Mandiant

Microsoft Azure Security Assessment

Benefits

- **Attacker perspective:** Translate frontline incident response experience into practical recommendations to improve your security posture.
- **Actionable recommendations:** Receive a clear, prescriptive roadmap covering configurations, policies and logging.
- **Remediation workflows:** Equip IT and security teams with the step-by-step workflows and guidance to confidently implement and verify controls.
- **Knowledge transfer:** Benefit from Mandiant mentoring and coaching to implement solutions and build long-term security resilience.

Why Mandiant?

- **Frontline expertise:** Mandiant incident responders are on the frontlines of the most complex cloud incidents worldwide so we understand the reality of the current threat landscape
- **Tested techniques:** Mandiant recommendations deliver battle-tested techniques that have successfully eliminated active threat actors from the most complex environments.
- **Holistic approach:** Mandiant evaluates your architecture, configurations, and operational processes to secure the supporting infrastructure.

Comprehensive architecture review, hardening, and threat mitigation for your Microsoft Azure infrastructure

A comprehensive evaluation of your Microsoft Azure tenant to identify architectural risks, harden configurations, and improve detection capabilities based on frontline intelligence.

Microsoft Azure is a common cloud platform in many modern enterprises, making it a high-value target for threat actors. As organizations scale their cloud footprints, they frequently struggle with publicly exposed resources, over-permissive access, and inadequate security governance. Securing this dynamic environment requires a deep understanding of how adversaries exploit cloud-specific misconfigurations to move laterally and access sensitive data.

Comprehensive security posture evaluation

Mandiant consultants will assess your Azure security posture by evaluating your current state across these critical pillars:

Identity and access management

Reviewing your admin models, PAM, MFA, and Conditional Access policies to prevent unauthorized entry and lateral movement across your cloud identities.

Architecture, network and data security

Inspecting resource configurations, network segmentation, and secrets management. Evaluating encryption and governance securing the Azure control and data planes.

Logging and threat detection

Assessing your ability to detect and respond to threats targeting Azure by reviewing centralized logging, anomaly detection, and incident response readiness.

The assessment cycle

Phase 1 | Discovery
Understanding your current state.

Phase 2 | Workshops
Interactive workshops focused on architecture.

Phase 3 | Reporting
Recommendations and roadmap.

A collaborative, three-phased methodology

Mandiant conducts a comprehensive security review spanning approximately six weeks, focusing heavily on collaboration with your key stakeholders:

- **Discovery:** We baseline your current configuration, ongoing initiatives and security enforcement state using non-disruptive data collection scripts and a technical documentation review.
- **Workshops:** Expert-led interactive, onsite (or remote) workshops help you bridge the gap between your current architecture and a modernized, resilient architecture. These sessions are based on a deep understanding of your current state.
- **Roadmap and technical reporting:** We deliver actionable technical recommendations mapped to your business, complete with a phased implementation roadmap and resource estimates.

Field-tested defense guidance

This service goes beyond basic compliance to secure your infrastructure against advanced threat actors. The assessment is built around the essential short-term containment and long-term remediation controls needed to expel attackers. Mandiant will provide practical guidance rooted in field-tested, proven techniques that have successfully driven attackers out of real-world environments.

Engagement deliverables

	Workshop and knowledge transfer materials	Detailed findings and remediation report	Executive out-brief
Details	Receive workshop materials, presentation slides, and technical documentation to empower your internal teams for long-term operational success.	A comprehensive guide to hardening your environment. This deliverable outlines the identified Azure misconfigurations, prioritizes misconfigurations by risk severity (Critical, High, Medium, Low), details the real-world impact of each finding, and provides step-by-step technical instructions for remediation.	Gain a high-level view of your security posture with an executive snapshot of the most pressing risks and their business impact. This deliverable includes a phased, effort-estimated waveplan to guide your security investments and streamline your roadmap for remediation.

Contact us today to discuss how we can help you achieve your program goals.