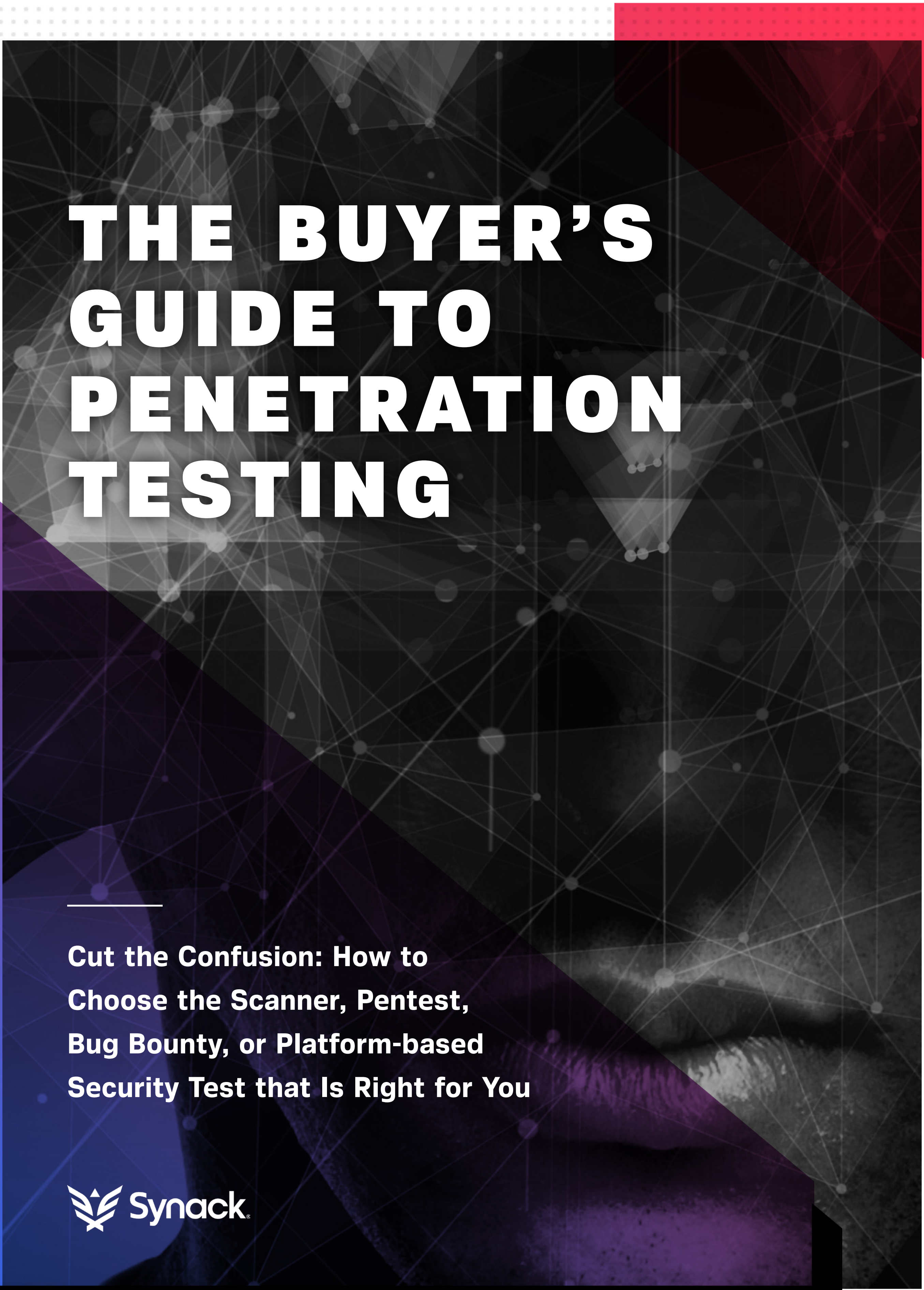


THE BUYER'S GUIDE TO PENETRATION TESTING

Cut the Confusion: How to Choose the Scanner, Pentest, Bug Bounty, or Platform-based Security Test that Is Right for You

Synack

Table of Contents

Breaches are all too common today as determined cyber criminals have become better organized and more targeted in their attacks. In many cases, a C-level executive loses their job as a result. That doesn't have to be you—or your organization.

The right testing solution is key to keeping you safe. While searching for the one that's the best fit for your organization, be sure to prioritize your goals. Are you seeking holistic security to mitigate the chance of a breach? Are you focused solely on compliance? Is there a customer or partner insisting that you get a checkup? Are you looking for a point-in-time test or for continuous security as your network and applications evolve?

