# Continuous Security Testing for Digital Transformation

How strategic penetration testing keeps your business prepared in the evolving digital landscape

Synack

Microsoft Security

# How can you ensure your security is keeping up with your transformation?

## Locate security gaps in real time as your business grows

As businesses evolve, they are continually integrating new technologies into their digital landscape. These solutions offer exciting innovations and efficiencies, but they can also carry risk if not properly configured into the organization's digital environment. Business leaders recognize the gap between the complex digital threat landscape and their ability to identify vulnerabilities. They also understand that a strong security posture is essential to maintaining customer trust and complying with the latest regulatory requirements.

## Contents

**600%** increase in cyberattacks due to the transitional requirements posed by the pandemic.[1]

**65%** of board members feel their organization is at risk of a cyberattack.[2]

**80%** of security incidents can be traced to a few missing elements that could be addressed through modern security approaches.[3]

## Prepare your business to handle evolving threats and requirements with experienced security testing

By combining Synack Security Testing together with the Microsoft Security product portfolio, you are better prepared to proactively identify emerging vulnerabilities that are putting your business at risk. Synack offers scalable penetration testing conducted by a vetted team of security experts and a premier testing platform that integrates seamlessly with the Microsoft Security products you already use.

### Prepare for the unexpected

Stay alert in a rapidly changing cloud ecosystem.

Read More

### Act swiftly to address gaps

Identify and address vulnerabilities in one integrated process.

Read More

### Maintain regulatory compliance

Meet compliance requirements in multiple jurisdictions.

