# [Externo] - Trabalhando com detecção de falhas, ataques e resposta a incidentes do Advanced Malware Protection (AMP)

## Contents



## Introduction

Sempre nos esforçamos para melhorar e expandir a inteligência de ameaças para nossa tecnologia de Proteção avançada contra malware (AMP). No entanto, se a solução AMP não disparou um alerta ou disparou um alerta de forma errada, você pode tomar algumas medidas para evitar qualquer impacto adicional no seu ambiente. Este documento fornece uma diretriz sobre esses itens de ação.

## Descrição

### Ações imediatas

Se você acredita que sua solução AMP não protegeu a sua rede de uma ameaça, execute as seguintes ações imediatamente:

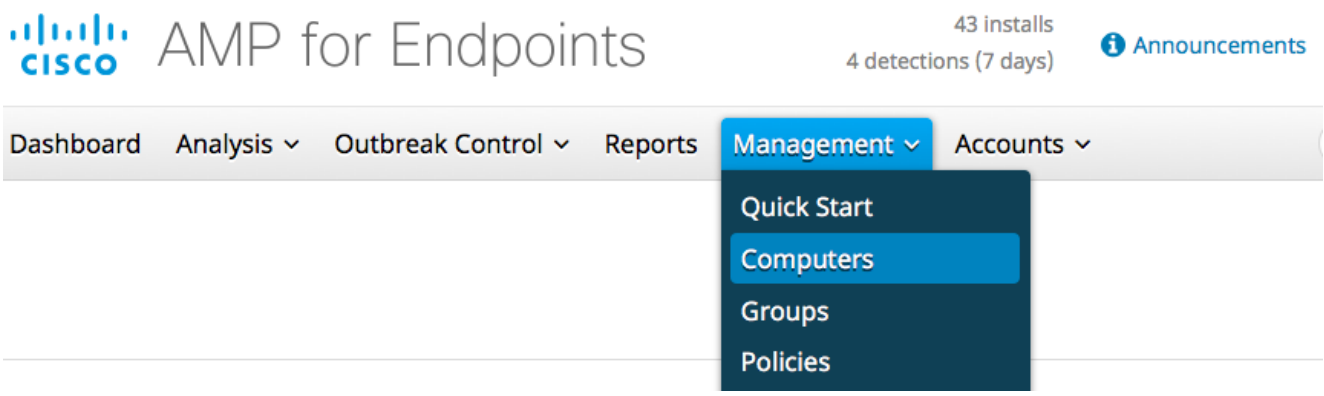
1. Isole as máquinas suspeitas do resto da rede. Isso pode incluir desligar a máquina ou desconectá-la fisicamente da rede.
2. Anote as informações importantes sobre a infecção, como, por exemplo, a hora em que a máquina pode estar infectada, as atividades do usuário nas máquinas suspeitas, etc.

**Aviso**: não apague nem recrie a máquina. Ele elimina as chances de encontrar o software ou arquivos ofensivos durante a investigação forense ou o processo de solução de problemas.

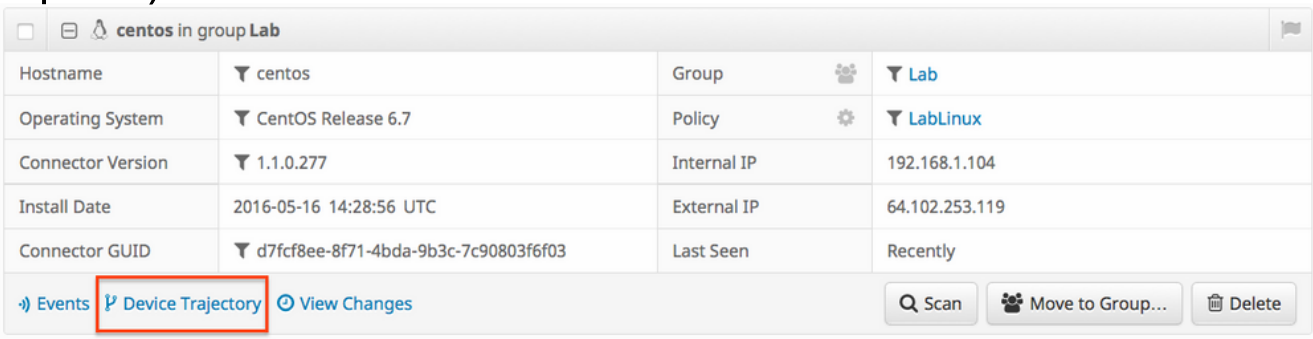
### Análise

1. Use o recurso **Trajetória do dispositivo** para iniciar sua própria investigação. A trajetória do dispositivo é capaz de armazenar aproximadamente os 9 milhões de eventos de arquivo mais recentes. A trajetória do dispositivo AMP for Endpoints é muito útil para rastrear arquivos ou processos que levaram a uma infecção.

No painel, navegue para **Management > Computers**.




Encontre a máquina suspeita e expanda o registro dessa máquina. Clique na opção **Device Trajettory (Trajetória do dispositivo)**.




2. Se encontrar algum arquivo suspeito ou hash, adicione-o às suas listas de detecção personalizadas. A AMP para endpoints pode usar uma lista de detecção personalizada para tratar um arquivo ou hash como mal-intencionado. Essa é uma excelente maneira de fornecer cobertura de falhas para evitar mais impacto.

## Análise da Cisco

1. Envie amostras suspeitas para análise dinâmica. Você pode enviá-los manualmente a partir de **Analysis > File Analysis** no painel. O AMP para endpoints inclui a funcionalidade de análise dinâmica que gera um relatório do comportamento do arquivo do Threat Grid. Isso também tem o benefício de fornecer o arquivo à Cisco caso seja necessária uma análise adicional por parte da nossa equipe de pesquisa.

2. Se suspeitar de *falsas* detecções *positivas* ou *negativas falsas* na sua rede, recomendamos que você aproveite a funcionalidade de lista negra personalizada ou de lista branca para seus produtos AMP. Ao entrar em contato com o Cisco Technical Assistance Center (TAC), forneça as seguintes informações para análise:O hash SHA256 do arquivo.Uma cópia do arquivo, se possível.Informações sobre o arquivo como de onde ele veio e por que ele precisa estar no ambiente.Explique por que você acredita que isso seja falso positivo ou falso negativo.
3. Se precisar de assistência para minimizar uma ameaça ou triagem de desempenho do seu ambiente, você precisará envolver a equipe do Cisco Talos Incident Response (CTIR) especializada na criação de planos de ação, pesquisa em máquinas infectadas e uso de ferramentas ou recursos avançados para atenuar um ataque ativo.
**Note**: O Cisco Technical Assistance Center (TAC) não fornece assistência para esse tipo de

compromisso.CTIR pode ser contactado aqui. Este é um serviço pago que começa em US$ 60.000, a menos que sua empresa tenha um retentor para serviços de resposta a incidentes da Cisco. Depois de envolvidos, eles fornecerão informações adicionais sobre seus serviços e abrirão um caso para o incidente. Também recomendamos o acompanhamento do seu gerente de contas da Cisco para que ele possa fornecer orientação adicional sobre o processo.

## Artigos relacionados

- Coleta de dados de diagnóstico de um conector FireAMP em execução no Windows
- Tipos de arquivos que são verificados pelo FireAMP Connector