思科域保护

实现 DMARC 身份验证和实施自动化，保护您的品牌和客户

为本地邮件部署以及诸如 Office 365 和 GSuite 等云邮件平台提供保护

在组织与客户和潜在客户互动中，邮件是最重要的沟通形式。同时，它仍然是网络犯罪分子通过网络钓鱼攻击组织客户群时所使用的头号入侵载体。

众多公司越来越多地依赖基于云的第三方邮件发件人进行品牌传播。这种做法导致客户和合作伙伴容易遭受未获域使用授权人员的攻击。而且，这种攻击会损害品牌声誉、破坏客户信任，并对组织的盈利能力产生负面影响。

思科®域保护能够自动识别、监控和管理第三方代表您发送的邮件。这为发现和消除非法邮件并阻止恶意邮件提供了一种简便方法，可抵御冒充您公司域的网络钓鱼攻击。域保护甚至可以检测以假乱真的仿冒域，从而快速阻止恶意 URL。

为规避这些漏洞，最有效方法是使用 DMARC 标准对您的邮件发件人进行授权和身份验证，防止您的客户遭受网络攻击，并保护您的品牌形象。DMARC 这项技术让邮件发件人和收件人能够更容易确定邮件是否来自合法发件人。由于组织的邮件生态系统非常复杂，因此识别所有合法发件人可能极具挑战性。如果没有合适的工具、流程和知识，该过程也可能会耗费大量时间且难以实施。

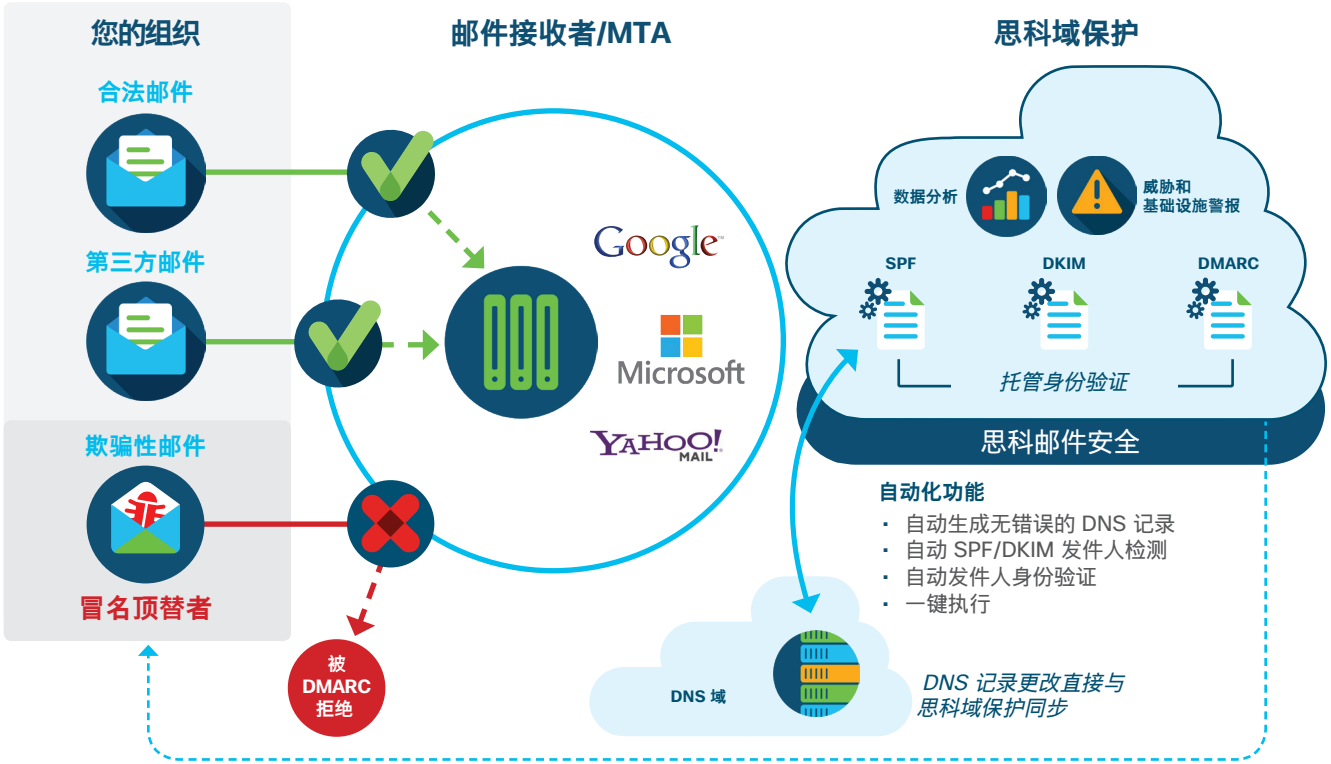
优势

- 防止通过仿冒公司域发动的品牌滥用
- 深入了解使用您的域代您发送邮件的内部和第三方发件人，为客户提供保护
- 实现基于域的邮件身份验证、报告和一致性 (DMARC) 身份验证以及执行流程的自动化，以识别非法发件人
- 阻止未经授权的发件人并设置 DMARC 保护，从而减少来自您的域的非法邮件，保护您的品牌价值
- 将信息与易于阅读的报告相关联，快速了解相关情况
- 提高出站邮件营销效果和营销活动收入

其他保护

- 实现 DMARC 部署自动化，减轻管理负担
- 邮件云智能可识别并直观呈现发件人域和 IP 地址
- EasySPF 可以快速自动构建无错误的 SPF 记录
- EasyDKIM 可自动执行选择器识别和 DKIM 的整体管理

思科域保护可让 DMARC 邮件身份验证过程实现自动化，并让您能够查看自己的邮件发件人和使用您的域的第三方邮件发件人。它会自动将信息关联到易于阅读的报告，并在报告中列出代表您发送邮件的人员以及他们是否符合 DMARC 标准。对于不符合 DMARC 标准的发件人，思科域保护提供了多种工具来帮助您实现合规性。思科域保护还提供了相关指导，帮助您阻止未经授权的发件人。



思科域保护额外提供了一层保护，不仅增强思科邮件安全的行业领先功能，而且更有效地保护您的邮件环境。它可以与任何捆绑包一起购买，以进一步保护您公司的域，并提高您的数字营销效果。