概览

优势

- 攻击前、攻击中和攻击后的防护
- 快速检测、响应和修复隐蔽的恶意软件
- 无与伦比的全球威胁情报和恶意软件分析
- 深入了解危害的起源和影响范围
- 更明智的安全决策和更快速的调查
- 无处不在的保护：网络、终端、服务器和数据中心、移动设备、虚拟环境、邮件和 Web 网关

思科高级恶意软件防护

通过可视性与可控性进行漏洞防御、检测和补救

组织每天都在遭受着攻击，安全漏洞无处不在。黑客正在创造高深的恶意软件，甚至可躲过最先进的时间点检测工具，如防病毒软件和入侵预防系统。这些工具会在您的扩展网络入口点监测流量，但它们却无法百分之百地检测出所有试图潜入组织的威胁。此外，如果威胁规避掉一线防御，这些工具将无法针对其活动提供深入的可视性。这将导致 IT 安全团队对于潜在影响范围一无所知，并且无法在恶意软件造成损害之前快速将其检测出并进行遏制。

思科® 高级恶意软件防护 (AMP) 超越了时间点功能，可以在攻击前、攻击中和攻击后为组织提供全面的保护。

- **在攻击前**，AMP 使用最先进的全球威胁情报来增强防御。
- **在攻击中**，AMP 使用全球威胁情报、已知文件签名和动态文件分析技术，阻止恶意软件侵入您的 IT 环境。
- **在攻击后**，AMP 将持续监控和分析所有文件活动、进程和通信。如果文件显露出恶意行为，AMP 将做出检测，并提供追溯性警报、IoC、跟踪和分析，以便安全团队采取行动消除威胁。

AMP 不仅能防止漏洞，还可以迅速检测、控制并修复躲过了第一道防线的威胁。一切工作都能经济高效地完成，不会影响运营效率。

威胁情报和恶意软件分析

构建 AMP 的基础是广泛深入的实时威胁情报和动态恶意软件分析，它们来自思科综合安全情报、Talos 安全情报和研究小组、AMP Threat Grid 情报源。

组织将受益于：

- 每天 150 万个传入恶意软件样本
- 全球 160 万个传感器
- 每天 100 TB 的数据
- 130 亿 Web 请求
- 工程师、技术人员和研究人员组成的全球团队
- 24 小时运行

不间断分析和追溯性安全

- 不论最终采取何种处理方式，思科 AMP 甚至在完成初步检测之后，还不间断地监控、分析和记录所有文件活动和行为。
- 如果以前视为“未知”或“良好”的文件显露出恶意行为，AMP 将自动发送一个警报并显示该文件的活动和行为历史记录，以便您可以确定受影响范围并快速修复。

可视性与可控性

- 追溯性警报会通知您有关文件处置方式的任何变化，包括网络上哪些用户可能已被感染及其感染时间。
- 控制面板可确切显示威胁所在的位置、威胁所进行的活动以及根本原因，因此您可以快速进行遏制和修复。

灵活性和可选择性

- 思科 AMP 可在多个平台上部署：终端、网络、移动设备、虚拟环境、服务器等。组织可以按照自己喜欢的方式在所需地点部署此解决方案。

后续行动

有关 AMP 如何帮助您保护组织抵御高级网络攻击，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：www.cisco.com/go/amp。

思科 AMP 与 AMP Threat Grid 技术的集成还提供了情景丰富的情报源。针对 560 多个行为指标，该技术每个月对数以百万计的示例进行分析，最终形成数十亿的模拟威胁和简单易懂的威胁评级，能够帮助安全团队优先处理响应。

思科 AMP 将针对此背景丰富的强大知识库，自动关联文件、行为、遥测数据和活动，以阻止威胁、提供更强大的威胁洞察能力并做出更迅速、更轻松的响应。

不间断分析和追溯性安全

不论最终采取何种处理方式，思科 AMP 甚至在完成初步检测之后，还不间断地监控、分析和记录所有文件活动。如观察到可疑或恶意活动，AMP 便会将向安全团队发出警报和 IoC。用户还可通过 AMP 全面了解所发生的情况。安全团队可以看到威胁的完整记录，从而快速获取重要安全问题的答案，例如：

- 恶意软件来自何处?
- 哪些系统受到了影响?
- 威胁造成了什么影响?
- 如何阻止威胁?

借助此信息，安全团队可以使用 AMP 简单易用的基于浏览器的管理控制台快速采取行动。

灵活的部署选项

思科 AMP 解决方案可在多个平台部署（见表 1）。

表 1. 思科 AMP 部署选项

产品名称	详细信息
面向终端的思科 AMP	使用 AMP 的轻量级连接器对运行 Windows、Mac、Linux 系统的 PC、Android 移动设备和虚拟环境进行保护，不会对用户产生任何性能影响。通过 AnyConnect v4.1 也可启动面向终端的 AMP。
面向网络的思科 AMP	部署 AMP 作为与思科 FirePOWER™ 网络安全设备集成的基于网络的解决方案。
具有 FirePOWER 服务的面向 ASA 的思科 AMP	部署集成 AMP 功能到思科 ASA 自适应安全设备防火墙。
思科 AMP 私有云虚拟设备	部署 AMP 作为本地气隙解决方案，专门针对具有限制使用公共云的高隐私要求的组织。
面向 CWS、ESA 或 WSA 的思科 AMP	对于思科云网络安全 (CWS)，邮件安全设备 (ESA) 或网络安全设备 (WSA) 而言，可以启用 AMP 功能以提供追溯功能和恶意软件分析。
面向 Meraki MX 的思科 AMP	部署 AMP 作为 Meraki MX 安全设备的一部分，利用高级威胁功能进行基于云的简化安全管理。
思科 AMP Threat Grid	AMP Threat Grid 与思科 AMP 集成，提供增强的恶意软件分析。它还可以在云端或设备上部署为独立高级恶意软件分析和威胁情报解决方案。