Resumo da solução

Advanced Threat Defense para IPS de rede

Amplie a proteção contra malwares ocultos.

Principais vantagens

- Automaticamente detecta, paralisa e elimina malwares avançados e ataques ocultos no tráfego de rede.
- Adiciona análise eficaz de código estático e área restrita para alvos específicos à segurança de rede sem aumento nas cargas de trabalho de IPS.
- Bloqueio imediato de ameaças sem o atraso da intervenção humana.

O IPS (sistema de prevenção de intrusões) de rede é a base das arquiteturas de segurança empresarial. Implantado em banda junto com a segurança com base no gateway e no host, o IPS monitora o tráfego de rede e o comportamento dos terminais usando diversas técnicas para detectar ataques e acionar reações defensivas.

No entanto, atualmente, um número cada vez maior de ameaças de dia zero estão burlando as defesas tradicionais. Furtivos, cuidadosamente camuflados, inteligentemente adaptáveis e, em geral, estrategicamente direcionados, esses ataques sofisticados consistem em uma parte pequena, mas desproporcionalmente perigosa e cara do cenário de ameaças em constante mudança.
Em resposta, algumas empresas estão adicionando a análise dinâmica à sua infraestrutura de IPS na forma de appliances de área restrita fora de banda. A área restrita inicia executáveis suspeitos em um ambiente virtual seguro e monitora o comportamento do tempo de execução para detectar intenção maliciosa. Porém, muitas vezes, esse aparente aumento na precisão da detecção é rapidamente perdido devido à baixa integração e a processos de reação manuais.
Por exemplo, a maioria dos appliances de área restrita de terceiros só é capaz de alertar um analista de segurança humano quando um novo ataque é detectado. O analista precisa criar manualmente novas regras de bloqueio para o IPS e o firewall e, em seguida, iniciar a tarefa de identificar e corrigir todos os terminais que foram comprometidos durante a análise de área restrita fora de banda. Outras limitações comuns das soluções existentes incluem:

- Necessidade de um appliance de área restrita por sensor de IPS, o que aumenta os custos.
- Dependência de um ambiente de execução virtual genérico, que pode ignorar comportamentos de ataque direcionados a alvos específicos.
- Dependência unicamente da análise dinâmica, tornando a área restrita vulnerável a diversas estratégias de malware que detectam ambientes seguros e atrasam a manifestação do comportamento identificável.

Uma solução de IPS e área restrita Security Connected

A McAfee oferece uma solução para todos esses desafios: uma combinação fortemente integrada do McAfee Network Security Platform, um sensor de IPS avançado de alto desempenho, e do McAfee Advanced Threat Defense, o appliance de detecção de malwares avançados mais eficiente e completo do mercado. O McAfee Network Security Platform oferece inspeção de tráfego na banda e bloqueio de ameaças através de um conjunto de tecnologias de detecção de malware otimizadas para execução em tempo real. O produto oferece um conjunto mais amplo e pesado de análises, que incluem análise eficaz de código estático e área restrita para alvos específicos. Juntos, esses dois dispositivos detectam e paralisam novas ameaças avançadas, desconhecidas e ocultas. Para ter uma solução completa de ponta a ponta, inclua o McAfee Real Time para rapidamente identificar e corrigir os sistemas afetados por malwares avançados.

- *Detecte*: as tecnologias de análise inovadoras funcionam em conjunto para detectar ameaças sofisticadas em vários protocolos com rapidez e precisão.
- *Paralise*: os produtos de segurança fortemente integrados da McAfee instantaneamente interrompem as tentativas de infiltração e isolam os terminais infectados.
- *Corrija*: a solução da McAfee automaticamente examina uma nova infiltração detectada no ambiente e inicia o processo de correção de terminais.

