

The CISO Dilemma

Comply with security testing requirements or try to find serious vulnerabilities? Option 1: You can get every compliance requirement met with a penetration test, but it still leaves you uneasy, wondering about what vulnerabilities you might have missed. Option 2: You know that those hidden vulnerabilities have the potential to severely damage your company. You could run a bug bounty program to find them, but you know you can't control a crowd of hackers and you wonder if the reward is worth the higher risk. Either choice will be a compromise.

Synack offers a solution that doesn't require any compromise—a crowd of skilled ethical hackers that help you find vulnerabilities, technology that makes testing efficient and effective, a managed compliance check process, and a self-service platform that gives you visibility and control over the crowd. The Synack team helps our customers scope, test, find, analyze, and patch—with ultimate efficiency and effectiveness.

Synack Crowdsourced Security Testing

Synack gives customers access to a unique security testing platform that consistently delivers results that make organizations more secure. Our customers gain three major benefits from this process:

INSIGHTS > CONTROL > ATTACKER RESISTANCE

The Synack process emphasizes customer control, minimizes burden on your people, and optimizes results to create a Zero Compromise approach to bug bounty and penetration testing. The Synack value is security testing with the speed and agility of software development, the data-driven intelligence of the world's best security researchers, and the convenience of a managed service. Synack's testing platform offers unique techniques for web, host, mobile, or API targets.

Synack has four offerings to meet a wide variety of needs for AppSec, network, mobile, and API security. These include compliance, audit, scoring, and standard security requirements, all delivered through a managed and controlled approach.

Managed Responsible Disclosure (MRD)

Synack Managed Responsible Disclosure program allows customers to accept reports of vulnerabilities with zero burden on the customer. No wading through submissions or facing time demands from submitters. All vulnerabilities reported go to Synack first. Synack screens, vets and prioritizes these submissions to unburden the customer's security team. Only valid, exploitable results are delivered to the customer for remediation and patching, making your security more effective.

Crowdsourced Vulnerability Discovery (CVD)

A better bug bounty. Synack Red Team researchers conduct a creative hunt across your environment, finding severe security vulnerabilities and weakness patterns left undetected by other methods. Known, vetted, and skilled researchers are incentivized through a responsive bug bounty model and supported by an AI security platform, resulting in rapid vulnerability detection, intelligence gathering, and quality, detailed report submissions. You get a comprehensive threat picture, encompassing both the vulnerability and its remediation routes. An on-demand two weeks engagement, CVD provides the results and transformative data that only truly simulated attacks can deliver.

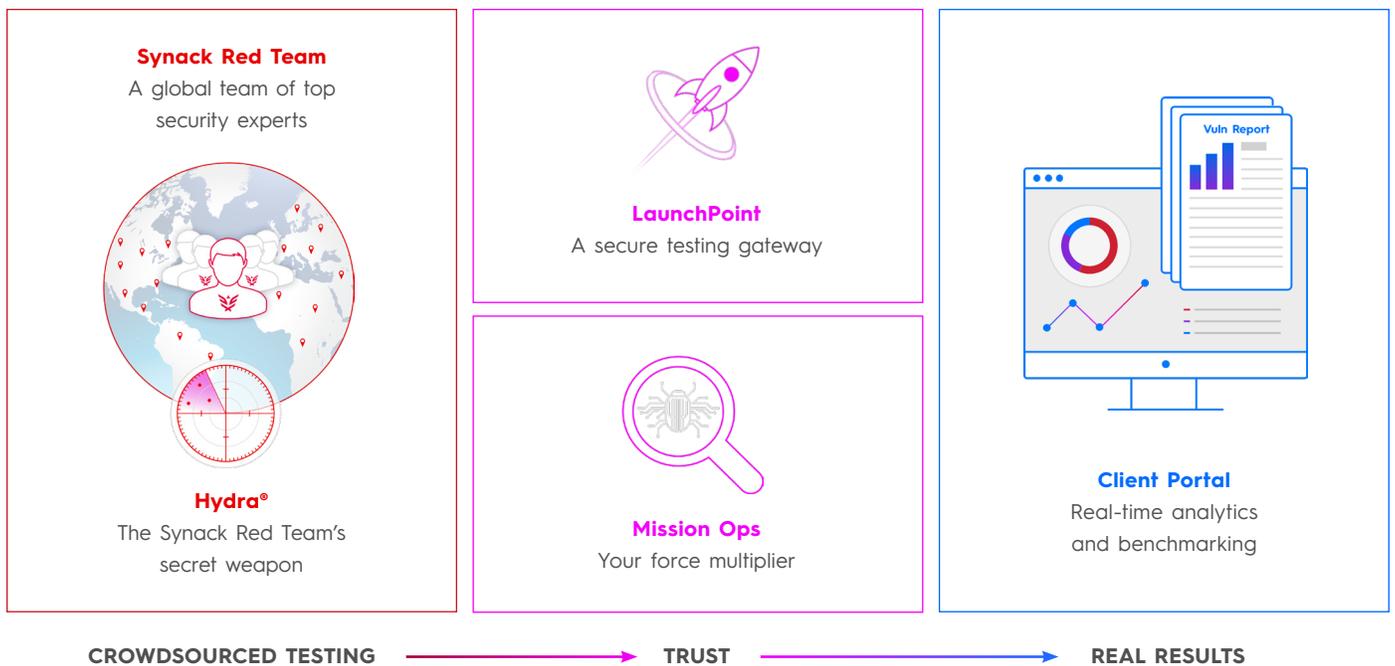
Crowdsourced Penetration Testing (CPT)

A better pen test. Synack's Crowdsourced Penetration Testing augments the capabilities of CVD with a checklist-driven testing approach built specifically for the compliance reports you need. To meet specific regulatory-driven compliance standards, CPT offers you OWASP and PCI-ready checks, documenting how each was done, and comprehensive data on positive or negative results. You also get Synack's Attacker Resistance Score, which quantitatively ranks your security posture through an attacker's vantage point and helps you easily communicate security status with people inside and outside your organization.

Crowdsourced Continuous Testing (CCT)

The Synack Crowdsourced Continuous Testing solution couples CVD and CPT at the cadence you operate, delivering continuous monitoring and regular penetration testing. CCT provides the most dynamic security assurance you can get: narrow security gaps and harden your attack surfaces, leverage advanced software-based change detection, continual scanning, and ongoing human analysis from the Synack Red Team. CCT moves testing from an intermittent cadence to an agile flow, matching your DevOps journey. Integrate security and development teams seamlessly.

Synack Crowdsourced Security Testing



Underlying Synack's offerings is the Synack platform and its unique components. Together, they deliver crowdsourced security testing that has been trusted by the U.S. Department of Defense, IRS, and over 100 organizations around the world.