Read More

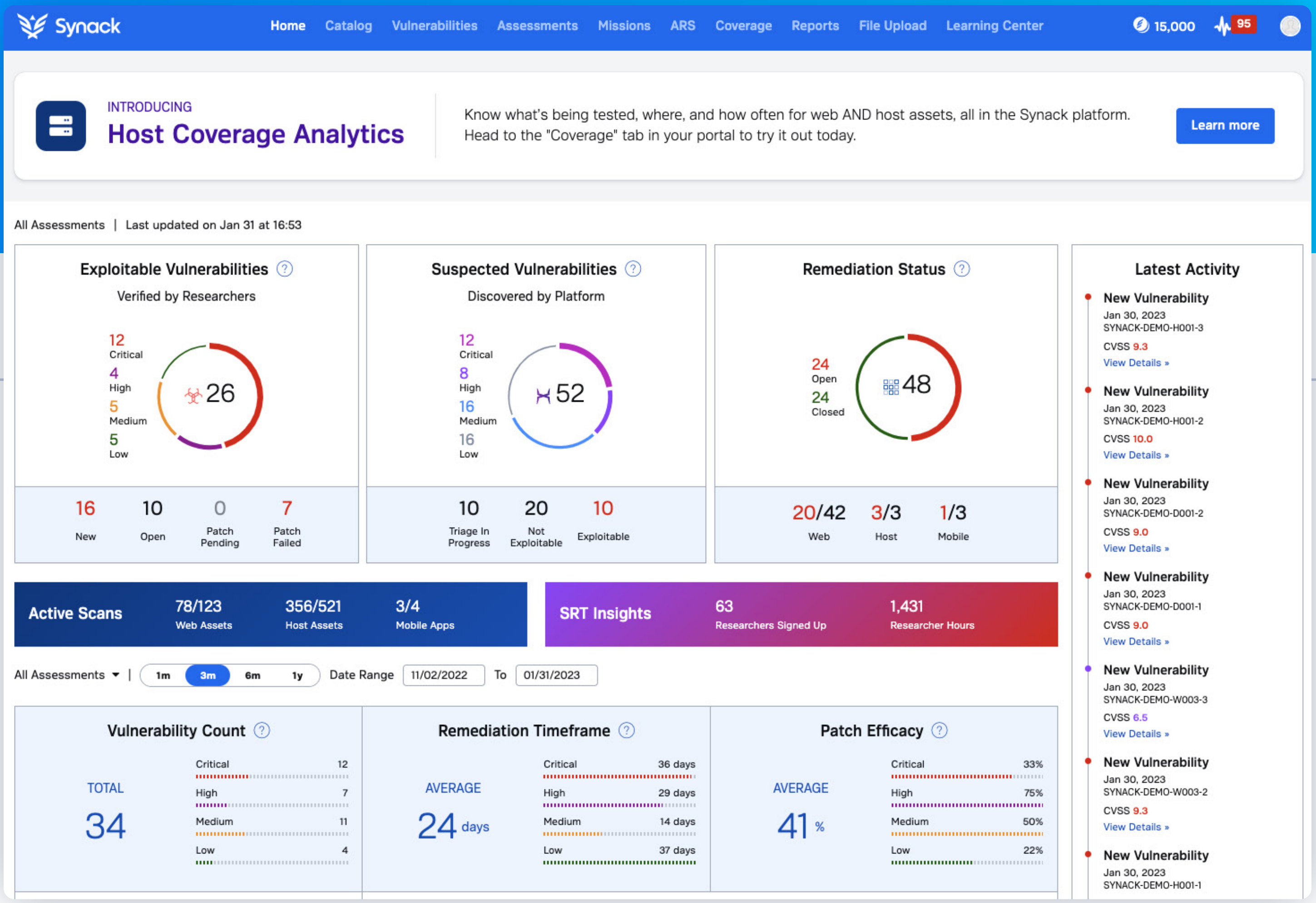
# Prepare for the unexpected

## Our digital ecosystems are changing at record speed and security teams are struggling to keep up

Mobile workforces, cloud migrations, and new innovations are just some of the trends pushing organizations through rapid digital transformation. With the sheer volume and speed of change, IT and security teams are stretched thin and lack the time and resources to effectively test their security on a regular basis. In this environment, it's no wonder that more than 90% of cloud security issues are directly caused by misconfigurations.[4]

Synack offers both continuous and on-demand penetration testing through an integrated platform that has the capacity to scale to meet your business needs. The Synack Platform is the central point of visibility and control that integrates the adversarial analysis from external security researchers into your standardized security and testing processes. A combination of automated processes and human insights from a team of trusted security experts offers effective testing that identifies vulnerabilities in days, not months.

# See exploitable vulnerabilities and improvements to your security posture in the Synack Platform



INTRODUCING
**Host Coverage Analytics**

Know what's being tested, where, and how often for web AND host assets, all in the Synack platform. Head to the "Coverage" tab in your portal to try it out today.

All Assessments | Last updated on Jan 31 at 16:53

**Exploitable Vulnerabilities**
Verified by Researchers

12 Critical
4 High
5 Medium
5 Low
26

| 16 | 10 | 0 | 7 |
|---|---|---|---|
| New | Open | Patch Pending | Patch Failed |

**Suspected Vulnerabilities**
Discovered by Platform

12 Critical
8 High
16 Medium
16 Low
52

| 10 | 20 | 10 |
|---|---|---|
| Triage In Progress | Not Exploitable | Exploitable |

**Remediation Status**

24 Open
24 Closed
48

| 20/42 | 3/3 | 1/3 |
|---|---|---|
| Web | Host | Mobile |

**Latest Activity**

New Vulnerability
Jan 30, 2023
SYNACK-DEMO-H001-3
CVSS 9.3
View Details »

New Vulnerability
Jan 30, 2023
SYNACK-DEMO-H001-2
CVSS 10.0
View Details »

New Vulnerability
Jan 30, 2023
SYNACK-DEMO-D001-2
CVSS 9.0
View Details »

New Vulnerability
Jan 30, 2023
SYNACK-DEMO-D001-1
CVSS 9.0
View Details »

New Vulnerability
Jan 30, 2023
SYNACK-DEMO-W003-3
CVSS 6.5
View Details »

New Vulnerability
Jan 30, 2023
SYNACK-DEMO-W003-2
CVSS 9.3
View Details »

New Vulnerability
Jan 30, 2023
SYNACK-DEMO-H001-1

**Active Scans**
78/123 Web Assets
356/521 Host Assets
3/4 Mobile Apps

**SRT Insights**
63 Researchers Signed Up
1,431 Researcher Hours

Date Range 11/02/2022 To 01/31/2023

**Vulnerability Count**
TOTAL 34

| | |
|---|---|
| Critical | 12 |
| High | 7 |
| Medium | 11 |
| Low | 4 |

**Remediation Timeframe**
AVERAGE 24 days

| | |
|---|---|
| Critical | 36 days |
| High | 29 days |
| Medium | 14 days |
| Low | 37 days |