Remembering those objectives as you navigate this guide will help maximize the following insights. But before we go into the detailed breakdown of alternatives and testing components, let's start with some context.

Genesis of Security Testing

Penetration testing has been around since the early 1970s. It's become more common as IT systems and services have evolved to be a crucial part of business operations. Organizations bring in specialists who use the same tactics, techniques, and procedures (TTPs) that an attacker would deploy. This third-party test provides an accurate, unbiased assessment of network and systems security.

However, as digital environments became increasingly pervasive, so did their attack surfaces. While humans are creative, we're finite, too. So, scanners emerged in the late 1990s to provide additional scale (if not depth) to security testing operations. Eventually, the need for additional talent and rigor in proactively finding and fixing vulnerabilities gave rise to crowdsourced security testing in the early 2000s.

BENEFITS OF PENTESTING

- ✓ **Executive Buy-in**—28% of vulns uncovered are high severity.[1] This means that without testing and remediation, the risk of breach is significant. This is something executives care about.
- ✓ **Actionable Data**—To be useful, each vulnerability found should be validated with explicit steps to reproduce, giving clients the ability to do quick remediation.
- ✓ **Vulnerability Risk Reduction**—Organizations become more secure by finding and reducing vulns, thereby mitigating the ways in which they might be breached.
- ✓ **Unbiased Assessment**—Industry best practices are brought to bear on the task of securing your organization by employing regulations and compliance criteria in the completion of a security test.

Effective Security Strategy

Effective security means both protecting high-value assets and shoring up the base level of security across the entire organization. In 2019, there were over 17,000 reported vulnerabilities in the U.S. (and the total number of discovered vulnerabilities is likely much higher).[2] To be secure, organizations need to find and patch every critical vulnerability in every important system since an attacker only needs one to be successful.

What Do We Mean by Test Depth and Breadth?

Security and penetration testing has evolved again to keep pace with continuous software development cycles and a continuous need for high quality security insights.

DEPTH

Criminals sometimes focus on a particular asset and perform many attacks with multiple steps to try to get in. Testing at a deep level can mitigate these kinds of attacks.

BREADTH

Attackers often use automated “bots” to look for easy ways into a network or asset. Broad (but shallow) testing using scanners can shore up these kinds of vulnerabilities.

[1] Synack Red Team data, 12 month period preceding 1/1/20.

[2] National Vulnerability Database, https://nvd.nist.gov/vuln/search.

Types of Security Tests

Security tests come in four basic categories:

- **Scanning** using software to search for vulnerable or unauthorized systems and services [machine-led]
- **Traditional Penetration** which involves evaluating systems for common vulnerabilities, leveraging the Open Web Application Security Project (OWASP) or other standards body [consultant-led]
- **Bug Bounty Testing** in which researchers are allowed to attack the asset in their own creative ways, incentivized by bounties [crowd-led]
- **Crowdsourced Security Testing Platform** which combines the best elements of the above three categories—this is the next generation of pentesting [platform-led, human-enabled]

Scanning

Scanners are used for broad attack surface coverage against assets that are relatively low risk. While scanners won't provide the depth of security testing necessary for holistic security (scanners can't perform multi-step attacks or offer the creativity that researchers can), they will give a "wide-but-shallow" measure of resistance against known vulnerabilities. Examples of players in this category include Tenable, Rapid7, WhiteHat, and Qualys.[3]

While scanners are ubiquitous and inexpensive, they have some fundamental limitations when employed as stand-alone solutions. For example, higher-value assets will almost always require some level of human interaction. Scanners also aren't able to perform complex, multi-step exploits or zero days like humans can. For these reasons, although scanners are considered an essential element of a security test, they are not considered sufficient in themselves to get a realistic assessment of security risk.

[3] Gartner Magic Quadrant for Application Security Testing, Horvath, Zumerle, and Gardner, ID G00394281 29 April, 2020

Traditional Pentesting (Checklist-based)

What used to be a "pentest" has changed significantly over the years. The traditional penetration test was designed to provide a best effort, point-in-time, creative, and primarily manual test. More recently, however, the term pentest (especially in the private sector) has devolved into a lesser version of itself, which often entails performing tests solely against a checklist. Through most of the rest of this document, we will refer to the "traditional pentest" to mean the more current "downscoped" version. The majority of pentesting teams consist of one or two people.

