DATA SHEET

McAfee Security Suite for Virtual Desktop Infrastructure

A segurança de que você necessita, com o mínimo de impacto sobre o desempenho

A adoção de desktops virtuais já está acontecendo, mas é necessário incorporar uma segurança de desktop mais forte na solução para que ela proteja os seus negócios sem causar problemas de desempenho ou afetar a densidade de servidores desejada. Os antivírus convencionais não funcionam bem dentro de uma infraestrutura virtualizada. A resposta? O McAfee® Security Suite for Virtual Desktop Infrastructure (VDI), que proporciona uma segurança abrangente e otimizada para desktops virtuais.

O McAfee Security Suite for VDI oferece uma proteção antimalware otimizada para virtualização, lista branca para proteção contra ameaças de dia zero, proteção contra intrusões no desktop e proteção de dados. Ele também adverte os usuários quanto a sites maliciosos e/ou os bloqueia.

Arquitetura de varredura otimizada

A natureza dinâmica dos desktops virtuais requer cuidado em sua utilização. As imagens devem estar livres de malware quando estiverem off-line ou serem submetidas a uma varredura assim que os usuários iniciarem uma sessão. O antimalware não é o único serviço inicializado e, frequentemente, os usuários começam a trabalhar em grupos, o que causa "transtornos de antivírus" com pico na demanda que consomem todos os recursos e impedem os usuários de obter uma sessão.

Para eliminar atrasos e gargalos de varredura, o McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) transfere as operações de varredura, configuração e atualização de DAT das imagens visitantes individuais para um servidor de varredura/appliance virtual blindado. 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 (VM, Virtual Machine) que o acessarem não precisarão esperar pela 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. Esse agendamento inteligente de varreduras por solicitação assegura que as varreduras não interfiram com o desempenho do hipervisor.

Principais vantagens

- Oferece descoberta e visibilidade com o software McAfee ePO e o Cloud Workload Discovery
- Proporciona uma combinação exclusiva de lista negra e lista branca para proteger desktops virtuais contra malware
- Otimiza a segurança da virtualização para o mínimo de impacto sobre o desempenho
- Acrescenta proteção contra intrusões e Web com proteção de memória e proteção contra aplicativos de Web
- Aproveita o software McAfee ePO para proporcionar visibilidade, controle e relatórios instantâneos de endpoints
- Viabiliza uma distribuição flexível, sem agentes e multiplataforma
- Permite um provisionamento elástico de mecanismos de varredura off-line para se expandir conforme a demanda (multiplataforma)
- Integra-se com inteligência de reputação local para uma resposta mais rápida às ameaças (multiplataforma)

Gerenciamento detalhado de políticas

O console do McAfee® ePolicy Orchestrator® (McAfee ePO™) oferece a capacidade de configurar políticas e controles para o McAfee MOVE AntiVirus. É possível acumular os dados dos computadores desktop virtuais com os de outros sistemas em relatórios e dashboards unificados. Os administradores podem configurar uma política exclusiva por máquina virtual, pool de recursos ou data center com o Cloud Workload Discovery para nuvem privada, adaptando suas necessidades de segurança especificamente à composição do data center.

Distribuição sem agentes 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 excluir, negar acesso ou colocar em quarentena os arquivos maliciosos.

Após você instalar e configurar o VMware 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 de nosso software 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 do McAfee MOVE AntiVirus com o vCNS permite monitorar o status da SVM no VMware vCenter e receber alertas caso a SVM perca a conectividade. O software McAfee ePO recebe os dados de eventos com os detalhes da máquina virtual específica afetada no caso de uma máquina virtual estar infectada. Uma integração profunda com o NSX sincroniza as políticas criadas no software 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.

Multiplataforma para todos os hipervisores

Em instalações multiplataforma, o agente do McAfee MOVE AntiVirus — um componente leve de endpoint — se comunica com o servidor de varredura (McAfee MOVE Offload Scan Server) para negociar o processamento do antivírus em nome de cada desktop virtual. Um agente do software McAfee ePO gerencia as políticas e as varreduras. Também é possível designar e efetuar varredura de uma imagem de referência a ser utilizada como imagem principal limpa. Como resultado, um administrador pode preencher previamente caches globais com imagens limpas para ajudar a acelerar a inicialização dos desktops virtuais.

