Cisco AMP Threat Grid：通过高级恶意软件安全措施赢得主动权

优点

- 通过动态恶意软件分析，更深入地了解更强的防御
- 通过聚焦情景的安全分析，实时准确识别攻击
- 使用来自高级威胁源的威胁情报，主动保护企业
- 使用能够集成并自动执行现有安全产品和流程的强大 API，加速威胁检测和响应功能
- 通过云服务每天分析成千上万个威胁的规模和强大功能，抵御来自任何地方的威胁

当今的高级恶意软件隐藏在常见文件中，躲避防御，耐心等待攻击时机。安全团队在面临检测和分析高级威胁挑战的同时，其安全技术也缺乏阻止这些威胁的复杂性和互联性。

公司正在遭受无休止的攻击，同时每天都会产生安全漏洞。最引人瞩目的攻击会登上头版头条。全球的攻击者群体正在不断制造高级恶意软件，并通过多层面攻击和多个攻击载体侵入各种规模的组织。然而，公司仍然依赖过时的工具和部分有效的方法来保护其敏感数据。这些敏感数据主要采用基于签名的技术进行保护。安全团队目前能够识别并补救恶意软件的时间窗非常短。此外，公司正面临着相关员工严重短缺的情况，缺乏具备了解和防御高级恶意软件必需技能和经验的员工。

Cisco AMP Threat Grid 可将动态恶意软件分析和威胁情报合并成一个解决方案，通过云或作为本地解决方案提供。它将实时行为分析、最新的威胁情报源与现有安全基础设施集成在一起。借助 AMP Threat Grid，您可以了解恶意软件正在执行或尝试执行的操作，它会造成多大的威胁，以及如何抵御它。

不断升级的攻击击败了传统的安全方法

根据 2015 年思科年度安全报告，网络犯罪分子正在设计能够依赖用户信任工具的恶意软件，以进行持续感染并躲藏在机器中不起眼的地方。2014 年普华永道 (PwC) 全球信息安全状态报告指出，相比前一年，组织检测到的攻击事件增加了 25%。较去年同期，这些事件造成的损失增加了 18%。2014 年 Verizon 数据泄露调查报告显示，四分之三的攻击会在数天或甚至几小时内危害整个组织，而组织可能需要数周或数月才能意识到正在遭受攻击，并且这一时间差距正在增加。

根据 ESG 2015 年全球 IT 支出调查，28% 的大中型企业表示他们组织中的 IT 安全技能持续短缺。

© 2015 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

安全组织不堪重负，正在进行一场艰苦卓绝的战斗，以应对高级威胁所带来的挑战。他们能够识别和响应攻击的技术非常少，更加难以了解大型、现代企业环境中所发生的事情。由于适用的专业安全人员很少且购买新防御的预算有限，企业正变得越来越容易受到攻击。

AMP Threat Grid 概述

AMP Threat Grid 提供更好地保护组织免遭恶意软件攻击所需的深入信息。借助其强大的、丰富的恶意软件知识库，组织可以了解恶意软件正在执行或尝试执行的操作，它会造成多大的威胁，以及如何抵御它。此解决方案包括以下功能：

恶意软件分析

AMP Threat Grid 通过安全众包形式收集来自封闭式社区的恶意软件信息，并使用专有技术（包括静态和动态分析）分析所有样本。不同于传统沙盒技术，我们的动态分析在虚拟环境以外，识别旨在躲避分析的恶意代码。作为分析的一部分，Glovebox 功能可帮助您与恶意软件进行实时交互，记录所有活动以备将来进行回放和报告。

威胁指数

凭借超过 350 项行为指标和源自全球的恶意软件知识库，AMP Threat Grid 能针对高级恶意软件提供前所未有的更准确且情景丰富的分析。提交到 AMP Threat Grid 的恶意软件示例基于两个关键要素提供威胁指数：严重性和信心。通过使用行为指标，AMP Threat Grid 会告诉您某个示例是恶意的、可疑的还是良性的，并告诉您原因，无需进行猜测。

增强现有安全技术

AMP Threat Grid 可透明地与组织的现有安全基础设施集成。它可自动利用来自终端代理、深度数据包检测平台、调查分析工具的提交示例，以及更多通过具象状态传输 (REST) API 和通过多种现有合作伙伴解决方案集成的提交示例。

有价值的威胁情报

AMP Threat Grid 提供高度精确的优质内容源。这些有助于组织生成有价值且具体的情景丰富的威胁情报。使用强大的 API，您可以将威胁信息直接导入现有的安全技术（包括安全信息和事件管理 (SIEM) 解决方案、网关、代理、可视化工具以及更多技术）来自动化检测和响应最复杂的威胁。