The Big Four consulting firms (Deloitte, E&Y, PwC, KPMG) are good examples of this category. More specialized players include NCC Group, Bishop Fox, and Cipher. And finally, there are a host of smaller independent regional pentesting firms (also known as boutique consulting firms) that use this process.

The efficacy of this method depends on the depth of the assessment an organization requires and the quality of the testers available to the provider. The advantages include simplicity and finite scope. Disadvantages include: no competition among testers, no incentive for creativity, a very limited skill set brought to bear on each vulnerability, no real-time insights into findings, and delayed remediation.

Bug Bounty Testing

Bug Bounty security testing harnesses a diverse set of testing skills, using bounties to incentivize ethical hackers to emulate the behavior of the adversary. This allows them to evaluate the target's overall security rather than simply test predefined security controls. In the process, it also allows them to fill some of the gaps where traditional pentesting falls short. There are several sub-categories involved in this grouping (see next page for details). Some players in this space include Cobalt, Bugcrowd, and HackerOne. Many of the afore-mentioned companies are oriented more toward performing checklists for their broad customer base, and reserving the true crowdsourcing methodology for their large enterprise customers; but they are categorized here for simplicity.

The advantage of bug bounty security testing is that it creates attractive incentives for ethical hackers to find more vulns than the traditional pentest would. A wider range of researchers and skills (often 50+ researchers applied to a given test), and competition brings out overall better performance and increased depth of assessment. This category is more complex and offers varying levels of control. A good buying decision requires discernment from the buyer. (See the next page for more detail on the pros and cons.)

The Skinny on Bug Bounty Testing

Although lumped into the same category, there are different types of bug bounty and crowdsourced security testing, some of which are more effective than others:

VULNERABILITY DISCLOSURE PROGRAMS (VDP, aka Responsible Disclosure Programs): Though not technically bug bounty (there is no actual bounty involved) this is a "see something, say something" policy in which an organization hosts, or enlists the help of, a vendor to manage a program through which anyone can report the discovery of a vulnerability.

Advantages: inexpensive, fairly simple to implement, positive public affairs opportunity.

Disadvantages: potential operational burden from high volumes of low-quality reports; lack of control since vulns can be submitted by anyone and some submitters will feel they are entitled to tell the public if you don't respond within a certain period of time.

BUG BOUNTY MARKETPLACE: a pot of money is put up for ethical hackers to try to hack corporate IT assets. This is similar to VDP except that there is compensation for vulnerability findings. In some cases, the bug bounty program is only available to a specific crowd of ethical hackers (aka security researchers).

Advantages: competitive nature brings out better performance; diversity of skills and experience brought to bear on testing.

Disadvantages: limited control and potential risk if the crowd is not vetted and managed; potential operational burden from high volumes of vulnerability reports of varying levels of quality.

MICRO-CROWDSOURCING: Some companies that use the crowdsourcing or bug bounty terms are actually bringing a finite number of (as few as 1-2) researchers who are often direct-salary rather than bounty-motivated and who typically follow checklists.

Advantages: cheap and relatively quick (though somewhat misleading)

Disadvantages: while this term gives the illusion of crowdsourcing, the small number of researchers and lack of competitive process render it less effective than true crowdsourcing. This really belongs in the category of "Traditional Penetration Testing".

Crowdsourced Security Testing Platform Approach

Combining the Essential Elements of a Security Test

The most robust testing solution—the crowdsourced security testing platform—combines the creativity and ingenuity of crowdsourced vulnerability discovery, the methodology-driven approach of penetration testing, and the scalability and coverage of a high-end scanner. This enables organizations to conduct targeted penetration testing, find unknown vulnerabilities, and gather new intelligence in a scalable way. This intelligence then feeds into the machine-led, human-augmented scanning system, teaching it what suspected vulnerabilities look like. The platform then conducts scalable, broad attack-surface coverage of the remaining assets and identifies sources of risk for the research team to investigate.

The crowdsourced security testing platform transforms all of these components into a continuous, always-on penetration testing process with well-orchestrated coordination between researcher, scanner, and compliance activities. It brings together a crowd of the top security researchers with a high-end, Artificial Intelligence / Machine Learning-enabled (AI/ML) scanner, and orchestrated workflows to engage the crowd for testing. Another way to say it is that all three above components are incorporated together and managed by a smart platform to get the best of each modality. To this day, Synack is the sole representative of this category, though many bug bounty players are claiming to be in this category.

Together, researchers and smart technology work in concert through an integrated platform, which coordinates their interactions; so they augment each other to provide both quality insights and continuous coverage. Because of the precision that comes from the app's smart orchestration, instead of a cap being placed on the bounty, the provider assumes responsibility for the full cost of testing, and all important vulnerabilities are brought to your attention.

