Synack Continuous Testing

Live an Agile Security Lifestyle with Crowdsourced Continuous Testing

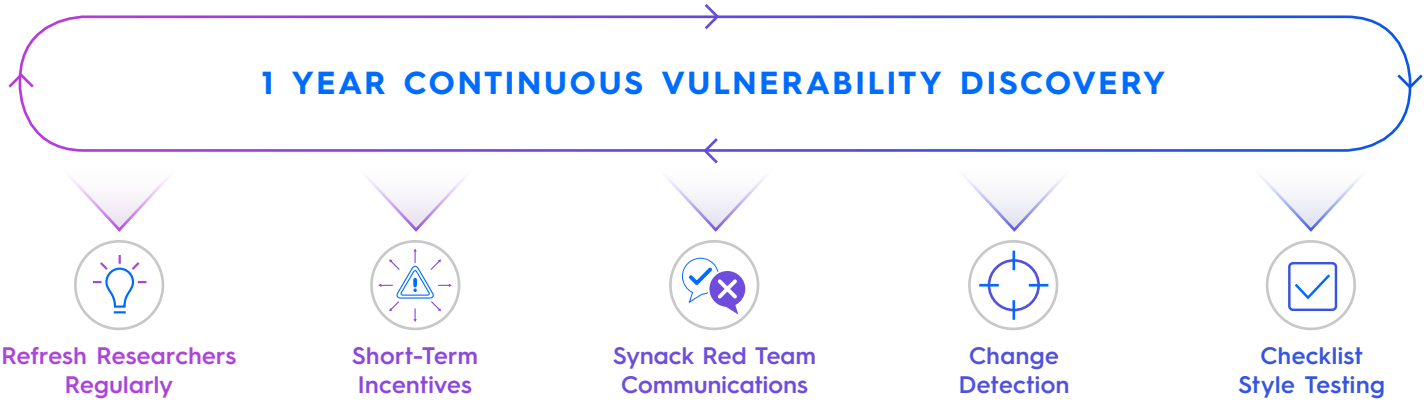
Synack Crowdsourced Continuous Testing (CCT) provides all of Synack's offerings in one complete, non-stop package. CCT delivers continuous security insight from the attacker's vantage point that is not possible with any ordinary testing, tools, or bug bounty platforms. Utilize the full suite of vulnerability discovery, compliance-ready checks, and real-time Attacker Resistance Scores to improve your security at the process level (not just one vulnerability at a time).

By implementing continuous security testing, you can live an agile security lifestyle and reduce risk:

- Align security operations with continuous integration/continuous deployment (CI/CD) practices
- Shorten and/or eliminate the life of exploitable vulnerabilities
- Continually increase your systems' resistance to cyber attack

What You Get

CCT comes with all of Synack's vulnerability discovery, compliance-ready weakness checks, the Synack Attacker Resistance Score and a human-written analysis.



Synack Process

The process starts with a simple launch meeting with Synack to get everyone ready to start. Synack will start providing validated vulnerability reports within hours of the first submissions. Alongside continuous vulnerability discovery, customers can schedule periodic checklist-style tests for compliance purposes. Unlike pen testing or bug bounty platforms, customers have complete control over testing traffic. Synack uses dynamic incentives to guide researcher traffic to key areas to ensure full coverage on customer assets on a continuous basis. During the testing, customers can view real-time results and work with their dedicated program manager for specific insights. All effort to produce the results is handled by Synack, including scoping, scanning, prioritizing, testing, triage, validation, motivating, paying and notifying. Data is collected throughout to understand not just what was found, but how it was found—an essential question to answer for better future security.

What Synack Tests

Synack handles a wide range of target types. They can be tested individually or in combination (such as a Mobile App using a REST API). **Don't see what you're looking for? Ask a Synack representative.**

Web Applications

Infrastructure

Mobile

Cloud

API

Features and Benefits

Top, Trusted Talent	Tested, interviewed and holistically evaluated. Not just ID checks.
Own your Vulnerability Intellectual Property	Vulnerabilities Reports belong to Synack customers, not Synack and not the researchers.
Control of Research Traffic	Research traffic can be paused instantly for any reason.
Full Service and Support	All work except turning valid reports into internal remediation plans is handled.
Scalable Recon and Scanning	Synack's hybrid software-human scales better than bug bounty hunters.
Divert Research from Public Internet	Research traffic is diverted to Synack's LaunchPoint VPN gateway for security and reliability, minimizing the strain on your production systems.
Measure Testing in Progress	Unlike Standard Penetration Testing, Synack measures the aggregate time and volume of activity researchers spend performing work.
Classified Attack Traffic	Synack provides classifications of most attack traffic to see alarming trends before they set off alarms.
Analytics	Spot trends through testing coverage analytics that could result in unfound vulnerabilities living longer than necessary.
Dashboard	See program status at a glance, including research hours logged, researchers engaged, patch statuses, vulnerability status, burndown chart, and much, much more.
Detailed Report	Reports on demand with results found to date, including methodology, targets, and results.
Non-Stop	Continual activity to find vulnerabilities can significantly shorten your window of exposure for security vulnerabilities.
Fair Liability Terms	Synack takes responsibility for the work of the Synack Red Team. It's not a contract directly between you and bug bounty hackers.

Synack, Inc.