Mandiant

Datasheet

Microsoft 365 Rapid Review

Benefits

- **Speed to value:** Quickly understand your security posture without a lengthy engagement.
- **Mitigate common exploits:** Proactively close the configuration gaps most frequently targeted by attackers.
- **Reduce attack surface:** Identify and disable unnecessary services and over-permissive settings.
- **Prioritized hardening:** Receive a stack-ranked list of high-impact changes to improve defenses immediately.

Why Mandiant?

- **Incident led:** Our checklist is built on the reality of the current threat landscape, not compliance manuals.
- **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 in your Microsoft 365 tenant

Evaluation of your tenant's security posture against Mandiant's most common incident investigation and remediation findings.
When you need immediate visibility into your cloud security posture, the rapid review delivers. This engagement quickly evaluates your tenant's current security settings against the most critical risks. It is the fastest path to gain visibility into your attack surface and provides prioritized hardening recommendations.

Rapid Microsoft 365 hardening

This review focuses strictly on configuration data to identify the critical security gaps that attackers use and exploit to gain initial access:

Identity and Access (Entra ID)	Exchange Online Security	SharePoint and Teams Governance
Review of MFA enforcement, admin privileges, and conditional access. Identification of risky OAuth bindings and legacy protocols that facilitate compromise.	Assessment of email hygiene, including transport rules and anti-phishing controls. Review of settings to identify gaps that could allow malware delivery or data exfiltration.	Analysis of external sharing settings and tenant-wide policies across SharePoint, OneDrive, and Teams. Identification of over-permissive configurations that risk data leakage.

Streamlined data-driven analysis

The Rapid Review is executed over approximately three weeks using a highly efficient process:

- **Phase 1 (Access):** Gain peace of mind with expert assistance in establishing a dedicated, read-only account. This ensures a comprehensive security analysis is performed while strictly adhering to your organization's least-privilege access policies and compliance requirements.
- **Phase 2 (Analysis):** Mandiant executes specialized scripts against your in-scope M365 tenants to extract configuration data. Our specialized scripts ensure a rapid, non-disruptive collection process, providing the visibility needed to identify hidden vulnerabilities without impacting your production environment.
- **Phase 3 (Reporting):** Move beyond raw data with a comprehensive findings matrix and a detailed executive report. Our experts evaluate your unique environment to deliver prioritized remediation steps, transforming complex configuration data into a clear roadmap for hardening your cloud posture.

Note: This review does not include deep-dive workshops or architecture design evaluation.

Target the top misconfigurations exploited in real world incidents

This service is specifically suited for organizations that need a "health check" or baseline assessment. It weighs your technology stack against the specific techniques Mandiant commonly finds used by adversaries in real-world incidents, allowing you to prioritize the changes that offer the highest return on security investment.

Engagement deliverables

Detailed findings and remediation report	Executive out-brief
Comprehensive Findings Report A document outlining the identified misconfigurations, explaining the associated risks. **Technical Implementation Guidance** Step-by-step, technical instructions to help you quickly remediate gaps and harden your environment efficiently. **Prioritized Remediation Roadmap** Findings are prioritized by risk severity (Critical, High, Medium) to help your team focus resources on the most urgent and important threats first.	A high-level presentation for executive leadership that summarizes the key assessment results and the immediate steps required to improve your security posture.

The security assessment cycle

Access: Establish a dedicated, read-only account for least-privilege access to your environment.

Analysis: Identification of complex misconfigurations and hidden vulnerabilities across your M365 stack using custom tools.

Reporting: Translation of findings into a prioritized execution plan and roadmap. You receive the exact technical steps to move from identified risk to verified resolution.

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