> “
>
> *Synack struck us as the most professional, the most responsive, the best designed, and had the best functioning product.*
>
> **CEO AND CO-FOUNDER,**
> **INTERNATIONAL FINANCIAL FIRM**

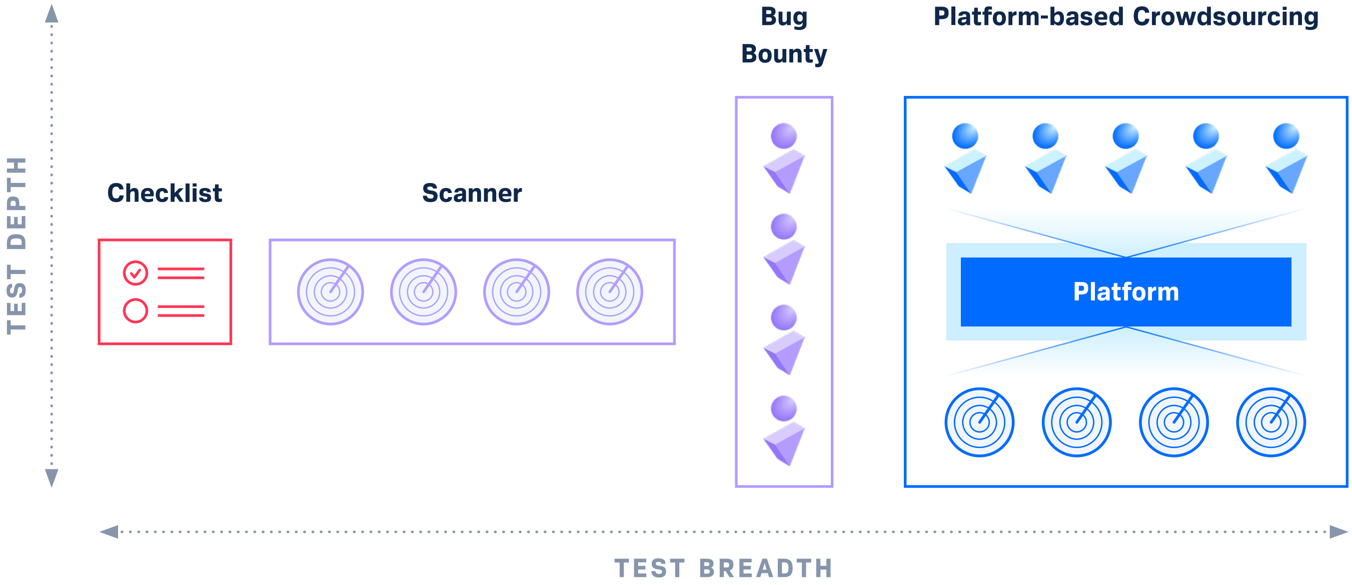
What's Good About Crowdsourced Security Testing Platforms?

- ✓ Scanning provides broad coverage of the lower-risk assets
- ✓ AI/ML orchestrates human effort
- ✓ Continuous, 24x7x365 penetration testing
- ✓ Researcher ingenuity focuses on the high-risk assets
- ✓ Researchers bring creativity, broad skill sets, and TTPs to the discovery process
- ✓ Unlike bug bounty, there are no caps on incentives
- ✓ You have control of the testing process (pause and start capability, asset protection through secure gateway) from start to finish
- ✓ Platform provides real-time, actionable results and analytics

