McAfee Security Suite for Virtual Desktop Infrastructure

A segurança necessária e a flexibilidade que você merece

A adoção de desktops virtuais (VDIs) já está acontecendo, mas é preciso integrar uma forte segurança de desktop à solução para que ela proteja os seus negócios sem causar problemas de desempenho ou afetar a densidade de servidor desejada. Os antivírus convencionais não funcionam bem dentro de uma infraestrutura virtualizada. A resposta? McAfee® Security Suite for VDI, que oferece uma segurança abrangente e otimizada para desktops virtuais.

Principais vantagens

- Descoberta e visibilidade para ambientes VMware vSphere com o software McAfee ePO e o McAfee Data Center Connector for VMware vSphere. A combinação exclusiva de lista negra e lista branca protege servidores físicos e virtuais contra malware
- Segurança de virtualização otimizada para mínimo impacto sobre o desempenho
- Proteção contra ameaças desconhecidas impedindo a execução de aplicativos indesejados nos seus desktops virtuais
- Proteção na Web e contra intrusões, juntamente com firewall de desktop, proteção de memória e proteção contra aplicativos da Web
- Aproveitamento do software McAfee ePO para obter visibilidade, controle e relatórios instantâneos sobre terminais

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 sobre sites maliciosos e/ou os impede de acessá-los.

Arquitetura de varredura otimizada

A natureza dinâmica dos desktops virtuais requer cuidado em sua utilização. É possível manter as imagens sem malware enquanto estão off-line ou efetuar uma varredura das imagens 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 (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 garante que estas não afetem o desempenho do hipervisor.

Gerenciamento detalhado de políticas

O console do software McAfee® ePolicy Orchestrator® (McAfee ePO™) permite configurar políticas e controles para o comportamento do 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, cluster ou data center por meio do McAfee Data Center Connector, adaptando suas necessidades de segurança especificamente para a configuração do data center.

intel Security

Configuração do McAfee Security Suite for VDI

McAfee MOVE AntiVirus for Virtual Desktops (VDI).

- McAfee MOVE AntiVirus
  - Distribuição de múltiplos hipervisores
  - Distribuição sem agentes
- McAfee Data Center Connector for vSphere
- Software McAfee VirusScan® Enterprise for Windows
- Software McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention System
- McAfee Application Control for Desktops
- Tecnologia McAfee SiteAdvisor® Enterprise
- Software McAfee ePolicy Orchestrator

A distribuição sem agentes aproveita o VMware vShield para aumentar a eficiência

Em distribuições sem agentes, o VMware vShield Endpoint utiliza o hipervisor como uma conexão de alta velocidade para permitir que o McAfee MOVE AntiVirus Security Virtual Appliance (SVA) efetue varredura em máquinas virtuais de fora da imagem visitante. Ao efetuar a varredura, o SVA vai direcionar o vShield para armazenar em cache os arquivos bons e excluir ou negar acesso aos arquivos maliciosos ou colocá-los em quarentena.

Após a instalação e a configuração do SVA e dos componentes do vShield necessários nos servidores ESX, juntamente com a instalação do driver do vShield em máquinas virtuais visitantes, todas as imagens estarão automaticamente protegidas no momento da criação. Não há nenhuma exigência para instalação do software da McAfee em cada máquina virtual cliente. Nossa implementação compatível com o vMotion possibilita que as máquinas virtuais migrem de um host para outro e continuem a ser protegidas pelo SVA no host de destino, sem afetar as varreduras ou a experiência do usuário. A integração da McAfee permite monitorar o status do SVA no vCenter e receber alertas caso o SVA 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.

Múltiplos hipervisores para padrões e conforto

Em instalações de múltiplos hipervisores, o agente do McAfee MOVE AntiVirus — um componente leve de terminal — se comunica com o servidor de varredura (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 funções de varredura. 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 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 software McAfee ePO. Os desktops virtuais podem, ainda, ser gerenciados como um grupo.

Saiba mais

As soluções da McAfee proporcionam a segurança necessária e a flexibilidade que você merece. Visite **www.mcafee.com/br/products/data-center-security-suite-for-vdi.aspx**.

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. • Opções de distribuição sem agentes e com múltiplos hipervisores: distribuição para ambientes de virtualização de vários fornecedores (VMware, Citrix, Hyper-V). • A distribuição sem agentes otimizada para o VMware ajuda a otimizar a densidade de máquinas virtuais e o desempenho. Não há necessidade de instalar/atualizar agentes da McAfee em cada desktop virtual — isso reduz a complexidade e facilita bastante o uso.
Proteção básica de terminais	• Proteção antivírus para servidores físicos considerada a melhor pelo NSS Labs contra explorações de dia zero e ataques de evasão. • 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.
Listas brancas (whitelists) de aplicativos	• Reduz significativamente o impacto sobre o desempenho do host em comparação com controles tradicionais de segurança de terminais. • Protege contra ameaças persistentes avançadas (APTs) e ataques de dia zero sem atualizações de assinaturas, o que resulta em uma proteção mais rápida. • Listas brancas dinâmicas impõem uma sobrecarga operacional menor em comparação com técnicas de lista branca tradicionais.
Visibilidade completa sobre máquinas virtuais na nuvem privada	• Descobre automaticamente máquinas virtuais na nuvem privada (VMware vSphere).
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 e transfiram informações de uma maneira segura. • Permite acesso seguro a dados de compartilhamentos de rede.
Gerenciamento centralizado com o software McAfee ePO	• Capacidade de gerenciamento de painel único para máquinas físicas e virtuais, incluindo aquelas nas nuvens pública e privada para maior visibilidade sobre a segurança. • Simplifica processos operacionais e reduz o investimento de tempo para a equipe administrativa. • Reduz os custos de hardware devido à menor exigência de servidores.

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070, São Paulo - SP, Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com