DATA SHEET

McAfee Virtual Network Security Platform

Detecção de ameaças completa para redes na nuvem

O McAfee® Virtual Network Security Platform é uma solução completa em termos de sistema de prevenção de intrusões e ameaças a redes, construída de acordo com as necessidades específicas de nuvens públicas e privadas. Ele descobre e bloqueia ameaças sofisticadas em arquiteturas de nuvem com precisão e simplicidade, permitindo às organizações restaurar a conformidade e adotar a segurança da nuvem com confiança. Suas tecnologias avançadas incluem detecção sem assinaturas, emulação em linha, correção de vulnerabilidades com base em assinaturas e suporte para Amazon Web Services (AWS) e virtualização de redes. Com fluxos de trabalho otimizados, múltiplas opções de integração e licenciamento simplificado, as organizações podem gerenciar e expandir facilmente sua segurança nas arquiteturas de nuvem mais complexas.

Segurança de nuvem pública completa com tecnologia de segurança avançada

As nuvens públicas proporcionam conveniência, economia e a oportunidade de mudar de investimento em infraestrutura para um modelo de despesas operacionais. Elas também introduzem um novo nível de risco, no qual uma vulnerabilidade no software acessível publicamente pode permitir que um atacante penetre a nuvem e vaze informações confidenciais, ou expor acidentalmente dados de clientes para outros usuários da nuvem que utilizem o mesmo serviço.

O McAfee Virtual Network Security Platform é compatível com o AWS — serviço de nuvem pública predominante atualmente — proporcionando visibilidade completa sobre ameaças nos dados que passam por um gateway de Internet e também no tráfego lateral. Com ele, você pode restaurar a visibilidade sobre as ameaças e a conformidade de segurança em arquiteturas de nuvem pública com uma plataforma de sistema de prevenção de intrusões (IPS) que proporciona uma autêntica inspeção de tráfego lateral.

Principais vantagens

Prevenção contra ameaças avançadas incomparável

- Análise de malware avançado sem assinatura
- Proteção contra scripts entre sites e injeção de SQL
- Detecção avançada de callback de redes de bots e malware
- Proteção contra negação de serviço distribuída (DDoS) e análise comportamental
- Integração com o McAfee Advanced Threat Defense
- Distribuição de sistemas de prevenção (IPS) e de detecção de intrusões (IDS)
- Solução VMware ESX-McAfee Virtual Network Security Platform sempre ativa

Arquitetura pronta para nuvem

- Uma única licença permite o compartilhamento da capacidade de processamento em qualquer combinação de nuvens públicas e privadas

Proteção de ambientes virtualizados

As corporações estão adotando rapidamente infraestruturas de TI virtualizadas (como nuvens públicas e privadas), nas quais servidores físicos podem hospedar simultaneamente várias máquinas virtuais (VMs) e até mesmo cargas de trabalho inteiras virtualizadas. A comunicação entre máquinas virtuais resultante, juntamente com a migração, replicação e backup instantâneos dessas cargas de trabalho, contribuiu para aumentar consideravelmente o tráfego lateral dentro de nuvens públicas e privadas, bem como em SDDCs. Somando-se ao caos, a flexibilidade proporcionada pela virtualização de rede torna dinâmica e imprevisível essa escalada nos fluxos de tráfego. Para se manterem à altura do desafio, as soluções de segurança virtualizadas precisam ser flexíveis e expansíveis, e o mais importante, precisam funcionar perfeitamente com as plataformas de rede definidas por software (SDNs) que coordenam essas cargas de trabalho e máquinas virtuais de vida normalmente curta.