Features by Category

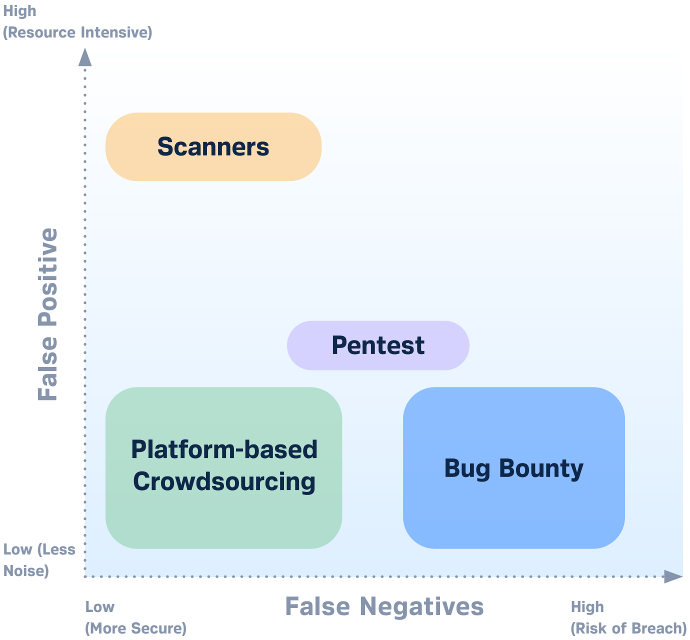
✓ Good ✗ Bad	Scanner	Trad Pentest (checklist)	Bug Bounty Test	Crowdsourced Security Testing Platform
Value (coverage/ cost)	✓	✓	✓ For some specific assets	✓
Security/Trust of Process	✓	✓	✗	✓
Scalability (across full attack surface)	✓	✗	✗ High-value assets only	✓
Test Accuracy (quality of vulns)	✗ False positives	✗ False negatives	✗ Some hyper-deep categories; some missing entirely	✓
Full Service Support	✗	✗	✗	✓

COMPARISON OF DIFFERENT SECURITY TESTING METHODS



What's the ROI from Pen Testing?

The bottom line here is that using the Platform-based Crowdsourcing technique gives 4x higher ROI than traditional pentesting. Quantitatively, this amounts to a 159% ROI due to increased effectiveness, efficiency, and scale.[4]



[4] *ROI estimate based on Synack data through Q1 2020. Assumes a comparison to a traditional pen test costing $30,000 for 80 hours of testing, 6 weeks to start an engagement with a new client, and 1 work week for report generation

ROI OF CROWDSOURCED SECURITY TESTING PLATFORM

159%

ROI—4x higher than traditional penetration testing

3x

more time on target compared to traditional pen testing

20%

reduction in failed patches due to patch verification process

<72 hr

onboarding versus weeks in traditional model

Why Synack Uses a Secure, Trusted Platform

Trust is key in crowdsourced solutions. If risks within the community (around communication of vulns to the public) are not contained, companies can find themselves engaged in a runaway process with vulns being discovered faster than they can remediate them; a lot of noisy results without a clear signal; and/or researchers threatening to divulge vulns if they are not fixed within a certain amount of time.

WATCH OUT FOR LAND MINES

- **Subcontracting a third-party pentest**—Often a principal security provider will subcontract a pentesting service to beef up their offering; or in some cases, multiple ones in order to get a more diverse researcher crowd. The problem is there is no clear responsibility in these scenarios and this often translates to a lot of finger-pointing and typically poor coordination between the two+ companies.

- **The fake crowdsourced pentest**—Many companies that claim to use a crowd of researchers actually assign 1–3 researchers to your project. This fails to bring sufficient breadth and depth to the test. This is also known as “Two testers, two laptops, two weeks”.

- **Lack of Crowd Competition**—An insufficient crowd environment can eliminate competition as well. In a true crowdsourced pentest, the crowd is unleashed and whomever finds and documents the vulnerability—the most thoroughly and quickly—gets paid. Think of what a boxing match would look like with only one boxer.

- **Bug Bounty Checklist**—Due to the allure of crowdsourcing, some organizations try to convolute the concept of incentive-driven crowdsourcing with a simple checklist model. Both modes are important to achieve security but don’t allow yourself to be deceived into thinking a “crowdsourced checklist” is a replacement for crowdsourced security testing.

- **Manual Analytics**—When it comes to analytics, it’s garbage in, garbage out. For analytics to be actionable, they need to be based on reliable data. Some platforms use analytics that are based on manual processes or human-assessments, rather than robust and unbiased algorithms, making them unreliable.

- **Illusion of Control**—Many crowdsourced security platforms boast customer control of the crowd. Furthermore, “vetting” of researchers has become loosely equated with control. Buyers should ask vendors how they vet their crowd, if they continuously monitor crowd activity, and if they will have 24/7/365 visibility into testing activity through the platform including the ability to pause and restart the entire testing process.

- **No patch verification**—Beware of those organizations that don’t provide patch verification testing. Roughly one-third of initial patches fail. Without retest, you can’t be assured the patch worked. The only way to know for certain that the patch has been successful is to confirm with a verification test.

Synack addresses this in two ways. First we vet every researcher to ensure only those who are professional and ethical—in addition to proving their high levels of skill and experience—are chosen for the Synack Red Team. Second, all testing is performed through a secure gateway and is managed through our platform. This allows us to continuously monitor and control testing activity and behavior to make sure it meets our high standards. Finally, to ensure maximal protection and privacy, we provide secure, virtualized environments for our security researchers, which offer greater data privacy through full endpoint control.

