers. This approach allows the organization to set its own testing schedule, and may reduce barriers in some areas, e.g., provision of credentials.

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



A MIXED TESTING APPROACH

Some organizations use a combination of traditional, crowdsourced, and internal testing 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-cost

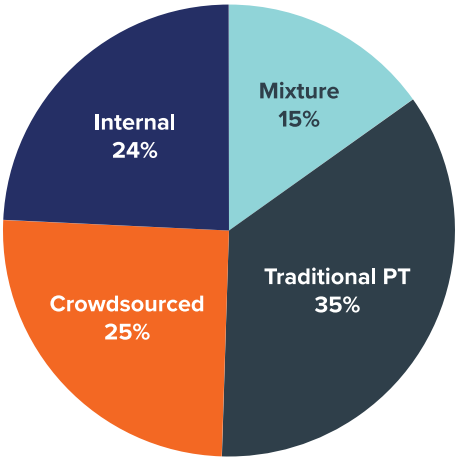
THE 2020 STATE OF PENETRATION TESTING

In March 2020, we surveyed 129 cybersecurity engineers, managers, and CISOs to find out how they conduct their penetration testing. All of our respondents had influence over their organization's security testing budget, methodology, and scope. Here's what we learned:

COMPLIANCE IS NO LONGER THE #1 REASON FOR TESTING.

While 55% of respondents cited compliance as *one* of their reasons for testing, only 16% test *purely* for compliance purposes. Meanwhile, 61% of respondents cited best practice as a reason for testing, and 38% cited stakeholder requirements.

TRADITIONAL PENETRATION TESTING SERVICES ARE STILL #1...JUST.



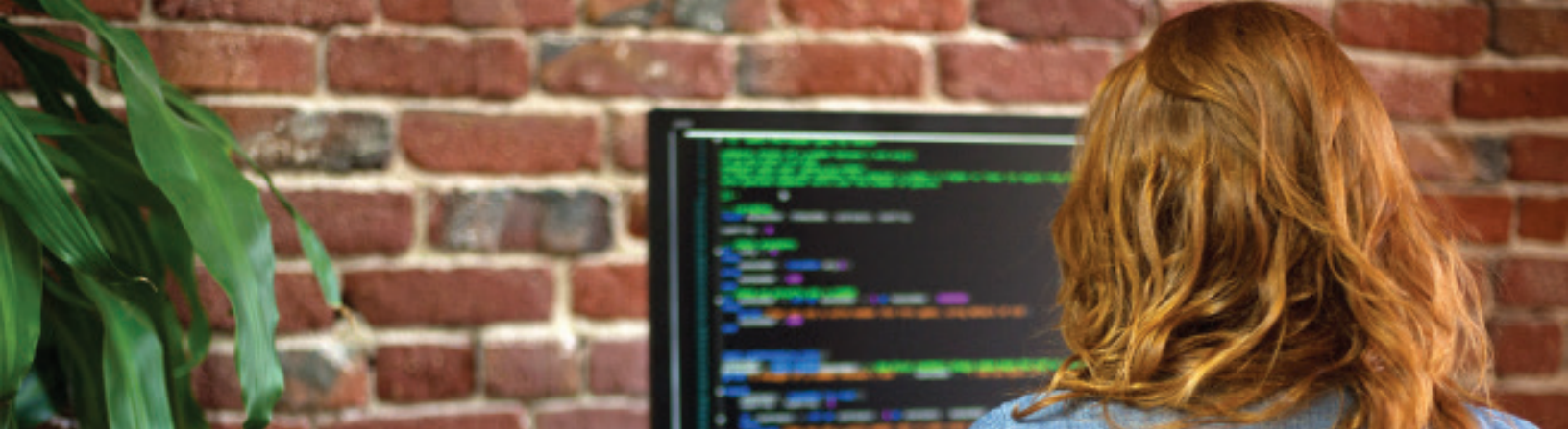
In the past, traditional penetration testing was a dominant force in security. However, recently, other approaches have gained popularity. Our survey shows that in 2020, across all industries and organization sizes, traditional penetration testing services account for just 35% of security testing.

Crowdsourced testing has jumped into second place at 25%, despite being around for a comparatively short time. 24% of organizations complete most of their testing internally, while 15% use a mixture of testing approaches.

