MANDIANT®

数据表

Microsoft 365 的威胁防护评估

亮点

- **移除**经常被利用的错误配置
- **减少** Microsoft 365 攻击面
- **深入了解**与现有配置有关的、最紧迫的安全风险
- **增强**监测、可见性和检测能力
- **优先**安全增强功能

为何选择 Mandiant Solutions

自 2004 年起，Mandiant Solutions 始终走在网络安全防护和网络威胁情报领域的前列。我们的事件响应产品不断用于处置全球最复杂的违规事件。我们通过结合对手、设备及受害者情报资源，深入了解威胁制造者及其快速多变的策略、技术及程序 (TTP)。

概要

随着向云技术的过渡，涉及云平台和服务的威胁防护事件显著增加。Microsoft 365 因其广受欢迎和宝贵的托管数据而成为攻击重点。Microsoft 365 租户被破坏后，攻击者无需渗透公司外围网络，即可远程访问云端的敏感数据。威胁制造者可通过以下利用或危害的方式，访问 Microsoft 365 租户：

- 身份验证机制较弱或老化
- 未优化配置威胁防护控制措施
- 特权访问级别账户
- 密码较弱或不需要多重身份验证的帐户

识别和降低 Microsoft 365 风险

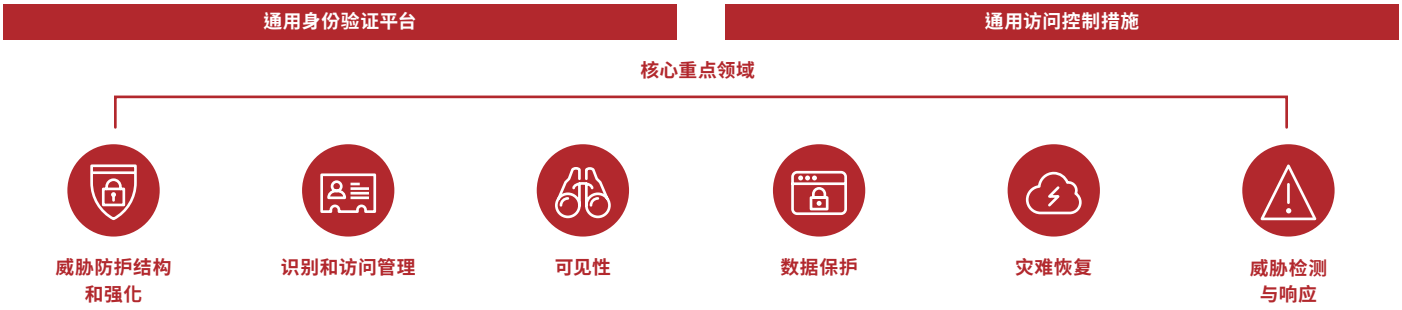
Microsoft 365 的 Mandiant Security Assessment（威胁防护评估）基于对“威胁制造者损害和访问组织的 Microsoft 365 租户”事件的广泛响应经验。通过主动评审和缓解常见的错误配置、流程弱点和利用方法，组织可以降低总体风险，并确保针对 Microsoft 365 租户内发生的事件，优化保护措施，提高透明度。

此评估基于消除租户攻击者所必须的短期抑制、长期修正安全控制措施和配置。

我们的方案

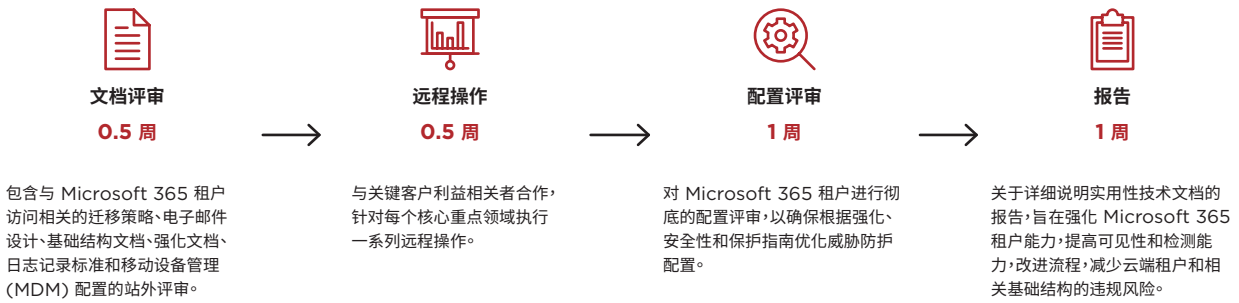
该 Mandiant 安全评估针对六个核心重点领域的常见 Microsoft 365 身份验证平台和访问控制：

- 威胁防护结构和强化
- 识别和访问管理
- 可见性
- 数据保护
- 灾难恢复
- 威胁检测与响应



评估持续时间

Microsoft 365 威胁防护评估通常分为四个阶段，持续三周时间。Mandiant 顾问执行以下活动：



交付项目

合约完成时，Mandiant 专家会提供一份详细的报告，其中包括：

- 当前 Microsoft 365 租户威胁防护配置的快照。
- 与当前配置和操作流程保持一致的特定 Microsoft 365 威胁防护最佳标准。
- 提高可见性和检测能力的实用性建议。
- 旨在进一步强化 Microsoft 365 租户威胁防护状态的优先、详细建议。

欲进一步了解 Mandiant Solutions，请访问：**www.FireEye.com/mandiant**

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

关于 Mandiant Solutions

Mandiant Solutions 将全球领先的威胁情报、一线事件响应数据、持续的安全性验证结合，为组织提供了所需工具，以提高安全性和降低业务风险。

MANDIANT®

M-EXT-DS-US-EN-000208-02