> “*They bring a lot of testers with a lot of experience and skills to the test. You don’t pay more to have more testers.... I am happy to say that our expectations have been exceeded.*
>
> **SENIOR CLOUD SECURITY ANALYST**
> **IN THE SERVICES INDUSTRY**

TRUSTED PLATFORM

How Synack Products Compare by Feature

For a macro view of high-level features and how they roll up to the various SKUs, the following table may offer some insight. This should help give context around key features and their respective value.

	Discover: Crowdsourced Vulnerability Discovery	**Certify:** Crowdsourced Penetration Test	**Synack365:** Crowdsourced Continuous Penetration Test
Duration	Time-Bound	Continuous	Continuous
Smart Platform, with Real-Time Results and Analytics	✓	✓	✓
Vulnerability Disclosure Program (VDP)	✓ Included with purchase of four or more tests	✓	✓
Incentive-Driven Vulnerability Hunting	✓	✓	✓
SmartScan with Triage	✓	✓	✓
Methodology-Driven Testing (Checklist)		✓	✓
365 Testing Coverage by Synack Red Team			✓

Conclusion

Stand-alone scanners will provide you broad (but shallow) attack surface coverage for low-value assets. Traditional pentesting will give a cursory view of some assets but is not scaleable, has poor traceability, and lacks analytics. Bug bounty security testing will provide deeper testing of one or more valuable assets.

However, for breadth and depth of assessments to achieve reliable, holistic security, a platform-based crowdsourcing solution provides the next generation in security testing. It combines the scalability, talent, and depth of an ethical hacker crowd, with the broad coverage of a scanner and the compliance requirement of a checklist; and gives you deep security coverage all year round. Only with a fully-vetted crowd, harnessed by a continuous, smart platform, will you get full security coverage and real ROI.

> “*Security testing has become a priority for every CEO and Security Engineer, alike. The global cost of cybercrime is projected to reach $6T by 2021. Organizations simply can’t hire the talent they need to meet this threat; nor can they rely on antiquated defenses. For organizations to succeed in minimizing their security risk, they need scalable, comprehensive security testing platforms, optimized for both depth and breadth, without compromise.*
>
> **—B CAPITAL GROUP**

Appendix A: Penetration Testing Vendor Selection Checklist

When researching traditional penetration testing, bug bounty, and platform-based crowdsourcing alternatives, this checklist may assist while evaluating vendors.

	Vendor Has:
Researchers	
Crowd of hundreds of available testers (50–80 avg per test) to ensure breadth and depth of skills and experience	○
Fully-vetted researcher community—including skills test, interviews, and background checks—to ensure security and quality	○
Incentive-driven model which rewards ingenuity and fosters competition	○
Researchers that are on-demand and independent rather than on the payroll, bringing their skills to bear on your security posture as needed	○
Protection and Trust	
Customer not liable for future researcher activities	○
Customer owns data and discovered vuln IP (not vendor or researcher)	○
Coverage analytics, when/what/how (i.e. attack attempts) the applications and assets in scope have been assessed based on researcher activities	○
Payouts managed by vendor to protect customer	○
No “Last Resort” exception to privacy for reporting vulnerabilities	○
Customer-controlled start, stop, and resume functions during testing	○
Technology	
Automated vulnerability scanning that augments and enables researchers	○
A centralized SaaS portal that gives customers 24x7x52 visibility into their testing, results, metrics, and reports	○
Researcher coordination/triage through a smart orchestration platform	○
Secure gateway through which all testing is performed	○

Vuln Discovery Process	
Compliance-driven, methodology-based testing that checks for known weaknesses	○
Incentive model of vulnerability discovery	○
Meets audit and compliance mandates, such as PCI, NIST	○
Elimination of duplicates	○
Audit trail and real-time updates on all research activity	○
Number of researchers, research hours logged for tracking & accountability	○
Ability to communicate directly with researchers	○
Effective Security	
Patch efficacy ratings for tracking progress	○
Fully managed patch verification service with guaranteed incentive	○
Risk-free patch process: verification request only goes to original reporter	○
Reporting and Scoring	
Audit-ready, professional, customizable reports (PDF) on demand	○
Human-written analysis in final report	○
Clear, objective scoring of asset hardening	○
Benchmarked results to track progress against own history and industry peers	○
Security Researcher Software Platform	
Foolproof workflow from scan, to mission, to triage, back to patch verification	○
Unique detection techniques for host, web, mobile	○
Real-time exploitability assessment workflow	○
Noise reduction and customer service streamlining	
Detailed directions for remediation directly from researchers	○
Full triage of every vuln submission	○
Dedicated account representative	○

Appendix B: Platform-based Crowdsourcing Features and Benefits

A Crowdsourced Security Testing Platform has many benefits compared to a traditional assessment.

