Cisco AMP Threat Grid - 设备

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 设备在单个设备中集成了两种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。借助该产品，安全专业人员可以主动防御网络攻击并实现快速恢复。

产品概述

AMP Threat Grid 设备可提供内部部署高级恶意软件分析功能，其中包含深度的威胁分析和丰富的内容。它支持组织上传恶意软件样本，从而有助于组织实现合规性并遵循政策限制。来自 AMP Threat Grid 的联合数据会形成单向连续数据流，可在提供所需恶意软件防护的同时，帮助确保遵守组织要求。

通过 AMP Threat Grid 设备，您可以使用高度安全的专有静态和动态分析技术来分析任何样本。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，从而全面地了解恶意软件攻击、活动及其分布的相关信息。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。此功能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。

特性和优势

表 1 显示了 AMP Threat Grid 设备的特性和优势。

表 1. Cisco AMP Threat Grid 设备的特性和优势

特性	优势
用户处部署设备	提供安全且高度可靠的内部部署静态和动态恶意软件分析功能。能够轻松与现有安全基础设施集成。可为恶意软件分析结果提供安全的用户内部部署存储。
高级分析	提供关于恶意软件行为的全面安全见解，以及与 AMP Threat Grid 庞大数据库中的样本源和相关行为对应的直接链接。支持轻松访问所有信息和分析结果，以进行进一步调查。
高级行为指标	可高度准确且切实有效地分析 350 多种高级行为表现，而且误判率非常低。通过涵盖大量恶意软件系列和恶意行为的高级静态和动态分析生成全面的威胁表现。围绕威胁提供最广泛的情景，帮助快速且自信地做出决策。
威胁分数	通过专有分析和算法自动得出威胁分数，其中会综合考虑已观察到的行为的可信度和严重性、历史数据、频率，以及聚类的表现和样本。设备将按可信度确定威胁优先级，以反映每个样本的恶意行为级别。增强威胁优先级的确定，从而为恶意软件分析人员、事件响应人员、安全工程团队以及使用 AMP Threat Grid 数据源的产品提高效率和准确性。
便于集成的 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。通过 AMP Threat Grid 的 REST API 可实现快速轻松的集成。该设备还提供面向各种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。

全面的内部部署恶意软件分析

对于受合规性和政策限制而无法将样本上传到云端的组织，AMP Threat Grid 可提供专用设备，用于在 AMP Threat Grid 联合威胁情报的全力支持下实现本地恶意软件分析。AMP Threat Grid 可提供有关恶意软件攻击、活动和分布的全局信息。它每月会分析数百万个样本，并生成数 TB 恶意软件分析信息，形成切实有效且内容丰富情报。

安全团队可以快速参照数百万个其他样本对单个恶意软件样本中观察到的活动和特征进行关联分析，从历史和全局角度全面了解其行为，从而有效地防范针对性攻击和来自高级恶意软件的更广泛威胁。AMP Threat Grid 的详细报告能够识别关键行为威胁表现并给出威胁分数，从而帮助快速而精确地确定高级攻击的优先级，并从中恢复。分析功能包括：

- 可提供对恶意软件行为的全面理解的动态和静态分析引擎
- 有关所有恶意软件样本活动（包括网络流量）的详细分析报告
- 专为安全运营中心 (SOC) 分析人员、恶意软件分析人员和事故调查人员而设计的用户界面工作流程

许可

Cisco AMP Threat Grid 设备的许可基于每天分析的最大文件数量，详见表 2。

表 2. Cisco AMP Threat Grid 设备型号和许可

	Cisco AMP Threat Grid 5000	Cisco AMP Threat Grid 5500
每天分析的最大文件数量	1500	5000

产品规格

产品规格如表 3 所示。

表 3. Cisco AMP Threat Grid 设备产品规格

特性	Cisco AMP Threat Grid 5000	Cisco AMP Threat Grid 5500
外形	1 机架单元 (1RU)	1RU
网络接口	10 GB 双端口铜缆	10 GB 双端口铜缆
电源选项	AC 或 DC	AC 或 DC

订购信息

要订购 Cisco AMP Threat Grid 设备，请访问思科订购主页。表 4 中提供了订购信息。

表 4. Cisco AMP Threat Grid 设备订购信息

部件号	产品说明
Cisco AMP Threat Grid 5000 设备和订用	
TG5000-BUN	Cisco AMP Threat Grid 5000 设备和订用捆绑包
TG5000-K9	Cisco AMP Threat Grid 5000 设备及软件
L-TG5000-1Y-K9	5000 型号的 Threat Grid 内容订用许可证，1 年
L-TG5000-3Y-K9	5000 型号的 Threat Grid 内容订用许可证，3 年
Cisco AMP Threat Grid 5500 设备和订用	
TG5500-BUN	Cisco AMP Threat Grid 5500 设备和软件捆绑包
TG5500-K9	Cisco AMP Threat Grid 5500 设备及软件
L-TG5500-1Y-K9	5500 型号的 Threat Grid 内容订用许可证，1 年
L-TG5500-3Y-K9	5000 型号的 Threat Grid 内容订用许可证，3 年

思科和合作伙伴服务

思科和思科认证合作伙伴提供的服务可帮助您规划并实施与 AMP Threat Grid 优质威胁数据源和 REST API 的集成。规划和设计服务可以调整现有的基础设施、AMP Threat Grid 优质数据源格式和操作流程，以便于您充分地利用高级威胁数据源。

后续计划

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 C78-733667-00 01/15