云的力量和规模

AMP Threat Grid 通过众包形式收集来自封闭式社区的恶意软件信息，并使用专有技术（包括静态和动态分析）分析所有样本。它将分析结果与数以亿计分析过的恶意软件示例相关联，以提供恶意软件攻击、活动及其分布的全局视图。安全团队可以快速地关联观察到活动和特征的单个样本并对照其他数百万个样本，从而透过历史和整体情景全面地了解其行为。

AMP Threat Grid 的云解决方案允许用户一次提交数千份示例进行分析，以便在几分钟内得到详细的报告，包括重要行为指标的确定以及威胁指数的分配情况。这可让安全团队迅速确定优先级并从高级攻击中进行恢复。

本地分析

AMP Threat Grid 设备可提供本地高级恶意软件分析功能，其中包含深度的威胁分析和内容。具有合规性和策略限制的组织将恶意软件示例提交到此设备进行分析，可帮助确保遵守组织的要求。借助 AMP Threat Grid 设备，所有样本都可使用专有且高度安全的静态和动态分析技术进行分析。它将结果与数十亿个经过分析的恶意软件标样，相关联，而无需在您组织的逻辑边界之外发送信息。

© 2015 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。

> “AMP Threat Grid 的解决方案首创在云中进行恶意软件分析，不仅能使我们更准确地检测和防御高级攻击，还能方便我们的州政府、地方政府、部落政府和准州政府合作伙伴之间快速共享威胁情报。”
>
> — William Pelgrin，互联网安全中心会长兼首席执行官，及美国多州信息共享与分析中心 (MS-ISAC) 主席

增强您的安全团队

无论在本地或在云中工作，安全团队可以对照其他数百万个样本，使用 AMP Threat Grid 快速地关联观察到活动和特征的单个样本或数百个样本，以便透过历史和整体情景全面地了解其行为。这可帮助您有效抵御针对性攻击和来自高级恶意软件的威胁。AMP Threat Grid 的详细报告（包括已发现的重要行为表现以及威胁分数评分）可帮助您快速确定高级攻击的优先级，并从中恢复。

不同的安全团队如何使用 AMP Threat Grid

表 1 显示了您的安全组织的不同成员如何使用 AMP Threat Grid。

表 1. 遍布整个组织的 AMP Threat Grid

应急响应	• 在数分钟内分析单个或数百个提交示例 • 使用 IP 地址、文件散列、互斥对象（互斥体）、域名、注册表项和 URL 来搜索恶意示例 • 使用 Glovebox 与恶意软件示例交互
安全运营部	• 生成所有恶意软件提交示例的威胁指数 • 为所有分析师提供简单易懂的行为指标 • 自动提交可疑示例进行分析
首席信息安全官	• 与现有安全技术集成 • 加快高级针对性攻击的检测速度 • 增强安全团队以便更快地做出反应

适用于 AMP Threat Grid 的思科高级服务

集成、自动化和补救

组织使用 AMP Threat Grid 更好地了解和保护他们的环境，以免遭当今高级恶意软件的攻击。思科高级服务可帮助您的组织完全集成 AMP Threat Grid 的动态恶意软件分析引擎和自动化示例提交。思科高级服务可帮助您快速利用 AMP Threat Grid 的威胁情报源，帮助现有安全技术自动提交和/或利用有价值的信息。

为什么选择思科？

现在的网络已扩展到所有有员工、数据以及可以访问数据的地方。因此，技术必须专注于检测、了解和阻止威胁。专注于威胁意味着应用可视性与情景以了解和适应环境中的变化，然后演变防护措施，从而采取行动并阻止威胁。如今，AMP Threat Grid 提供保护您的组织所需的深入级别的分析和威胁内容。

后续计划

有关详细信息或要观看组织使用 AMP Threat Grid 打击高级网络威胁的真实示例，请访问 http://www.cisco.com/go/amptg。

美洲总部
Cisco Systems, Inc.
加州圣荷西

亚太总部
Cisco Systems (USA) Pte, Ltd.
新加坡

欧洲总部
Cisco Systems International BV Amsterdam.
荷兰

思科在全球设有 200 多个办事处。www.cisco.com/go/offices 中列有各办事处的地址、电话和传真。

思科和思科徽标是思科和/或其附属公司在美国和其他国家/地区的商标或 注册商标。要查看思科商标的列表，请访问此 URL：www.cisco.com/go/trademarks。
本文提及的第三方商标为其相应所有者的财产。使用“合作伙伴”一词并不意味着思科和其他任何公司之间存在合作伙伴关系。(1110R)

美国印刷 C22-734156-00 03/15

© 2015 思科和/或其附属公司。版权所有。本文档所含内容为思科公开发布的信息。