摆脱被动防御：
思科下一代终端安全

概述

战胜当今安全威胁的唯一方法就是，在整个攻击过程中（攻击前、攻击中和攻击后）进行全面防护。思科的持续终端分析方法与集成架构方法相结合，为这一模式奠定了基础。我们在高级恶意软件防护方面的创新包括：

- 对所有文件进行持续分析和记录
- 追溯功能
- 基于行为的感染指标
- 设备和文件轨迹
- 爆发控制
- 低事件率
- 漏洞防御
- 内置沙盒和防病毒检测功能

通过跨多种安全工具将这些功能整合为一个集成的工作流程，可以在恶意软件检测、监控、分析、调查、遏制和补救方面带来明显的实际影响。

变革中的网络安全性

在十多年前，网络可视性的标准是使用防网络入侵或“时间点”扫描工具。这些工具需要花费大量时间来完成整个扫描，而且对扫描的网络和系统具有破坏性。更麻烦的是，由于网络具有动态性，这些数据很快就会过时，因此必须反复运行整个过程。而且，这些数据充满盲点，难以关联实时威胁数据。

思科（Sourcefire 的收购者）已经认识到这些困难，早在 2003 年，思科便开始率先提出持续网络发现的概念。思科意识到，许多防御者面临的基本安全问题不是保护他们的环境，而是充分了解他们所保护的对象及其排列方式，只有这样，他们才能随着保护对象的演变而进行持续保护。借助持续实时网络感知，可视性能够史无前例地与威胁检测紧密集成，从此改变了网络威胁防御方式。持续网络发现的概念造就了我们的 Firepower™ 下一代入侵防御系统 (NGIPS)，该系统最终成为各种下一代入侵防御系统 (NGIPS) 的基础。而且，按照 Gartner 的定义，实时网络感知已经成为 NGIPS 的一个关键要求。而现在，我们的思科 Firepower™ 管理中心技术就是基于实时网络感知。

保护终端的全新模式

当前的威胁形势再次迫使我们转变思维并提供有效的安全解决方案，为各种终端（PC、Mac、Linux、移动设备等）提供保护。当今的恶意软件不是已经侵入终端，就是正在向终端渗透。高级恶意软件具有动态性，可以利用各种攻击媒介危害环境。它们形式多变，随着时间推移不断发动攻击，并且可以快速从终端盗取数据。此类恶意软件（包括多态恶意软件和环境感知型恶意软件）很擅长伪装自己并规避传统安全工具，从而导致漏洞发生。因此，问题已不再是恶意软件会不会穿透防御并到达终端，而是它们何时会穿透防御并到达终端。

遗憾的是，终端威胁检测方面的许多最新改进还不足以解决这些问题。其中一些改进包括：在沙盒中执行文件以进行检测和分析，使用虚拟仿真层阻止来自用户和操作系统的恶意软件，以及使用基于信誉的应用白名单区分可接受的应用与恶意应用。近来，攻击链模拟和分析检测开始发挥作用。这些积极的开发活动确实起到一定作用，许多公司（包括思科）都已开始实施。但它们在本质上仍然是“静态”的。攻击者了解这些安全技术的静态性质，他们可能会围绕这些技术的相关局限性进行创新，从而突破网络和终端防御。

1. 思科 2014 年度安全报告
2. 2014：数以百万漏洞涌现的一年 (2014: A Year of Mega Breaches)，Ponemon Institute。
3. 数据泄露的代价 (Cost of a Data Breach)，2013/2014 年，Ponemon Institute。

而且，市场与技术的走向并不完全相同。在终端安全领域，充斥着各种高级品牌宣传和消息，听起来全都是一样的。它们都声称自己将会引领恶意软件检测的下一轮革命。它们纷纷声称能比其他产品提供更好的实时和持续防护，但实际上只是对同一工具进行了微小改进，而根本的局限性仍未得到解决。

为了能够有效地远程应对当今威胁，终端安全防御解决方案需要经历巨变，必须采用多维方法，而且能够像恶意软件一样动态变化。我们必须转变想法，不再寄希望于通过某种卓越的预防或检测技术一劳永逸地解决问题。

真正的持续模式能够回答最重要的问题

- 入侵方法和入口点是什么?
- 哪些系统已经受到影响?
- 威胁已经进行了哪些活动?
- 能否阻止威胁并找到根本原因?
- 如何才能恢复正常?
- 如何防止此类事件再次发生?
- 我能否在威胁影响我的组织之前提前发现感染指标 (IoC)?