Quando o usuário acessa um arquivo, o McAfee MOVE Offload Scan Server realiza uma varredura ao acessar, dando uma resposta à máquina virtual. Os usuários

Configuração do McAfee Security Suite for VDI

- McAfee MOVE AntiVirus
  - Distribuição multiplataforma
  - Distribuição sem agentes
- Cloud Workload Discovery para nuvem privada (VMware e OpenStack)
- McAfee VirusScan® Enterprise for Windows
- McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention for Desktops
- McAfee Application Control for Desktops
- Tecnologia McAfee SiteAdvisor® Enterprise
- McAfee ePolicy Orchestrator

podem ser notificados sobre problemas por meio de um alerta pop-up, e é possível colocar os arquivos em quarentena para aguardar uma decisão. É possível configurar cada desktop virtual com políticas exclusivas e individuais definidas no console do McAfee ePO. Os desktops virtuais podem, ainda, ser gerenciados como um grupo.

Conforme as cargas de trabalho aumentam ou diminuem em distribuições multiplataforma, SVMs podem ser adicionadas ou removidas automaticamente do pool de recursos para adequar a sua capacidade, resultando em dimensionamento ilimitado e 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 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. Usando 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 (sandbox). Ele imuniza automaticamente todos os desktops virtuais contra o malware recém-detectado.

Recurso	Por que você precisa dele
Segurança de virtualização	▪ Melhora a segurança de cargas de trabalho distribuídas em infraestruturas de desktop virtual sem comprometer o desempenho e a utilização dos recursos. ▪ A distribuição sem agentes otimizada para o VMware ajuda a proporcionar excelentes desempenho e densidade de máquinas virtuais. Não há necessidade de instalar/atualizar nossos agentes em cada desktop virtual — isso reduz a complexidade e facilita bastante o uso. ▪ A distribuição multiplataforma para todos os hipervisores viabiliza um provisionamento elástico dos mecanismos de varredura off-line conforme a demanda, integrando-se com inteligência de reputação local para uma resposta mais rápida às ameaças.
Proteção básica de endpoints	▪ A proteção antivírus da McAfee faz varreduras mais rápidas, usa menos memória, exige menos ciclos de CPU e protege melhor do que outros produtos. ▪ A prevenção de intrusões no host protege sua empresa contra ameaças complexas à segurança que poderiam ser introduzidas ou permitidas acidentalmente. ▪ O McAfee SiteAdvisor® Enterprise impede que os usuários interajam com sites perigosos e permite a personalização de políticas para restringir o acesso a sites potencialmente nocivos, assegurando com isso a conformidade com políticas.

Recurso	Por que você precisa dele
Listas brancas (whitelists) de aplicativos	▪ Impacto significativamente menor sobre o desempenho do host em relação aos controles tradicionais de segurança de endpoint. ▪ Proteção contra ameaças persistentes avançadas (APTs) e de dia zero sem atualizações de assinaturas, resultando em uma proteção mais rápida. ▪ Listas brancas dinâmicas impõem uma sobrecarga operacional menor em comparação com técnicas de lista branca tradicionais.
Cloud Workload Discovery	▪ Total visibilidade sobre cargas de trabalho em nuvem privada e suas plataformas subjacentes para identificar controles de segurança deficientes.
Proteção de arquivos e mídias removíveis (criptografia)	▪ A criptografia torna-se excepcionalmente mais fácil e menos arriscada de distribuir com proteção de arquivos e mídias removíveis. ▪ Desempenho praticamente nativo em hosts criptografados através de uma implementação otimizada da tecnologia Intel® AES-NI. ▪ Oferece criptografia de mídias removíveis (unidades USB, CDs, DVDs) e de arquivos/pastas, transparente, automática e com base em políticas. ▪ Permite que os usuários criptografem mídias USB removíveis e transfiram informações de uma maneira segura. ▪ Permite acesso seguro a dados em compartilhamentos de rede.
Gerenciamento centralizado com o software McAfee ePO	▪ Gerencie distribuições físicas, virtuais e de nuvem de maneira centralizada para um melhor controle da segurança, incluindo gerenciamento de políticas, distribuição, visibilidade e gerenciamento de segurança em todas as plataformas. ▪ Simplifica processos operacionais e reduz o investimento de tempo para a equipe administrativa. ▪ Reduz os custos de hardware devido à menor exigência de servidores.

Saiba mais

As soluções da McAfee proporcionam a segurança necessária com o mínimo de impacto sobre o desempenho. Visite **www.mcafee.com/br/products/data-center-security-suite-for-vdi.aspx**.

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