Cisco AMP Threat Grid — 云

为了对抗恶意软件和高级威胁，您必须拥有最佳安全工具。思科® 高级恶意软件防护（AMP）Threat Grid 兼具两大领先的恶意软件防护解决方案：统一恶意软件分析和情景丰富的情报。它支持安全专业人员主动地防御网络攻击并快速地进行恢复。

产品概述

Cisco 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，并使用高度安全的专有技术（包括静态和动态分析）分析所有样本。它将结果与上百万个其他经分析的恶意软件人为因素相关联，以提供有关恶意软件攻击、活动及其分布的完整视图。安全团队可以对照其他上百万个样本，快速地关联所观察到的活动和特征的单个样本，以便透过历史和整体情景全面地了解其行为。该功能可帮助安全团队有效地抵御目标攻击和来自高级恶意软件的更加广泛的威胁。Cisco AMP Threat Grid 的详细报告包括标识重要的行为指标以及分配威胁指数，让您可以快速地划分高级威胁的优先级并从中恢复。

特性和优势

表 1 显示了 Cisco AMP Threat Grid 特性和优势。

表 1. Cisco AMP Threat Grid 的特性和优势

特性	优势
高级分析	• 针对恶意软件行提供全面的安全见解 • 在 Cisco AMP Threat Grid 的丰富数据库中提供指向样本源的直接链接以及关联行为 • 支持轻松地访问所有信息，并分析结果以进行进一步调查
高级行为指标	• 分析超过 300 个高度准确且实用的高级行为指标，而且误判率非常低 • 通过覆盖大量恶意软件系列和恶意软件行为的高级静态和动态分析生成全面的指标 • 围绕威胁提供最广泛的情景并帮助快速、自信地制定决策
威胁指数	• 通过专有分析和算法自动得出威胁指数，其中综合考虑了观察到的行为的把握程度和严重性、历史数据、频率和汇总指标以及样本 • 按把握程度划分威胁优先级，以反映每个样本的恶意行为级别 • 改善威胁的优先级划分，从而提高恶意软件分析人员、事件响应人员、安全工程团队的效率和准确性，并根据 Cisco AMP Threat Grid 的馈送完善产品
标准馈送格式	• 采用 JavaScript Object Notation（JSON）、网络观测表达式（CybOX）、结构化威胁信息表达式（STIX）和逗号分隔的值（CSV）等标准格式，提供易于集成的标准化馈送，并且作为 Snort 规则 • 为特定的安全产品提供自定义的馈送格式 • 随着时间推移，轻松一致地跟踪趋势并生成实用的报告
适用于集成的 API	• 利用现有的安全和网络基础设施，简化并快速实现威胁情报的运营化 • 利用 Cisco AMP Threat Grid 的表述性状态转移（REST）API 快速轻松地进行集成 • 提供有关大量第三方产品的集成指南，包括网关、代理以及安全信息和事件管理（SIEM）平台

全面的优质馈送内容

Cisco AMP Threat Grid 通过众包形式收集来自封闭式合作伙伴和客户社区的恶意软件信息，从而提供有关恶意软件攻击、活动及其分布的全局视图。AMP Threat Grid 每月分析数百万份样本并提取数 TB 丰富而实用的内容，形成分类清晰且容易使用的内容馈送。这样可帮助您有效地抵御各种各样的威胁并减少来自攻击的损害。Cisco AMP Threat Grid 提供了几种可应对大量威胁类型的预封装优质馈送，其中包括：

- 各种木马病毒，包括远程访问木马（RAT）和一般会传播更多恶意软件并且表现出特定行为（如下载可执行文件）的恶意软件系列。
- 试图建立出站网络通信并表现出异常网络活动的恶意软件。例如，发起恶意网络活动的 PDF 文件和 Microsoft Office 文档，通过各种协议和通道进行通信的恶意软件，使用非标准或错误匹配的网络协议的恶意软件，以及与已知“排水口”进行通信的恶意软件。Cisco AMP Threat Grid 使用特定的行为指标来生成馈送。其中包括用于帮助确定出站通信的网络指标。
- 主机上的恶意活动，包括对 Windows 主机文件和动态链接库（DLL）的修改以及劫持技术（无需修改注册表，便可在主机上安装恶意文件并保持持久性）。
- 经 Cisco AMP Threat Grid 确定具有高威胁指数的恶意软件。

表 2 显示了 Cisco AMP Threat Grid 所支持的平台和 Cisco IOS® 软件版本。

表 2. Cisco AMP Threat Grid：支持的平台和 OS

产品系列	支持的平台	支持的 Cisco IOS 映像（功能集）
Cisco AMP Threat Grid 门户	• Windows XP • Windows 7	**不支持**
Cisco AMP Threat Grid 动态分析	支持的分析文件类型： • 可移植的可执行 32 位（PE32）文件：可执行文件（exe）、动态链接库（dll） • Java 存档（jar） • Adobe 便携式文档格式（pdf） • Microsoft Office 文档：rtf、doc(s)、xls(x)、ppt(x) • ZIP（zip）作为容器 • URL：互联网快捷方式文件（url） • HTML 文档	**不适用**

许可

Cisco AMP Threat Grid 功能提供深度分析和结果，其中包括流程映射和注册表分析、网络连接以及关于恶意软件在环境中的执行情况的视频（如果适用）。还可以提供经分析的情报数据的批量馈送，并且能够从一套更加广泛的 Cisco AMP Threat Grid 数据中创建自定义馈送。

而且，Cisco AMP Threat Grid 的客户还可以通过云门户直接提交样本，也可以通过 Cisco AMP Threat Grid API 自动提交。依据 1 年或 3 年内容订阅许可所有云服务元素。订阅级别包括每个级别的用户帐户数量以及每天提交到 Cisco AMP Threat Grid 云以进行分析的文件数量。

表 3 显示了创建的分析人员（能够登录 Cisco AMP Threat Grid 门户进行调查和分析）帐户数量以及可以手动提交或者通过 API 提交到 Cisco Threat Grid 云以进行静态和动态分析的相应文件数量。

表 3. 分析人员帐户许可证以及可提交以进行分析的文件

许可级别：帐户数量	每天最大提交量
5	500
10	1,500
25	2,500
100	10,000

思科和合作伙伴服务

来自思科和思科认证合作伙伴的服务可帮助您规划并实施与 Cisco AMP Threat Grid 的优质威胁馈送和 REST API 的集成。规划和设计服务可以调整现有的基础设施、Cisco AMP Threat Grid 优质内容馈送格式和操作流程，以便于您充分地利用高级威胁馈送。

更多详情

有关 Cisco AMP Threat Grid 统一恶意软件分析和威胁分析的更多信息，请访问 http://www.cisco.com/c/en/us/solutions/enterprise-networks/advanced-malware-protection/index.html。

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 C78-733495-00 12/14