LARGER ORGANIZATIONS ARE MOVING AWAY FROM TRADITIONAL PENETRATION TESTING SERVICES.

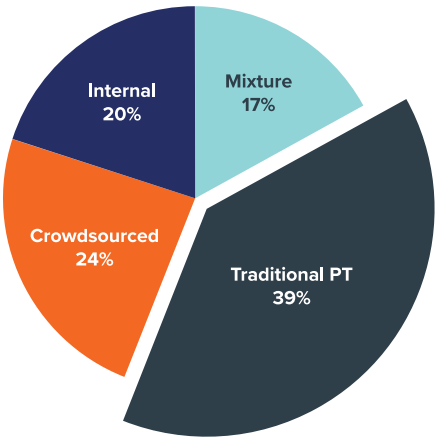
While other options are catching up, traditional penetration testing is the most common testing method among small organizations with under 1,000 employees. For larger organizations — where increased budgets open up more options — things are less clear.

Traditional penetration testing and crowdsourced testing are both utilized by just under a third of organizations with 1-10k employees. Considering that crowdsourced testing is a far more recent option, this highlights a rapid movement away from traditional penetration testing services.

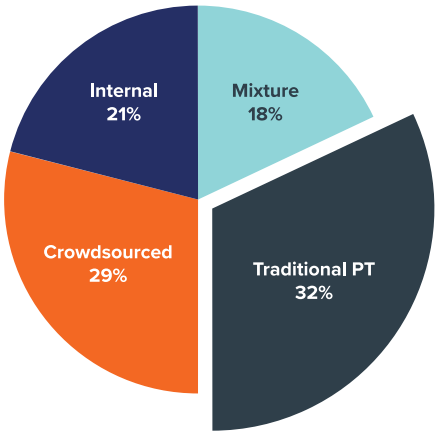


At the enterprise level (10K + employees) the percentage of organizations relying on traditional penetration testing services is barely *half* the rate we see in small organizations (21% vs. 39%). It's also dead equal with the percentage of enterprises using crowdsourced testing. Meanwhile, more than half (57%) of enterprises rely primarily on internal security testing.

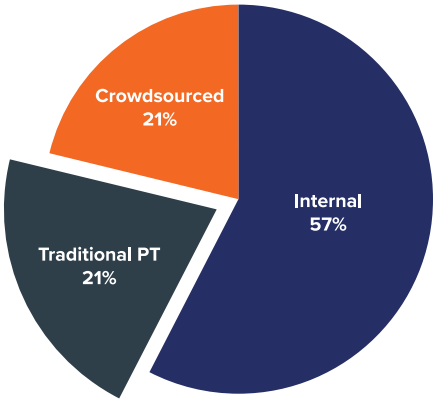
ORG SIZE: <1K



ORG SIZE: 1-10K



ORG SIZE: 10K+



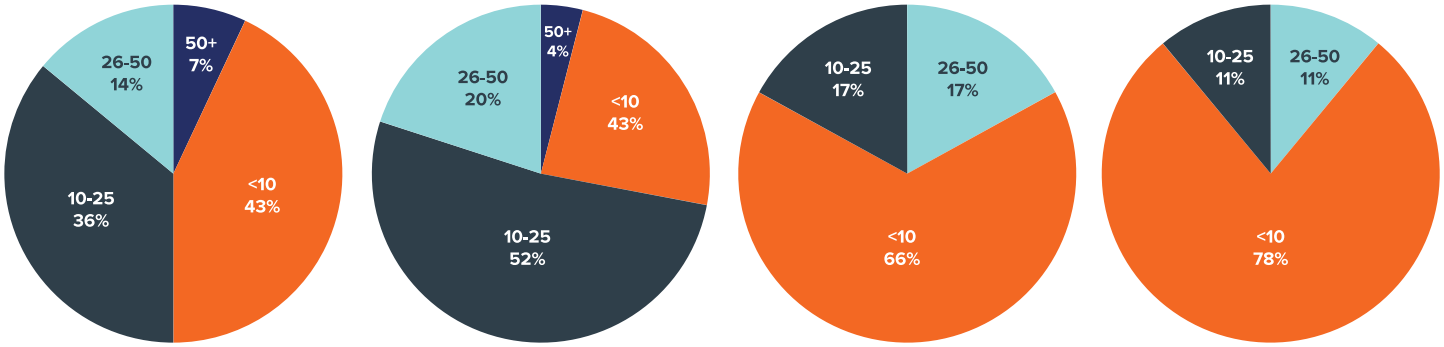
CROWDSOURCED TESTING FINDS MORE, HIGHER-VALUE VULNERABILITIES.

