

McAfee Management for Optimized Virtual Environments AntiVirus

Segurança para a sua nuvem privada sem sacrificar o desempenho

Os antivírus convencionais não funcionam bem na infraestrutura virtualizada. O McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) proporciona uma proteção avançada e otimizada contra malware em seus computadores desktop e servidores virtualizados. Implemente em múltiplos hipervisores ou escolha uma opção ajustada e sem agente para VMware NSX ou VMware vCNS. De uma forma ou de outra, você recebe uma segurança de ponta, para detecção e contenção instantânea de ameaças com o mínimo de impacto sobre o desempenho das máquinas virtuais (VMs). O McAfee MOVE AntiVirus otimiza a proteção antimalware de distribuições virtualizadas, liberando recursos do hipervisor ao mesmo tempo que garante que varreduras de segurança atualizadas sejam realizadas de acordo com as políticas.

Controle otimizado de varredura

A natureza dinâmica dos computadores desktop visitantes e servidores virtuais exige um tratamento cuidadoso. As imagens precisam estar livres de malware quando os usuários iniciam uma sessão. Isso pode ser desafiador porque frequentemente os usuários começam a trabalhar em grupos, causando “transtornos de antivírus” com picos de demanda que consomem recursos e impedem os usuários de obter uma sessão.

Para eliminar atrasos e gargalos de varredura, o McAfee MOVE AntiVirus transfere as operações de varredura, configuração e de atualização de arquivos .DAT das imagens visitantes individuais para um servidor de varredura separado. Desenvolvemos e mantemos um cache global de arquivos examinados para garantir que, quando um arquivo for examinado e confirmado como limpo, as próximas máquinas virtuais que o acessarem não precisarão esperar por uma varredura. Assim, menos recursos de memória são alocados para cada máquina virtual e é possível liberá-los de volta ao pool de recursos para que sejam utilizados de forma mais eficaz.

Principais vantagens

- **Transfere a responsabilidade pela varredura de malware:** proteção instantânea com baixo impacto sobre a memória e o processamento
- **Previne transtornos de antivírus:** inclui as opções de varredura sob solicitação e ao acessar
- **Permite uma distribuição flexível:** multiplataforma (máquinas virtuais Windows e todos os principais hipervisores) ou sem agente (máquinas virtuais VMware, Windows e Linux)
- **Otimização de recursos aprimorada:** provisionamento elástico de mecanismos de varredura off-line com notificações de eventos (multiplataforma)
- **Bloqueia ameaças de dia zero e desconhecidas em questão de segundos:** inteligência de reputação local combinada com análise comportamental em uma área restrita (multiplataforma; módulo adicional vendido separadamente)

DATA SHEET

O McAfee MOVE AntiVirus permite políticas separadas para varreduras ao acessar e solicitadas, possibilitando uma execução bem aprimorada da segurança. Por exemplo, os administradores podem assumir um nível razoável de risco em varreduras ao acessar e em tempo real para evitar degradação do desempenho e, em seguida, utilizar varreduras solicitadas com políticas mais rígidas para serem executadas posteriormente, quando o impacto for menor.

Visibilidade completa, de ponta a ponta, em todas as nuvens

A falta de visibilidade dificulta a implementação de políticas de segurança adequadas a ambientes virtualizados. O McAfee Cloud Workload Discovery para nuvem privada, que abrange VMware e OpenStack, proporciona uma visão completa de data centers virtuais e insere propriedades fundamentais, como servidores, hipervisores e máquinas virtuais, no console do McAfee ePO. Assim que os administradores obtêm visibilidade sobre o status de segurança de todas as máquinas virtuais e podem monitorar os relacionamentos entre hipervisor e máquina virtual quase em tempo real, a proteção do seu data center virtual torna-se muito mais fácil. Um dashboard personalizável exibe o status das varreduras de segurança, resumos executivos e dados históricos de segurança sobre os ativos.

O McAfee Server Security Suite Essentials e o McAfee Server Security Suite Advanced levam visibilidade e controle a servidores físicos e nuvens públicas Amazon Web Services (AWS) e Microsoft Azure.

