

Continuous penetration testing

Synack90 and Synack365

Synack's continuous penetration testing enables security teams to keep pace with a rapidly changing attack surface.

The rate of modern software development and infrastructure change strains our security testing and operations capacity. Organizations have gone remote and digital, increasing the risk of introducing new vulnerabilities and creating a continuous stream of new risks and challenges to maintain compliance.

Continuous penetration testing

Synack provides an all-in-one security testing platform, designed for scale. After joining the Synack Platform, select a continuous pentesting option that aligns to your goals. Synack's continuous open vulnerability discovery solution (OVD) is available in 90 and 365 day increments. The test leverages varied skill sets and experiences levels of the Synack Red Team, all the advanced capability in the Synack Platform, and vulnerability operations to deliver a better pentest experience.

- Starts in days, not months
- Can be run on-demand for web, host, API and mobile
- Offers technical analysis that typically involves 50+ experts from a diverse community of 1,500+ vetted security researchers, not just one or two pentesters
- Blends automatic and adversarial human analysis with the platform's vulnerability management to maximize efficacy
- Produces real-time insight and control of current testing scope and activities with a standard set of reports that make the results actionable
- Can also leverage the SRT and Synack Platform to respond to additional testing requirements from unexpected vulnerabilities like Log4j

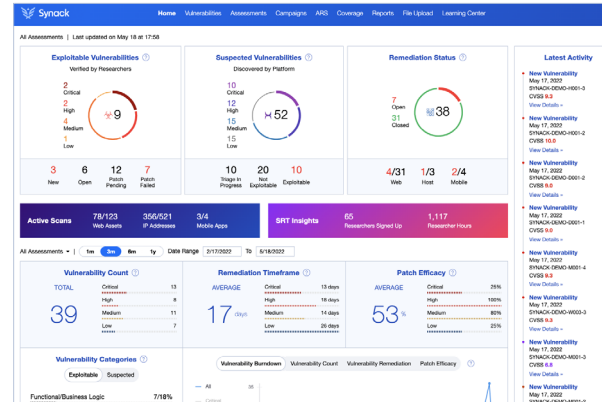
Synack Red Team (SRT)

The Synack Red Team (SRT) is a diverse, vetted and trusted community of the most talented security researchers across the globe. The SRT uses the Synack Platform to provide a world-class adversarial perspective on your web, host, mobile and API attack surface to find vulnerabilities that go undetected by automated scanners and traditional pentesters.



Synack Platform

The Synack Platform is our base subscription for each client, within which any additional testing performed is captured. It 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 standard pentesting and security processes. The following platform capabilities are instrumental in delivering a superior security testing experience.

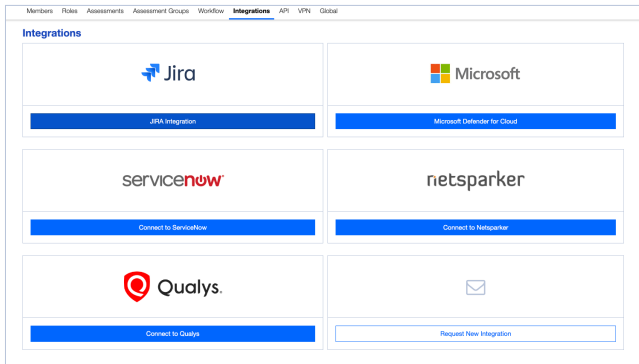
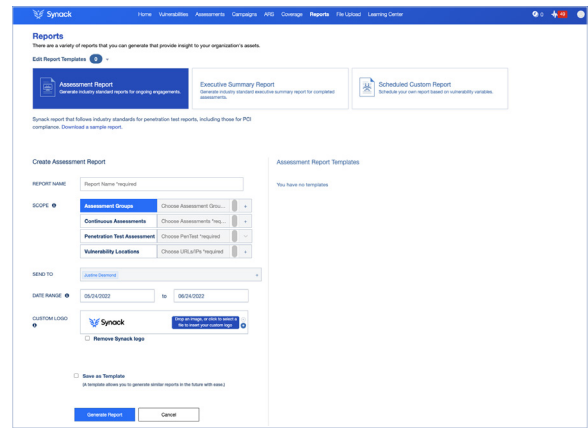


PILLAR	DESCRIPTION
Vulnerability Management	Read comprehensive summaries of exploitable vulnerability findings, communicate with researchers, and request patch verification all through convenient workflows.
Reporting and Analytics	Custom reports that outline vulnerability findings, test coverage analytics, 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.
Operations and 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 and 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 process with Microsoft, Splunk, Jira, and ServiceNow integrations.
Managed Community Access	There is no substitute for human ingenuity. The Synack Red Team, an elite community of security experts brings their diverse skills to all your offensive security testing needs.

Synack in action

Third-party testing and reporting for compliance

Compliance frameworks like PCI DSS 11.3 encourage frequent pentesting to keep up with significant infrastructure or application changes. Organizations may need to test for a longer duration to keep up with their dynamic environment. Synack's audit-ready reports include information on scope, testing information, vulnerability (description, severity, status, impact, CVSS) and more to share internally or externally.



Integrating testing into software development life cycles (SDLC)

As companies move to an agile model for software development they often release new features or products on a daily basis. Synack can test pre or post production and assist developers with quick remediation through integrations with Jira and ServiceNow. Synack can help you ship products on time by providing real-time reporting on vulnerabilities that matter.

Synack continuous testing product comparison

SYNACK TESTING FEATURES	SYNACK14	SYNACK90	SYNACK365
SRT Open Vuln Discovery (OVD)	7 Days	90 Days	365 Days
SmartScan	7 Days	90 Days	365 Days
Compliance and industry standards testing	Add-on checklist (OWASP or NIST800+53)	Add-on checklist (OWASP or NIST800+53)	Included

Synack Platform annual subscription

A Synack Platform annual subscription is required for all pentesting products and includes the following features.

Vulnerability Management – customer portal access, patch verification, RBAC.

Operations and Support – program and researcher management, operational support, vulnerability triage.

API and Integrations – Synack API, ServiceNow, Jira, Microsoft and more integrations.

Reporting and Real-time Analytics – real-time exploitable and susceptible vulnerabilities, ARS risk score, coverage analytics, audit-ready reports.

Managed Community Access – controls for researcher traffic, researcher payments, full testing transparency.