MANDIANT®

DATA SHEET

Security Assessment for Microsoft 365

HIGHLIGHTS

- **Mitigate** commonly exploited misconfigurations
- **Reduce** the Microsoft 365 attack surface
- **Gain** insights into the most pressing security risks relating to existing configurations
- **Enhance** monitoring, visibility, and detection
- **Prioritize** security enhancements

Why Mandiant Solutions

Mandiant Solutions has been at the forefront of cyber security and cyber threat intelligence since 2004. Our incident responders are on the frontlines of the most complex breaches worldwide. We have a deep understanding of threat actors and their rapidly changing tactics, techniques and procedures (TTPs) by leveraging our combined adversary, machine and victim intelligence sources.

Overview

With the transition to the cloud, there is a notable rise in security incidents involving cloud platforms and services. Microsoft 365 is highly targeted due to its popularity and the valuable hosted data. Compromising Microsoft 365 tenants allows attackers to remotely access sensitive data in the cloud without having to penetrate the corporate perimeter. Threat actors can access Microsoft 365 tenants by exploiting or compromising:

- Weak or legacy authentication mechanisms
- Security controls which have not been optimally configured
- Accounts with privileged access levels
- Accounts with weak passwords or those that do not require multifactor authentication

Recognize and Reduce Risk in Microsoft 365

The Mandiant Security Assessment for Microsoft 365 was developed based on extensive experience responding to incidents where threat actors have compromised and gained access to an organization's Microsoft 365 tenant. By proactively reviewing and mitigating common misconfigurations, process weaknesses, and exploitation methods, organizations can reduce overall risk and ensure optimized protection and visibility for events occurring within a Microsoft 365 tenant.

The foundation of this assessment includes both the short-term containment and longer-term remediation security controls and configurations required to eradicate attackers from a tenant.

Our Approach

This Mandiant security assessment evaluates common Microsoft 365 authentication platforms and access controls across six core focus areas:

- Security architecture and hardening
- Identity and access management
- Visibility
- Data protection
- Disaster recovery
- Threat detection and response

Common Authentication Platforms | **Common Access Controls**

CORE FOCUS AREAS

- **Security Architecture and Hardening**
- **Identity and Access Management**
- **Visibility**
- **Data Protection**
- **Disaster Recovery**
- **Threat Detection and Response**

Assessment Duration

The Microsoft 365 security assessment typically takes three weeks, consisting of four phases. Mandiant consultants perform the following activities:

Documentation Review
0.5 week

Includes an offsite review of migration strategies, email design and architecture documentation, hardening documentation, logging standards and Mobile Device Management (MDM) configurations as they relate to accessing a Microsoft 365 tenant.

Remote Workshops
0.5 week

A series of remote workshops for each core focus area in collaboration with key client stakeholders.

Configuration Review
1 week

A thorough configuration review of the Microsoft 365 tenant to ensure that security configurations are optimized in accordance with hardening, security, and protective guidance.

Reporting
1 week

A report that details practical technical recommendations to harden the Microsoft 365 tenant, enhance visibility and detection and improve processes to reduce the risk of compromise for the cloud tenant and related infrastructure.

Deliverables

At the completion of the engagement, Mandiant experts provide a detailed report that includes:

- A snapshot of the existing Microsoft 365 tenant security configuration.
- Specific Microsoft 365 security best practices to align with current configurations and operational processes.
- Practical recommendations for enhancing visibility and detection.
- Prioritized and detailed recommendations for further hardening the security posture of the Microsoft 365 tenant.

To learn more about Mandiant Solutions, visit: **www.FireEye.com/mandiant**

FireEye, Inc.
601 McCarthy Blvd. Milpitas, CA 95035
408.321.6300/877.FIREEYE (347.3393)
info@FireEye.com

About Mandiant Solutions

Mandiant Solutions brings together the world's leading threat intelligence and frontline expertise with continuous security validation to arm organizations with the tools needed to increase security effectiveness and reduce business risk.

MANDIANT®