思科终端高级恶意软件防护

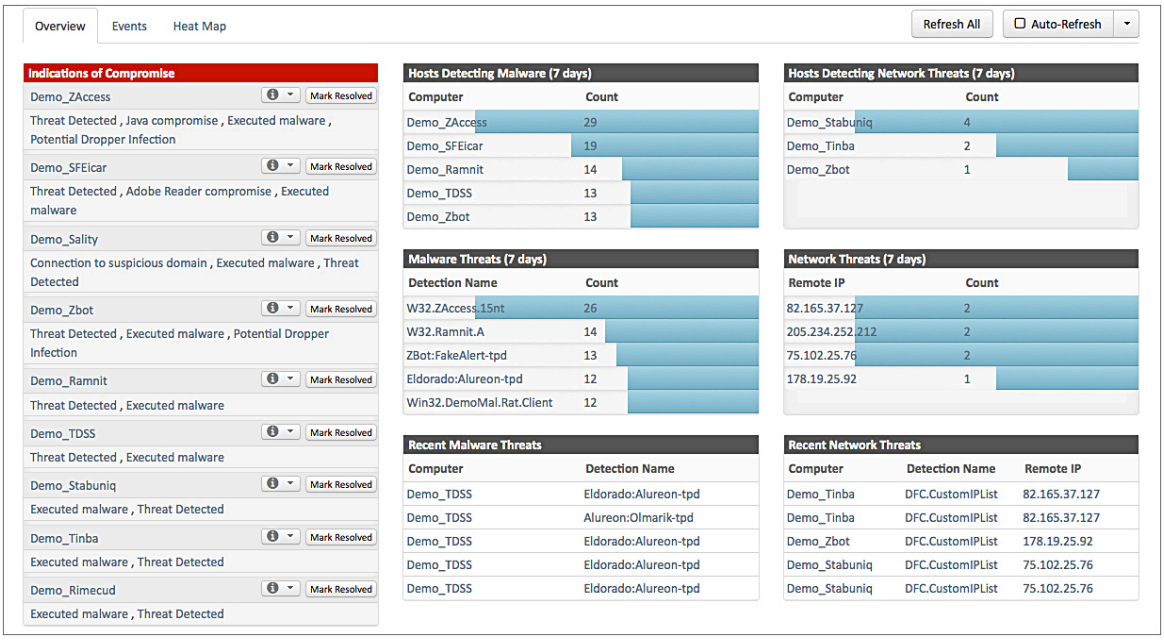
产品概述

当今的恶意软件高度复杂，您对终端的保护必须贯穿攻击前、攻击中和攻击后整个过程。面向终端的思科® 高级恶意软件防护 (AMP) 超越时间点检测，可提供所需的可视性和可控性，帮助您阻止未被其他安全层发现的高级威胁。您可以在整个攻击过程中（攻击前、攻击中和攻击后）为贵组织带来全面的全程保护。面向终端的思科 AMP 是一种智能的企业级高级恶意软件分析与防护解决方案，它采用了一种遥测模型，这种模型依靠大数据、不间断分析和高级分析，跨所有终端（PC、Mac、移动设备和虚拟系统）检测、跟踪、分析、控制和拦截高级恶意软件攻击。

