Synack

Member of
Microsoft Intelligent
Security Association
Microsoft

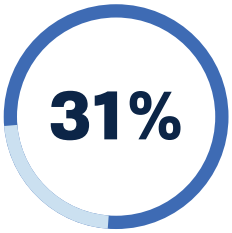
Microsoft Security & Compliance for Cloud Infrastructure

Integrated with Synack offensive security testing

Cloud configuration and security

80% of cloud breaches in 2020 were due to misconfiguration, mismanaged credentials or insider theft attacks, according to Gartner. Security teams are left responsible for not only securing cloud assets, but for rolling out security hygiene training and policies to developers.

Based on an increase in cloud misconfiguration vulnerabilities reported by the Synack Red Team in 2020, such as the examples shown below, it is clear that existing solutions and frameworks are fragmented leaving ample room for malicious exploit.



Default Credentials

Directory Contents

Code Injection

Microsoft and Synack have partnered to launch the first end-to-end, proactive cloud security framework and testing solution.

Microsoft Security and Compliance for Cloud Infrastructure (S&C4CI)

S&C4CI from Microsoft Industry Solutions helps make sure your cloud workloads are secure at any scale. S&C4CI's continuous security model gives you visibility into potential vulnerabilities while keeping you compliant with data protection and privacy regulations. S&C4CI can be scoped for Azure platform, services and workloads and scaled to your needs.

Synack Security Testing

Pairing Microsoft S&C4CI with Synack's premier security platform and researchers creates an efficient feedback loop in which Microsoft integrates Synack offensive security testing data into your enterprise security and development programs. Microsoft Azure-specific procedures, policies and environments are designed, developed and refined based on your actual resilience to attack. Testing includes web, infrastructure, mobile and API assets across internal, external and Azure networks.

Outcomes of the Microsoft/Synack joint solution

Integrated

- Microsoft Azure policy development and management
- Turnkey integrations for testing across web, infrastructure and API assets
- Microsoft-specific security testing campaigns
- Microsoft Sentinel, Defender for Cloud and Azure DevOps Boards integrations

Agile

- Scalable security controls deployed in your CI/CD pipeline via Microsoft Azure Policy or Azure Resource Manager
- Continuous testing for dynamic cloud threats across production or pre-production environments
- Sprint testing: Launch microtests for vulnerability checks and coverage reports aligned to DevOps releases

Transparent

- Microsoft best practices aligned to your business risk appetite and compliance requirements
- Built-in Microsoft Defender for Cloud integration to audit security requirements
- Testing and analytics via Synack Platform for continuous review of coverage and security posture adjustments

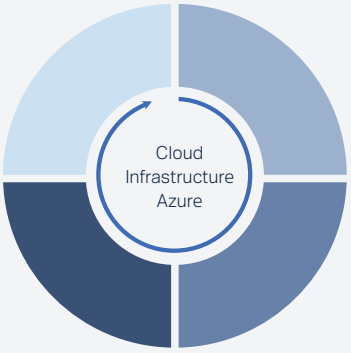
Compliant

- Microsoft Azure Security Benchmark framework deployed according to your business and compliance requirements
- Penetration testing and reporting aligned to industry standards (NIST, CIS, OWASP, PCI and HIPAA)

Microsoft Security & Compliance for Cloud Infrastructure approach

Plan
Create a security baseline that fits your requirements and is tracked using modern agile methodology.

Develop
Automate security controls as code so you can scale them to current and future requirements.



Deliver
Apply a continuous integration workflow to seamlessly update your environment based on control updates.

Measure
Audit controls, measure threats, reduce risk and meet compliance requirements.

Why Microsoft Security?

For over 35 years Microsoft has been committed to promoting security in their products and services—from helping their customers and partners protect their assets to working to help make sure that their data is kept secure and private. Microsoft focuses on security, identity and information protection ecosystems, leveraging partnerships with vendors and consulting firms around the world to drive changes in Microsoft products and services to provide you with protection for your intellectual assets.

The Synack Platform

Synack's premier security testing platform harnesses a diverse, talented and vetted community of security researchers and technology to deliver continuous and scalable penetration testing and vulnerability management with immediately actionable results.

- Exploitable vulnerability details and risk ratings
- Security controls testing
- Researcher data and insights
- Attacker Resistance Scores
- On-demand retesting via Patch Verification
- On-demand custom and comprehensive reporting

Learn More

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