优势

- **高级威胁检测：**适用于网络安全的 AMP 在攻击前、攻击中和攻击后为您提供全面的网络相关威胁防护。
- **不间断分析和追溯性安全：**无论最初的处理结果如何，文件进入网关后，AMP 会继续观察、分析和记录文件的活动。如果稍后发现文件表现出恶意行为，AMP 会发送追溯性警报，以便您可以遏制和修复恶意软件。
- **增强的网络防御：**适用于网络安全的 AMP 基于大数据和出色的安全情报构建。我们的思科 Talos 团队每天分析数百万恶意软件样本和数万亿字节的数据，并将情报推送给 AMP。然后，AMP 会依据这个情景丰富的知识库关联文件、遥测数据和文件行为，从而主动防范各种已知威胁和新型威胁。

适用于网络安全的思科高级恶意软件防护

面向复杂威胁的复杂网络安全

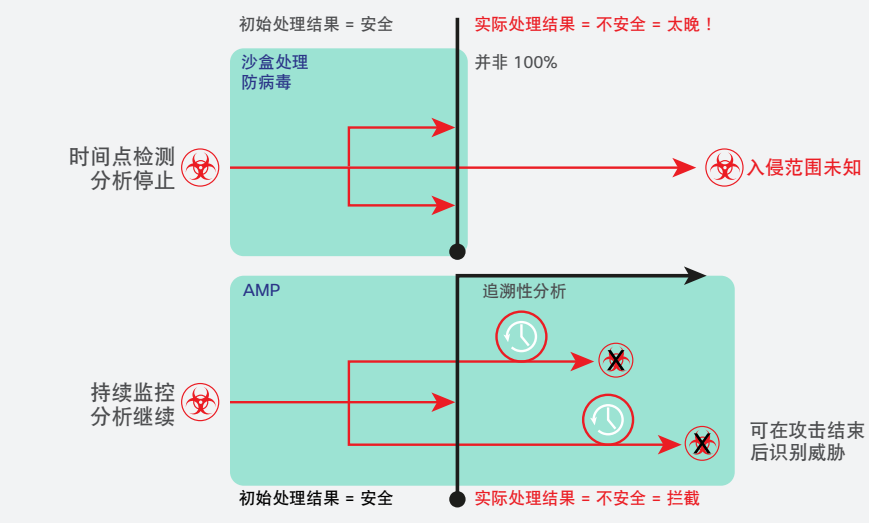
如今要有效地确保网络安全，不仅仅只是阻止用户导航至恶意网站。在合法网站上也可能下载到病毒或恶意软件。而且移动访问、社交媒体和交互式应用存在新的漏洞。随着网络威胁持续增加，拥有超越威胁检测、URL 过滤和应用控制等基本功能的解决方案至关重要。

您需要提供持续监控和分析的网络安全解决方案，以帮助安全团队捕获最隐蔽的威胁。您需要适用于网络安全的支持 WSA 感知威胁分析 (CTA) 的思科® 高级恶意软件防护 (AMP)。

AMP 为何如此重要

传统的网络安全措施已不足以阻止当前的高级威胁。AMP 与思科网络安全解决方案的集成，为您提供传统的网络安全功能和高级威胁防护功能，以抵御最高级的攻击。

图 1. 使用 AMP 进行追溯分析



AMP 将恶意软件检测、拦截、持续分析和追溯性警报（图 1）添加至您的思科网络安全工具许可证。功能包括：

- **灵活性和可选择性：**AMP 可与现有的思科安全网关集成，从而为您提供另外一种适合您环境的 AMP 部署选项。

- **高级沙盒处理：**获得关于试图进入网络的文件的行为、信誉和威胁级别的包含大量数据的详细分析。您获得对您的环境的可视性和可控性。
- **缩短发现在网络内部运行的威胁所需的时间：**将您的 Web 代理转变为安全传感器并自动调查可疑的 Web 流量。

后续行动

想要了解有关适用于网络安全的思科 AMP 的更多信息，请登录 http://www.cisco.com/go/ampforweb

思科的销售代表、渠道合作伙伴或系统工程师可以帮您评估思科网络安全将如何为您提供帮助。

- **文件信誉：**在文件通过思科网络安全网关时，AMP 会捕捉每个文件的指纹，并将其发送到思科的云端情报网络进行信誉鉴定。利用这些结果，您可自动拦截恶意文件，并应用管理员定义的策略。
- **文件分析：**借助 AMP Threat Grid 技术，您可以获得通过 Web 网关的未知文件的静态和动态分析（沙盒处理）。Threat Grid 在高度安全的环境中通过 700 多个行为指标及全球威胁情报来分析样本，以收集有关文件行为和威胁级别的准确详细信息。
- **文件追溯性：**AMP 可解决躲过边界防御的恶意文件的问题。无论最初的处理结果如何，AMP 会持续分析通过安全网关的文件。文件被识别为威胁后，AMP 会发出追溯性警报，让您一目了然地了解哪些用户可能已被感染以及何时被感染。这样安全团队就能在病毒有机会传播前迅速识别和解决攻击。

感知威胁分析帮助 AMP 进一步提高可视性

思科基于云的感知威胁分析解决方案是网络安全设备的 AMP 附加许可功能的一部分。借助感知威胁分析，您可以对进行中或试图在您的环境中运行的复杂隐秘攻击进行检测和做出响应。

将感知威胁分析与适用于网络安全的 AMP 集成，您可以：

- 自动识别和调查可疑或有恶意的基于 Web 的流量。
- 分析现有网络安全解决方案生成的信息，无需额外的硬件或软件。
- 锁定绕过安全控制并使用基于 Web 的通信（包括可用于攻击贵组织的标准通道、加密通道和匿名通道）的恶意活动。
- 创建正常活动基准并确定发生在您网络中的异常流量。
- 分析设备行为和网络流量以查明命令和控制通信以及数据渗露。

有关思科感知威胁分析的详细信息，请访问 www.cisco.com/go/cognitive。

C45-730851-03 10/16