我们将依赖“防御”和“时间点检测”的传统终端保护方法改进为一种持续方法，从而构建了一个保护终端的新模式。

此模式将：

- 超越仅依靠初始检查来防御或捕捉恶意软件的做法，改为持续监控和检测威胁，并在威胁进入系统后做出响应
- 着眼于高级威胁，而不仅仅是常见危害
- 针对持续性感染和攻击提供前所未有的可视性
- 使安全团队能够快速精确地遏制感染并进行补救，同时不对终端用户和安全人员造成困扰
- 助力安全团队化被动为主动

我们需要彻底转变我们检测高级威胁和违规活动的方式。从恶意软件侵入到传播，再到感染后的补救，我们需要在整个过程中提供持续的防护和可视性。面向终端的思科® 高级恶意软件防护 (AMP) 解决方案将持续方法与大数据和集成安全架构相结合，解决了传统防御、时间点检测和响应技术的局限性。

在此模式中，系统会持续收集所有来源产生的进程级遥测数据，当需要使用数据时，数据始终是最新的。分析可以分层进行，以消除对控制点的影响，并在一段时间内提供高级检测。分析不仅涉及事件枚举和关联；它还意味着交织遥测数据，以便更深入地了解环境中的情况。Talos 安全情报和研究团队深入到更广泛的用户社区，收集思科综合安全情报和信息，并在全球范围内进行持续更新和即时共享。这些全球情报与本地数据关联之后，能够帮助制定更明智的决策。

在此模式中，检测和响应不再是独立的领域或流程，而是同一目标的延伸：在高级威胁阻止您之前阻止它们。检测和响应功能是持续且集成的，超越了传统的“防御”或“时间点检测”方法。

持续分析的优势

- 自动执行高级分析
- 更好地确定威胁优先级
- 缩短补救时间

检测

没有哪个防御或检测方法是 100% 有效的，因为攻击者会通过持续创新来避开这些前线防御。尽管时间点检测具有一定的局限性，但是它在消除绝大部分潜在威胁方面仍然具有重要作用。此外，通过在传统检测中应用持续方法，防御者可以改进时间点技术，使其更加有效、高效且广泛。

但这仅仅是思科的持续方法转变高级恶意软件防护的一个开端。更重要的是，它有助于我们提供一系列其他创新，从而加强从检测到响应的整个高级恶意软件防护流程。

持续的可视性

战胜高级威胁的唯一方法就是，在整个攻击过程中（攻击前、中、后）进行全面防护。我们的持续方法为这种模式奠定了基础，并且促进了高级恶意软件防护领域的一系列其他创新，包括：

- 追溯：这项功能在初始时间点以及更长一段时间内执行分析,且不仅限于文件。它还能处理进程、通信和其他遥测数据，这是传统时间点模式无法做到的。
- 攻击链组合：这项创新方法可随时间推移在文件、进程和通信流之间建立清晰的脉络，利用基于行为的感染指标 (IoC) 掌握各个对象的关系，避免仅依靠静态标样做出判断。这些信息为攻击链组合实时捕获提供了综合全面的行为线索，而基于行为的感染指标会实时检测捕获的数据
- 轨迹：所谓“轨迹”，并不是在营销上对“跟踪”所做的文字游戏。“跟踪”会生成时间点事件的枚举列表，用于显示某个事件的发生位置。“轨迹”是指某个对象（在这种情况下指恶意软件）随着时间移动的连续路径。实质上，相对于恶意软件的位置和行为，它能够更有效地显示恶意软件的范围和根本原因。

需要注意的是，这些创新中每种创新都能独立对抗恶意软件及其所代表的高级威胁，但是只有当它们组成一个集成工作流程时，才能显现恶意软件检测、监控、分析、调查和遏制方面的实际影响。