您可以获得以下优势：

- **超越时间点的保护：**面向终端的思科 AMP 超越时间点检测持续分析文件和流量。此功能帮助实现追溯性安全，您可以回顾并跟踪进程、文件活动和通信，以了解感染的完整范围，确定根本原因并执行补救。结果：实现对贵组织更有效、更高效且更广泛的保护。
- **实现无与伦比的可视性的监控：**面向终端的思科 AMP 提供不仅限于追溯的功能。它引入新的情报级别，将各种形式的追溯性信息与一系列可供实时分析的活动联系并关联在一起。然后，它可从个别终端或整个终端环境寻找恶意行为的模式。
- **持续关注行为的高级分析：**面向终端的思科 AMP 通过高级行为检测功能实现自动化，该功能可提供经过优先级划分和整理的危害与风险高发区域视图。
- **变被动为主动的调查：**面向终端的思科 AMP 将活动从在调查期间寻找事实和线索转变为专注于根据实际事件（例如恶意软件检测和行为危害表现 [IoC]）搜寻漏洞。
- **真正简单的控制：**面向终端的思科 AMP 提供对事件链以及情景（用于对其控制面板和轨迹视图加以补充）的可视性。AMP 能够将特定应用、文件、恶意软件和其他根本原因锁定为目标。切断攻击链将变得快速而简单。
- **可操作的因情景而异的控制面板：**报告并不局限于事件枚举和聚合。面向终端的思科 AMP 报告包括实用的控制面板，以及从风险角度突出显示业务相关性和影响的趋势数据（参见图 1）。
- **更适合于协作的集成平台：**面向终端的思科 AMP 可与面向网络的思科 AMP 解决方案完全集成，以进一步提高对贵组织的监视和控制。

图 1. 可操作的因情景而异的控制面板



提高监视和控制以实现有效的安全性

各组织努力寻求能够有效应对高级恶意软件问题的完整生命周期的解决方案：提供面向最新威胁的防护、事件响应和补救措施，而不过度加重预算负担或牺牲运营效率。部分挑战源于检测和拦截技术与事件响应和补救技术之间缺乏连续性和智能。

通常，缺乏智能会使组织无法了解攻击的完整范围和深度，导致在出现攻击后无法有条不紊地开展事件响应和补救工作。此外，缺乏连续性导致在这些工作期间系统受感染且无法确定根本原因，造成无休止的重复感染循环。

因此，安全专业人员往往无法了解高级恶意软件在其网络中的影响范围，而是在攻击爆发后费力地对其加以遏制和补救，并且无法解决根本问题，包括：

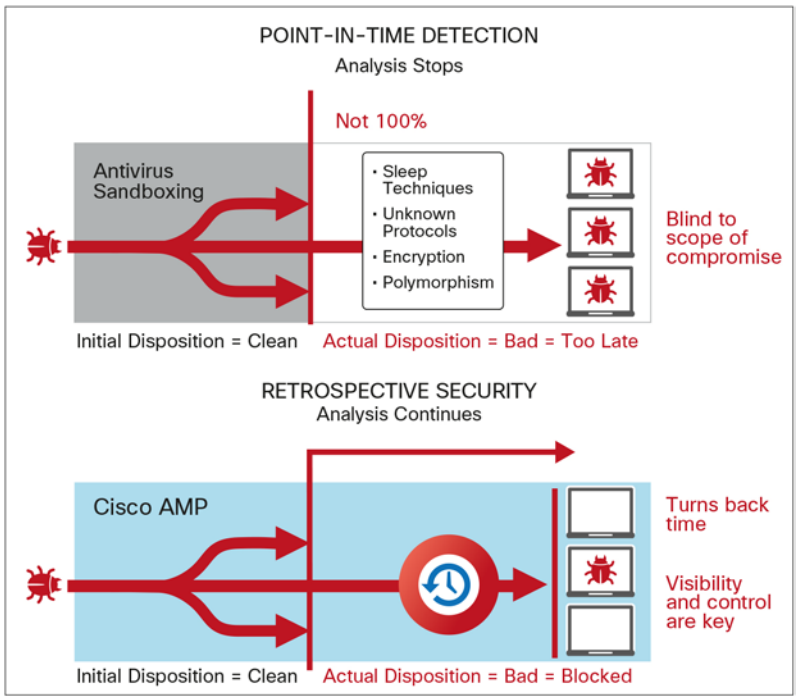
- 进入的方法和进入点是什么？
- 哪些系统受到了影响？
- 威胁进行了哪些活动？
- 我们如何能够阻止威胁并消除根本原因？
- 我们如何从攻击中恢复？
- 如何防止此类事件再次发生？