When it comes to results, crowdsourced testing is the clear winner. 76% of crowdsourced testers received at least 10 vulnerabilities per two-week test, compared to 57% of traditional penetration testing services.

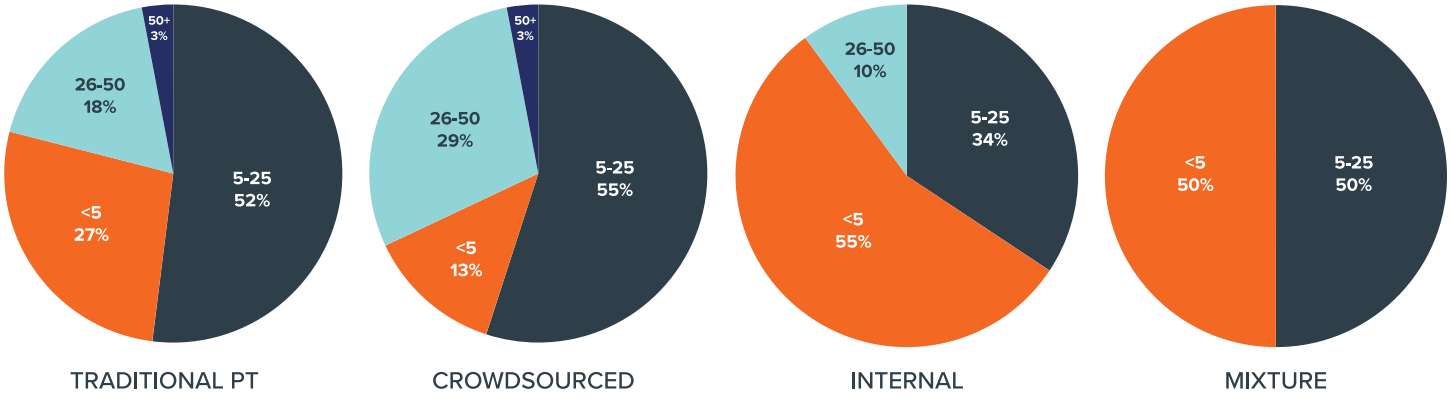
The quality of results was also higher. Only a small fraction (13%) of crowdsourced testers received less than 5% high-value vulnerabilities, while traditional penetration testing services were *twice* as likely to deliver a poor result. Meanwhile, crowdsourced testing was 60% more likely than traditional penetration testing services to deliver a large proportion (26%+) of high-value vulnerabilities.

Internal testing programs performed extremely poorly on both the quality and quantity of results, despite their popularity with enterprises.

VULNS FOUND/TWO-WEEK TEST



% VULNS THAT ARE HIGH-VALUE



TRADITIONAL PENETRATION TESTING IS FAVORED BY INFREQUENT TESTERS.

66% of organizations that use traditional penetration testing services test *very infrequently* — once per year or less. By contrast, over half (52%) of organizations that use crowdsourced testing test at least quarterly. Organizations that test internally are the most frequent testers, with 60% testing at least quarterly.

COSTS ARE COMPARABLE, BUT ROI ISN'T.

Our respondents placed traditional penetration testing neck-and-neck with crowdsourced testing on total cost. However, since crowdsourced delivers more, higher-quality results, it's a clear winner for ROI.

While the cost of maintaining an internal testing capability varies, there's no question that it falls beyond what most organizations can afford. And, given its poor results, the ROI is questionable at best.

WHAT CAN WE LEARN FROM THIS?

Larger organizations recognize the issues with traditional penetration testing services... but haven't chosen the best alternative. Internal testing performs poorly on the number and quality of vulnerabilities found.

Crowdsourced testing finds more and higher-value vulnerabilities than traditional penetration testing services, internal security testing, and mixed programs.