图 1 显示了恶意软件的传播过程，其中包括进入点、恶意软件活动和受影响的终端等信息。图 2 显示了设备轨迹屏幕，其中包括进入点、恶意软件活动和影响特定终端的二进制文件和可执行文件等信息。这些信息在整个扩展网络中的终端之间关联和共享，并与图 1 中的网络视图集成。

图 1. 面向终端的思科 AMP 文件轨迹屏幕

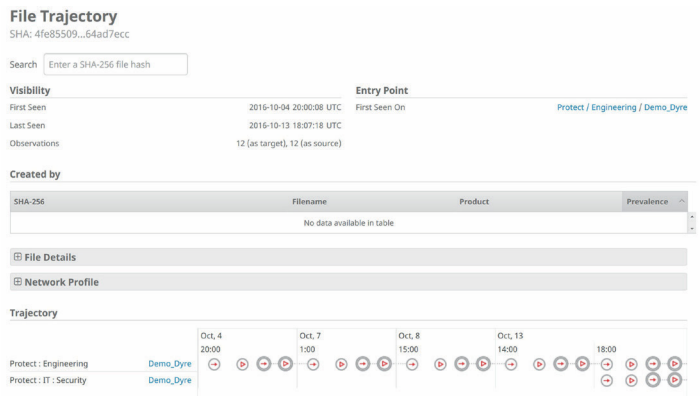
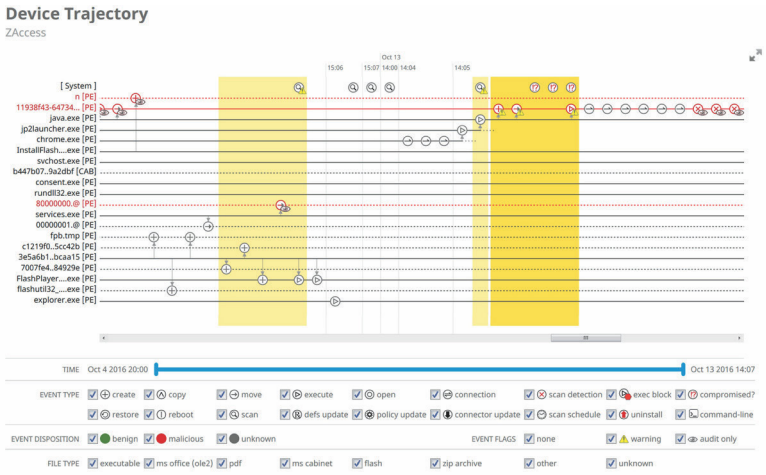


图 2. 面向终端的思科 AMP 设备轨迹屏幕



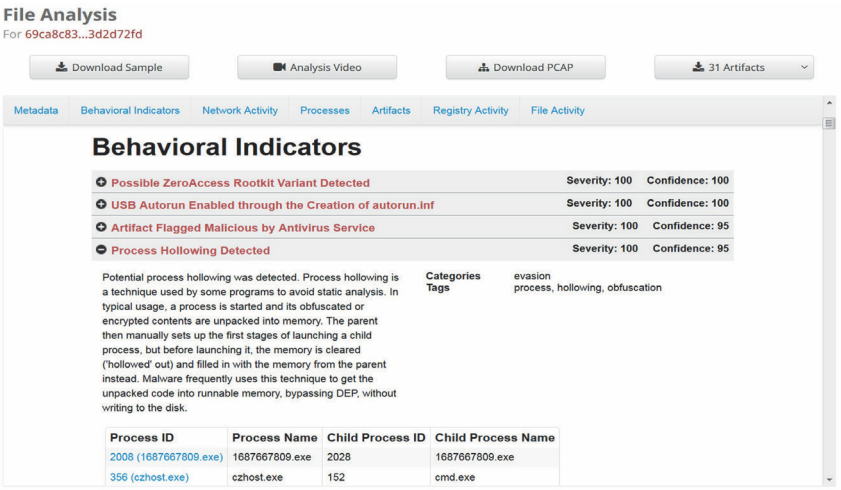
自动执行高级分析

为了在高级攻击横向通过网络和穿过终端时检测到高级攻击，防御者需要利用相关技术，自动查找恶意软件和漏洞利用所产生的 IoC，同时查找随着时间推移出现的更高级的危害行为。思科的持续方法可以借助高级行为检测功能来达到这种自动化程度，它的目的不是提供另一个警报列表来供调查，而是围绕危害和违规活动的主要领域，提供一个经过排列整理的视图。借助大数据分析并使用持续功能，模式和 IoC 一旦出现，系统就能识别出来，因此安全团队可以专注于损害可能性最大的威胁。

