



McAfee Virtual Network Security Platform

Detecção de ameaças completa para redes na nuvem

Principais vantagens

- Prevenção contra ameaças avançadas incomparável
- Análise de malware avançado sem assinatura
- Emulação em linha de navegador e JavaScript
- Detecção avançada de callback de malware e redes de bots
- Proteção DDoS e análise baseada no comportamento
- Integração com o McAfee Advanced Threat Defense

Arquitetura pronta para nuvem

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

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, bem como de centros de dados definidos por software (SDDCs). 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 serviço de nuvem pública predominante atualmente, o AWS, proporcionando total visibilidade sobre os dados que passam por um gateway de Internet e também sobre o tráfego lateral. Com isso, você pode restaurar a visibilidade sobre as ameaças e a conformidade de segurança em arquiteturas de nuvem pública com uma plataforma de IPS que proporciona uma autêntica inspeção de tráfego lateral.

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.

Arquitetura de defesa unificada

Ataques sofisticados não respeitam limites entre produtos, aproveitando qualquer brecha na infraestrutura, especialmente entre produtos de segurança. O McAfee 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
- 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 — para estender a visibilidade sobre a rede
- Mecanismos de varredura de vulnerabilidades de terceiros — análises de host e de risco para endpoints

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 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.

Simplifique com compartilhamento em 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 Intel® Security simplifica o licenciamento e reduz os custos por meio do compartilhamento em 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 em nuvem também melhora a segurança ao permitir que os administradores ofereçam rapidamente proteção para tráfego lateral e microssegmentação para cargas 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 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, 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.

Recursos adicionais

Prevenção contra ameaças avançadas

- Mecanismo de emulação do McAfee Gateway Anti-Malware.
- Mecanismo de emulação do JavaScript de 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 DNS/DGA.
- “Sinkholing” de DNS.
- Detecção heurística 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 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.

Gerenciamento inteligente da segurança

- 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

Visibilidade e controle

- Identificação de aplicativos
- Identificação do usuário
- Identificação de dispositivo

	IPS-VM100	IPS-VM600	IPS-VM100-VSS ¹
Plataforma	VMware ESX 5.5	VMware ESX 5.5	VMware ESX 5.5
	VMware ESX 6.0	VMware ESX 6.0	VMware ESXi 6.0/NSX 6.2.4
	KVM/OpenStack	KVM/OpenStack	
	AWS		
Suporte para NSX	Não	Não	Sim
Número de núcleos lógicos ²	3	4	3
Memória necessária ³	4 GB	6 GB	5 GB
Especificações dos sensores virtuais			
Taxa de transferência máxima ⁴	Até 1 Gbps	Até 2 Gbps	Até 600 Mbps
Conexões simultâneas	200.000	600.000	200.000
Conexões estabelecidas por segundo	6.000	20.000	6.000
Fluxos UDP suportados	39.000	254.000	39.000
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 para NSX

1. Para uso somente em ambientes NSX como um serviço inserido.

2. Os requisitos de 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 NSX na camada de kernel.