面向终端的思科 AMP 发现、分析、拦截和修复高级恶意软件

仅靠时间点检测并不能保证 100% 有效，只要有一个威胁逃避检测便会危害您的环境。老练的攻击者拥有丰富的资源和专业知识且顽固持久，他们会借助针对性的情景感知恶意软件，随时攻破时间点防御并危害任何组织。此外，时间点检测完全无法检测到已发生的漏洞的范围和深度，致使各组织无法阻止攻击扩散或防止再次发生类似攻击。

面向终端的思科 AMP 可超越时间点检测，提供检测功能与大数据分析，从而持续分析终端上的文件和流量，确定是否存在高级恶意软件（图 2）。先进的机器学习方法可以评估 400 多个与各文件关联的特性，进而分析并阻止高级恶意软件。该组合可提供超越传统时间点检测的防护。追溯性安全（能够回滚攻击时间）可以检测在初始进入点后变为恶意的文件，并向您发出警报。

图 2. 相比于持续分析和追溯性安全的时间点检测



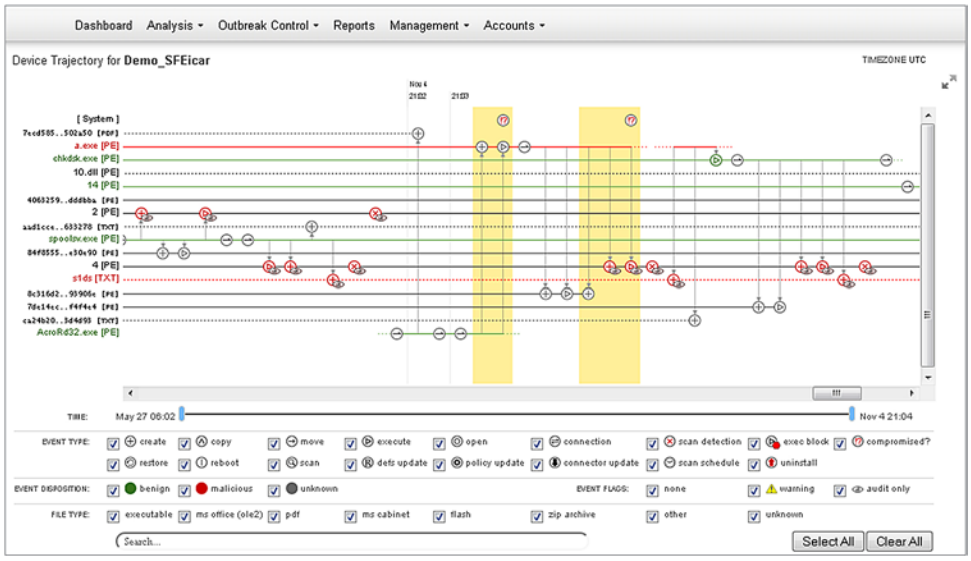
监视力度空前大并控制高级恶意软件

当今的恶意软件无比尖端，其演变迅速，可在危害系统后逃避发现，同时为长期攻击者在组织内四处移动提供启动平台。休眠技术、多态性、加密及使用未知协议只是恶意软件隐藏不被发现的部分方法。利用面向终端的思科 AMP 的持续分析和追溯性安全功能，可以发现难以捉摸的恶意软件，并在打击高级威胁的过程中帮助回答以下关键问题。

- **进入的方法和进入点是什么？ 哪些系统受到了影响？**

  文件轨迹和设备轨迹（图 3）之类的强大创新使用 AMP 的大数据分析和持续分析功能向您展示受恶意软件影响的系统，包括与潜在危害关联的病原体和根本原因。这些功能通过识别恶意软件网关和攻击者用于在其他系统中获取立足点的途径，帮助您快速了解问题的范围。

