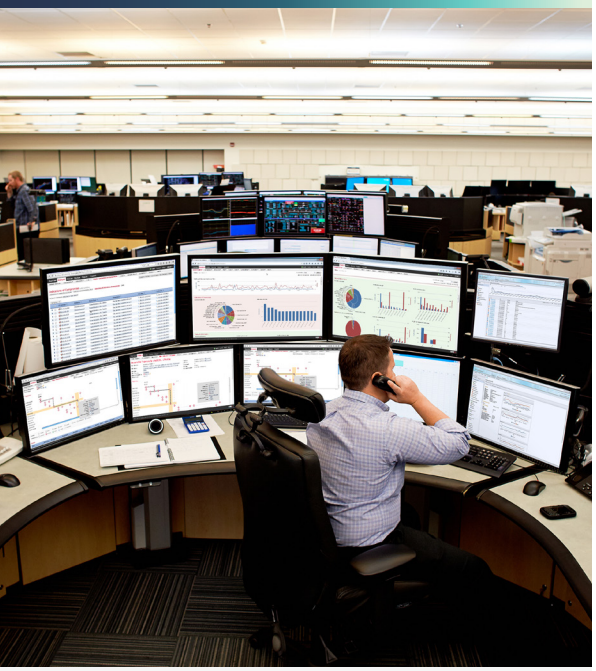
概览



优势

- **检测并阻止**漏洞攻击企图、恶意文件和违反策略的文件
- **持续分析和记录**文件活动以跟踪恶意软件的传播和影响范围
- **将分散事件与**协同攻击相关联
- **获取深度可视性和可控性**以快速检测、分析并遏制漏洞
- **通过无与伦比的全球威胁情报**加强网络防护
- **通过** AMP 提供的易于使用的基于 Web 浏览器的控制台、FireSIGHT 管理中心管理解决方案

适用于网络的思科高级恶意软件防护

针对实际情况的漏洞防护、检测和响应

组织每天都在遭受着攻击，安全漏洞无处不在。黑客们还会开发高级恶意软件，这些软件甚至可以规避最好的时间点检测工具，例如防火墙和入侵防御系统。这些工具会在网络入口点监测流量，但这对于检测所有试图潜入组织的威胁并不是百分百有效。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。

适用于网络的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，为组织提供全方位保护。

- **在攻击前**，AMP 使用最佳全球威胁情报加强网络防御。
- **在攻击中**，AMP 使用该情报、已知文件签名和动态文件分析技术，阻止恶意软件入侵网络。
- **在攻击后**，或者在文件遍历网络之后，AMP 将持续监控和分析所有文件活动和流量。如果文件显露出恶意行为，AMP 将对威胁活动提供深入的可视性，并使用户可快速响应威胁并进行遏制。

适用于网络的 AMP 不仅提供漏洞防御功能，而且还在出现未察觉入侵的情况下，提供快速漏洞检测、响应和遏制功能 – 所有这些都具有成本效益且不影响运营效率。

威胁情报和动态恶意软件分析

适用于网络的 AMP 基于 Cisco 综合安全情报和 Talos 安全情报和研究小组提供的最大实时威胁情报和动态恶意软件分析集合构建。组织将受益于：

- 每天 110 万传入恶意软件示例
- 全球有 160 万个传感器
- 每天 100 TB 的数据
- 130 亿网络请求
- 600 位工程师、技术人员和研究人员
- 24 小时运营

根据这一信息，AMP 将生成可操作情报，例如威胁评分以帮助安全团队确定响应的优先次序。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，以阻止威胁试图渗入网络。安全团队通过 AMP 可以深入了解网络内的威胁，并能够对事件更轻松地做出更快响应。

特点

不间断分析：即使在文件遍历网络控制点后，AMP 仍可继续监控、分析和记录文件活动和行为，以快速检测规避了一线防御的恶意软件。

追溯性安全：如果以前视为“未知”或“良好”的文件显露出恶意行为，AMP 将发送一个追溯性警报并显示该文件活动的历史记录，以便您可以确定受影响范围并快速响应。

Cisco FireSIGHT 管理中心：通过单一管理平台上的威胁活动、主机、操作系统、应用、用户、文件以及地理位置信息视图了解您的环境。

动态恶意软件分析和沙盒功能：一个高度安全的环境，可帮助您针对大量行为指标启动并分析恶意软件，以发现以前未知的零日威胁。

危害表现 (IoC)：AMP 将自动关联多源安全事件数据，如文件、遥测、入侵和恶意软件事件并将其作为潜在活动漏洞优先处理。这有助于安全团队将这些事件与更大的协同攻击关联并优先处理高风险事件。

文件轨迹：文件传播会随着时间推移得到持续跟踪，以提供可视性并缩短确定恶意软件影响范围的时间。

与适用于端点的 Cisco AMP 集成：为增加对端点上可执行活动的可视性并将网络事件与端点事件相关联，适用于网络的 AMP 与适用于端点的 AMP 相集成。

不间断分析和追溯性安全

适用于网络的 AMP 可以持续监控、分析并记录所有文件活动（无论处置如何），即使在网络控制点的初始检查后也是如此。如果 AMP 观察到可疑或恶意的活动，或者，如果以前被视为“良好”的文件变“坏”了，安全团队将发送一个追溯警报并指示受影响范围。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历史记录，从而确定恶意软件的回滚时间并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？
- 如何停止威胁？

使用“文件轨迹”功能，安全团队可以查看文件传输随着时间推移的直观显示以及文件的其他信息，从而跟踪通过网络的文件传输。然后，可以轻松地使用简单的策略更新和自定义检测列表阻止这些恶意文件和通信。您一旦有所决定就可开始操作，无需等待供应商提供更新。

这得益于不间断分析与追溯性安全，安全团队通过其获得可视性与可控性，以快速检测、响应并遏制威胁。

部署

适用于网络的 AMP 通过 Cisco FireSIGHT ™ 管理中心进行管理，这是一个易于使用的基于 Web 的管理控制台。其作为思科 FirePOWER 下一代入侵防御系统 (NGIPS) 的订阅进行部署，涵盖大范围的网络吞吐量和处理能力。

后续计划

联系思科销售代表或渠道合作伙伴以了解适用于网络的 AMP 如何帮助组织防御高级网络攻击。更多详情，请访问 www.cisco.com/go/ampnetwork。

C45-731875-01 03/15