思科高级恶意软件防护

针对实际情况的漏洞防御、检测、响应和补救

优势

- 通过无与伦比的全球威胁情报加强一线防御
- 深入了解危害的起源和影响范围
- 快速检测、响应和补救恶意软件
- 避免昂贵的重复感染和补救方案
- 随时随地保护 - 网络、终端、移动设备、邮件、网络 - 攻击前、攻击中和攻击后

如今，针对组织的网络攻击层出不穷，安全入侵事件屡屡登上新闻头条。现今，全球的黑客群体正在不断制作出高级恶意软件并通过各种攻击媒介侵入组织。这种多层面的定向攻击甚至可以躲过最出色的防御工具。防御工具会在网络入口点检查流量和文件，阻止已知威胁，但是“良好”或“未知”的文件都能进入网络。遗憾的是，防御工具的分析将到此为止。如果隐蔽的恶意文件能够避开这些防线并侵入系统，这些工具基本无法对已入侵的威胁进行的活动提供任何可视性。这会导致安全专业人员对潜在危害的影响范围一无所知，无法在恶意软件造成明显损害之前快速检测恶意行为、快速响应，以及遏制并消除恶意软件。

思科® 高级恶意软件防护 (AMP) 是一个能够解决高级恶意软件整个生命周期问题的安全解决方案。它不但能防止出现漏洞，还可提供可视性、情景感知能力与可控性，确保能够快速检测躲过一线防御的威胁，并做出遏制和补救。更重要的是，这些功能是在不影响运营效率的情况下，以具有成本效益的方式实现的。

产品概述

AMP 是情报驱动的、集成式企业级高级恶意软件分析和保护解决方案。您可以在攻击全程（攻击前、攻击中和攻击后）中为组织获取全面的防护。

- **攻击前**：AMP 使用来自思科 Talos 安全情报和研究团队以及 Threat Grid 威胁情报源的全球威胁情报，帮助加强防御，并防范各种已知威胁和新型威胁。
- **攻击中**：AMP 将这些情报与已知文件签名相结合，运用思科 Threat Grid 的动态恶意软件分析技术来识别并阻止违反策略的文件类型、漏洞尝试及尝试渗入网络的恶意文件。

- **攻击后**（即对文件执行最初的检查后）：AMP 可超越时间点检测功能（即进行不止一次的检测），持续监控和分析所有文件活动及流量（无论处置方式如何），以搜索任何恶意行为迹象。如果未知或之前被视为“良性”处置的文件开始出现不良行为，AMP 将对其进行检测并立即向安全团队发出警报，提示出现危害迹象。然后，它会提供全面的可视性，以供深入了解恶意软件的源头、受影响的系统，以及恶意软件正在进行的活动。它还提供各种控件，迅速地响应入侵，并且只需点击几下即可进行补救。这使得安全团队能够获得所需的深入可视性与可控性，以快速检测出攻击、确定受影响范围并在恶意软件造成损害之前并对其进行遏制。

全球威胁情报和动态恶意软件分析

AMP 的构建基于无与伦比的安全情报和动态恶意软件分析。思科 Talos 安全情报和研究团队以及 AMP Threat Grid 威胁情报源代表了行业领先的实时威胁情报和大数据分析集合。此数据将从云推送至 AMP 客户端，以便您通过最新的威胁情报，主动防御各种威胁。您将从以下优势中获益：

- 每天 150 万个传入恶意软件样本
- 全球有 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

AMP 对照此强大、情景丰富的知识库关联文件、行为、遥测数据和活动以快速检测恶意软件。安全团队受益于 AMP 的自动化分析，节省了搜索漏洞活动时间并随时拥有最新的威胁情报，可以快速了解、优先处理和阻止复杂的攻击。

我们 Threat Grid 技术与 AMP 相集成，还可以：

- 按照标准格式提供的高度准确和情景丰富的情报源与现有安全技术无缝集成
- 每月对照 700 多个行为迹象对数百万示例进行分析，可生成数十亿标样
- 简单易懂的威胁指数，帮助安全团队确定威胁的优先级

AMP 使用所有这些情报和分析告知您安全决策，或自动地代表您采取行动。例如，借助不断更新的情报，系统可以阻止已知恶意软件和违反策略的文件类型，动态地将已知恶意的连接放入黑名单，并阻止从那些被归类为恶意的网站和域下载文件。

不间断分析和追溯性安全

大多数基于网络和终端的防恶意软件系统仅在文件穿过控制点进入您的扩展网络时检查文件。这也是分析终止的地方。但是，恶意软件比较复杂并且擅长规避初始检测。休眠技术、多态、加密和使用未知协议是恶意软件用于遮蔽自身的一些方法。您无法防范您看不到的事物，这也是大多数安全漏洞产生的原因。安全团队在入口点看不到威胁且在事后无视它的存在。他们不具备可供快速检测或遏制威胁的可视性，不久之后，恶意软件实现了目标，损害也已经造成。

