Mandiant

Datasheet

Microsoft 365 Security Assessment

Benefits

- **Attacker perspective:** We translate frontline incident response experience into practical recommendations to improve your security posture.
- **Actionable recommendations:** Receive comprehensive guidance covering configurations, policies, logging, and tooling.
- **Remediation guidance:** Empower technical and security teams with resources to remediate and validate the implementation of security recommendations.
- **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 breaches worldwide so we understand the reality of the current threat landscape.
- **Tested techniques:** Mandiant recommendations reflect vetted techniques that have successfully eradicated attackers from client environments.
- **Holistic approach:** Mandiant evaluates the architecture, configurations, and operational processes to secure the supporting infrastructure.

Comprehensive architecture review, hardening, and threat mitigation

A comprehensive evaluation of your Microsoft 365 tenant to identify architectural risks, harden configurations, and improve detection capabilities based on Mandiant frontline intelligence.

Microsoft 365 is a high-value target for brute force attacks, credential stuffing, fraud, and unauthorized data access. As organizations evolve, IT and security teams frequently struggle to maintain secure configurations, monitor for anomalies, and keep pace with new security enhancements. Defending this environment requires a deep understanding of how threat actors operate and actively bypass standard controls.

Comprehensive security posture evaluation

Mandiant experts evaluate your current security posture across the entire M365 ecosystem.

Identity and access management

Proactively secure your environment through an in-depth architectural review of your administration models, PAM, MFA, and Conditional Access policies.

Data protection, governance and risk mitigation

Harden your M365 environment by aligning security policies and procedures with industry standards.

We evaluate email security, cloud application hardening and data classification against modern attacks with a clear roadmap to remediate risks.

Logging, detection, and response

Eliminate blind spots by validating your ability to detect and respond to M365 threats.

We review centralized logging, anomaly detection, and incident response readiness.

The assessment cycle

Phase 1 | Discovery
Understanding your current state.

Phase 2 | Strategic transformation
Interactive workshops focused on architecture modernization.

Phase 3 | Technical reporting
Recommendations and roadmap.

A collaborative, three-phase 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.
- **Strategic transformation:** Expert-led interactive, onsite or remote workshops bridge the gap between your current M365 architecture and a modernized resilient architecture. These sessions transform technical analysis into a strategic roadmap, ensuring your roadmap is tailored to your business objectives, stakeholders and operational needs.
- **Technical reporting:** We transform technical findings into an actionable waveplan, complete with effort estimations and risk-based prioritization. This detailed roadmap includes prioritized workstreams, allowing your team to allocate resources efficiently and demonstrate immediate progress.

Field-tested, practical defense guidance

This service goes beyond basic compliance checks. Mandiant provides practical, tested, and effective guidance for hardening, securing your environment, and enhancing visibility. Receive actionable recommendations and strategic guidance to implement critical short-term containment and long-term security controls—empowering you to rapidly isolate and eradicate advanced threat actors from your environment.

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 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, Low).	A high-level snapshot for executive stakeholders detailing the most pressing risks, the strategic business impact of those vulnerabilities, and a phased migration roadmap (waveplan) with effort estimation to guide your security investments.

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