

Synack Platform Overview

Strategic Security Testing That Improves Your Security Posture

Synack's Platform enables pentesting that is strategic instead of compliance-driven by illustrating actionable data about your attack surface and guiding your security team through comprehensive remediation of exploitable vulnerabilities.

Synack's strategic approach provides point-in-time and continuous pentesting and remediation guidance that actually improves your security posture, unlike more tactical approaches that claim success when regulators are satisfied. Annual testing does not keep pace with today's agile development life cycles that introduce new code daily. Moreover, current security testing methodologies often treat all assets the same despite a varied level of risk. Finally, most firms don't take action on results due to poor vulnerability report quality, visibility and consistency. It's time to embrace security testing that focuses on risk instead of compliance.

The Synack Platform: A Continuous and Risk-Driven Approach

Synack combines vulnerability management, operations and support, an API and integrations, reporting and real-time analytics, and managed community access in a single SaaS platform. Synack provides a strategic security testing platform that can:

- Find root causes of vulnerabilities and materially improve your security posture
- Launch a test in days, not weeks or months
- Do more testing without compromising on quality
- Give your team visibility into vulnerabilities, coverage and remediation status
- Increase collaboration with developers, leadership, and even the board
- Provide an extra layer of security for your data
- Visibility and control of all researchers and testing across your environment

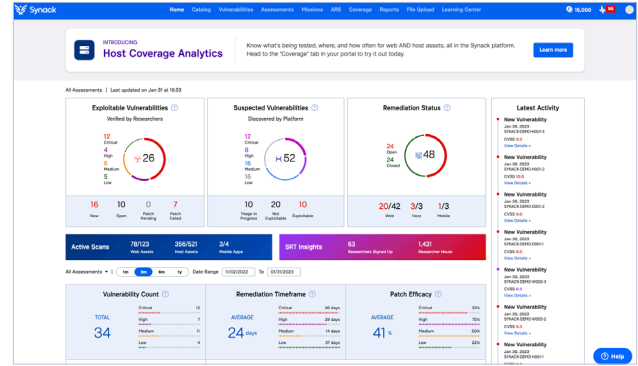
A CISO PERSPECTIVE

Security Testing Today

"All the money we spent on security testing and remediation yesterday is gone. We don't learn anything from the process or leverage the data strategically. We claim success if the regulators are satisfied."

The Synack Platform Pillars

The Synack Platform is the central point of visibility and control of Synack’s on-demand security testing that integrates the adversarial analysis from external security researchers into your standardized pentesting and security processes. The following platform capabilities are instrumental in delivering a superior security testing experience.



PILLAR	DESCRIPTION
Vulnerability Management	Read comprehensive summaries of exploitable vulnerability findings, communicate with researchers, and request patch verification all through convenient workflows.
Reporting & Analytics	Custom reports that outline vulnerability findings, test coverage analytics, and patch efficacy that satisfies compliance requirements and provides insights necessary to identify vulnerability root cause(s). A powerful metric, the Attack Resistance Score, conveys asset-level risk and changes to your security posture over time.
Test Controls	Test controls provide security teams with visibility and control of all researchers and testing across your environment. Platform controls include full packet capture of all testing activity, the ability to pause testing at the click of a button, and testing data stored on Synack-owned endpoints. Synack also provides visibility into researcher testing hours and a source IP address for all researcher traffic.
Operations & Support	In addition to customer support teams, Synack’s vulnerability operations team ensures that only verified, exploitable vulnerability findings are presented to you, reducing false positives and noise.
API & Integrations	The Synack API and integrations enables you to integrate security testing and data into existing security processes to improve responsiveness, triage and remediation of vulnerabilities. Share data and streamline processes with Microsoft, Splunk, Jira, and ServiceNow integrations.
Managed Community Access	Synack goes beyond bug bounty models by handling payments, performing rigorous background checks and indexing researcher skills, so you don’t have to.

Synack Platform Tiers

To get started on the Synack Platform, enterprise customers need to select either the *Standard* or *Premium* tier; [click here](#) to learn about the tiers and to find the program that works best for your security organization.

Synack’s *Premium* tier includes the Synack Managed VDP, a white-glove service for busy security teams. The Synack Managed VDP handles vulnerability triage with remediation guidance, coordinates researcher recognition and delivers data to support CISA or Board reporting, all backed by the premier security testing services available on the Synack Platform.