DATA SHEET

Cloud Adoption Framework for Azure

Accelerate and Secure Workload Migrations to the Cloud with Synack

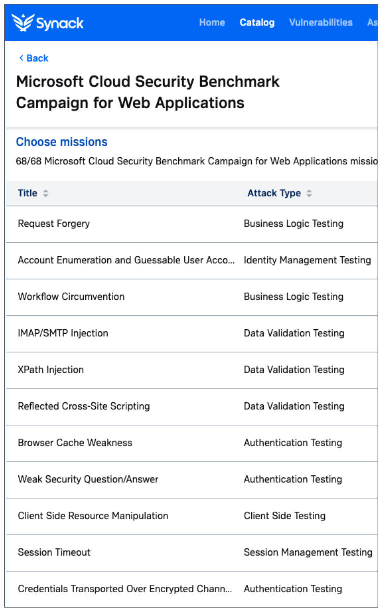
The Microsoft Cloud Adoption Framework for Azure is a widely recommended and used methodology for cloud migrations that provides guidance to help prepare for and execute workload migration efforts smoothly. Ensuring that migrated workloads remain secure is a critical component of these efforts. The migration process includes four stages: **prepare, assess, deploy and release.**

Synack's suite of security testing options can be applied at each of the four stages, helping customer confidence and accelerating their workload migration to the cloud. Customers have seen workload migration times accelerate by up to 20% when wrapping Synack's cloud security testing into their migration approach.

Prepare

Before planning individual workload migrations, you must ready your organization and cloud resources to support the migration. An Azure landing zone is an environment that follows key design principles across eight design areas, including security. The security design principle specifies adherence to the Microsoft Cloud Security Benchmark (MCSB), a set of security controls and services recommendations.

Synack testing verifies adherence to MCSB. Use Synack's Microsoft Cloud Security Benchmark missions to test the landing zone for adequate protections, then leverage Microsoft Azure Security Controls to update and protect the environment.



Microsoft Cloud Security Benchmark Campaign for Web Applications

Choose missions

68/68 Microsoft Cloud Security Benchmark Campaign for Web Applications missio

Title	Attack Type
Request Forgery	Business Logic Testing
Account Enumeration and Guessable User Acco...	Identity Management Testing
Workflow Circumvention	Business Logic Testing
IMAP/SMTP Injection	Data Validation Testing
XPath Injection	Data Validation Testing
Reflected Cross-Site Scripting	Data Validation Testing
Browser Cache Weakness	Authentication Testing
Weak Security Question/Answer	Authentication Testing
Client Side Resource Manipulation	Client Side Testing
Session Timeout	Session Management Testing
Credentials Transported Over Encrypted Chann...	Authentication Testing

Customer Use Case

A highly regulated energy provider was planning their migration to the cloud and needed to create secure, templatized landing zones and migrate hundreds of workloads to the cloud. Government regulators required detailed security control planning and reported security assurance of the landing zone in advance of any actual workload migration.

Synack provided in-depth security testing of initial landing zone templates and associated controls, providing continuous penetration testing for attacker threats and configuration vulnerabilities as the landing zones were built and the controls were tuned. Testing for lateral and/or horizontal flow between the management groups, subscriptions and workloads was particularly important to securing the landing zone as regulators were interested in vulnerabilities that could result in data exfiltration and identity compromise.

Assess Workloads

In the assess phase, you evaluate the readiness of your workload(s) and plan for the migrated state. An occasionally overlooked component of this evaluation is pentesting of the workload to check for vulnerabilities that may be exploitable when exposed to the cloud attack surface. For example, you should test application workloads for critical authentication and authorization schema bypass issues, and then tune AzureMFA and EntraID controls based on those test findings.