**Patch Efficacy**
AVERAGE 41 %

| | |
|---|---|
| Critical | 33% |
| High | 75% |
| Medium | 50% |
| Low | 22% |

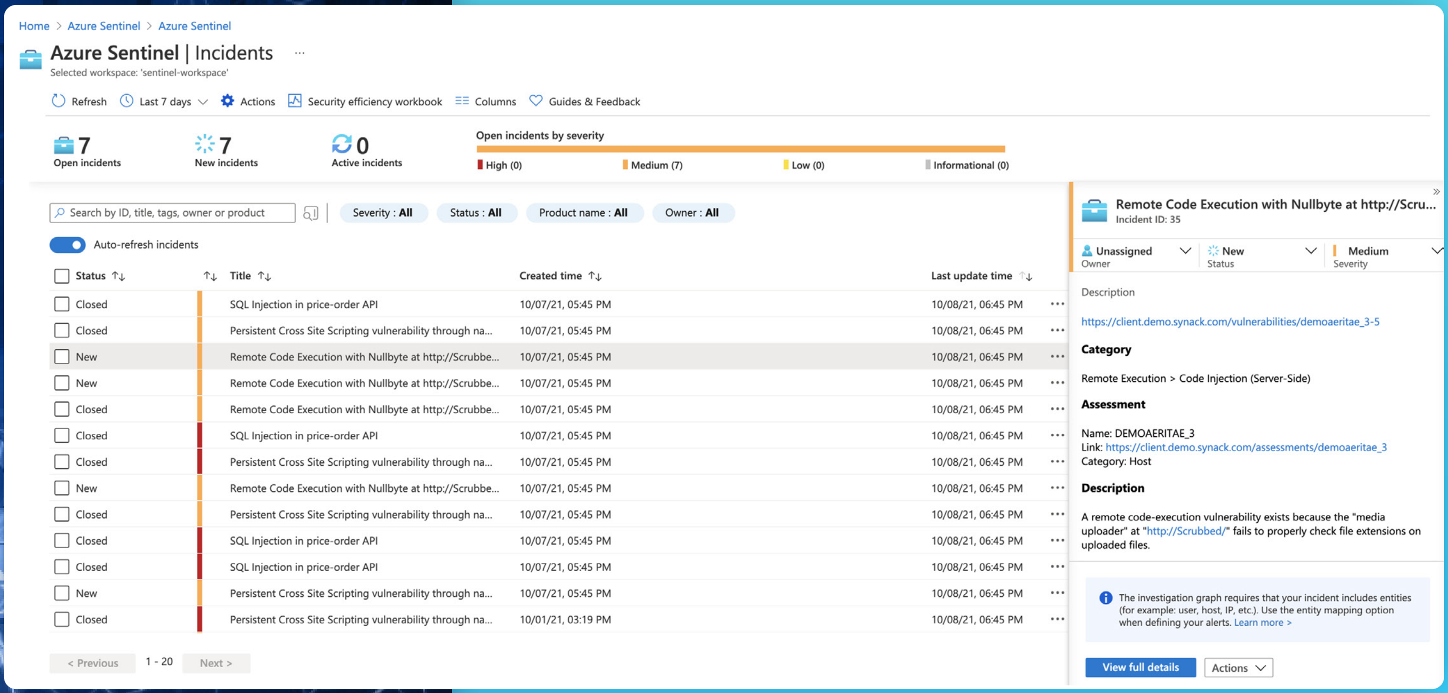
# Act swiftly to address gaps

## It’s one thing to identify security gaps, it’s another to build actionability into the structure of analysis

Knowing your security risks is only as helpful as your ability to proactively address them. In order to truly add value for your organization, the Synack Platform provides details, fixes, and actionable insights on exploitable vulnerabilities. Through an application programming interface (API) integration, this Synack data is automatically pulled into your local tools – like Microsoft Defender for Cloud or Microsoft Sentinel – for added efficiency and decreased risk.

