IBM Security

IBM Security Services for Cloud:

Rapid Microsoft Azure Assessment

As you accelerate your migration to Microsoft Azure, how can you ensure your environment is secure and compliant?

99%

of cloud failures through 2023 will be the customer's fault[1]

66%

Of security decision makers see cloud security best practice frameworks as very valuable[2]

[1] Gartner, Innovation insight for Cloud Security Posture Management , 2019

[2] Forrester Cloud Security Spotlight Report, 2021

IBM

Dive deep into your Microsoft Azure environment's security posture with IBM Security

Our Rapid Cloud Security Assessment can bring visibility into security misconfigurations, traffic analysis, and your compliance posture against security and data privacy frameworks (such as NIST, ISO, CCPA, HIPAA, and PCI) across your Microsoft Azure environment. This assessment walks through the security findings in an interactive, structured session which provides key recommendations to closing those gaps in a security assessment report.

This assessment is performed within a 2-week period and provides a comprehensive analysis of:

- **Your existing cloud architecture** for security implementation
- **Account structure** including subscriptions and resource tagging
- **Monitoring and log management** including Azure Monitor, Log Analytics, and Microsoft Defender for Cloud
- **Compliance checks** for PCI DSS, HIPAA, CIS Benchmarks, NIST CSF/800-53, etc.
- **Data encryption** including Azure Key Vault, Azure Information Protection, and storage objects
- **Network and application security** including Azure Firewall, Network Security Groups, Azure WAF, and Azure DDoS
- **Identity and access management** including SSO, conditional access, MFA, and rotation of credentials
- **Monitoring controls** for MS Defender for Cloud, insights and recommendation
- **Your incident response plan** along with recommendations based on what is uncovered

Format and deliverables

- A typical rapid assessment is completed over a 2-week period and can be delivered in person or virtually
- The format is an interactive session combined with automated analysis
- This assessment is facilitated and reviewed by cloud security specialists – ensuring contextualized and tailored recommendations

Client success story

A multi-national apparel retailer had more than 31,000 unique resources across 2 different cloud environments, including Microsoft Azure. They needed to quickly assess their current implementation for cloud inventory, safe configurations, and compliance visibility.

IBM Security conducted a rapid cloud security assessment against the client's cloud environments in AWS and Microsoft Azure for safe configurations and compliance checks. After validating assessment results, IBM Security prepared a findings summary, detailed reporting, and remediation recommendations for the client by unique regions.

Key benefits

- Get a deep understanding of your vulnerabilities to cyber attack and risk of business loss across your Microsoft Azure environment
- Align compliance policies to industry standards, Microsoft Azure recommend best practices, CIS benchmarks, NIST CSF, MITRE ATT&CK, etc.
- Remediation recommendations based on analysis of your organization's security posture by evaluating vulnerabilities, identity, and compliance risks.

Member of Microsoft Intelligent Security Association

Microsoft

Gold Microsoft Partner

Microsoft

IBM **Security**