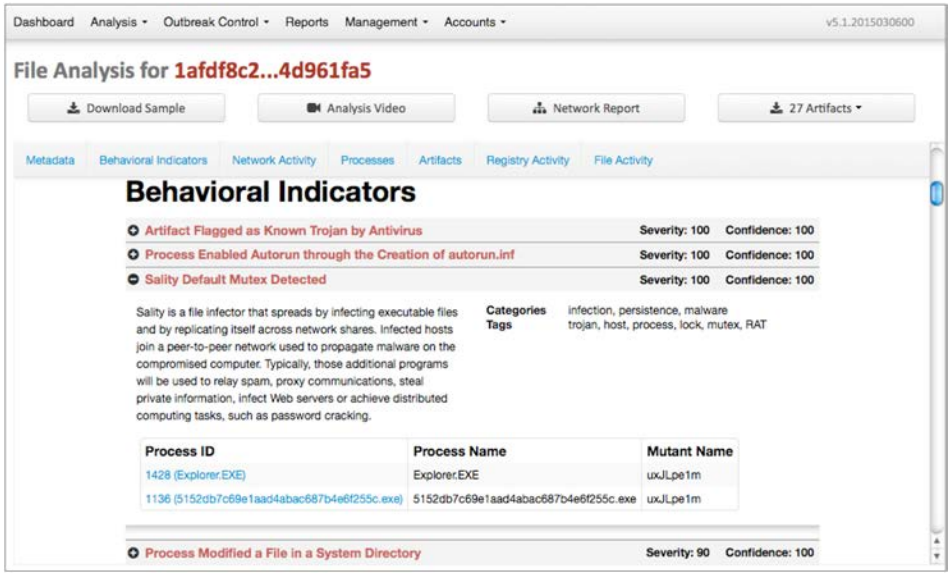
图 3. 借助设备轨迹的深入分析



- **威胁进行了哪些活动？**

  面向终端的思科 AMP 文件分析（图 4）由 Talos 安全情报与研究小组支持并藉由 AMP Threat Grid 的沙盒技术，提供安全、高度可靠的沙盒环境，供您分析恶意软件和可疑文件的行为。文件分析产生有关文件行为的详细信息，包括行为严重性、原始文件名、恶意软件执行屏幕截图，以及样本数据包捕获。借助这些信息，您将更全面地了解遏制感染和阻止未来攻击需要采取的措施。

图 4. 文件分析



设备轨迹通过按时间顺序跟踪终端上的文件和网络活动进一步协助快速分析计算机上的威胁活动。您可完全监视造成危害或在危害后发生的事件，包括父进程、与远程主机的连接，以及恶意软件可能已下载的未知文件。

危害表现 (IoC) 通常难以察觉，并且需要在其被清除或攻击者发起行动之前立即调查。通过面向终端的思科 AMP 弹性搜索，安全团队可以使用简单而又灵活的搜索功能迅速确定攻击的覆盖范围，这些功能立即呈现结果而无需从终端扫描并提取数据。

- **我们是否可以阻止威胁并找到根本原因？我们可以防止其再次发生？**

  面向终端的思科 AMP 感染控制功能为您提供一整套功能，来有效阻止恶意软件和恶意软件相关活动（例如回叫通信或已丢弃文件执行）的扩散，而不必等待安全供应商提供更新。借此只需点击几下鼠标即可从调查直接转向控制，从而显著缩短威胁扩散或造成更大破坏所用的时间，及其采取适当控制通常所需的时间。

  此外，AMP 还可以自动修复系统而无需全面扫描。该技术会根据最新威胁情报不断交叉引用已分析过的文件，并隔离任何之前被视为安全或未知、但现在被确定为威胁的文件。

保护终端、移动设备、虚拟系统和网络

面向终端的思科 AMP 保护您抵御高级恶意软件，并扩充所有终端（PC、Mac、移动设备和虚拟系统）上的安全情报。其轻型连接器架构使用大数据分析，从而简化深度防御要求以应对高级恶意软件，您将不再需要传统的防病毒安全层（这些层可能会显著增加终端上的性能和资源限制）。

此外，面向终端的思科 AMP 与面向网络的思科 AMP 集成，通过单一虚拟管理平台在扩展网络和终端之间提供全面的防护。现在，借助持续分析、追溯性安全和多源危害表现，您可以识别设法从终端穿越以在网络级别内联的隐秘攻击，将这些事件关联以实现更快的响应，以及实现更好的监视与控制。

