McAfee Threat Intelligence Exchange

Inteligência contra ameaças compartilhada para combater ataques direcionados

O McAfee® Threat Intelligence Exchange permite detecção e resposta adaptáveis a ameaças operacionalizando a inteligência pelos seus endpoints, gateways, redes e soluções de segurança de data center em tempo real. A combinação de informações globais de ameaças importadas com inteligência coletada localmente e seu compartilhamento instantâneo permitem que suas soluções de segurança operem como se fossem uma só, trocando e agindo com base em inteligência compartilhada. O McAfee Threat Intelligence Exchange reduz o tempo entre a localização e a contenção, de dias, semanas e meses para milissegundos.

Principais vantagens

- A proteção adaptável contra ameaças reduz o tempo entre a localização e a contenção de ataques direcionados avançados, de dias, semanas e meses para milissegundos
- A inteligência contra ameaças colaborativa é criada a partir de fontes globais de dados de inteligência combinadas com a coleta de dados locais de inteligência contra ameaças
- Você tem a visibilidade imediata da presença de ataques direcionados avançados em sua empresa
- A inteligência de segurança relevante é compartilhada em tempo real entre endpoints, gateways, redes e soluções de segurança de data center

Crie um ecossistema colaborativo de inteligência contra ameaças

O McAfee Threat Intelligence Exchange compartilha informações pelo McAfee Data Exchange Layer e fornece segurança integrada. Entradas combinadas a partir de múltiplas fontes de informações de ameaças são compartilhadas instantaneamente com todas as soluções de segurança conectadas, incluindo soluções de terceiros.

Quando componentes de segurança atuam como um só, o compartilhamento de inteligência relevante para a detecção de ameaças é feito imediatamente entre endpoints, gateways, data centers, nuvem e outros pontos de controle de segurança em seu ambiente. A simplicidade na integração, ativada pelo McAfee Data Exchange Layer, reduz substancialmente os custos operacionais e de implementação, oferecendo segurança, eficiência operacional e eficácia incomparáveis.

Projetado como um framework aberto, o McAfee Data Exchange Layer permite que todas as soluções de segurança ingressem dinamicamente no ecossistema do McAfee Threat Intelligence Exchange, incluindo produtos de segurança de terceiros. O custo total de propriedade diminui e você pode aproveitar melhor o valor dos seus produtos de segurança e investimentos em soluções existentes com os seus componentes de segurança, que agora se comunicam plenamente uns com os outros.

A prevenção contra ameaças colaborativa e adaptável é uma abordagem nova e radical para implementar segurança de TI, unindo os seus diferentes sistemas para promover uma verdadeira coordenação de segurança. As equipes de segurança precisam ter a capacidade de automatizar o compartilhamento de informações sobre ameaças à segurança e aplicar proativamente

Principais vantagens (continuação)

- Você ganha o poder de tomar decisões sobre arquivos nunca vistos com base no contexto dos endpoints (atributos de ambiente, arquivo e processo), combinado com a inteligência contra ameaças coletiva
- A integração por meio do McAfee Data Exchange Layer é simplificada. A coordenaçao das soluções de segurança da Intel Security e de terceiros reduz os custos operacionais e de implementação e operacionaliza a sua inteligência contra ameaças em tempo real

políticas de prevenção e proteções a todos os pontos da rede, rompendo barreiras organizacionais e orçamentárias.

Transformando a infraestrutura de segurança em um sistema colaborativo, os administradores de segurança podem detectar, compartilhar e imunizar seus ambientes contra ameaças. O McAfee Threat Intelligence Exchange oferece um aumento significativo da resiliência e do controle na batalha contra ataques emergentes e direcionados.

Adapte-se e imunize-se contra ameaças

Todas as identificações compartilhadas, detectadas em todos os locais de sua rede, aumentam a profundidade da conscientização na batalha contra ataques direcionados. Como essas ameaças são ataques direcionados com precisão, as empresas precisam de um sistema local de vigilância para capturar as tendências e os ataques únicos que encontrarem. Estes dados contextuais locais reunidos a partir da localização e combinados com inteligência global sobre ameaças permitem uma melhor tomada de decisões sobre arquivos nunca vistos antes, resultando em tempos de proteção e detecção menores.