Promova a agilidade nas nuvens privadas

Desenvolvido para atender às exigências de proteção dos ambientes virtualizados, o McAfee Virtual Network Security Platform integra-se perfeitamente com plataformas de nuvem privada populares, como ambientes SDN baseados em VMware NSX e OpenStack. Com efeito, o McAfee Virtual Network Security Platform é a única solução específica de IPS virtual certificada para funcionar com o VMware NSX. A microssegmentação de máquinas virtuais e a inspeção profunda do tráfego lateral são mantidas automaticamente nos ambientes virtualizados, mesmo que as cargas de trabalho surjam, migrem e cessem rapidamente.

Prevenção de ameaças incomparável

O McAfee Virtual Network Security Platform baseia-se em uma arquitetura de inspeção de próxima geração desenvolvida para oferecer inspeção profunda de tráfego em redes virtuais. Ele utiliza uma combinação de tecnologias avançadas de inspeção, incluindo análise completa de protocolo, reputação de ameaças, análise comportamental e análise de malware avançado, para detectar e impedir ataques conhecidos e de dia zero à rede.

Nenhuma tecnologia de detecção de ameaças pode, isoladamente, prevenir todos os ataques. É por isso que o McAfee Virtual Network Security Platform sobrepõe vários mecanismos de detecção com e sem assinaturas para ajudar a impedir que o malware indesejável espalhe o caos pelas suas nuvens. Ele oferece várias tecnologias de inspeção, como emulação em linha de navegador, JavaScript e arquivos Adobe, detecção de callback de malware e redes de bots, detecção de DDoS com base em comportamento e proteção contra ataques avançados, como scripts entre sites e injeção de SQL. O McAfee Virtual Network Security Platform também pode identificar e bloquear os mais ocultos dos arquivos por meio de integração com o McAfee Advanced Threat Defense, no qual os arquivos são submetidos a análises comportamentais profundas. O McAfee Advanced Threat Defense combina análise detalhada e estática de código, análise dinâmica (área restrita de malware) e autoaprendizagem para aumentar a detecção de ameaças de dia zero, incluindo ameaças que usam técnicas de evasão e ransomware.

- Uma abordagem inovadora de inspeção de AWS proporciona uma autêntica proteção para tráfego lateral na nuvem pública
- O suporte para orquestração com ambientes SDN baseados em VMware NSX e OpenStack permite microssegmentação e inspeção de tráfego automatizadas entre cargas de trabalho de nuvem privada
- Dashboard compatível com máquinas virtuais e com capacidade de imposição de quarentena disponível na integração com VMware
- Console único de gerenciamento centralizado para os sensores físicos e virtuais, no local e na nuvem

Gerenciamento inteligente de segurança

- Um console único gerencia sensores no local e na nuvem
- Priorização e correlação inteligente de alertas
- Dashboards robustos de investigação de malware
- Fluxos de trabalho de investigação pré-configurados
- Gerenciamento expansível com base na Web

Simplifique com compartilhamento de licenças na nuvem

Atualmente, muitas empresas espalham sua infraestrutura e seus recursos de TI por várias nuvens e plataformas, seja para preservar a compatibilidade com aplicativos legados, para reduzir a dependência em um único fornecedor, por questão de redundância de sistemas ou para reduzir custos. O licenciamento de soluções de segurança para ambientes virtualizados pode ser complicado e caro, pois a maioria dos fornecedores exige a compra de licenças separadas para nuvens privadas e públicas e para plataformas SDN diferentes.

A McAfee simplifica o licenciamento e reduz os custos por meio do compartilhamento de licenças na nuvem, um novo conceito que permite aos clientes compartilhar sua capacidade de processamento e suas licenças do McAfee Virtual Network Security Platform por qualquer combinação de plataformas de nuvem pública e privada. O compartilhamento de licenças na nuvem também melhora a segurança ao permitir que os administradores ofereçam rapidamente proteção para tráfego lateral e microssegmentação para cargas de trabalho virtuais, onde quer que estejam, sem passar por um demorado processo de aquisição.

