Synack

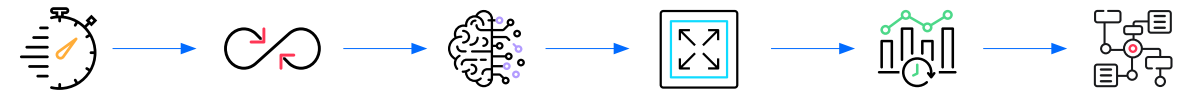
accenture

Accenture Federal Services

Synack/Accenture Federal Services Overview

Who is Synack?

Synack's Premier Security Testing Platform harnesses a talented, vetted community of security researchers and smart technology to deliver continuous penetration testing and vulnerability management with actionable results. We are committed to making the world more secure by closing the cybersecurity skills gap and giving organizations on-demand access to the most-trusted security researchers in the world.



Start in days, not months → Run on-demand or continuously → Tech & human intelligence → Breadth & depth of expertise → Real-time testing insights → Actionable vulnerabilities

Synack differentiators

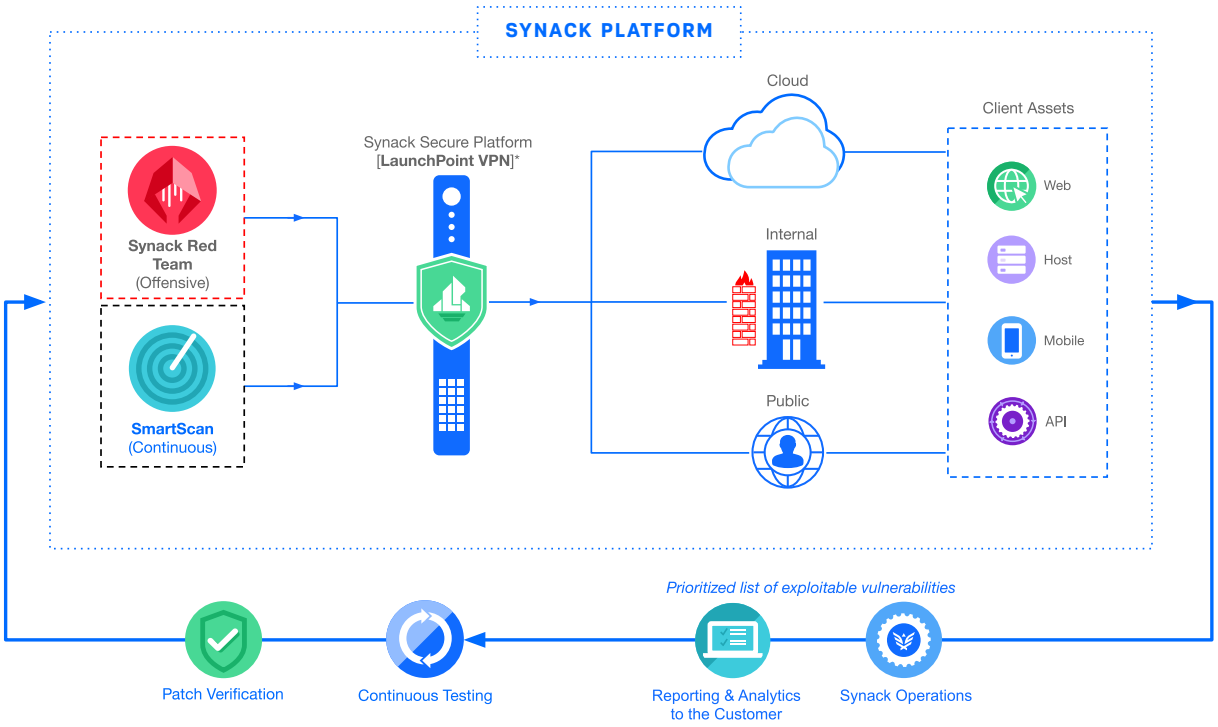
- Pentest immediately as new vulnerabilities emerge
- Elastic resources to scale & adjust scope of tests on-demand
- Offers near real-time insights & security fix recommendations
- Flexible remote deployment, get started in days not months
- Automated platform for continuous testing & patch verification
- Elite diverse security researchers using secure Synack platform
- Managed vulnerability disclosure program available in platform

Synack/Accenture joint value proposition

- Combine Synack's on-demand platform with Accenture's customer-specific expertise, assessments and consultancy for maximum security testing coverage and scale.
- Nimble but comprehensive security testing, adaptable to the unpredictable and unscheduled surges in threats to security posture.
- Offers a vetted and safe way to take advantage of the benefits of diversity security researchers.
- Integrations with SOC tools including ServiceNow, Jira and Splunk.

Associated Accenture Federal Services offerings

- Accenture Compliance Testing on scheduled basis (supplemented by dynamic surge testing by Synack)
- Accenture Security Assessments and Remediation (use exploits discovered by Synack to help target specific efforts)
- Accenture Managed Security Services (including Synack platform and on-demand Synack Red Team)



- All Synack assessments start with a SmartScan automated scanning analysis and results are sent to the Synack Red Team (SRT) as reconnaissance data and surfaced to the Synack Client Portal.
- The SRT is our global network of highly vetted, skilled and diverse security researchers who will provide adversarial analysis against an organization's in-scope assets.
- All SRT testing is performed through LaunchPoint® (LP), Synack's secure testing gateway that enables monitoring and control of all SRT activities.
- Only after connecting to LP and agreeing to the Rules of Engagement do SRT get access to scope and connect to the client in-scope asset(s).
- When a member of the SRT discovers a vulnerability in the target environment, it will be reported to Synack's Vulnerability Operations team for triage, reproduction and analysis.
- When a reported vulnerability presents a demonstrable risk, it is escalated to the client via Synack's secure platform (and available SIEM integrations) within one business day.
- Once a client has reviewed and remediated the finding, they can leverage the workflows in the client portal to submit a Patch Verification to tap the SRT for retesting and verification.