Security Testing for Cloud Migration

Assure your customers' transformation and modernization efforts

Cloud chaos

Digital transformation and modernization have introduced new security and compliance risk for organizations. Public cloud is growing fast (23.1% growth rate for 2021[1]), and your customers are quickly migrating applications to be hosted by cloud providers such as Azure, AWS and GCP. Vulnerabilities that may exist in customer software then become accessible via the cloud, and at the same time the comfort and clarity afforded by traditional enterprise perimeter security defenses become less relevant. Adversaries are looking to exploit freshly arrived targets in the cloud, leaving your customers uncertain of their security posture.

As a partner in your customers' cloud migration efforts, you offer a variety of new defensive security architectures and solutions aligned to cloud hosted applications such as Zero Trust Network Access, Cloud Secure Web Gateway, Cloud Security Posture Management, Web Application & API Security, and Extended Detection and Response. You might be reselling such solutions that are offered by your traditional enterprise security partners, new cloud-centric vendors, or you may find yourself competing with solutions offered directly by the cloud providers themselves.

Our solution

Synack offers offensive security testing which validates whether applications are secure, regardless of which cloud provider is hosting them or which defensive security tools are used to protect them.

Synack blends the benefits of automated intelligent scanning with on-demand access to our vetted, expert team of over 1,500 security researchers, offering thorough testing and validation of security posture in the cloud.

Synack premier security testing is architected with cloud security in mind and does not depend on static access to infrastructure that traditional security testing solutions require.

Synack testing offers specific recommendations on how to close security gaps, along with patch verification, to assure that implemented fixes have been successful.

Synack partners can offer offensive testing alongside defensive security tools, specific cloud migration efforts or as a continuous security testing service.

Regardless of the defensive security architectures that your customers choose, each customer will have a common need to validate and be assured that the cloud migrated applications are indeed secure.

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

Partner benefits

By offering Synack Security Testing to your customers, you can assure the integrity of their cloud migration efforts while bolstering your revenue streams with an offering that is agnostic to the demands and constraints of any one individual cloud provider.

SYNACK OFFER	PARTNER BENEFIT
Increase customer confidence in security of cloud migrations	Increase in scope and sales for additional migrations
Accelerate cloud adoption by validating security faster	Stay competitive and recognize revenue faster
Measure improvements in attacker resistance	Proof of value facilitates follow on engagements
Validate security defenses and guide best practices	Proof of value in security tools sold, paid expansion and renewal
Offensive security testing for cloud	Additional revenue opportunity beyond defensive security
Recommendations to fix and remediate security gaps	Opportunity to add additional partner consultancy services
Cloud-agnostic testing architecture	Co-exist and complement any cloud provider features used
Test any customer security defenses	Compatible to test any security tools which you sell
Continuous security testing	Build Annual Recurring Revenue (ARR)
Integrations and API	Fits existing customer workflows, reducing friction of adoption

Cloud-aware security testing can help your customers

Synack offers 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 (e.g., 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: Microsoft Azure, Amazon and Google Cloud Platform (GCP)

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

Synack cloud testing offerings examples

SYNACK14 Vulnerability Discovery	SYNACK90 Strategic Security Testing	SYNACK365 Continuous Security Testing
Leveraging the Synack Platform, Synack14 finds vulnerabilities by setting creative hackers on an unstructured hunt in web, mobile, and host/ infrastructure assets.	In-depth security testing with Synack90 includes continuous SmartScan, pentesting, recommendations for remediation and re-testing to verify succesful patching.	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	90 days of testing	365 days of testing

How does it work?

Your Synack representative helps your customer through all the steps needed to enumerate their cloud assets and allow Synack testing and cloud scanning to begin. The Synack Platform, using SmartScan, continuously scans cloud assets (host, application and/or mobile) for potential vulnerabilities and engages the SRT to triage and validate so we don't waste 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. With the the Synack Platform, results of individual checks for known weaknesses are provided as soon as they are made.

Inventory and test 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

Test, confirm and detail exploitable 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.

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 SRT are contractually conveyed to the customer—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: The Synack Platform conducts attack surface recon and scans for potential vulnerabilities for the SRT and then Synack Operations to verify.

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.

Continuous Improvement: Attacker Resistance Score provides a realistic assessment of risk for specific customer assets, along with historical reporting to track improvement to security posture.

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.

SOC Tool Integrations: Pre-built modules and API allows integration with leading SOC tools including Microsoft, Splunk, ServiceNow, Jira and more.

To learn more about the benefits of Synack partnership please contact us at channel@synack.com.