思科 AMP 则不同。AMP 系统认识到时间点、主动检测和拦截方法并不是百分百有效，因此即使通过了初始检测，之后也会持续分析文件和流量。AMP 监控、分析并记录终端、移动设备上以及网络中的所有文件活动和通信，以便快速找到显露出可疑或恶意行为的隐蔽威胁。一旦出现麻烦，AMP 就会向安全团队发出警报并提供有关威胁行为的详细信息，以便您可以回答重要的安全问题，例如：

- 恶意软件来自何处？
- 进入的方法和入口点是什么？
- 它在何处以及哪些系统受到影响？
- 威胁的目的是什么以及它正在做什么？
- 如何阻止威胁并消除根本原因？

使用此信息，安全团队能够及时了解情况并使用 AMP 的遏制和补救功能采取行动。通过 AMP 中易于使用的、基于浏览器的管理控制台，管理员只需点击几下，即可通过阻止此文件在另一个终端上再次执行，从而遏制恶意软件。而且，由于 AMP 知晓文件曾经去过的所有地方，因此它可以将文件从内存中去除并将其与所有其他用户隔离。在恶意软件入侵时，安全团队不再需要重新映像整个系统以消除恶意软件。那样做需要耗费时间、资金和资源，并且会中断关键业务功能。采用 AMP 后，恶意软件补救类似一个外科手术，不会对 IT 系统或业务造成相关的间接损害。

这就是持续分析、持续检测和追溯性安全功能的强大所在 - 能够记录系统中每个文件的活动。并且，如果认为“良性”文件变“坏”了，则能够对其进行检测并回退历史记录以查看该威胁的起源和其显露的行为。然后，AMP 会为您提供内置响应和补救功能以消除威胁。AMP 还会记住其所见内容（从威胁的签名到文件的行为），并将这些数据记录在 AMP 的威胁情报数据库中以进一步加强一线防御，因此该文件及类似的文件将无法再次规避初始检测。

借助 AMP，安全团队具备了必要的深入可视性与可控性，可以快速、有效地检测攻击并发现隐蔽的恶意软件；了解并确定受影响范围；在恶意软件（甚至是零日攻击）造成任何损害之前快速将其遏制并补救；并防止类似的攻击发生。

主要特性

AMP 的持续分析和追溯性安全功能的实现皆是因为以下这些强大特性：

- **全面的全球威胁情报：**思科 Talos 安全情报与研究团队和 Threat Grid 威胁情报源是行业最大的实时威胁情报集合，不仅拥有最广泛的监视和覆盖范围，并且能够跨多个安全平台实施。
- **危害表现 (IoC)：**将文件和遥测事件进行关联，并根据潜在活动漏洞确定优先级。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更大规模的协同攻击并优先处理高风险事件。
- **文件信誉：**将高级分析与综合情报相结合，以确定文件是安全还是具有恶意，从而进行更为准确的检测。
- **防病毒引擎：**执行脱机和基于系统的检测（包括 Rootkit 扫描），以补充思科高级终端保护功能（例如本地 IoC 扫描以及设备和网络流量监控）。通过启用和使用该引擎，客户可以将防病毒和高级终端保护整合到一个代理中。
- **静态和动态恶意软件分析：**高度安全的沙盒环境可帮助您运行、分析和测试恶意软件，以发现之前未知的零日威胁。AMP 解决方案中集成了 Threat Grid 的沙盒与静态和动态恶意软件分析技术，因此可以根据更大的一组行为迹象进行更为全面的分析。
- **追溯性检测：**如果文件处置在扩展分析之后发生了变化，AMP 会发出相关警报，以便您知晓并发现成功躲过初始防御的恶意软件。
- **文件轨迹：**文件在您环境中的传播会随着时间推移得到持续跟踪，以实现可视性并缩短确定恶意软件影响范围的时间。
- **设备轨迹：**持续跟踪设备上和系统级的活动和通信，以在损害后快速了解导致损害的根本原因以及事件历史记录。

- **弹性搜索：**跨文件、遥测以及综合安全情报数据的简单无界搜索可帮助您快速了解暴露给 IoC 或恶意应用的情景和范围。
- **威胁防御常见度：**按照威胁防御常见度从最低到最高的顺序，显示组织内已运行的所有文件，以帮助您发现之前未检测到但被少量用户发现的威胁。少数用户运行可能具有恶意的文件（例如一个定向高级持续威胁）或可疑应用。您可能不希望自己的扩展网络上存在。
- **终端 IoC：**用户可以提交其自己的 IoC 以捕捉定向攻击。这些终端 IoC 允许安全团队对特定于其环境中应用的鲜为人知的高级威胁执行更为深入调查。
- **漏洞：**通过列表指出您系统上存在漏洞的软件、包含该软件的主机，以及最可能受到损害的主机。凭借我们的威胁情报和安全分析，AMP 可识别易受恶意软件攻击的软件和潜在的漏洞，为您提供按优先顺序排列的需要修补的主机列表。
- **爆发控制：**实现对可疑文件或爆发的掌控，无需等待内容更新即可修复感染。在爆发控制功能中：
  - 简单自定义检测可以跨所有或选定系统，快速阻止特定文件
  - 高级自定义签名可以阻止多态恶意软件系列
  - 应用阻止列表可以强制执行应用策略或遏制受危害应用用作恶意软件网关并终止再次感染循环
  - 自定义白名单，有助于确保安全、自定义或关键任务型应用无论如何都可继续运行
  - 设备流关联将在源头阻止恶意软件回调通信，尤其针对公司网络之外的远程终端