Gerenciamento detalhado de políticas

O conhecido console do McAfee ePO permite configurar políticas e controles para o McAfee MOVE AntiVirus. Você pode complementar os dados virtuais com dados dos seus sistemas físicos e nuvens públicas para proporcionar relatórios e dashboards unificados. Os administradores podem configurar uma política exclusiva por máquina virtual, cluster ou data center por meio do McAfee Cloud Workload Discovery, adaptando a segurança especificamente à configuração do data center.

Recursos adicionais do McAfee MOVE AntiVirus

Gerenciamento e visibilidade:

- Programe instantaneamente uma varredura por solicitação em uma máquina virtual ou grupo de máquinas virtuais.
- Aumente a precisão utilizando varreduras direcionadas sob solicitação.
- Distribua automaticamente um mecanismo de varredura separado em cada hipervisor por meio de integração com o VMware NSX Service Composer.
- Fique a par dos problemas utilizando dashboards, relatórios e alertas de e-mail.

Distribuição e configuração simplificadas:

- Distribua e configure um mecanismo de varredura separado em vários hipervisores (sem agente).
- Restaure, com o console do McAfee ePO, arquivos colocados em quarentena (multiplataforma).

Principais vantagens (continuação)

- **Aproveita o console do McAfee® ePolicy Orchestrator® (McAfee ePO™):** controle e visibilidade total em distribuições físicas, virtuais e de nuvem

Configurações do McAfee MOVE AntiVirus

McAfee MOVE AntiVirus for Virtual Servers

- McAfee MOVE AntiVirus:
 - Distribuição multiplataforma
 - Distribuição sem agentes
- Cloud Workload Discovery para nuvem privada (VMware e OpenStack)
- Software McAfee ePO

McAfee MOVE AntiVirus for Virtual Desktops

- McAfee MOVE AntiVirus:
 - Distribuição multiplataforma
 - Distribuição sem agentes
- Cloud Workload Discovery para nuvem privada, abrangendo VMware e OpenStack
- McAfee Host Intrusion Prevention System
- McAfee SiteAdvisor® Enterprise
- Proteção de memória e proteção de aplicativos da Web
- Software McAfee ePO

DATA SHEET

- Diagnósticos aprimorados para ajuste do desempenho do antivírus.
- Gerenciamento simplificado de políticas, sem agente e multiplataforma.

Opção sem agente para VMware

O McAfee MOVE AntiVirus aproveita o VMware NSX ou o VMware vCNS para uma eficiência maior. Em distribuições sem agentes, eles utilizam o hipervisor como uma conexão de alta velocidade para que a máquina virtual de segurança (SVM) do McAfee MOVE AntiVirus faça varredura de máquinas virtuais de fora da imagem visitante. Ao efetuar a varredura, a SVM instrui o VMware NSX ou o VMware vCNS a armazenar em cache os arquivos bons e a excluir, negar acesso ou colocar em quarentena os arquivos maliciosos.

Após você instalar e configurar o SVM e os componentes VMware NSX ou VMware vCNS em servidores VMware ESX, bem como instalar o driver de endpoint VMware NSX ou VMware vCNS nas máquinas virtuais hóspedes, cada imagem é protegida automaticamente sem a instalação do software McAfee em cada máquina virtual cliente. Nossa implementação compatível com o vMotion possibilita que as suas máquinas virtuais migrem de um host para outro e continuem a ser protegidas pela SVM no host de destino, sem afetar as varreduras ou a experiência do usuário.

A integração dos produtos McAfee com o VMware vCNS permite monitorar o status da SVM no VMware vCenter e receber alertas caso a SVM perca a conectividade. O console do McAfee ePO recebe dados de eventos com os detalhes da máquina virtual específica afetada no caso de uma máquina virtual estar infectada. Uma integração profunda com o VMware NSX sincroniza as políticas criadas no console do McAfee ePO e as regras atribuídas no VMware NSX. A marcação de máquinas vulneráveis sem proteção antimalware ou de máquinas com malware possibilita colocar as máquinas virtuais imediatamente em quarentena por meio do firewall VMware NSX.

