优势

- 通过详细而切实可行的报告和分析提供对整个环境的可视性与可控性
- 为您的安全分析师创建切实可行的情报，包括追溯性安全
- 将面向终端的高级恶意软件防护与您的现有安全流程相集成
- 确保您的员工掌握在整个互动过程中通过知识传授运行解决方案的技能
- 针对不同的部门构建定制的防护配置文件
- 充分利用供应商最佳实践，满足与实施相关的内部和外部审核要求

面向终端的思科 AMP 部署

防范恶意软件入侵您的网络终端

即使您在网络入口实施了最佳防护措施，您仍需要为内部提供保护。面向终端的思科® 高级恶意软件防护 (AMP) 为您提供的正是这种全面保护。当犯罪分子试图进入您的网络时，入侵防御系统可以一举将其抓获，但这不过是对传入通信的一次性评估而已。一旦某个文件潜入网络，入侵防御系统就无法再发现其踪迹。如果某个文件通过了网络入口，被发现是恶意软件，那该怎么办?

AMP 具有持续数据收集和高级分析功能，采用独一无二的高级恶意软件防护系统，可在整个攻击过程（攻击前、攻击中和攻击后）中为终端提供防护。安全管理员能够利用追溯、攻击链互联、危害行为表现 (IoC)、轨迹和漏洞搜索等思科追溯性安全工具提供的信息对威胁执行追溯性分析。您可以通过跟踪进程、文件活动和通信，了解感染的完整范围，确定根本原因并执行补救。

面向终端的思科高级恶意软件防护 (AMP) 部署服务可以帮助您顺利安装此防护。我们可以在 45 天内对六 (6) 个终端组完成实施的部署、配置、测试和初始调整。我们利用思科最佳实践帮助您避免各种错误，以防这些错误减缓部署速度、增加成本，以及让您的网络失去保护。

实现防护快速启动和运行

规划和实施部署不仅速度相当快，而且非常详尽全面。以下是我们在部署前、部署中和部署后采取的措施。

部署前

- 执行远程启动呼叫和项目计划审核，确定关键利益相关者，并提供项目管理计划（包括活动时间表和计划）
- 基于网络拓扑审核、资产分类、当前技术配置和防御状况提供配置及部署建议
- 查看客户的信息安全、信息技术、变更控制策略和物料清单
- 查看与部署、策略、设计和配置相关的最佳实践

部署中

- 定义面向终端的 AMP 策略
- 确定初始 alpha 部署终端
- 部署面向终端的 AMP（带有数量有限的预定义终端连接器）的 alpha 实施，并进行配置、初始调整和验证
- 确定受限生产部署的优先终端
- 最多对六个终端组执行统一连接器软件包推送

部署后

- 验证受限生产部署的性能并提供远程补充优化调整（约部署后 30 天）
- 进行有关使用面向终端的 AMP 分析组件的知识传授
- 提供并查看对面向终端的 AMP 部署进行总结的部署摘要报告 (DSR)

面向终端的思科 AMP 部署以两种规格出售：最多 5000 台设备的部署或最多 25,000 台设备的部署，可自定义范围以满足您的特定需求。

后续行动

有关详情，请访问 www.cisco.com/go/services/security 。