Synack

THE SYNACK VALUE

CROWDSOURCED SECURITY TESTING PLATFORM: SMART PENETRATION TESTING

In today's agile environment that demands comprehensive coverage so you have a realistic view of your attack surface, crowdsourced solutions fall short lacking the control, technology, and coverage needed for continuous security. We are learning that:

- Quantity of vulnerabilities found does not mean the most critical vulnerabilities have been found
- The security industry can't only rely on crowdsourced human talent: 3.5 million cybersecurity jobs are predicted to go unfilled by 2021, while organizations have turned to bug bounty-type testing to fill their internal gaps, there are still a limited number of ethical hackers around the world with the right skills
- Purely unstructured incentive-based models do not achieve compliance requirements
- Clients need control and auditability with full transparency of testing coverage and findings for secure crowdsourced testing of an enterprise environment

For the last 6 years Synack has been the leader in trusted Crowdsourced Penetration Testing using the world's most skilled red team (SRT), smart technology, and a trusted platform. The quality of the vulnerabilities, end-to-end program management, and white glove service ensures that we do the work, not our clients. This is why Synack has become the most trusted crowdsourced security platform protecting leading global banks, DoD classified assets, and close to $1 trillion in Fortune 500 revenue.

The attackers are changing the rules, so Synack has changed the game. Synack leads the market in a **more effective, efficient solution through our Crowdsourced Security Testing Platform**. Synack is the industry's only crowdsourced security test to seamlessly combine crowdsourced human testing talent with proprietary AI technology—making your security team smarter and faster providing a greater level of intelligence to help you find and fix vulnerabilities, and achieve compliance, at scale.

Crowdsourced Security Tests		Synack Crowdsourced Security Testing Platform
PEOPLE		
Open to anyone with an email address Varied levels of pre-check No interviews/ ongoing monitoring	**Ethical Hackers**	100% vetted. Exclusive community. 5 stage vetting process for skill & trust goes beyond ID/background; 12% acceptance rate Ongoing monitoring and engagement
Unstructured hacking. High volume of vulnerabilities (often lower severity) and duplicates waste precious security team resources No centralized research guidance	**Testing Approach**	Compliance-based testing and creative hunt for vulnerabilities Centralized research guidance by Synack

Crowdsourced Security Tests		Synack Crowdsourced Security Testing Platform
	TECHNOLOGY	
SAAS portal to manage testing and payments. Limited analytics	**Efficiency**	Goes beyond program management. Combines crowdsourced human testing talent with proprietary AI technology to focus researcher time on the most critical targets. SmartScan reduces scanner noise by >99%.
None	**Automated Vulnerability Scanning**	SmartScan harnesses Hydra, Synack's proprietary scanner, to continuously discover suspected vulnerabilities, engage researchers for triage, and deliver more testing coverage and insight to the end customer
Some claim ServiceNow	**Integrations**	Splunk, ServiceNow, JIRA
	PROCESS	
Optimized for vulnerability volume only, not quality or improving security	**Effectiveness**	Achieves both compliance and security through a combination of structured (checklist-based) and unstructured (mimics a realistic attack) testing
Risk borne by customers Bounty pool is unpredictable liability	**Financial Risk**	Fixed-fee model protects clients from future liability
Optional (for fee)	**Triage and Payment Management**	Always included—executed by SRT & Synack Mission Ops
	TRUST	
Limited VPN access for researchers	**Control**	Gives control to the customer to decide where, how, and when to test. LaunchPoint VPN network provides audit trail and technical controls for all testing activity LaunchPoint+ offers Amazon workspaces that provide endpoint control. Data never leaves the workspaces to migrate onto researchers' computers.
Vulnerability Reports and IP owned by hacker or bug bounty company	**IP Ownership**	Vulnerability Reports and all associated IP ALWAYS owned by the customer
Segregated by tag, controlled by researchers	**Traffic Segregation**	Segregated by port, controlled by Synack as agreed to with customer
None	**Auditable Testing**	Testing gateway captures coverage analytics and attack classification
Not included	**Assessment On/Off Switch**	Pauses and restarts testing activity with the press of a button

Crowdsourced Security Tests		Synack Crowdsourced Security Testing Platform
	RESULTS	
Varies	**Vulnerability Remediation**	Included: Remediation guidance and paid patch verification
Portal-centric data access, sometimes with machine-generated summary reports	**Reporting & Analytics**	Real-time portal access with on-demand vulnerability intelligence, audit quality customizable reports, human-augmented analysis, coverage analytics
None	**Security Score**	Attacker Resistance Score gives empirical hardness assessment
For public-facing bug bounty programs from Google, Facebook, and GitHub, 4–5% of bugs were eligible for payment	**Valid Vulnerabilities**	Synack maintains a >98% signal-noise ratio, which means almost all vulns submitted are eligible for payment

SYNACK'S RETURN ON INVESTMENT (ROI)—159%

>30% higher ROI compared to other crowdsourced solutions due to increased effectiveness, efficiency, and scale.

Synack Benefits Included:

- **Effectiveness and Efficiency**
  - **Operational Efficiency:** up to **3 internal FTEs** are removed from the unnecessary increased operational burden seen in bug bounty models
  - **Patch Verification: 15% reduction** of failed patches using our Patch verification service
  - **Team/Reporting Efficiency: 20+ hours** of idle time avoided due to Synack's iterative reporting feature
- **Smart Technology:**
  - **Increased Coverage:** 43% additional value with SmartScan, Synack's intelligent vulnerability assessment included in every penetration test
  - **262% ROI from SmartScan** compared to traditional scanners
- **Synack Costs:**
  - **One Flat Fee.** Nothing Hidden. No Surprises.
  - Synack's flat solution fee is the only direct cost to the customer. This does not include the cost of time required to sign the initial contract or interface with our Customer Success team.
- **Synack's crowdsourced penetration testing solution offers additional features whose benefits cannot be easily quantified, including:**
  - Full packet capture of all testing activities for continuous visibility into testing activities
  - Coverage analytics that show what, when, and how a target is being tested
  - Synack's Attacker Resistance Score provides organizations with a metric to present the security of their organization to their executives and boards.

Furthermore, Synack's top researcher talent finds security vulnerabilities left undetected by traditional security solutions, significantly increasing clients' security intelligence and reducing overall security risk.

**ROI estimate based on data through Q2 2019. 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.*

Synack, Inc.
855.796.2251 | www.synack.com | info@synack.com