纵向扩展企业保护

AMP 面向企业进行了优化。就隐私方面而言，所有面向终端的思科 AMP 连接器都使用元数据进行分析。实际文件并不需要，且未将其发送到云进行分析。对于具有高隐私要求的组织而言，还提供私有云选项。此单一的现场解决方案使用大数据分析、持续分析和现场本地存储的安全情报提供全面的高级恶意软件防护。

就可管理性而言，面向终端的思科 AMP 为 Windows 系统、Mac 系统、移动设备和虚拟系统提供全面的管理、部署、策略配置和报告。

就性能而言，部署在 PC、Mac、移动设备和虚拟环境上的面向终端的思科 AMP 使用轻型连接器架构，需要的存储、计算和内存比安全解决方案更少，从而更快地防御攻击。

实现真正全面的安全情报

面向终端的思科 AMP 基于大数据和无与伦比的安全情报。思科安全情报运营、Talos 安全情报与研究小组和 AMP Threat Grid 威胁情报源代表行业最大的实时威胁情报集合，其监视范围最广、覆盖面积最大，并且能够跨多个安全平台付诸行动。然后，此数据从云推送至 AMP 客户端，以便您时刻拥有最新的威胁情报。

通过将 AMP Threat Grid 技术集成到面向终端的 AMP 中，可以提供 350 多个用于评估文件提交操作（不仅仅是其结构）的特有行为指标，从而提供对未知恶意软件的洞察，包括关联的 HTTP 和 DNS 流量、TCP/IP 数据流、受其影响的进程，以及注册表活动。AMP Threat Grid 还每日为用户提供情景丰富、可操作的内容（每月分析 800 多万份样本，产生数十亿个工件）。最后，AMP Threat Grid 的高度准确的内容源（以标准格式提供以与现有安全技术无缝集成）可使各组织生成因其组织而异的情景丰富的情报。

思科 AMP 引领第三方测试

根据《2014 年 NSS Labs 漏洞检测系统比较分析报告》，思科在 NSS Labs 的漏洞检测系统安全价值图中居于领导者地位。在此比较性产品测试中，AMP：