Crowdsourced testing offers higher ROI than other methods, as costs remain comparable while results are consistently better.

WHAT'S NEXT FOR SECURITY TESTING?

Traditional penetration tests don't meet the needs of modern organizations. A different solution is needed.

Crowdsourced testing approaches such as bug bounty programs have addressed many of the shortcomings of traditional penetration tests. By operating on a pay-for-findings model, these programs harness the power of the global hacking community to provide on-demand access to the expertise needed for each engagement.

However, bug bounty programs haven't fully replaced the need for standardized testing. Compliance is still a crucial part of security, and most frameworks demand that testing follows a recognized methodology.

THE NEXT GENERATION PENETRATION TEST

While many organizations share a need for compliance, not all have the same testing requirements or capacity. Some seek continuous coverage, to match increasingly rapid development cycles. Others need shorter testing windows throughout the year, as dictated by engineering workflows or budgetary and procurement cycles. Equally, an organization's appetite for tester incentivization may be shaped by its bandwidth to address vulnerabilities and ability to maintain an elastic pool of monetary rewards.

To address these varied needs, Bugcrowd has launched the next generation of penetration testing. One that taps into the diverse expertise of the global hacking community, while providing methodology-based coverage and essential compliance reporting. And vitally, one where the **customer** chooses the terms.

CROWD-POWERED PENETRATION TESTING

'NEXT GENERATION' PENETRATION TEST

- Continuous coverage *and* on-demand methodology-driven testing
- Testers incentivized through rewards for valid vulnerabilities
- Re-testing of fixed vulnerabilities
- Premium SLAs and Coverage Analysis

Cost: Platform + incentive pool

'CLASSIC' PENETRATION TEST

- On-demand methodology-driven testing
- Testing completed over a defined period based on project scope
- Options for re-testing, expedited reporting, and rare skills

Cost: Per-test, no incentive pool

BOTH

- QSA-ASSESSED COMPLIANCE REPORT: Helps meet PCI-DSS, NIST 800-53 rev4, ISO 27001 etc.
- SET UP IN <72HRS ON AVERAGE: Avoid lengthy scheduling delays waiting for the right resources
- STREAMING RESULTS: View vulnerabilities as they are submitted, directly in-platform
- SDLC INTEGRATIONS: Connect to developer workflows, e.g., GitHub and ServiceNow
- REMEDIATION ADVICE: Help dev fix quickly with prescriptive instructions by vulnerability type
- CROWDMATCH™: Draw from the largest pool of talent; ensure skills match project needs.
- ON-DEMAND IN-PLATFORM REPORTING: Monitor vulnerability status and program activity
- FULLY MANAGED: Bugcrowd handles pentester matching, activation, and remuneration, as well as vulnerability triage and prioritization

HARNESSING THE CROWD

Harnessing the power of the global hacking community requires structure, process, and deep experience in human-to-human interaction. All Bugcrowd's crowd-powered penetration tests utilize the Bugcrowd security platform, which provides dedicated program management.

This combination of technology-enabled expertise enables us to provide:

Thorough vetting and expert skills-matching of every crowdsourced penetration tester.

Rapid triage, validation, and risk-ranking of all discovered vulnerabilities.

Numerous software development integrations for faster remediation.

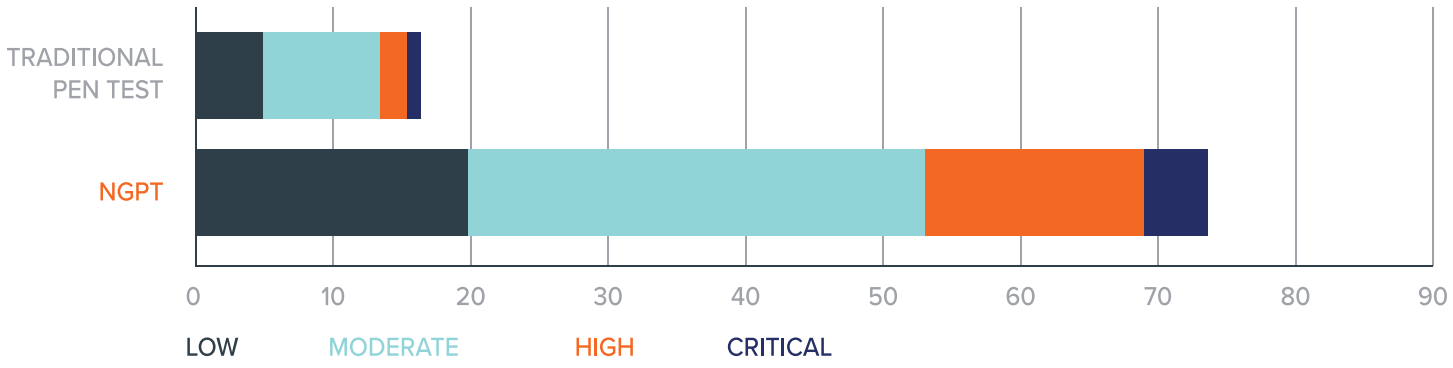
Rapid time to value as results are streamed immediately post-validation (rather than at program end).

