适用于网络的思科高级恶意软件防护

产品概述

如今，有效对抗恶意软件需要新的方法、策略和技术。面向网络的思科® 高级恶意软件防护 (AMP) 提供基于网络的高级恶意软件防护，它超越了时间点检测方法，可在攻击的整个过程（攻击前、攻击中和攻击后）为您的组织提供保护。它专为 Cisco FirePOWER™ 网络安全设备而设计，可在单个系统内针对多种威胁媒介检测、拦截、跟踪和遏制恶意软件威胁。它还提供保护您的组织免受高度复杂且具有针对性的持续零日高级恶意软件威胁所需的可视性和可控性。

借助面向网络的 Cisco AMP，您可以：

- **获得超越时间点检测的可靠保护：**面向网络的思科 AMP 超越了时间点检测，可对文件和流量进行持续分析。此功能有助于实现追溯性安全，即能够回顾并跟踪进程、文件活动和通信。您可以了解感染的完整范围，确定根本原因并执行补救。这样一来，您的组织将获得更有效、更高效且更广泛的保护。
- **限制违反策略的文件和更多内容：**通过跟踪经网络、电子邮件或其他攻击媒介传递的数据，面向网络的思科 AMP 可自动识别文件和应用。然后，可使用您设置的应用与文件控制策略，对文件执行广泛过滤。
- **检测并阻止漏洞攻击尝试：**利用内联部署，思科解决方案可检测并阻止客户端漏洞攻击尝试。您还可以防范针对 Adobe Acrobat、Java、Flash 以及其他常被作为攻击目标的客户端应用的漏洞攻击尝试。
- **识别、阻止并分析恶意文件：**系统会阻止来自其目标系统的恶意软件，并在本地对处理结果未知的文件进行分析。可疑文件可选择性地提交给思科综合安全情报云进行分析。
- **持续分析文件与流量：**面向网络的思科 AMP 系统一旦确定观察到的文件为恶意文件，便会触发追溯性警报（即使该文件是在数小时或数天前侵入网络也是如此），因此您仍然可以采取措施并减轻损失。
- **将离散事件与协同攻击相关联：**面向网络的思科 AMP 可展示与正在进行的攻击相关的风险。它会自动按优先级列出可能受影响的设备，其中包括来自多个事件源的安全事件数据。
- **跟踪恶意软件的传播和通信：**利用面向网络的思科 AMP 的文件轨迹功能，可以跟踪某个文件在整个网络中传输的过程。文件轨迹视图中的每个文件都具有相关的轨迹图，其中包含文件在各个阶段的传输轨迹视觉展示和其他文件补充信息。
- **遏制恶意软件以防止损失和病毒爆发：**借助于面向网络的思科 AMP，可通过简单的策略更新轻松拦截高级威胁和恶意软件通信。借助自定义检测列表，您可以在需要时随时采取行动，而不是等待供应商提供更新后才能采取措施。

有效的安全保护依靠的不仅仅是检测

仅时间点检测并不能保证 100% 有效，只要有一个威胁逃过检测便会危害您的环境。老练的攻击者不仅具有资源和专业知识，而且不达目的不罢休。利用有针对性的情景感知型恶意软件，他们随时都有可能攻破时间点防御，危害任何组织。此外，时间点检测完全无法检测到漏洞的范围和深度，致使各组织无法阻止攻击扩散或防止再次发生类似病毒爆发。

面向网络的思科 AMP 是唯一一款基于网络的系统。它超越了时间点检测，可使用集成的控制与持续分析功能集来检测、确认、跟踪、分析威胁，并采取补救措施，从而在整个高级恶意软件攻击过程中（攻击前、攻击中和攻击后）提供保护。在攻击前，面向网络的思科 AMP 防止已知的恶意软件以及违反策略的文件类型和通信进入您的网络，从而减小攻击面。在攻击期间，它能够检测漏洞攻击尝试、恶意文件和恶意流量，并加以阻止。

在攻击后，AMP 系统会继续分析文件和网络流量，查找可能已逃过初始检测的隐藏威胁（因为我们认识到主动检测和拦截方法不可能 100% 有效）。如果出现新的危害表现 (IoC)，系统会自动在一个优先视图中关联来自多个来源的安全事件数据（例如追溯性恶意软件警报、入侵事件和恶意软件回叫尝试）。这样一来，在发生攻击时，这个智能的自动功能可帮助您快速高效地了解活动的攻击、界定其范围，并加以遏制（即使在攻击发生后也是如此）。这有助于缩短从发现到遏制这一重要过程，使您能够在恶意软件造成破坏之前阻止其传播。