- 整体检测率领先
- 提供最佳检测时间
- 产生最低的受保护单位传输速度的总拥有成本
- 在安全价值图中排名前列

NSS Labs 的结果表明，面向终端的思科 AMP 提供最高级别的安全效力和性价比。

表 1 突出显示面向终端的思科 AMP 的最佳功能。表 2 列出软件要求。

表 1. 面向终端的思科 AMP 的功能和优势

功能	优势
持续分析	面向终端的思科 AMP 使用基于云的大数据分析超越时间点检测的范畴，不断重新评估长期收集的数据以检测隐秘攻击。
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。当出现任何 IoC 时（例如事件触发器、文件性质的变化或 IoC 触发器），就需要追溯性安全。
控制面板	通过单一虚拟管理平台监视您的环境 — 监视主机、设备、应用、用户、文件和地理定位信息，以及高级持续性威胁 (APT)、威胁根本原因和其他漏洞，从而提供全面的情景视图，以便您做出明智的安全决策。
综合安全情报	思科安全情报运营、Talos 安全情报与研究小组和 AMP Threat Grid 威胁情报源代表行业最大的实时威胁情报集合，其监视范围最广、覆盖面积最大，并且能够跨多个安全平台付诸行动。
威胁表现	IoC 是作为潜在活动漏洞进行关联和优先化的文件与遥测事件。面向终端的思科 AMP 自动关联多源安全事件数据（例如入侵与恶意软件事件），以帮助安全团队将事件连接到更大规模的协同攻击，此外还优先处理高风险事件。
文件信誉	收集高级分析和综合情报旨在确定文件是安全的还是恶意的，从而进行更为准确的检测。
文件分析与沙盒	高度安全的环境有助于执行、分析和测试恶意软件行为，以便发现以前未知的零日差威胁。通过将 AMP Threat Grid 的沙盒技术集成到面向终端的 AMP 中，可以根据更大一组行为指标检查更动态的分析。
追溯检测	当文件性质在扩展分析之后发生变化时，系统将发出警报，使您感知并发现避开初始防御的恶意软件。
文件轨迹	在您的整个环境中长期持续跟踪文件传播，以便实现持续监视并缩短确定恶意软件漏洞范围的时间。
设备轨迹	在设备上和系统级别持续跟踪活动与通信，以快速了解导致危害和危害后的事件的根本原因及历史记录。
弹性搜索	一种跨文件、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于 IoC 或恶意应用的情景和范围。
低普遍性可执行文件	显示贵组织内已执行的所有文件（按普遍性从最低到最高排序），以帮助您发现以前未检测到但被少数用户看到的威胁。您可能不希望自己的扩展网络上存在只有少数用户执行但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。
终端 IoC	用户可以提交其自己的 IoC 以捕捉针对性攻击。借助这些终端 IoC，安全团队可以在其环境中针对因应用而异的鲜为人知的高级威胁执行更深入级别的调查。
漏洞	此功能显示一个包含易受攻击软件的主机的列表、一个每台主机上易受攻击软件的列表以及最可能受危害的主机。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，向您显示潜在漏洞，并为您提供按优先顺序排列的需要修复的主机列表。
感染控制	实现对可疑文件或攻击的控制，并且快速精准地控制和补救感染，而不等待内容更新。在攻击控制功能中，简单的自定义检测可以跨所有或选定的系统阻止特定文件；高级自定义签名可以阻止多态恶意软件系列；应用阻止列表可以实施应用策略或包含用作恶意软件网关的受损应用并终止再感染循环；自定义白名单有助于确保安全、自定义或任务关键型应用无论任何情况都继续运行；设备流关联将在源头阻止恶意软件回拨通信，尤其对于公司网络外的远程终端更加如此。
与 AMP Threat Grid 的集成	通过将 AMP Threat Grid 的沙盒技术和高级恶意软件分析功能集成到面向终端的 AMP 中，可提供 350 多个用于分析文件操作的特有行为指标、易于理解的威胁评分，以及来自全球威胁的规模与覆盖范围无与伦比的数十亿个待处理恶意软件工件。
AMP 私有云虚拟设备	面向终端的 AMP 可以部署为现场气隙解决方案，专门用于具有限制使用公共云的高隐私要求的组织。
从 AnyConnect v4.1 启动	在安装了 Cisco AnyConnect v4.1 远程访问 VPN 客户端的情况下，用户可以选择在该远程终端上启动面向终端的 AMP 连接器。借此可以将终端威胁防护快速扩展至支持 VPN 的终端，并进一步尽量控制可能来自远程主机的攻击。在攻击中或攻击后更深入洞察远程终端，并加快补救工作。

表 2. 软件要求

面向终端的思科 AMP	• Microsoft Windows XP Service Pack 3 或更高版本 • Microsoft Windows Vista Service Pack 2 或更高版本 • Microsoft Windows 7 • Microsoft Windows 8 和 8.1 • Microsoft Windows Server 2003 • Microsoft Windows Server 2008 • Microsoft Windows Server 2012 • Microsoft Windows Embedded POSReady 2009 • Microsoft Windows Embedded POSReady 7 • Mac OS X 10.7 及更高版本
Android 移动设备上的面向终端的思科 AMP	• Android 版本 2.1 及更高版本

平台支持和兼容性

面向终端的思科 AMP 包括面向终端的思科 AMP 许可证和订用（选项为 1 年、3 年和 5 年）和轻型连接器。面向终端的思科 AMP 与面向网络的思科 AMP 兼容。面向终端的思科 AMP 还可在远程终端上从 Cisco AnyConnect v4.1 启动。

保修信息

有关保修信息，请访问 Cisco.com 产品保修页面。

订购信息

要下订单，请访问思科订购主页，与您的思科销售代表联系或致电 800 553-6387。

更多详情

有关详细信息，请访问以下链接：

- 面向终端的思科 AMP

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 C78-733181-02 05/15