Synack

Member of
Microsoft Intelligent
Security Association
Microsoft

Manage Synack Pentest Results from Microsoft Defender for Cloud

Synack and Microsoft Defender for Cloud — a powerful security partnership

Keeping your hybrid cloud safe from cyber criminals is a daunting task. Hackers are constantly searching for vulnerabilities in your cloud hosted assets that they can exploit to gain access to your core systems. Microsoft Defender for Cloud helps protect against threats by providing tools to manage your organization's security policy and compliance. It allows you to monitor for misconfigurations and known vulnerabilities, giving security engineers and managers a real time view of the security state of their Microsoft Azure cloud in simplified dashboards.

But there is a critical piece missing in this security view. You need to be able to validate those misconfigurations and create attack vectors to search for and report vulnerabilities at the network layer as well as internally in your cloud environment. Synack, the premier security testing platform powered by a skilled and trusted community of global security researchers, provides continuous pentesting and vulnerability discovery with actionable results. These results are reported to Microsoft Defender for Cloud where the vulnerabilities can be investigated and resolved.

Vulnerability management optimization in Microsoft Azure

Via Synack's integration with Microsoft Defender for Cloud, you can have the results of your Synack pentest automatically sent to and displayed in a Microsoft Defender for Cloud custom workbook. This means that security engineers and managers already familiar with Microsoft Defender for Cloud dashboards and displays don't have to learn another tool's display format to view and act on vulnerability information.

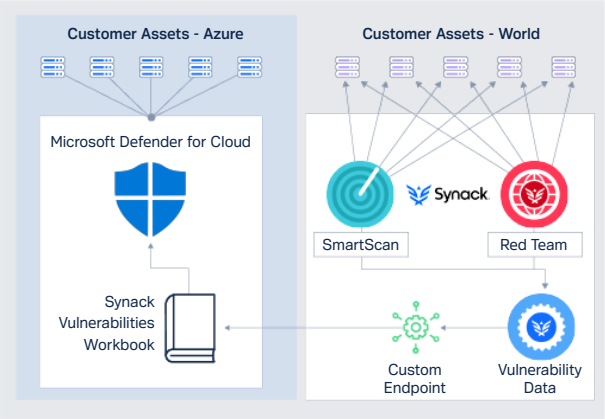
As part of Microsoft and Synack's global partnership, your Synack assessment results are automatically populated into Microsoft Defender for Cloud through one of our easy Microsoft Platform integrations.

- Integrate Synack discovered vulnerability data into your Microsoft Defender for Cloud instance to streamline your vulnerability management processes.
- Help protect your dynamic cloud environment with Synack pentests and continuous security testing through an integration with Microsoft Azure.
- Automatically send your Synack assessment results to Microsoft Defender for Cloud with our easy integration.
- View and manage your network vulnerability status in familiar Microsoft Defender for Cloud displays.

Integration

Synack provides a custom Microsoft Azure workbook with Synack vulnerability data within your Microsoft Defender for Cloud. A backend application hosted by Synack provides a custom endpoint for the workbook. Synack provides the default template for the Synack Vulnerabilities workbook, allowing the end user to further modify the look of the Workbook or use the endpoint to create new workbooks.

Synack makes the integration simple. A Synack API token must first be created in order to deploy the Synack workbook ARM (Microsoft Azure Resource Manager) template with Microsoft Defender for Cloud.



The workbook is then made accessible in Microsoft Defender for Cloud. Each time Synack performs a pentest, the results will be displayed in the Microsoft Defender for Cloud Workbook.

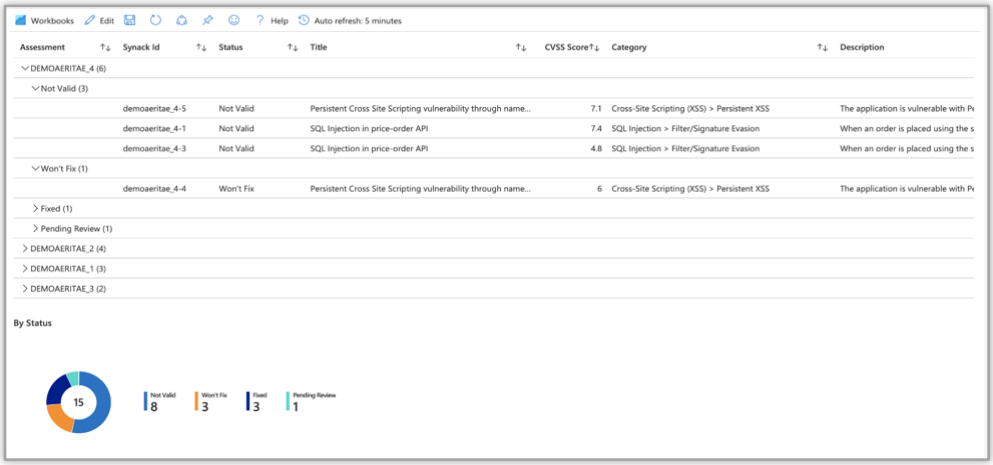
View Synack assessment results in Microsoft Defender for Cloud

More than 90% of cloud security issues are directly caused by misconfigurations.[1] Synack helps you discover exploitable vulnerabilities that may result from these misconfigurations. Authentication session vulnerabilities, including default credentials, directory content and code injection, make up 40% of Synack reported cloud exploits. Now you can view and manage these vulnerabilities right in Microsoft Defender for Cloud.

With this integration, customers can automatically sync their data from the Synack Platform to Microsoft Defender for Cloud. All vulnerability information output becomes centralized and leverages formats widely used by Microsoft Azure users, enabling security engineers and managers to efficiently monitor the overall network security posture.

Synack manually calculates and assigns each discovered vulnerability with a CVSS score as part of the robust quality assurance review included in each assessment. Any vulnerabilities identified are displayed in the Microsoft Defender for Cloud Workbook. Security teams can view the vulnerability status in the Workbook and take appropriate action. Authorized users are able to request additional information on any vulnerability identified and made readily available in the Synack Platform.

Vulnerabilities list in Microsoft Defender for Cloud Workbook



Learn more

Contact your Synack/Microsoft Security representative at microsoft@synack.com

1. XM Cyber, "What is Cloud Security Posture Management," 2021, https://www.xmcyber.com/what-is-cloud-security-posture-management/