通过把 Threat Grid 沙盒技术集成到面向终端的 AMP 中，可以提供 700 多个用于评估文件提交操作（不仅仅是其结构）的特有行为迹象，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。Threat Grid 还每日为用户提供情景丰富的有价值内容（每月分析 800 多万份样本，产生数十亿个标样）。最后，利用 Threat Grid 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），各组织可生成特定于自己组织、情景丰富的情报。

图 3 显示了内置沙盒提供的关于文件行为的详细信息，包括行为的严重性、原始文件名、恶意软件执行过程的屏幕截图和样本数据包捕获。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 3. 面向终端的思科 AMP 文件分析屏幕



威胁搜索与调查

在缺乏情景证据的情况下，安全团队尝试跟踪某个违规行为将是非常痛苦的体验，若没有持续方法的情景和功能，术语“调查”很可能使他们不寒而栗。通常，最难回答的问题是“我们该从哪里入手”。在持续方法中，调查会更快速、更有针对性，也会更加高效。

持续方法从搜索难以捉摸的事实和线索，转变为依据实际事件（比如恶意软件检测及静态和基于行为的感染指标等）针对性地搜索违规行为。您可以随时很容易地搜索所有数据，更加快速有效地捕获恶意软件。您可以直观地了解感染的进入点、范围和根本原因。它还包括识别搜索时间窗口，扩展或收缩时间窗口，以及使用过滤器查明和定位搜索的功能。此功能成为了一项重要工具，并且能够提高效率，因为安全团队已从盲目地响应警报和事件，转为在攻击扩大之前迅速捕获恶意软件。

感染控制与遏制

如果遏制恶意软件意味着必须将一切过程重现在眼前，那就很难实现遏制。由于时间点技术不关注事件链和相关的情景信息，因此想精确地遏制恶意软件是不可能的。

借助持续方法提供的可视性，再加上确定特定根本原因的能力，即可快速且轻松地阻止攻击的爆发。由于持续模式保留所有检测和遥测数据，因此您可以在整个攻击路径的多个不同点遏制威胁，而且可以关闭相应感染网关以抵御后续攻击。

从部署的那一刻起，AMP 持续方法就会立即开始收集重要检测和遥测信息，这些信息将帮助响应者了解攻击的危害程度，以及恶意软件来自的位置、经过的地方和造成的破坏。您可以在所有或选定系统中快速阻止特定文件，使用高级自定义签名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调通信，尤其针对公司网络之外的远程终端。

