适用于内容的思科高级恶意软件防护

思科高级恶意软件防护 (AMP) 提供独一无二的可在整个攻击过程（攻击前、攻击中和攻击后）中提供防护的高级恶意软件防护系统。它提供不间断分析和高级分析，可支持思科邮件与网络安全设备上的思科追溯性安全功能。此功能可让安全管理员开展追溯分析来调查系统中的威胁。高级分析和综合智能可判断一个文件是否安全不可疑。如果经过进一步分析后，文件的处置方式发生变化，系统就会发出警告。利用文件沙盒可以在一个高度安全的环境中执行、分析及测试恶意软件行为。有了这些追溯性安全工具，您可以在漏洞事件中确定攻击范围、可视性和可控性，帮助安全团队快速有效地修复环境中的所有威胁，避免事态失控。

仅时间点检测的缺陷

仅时间点检测并不能保证 100% 有效。只要一个威胁能避开检测就会威胁您的环境。老谋深算的攻击者采用针对性的情景感知恶意软件，且拥有丰富的资源、专业知识及超人的毅力，可随时攻破时间点防御，威胁任何组织。此外，出现漏洞后，时间点检测根本无法确定漏洞的范围和深度。

适用于内容的 AMP 的功能

适用于内容的 Cisco AMP 基于三大主要功能：

- **文件信誉：**在文件通过网关时，AMP 会捕捉每个文件的指纹，并将其发送到 AMP 的云端情报网络进行信誉鉴定以找出零日漏洞。
- **文件沙盒处理：**检测到恶意软件时，AMP 会收集有关文件行为的精确详细信息。然后，AMP 会结合人工与机器分析的详细数据来判断沙盒中文件的威胁级别。
- **不间断分析：**适用于终端的 AMP 超越了时间点检测功能，它使用基于云的大数据分析，并通过不断重新评估随时间收集的新数据和历史数据来检测隐藏的攻击。

这些功能支持多种性能，包括以下内容。

针对高级威胁的追溯性安全：为了有效抵御高级威胁和定向攻击，AMP 并不依靠恶意软件签名，因为创建每个新恶意软件样本的签名需要几个星期或几个月的时间。相反，AMP 使用文件信誉和文件沙盒来识别和拦截那些含有未知签名的恶意文件。追溯性文件分析具有一项独一无二的功能，它能够让您及时返回查明爆发发生的时间并查看攻击的范围。

覆盖整个攻击时间轴的保护：在整个攻击过程（攻击前、攻击中和攻击后）内获得保护。思科智能运营中心 (SIO) 的垃圾邮件过滤和零日威胁情报可将威胁拦截在进入网络之前，同时文件信誉和文件沙盒能在攻击过程中识别威胁。最后，追溯性分析可在高级恶意软件躲过其他防御层之后，提供攻击后保护。

可视性与可控性：您可以通过包含丰富数据并且一目了然的报告，了解那些曾经试图进入网络的文件的信誉和行为，并且如果处置方式出现任何变化，您都会收到通知，包括网络上哪些用户可能已被感染及其感染时间。您可以根据文件信誉和文件行为等数据来制定策略，确定安全网关所要采取的操作（允许、拦截或隔离）。

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 部署方式，让您获得灵活性和可选择性。通过将 AMP 激活为思科网络与邮件安全的附加许可功能，您可以使用最简单、最具成本效益的方法获得高级恶意软件防护。

追溯性安全：追溯性安全功能能够回顾并跟踪进程、文件活动和通信，从而了解感染的完整范围、确定根本原因并执行补救。只要出现威胁表现（例如事件触发器、文件处置方式发生变化或 IoC 触发器），就需要追溯性安全。

优势

- 准确地检测文件中的恶意软件
- 发现以前未知的零日威胁
- 找到并禁用已成功避过初始防御系统的恶意软件

综合安全智能

思科 SIO 与 Sourcefire 漏洞研究团队 (VRT) 联合推出的综合安全情报集结了大量实时威胁情报。（Sourcefire 现已成为思科的一员。）该情报收集包括分布在全球各地的 160 万个传感器。每天，我们会收到 100 TB 的数据和超过 18 万件的文件样本，而且，我们能够监测全球 35% 的邮件流量。超过 600 位工程师、技术人员和研究人员使用 40 多种语言，一年 365 天昼夜不停地分析此类信息以及公共与私人威胁源。同时，我们还与 FireAMP™、Snort、ClamAV 社区保持着不间断互动，并参与了 Sourcefire 宣传、教育、指导和情报共享 (AEGIS) 计划，这有助于我们共享威胁情报和最佳修复方法。所有的这一切意味着我们已为应对未来攻击做好更充分的准备。

为什么选择思科?

思科提供了业界最广泛的集成高级恶意软件防护解决方案产品组合，为客户提供持续的可视性和可控性，以抵御恶意软件对整个扩展网络的功能，并在整个攻击过程（攻击前、攻击时和攻击后）中提供保护。作为跨越思科电邮和 Web 安全、FirePOWER® 网络安全设备、移动和虚拟系统以及 PC 终端保护的集成功能，AMP 可以提供灵活的部署选项和广泛的覆盖范围，将不断扩展的攻击载体拒之门外。

后续行动

想要了解更多信息，请登录思科 AMP 主页。此外，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产品将如何为您提供帮助。

C45-731873-00 05/14