# Penetration Testing in the Cloud

## Reduce Migration Risk with Dedicated Host and Application Security Testing

## Migrations

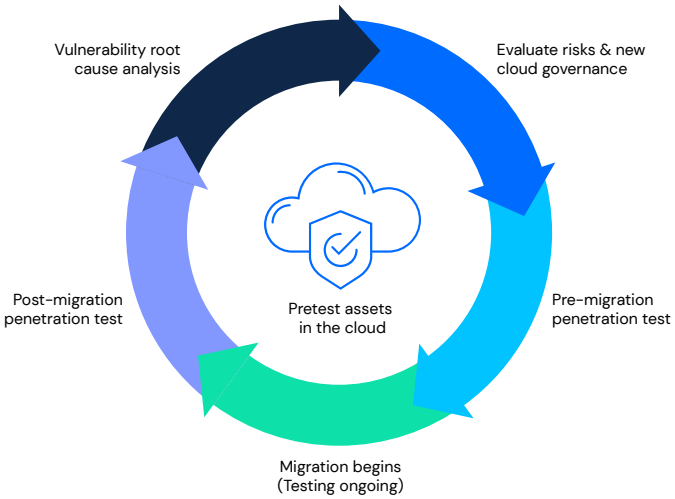
### A Natural Breeding Ground for Vulnerabilities

Some of the most exploitable vulnerabilities observed in cloud environments have originated from misconfigurations related to migration from on-premise to cloud, or from one cloud environment to another. And, according to the Wall Street Journal, "misconfigurations have [also] become one of the most common security issues when deploying new cloud-based applications." Infrastructure and applications hosted in the cloud can be penetration tested before, during and after a deployment or migration to minimize chances of exposure.

## Key Takeaways

### Migration to the Cloud

- Lifting and shifting a vulnerable application from on-premise to the cloud, or from one cloud container to another, poses increased risk due to an expanded attack surface. Remediation of vulnerabilities prior to migration is an important way to reduce exposure.
- Migrating an asset to the cloud can introduce new cloud configuration-related vulnerabilities that should be tested and remediated immediately.
- Traditional and scheduled pre- and post-migration pentesting is cumbersome and operationally complex because cloud migration usually takes place via a rolling process. Apps and systems are migrated at different times, and updates are frequent — necessitating a more continuous testing approach.
- Those responsible for application security or infrastructure security, including cloud security engineers, are using the Synack Platform to deploy continuous and/or on-demand testing that adapts to the dynamics of cloud migration, reducing the risk of vulnerabilities within the process.




*Pentesting for hosts and applications in the cloud.*

The Synack Platform combines automation tools with human-led security testing, via the Synack Red Team (SRT), to continuously reduce risk for organizations during and after cloud migrations.

## Get Started

# Pentesting in the Cloud: Applications & Infrastructure

The Synack Platform enables continuous security testing of your cloud assets (hosts and/or applications) for potential vulnerabilities. The Synack Red Team, a group of 1,500+ vetted security researchers, is then engaged to test and triage exploitable vulnerabilities and provide detailed reports of findings along with recommendations for remediation. This human-augmented approach greatly reduces alert noise compared with automated scanning alone.

Your Synack representative works with you to enumerate your cloud assets and allow Synack's pentesting in the cloud to begin. The platform is designed for 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 capabilities that don't rely on voluntary traffic tagging give 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 Platform, you also receive results of individual checks for known weaknesses as soon as they are made.

## Steps in a Synack Cloud Security Test

**Scope Testing**

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

**Integrated Vulnerability Scanning**

Recon to find suspected vulnerabilities

**Vulnerability Discovery**

Community of vetted researchers incentivized to test & share findings

**Penetration Testing**

Documented testing for weaknesses & vulnerabilities

**Consolidated Report**

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

## The Synack Cloud Security Benchmark Checklist

The checklist examines many categories of cloud vulnerabilities. Examples of these appear below.

### Cloud Security Benchmark Checklist – commonly tested categories

- ✓ API Vulnerabilities
- ✓ Authentication
- ✓ Authorization
- ✓ Injection
- ✓ Code injection

### Common vulnerabilities found by Synack testing hosts and apps in cloud environments

- ✓ Account enumeration & guessable user account code injections
- ✓ Cross-Site Request Forgery (CSRF)
- ✓ Directory traversal/files
- ✓ Privilege escalation
- ✓ Unexpected file types upload

## Pentesting in the Cloud: A Benefit of Testing on the Synack Platform

The Synack Platform is the central point of control and visibility for customers. The platform capabilities below highlight the ways that Synack delivers premier security testing.

| 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 satisifies 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 vulnearability 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. |

### Learn more

To learn more about the Synack Platform, contact your Synack representative or reach out to us at synack.com/demo.