Accelerate Penetration Testing for the Cloud

Moving to the Cloud is Not A Magical Security Fix

The same protections and vulnerabilities that may exist in your software become accessible via the cloud—for good and for ill. The comfort and clarity of a network perimeter disappears with cloud. Control mechanisms—

such as firewalls—have less relevance in the cloud. And with public cloud growing fast (23.1% growth rate for 2021[1]), there are more adversaries looking to fresh targets newly arrived in the cloud.

Cloud Aware Security Testing Can Help

Security testing in the cloud needs to be cloud aware. Synack offers testing options that take into account the requirements of cloud testing.

Requirements of Cloud Testing:

- **Humans + Technology:** Both Synack researchers and software understand cloud
- **Expertise:** Synack Red Team (SRT) members have hacked hundreds of cloud environments
- **Dynamic:** Because assets appear and disappear constantly, the scope must respond in turn, so that researchers scan the right assets (ie: IP addresses)
- **Flexible:** Scope can be defined by API-based asset enumeration AND specified targets
- **Comprehensive:** Allows access to public and virtual private cloud (VPC) and network (VPN) assets for complete testing
- **Throttled:** Does not trip rate limits built into most public cloud platforms
- **Integrated:** Work seamlessly with common public cloud vendors (Amazon, Google Cloud Platform (GCP), and Microsoft Azure)

Synack can bring the power and creativity of security testing to your cloud assets via a variety of options

Synack Cloud Testing Offerings:

DISCOVER Vulnerability Discovery	**CERTIFY** Penetration Testing	**SYNACK365** Penetration Testing 365
Leveraging the Synack Platform, Discover finds vulnerabilities by setting creative hackers on an unstructured hunt in web, mobile, and host/ infrastructure assets.	In addition to all the features of Discover, Certify yields documented proof that specific security checks, such as OWASP or PCI, were completed at a point in time.	Year-round human testing, augmented by SmartScan, with compliance- friendly test. Synack365 provides active, SRT-led testing and coverage for 365 days of the year.
TIME OF ENGAGEMENT		
Two weeks of Testing	**Two weeks of Testing + Continuous SmartScan**	**24/7/365 Testing + Continuous SmartScan**

[1] Source: Gartner, Worldwide Public Cloud Revenue Forecast, April 2021

How Does It Work?

Your Synack representative helps you through all the steps needed to enumerate your cloud assets and allow Synack testing and cloud scanning to begin. Synack's Security Platform, using SmartScan, continuously scans your cloud assets (host, application and/or mobile) for potential vulnerabilities and engages the SRT to triage and validate so we don't waste your valuable time on low quality intelligence. The Platform understands the nuances of cloud infrastructure (such as Access Keys, Identity Management, short-lived VMs) and networks (such as DNS routing, virtual instances, storage) to effectively perform reconnaissance and scan for weaknesses. Secure site-to-site gateway capability that doesn't rely on voluntary traffic tagging provides secure and limited access to a set of pre-approved researchers. As vulnerabilities and weaknesses are found, they are triaged and reported to you. With the Synack Security Platform, you also receive results of individual checks for known weaknesses as soon as they are made.

Inventory Cloud Assets

SCOPE TESTING

Enumerated assets (via AWS Key, Credential JSON, Subscription ID, etc.) + Client Provided List

SYNACK SMARTSCAN-POWERED RECON

Find suspected vulnerabilities

SRT VULNERABILITY DISCOVERY

Bug Bounty and Missions Rewards

PENETRATION TESTING

Document checks that don't find vulnerabilities

CONSOLIDATED REPORT

Audit quality customizable reports available on-demand, human-augmented analysis

Synack Features

Top, Trusted Talent: Synack provides access to the world's best, most trusted security talent. Vetting that goes well beyond ID and background checks.

Cloud Integration: Synack testing has out of the box integration with major cloud providers— AWS, Azure, and GCP, and Oracle Cloud— no notice needed!

Dynamic Cloud Asset Inventory: Your cloud assets are always up-to-date. When an asset is added or removed, it is immediately known to Synack for scanning and security testing.

Own your Vulnerability Intellectual Property: Vulnerabilities found by the Synack Red Team are contractually conveyed to you—not Synack and not the Researcher.

Cloud Traffic Control: Research traffic is under client control—pausable instantly for any reason, such as to diagnose other cloud performance issues.

Full Service and Support: Synack Operations is your partner for every step in the intricate world of working and paying security researchers.

Scalable Scanning, without Noise: Synack's Hydra conducts attack surface recon and scans for potential vulnerabilities for the Synack Red Team and Synack Operations to verify. Our SmartScan product triages and removes all noise from the findings, enhancing the efficiency of security teams.

Divert Research from Public Internet: Research traffic is diverted to Synack's LaunchPoint VPN gateway for security and reliability, minimizing the strain on your production systems.

Measure Testing in Progress: Unlike standard Penetration Testing, Synack measures the aggregate time and volume of activity researchers spend performing work.

Analytics: Spot trends that could result in unfound vulnerabilities living longer than necessary.

Dashboards: See program status at a glance, including research hours logged, researchers engaged, patch statuses, vulnerability status, burndown chart, and more. For example, see S3 call-out data for Web Apps in AWS.

Detailed Report: Reports on demand, including an expert- written summary, results found to date, including methodology, targets, and results.