Resumo da solução

Segurança em conjunto

Informações adaptáveis permitem que você reaja imediatamente às ameaças emergentes.

TM

As organizações enfrentam vários problemas operacionais e de segurança na tentativa de erguer uma defesa eficaz contra as ameaças emergentes de hoje. Os ataques dirigidos avançados e do dia-zero usam cargas que nunca foram vistas antes. As ameaças de malwares polimórficos também representam problemas semelhantes. As contramedidas tradicionais por assinatura têm dificuldade de detectar cargas avançadas de malware.

Para combater de maneira eficaz as ameaças emergentes, as empresas precisam de um sistema de segurança que combine recursos de avaliação comportamental, de reputação e baseado em assinatura, tanto na rede quanto nos terminais (endpoints). Embora cada uma dessas camadas de tecnologia possa ser eficaz na identificação individual de ameaças, é importante que elas trabalhem juntas para dividir informações, adquirir conhecimento e adaptar-se para enfrentar as ameaças em evolução. As demoradas comunicações manuais entre as soluções de rede e terminais simplesmente não são rápidas o suficiente para neutralizar as ameaças da atualidade.

O McAfee® Threat Intelligence Exchange e o McAfee Advanced Threat Defense trabalham em colaboração para oferecer uma proteção automatizada e adaptável contra as ameaças emergentes. Independentemente do primeiro ponto de contato de um arquivo de malware desconhecido, assim que ele for identificado, todo o ambiente conectado será imediatamente atualizado. Se um arquivo for detectado pelo McAfee Advanced Threat Defense, o McAfee Threat Intelligence Exchange publicará essa detecção através de uma atualização de reputação, por meio da camada de troca de dados (DXL – data exchange layer), para todas as contramedidas na organização. Os terminais que operam com o McAfee Threat Intelligence Exchange contarão com proteção preventiva caso o arquivo apareça no futuro. Os gateways que operam com o McAfee Threat Intelligence Exchange impedem que o arquivo entre na empresa. Além disso, quando os terminais que operam com o McAfee Threat Intelligence Exchange encontram arquivos com reputações desconhecidas, eles são submetidos ao McAfee Advanced Threat Defense para definir se o objeto é mal-intencionado, eliminando os pontos cegos da distribuição de cargas fora da banda.

Preencha a lacuna de exposição

Identifique as cargas de malwares ocultos.

O McAfee Threat Intelligence Exchange e o McAfee Advanced Threat Defense trabalham em conjunto para analisar objetos suspeitos, seja qual for o ponto do primeiro contato. Quando novos arquivos tentam ser executados, eles ficam sujeitos às regras combinadas de terminais, ao conhecimento da reputação global e do ambiente, e a uma verificação estática e dinâmica aprofundada dos componentes conectados nesta solução colaborativa. Essa abordagem conectada de análise de ameaças gera uma identificação mais precisa do malware oculto que, de outra forma, poderia passar despercebido.

Principais benefícios

- Diminui drasticamente o tempo até a contenção, através de uma reação automatizada e adaptável.
- Proporciona maior visibilidade, agilidade e controle através da colaboração da rede aos terminais.
- Reage com inteligência aos eventos com informações conclusivas sobre reputação de arquivos e execução.
- Melhora a segurança, otimizando o TCO, graças à integração e implementação simplificadas.

intel Security

Reforce a detecção de ameaças com análise de ameaças por comportamento.
O McAfee Advanced Threat Defense oferece uma classificação de reputação com recursos inovadores de desconstrução de malware, incluindo uma "desembalagem" que atravessa as técnicas evasivas para expor o código executável original para determinar os comportamentos pretendidos. Juntos, o código estático e a análise dinâmica permitem uma avaliação completa e representam a tecnologia mais forte do mercado para detecção de ameaças avançadas.

Obtenha visibilidade e controle, do terminal até a rede.
O McAfee Advanced Threat Defense também recebe amostras de malware coletadas nos pontos de entrada da rede por outros produtos em seu ambiente. Por sua vez, esses componentes de rede podem dividir as informações recém-descobertas que foram adquiridas dessas amostras através do McAfee Threat Intelligence Exchange. Esse compartilhamento de informações e reputação demonstra como a rede e os terminais aproveitam a plataforma Security Connected da McAfee. Além disso, o McAfee Threat Intelligence Exchange mantém um banco de dados de conhecimento que indica onde foram executados os últimos objetos no ambiente de terminais, proporcionando uma visibilidade conclusiva dos encontros.