部署选项让保护无处不在

网络犯罪分子通过各种入口点向组织发起攻击。为了真正有效地捕获隐蔽攻击，组织需要尽可能多地了解各种攻击媒介。因此，AMP 解决方案可部署在整个扩展网络中的不同控制点。组织可以按照自身特定的安全需求，以喜欢的方式在所需地点部署此解决方案。选项如下表所列：

产品名称	详细信息
面向终端的思科 AMP	使用 AMP 的轻量级连接器保护运行 Windows、Mac、Linux 系统的 PC，对用户不会产生任何性能影响。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 NGIPS 安全设备集成的基于网络的解决方案。
防火墙和具备 FirePOWER 服务的 ASA 上的思科 AMP	部署集成到思科 NGFW 或 ASA 自适应安全设备防火墙中的 AMP 功能。
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。
ESA 或 WSA 上的思科 AMP	对于思科邮件安全设备 (ESA) 或网络安全设备 (WSA) 而言，可以启用 AMP 功能以提供追溯性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 Threat Grid	Threat Grid 与思科 AMP 集成，能够增强恶意软件分析能力。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。

现在，思科高级恶意软件防护真正能够做到“无处不在”。这种跨多种攻击媒介的可视性与可控性，从网络边缘到终端，正是您快速发现和消除隐秘恶意软件所需要的。但是，要快速彻底地采取行动，您还需要在您的整个基础设施中共享信息的能力。这些解决方案之间的互联、通信和集成也是亮点所在。它们不是孤立工作的单点产品。这些解决方案部署到一起时，可以相互协作，提供集成式防御，有系统地快速应对威胁。这些 AMP 解决方案将形成一个生态系统，在所有部署方案之间自动分享威胁情报、危害表现、事件信息以及隔离信息。凭借 AMP“无所不在的防御”，组织可以大幅缩短检测恶意软件和实施补救的时间。

思科 AMP 在第三方测试中一马当先

根据《2016 年 NSS Labs 漏洞检测系统比较分析报告》，思科在 NSS Labs 的漏洞检测系统报告中连续三年一马当先。2016 年 NSS Labs 产品比较测试详细介绍了思科 AMP 如何实现以下成就：

- 获得 100% 的安全效力评分，这是所有受测供应商中的最高分
- 在测试期间对恶意软件、漏洞攻击和逃避技术的检测率和阻止率均达到 100%，在所有接受测试的供应商中仅此一家
- 检测速度在所有接受测试的供应商中排名第一
- 性能卓越，对终端或应用延迟的影响最小

为什么选择思科？

问题不是你是否会遇到安全攻击，而是什么时候会遇到。单靠防御工具无法做到万无一失，无法主动检测和阻止所有攻击。有些攻击终会成功。因此，在出现漏洞后，组织需要准备工具快速检测入侵、响应并补救。

思科 AMP 是一款情报驱动的集成式企业级高级恶意软件分析和保护解决方案。它可提供加强网络防御的全球威胁情报和实时阻止恶意文件的分析引擎，并能够在初始检查后持续监控和分析所有文件行为和流量。这些功能可提供无与伦比的可视性与可控性，以便您深入了解潜在的威胁活动并随后快速地检测、遏制并消除恶意软件。

思科 Capital

提供融资服务，助您实现目标

思科 Capital® 融资有助于您获得所需的技术来实现目标和保持竞争力。我们可以帮助您减少资本支出。加速业务发展。并优化投资和投资回报率。借助思科 Capital 融资服务，您在购买硬件、软件、服务和第三方补充设备时将拥有更多灵活性。思科 Capital 可以为您提供一种可预测的支付方式。思科 Capital 目前在 100 多个国家/地区推出了融资服务。了解更多。

后续计划

要了解有关思科 AMP 的详情，请访问 http://www.cisco.com/go/amp。您还可观看这个简短的概述视频，查看对此技术的简明演示或详细演示，听取客户评价，了解 AMP 的竞争优势，或联系您的思科销售代表，与思科 AMP 专家一起设置 POV。

美洲总部
Cisco Systems, Inc.
加州圣何西

亚太地区总部
Cisco Systems (USA) Pte.Ltd.
新加坡

欧洲总部
Cisco Systems International BV
荷兰阿姆斯特丹

思科在全球设有 200 多个办事处。地址、电话号码和传真号码均列在思科网站 www.cisco.com/go/offices 中。

美国印刷 C22-734228-05 11/16