Implantação centralizada

Dimensionamento e menor custo total de propriedade

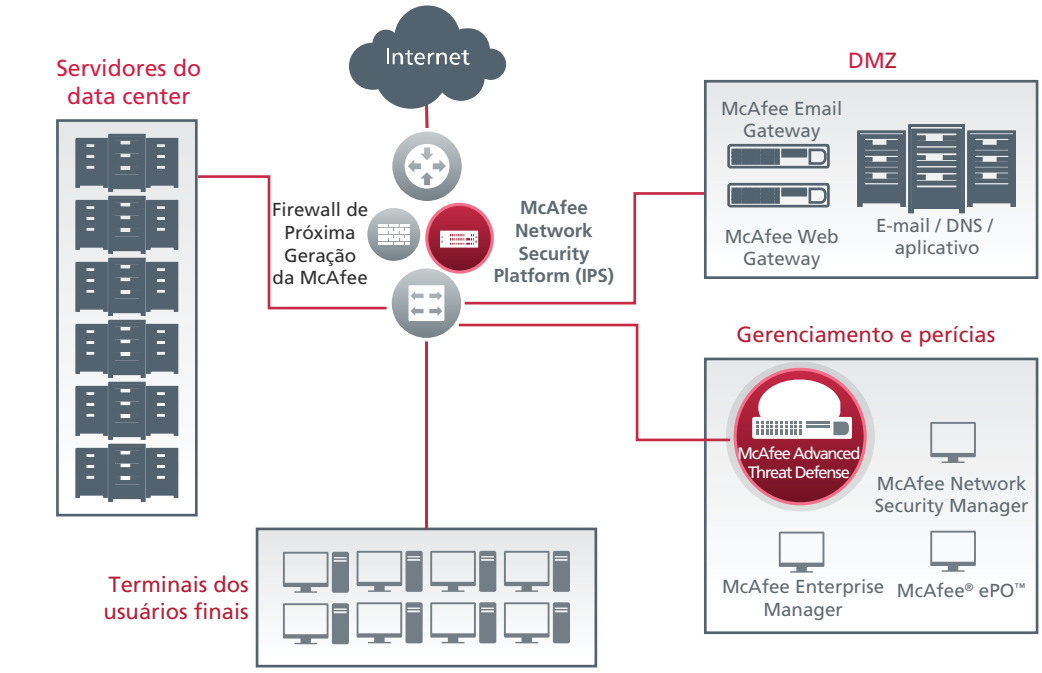

Figura 1. Implantação centralizada da solução de IPS McAfee® Network Security Platform.

Como a solução McAfee Advanced Threat Defense para IPS de rede segue a abordagem Security Connected para integração da segurança empresarial, ela oferece diversas vantagens operacionais e defensivas exclusivas no setor, incluindo:

- *Bloqueio imediato de ameaças:* os ataques detectados pelo McAfee Advanced Threat Defense são automaticamente bloqueados pelo McAfee Network Security Platform sem necessidade da intervenção humana e seu atraso.
- *Integração de relatórios e fluxos de trabalho:* os relatórios gerados pelo McAfee Advanced Threat Defense são automaticamente integrados aos fluxos de trabalho do McAfee Network Security Platform, eliminando a incessante alternância entre telas durante as investigações.
- *Visibilidade dos terminais:* o McAfee Advanced Threat Defense pode acessar e aproveitar todas as informações sobre terminais armazenadas no McAfee Network Security Platform para aumentar a velocidade e a precisão da detecção de ameaças.

Melhores juntos

- Aumente o retorno sobre os investimentos existentes em segurança.
- Reduza a necessidade de rearquitetar a rede.
- Amplie e automatize a proteção.
- Reduza o trabalho de correção e investigação com o bloqueio automático confiável.
- Simplifique os fluxos de trabalho com a interface do McAfee Network Security Platform.

Security Connected

A plataforma Security Connected da McAfee oferece um framework unificado para centenas de produtos, serviços e parceiros, possibilitando o aprendizado mútuo, o compartilhamento de dados de contextos específicos em tempo real e o trabalho em equipe para manter as informações e as redes seguras. Qualquer empresa pode reduzir os riscos e o tempo de resposta, bem como as despesas gerais e os custos com mão de obra operacional através dos conceitos, dos processos otimizados e das recomendações práticas da plataforma.

O IPS: McAfee Network Security Platform

O McAfee Network Security Platform é uma família de appliances integrados de IPS (sistema de prevenção de intrusões) que detectam e bloqueiam ameaças sofisticadas na rede, incluindo malwares avançados, ameaças de dia zero, ataques de negação de serviço e redes de bots. Combinando uma arquitetura de inspeção aprofundada de passagem única ultraeficiente com hardware especializado de categoria de operadora, o McAfee Network Security Platform oferece velocidades de linha de até 40 Gbps com um único dispositivo e mantém desempenho de taxa de transferência e precisão excepcionais, sejam quais forem as configurações de segurança. A análise integrada de ameaças inclui assinaturas personalizadas, análise completa de protocolos, reputação de ameaças, análise aprofundada de ameaças com emulação e detecção de JavaScript e correlação de comportamentos de ameaças ao uso de aplicativos com base na visibilidade de camada 7 de mais de 1.500 aplicativos e protocolos.

Talvez o recurso mais avançado do McAfee Network Security Platform seja sua capacidade de integração e aproveitamento de informações e recursos de outras soluções da McAfee. Para essa solução, são particularmente importantes as integrações diretas com:

- Real Time para McAfee® ePolicy Orchestrator® (McAfee ePO), que oferece o acesso de gerenciamento e a visibilidade de dispositivos em tempo real necessários para isolar e corrigir ataques bem-sucedidos.
- McAfee Enterprise Security Manager, uma solução de SIEM (gerenciamento de informações e eventos de segurança) que oferece uma visualização em tempo real do ambiente de TI interno combinada e correlacionada ao contexto global do mundo externo. O banco de dados amplamente atualizado do McAfee Enterprise Security Manager coleta bilhões de eventos de registro e os correlaciona a outros fluxos de dados relevantes, tornando imediatamente acessíveis vários anos de dados de eventos de segurança. Ele calcula padrões para todos os fluxos de dados de entrada para identificar anormalidades e ameaças em potencial antes que elas se desenvolvam, além de simplificar o gerenciamento de conformidade com centenas de painéis incorporados e relatórios relacionados a normas específicas.
- O McAfee Advanced Threat Defense é o componente de detecção de malwares avançados dessa solução.