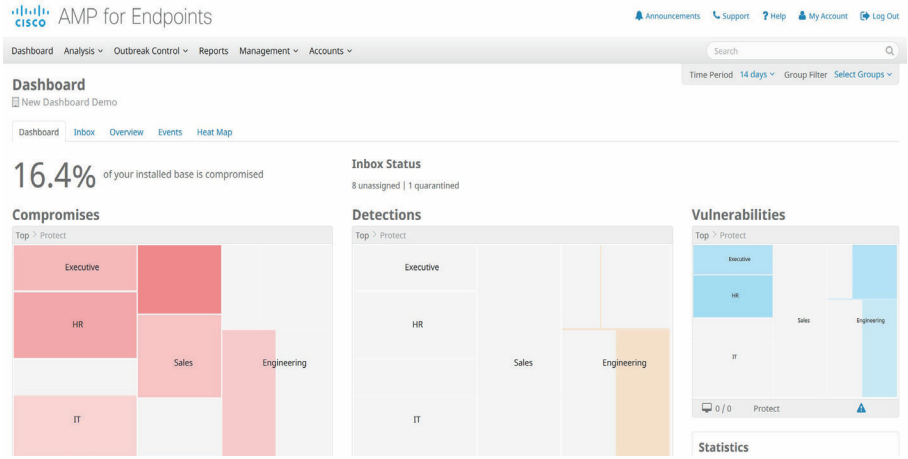
报告

持续方法还扩展了报告功能。报告并不限于事件枚举和汇聚。它们可能包括切实可行的控制面板和趋势，突出显示业务相关性和潜在的风险。尽管时间点技术也可以提供控制面板和风险相关性，但它们通常需要一层额外的安全情报和事件管理 (SIEM) 集成，才能筛选和关联数量庞大的事件数据。

大数据架构可以处理不断增长的海量数据，这些数据对于有效地执行恶意软件检测和分析至关重要；持续方法使用这些数据，随时随地按照您的需求提供情景信息和优先顺序。

图 4 显示了面向终端的思科 AMP 切实可行的控制面板和趋势视图，从风险的角度突出显示了业务相关性和影响。报告并不限于事件枚举和汇聚。在此视图中，我们可以看到按优先顺序排列的感染指标，主机负责检测其他数据中的恶意软件和网络威胁。

图 4. 面向终端的思科 AMP 的控制面板



集成的安全架构

同样需要注意，面向终端的 AMP 并非孤立的单点产品。它具有 API，可允许客户将面向终端的 AMP 与其他安全工具或 SIEM 同步。但是，最重要的是，面向终端的 AMP 是更大的“AMP 无处不在”集成安全生态系统的一部分。面向终端的 AMP 可以共享来自终端的信息，将其与网络 IPS、防火墙、Web 或邮件网关等关联。因此，当您在某个位置看到威胁时，整个安全生态系统可以系统地做出响应。这意味着您的响应将会更加快速、更加全面。这种集成架构使安全团队的力量倍增。

结论

在抵御面向终端的高级威胁时，持续方法和大数据架构可在关键领域实现变革性的创新：

超越时间点的检测：持续方法可以使检测变得更有效、更高效且更全面。诸如沙盒等行为检测方法经过优化，活动一旦出现便会被捕获，而且所获得的情报会在检测引擎和控制点之间共享。

为攻击链组合提供支持的监控：追溯功能可以持续监控文件、进程和通信，然后将这些信息组合在一起建立活动轨迹，实时提供前所未有的攻击洞察力。

持续观察各种行为的自动化高级分析：将大数据分析和持续功能相结合，实时确定攻击模式和感染指标，有助于安全团队集中精力应对最重要的威胁。

化被动为主动的调查：通过从被动调查转变为依据实际事件和感染指标有针对性地搜索威胁，安全团队将能够快速有效地了解攻击并确定攻击范围。

非常简单的遏制：持续方法提供的可视性级别与确定具体根本原因的功能相结合，能够快速有效地截断攻击链。

切实可行且情景丰富的控制面板：跨各个控制点广泛收集文件和遥测数据并进行高级分析，然后结合情景信息得出报告，可在报告中突出显示趋势、业务相关性和风险的影响。

为了有效地防御当今的各种高级威胁，您所需的解决方案应该涵盖多种攻击媒介，共享信息，降低复杂程度，提高管理层使用便捷性，并且最根本的是能为您的组织提供您所需的深刻可视性与可控性，不仅可以预防漏洞，而且在恶意软件入侵的情况下，能够快速检测、控制恶意软件并进行补救。思科高级恶意软件防护能够提供这一切，让您可以在攻击前、攻击中和攻击后保护您的组织。

附录：持续方法与仅防御模式的比较

以下是对持续方法与仅防御模式功能差异的详细比较。

表 1. 检测

持续方法	仅防御模式
• 系列集成引擎可以协同工作，通过共享情景信息来提高检测功能。 • 通过减少工作负载和延迟，消除为每个新文件建立沙盒的必要性，沙盒等行为检测方法得以优化。 • 检测会在一段时间内持续进行，因为攻击正是随着时间推移逐渐显露的。 • 审核模式从一个用来减少误报的简单调整参数，转变成了一个用来捕获实时活动同时不会让攻击者察觉的事件响应收集工具。 • 检测情报跨多个控制点即时集体共享。	• 如果有多个引擎，这些引擎将会作为一个堆栈，依次独立运行，这会降低终端处的效能和性能。 • 供应商需要进行更新，而这不仅耗费时间，而且会产生另外的安全漏洞。

