



思科高级网络钓鱼保护：实施流程（托管）

发布日期：2018 年 6 月 22 日

思科高级网络钓鱼保护的部署流程简单而明确。此流程根据思科多年为大型组织提供电子邮件安全保护的丰富经验提炼而成。部署项目包括三个主要要素：1) 思科邮件安全网络、2) 托管思科高级网络钓鱼保护传感器，以及 3) 思科高级网络钓鱼保护

此流程将实现以下目标：

- 了解邮件架构
- 部署思科高级网络钓鱼保护传感器
- 确认邮件流量
- 验证邮件评分的准确性
- 以“执行”模式启用单一思科高级网络钓鱼保护策略

其他独立步骤另行说明。

部署项目的主要任务

主要部署任务具体如下：

- 配置思科邮件安全设备，使用 **Dual Delivery**（双重投递）功能将所有邮件同时发送至思科高级网络钓鱼保护传感器。确保组织的进站邮件流具有全面可视性。
- 部署托管思科高级网络钓鱼保护传感器。向思科高级网络钓鱼保护邮件信任平台提供必要的邮件详情（例如身份验证标头）。
- 调整策略和数据模型。通过调整模型，确保准确识别您组织的有效邮件。调整策略，以便有效识别恶意邮件（例如商业电子邮件诈骗 [BEC]）。
- 启用策略。
- 通过执行策略拦截恶意邮件（例如冒充熟人诈骗）。