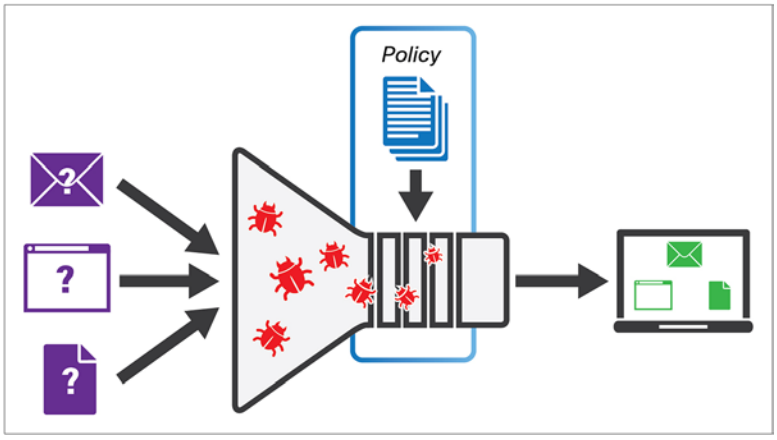
面向网络的思科 AMP 还可减少您日常处理的可操作事件数，并提供可行的见解，以便您可以将时间用于解决最重要的高风险高级恶意软件威胁。

此外，面向网络的思科 AMP 可与面向终端的思科 AMP 兼容。面向终端的思科 AMP 是思科的一款功能全面的高级恶意软件保护产品，适用于 PC、Mac、移动设备，以及作为基于软件的收集器部署在设备中的虚拟系统。无论终端是连接到受保护的网络还是在互联网上漫游，该产品都能对其进行保护。通过同时部署面向网络的思科 AMP 和面向终端的思科 AMP，您的组织将获得对整个扩展 IT 生态系统的完整可视性和可控性。

限制违反策略的文件和更多内容

通过面向网络的思科 AMP，可以定义允许通过系统的文件类型。无论文件从网络、电子邮件还是其他攻击媒介到达，系统都可自动识别文件和应用。然后，系统会使用您设置的应用和文件控制策略执行大范围文件过滤（请参阅图 1）。这些策略可应用于入站和出站文件，因此您可以对已下载和已上传的文件进行控制。这种机制可同时解决外部和内部威胁因素。

图 1. 限制违反策略的文件



该系统还包括全局安全情报源，用于将确定为恶意的连接动态列入黑名单。通过可选的 URL 过滤许可证，可以阻止从分类为恶意的网站和域进行的文件下载尝试。

检测并阻止漏洞攻击尝试

面向网络的思科 AMP 基于 Cisco FirePOWER 下一代入侵防御系统 (NGIPS)。此系统以内联方式部署时，会检测并阻止可能导致恶意文件下载（通常称为路过式攻击）的客户端漏洞攻击尝试。NGIPS 系统也可以防范针对 Web 浏览器、Adobe Acrobat、Java、Flash 和其他常被作为攻击目标的客户端应用的漏洞攻击尝试。通过在攻击链中尽早做出行动，此系统旨在抑制附带损害，并避免成本高昂的清理工作。

检测、阻止和分析恶意文件

面向网络的思科 AMP 使用思科的综合安全情报云实现针对多种攻击媒介（如网络和电子邮件）的实时文件处理。已知恶意文件会被阻止，而无法到达目标系统。具有未知性质的文件可选择性地提交给思科综合安全情报云进行分析。在云中分析的文件会得出一个威胁评分，而且管理控制台中会提供详细的威胁报告，用于帮助做出决策。任何类型的文件都可以选择性地保存到系统并安全地进行检索，以便手动启用进一步分析。

