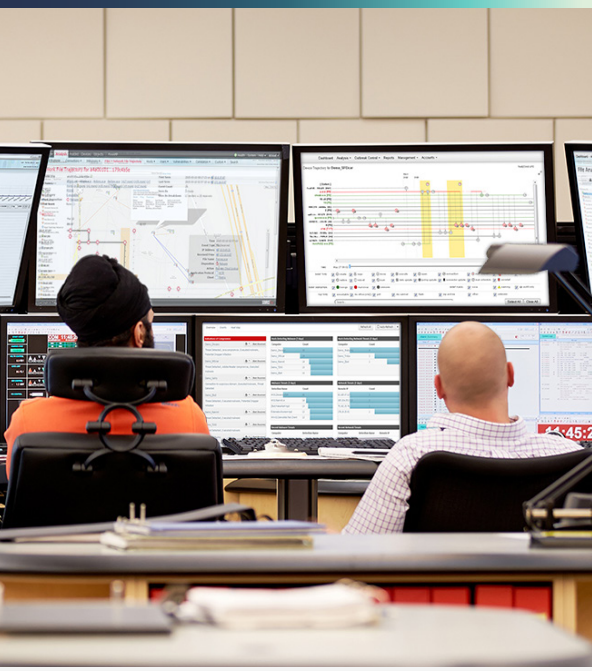
概览



优势

- **不间断检测并监控**恶意软件，立即处理并进行追溯性分析
- **保护 PC、Mac、移动设备**和虚拟环境
- **随时记录文件活动**，跟踪恶意软件的传播并确定感染范围
- **将分散事件与**协同攻击相关联
- **接入全球威胁情报**，增强网络防御
- **拥有全面的可视性和可控性**，快速检测、分析和修复漏洞

思科终端高级恶意软件防护

现实情况中的漏洞预防、检测、响应和修复

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。这些工具对检测所有威胁并不是 100% 有效。此外，如果躲过了最初检测，这些工具几乎不能再检测到威胁。这使 IT 安全团队无法看到潜在的感染范围，并且无法在恶意软件造成破坏之前快速检测并修复恶意软件。

面向终端的思科 ® 高级恶意软件防护 (AMP) 超越了时间点工具的功能，能够在攻击前、攻击中和攻击后，对组织进行保护。

- **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 IT 环境。
- **在攻击后**，AMP 监控所有文件和可执行活动，以捕获躲过最初检测的恶意软件，并提供可视性和可控性，从而快速修复恶意软件。

面向终端的 Cisco 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。

威胁情报和动态恶意软件分析

构建 Cisco 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 Cisco 综合安全情报、Talos 安全情报和研究小组、AMP Threat Grid 情报源。

组织将从以下方面受益：

- 每天 110 万传入恶意软件示例
- 全球有 160 万个传感器
- 每天 100 兆兆字节数据
- 130 亿网络请求
- 600 多位工程师、技术人员和研究人员
- 24 小时运行

面向终端的 Cisco AMP 与 AMP Threat Grid 技术的集成还提供了情景丰富的情报源。针对 350 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。

特点

不间断分析和追溯性安全：AMP 不间断监控、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，帮助您确定感染范围并快速做出响应。

动态恶意软件分析和沙盒：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)：文件和遥测事件进行关联，并作为潜在活动漏洞优先处理。AMP 可自动关联多个来源的安全事件数据（例如入侵与恶意软件事件），以帮助安全团队将事件关联到协同攻击，并优先处理高风险事件。

设备轨迹：您可以持续跟踪设备和系统级的可执行操作和通信，以快速了解导致损害的根本原因以及事件历史记录。

感染率：AMP 按照感染率显示组织中运行的所有文件，以帮助您发现之前未检测到但被少量用户看到的威胁。只能由少数用户打开的文件可能是恶意的。

漏洞：AMP 显示您系统上易受攻击的软件列表，如果主机包含该软件，则主机可能受到感染。AMP 可识别易受攻击软件以及潜在漏洞，为您提供按优先顺序排列的需修补的主机列表。

病毒爆发控制：AMP 帮助您实现可疑文件或病毒爆发的控制和修复，而无需等待内容的更新。它还具有以下优点：

- 跨所有或选定系统，快速阻止特定文件
- 阻止多态恶意软件系列
- 包含用作恶意软件网关的感染应用，并终止再次感染
- 从源头上阻止恶意软件回拨通信，即使在公司网络外的远程端点也可以阻止
- 在任何情况下，帮助确保完成关键任务的应用程序继续运行

有关更多的功能，请参阅面向端点 AMP 产品手册。

不间断分析和追溯性安全

不论最终采取何种处理方式，面向终端的 Cisco 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和可执行操作。如果 AMP 观察到可疑活动，将会向安全团队发送警报。安全团队可以看到威胁的完整历史记录，并且快速地得到有关以下问题的答案：

- 恶意软件来自何处？
- 进入的方法和进入点是什么？
- 它曾到过何处？ 哪些系统受到了影响？
- 威胁执行过什么操作，它现在正在执行什么操作？
- 我们如何阻止威胁并消除根本原因？

从 AMP 基于浏览器的管理控制台点击几下，就可以阻止文件在另一个终端上执行操作。既然 Cisco AMP 知道该文件曾到过的所有其他终端，它就可以将该文件从内存中拖出，并将其与所有用户隔离。安全团队不再需要重新映像完整的系统来消除恶意软件。重新映像需要时间、金钱和资源。借助 AMP，恶意软件补救就像是外科手术，而不会对 IT 系统或业务造成相关联的附带损害。

此外，AMP 会记录它所看到的内容，从威胁的签名到文件的行为，并在 AMP 威胁情报数据库中记录这些数据。这会进一步强化第一道防线，因此，该文件和类似文件将无法再次躲过最初检测。

部署

面向端点的 Cisco AMP 是通过易于使用、基于 Web 的控制台管理的。它通过 AMP 轻量级终端连接器部署，不会影响用户的性能 – 分析是在云中完成的，而非终端。这种解决方案在终端上作为订阅提供，包括 PC、Mac、移动设备和虚拟系统。

后续计划

有关面向终端的 Cisco AMP 如何帮助您保护组织免遭高级网络攻击，请与思科销售代表或渠道合作伙伴联系。更多详细信息，请访问 www.cisco.com/go/ampendpoint。

C45-731874-03 03/15