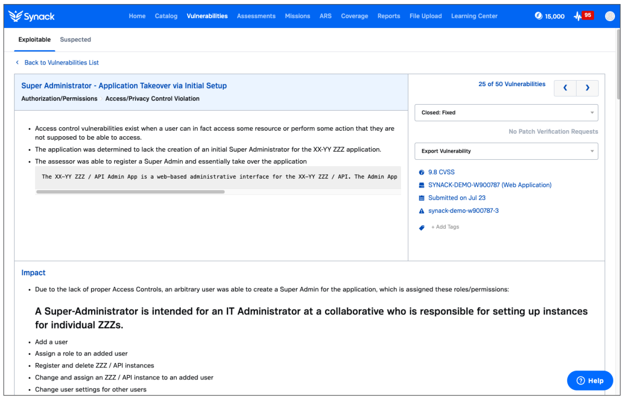
Synack [Penetration Testing as a Service](#) (PTaaS) is used to evaluate the security, health and readiness of an application workload pre-migration. The customer receives a detailed report of exploitable vulnerabilities found on pre-migration workload assets, as well as recommendations to close security gaps.

Customer Use Case

Synack helps F50 bank safely migrate heavily regulated on-premise workloads to the cloud.

The bank used Synack authenticated web application testing to:

1. Identify and fix issues pre-migration
2. Detect and mitigate new vulnerabilities that arose during migration
3. Test and report on the efficacy of the new cloud security controls for regulators



Super Administrator - Application Takeover via Initial Setup

Authorization/Permissions › Access/Privacy Control Violation

- Access control vulnerabilities exist when a user can in fact access some resource or perform some action that they are not supposed to be able to access.
- The application was determined to lack the creation of an initial Super Administrator for the XX-YY ZZZ application.
- The assessor was able to register a Super Admin and essentially take over the application

```
The XX-YY ZZZ / API Admin App is a web-based administrative interface for the XX-YY ZZZ / API. The Admin App
```

Closed: Fixed

No Patch Verification Requests

9.8 CVSS

SYNACK-DEMO-W900787 (Web Application)

Submitted on Jul 23

synack-demo-w900787-3

Impact

- Due to the lack of proper Access Controls, an arbitrary user was able to create a Super Admin for the application, which is assigned these roles/permissions:

A Super-Administrator is intended for an IT Administrator at a collaborative who is responsible for setting up instances for individual ZZZs.

- Add a user
- Assign a role to an added user
- Register and delete ZZZ / API instances
- Change and assign an ZZZ / API instance to an added user
- Change user settings for other users

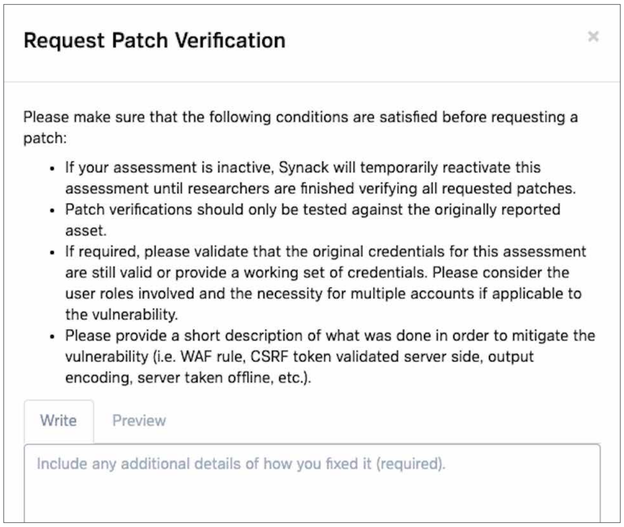
Deploy

An important component of this stage of the Cloud Adoption Framework is to remediate workload assets for security incompatibilities identified during the assessment. In this phase you test for configuration and deployment management issues to minimize risk exposure and then quickly mitigate vulnerabilities using Azure Defender for Cloud.

Synack's PTaaS includes patch verification services to re-test workloads, confirming that workload exploitable vulnerabilities have been successfully remediated.

Large E-commerce customer example

This company manages a massive external attack surface, using Synack's patch verification minimizes risk exposure to identified vulnerabilities across their cloud environments. Through the Synack Platform they can now patch issues and retest the fixed endpoint in minutes, instead of days, weeks or months. When leveraging Synack, average vulnerability remediation timeframe improved by 48% year-over-year.