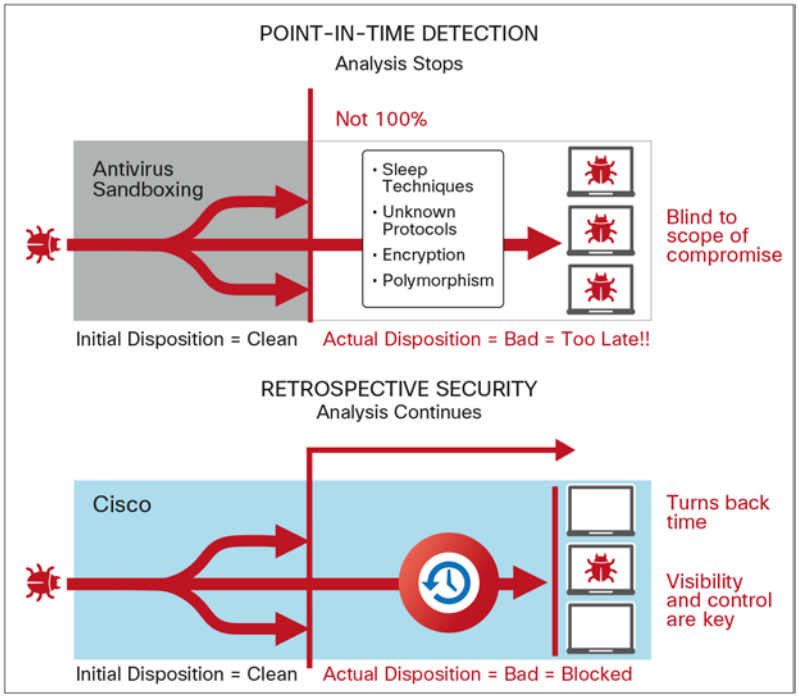
持续分析文件和流量

典型的基于网络的防恶意软件系统仅在恶意软件穿越网络设备的时间点对其进行检查。由于没有任何检测技术 100% 有效，而且高级恶意软件可通过自我伪装逃避外围防线，因此在经过初始检查后，您通常无法掌握随后的情况。

思科采用大数据分析进行持续分析，作为时间点检测的补充，从而解决了这一挑战。这种持续分析可确保当恶意软件在经过首次检测并被允许进入设备后，再次对其做出恶意裁定。持续分析是实现追溯性安全的关键促进因素（图 2）。

面向网络的思科 AMP 系统的追溯性警报可告知您观察到的文件是在何时被确定为恶意的（即使该文件是在数小时或数天前侵入网络也是如此），从而使您能够采取措施减轻损失。

图 2. “时间点检测”方法与“持续分析和追溯性安全”方法的比较



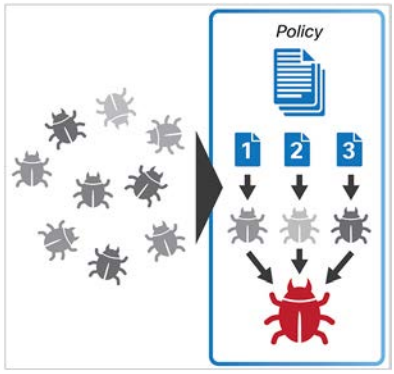
将离散事件与协同攻击相关联

面向网络的思科 AMP 还包括 Cisco FireSIGHT™ 管理中心（图 3），即结合了思科发现与感知技术的控制面板。它收集有关主机、操作系统、应用、用户、文件、网络、地理位置信息和漏洞的信息。面向网络的 Cisco AMP 在 FireSIGHT 管理中心内将这些离散但相关的事件组合成一个聚合视图，称为 IoC。

图 3. Cisco FireSIGHT 管理中心

此视图会自动按优先级列出可能受影响的设备，其中包括来自多个事件源的安全事件数据，以说明与现行攻击关联的风险（图 4）。助这些补充的情景数据，您可以做出更明智的决策并确定最佳做法。