FEATURE	BENEFIT
Scoring	While a simple list of vulns lacks actionable risk information, the real value comes with scoring of vulns. Synack uses the Attacker Resistance Score (ARS) metric, which quantifies variables including the difficulty of discovering a vulnerability, the severity of the vulnerability, and how efficiently the vulnerabilities can be remediated.
Data-driven Insights	Getting information into the relevant hands (that need it) is critical. Synack provides vuln data to researchers, allowing them to make informed decisions and find vulns more quickly to arm you with the most accurate info with which to assess your risk.
Pattern Detection	Continuous scanning and testing highlights changes in an attack surface and potential areas of risk. Knowledge of these trends can be invaluable to an organization in determining if they are undergoing a targeted attack or if organizational policies or procedures are insufficient to meet security needs.
Breadth of Skills	Some large consulting firms often assign teams as small as one person for a pentest. This translates to a limited range of technical skills and few tools being used to uncover security holes. Synack's true crowdsourcing method not only ensures a wider range of skills brought to the party, but our curation and vetting process ensures you have the best researchers based on both skill and integrity.
Security (vs Compliance)	Compliance checks achieve little towards true security. Combining a compliance checklist with incentive-driven crowdsourced security testing AND ongoing missions orchestrated by a smart platform brings your organization compliance AND security.
Results and Incentives	In traditional penetration testing, engagements are time and materials based. This means the consulting firm gets a paycheck irrespective of how many security holes are discovered, exploited, and reported. Synack's method rewards only confirmed vulnerabilities and exploits. This ensures customers pay for real value and not just time spent on an engagement.

FEATURE	BENEFIT
Validation of Remediated Vulnerabilities	Traditional penetration testing engagements don't always verify that the holes have been plugged. Instead, it is left for the customer to perform the fix and self-validate that it is effective. Synack procedurally ensures that not only are clear steps to reproduce given, but also that exploits previously demonstrated are no longer effective, thereby avoiding the failed patch syndrome. Researchers that discover and report successful exploits are further rewarded with bounties to verify that they have been resolved.
Audit Trails	Not all tests capture adequate information about the testing process to ensure success. For both compliance and best security practices, Synack captures both audit trails and technical controls and makes them fully available to customers.
Start/Stop Button for Testing	Having control of the testing process is more important than you might think. There could be a surprise audit which necessitates a halt in testing in order to avoid embarrassing problems. Synack has set up a secure, vetted, and flexible platform that not only puts a global community at your service, but also keeps it under your control. This includes a stop/start button which allows you to control when the testing stops and restarts.
Ownership of Vulnerabilities and IP	Once you have performed testing and done remediation, the next most important factor is keeping control of the vuln data. Some contracts allow public disclosure of vulnerabilities after a certain period of time, regardless of mitigation status. Synack always gives the ownership of discovered vulnerabilities and intellectual property to the customer.
Smart Platform	A truly effective pentest requires three primary components. First, you need a vetted, highly-qualified crowd of researchers with diverse skills and tools. Second, you need a smart scanning technology to enable the crowd and accelerate their vulnerability discovery process. Finally, you need a platform on which to let the researchers work (and with which you can monitor and control their activities, and through which you can view findings). This gives you unmatched talent delivered in a controllable package so you get the quality and contain the risk.

Appendix C: Glossary of Terms

Black-box Model—A black-box penetration test determines the vulnerabilities in a system that are exploitable without authentication. The penetration tester has no internal knowledge of the target system, its architecture, source code, etc.

Blue Team—Internal teams designed to defend their organization from real-world attackers by understanding their TTPs and evolving the company's defenses along with the adversary.

Bug Bounty Model—A pay-for-results model where a pot of money is provided as an incentive for researchers to find vulns. Typically when the pot is gone, the test is over. These tests are less focused around complete testing and security, but act more as a starting point toward hardening your environment.

Compliance Checklist—A specific checklist (such as OWASP, NIST 800-53, or PCI) is used as a guide for researchers to hunt for specific vulnerabilities based on specific compliance and audit standard checks. This method effectively tests for compliance but not full security.