Simplifique análises e fluxos de trabalho

Descubra e bloqueie facilmente as ameaças mais sofisticadas. O McAfee Virtual Network Security Platform inclui análises avançadas e integrações com soluções de segurança adicionais para criar uma plataforma de detecção e resolução de ameaças amplamente abrangente e conectada.

As ameaças modernas podem gerar grandes volumes de alertas e exceder rapidamente a capacidade do operador de segurança de priorizá-los e acompanhá-los. Se os pontos não forem ligados a tempo, ameaças reais podem passar sem serem detectadas. Os fluxos de trabalho decisivos e as análises avançadas que acompanham o McAfee Virtual Network Security Platform correlacionam múltiplos alertas de IPS em um único evento decisivo, ajudando os administradores a discernir rapidamente as informações mais relevantes e decisivas em meio ao ruído.

Gerenciamento centralizado com controle em tempo real de dados em tempo real

Um único appliance do McAfee Network Security Manager oferece gerenciamento centralizado, com base na Web e facilidade de uso incomparável. O console de última geração e a interface gráfica de usuário aprimorada põem você no controle dos dados em tempo real. Você pode gerenciar, configurar e monitorar facilmente todos os appliances do McAfee Network Security Platform, virtuais ou físicos, bem como appliances do McAfee Network Threat Behavior Analysis por todos os seus recursos de nuvem pública, de nuvem privada e tradicionais, a partir de um único console. A interface de gerenciamento intuitiva com base na Web atende qualquer distribuição, de dispositivos isolados a clusters amplamente distribuídos de missão crítica. O McAfee Network Security Manager também pode ser distribuído como uma instância virtual em servidores VMware ESX e no AWS.

Visibilidade e controle

- Identificação de aplicativos
- Identificação do usuário
- Identificação de dispositivo
- Status da segurança de todas as VMs no AWS

Alta disponibilidade e recuperação de desastres

O McAfee Network Security Manager faz arbitragem entre os controladores e determina um como ativo e o outro como reserva. Quando o controlador ativo torna-se indisponível, o controlador reserva torna-se ativo. Assim, obtém-se uma alta disponibilidade (HA) de controladores em distribuições AWS, proporcionando um mecanismo de failover no qual um controlador está sempre ativo e alcançável. Além disso, um McAfee Network Security Manager reserva proporciona recuperação de desastres para ambientes AWS.

O McAfee Virtual Network Security Platform oferece alta disponibilidade com os recursos de recuperação de desastres do gerenciador (MDR), de alta disponibilidade de controladores (HA) e de redimensionamento automático do sensor de IPS virtual. Isso permite que o McAfee Virtual Network Security Platform trabalhe perfeitamente, sem interrupções. A solução MDR oferece um gerenciador secundário que assume o controle quando o gerenciador principal está fora do ar. No par de controladores HA, um dos controladores está sempre ativo e alcançável para que não haja paralisação na rede. O recurso de redimensionamento automático para sensores de IPS virtuais cria um novo sensor de IPS virtual quando uma instância do sensor fica fora do ar. Isso desempenha uma função de balanceamento de carga quando há um aumento no tráfego de rede.

Arquitetura de defesa unificada

Ataques sofisticados não respeitam limites entre produtos, aproveitando qualquer brecha na infraestrutura, especialmente entre produtos de segurança. O McAfee Virtual Network Security Platform é o único IPS a se integrar com múltiplos produtos de segurança, aproveitando dados e fluxos de trabalho para fechar essas brechas, o que resulta em maior retorno do investimento e menor custo total de propriedade. Integrações com produtos de segurança adicionais:

- **Software McAfee ePolicy Orchestrator® (McAfee ePO™):** visibilidade total de todos os alertas e eventos de IPS dos endpoints.
- **McAfee Endpoint Intelligence Agent:** combina perspectivas de rede e de endpoint para deter vazamentos de dados.
- **McAfee Enterprise Security Manager:** compartilhamento de dados ricos e quarentena de IPS para alertas de IPS.
- **McAfee Threat Intelligence Exchange:** aprendizagem compartilhada entre diversos tipos de dispositivos.
- **McAfee Global Threat Intelligence:** maior e mais ativo serviço de reputação do mundo.
- **McAfee Network Threat Behavior Analysis:** estenda a visibilidade pela rede.
- **McAfee Virtual Advanced Threat Defense**
- **McAfee Cloud Threat Detection**
- **McAfee Management for Optimized Virtual Environments (McAfee MOVE)**
- **Mecanismos de varredura de vulnerabilidades de terceiros:** análises de host e de risco para endpoints.