## Integrate with the Microsoft Security products you already use

- Microsoft Defender for Cloud: Automatically send Synack testing results to Microsoft Defender for Cloud, allowing your team to view and manage findings in an already familiar display.
- Microsoft Azure DevOps: Create a work item in Azure Project for each vulnerability and keep that work item data up to date with the latest changes from Synack.
- Microsoft Sentinel: Synchronize with Synack's findings, create an incident in Microsoft Sentinel for each vulnerability, and update with real-time changes.


Home > Azure Sentinel > Azure Sentinel
Refresh
Last 7 days
Actions
Security efficiency workbook
Columns
Guides & Feedback

Azure Sentinel | Incidents

Selected workspace: 'sentinel-workspace'

7 Open incidents

7 New incidents

0 Active incidents

Open incidents by severity

🟥 High (0) 🟧 Medium (7) 🟨 Low (0) ⬜ Informational (0)

Search by ID, title, tags, owner or product

Severity : **All** Status : **All** Product name : **All** Owner : **All**

Auto-refresh incidents

| □ | Status ↑↓ | ↑↓ | Title ↑↓ | Created time ↑↓ | Last update time ↑↓ | |
|---|---|---|---|---|---|---|
| □ | Closed | 🟧 | SQL Injection in price-order API | 10/07/21, 05:45 PM | 10/08/21, 06:45 PM | ··· |
| □ | Closed | 🟧 | Persistent Cross Site Scripting vulnerability through na... | 10/07/21, 05:45 PM | 10/08/21, 06:45 PM | ··· |
| □ | New | 🟧 | Remote Code Execution with Nullbyte at http://Scrubbe... | 10/07/21, 05:45 PM | 10/08/21, 06:45 PM | ··· |
| □ | New | 🟧 | Remote Code Execution with Nullbyte at http://Scrubbe... | 10/07/21, 05:45 PM | 10/08/21, 06:45 PM | ··· |
| □ | Closed | 🟧 | Remote Code Execution with Nullbyte at http://Scrubbe... | 10/07/21, 05:45 PM | 10/08/21, 06:45 PM | ··· |
| □ | Closed | 🟥 | SQL Injection in price-order API | 10/07/21, 05:45 PM | 10/08/21, 06:45 PM | ··· |
| □ | Closed | 🟥 | Persistent Cross Site Scripting vulnerability through na... | 10/07/21, 05:45 PM | 10/08/21, 06:45 PM | ··· |
| □ | New | 🟧 | Remote Code Execution with Nullbyte at http://Scrubbe... | 10/07/21, 05:45 PM | 10/08/21, 06:45 PM | ··· |
| □ | Closed | 🟧 | Persistent Cross Site Scripting vulnerability through na... | 10/07/21, 05:45 PM | 10/08/21, 06:45 PM | ··· |
| □ | Closed | 🟥 | SQL Injection in price-order API | 10/07/21, 05:45 PM | 10/08/21, 06:45 PM | ··· |
| □ | Closed | 🟥 | SQL Injection in price-order API | 10/07/21, 05:45 PM | 10/08/21, 06:45 PM | ··· |
| □ | New | 🟧 | Persistent Cross Site Scripting vulnerability through na... | 10/07/21, 05:45 PM | 10/08/21, 06:45 PM | ··· |
| □ | Closed | 🟥 | Persistent Cross Site Scripting vulnerability through na... | 10/01/21, 03:19 PM | 10/08/21, 06:45 PM | ··· |

< Previous 1 - 20 Next >

Remote Code Execution with Nullbyte at http://Scru...

Incident ID: 35

Unassigned<br>Owner | New<br>Status | Medium<br>Severity

Description

https://client.demo.synack.com/vulnerabilities/demoaeritae_3-5

**Category**

Remote Execution > Code Injection (Server-Side)

**Assessment**

Name: DEMOAERITAE_3
Link: https://client.demo.synack.com/assessments/demoaeritae_3
Category: Host

**Description**

A remote code-execution vulnerability exists because the "media uploader" at "http://Scrubbed/" fails to properly check file extensions on uploaded files.