Um arquivo não identificado, encontrado em qualquer local de sua rede, é avaliado localmente pelo McAfee Threat Intelligence Exchange. Baseada na confirmação, a proteção é propagada por todos os sistemas em tempo real. Esta inteligência local contra ameaças fica guardada para futuras localizações e deixa de ser desconhecida, sendo detectada imediatamente caso seja vista novamente ou esteja em outro dispositivo ou servidor.

Por exemplo, a informação sobre um arquivo malicioso encontrado em seu gateway é enviada pelo McAfee Data Exchange Layer para o McAfee Threat Intelligence Exchange, chegando aos seus endpoints e data centers em milissegundos e imunizando-os proativamente contra a ameaça com a informação necessária. Uma tentativa de comprometimento bloqueada em um endpoint revela a existência de malware e compartilha essa informação instantaneamente, chegando ao gateway e a outros componentes de segurança e blindando o perímetro contra a ameaça.

Operacionalize a inteligência contra ameaças em tempo real

Agora você pode combinar a inteligência contra ameaças a partir de fontes globais importadas, como o McAfee Global Threat Intelligence (McAfee GTI), informações de ameaças de terceiros e indicadores de comprometimento (IoCs) compartilhados, como arquivos Structured Threat Information eXpression (STIX). O McAfee Global Threat Intelligence coleta dados históricos e locais em tempo real a partir de endpoints, data centers, gateways, da sua rede e de sua solução em área restrita McAfee Advanced Threat Defense. A combinação desses dados globais e locais de ameaças é operacionalizada e compartilhada por todo o seu ecossistema de segurança em tempo real.

O McAfee Threat Intelligence Exchange torna possível aos administradores personalizar com facilidade a inteligência abrangente contra ameaças a partir de fontes globais, como o McAfee GTI, dados de terceiros e arquivos STIX importados. Isso é combinado com a inteligência contra ameaças local proveniente de dados de eventos históricos e em tempo real entregues por endpoints, gateways, soluções em área restrita e outros componentes de segurança. Os administradores de segurança ganham o poder de montar, sobrepor, aumentar e ajustar as informações de inteligência abrangentes a fim de personalizar a proteção de seus ambientes e empresas, incluindo listas negras e listas brancas de arquivos, ou certificados atribuídos para e utilizados pela organização.

Estas informações contra ameaças priorizadas localmente e ajustadas fornecem respostas imediatas a quaisquer identificações futuras. Metadados descritivos sobre objetos essenciais são mantidos e refletidos na inteligência coletiva. Os administradores

Os ataques direcionados avançados são um desafio do mundo real

Projetados para evitar a detecção e estabelecer uma presença duradoura na organização a fim de vazar dados valiosos, os ataques direcionados avançados continuam causando problemas para as empresas. De acordo com dados divulgados recentemente como parte do *Verizon 2015 Data Breach and Investigations Report (Relatório de investigação de violações de dados da Verizon em 2015)* 70% a 90% das amostras de malware são exclusivas de uma única empresa, indicando que a detecção de indicadores de ameaças únicas é o maior desafio da atualidade.[1]

Para mais informações, visite **www.mcafee.com/br/products/threat-intelligence-exchange.aspx**

e produtos de gerenciamento de eventos e informações de segurança (SIEM) podem colaborar com base nas informações coletadas para identificar instantaneamente sistemas com uma alta probabilidade de serem comprometidos, de acordo com as atividades maliciosas anteriores.

Obtenha uma proteção avançada para endpoints

Com seu módulo VirusScan® Enterprise, o McAfee Threat Intelligence Exchange oferece uma proteção de endpoints inovadora. Usando regras configuráveis, o módulo toma decisões precisas sobre a execução de arquivos e aproveita a inteligência combinada a partir do contexto local do endpoint (atributos de ambiente, arquivo e processo) e da inteligência coletiva contra ameaças disponível no momento (por exemplo, prevalência organizacional, idade, reputação e mais).

Ao personalizar o módulo VirusScan Enterprise do McAfee Threat Intelligence Exchange com base no nível de tolerância ao risco da sua empresa nos endpoints, os administradores têm flexibilidade para definir condições de execução orientadas por seus requisitos específicos. Isso pode ser tão rígido quanto aderir a uma política de tolerância zero para arquivos desconhecidos ou "cinza", definindo regras para que nenhum arquivo seja acessado a menos que tenha uma reputação conhecida e aceitável.