A distribuição do McAfee MOVE AntiVirus sem agente com o VMware vCNS e o VMware NSX tem suporte simultâneo, o que torna extremamente fácil e simples para os usuários do VMware vCNS fazer a transição para o VMware NSX.

Multiplataforma para todos os principais hipervisores

Em instalações multiplataforma, incluindo vSphere, Hyper-V, KVM e XenServer, o agente do McAfee MOVE AntiVirus — um componente leve de endpoint — comunica-se com a SVM para negociar o processamento do antivírus em nome de cada máquina virtual. O agente do McAfee MOVE AntiVirus mantém um cache local e gerencia políticas e funções de varredura. É possível designar e efetuar varredura de uma imagem de referência, que será utilizada como imagem principal limpa. O preenchimento prévio do cache local com imagens limpas proporciona a inicialização mais rápida possível da máquina virtual.

DATA SHEET

Quando um arquivo é acessado, o McAfee MOVE Offload Scan Server realiza uma varredura ao acessar, dando uma resposta à máquina virtual. Os usuários são notificados sobre problemas por meio de um alerta pop-up e podem, então, colocar os arquivos maliciosos em quarentena, negar acesso a eles ou excluí-los.

Como as exigências de varredura variam em distribuições multiplataforma, SVMs podem ser adicionadas ou removidas automaticamente do pool de recursos para adequar a sua capacidade, para um dimensionamento ilimitado e uma utilização eficiente dos recursos. Notificações de eventos ajudam os administradores a compreender as tendências de utilização de SVMs para otimizar o gerenciamento de recursos.

O McAfee MOVE AntiVirus em distribuições multiplataforma pode complementar a inteligência de reputação global do McAfee Global Threat Intelligence (McAfee GTI) com dados locais do McAfee Threat Intelligence Exchange, um módulo adicional vendido separadamente, para identificar e combater instantaneamente a quantidade sempre crescente de

amostras de malware exclusivas. Ao utilizar o McAfee Threat Intelligence Exchange, o McAfee MOVE AntiVirus coordena-se com o McAfee Advanced Threat Defense para analisar dinamicamente o comportamento de aplicativos desconhecidos em uma área restrita e imuniza automaticamente todos os endpoints contra o malware recém-detectado. A integração do McAfee MOVE AntiVirus com o McAfee Network Security Platform por meio do McAfee Threat Intelligence Exchange constitui uma abordagem de segurança em camadas que proporciona proteção para máquinas virtuais e perímetro unificado.

Gerenciamento unificado de políticas sem agente e multiplataforma

Muitas organizações desejam aproveitar o suporte do McAfee MOVE AntiVirus para ambas as distribuições sem agente e multiplataforma. O McAfee MOVE AntiVirus oferece aos administradores de segurança a capacidade de definir e gerenciar políticas de segurança consistentes utilizando um ponto de extensão no console do McAfee ePO para que o gerenciamento desses métodos diferentes seja simples e fácil.

DATA SHEET

Arquitetura	Distribuição multiplataforma	Distribuição sem agentes
Compatibilidade com hipervisores/plataformas	Todos os principais hipervisores, incluindo VMware, Citrix, Hyper-V e KVM	VMware
Plataforma de varredura	Windows 2008, Windows 2012 R2 e Windows Server 2016	Linux Ubuntu 16.04
Expansibilidade da distribuição	Uma SVM pode proteger máquinas virtuais de vários hipervisores. As SVMs podem ser provisionadas elasticamente.	Uma SVM por host ESX
Comunicação com máquinas virtuais	Pela rede	Pelo hipervisor
Proteção de máquinas virtuais	Windows	Windows e Linux

Saiba mais

As soluções da McAfee proporcionam a segurança necessária e a flexibilidade que você merece.

Saiba mais em www.mcafee.com/br/products/move-anti-virus.aspx.



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

McAfee e o logotipo da McAfee, ePolicy Orchestrator, McAfee ePO e SiteAdvisor são marcas comerciais ou marcas registradas da McAfee, LLC ou de suas afiliadas nos EUA e em outros países. Outros nomes e marcas podem ser propriedade de terceiros. Copyright © 2017 McAfee, LLC. 2721_0317
MARÇO DE 2017