表 2. 监控

持续方法	仅防御模式
• 文件追溯：在完成初始检测分析后，使用最新检测功能和综合威胁情报，继续在一段时间内质询文件。这样，在第一次查看文件的时间点过去很长时间后，仍可提出更新后的处置方法，并可执行进一步分析。 • 进程追溯：类似于文件追溯，进程追溯是指在一段时间内持续捕获和分析系统进程 I/O，以进行攻击链分析和行为感染指标 (IOC) 检测。 • 通信追溯：持续捕获与终端之间的通信，以及发起或接收通信的相关应用和进程。此信息可提供额外的情景数据，可作为攻击链分析和行为 IoC 检测的一部分。 • 攻击链交织：面向终端的思科 AMP 不止具有追溯功能；它将各种形式的追溯交织成一系列活动。这些活动可在任何时候实时用于分析，因而提高了智能化水平。具体而言，通过分析查找各个终端或终端社区中的相关行为模式，可以将不同形式的追溯交织在一起。	• 没有追溯：除了检测活动，该模式不关注终端处的关系活动。 • 该模式也完全不关注恶意软件通过控制点后网络中发生的事件。

表 3. 自动执行高级分析

持续方法	仅防御模式
• 实时响应：由于终端遥测数据会不断收集并添加到数据存储区，因此这些数据可自动与静态和行为 IoC 进行比较。进而可以显著减少静态或行为 IOC 的检测时间。 • 行为感染指标 (IOC)：借助攻击链交织功能，行为 IOC 会跨检测事件、静态 IOC 和遥测数据，查找那些表征潜在危害的复杂活动模式。一个典型例子是在初始检测中蒙混过关的植入程序。 • 攻击链交织：攻击链交织功能还会记录触发行为 IOC 前后发生的事件。安全团队可以围绕警报快速展开调查，而警报对于全面了解感染范围和精确遏制问题非常有用。 • 开放 IOC：借助开放 IOC，客户可以使用自己自定义的静态 IOC 检测列表。 • 基于情报的 IOC：除了静态情报、黑名单或检测脚本，这些 IOC 还基于行为算法，即随着时间推移查找特定的恶意操作和相关操作。基于情报的 IOC 由思科 Talos 安全情报与研究小组开发并提供全面支持。 • 事件率：高级分析引擎可确定检测到的恶意软件相对于组织和更广泛的全球社区的事件率。通常，低事件率的恶意文件表示有针对性的恶意软件和有针对性的危害尝试。安全团队常常会错过这些文件。事件率分析会突出显示此类攻击，尤其是与涉及这些系统的其他静态或行为 IOC 相关时更是如此。	• 有些时间点技术可以查找静态 IOC 结果，但是无法实时完成这项任务，而且在 IOC 可以运行之前，通常需要花费大量时间收集数据。 • 此模式可能会显示发现恶意软件的次数和位置，但是缺少根本原因的相关信息。 • 没有显示威胁的重要性或事件率。 • 如果确实存在事件率功能，它们也无法实时实施，而且也无法继续跟踪特定文件、进程或通信。 • 无法识别行为 IOC。

