Mandiant

Datasheet

Microsoft Azure Rapid Review

Benefits

- **Rapid speed to value:** Gain fast visibility into your Azure cloud security posture without a lengthy engagement.
- **Threat-informed mitigation:** Identify the critical configuration gaps that real-world attackers use to gain initial access and move laterally within Azure environments.
- **Minimized attack surface:** Pinpoint over-permissive identity settings and exposed services.
- **Prioritized hardening roadmap:** Receive a findings matrix ranked by risk severity to immediately implement changes yielding the highest return on security investment.

Why Mandiant?

- **Frontline expertise:** Mandiant incident responders are on the frontlines of the most complex cloud breaches worldwide so we understand the reality of the current threat landscape.
- **Speed:** Get actionable results in weeks, not months.
- **Focus:** We cut through the noise to focus on the misconfigurations that actually lead to breaches.

High-impact analysis of the top security risks related to your Microsoft Azure infrastructure

A streamlined analysis of your Azure tenant, evaluating your current configurations against the critical misconfigurations most frequently exploited in real-world breaches.

When you need fast visibility into your Azure cloud security posture, the Rapid Review delivers. Mandiant experts evaluate your tenant against the most critical risks. It is a fast path to understanding your attack surface and receiving prioritized, actionable, hardening recommendations for your Azure environment.

Rapid Azure hardening

This service focuses strictly on configuration data to identify the critical security gaps that attackers may use to gain initial access and move laterally within Azure:

Identity and access management

Review of Multi-Factor Authentication (MFA) enforcement, the scope of privileged roles, and the effectiveness of Conditional Access Policies protecting Azure access.

Posture and control validation

Evaluation of your Azure services to secure exposed resources, validate network controls, and ensure correct secrets management.

Logging and threat detection

Inspection of the configuration of Azure's logging and threat detection capabilities to ensure essential security events are being captured and alerts are in place.

Streamlined data-driven analysis

The Rapid Review is executed over approximately three weeks:

1. Phase 1 (Discovery): Understanding of the current state of your Azure subscriptions. Mandiant provides guidance for creating a read-only account with only the precise permissions needed to conduct analysis while strictly adhering to your organization's least-privilege access policies and compliance requirements.

2. Phase 2 (Analysis): A deep dive into your Azure security configurations. Mandiant executes specialized scripts against your in-scope Azure subscriptions to extract configuration data.

3. Phase 3 (Reporting): Recommendations and roadmap. Mandiant evaluates the data to develop a findings matrix and detailed report with prioritized hardening actions for your Azure environment.

The assessment cycle

Discovery:
Understanding the current state.

Analysis:
Deep dives into the security configuration.

Reporting:
Recommendations and roadmap.

Targeted configuration review

The rapid review is ideal for organizations seeking a "health check" or baseline assessment of their Azure environment. The review compares your environment against the real-world attack techniques Mandiant sees on the frontlines of incident response. This allows you to prioritize the specific changes that yield the highest return on your security investment.

Engagement deliverables

	Detailed findings and remediation report	Executive out-brief
Details	A comprehensive document outlining the identified misconfigurations, explaining the associated risks, and providing detailed, step-by-step technical instructions for implementing the recommended changes. Findings are prioritized by risk severity (Critical, High, Medium).	A presentation summarizing the assessment results, suitable for briefing technical leadership on the immediate actions required.

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