

Hybrid & Multi-Cloud Threat Check



USA TOP 10



Microsoft Security

Value proposition

The Multi-Cloud Threat Check Assessment is an engagement allowing you to gain insights on active threats and vulnerabilities related to your Azure, multi-cloud, and/or hybrid workloads using Microsoft Defender for Cloud, Azure Arc, and other Azure security capabilities.

Workloads

- Microsoft Defender for Cloud
- Microsoft Sentinel
- Azure Arc
- Azure Firewall, Firewall Manager, & WAF
- Azure DDoS Protection
- Multi-Cloud Support - Azure and AWS, and/or GCP

Engagement Outcomes

- Assessment risk report deliverable
- High-level roadmap to remediate permission risk across all major cloud platforms
- Up to 17 hours of collaborative sessions scheduled over 2-3 weeks

Assessment offers

- *Microsoft funding for Invoke-led Assessment may be available upon request*
- **Invoke-led trial licensing for qualified customers*

Timeline & Scope – Customer customizable (minimal customer effort)



Stage 1

Engagement Setup

- Pre-Engagement Call
- Questionnaire
- Pre-requisites and scope



Stage 2

Kick-Off, Onboarding & Discovery

- Kick-off meeting with all stake holders
- Configuration and onboarding
- Secure Score
- Cloud Security Posture Management (CSPM)
- Azure Defender Plans
- Threat Protection
- Regulatory Compliance
- Azure Network Security
- Hybrid & Multi-Cloud Protection
- SIEM Integration



Stage 3

Findings Presentation & Closeout

- Threat data collection & Documentation
- Write up and recommendations
- Threat Assessment report presentation
- Recommended Next Steps
- Engagement Closeout