图 4. 事件关联

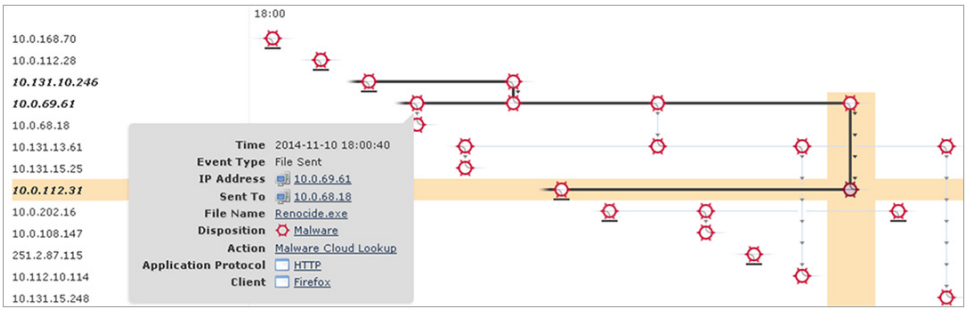


跟踪恶意软件的传播和通信

面向网络的思科 AMP 使用的文件轨迹功能可供您在整个网络中跟踪文件传输。文件轨迹视图中的每个文件都具有关联的轨迹图，其中会直观地显示出文件随时间推移的传输情况，并包含文件的其他相关信息。

文件轨迹对于确定潜在感染的影响和范围至关重要，该视图可提供有助于决策的重要 FireSIGHT 数据。情景信息（例如目标系统和该系统的用户，以及协议和通信尝试）均可用于更好地了解与文件关联的风险。

图 5. 文件轨迹



遏制恶意软件以防止损失和病毒爆发

如果您决定对活动的攻击采取措施，面向网络的思科 AMP 具有快速遏制攻击的功能。可以通过简单的策略更新将文件列入黑名单并阻止恶意软件通信。借助自定义检测列表，您可以在需要时随时采取行动，而不是等待供应商提供更新后才能采取措施。

无与伦比的安全情报和动态分析

面向网络的思科 AMP 基于大数据和无与伦比的安全情报。思科安全情报运营中心和 Talos 安全情报与研究小组可提供业内最大的实时威胁情报集合，不仅具有最广泛的可视性和覆盖范围，而且能够在多种安全平台上转化为可执行的信息。这些数据会在准备就绪后从云端推送至 AMP 客户端，以便您时刻拥有最新的威胁情报。

组织可以从这个庞大的实时威胁情报集合中受益，它包括：

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

面向网络的 AMP 会依据这个情景丰富的强大知识库自动关联文件、行为、遥测数据和活动，阻止各种试图渗入网络的威胁。安全团队通过 AMP 可以深入了解网络内的威胁，并能够对事件更轻松地做出更快响应。

思科 AMP 在第三方测试中一马当先

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。根据《2013-14 年 NSS Labs 产品分析报告》和《2014 年 NSS Labs 漏洞检测系统比较分析报告》，思科 AMP：

- 具有最高的整体检测率
- 具有最出色的检测时间
- 产生最低的受保护单位传输速度的总拥有成本
- 在安全价值图中名列前茅

NSS Labs 的结果表明，面向网络的思科 AMP 提供最高级别的安全效力和性价比。作为 Snort（入侵检测和防御标准）的创始者，我们以安全为本。我们的 FirePOWER 设备阵容实现了前所未有的吞吐量性能、成本效益和规模。FireSIGHT 管理中心通过使用情景感知了解网络的组成来提高准确性并加强自动化。

表 1 突出显示面向网络的思科 AMP 的同类最佳功能。

表 1. 面向网络的思科 AMP 的功能和优势

功能	优势
持续分析	面向网络的思科 AMP 利用基于云的大数据分析不断对持续收集的数据进行重新评估，以检测隐藏的攻击，从而超越了时间点检测方法。
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。当出现任何危害表现时（例如事件触发器、文件处理结果变化，或 IoC 触发器），都将需要追溯性安全。
FireSIGHT 管理中心	通过单一管理平台提供全面的情景视图（有关主机、操作系统、应用、用户、文件、网络、地理定位信息和漏洞的视图），使您获得对整个环境的可视性，进而做出明智的安全决策。
综合安全情报	思科安全情报运营中心和 Talos 安全情报与研究小组可提供业内最大的实时威胁情报集合，不仅具有最广泛的可视性和覆盖范围，而且能够在多种安全平台上转化为可执行的信息。
危害表现	危害表现 (IoC) 是按照可能处于活动状态的漏洞进行关联和优先级划分的文件事件和遥测事件。面向网络的思科 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，并确定高风险事件的优先级。
文件信誉	通过收集高级分析和综合情报来确定文件是安全的还是恶意的，从而进行更准确的检测。
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时差威胁。
追溯检测	当文件处理结果在扩展分析之后发生变化时，系统将发出警报，使您感知并发现逃过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。
集成式 SSL 解密	识别并解密 SSL 加密网络流量，并对该流量执行检查和检测。您也可以实施 SSL 证书策略并对网络启用中央 SSL 策略控制。
与面向终端的 AMP 集成	面向网络的思科 AMP 与面向终端的思科 AMP（一种适用于 PC、Mac、移动设备和虚拟系统的高级恶意软件防护产品）相兼容。通过部署这两种系统，贵组织可以在整个扩展 IT 生态系统中实现无与伦比的监视和控制。