Gerencie endpoints em qualquer lugar e a qualquer momento

O McAfee Threat Intelligence Exchange oferece prevenção adaptável contra ameaças e gerenciamento da segurança com alcance global. O McAfee Threat Intelligence Exchange alcança os endpoints, não importa onde estejam, e fornece os meios para gerenciar políticas de ameaças, detecções, atualizações de segurança e investigações remotas. Os componentes de segurança funcionam como um só, independentemente de limites físicos. Eles compartilham imediatamente os dados relevantes de segurança entre endpoints, gateways e outros produtos de segurança, independente da localização, permitindo uma prevenção adaptável contra ameaças.

Outras soluções de gerenciamento de segurança não são capazes de fazer o envio por push de alterações de políticas, conteúdo e atualizações de programa para os endpoints. Isso abre uma brecha que deixa as organizações expostas a um risco maior. Utilizando o McAfee Data Exchange Layer, o McAfee Threat Intelligence Exchange pode manter uma conexão persistente, independente de obstáculos na rede. Ele fecha efetivamente essa brecha de risco e garante que nenhum endpoint seja deixado desprotegido.

Beneficie-se da colaboração

Consulta de reputação com um clique

Quando um arquivo desconhecido é localizado por qualquer um dos componentes de segurança da sua empresa, seja o gateway, os endpoints ou a rede, a reputação do arquivo pode ser facilmente determinada de acordo com os atributos e com a sua inteligência composta contra ameaças.

Análise de ameaças avançadas
Caso sejam necessárias mais informações sobre um arquivo, o McAfee Threat Intelligence Exchange pode enviá-las automaticamente para o McAfee Advanced Threat Defense a fim de obter informações adicionais sobre novas ameaças potenciais imediatamente. Juntos, eles aproveitam a análise de ameaças feita com o exame estático e dinâmico do código a fim de determinar a reputação do arquivo em questão. Tudo isso é automatizado, documentado e compartilhado coletivamente pelo McAfee Data Exchange Layer para proteger todo o seu ecossistema de segurança.

Gerenciamento de eventos de segurança
O McAfee Enterprise Security Manager permite examinar mais profundamente quando indicadores de comprometimento são identificados pelo McAfee Threat Intelligence Exchange. O acesso às informações do histórico de segurança e a capacidade de criar listas de observação automatizadas aumentam a eficiência da segurança para as empresas.

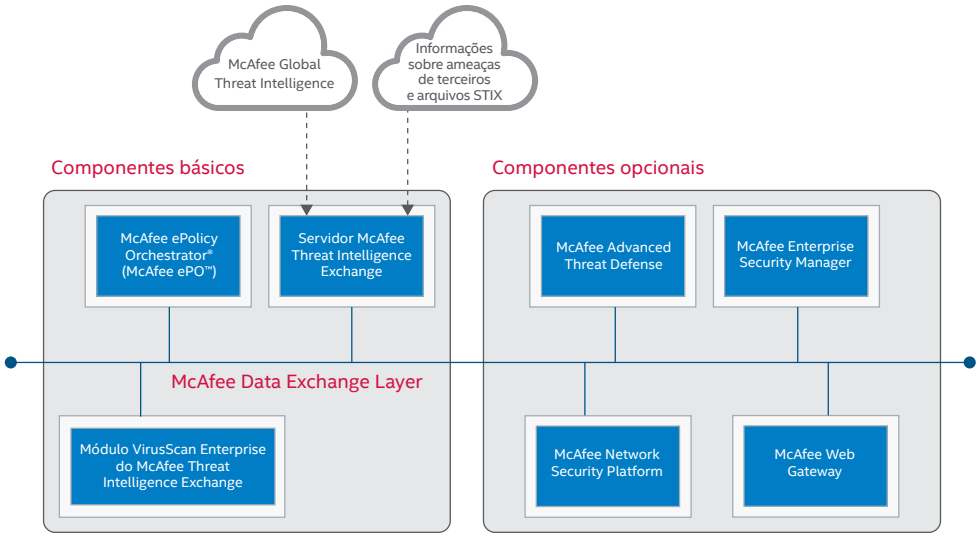

Figura 1. A simplicidade na integração por meio do McAfee Data Exchange Layer reduz custos operacionais e de implementação e permite uma eficiência operacional incomparável enquanto promove a evolução da plataforma Security Connected.

1. http://www.verizonenterprise.com/DBIR/2015/

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

62276ds_threat-intelligence-exchange_0216