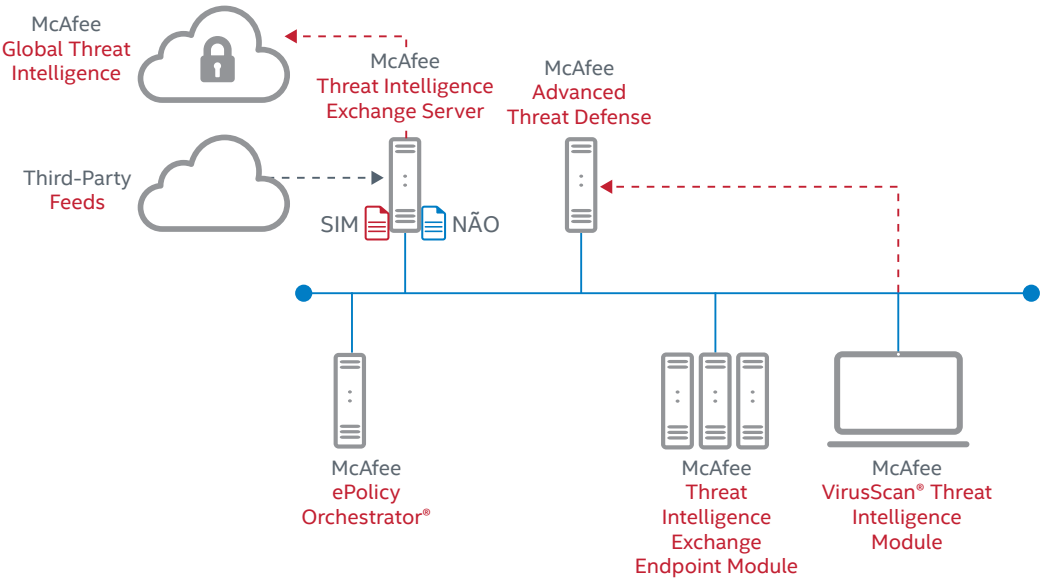

Figura 1. Síntese de informações e reputação da nuvem, rede e terminais.

Reação adaptável

Depois que o McAfee Advanced Threat Defense analisa e classifica um arquivo, os resultados são enviados ao McAfee Threat Intelligence Exchange. A nova reputação dos arquivos, seja ela boa ou má, é publicada de imediato para todas as contramedidas do ambiente que operam com o McAfee Threat Intelligence Exchange. Qualquer instância futura do arquivo será compreendida e todos os componentes que operam com o McAfee Threat Intelligence Exchange tomam as medidas de acordo com a política para liberá-la, bloqueá-la ou limpá-la. Essa reação adaptável protege o ambiente de maneira instantânea, inclusive a rede, o gateway e os terminais. A agilidade de reação aumenta, ao passo que o tempo de contenção e correção diminui drasticamente, tudo isso dispensando a remodelagem da rede.

Ativação do Security Connected com McAfee Data Exchange Layer

O McAfee Threat Intelligence Exchange é a primeira solução que usa a camada de troca de dados (DXL) da McAfee, uma estrutura de comunicação leve, ultrarrápida e bidirecional que viabiliza informações de segurança e a segurança adaptável por meio da integração dos produtos e do compartilhamento de contexto. Os produtos com o DXL da McAfee recebem dados e publicam informações na estrutura, sem a necessidade de trabalhos de integração por interfaces de programação de aplicativos (API) complexas nem configurações pesadas. Isso marca uma nova era na segurança, em que todos os componentes se reúnem para trabalhar como um sistema coeso.

Facilidade de implementação e gerenciamento

A integração entre o McAfee Threat Intelligence Exchange e o McAfee Advanced Threat Defense é perfeita em todo DXL. Projetada como uma estrutura aberta, o DXL permite que os componentes de segurança passem a fazer parte dinamicamente do McAfee Threat Intelligence Exchange, dispensando APIs extensas ou configurações complexas de produtos, o que diminui os erros e elimina grandes trabalhos manuais.

Figura 2. Integração perfeita em toda a camada de troca de dados (DXL) através do Security Connected.

Saiba mais

O McAfee Threat Intelligence Exchange e o McAfee Advanced Threat Defense são essenciais para conectar componentes de segurança diferentes, protegendo o seu ambiente, reagindo aos encontros e adaptando-se automaticamente às novas ameaças. Criando um ecossistema de segurança que integra análise avançada de ameaças, produtos de rede e soluções de terminal, a McAfee oferece visibilidade e contexto das ameaças, além de acelerar a reação e simplificar a correção.

http://www.mcafee.com/TIE

http://www.mcafee.com/ATD

http://www.mcafee.com/securityconnected

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com