产品性能和规格

可以在任何 Cisco FirePOWER 安全设备上部署面向网络的 Cisco AMP。但是，思科 AMP 专用设备 AMP7150、AMP8050、AMP8150、AMP8350、AMP8360、AMP8370 和 AMP8390（请参阅表 2）提供面向网络的 Cisco AMP 解决方案中所提供的所有优势。它们部署在提供专用处理能力和存储以在严苛环境中实现特定目标的设备型号上。

表 2. 硬件规格：面向网络的专用思科 AMP 设备

	AMP7150	AMP8050	AMP8150	AMP8350	AMP8360	AMP8370	AMP8390
高级恶意软件防护吞吐量 [1]	500 Mbps	1 Gbps	2 Gbps	5 Gbps	10 Gbps	15 Gbps	20 Gbps
最大监控接口数 [2]	12	12（3 x 4-端口 RJ45 网络模块）	12（3 x 4-端口 RJ45 网络模块）	28（7 x 4-端口 RJ45 网络模块）	24（6 x 4-端口 RJ45 网络模块）	20（5 x 4-端口 RJ45 网络模块）	16（4 x 4-端口 RJ45 网络模块）
固定监控接口数	4 x 10/100/1000 (RJ45)	0	0	0	0	0	0
模块化接口	8 SFP (1GB) 无故障切换	是（需要网络模块）	是（需要网络模块）	是（需要网络模块）	是（需要网络模块）	是（需要网络模块）	是（需要网络模块）
网络模块扩展插槽	0	3	3	7	6	5	4
可编程故障开放接口	4 x 10/100/1000 (RJ45)	是（需要网络模块）	是（需要网络模块）	是（需要网络模块）	是（需要网络模块）	是（需要网络模块）	是（需要网络模块）
管理接口数	1 x 10/100/1000 (RJ45)	1 x 10/100/1000 (RJ45)	1 x 10/100/1000 (RJ45)	2 x 10/100/1000 (RJ45)	2 x 10/100/1000 (RJ45)	2 x 10/100/1000 (RJ45)	2 x 10/100/1000 (RJ45)
平均延迟	< 150 微秒	< 150 微秒	< 150 微秒	< 150 微秒	< 150 微秒	< 150 微秒	< 150 微秒
存储容量 (SSD)	120 GB	400 GB+	400 GB	400 GB+	800 GB+	1200 GB+	1600 GB+
堆叠式	否	否	否	是	是	是	是
冷却风扇	5	10	10	6	12	18	24
电源	2（热插拔）	2（热插拔）	2（热插拔）	2（热插拔）	4（热插拔）	6（热插拔）	8（热插拔）
外形规格	1U	1U	1U	2U	4U	6U	8U
尺寸（以英寸为单位）（深度 x 宽度 x 高度）	21.6 x 19.0 x 1.73	27.25 x 16.93 x 1.7	27.25 x 16.93 x 1.7	29 x 17.2 x 3.48	29 x 17.2 x 6.96	29 x 17.2 x 10.44	29 x 17.2 x 13.92
最大发货重量	29 磅（13.2 千克）	54 磅（25.5 千克）	54 磅（25.5 千克）	67 磅（30.5 千克）	2 x 67 磅	3 x 67 磅	4 x 67 磅
交流电压 [3]	100 - 240 VAC（额定） 90 - 264 VAC（最大）	100 - 240 VAC（额定） 85 - 264 VAC（最大）	100 - 240 VAC（额定） 85 - 264 VAC（最大）	100 - 240 VAC（额定） 85 - 264 VAC（最大）	100 - 240 VAC（额定） 85 - 264 VAC（最大）	100 - 240 VAC（额定） 85 - 264 VAC（最大）	100 - 240 VAC（额定） 85 - 264 VAC（最大）
当前 [4]	8 安（最大值超过完整范围）	8 安（最大值超过完整范围）	8 安（最大值超过完整范围）	11 安（最大值超过完整范围）	2 X 11 A	3 X 11 A	4 X 11 A
直流电压选项	否	否	否	是	是	是	是
最大功率输出 [5]	450 W	650 W	650 W	1000 W	2 X 1000 W	3 X 1000 W	4 X 1000 W
平均功耗 [7]	200 W	400 W	400 W	635 W	2 X 635 W	3 X 635 W	4 X 635 W
工作温度	5° C - 40° C	10° C - 35° C	10° C - 35° C	5° C - 40° C	5° C - 40° C	5° C - 40° C	5° C - 40° C
频率范围	47 Hz - 63 Hz	47 Hz - 63 Hz	47 Hz - 63 Hz	47 Hz - 63 Hz	47 Hz - 63 Hz	47 Hz - 63 Hz	47 Hz - 63 Hz
气流	从前到后	从前到后	从前到后	从前到后 [6]	从前到后 [6]	从前到后 [6]	从前到后 [6]
BTU/小时额定（重负载）	900 BTU	1725 BTU	1725 BTU	2900 BTU	2 X 2900	3 X 2900	4 X 2900
工作湿度	5 - 85%	5 - 85%	5 - 85%	5 - 85%	5 - 85%	5 - 85%	5 - 85%
符合 RoHS	是	是	是	是	是	是	是

