适用于 Meraki MX 的思科高级恶意软件防护

优势

- 获得对网络内和多个分支机构间的**威胁的可视性**
- 利用基于云的网络安全平台**简化安全管理**
- 通过深度威胁可视性，**快速检测、分析和补救漏洞**
- 通过全球威胁情报**增强网络防御**
- 使用单个基于 Web 的控制面板管理云中的安全服务，从而**降低复杂性**
- 使用易于部署、易于管理且经济实惠的订用服务，**降低成本并节约时间**

利用高级威胁防护功能简化基于云的安全管理

零日攻击、高级持续威胁 (APT) 和恶意软件，这些只是当今创新型、持续性的活跃网络犯罪的几个例子。攻击者正不断发现新的方式来破坏您的组织，然而安全专业人员在处理这些网络攻击时却往往心有余而力不足，因为他们缺乏协调有效的安全解决方案的可视性、工具和专业技能。攻击者利用这些安全漏洞，能够轻易躲避检测和掩盖恶意行为。攻击方式正越来越先进，所以组织用于保护自己的安全解决方案也必须与时俱进。

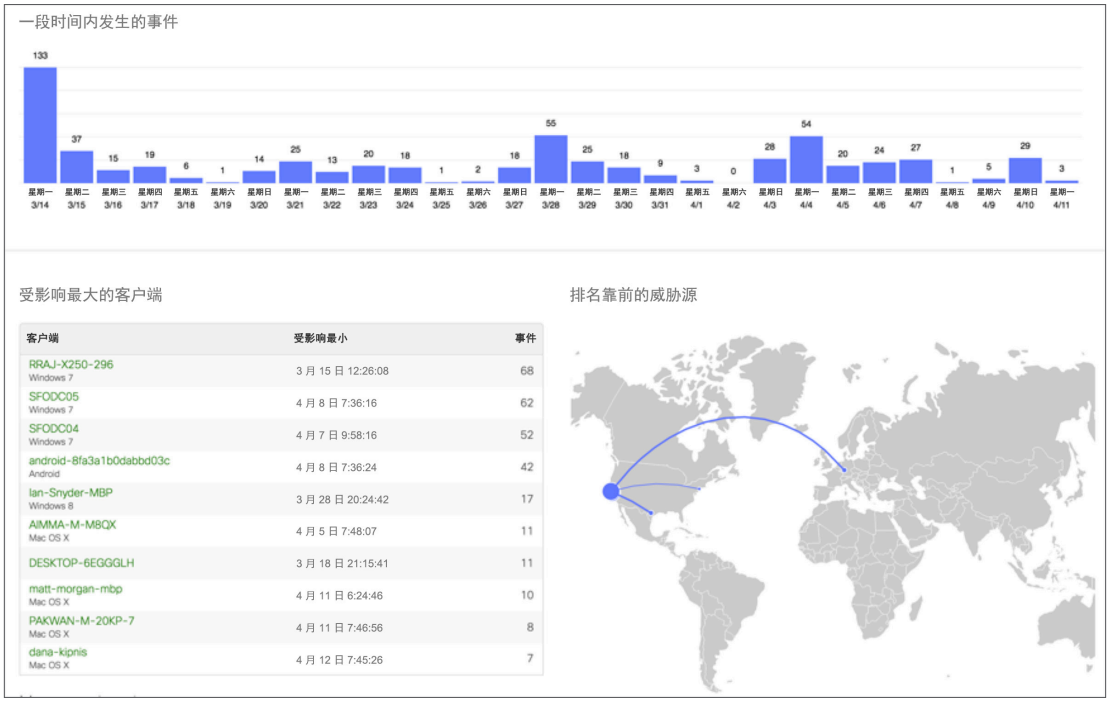
组织比以往任何时候都需要在整个网络中实现出色的可视性、持续的可控性和高级威胁防护。面向 Meraki MX 的思科® 高级恶意软件防护 (AMP) 正好能提供此等安全水准。

AMP + Meraki MX：全面的安全防护

思科 AMP 结合面向 Meraki MX 统一威胁管理 (UTM) 的 Threat Grid，提供基于云的安全管理平台，帮助您执行先进的威胁防范。该解决方案的高级威胁功能使组织突破传统检测工具限制，获得所有分支机构位置和远程办公室的恶意软件的威胁可视性，使他们能够快速检测、遏制和修复漏洞。