A área restrita: McAfee Advanced Threat Defense

O McAfee Advanced Threat Defense é uma solução multicamadas de detecção de malware que combina uma ampla série de mecanismos de inspeção e recursos analíticos em uma sequência de intensidades computacionais que aumentam gradualmente e podem ser selecionadas em um menu suspenso. Essa abordagem exclusiva para uma avaliação completa e eficiente oferece um altíssimo nível de precisão na detecção e confiabilidade com um desempenho de taxa de transferência extremamente alto. A análise integrada aplicada pelo McAfee Advanced Threat Defense inclui:

- Detecção com base em assinatura de vírus, worms, spyware, bots, cavalos de Troia, estouro de buffer e ataques mistos usando uma abrangente base de conhecimento criada e mantida pelo McAfee Labs, que atualmente inclui quase 150 milhões de assinaturas.
- Detecção com base na reputação usando a rede do McAfee Global Threat Intelligence para detectar novas ameaças emergentes.
- Emulação e análise estática em tempo real para rapidamente detectar malwares e ameaças de dia zero não identificadas pelas técnicas com base em assinatura e reputação.
- Análise completa de código estático que faz engenharia reversa do código do arquivo para avaliar todos os atributos e conjuntos de instruções e analisar completamente o código-fonte sem execução. Os recursos abrangentes de desempacotamento abrem todos os tipos de arquivos empacotados e compactados para permitir a análise completa e a classificação dos malwares, ajudando as empresas a entender melhor os malwares específicos com os quais estão lidando e seu impacto na organização. A análise completa de código estático oferece informações essenciais sobre comportamentos dependentes de digitação e caminhos de execução atrasados ou ocultos que geralmente não são executados durante a análise dinâmica ou que são ignorados por soluções de área restrita menos abrangentes.

- Análise dinâmica de área restrita que executa o código do arquivo em um ambiente de tempo de execução virtual e observa o comportamento resultante. Exclusivo entre as soluções de área restrita atuais, o McAfee Advanced Threat Defense configura os ambientes de tempo de execução virtuais para refletir o host de destino com base em consultas ao software McAfee ePO. A análise do comportamento dos arquivos nas condições exatas do host-alvo produz resultados precisos com rapidez e eficiência, revelando comportamentos maliciosos que possivelmente não seriam acionados em um ambiente genérico. Como muitos ataques avançados são projetados para burlar a detecção na área restrita, o McAfee Advanced Threat Defense inclui técnicas inovadoras para garantir a execução do código durante a análise dinâmica.

Essas técnicas funcionam juntas de forma coordenada para identificar de maneira eficaz muitos tipos de malwares conhecidos e desconhecidos. A combinação da análise completa dinâmica e estática revela os malwares ocultos e avançados que não são positivamente identificados através de mecanismos de análise mais leves.

Os appliances do McAfee Advanced Threat Defense são facilmente configurados para aplicar somente as análises que ainda não foram executadas em sensores de upload do IPS, eliminando o comprometimento de desempenho decorrente de inspeções redundantes. Os appliances do McAfee Advanced Threat Defense podem ser dimensionados para capacidades de taxa de transferência de até 250 mil objetos por dia, permitindo que um único sistema contra malwares avançados dê suporte a vários sensores do McAfee Network Security Platform. Junto com o McAfee Network Security Platform, os appliances do McAfee Advanced Threat Defense são gerenciados de forma centralizada através da interface on-line oferecida pelo McAfee Network Security Manager.

Uma solução independente e eficiente para a prevenção de ameaças avançadas

A combinação do McAfee Network Security Platform e do McAfee Advanced Threat Defense oferece uma proteção de IPS de rede excepcionalmente eficiente, bem como detecção e resposta eficazes a malwares avançados. Esta é uma solução automatizada e independente que detecta ataques sofisticados, paralisa-os e corrige os sistemas host afetados sem necessidade de intervenção manual dos operadores de rede e analistas de segurança, cujo tempo é curto.
Para obter mais informações sobre como as soluções da McAfee podem proteger sua rede contra ameaças ocultas e avançadas, entre em contato com seu representante McAfee ou acesse www.mcafee.com/atd.

McAfee
An Intel Company

2821 Mission College Boulevard
Santa Clara, CA 95054
888 847 8766
www.mcafee.com

61051brf_atd-network-ips_0514_fnl_ETMG