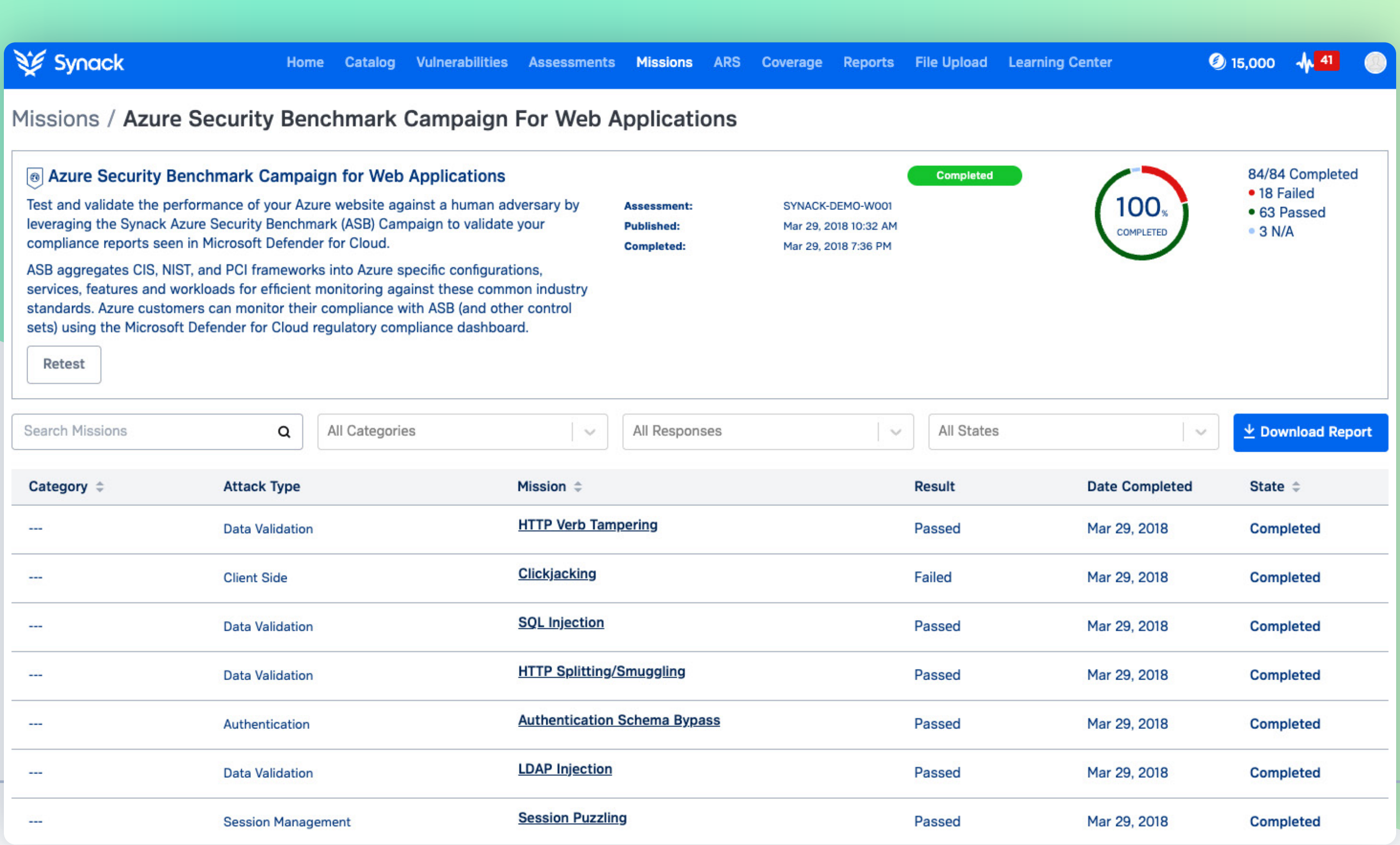
The investigation graph requires that your incident includes entities (for example: user, host, IP, etc.). Use the entity mapping option when defining your alerts. Learn more >

# Maintain regulatory compliance

## Organizations must accommodate continually changing compliance laws, often in multiple jurisdictions

Testing for and addressing security vulnerabilities can be a daunting task for in-house security teams, especially at the level required by heavily regulated industries. On average, 44% of organizations say their top compliance management challenges are handling compliance assessments, undergoing control testing, and implementing policy and process updates.[5]

Rather than overextending resources or leaving security gaps unchecked, adopt Synack and the Microsoft Security product portfolio for a comprehensive testing and mitigation workflow that makes it far easier to meet your specific data security and compliance requirements. Synack's on-demand security testing platform and team of experts can handle the scope and scale of testing needed to keep you compliant while giving critical time back to your in-house security team.