功能

- **增强的威胁防护：**AMP 在网络周界提供业界领先的威胁防护功能，有助于在漏洞发生之前阻止攻击。
- **不间断文件监控：**AMP 会持续监控、分析和记录文件活动，以快速检测躲过第一道防线的恶意软件，帮助您确定受影响范围并快速做出响应。
- **追溯性警报：**AMP 会向管理员发出有关恶意文件进入网络的可追溯性通知，即便这些文件在进入网络时并未被认定为恶意文件。
- **高级恶意软件分析：**一个高度安全的环境可帮助您根据大量行为指标启动并分析恶意软件，以发现过去未知的零日威胁。
- **集中安全管理：**该解决方案可为您提供一个一体化、云托管的网络安全平台，从一个中央位置管理所有分支机构的安全、网络和应用控制。
- **Talos 威胁研究：**AMP 会根据全球 Talos 数据库来检查进入网络的所有文件，以确定它们是否为恶意文件。



面向 Meraki 的 AMP 适用于分布式企业和中小型企业，提供：

威胁的深层可视性

当今的网络攻击都非常隐蔽。要进行防御，您需要能够跨多个站点和时间提供网络威胁形势可视性的解决方案。面向 Meraki MX 的 AMP 超越传统检测功能，可持续捕获并分析整个网络中的文件和流量活动。这可让您清晰了解您的网络中正在发生或已经发生的情况。

缩短检测时间

网络威胁无孔不入，一旦受侵入，您需要快速检测到入侵并采取行动。

有了面向 Meraki 的 AMP，安全团队就能利用追溯性恶意软件警报。在发现已通过网络周界的文件为恶意文件时，这些警报会向客户发送通知，从而缩短检测时间。

高级沙盒功能

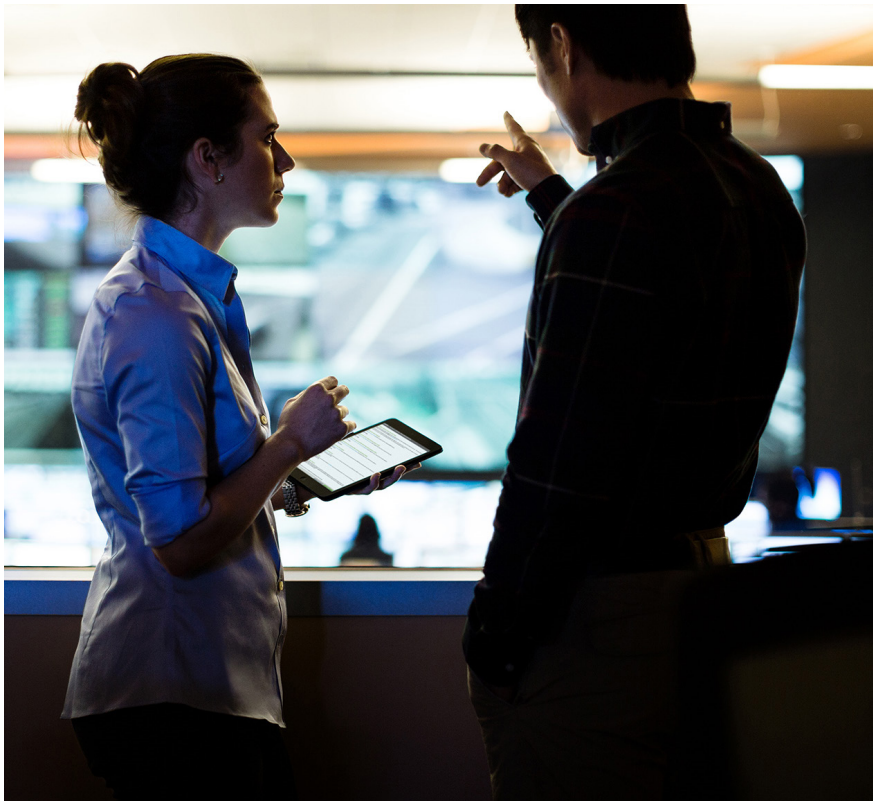
面向 Meraki MX 的 Threat Grid 通过先进的沙盒技术，即使是最复杂的恶意软件，也能提供深入的可视性。安全管理员可以将未知文件发送到云或本地沙盒，使恶意软件在虚拟环境中安全运行并检查恶意内容。这将帮助安全团队了解恶意软件的行为、受其影响的进程以及其进行的更改。此功能使他们获得比以往更准确、情景更丰富的分析。

简化安全管理

Meraki MX UTM 提供一体化、云管理的网络安全平台，能够从一个中央位置管理安全、网络和应用控制。组织可借助 Meraki 提高运营效率和简化管理，同时受益于 AMP 一流的威胁防范和恶意软件分析。

后续行动

有关面向 Meraki MX 的思科 AMP 如何帮助您保护组织抵御高级网络攻击的信息，请与思科销售代表或渠道合作伙伴联系。
有关更多信息，请访问：https://meraki.cisco.com/amp。



C45-737164-00 05/16