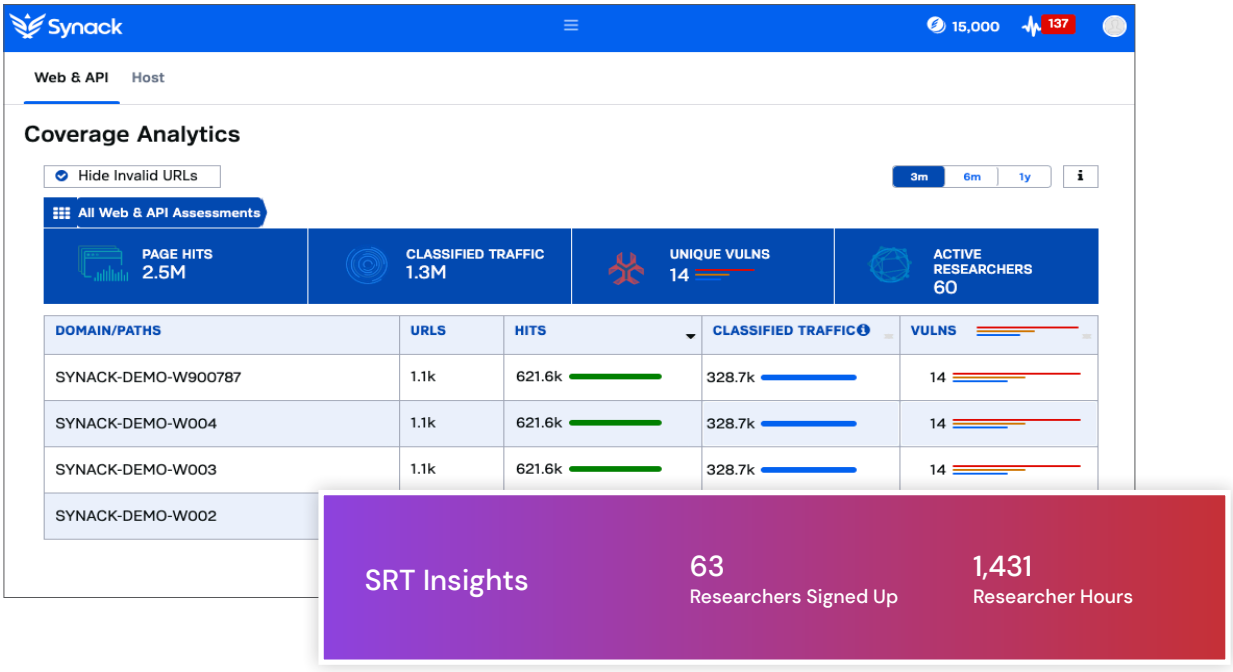
DATA SHEET

Test Controls on the Synack Platform

Unlike traditional penetration testing, the Synack Security Testing Platform provides full visibility and control essential for testing today's dynamic attack surface.

Synack Platform Test Controls

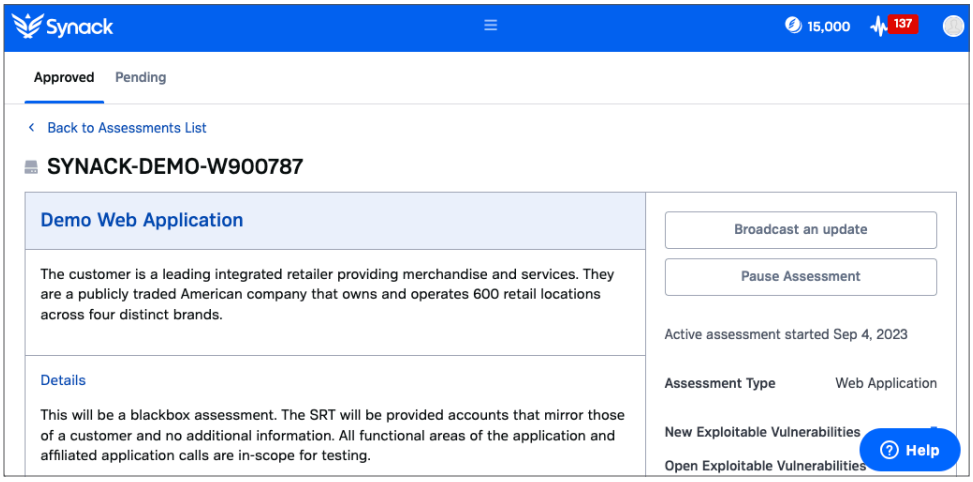
- **Pause testing:** Stop testing at the click of a button to avoid disruptions to production systems and customers
- **Identify source IP range:** Obtain a predictable source IP range for all testing and scanning activities, so you can separate trusted traffic from potential adversaries
- **Attack surface coverage:** Track which domains, subdomains, API endpoints and IPs have been tested during the assessment to ensure comprehensive coverage of your attack surface
- **Track Synack Red Team (SRT) hours:** Track and calculate researcher testing hours to discern researcher effort and return on your investment
- **Testing audit trail:** Full packet capture of all SRT testing and scanning activity for full accountability and trust
- **Data security:** Ensure data protection during the exploitation process with Synack-owned virtual desktop infrastructure for all SRT members



