# [外部] — 使用高级恶意软件防护(AMP)错误检测、爆发和事件响应

## 目录



## 简介

我们始终努力改进和扩展高级恶意软件防护(AMP)技术的威胁情报，但是，如果您的AMP解决方案未触发警报或错误触发警报，您可以采取一些措施来防止对环境造成任何进一步影响。本文档提供了有关这些措施项的指南。

## 描述

### 即时动作

如果您认为AMP解决方案无法保护您的网络免受威胁，请立即采取以下操作：

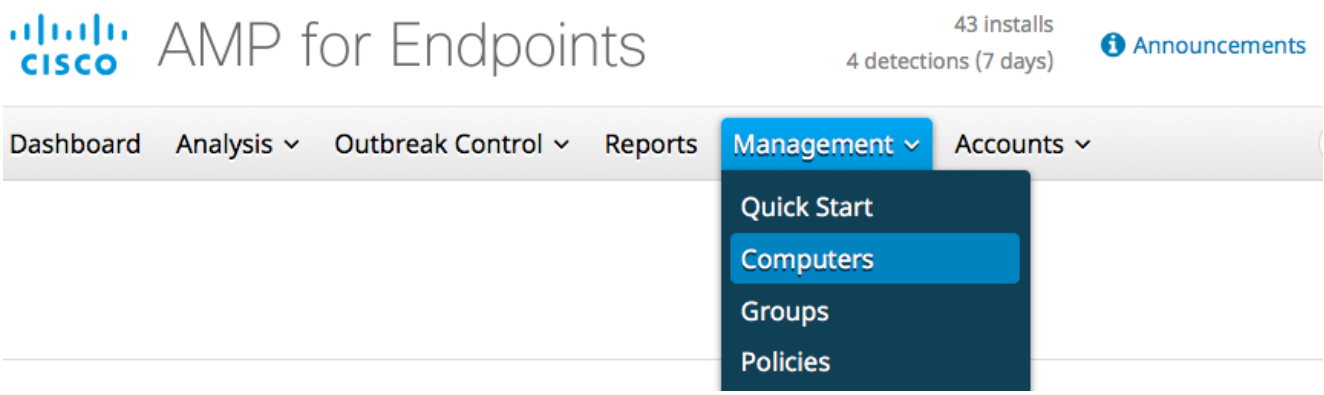
1. 将可疑计算机与网络的其余部分隔离。这可能包括关闭计算机或从物理上将其与网络断开。
2. 写下有关感染的重要信息，例如计算机可能受感染的时间、可疑计算机上的用户活动等。

   **警告**：请勿擦除或重新映像计算机。它消除了在取证调查或故障排除过程中发现违规软件或文件的机会。

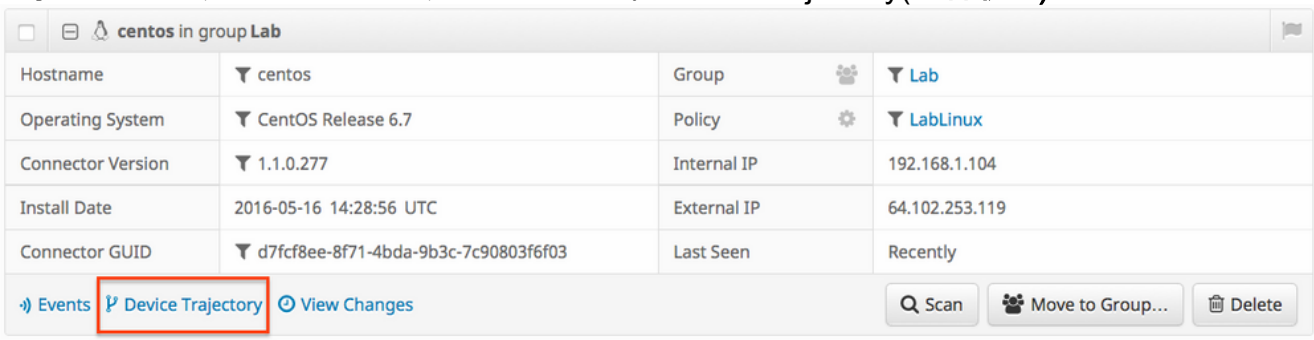
### 分析

1. 使用“设**备轨迹**”(Device Trajectory)功能开始您自己的调查。Device Trajectory能够存储大约900万个最新文件事件。面向终端的AMP设备轨迹对于跟踪导致感染的文件或进程非常有用。

   在控制面板中，导航至**Management > Computers**。




查找可疑计算机并展开该计算机的记录。单击“Device Trajectory(**设备轨迹**)”选项。




2. 如果发现任何可疑文件或哈希，请将其添加到自定义检测列表。面向终端的AMP可以使用自定义检测列表将文件或散列视为恶意。这是提供止裂覆盖以防止进一步影响的绝佳方法。

## 思科分析

1. 提交任何可疑样本以进行动态分析。您可以从仪表板中的“分析”**>“文件分析”**手动提交这些样本。面向终端的AMP包括动态分析功能，可从Threat Grid生成文件行为报告。如果需要我们的研究团队进行其他分析，这也有为思科提供文件的好处。

2. 如果您怀疑网络*中存*在误*报或误*报检测，我们建议您对AMP产品使用自定义黑名单或白名单功能。当您联系思科技术支持中心(TAC)时，请提供以下信息以供分析：文件的SHA256哈希。文件的副本（如果可能）。有关文件的信息，如文件的来源以及文件在环境中的原因。解释为什么您认为这是误报或误报。
3. 如果您需要帮助缓解威胁或执行环境分类，您需要与Cisco Talos事件响应(CTIR)团队合作，该团队专门负责制定行动计划、研究受感染的计算机，以及利用高级工具或功能来缓解活动爆发。
   **注意**：思科技术支持中心(TAC)不提供此类活动的帮助。可在此处联系CTIR。除非您的组织有思科事故响应服务的固定费用，否则此服务的起价为60,000美元。参与后，他们将提供有关其服务的其他信息，并为您的事件提交案例。我们还建议您跟进您的思科客户经理，以便他们能提供有关流程的其他指导。

# 相关条目

- WindowsFireAMP
- FireAMP