Synack Crowdsourced Vulnerability Discovery

Enhance your security with top talent and intelligent platform technology

Synack's Crowdsourced Vulnerability Discovery (CVD) helps you close vulnerabilities that other methods don't even find. That's because Synack uses a proven combination of software scanning, tooling, humans, platform, and processes to find critical, high-impact vulnerabilities for over 100 organizations around the world. We don't stop there—we help with verifying your remediation cannot be circumvented by a clever attacker.

The heart of Synack is the Synack Red Team (SRT), who performs controlled testing through Synack's secure platform. The SRT allows you to augment and scale your testing without burdening your team with more work and without compromising control. Every vulnerability report and every bounty payment is managed and validated by Synack. However, you decide how you want to activate the crowd; you have clear visibility into all testing and full ownership of all findings. With CVD, you eliminate the root causes of future breaches, secure development, and gain peace of mind.

What You Get

Vulnerabilities

Diverse, Skilled Crowd of Researchers

Testing Data

Professional Report

The Synack Process

During a two-week engagement, customers participate in a simple launch process, then start receiving validated vulnerability reports. Unlike pen testing or bug bounty platforms, customers have complete control over testing traffic. During the testing, customers can view real-time results via the Synack portal or 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 Apps

Infrastructure

Mobile

Cloud

API

Synack

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.
Time-Bound	Bundled in two-week bursts of research activity to fit with your development and security cadence.
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.

855.796.2251 | www.synack.com | info@synack.com