Key Test Control Features

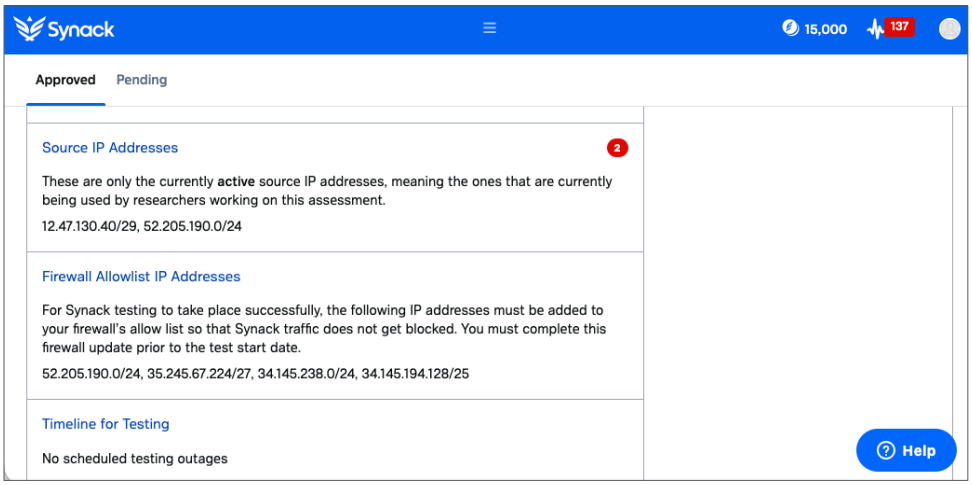
Pause Assessment

- Pause a single assessment at any time to avoid workplace or customer disruptions
- Synack will shut down all the infrastructure associated with the test and notify researchers in seconds



Firewall Allowable IP Address

- Synack's predictable IP source range helps you to identify friendly fire and reduces potential challenges of firewalls blocking researcher testing traffic

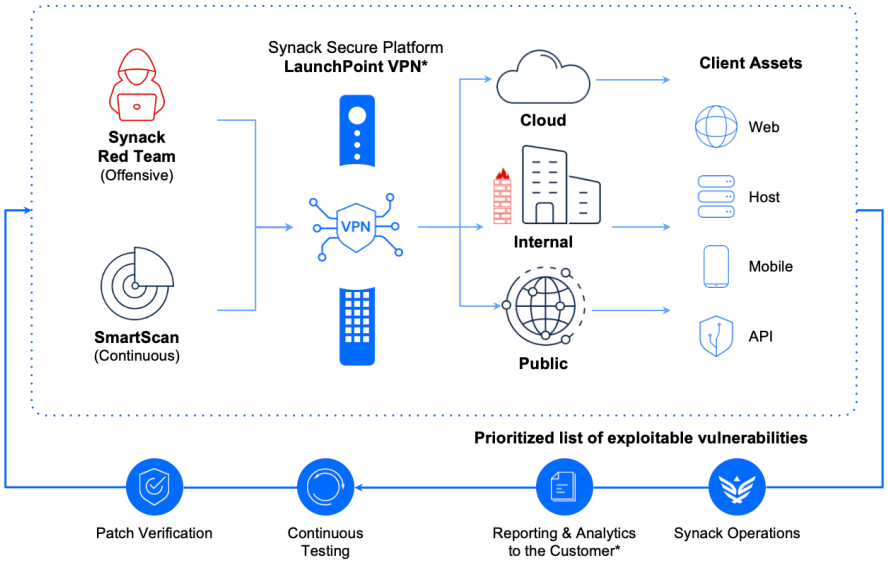


Coverage Analytics

Traditional pentests only provide vulnerabilities found and undocumented time estimates. Synack provides coverage analytics based on full packet capture of all scanning and testing conducted by SRT researchers. You will know what was tested, the total number of researchers testing your attack surface and the total number of hours spent testing. Our customers find coverage data is equally as helpful as vulnerabilities when considering a holistic view on their security.

How It Works

Synack's test controls are enabled by patented LaunchPoint™ technology. LaunchPoint provides access and management for researcher's entire testing activity, giving clients full auditability and control. All SRT sign into Launchpoint VPN for all testing activities, allowing them to securely use all their TTPs while delivering clients full packet capture of all testing. Synack's virtual desktop infrastructure augments LaunchPoint by providing cloud workspaces for researchers as an additional control.



What Is Synack Red Team Virtual Desktop Infrastructure?

SRT researchers conduct all testing in Synack-owned and controlled workspaces. These secure workspaces provide the following benefits for customers:

- Testing data is stored on Synack-owned endpoints
- Ensures customer data protection during the exploitation process
- Synack-owned callback servers for exploit methodologies that require them
- Site-to-site VPN connectivity