Continuous Testing—Coverage for 24x7x365 days of the year. This can be a subscription-based yearly engagement that includes a scanner and/or a fully managed service with regular compliance verification, a dedicated program manager, scoping services, vulnerability triage, alerts, patch verification, vulnerability disclosure program management, and detailed data analytics and reporting. The goal is to shorten and/or eliminate the life of exploitable vulnerabilities, and continually increase systems' resistance to cyber attacks.

Crowdsourced Vulnerability Discovery—A testing model which incentivises a large group of ethical hackers to compete to find vulnerabilities. Typically this might involve 50 - 100 researchers with varied skills and experience and many different tactics, techniques, and procedures.

Gray-box Model—Pentesters typically have some knowledge of a network's internals, potentially including design and architecture documentation and an account internal to the network, providing a more focused assessment of a network's security than a black-box assessment.

Internal Asset Testing—Emulates an attacker trying to gain access to an asset after(italics) they have already breached the internal network. The target is typically the same as external pen-testing, but the major differentiator is the "attacker" either has some sort of authorized access or is starting from a point within the internal network. Specifically in the case of

Synack, Internal Asset Testing (IAT) creates a private channel between the trusted researchers and client assets, such as sensitive or pre-released apps, behind a firewall. By using a site-to-site VPN, the benefits of Synack LaunchPoint are extended from the client asset to the researcher.

Missions Checklist—This is something unique to Synack in which the researcher crowd is delegated suspected vulnerabilities to exploit. The direction comes from the ML-based scanning system (SmartScan). The control and timing of exploits is controlled by the scanner (and ultimately the customer). Synack offers checklist-style tests that complement freeform vulnerability discovery. The result is a high-quality version of a compliance-based penetration test, where success is based upon specific tests being completed and logged. Synack Red Team researchers execute a set of specific missions (or tasks) and document their findings for payment. Researchers are paid on the quality of their work and detail of their submission. Checklists are often designed from either OWASP or PCI/OWASP-based guidelines.

Open Vulnerability Discovery (OVD)—Sometimes referred to as creative vulnerability discovery, this is a process in which ethical hackers try to break into a network, host, device or application.

Penetration Test—An authorized simulated cyberattack on a computer system, performed to evaluate the security of the system, traditionally using 1–2 ethical hackers that work for a consulting company, who work off of a checklist, or in some cases, creatively hunt for vulnerabilities.

Point-in-time testing—This method is distinguished from continuous testing and usually is the result of an immediate need for a test to be performed to meet a compelling event, such as an audit, key customer request, or acquisition. The standard timeframe is two weeks.

Synack Red Team (SRT)—This is a Synack term and represents the private network of highly-trusted, diverse and vetted security researchers. The SRT enables the most talented security researchers across the globe through a platform to do what they love and get paid for it.

Purple Teams—Purple teams enhance information sharing between the Red and Blue teams to maximize their respective and combined effectiveness.

Scanner—tool that scans for security vulnerabilities and loopholes. These are automated and scalable but can produce copious amounts of data that burdens the security team if not triaged by the provider.

Social Engineering test—Social engineering penetration testing is the practice of attempting typical social engineering scams on a company's employees to ascertain the organization's level of vulnerability to that type of exploit. This is typically outside the scope of a pentest.

Triage—The process of dispositioning reported vulnerabilities by either a researcher or vulnerability operations team to definitively identify if a vulnerability is exploitable.

TTP—This refers to the Tactics, Techniques, and Procedures used by threat agents (cybercriminals) to orchestrate and manage attacks. On a related note, it can also refer to those methods used by "white hat" researchers to identify vulnerabilities during penetration testing.

VDP—Vulnerability Disclosure Program is a process in which general public hackers are allowed to report vulns in an organization's assets and submit these vulns formally to that organization. The VDP can be managed by the organization or a third party and involves no vetting, no protections, high-noise, and the opportunity for malicious actors to operate under cover.

Vulnerability Assessment (or Intelligent Vulnerability Assessment)—while may be used in a broader, generic way, practically speaking it often means the market category for network scanners.

Vulnerability Discovery—a testing methodology that relies on the variety, creativity, and expertise of the trusted Synack Red Team to emulate attacker methods. Deployed to find exploitable and previously unknown vulnerabilities in client attack surfaces, Vulnerability Discovery uncovers findings that checklist-driven tests often miss. Once a vulnerability submission is confirmed to be valid, the SRT researcher is paid via an incentive-based bug bounty model. Vulnerability Discovery allows organizations to manage risk associated with unknown vulnerabilities.

White-box model—In contrast to black-box testing, penetration testers are given full access to source code, architecture documentation and so forth.