[1] AMP 吞吐量数字包括已启用的防火墙、IPS 和 AMP 功能。根据思科控制范围之外的情况（包括应用的策略、协议组合以及检测到的平均数据包大小），实际体验到的网络性能会有所不同。

[2] 网络模块可能是故障转移或非故障转移。

[3] 所有机箱都具有相同的电压输入。

[4] 每个机箱都将通电。

[5] 每个机箱电源都向机箱额定输出 1000 W 电力。

[6] 每台设备有 2 个 1 平方英寸大小的 侧进气口。

[7] 电源需要 1+1 冗余。

[8] AMP 8360、8370 和 8390 是堆叠设备，因此某些规格乘以各堆叠中的数量即可（分别为 2、3 和 4）。

[*] 可能在 Cisco Firepower 设备数据表上引用了有关 NGIPS/NGFW 性能数字的规格 (http://www.cisco.com/go/ngips)。

[**] FirePOWER 设备和专用 AMP 设备维护同一平台等效性（例如，FP8350 与 AMP8350），并且是相同的设备与集成恶意软件存储包。

软件要求

表 3 中概括了软件要求。

表 3. 软件要求

基于网络的高级恶意软件防护 • 在所有 Cisco FirePOWER 7000 和 8000 系列设备（虚拟 64 位设备）上都受支持 • 需要 v5.3 或更高版本 • 需要 Cisco FireSIGHT 管理中心（管理中心需要通过互联网连接到综合安全情报云或现场思科 AMP 私有云虚拟设备）	信誉查找支持的文件类型（使用示例扩展名）： • Microsoft Office 文档（doc 和 xls） • 可移植文档 (pdf) • 存档文件 (jar) • 多媒体文件 (swf) • 可执行二进制文件（msexe 和 jar.pack）
支持的应用协议： • HTTP • SMTP • IMAP • POP3 • FTP • NetBIOS-ssn (SMB)	信誉查找的性质 • 安全（已知良好） • 未知（中立或数据不足） • 恶意（已知不好）
双向检查和控制	文件识别操作 • 检测或阻止（按文件类型、传输方向或协议） • 恶意软件云查找（查询信誉）
支持按地理源或目标阻止文件	IoC 关联支持的事件类型或数据源 • IPS 事件（网络） • 面向终端的思科 AMP • 恶意软件事件（网络） • 安全情报（网络及终端） • Cisco FireSIGHT 情景数据
支持综合安全情报云 提供的动态黑名单	自定义检测（用户定义的黑名单和白名单）
自动提交供在综合安全情报云中执行动态分析： • Microsoft 可执行文件（msexe 和 dll） • 分析后提供的威胁评分和动态分析报告	

平台支持和兼容性

面向网络的思科 AMP 包括您选择的 Cisco FirePOWER 设备、面向 AMP 的 Cisco FirePOWER 设备订用、Cisco FireSIGHT 管理中心，以及 IPS、应用和 URL 过滤的可选订用。

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：

- 面向网络的思科 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 C78-733182-02 03/15