Recursos adicionais

Prevenção contra ameaças avançadas

- Mecanismo de emulação do McAfee Gateway Anti-Malware.
- Mecanismo de emulação de código JavaScript incorporado em arquivos PDF (área restrita leve).
- Mecanismo de análise comportamental do Adobe Flash.
- Proteção avançada contra evasão.

Proteção contra callback de malware e rede de bots

- Detecção de callback de fluxo rápido em servidores de nome de domínio (DNS)/algoritmos de geração de domínios (DGA).
- "Sinkholing" de DNS.
- Detecção heuristica de bots.
- Correlação de ataques múltiplos.
- Banco de dados de comando e controle.

Prevenção avançada de intrusões

- Desfragmentação de IP e remontagem de fluxos TCP.
- Assinaturas da McAfee, definidas pelo usuário e de código aberto.
- Quarentena de host e limitação de taxa.
- Inspeção de ambientes virtuais.
- Prevenção de negação de serviços (DoS) e DDoS.
- Detecção com base em limiares e heurística.
- Limitação de conexões com base no host.
- Detecção por autoaprendizagem e com base em perfis.

McAfee Global Threat Intelligence

- Reputação do arquivo.
- Reputação do IP.
- Acesso restrito com base em geolocalização.
- Controle de acesso com base em endereço IP.

	Tipo de sensor 1	Tipo de sensor 2	Tipo de sensor 3
Plataforma	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 KVM/OpenStack	VMware ESX 5.5/6.0/6.5 NSX 6.3 AWS
Modelo de sensor IPS virtual	IPS-VM100	IPS-VM600	IPS-VM100-VSS[1]
Tipo de distribuição de IPS virtual	Independente	Independente	Distribuída
Suporte para VMware NSX	Não	Não	Sim
Suporte para AWS	Não	Não	Sim
Número de núcleos lógicos de CPU[2]	3	4	3
Memória necessária[3]	4 GB	6 GB	5 GB
Especificações dos sensores virtuais			
Taxa de transferência máxima[4]	Até 500 Mbps	Até 1 Gbps	Até 500 Mbps
Conexões simultâneas	200.000	600.000	200.000
Conexões estabelecidas por segundo	6.000	20.000	6.000
Fluxos UDP suportados	39.168	254.208	39.168
Número de pares de portas de monitoramento	2	3	1[5]
Interfaces virtuais (VIDS) por sensor	32	100	32
Perfis de DoS	100	300	100
Porta de gerenciamento	Sim	Sim	Sim
Porta de resposta	Sim	Sim	Não
Modos de distribuição	Inspeção entre VMs, inspeção físico para VM, inspeção físico para físico, inspeção de porta SPAN		Inspeção em linha de VMware NSX

1. Para uso somente em ambientes VMware NSX como um serviço inserido.
2. Os requisitos dos recursos de VM podem variar dependendo da versão. Consulte a documentação específica da versão.
3. Ibid.
4. Medida com pacotes UDP de 1.518 bytes sob condições de teste ideais.
5. Representação virtual de entrada e saída. A inspeção está intimamente vinculada ao VMware NSX na camada de kernel.

McAfee
Together is power.

Av. Nações Unidas, 8.501 – 16º andar
Pinheiros – São Paulo – SP
CEP 05425-070, Brasil
+(11) 3711-8200
www.mcafee.com/br