表 4. 威胁搜索与调查

持续方法	仅防御模式

• 文件轨迹：通过查看时间、方法和进入点、受影响的系统以及事件率，可以快速了解恶意或可疑文件的暴露范围，而这一切都无需进行终端扫描或快照拍摄。
• 设备轨迹：在文件轨迹提供的范围级别的基础之上，设备轨迹针对系统进程提供了强大的时间窗口分析，用于了解根本原因的历史记录和沿袭情况。它还可以扩展或收缩时间窗口和过滤器，以便快速找到危害的确切原因。
• 弹性搜索：弹性搜索提供了一种快速、简单的方法，只需要询问“此指标还在哪里出现过？”，不需要考虑关系数据库查询的典型边界。可以跨整个数据集和全球综合情报搜索从主机名、文件名、URL 和 IP 地址到文本字符串的一切内容。由于它会定期分析数百万个文件，因此它已成为在事态严重之前快速捕获高级威胁的一款强大工具。
• 文件分析：第一，该模式提供了一种在沙盒中运行文件的安全机制，用于全面分析行为并评价该行为的威胁级别。第二，它会在详细的报告中提供该分析的输出。第三，所有分析结果都将添加到综合情报。第四，通过弹性搜索功能可以搜索所有分析结果。同样，安全团队可以围绕文件分析报告中的指标，快速展开调查，以查看整个企业中发现该指标的其他位置。当攻击具有针对性，但采用了一般感染方法时，这一点便至关重要。
	• 这是传统时间点检测技术的不足之处。它们无法提供任何检测后监控或情景信息。
	  ◦ 检测结果通常是捕获到的独立事件，这些事件将添加到事件枚举列表。该列表会持续更新，但是没有任何情景追溯。
	  ◦ 无法查看检测前后的事件。
	  ◦ 无法全面分析文件中的相关行为，然后跨所有终端快速搜索特定的 IOC。
	• 有些技术可能会提供有限的功能（例如，根据事件枚举数据确定检测到恶意软件的时间和位置），但是它们无法显示危害前后相关事件的时间窗口。
	• 即使声称自己具有持续性，传统的时间点取证和调查工具也没有比其检测对手出色多少。
	  ◦ 它们没有任何高级威胁检测方法。检测功能如果与持续情景信息相结合，可以作为一个重要起点，但是取证工具是用来查找结果和线索的，不是用来查找关系的。
	  ◦ 它们无法显示危害前后的相关事件的时间窗口。
	  ◦ 它们无法在不更新所有数据的情况下快速搜索特定的 IOC。

表 5. 感染控制与遏制

持续方法	仅防御模式
• 简单遏制措施：您是否怀疑某个文件是恶意的？没有问题，无需等待。使用该文件的 SHA256（安全散列算法），点击几次鼠标即可立即在所有终端、一组终端或某一个终端上阻止该文件。 • 高级遏制措施：类似于 Snort® 脚本，高级自定义检测提供处理各种恶意软件的功能，无需等待签名更新。 • 应用白名单和黑名单：借助大量情景信息，可以使用控制列表来更有效地确定安全应用是否被用作了恶意活动的网关，并且可以阻止可疑的恶意应用。这些列表扩展了持续分析和遥测数据。安全团队可以快速控制局势，同时遵循标准响应程序。 • IP 黑名单：类似于应用控制列表，IP 黑名单可以更加有效地用于实际事件或企业策略中，用于控制感染并监控终端，从而查找来自终端的可疑通信。当实施遏制计划时，需要终止攻击者使用的所有交叉通信，在这种违规情形中，此功能至关重要。	• 时间点技术遏制恶意软件或疑似恶意软件的能力存在严重的局限性，因为它们旨在关注检测点，而不关注攻击全程的后面部分，而在后面部分遏制措施是一项重要要求。 • 有些时间点检测技术支持应用黑名单。对于遏制会给组织带来风险的应用，或者尚未确定好坏，但是作为预防措施应当加以阻止的可疑应用，这是一种很有效的方法。但是，只有通过一组强大的文件和行为检测功能完成检测、分析和遏制等主要功能时，黑名单才是最有效的。主要弊端在于，将这些技术作为主要的防护层进行管理时会非常耗费人力，而且容易错过攻击并忽视攻击链活动。 • 最后，时间点取证和响应工具不具备快速控制感染的能力，而这种能力正是应对当前各类高级威胁所急需的。它们在调查过程中会很有用，但是它们无法将数据枚举转变为遏制措施。通常，这一步骤非常耗费人力，为了简化映像重建方法，一般会避免此步骤。

更多相关信息

如需详细了解面向终端的思科 AMP 和思科安全方法，请访问 www.cisco.com/go/ampendpoint，您也可以发送邮件至 ciscosecurityinfo@cisco.com 或拨打电话 800-553-6387 与我们联系。