Request Patch Verification

Please make sure that the following conditions are satisfied before requesting a patch:

- If your assessment is inactive, Synack will temporarily reactivate this assessment until researchers are finished verifying all requested patches.
- Patch verifications should only be tested against the originally reported asset.
- If required, please validate that the original credentials for this assessment are still valid or provide a working set of credentials. Please consider the user roles involved and the necessity for multiple accounts if applicable to the vulnerability.
- Please provide a short description of what was done in order to mitigate the vulnerability (i.e. WAF rule, CSRF token validated server side, output encoding, server taken offline, etc.).

Include any additional details of how you fixed it (required).

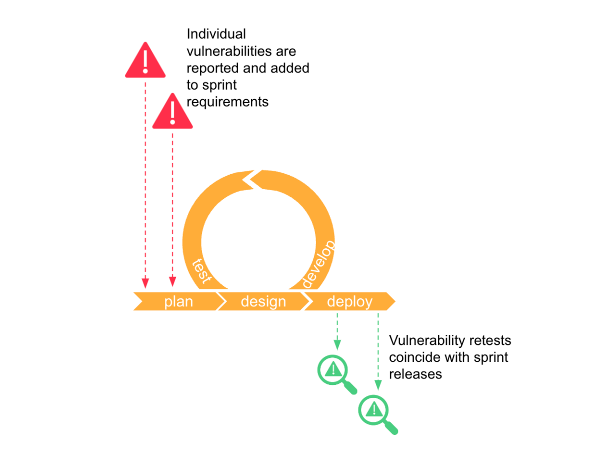
Release

This phase guides you through releasing your deployed workloads to production use. It is important to re-test and verify that the workloads remain secure after exposure to production use.

Synack PTaaS allows for re-testing of application workloads post migration to identify any inconsistencies or vulnerabilities that may have surfaced as a result of migration or as development operations teams are running sprint cycles and pushing software updates. Synack PTaaS may also be used to monitor and regularly re-test workloads for exposure to new exploitable cyber vulnerabilities present in the wild, such as clickjacking and SQL injection. Customers also have the option to integrate vulnerability findings into Microsoft Sentinel, Azure DevOps and Microsoft Defender for Cloud for efficient handling by their security operations team processes.

Fortune 1000 Retailer example

Increasing digital sales and adoption of online apps necessitated this organization’s team to roll out code across one or all of their geographes at least every two weeks. Any new and unchecked vulnerability could trigger costly business downtime. Because of the continuous scalable Synack model, their security team was able to put a high volume of tests into action at an aggressive cadence. Further, their development and security teams could work together dynamically.


Individual vulnerabilities are reported and added to sprint requirements
test
develop
plan
design
deploy
Vulnerability retests coincide with sprint releases

Conclusion

Synack is a tool to help adherence to security related components of the Cloud Adoption Framework, which builds confidence in cloud workload migrations. The following Synack products are mentioned in this document:

- **Synack Platform** (*use at all 4 stages to manage and view data*)
  - Standard (Product Code: SYNACK-PLATFORM-01)
  - Premium (Product Code: SYNACK-PLATFORM-02)
- **Synack Microsoft Cloud Security Benchmark Missions** (*use at Prepare phase*)
  - Web Testing (Product Code: SYN-CT-AZUREWEB-01)
  - Host Testing (Product Code: SYN-CT-AZUREHOST-01)
- **Synack PTaaS** (*use at Access/Deploy/Release phases*)
  (available in different time periods and options depending on project scope & complexity, please contact us for more details)
  - Synack-90 (Product Code: 365-APP-ENT)
  - Synack-365 (Product Code: 90-APP-ENT)

Synack is available for purchase via Azure Marketplace.

Synack is a Microsoft Intelligence Security Association member and Microsoft partner.

For further information, connect to the Synack team microsoft@synack.com