Missions / Azure Security Benchmark Campaign For Web Applications

**Azure Security Benchmark Campaign for Web Applications**

Test and validate the performance of your Azure website against a human adversary by leveraging the Synack Azure Security Benchmark (ASB) Campaign to validate your compliance reports seen in Microsoft Defender for Cloud.

ASB aggregates CIS, NIST, and PCI frameworks into Azure specific configurations, services, features and workloads for efficient monitoring against these common industry standards. Azure customers can monitor their compliance with ASB (and other control sets) using the Microsoft Defender for Cloud regulatory compliance dashboard.

**Assessment:** SYNACK-DEMO-W001
**Published:** Mar 29, 2018 10:32 AM
**Completed:** Mar 29, 2018 7:36 PM

84/84 Completed
- 18 Failed
- 63 Passed
- 3 N/A

| Category | Attack Type | Mission | Result | Date Completed | State |
|---|---|---|---|---|---|
| --- | Data Validation | HTTP Verb Tampering | Passed | Mar 29, 2018 | Completed |
| --- | Client Side | Clickjacking | Failed | Mar 29, 2018 | Completed |
| --- | Data Validation | SQL Injection | Passed | Mar 29, 2018 | Completed |
| --- | Data Validation | HTTP Splitting/Smuggling | Passed | Mar 29, 2018 | Completed |
| --- | Authentication | Authentication Schema Bypass | Passed | Mar 29, 2018 | Completed |
| --- | Data Validation | LDAP Injection | Passed | Mar 29, 2018 | Completed |
| --- | Session Management | Session Puzzling | Passed | Mar 29, 2018 | Completed |

## Get the information you need for your specific requirements

- Access compliance-ready reports that cover scope, testing information, vulnerabilities, and remediation status.
- Align to industry standards in penetration testing and reporting, such as:
  - NIST
  - CIS
  - OWASP
  - PCI
  - HIPAA
- Deploy the Microsoft Cloud Security Benchmark (Azure Security Benchmark v3) framework according to your security requirements and use Synack testing to validate adherence to MCSB security controls.

CASE STUDY

# Allianz Direct

## Situation

Allianz Direct, part of the Allianz Group (#24 in the Forbes Global 2000), is a direct insurance company operating in Germany, Italy, The Netherlands, and Spain. Allianz Direct sells their products via their online platform and places a high priority on delivering value faster than the competition. As an insurance company, customer trust is critical. Security, therefore, is built into everything they do.

## Challenge

Allianz Direct's challenge was safeguarding their data and complying with regulations. And they needed to do this without impacting their service delivery or customer experience. Allianz Direct was performing pentesting in-house, but examined available alternatives to maximize ROI for their pentesting program.

## Solution

Allianz Direct sought a solution that would provide a standardized process for continuously checking the security of their platform from an attacker's perspective. They chose Synack for its ability to provide continuous, high-quality testing at scale and with speed.

## Results

- Allianz Direct delivers services faster than the competition using better security testing.
- Ensures comprehensive vulnerability results are easily understood and reproducible for quicker remediation.
- Provides improved confidence in making risk-based trade-offs for new services and features.
- Achieves more and better pentesting at the same cost as in-house pentesting.
- Offers faster and easier retrieval and importing of current security status for review and for auditor reports.
- Facilitates testing for quick validation of log4shell vulnerability patching.

Read Entire Case Study

# Feel confident in your security throughout your digital transformation

## Continually validate your security posture as your business evolves.

No matter what the future holds for your business, robust continuous security testing can help you keep up with dynamic security risks and complex regulatory requirements.

Schedule a Demo

Find Synack in the Microsoft Commercial Marketplace.

Learn More

[1] CyberSecurity Statistics: The Ultimate List of Stats, Data, and Trends for 2022 | PuepleSec
[2] Report from Proofpoint and Cybersecurity at MIT Sloan | Proofpoint
[3] Microsoft Digital Defense Report for 2022 | Microsoft
[4] What is Cloud Security Posture Management? | XM Cyber
[5] Power What's Next | MetricStream

Synack

Microsoft Security

Synack®