Full program onboarding, clearly defined SLAs, and dispute resolution.

Full, real-time visibility into team activity, program outcomes, and costs.

Combined, these factors enable crowd-powered penetration tests to identify on average 7X more high-priority vulnerabilities than traditional penetration tests.

NEXT GEN PEN TESTS FIND 7X MORE HIGH PRIORITY VULNERABILITIES

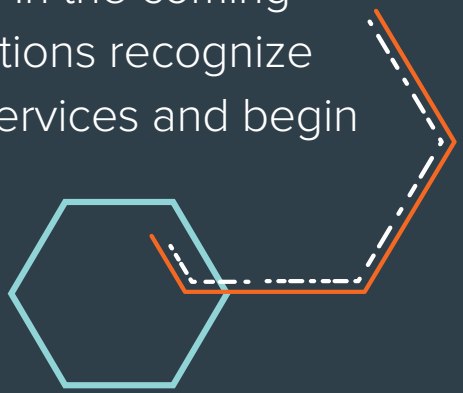


THE END OF AN ERA

Once the gold standard for cybersecurity, traditional penetration testing now falls far short of what's needed by a modern organization. From cost, to time, to quality of results, these services are not an effective tool for improving security outcomes or managing cyber risk. With the emergence of alternative methods, a compliance report alone no longer justifies the opportunity cost of a test that fails to deliver real results.

Penetration testing providers must evolve to both satisfy compliance requirements and provide deep security insights. Modern, agile development lifecycles have highlighted the inability of traditional providers to deliver penetration testing in a way that is both functional and cost-effective. A new model is required. By drawing on an elastic, fully-managed network of premium testing talent, crowdsourced security platforms offer organizations a faster path to compliance without sacrificing the critical insights that help keep products and customers safe.

In 2020, crowdsourced security testing has already caught up with traditional penetration testing services in the enterprise market, and is rapidly closing the gap with smaller organizations. In the coming years, this trend will only continue as more organizations recognize the shortcomings of traditional penetration testing services and begin to evaluate their options.



KEY TAKEAWAYS

PENTESTING FOR COMPLIANCE ALLONE DOESN'T CUT IT.

Modern organizations have to balance compliance with other needs, including customer and stakeholder requirements, financial concerns, and cyber risk management.

ORGANIZATIONS ARE NOW RELYING ON ALTERNATIVE METHODS FOR PENETRATION TESTING.

To fill the gaps left by traditional testing services, modern organizations have begun incorporating other methods where appropriate, for example, crowdsourced testing, internal testing, and hybrid testing programs.

CROWDSOURCED TESTING DELIVERS MORE AND HIGHER QUALITY VULNERABILITIES.

Users of crowdsourced security programs benefit from expert skills matching, and those who provide further incentives for valid vulnerabilities report a greater volume of higher-quality vulnerabilities than traditional penetration testing services provide.

TRADITIONAL PENETRATION TESTING SERVICES ARE LOSING POPULARITY.

Traditional services are just barely holding the top spot, while organizations are increasingly incorporating or switching to crowdsourced methods.

CROWDSOURCED PENETRATION TESTING IS GAINING TRACTION WITH ORGANIZATIONS OF ALL SIZES.

Crowdsourced programs now account for between 20 - 30% of all security testing, depending on organization size.