

McAfee Enterecept Desktop Agent

Prevenção de invasões para notebooks e desktops

O Desafio

Sozinhos, os produtos antivírus tradicionais não conseguem garantir a disponibilidade, a integridade e o sigilo de sistemas portáteis e desktops. Esses sistemas contêm os mesmos dados reservados ou regulamentados encontrados em servidores de grande porte e, mesmo assim, muitas vezes não contam com a proteção de ferramentas corporativas de segurança tais como firewalls e sistemas de prevenção de invasão de redes, deixando portas abertas para exploração de falhas de segurança.

As empresas precisam defender seus sistemas mais vulneráveis com medidas avançadas e preventivas contra ameaças e ataques que exploram vulnerabilidades.

Os produtos antivírus tradicionais são reativos e não fazem nada para bloquear ataques desconhecidos que utilizam vulnerabilidades recém-descobertas. Além disso, as empresas, independentemente do seu porte, estão sofrendo intensas pressões legais para garantir a privacidade de dados confidenciais e controlar o acesso a sistemas e aplicativos. Para proteger de maneira ampla e preventiva sistemas portáteis e desktops, as empresas precisam implementar uma prevenção de nível profissional contra invasões.

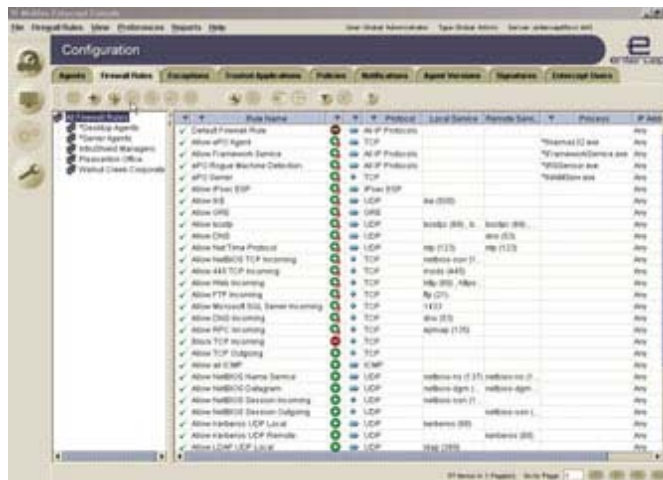
O McAfee® Enterecept® é a solução de prevenção contra invasões mais precisa e flexível para desktops e sistemas portáteis do mercado, permitindo que as empresas reduzam os riscos, garantam a disponibilidade dos negócios e reduzam seu custo total de propriedade.

A solução McAfee Enterecept para notebooks e desktops

Os agentes do McAfee Enterecept protegem sistemas portáteis e desktops contra ataques conhecidos e desconhecidos com a mesma tecnologia patenteada e premiada disponível nos agentes Enterecept para servidor. Os agentes Enterecept para desktop contam com regras de comportamento desenvolvidas especificamente para proteger os aplicativos de desktop mais explorados, tais como o Microsoft® Internet Explorer e o Outlook contra explorações desconhecidas, sem qualquer atualização.

Cada agente gerenciado de maneira centralizada utiliza uma combinação exclusiva de três tecnologias de prevenção de invasões para bloquear ataques contra aplicativos e serviços de desktop, com precisão inigualável:

- Regras de comportamento protegem contra ataques desconhecidos dirigidos a novas vulnerabilidades ou explorações para as quais ainda não há nenhum patch, reduzindo a urgência da distribuição de patches.
- Assinaturas protegem o host, identificando com precisão conteúdos hostis conhecidos nos dados, além de bloquear pacotes com tráfego malicioso antes que elas sejam processadas, reduzindo consideravelmente os falsos positivos.
- O Firewall de Sistema protege aplicativos e dados, bloqueando o tráfego que entra ou sai do sistema, de acordo com o endereço IP, o protocolo ou a porta.



O Enterecept é completamente invisível para o usuário final, com políticas individualizadas e personalizáveis controladas por administradores.

Benefícios

Abrangente

- Bloqueia ataques desconhecidos sem atualizações
- Reduz consideravelmente a criticidade da distribuição de patches contra novas ameaças
- Protege a disponibilidade, a integridade e o sigilo de dados e sistemas
- A prevenção de invasões aliada à proteção por firewall protege sistemas portáteis e desktops contra ataques

Preciso

- O Trusted Applications permite que as empresas eliminem os falsos positivos de aplicativos essenciais
- Os arquivos de características reduzem significativamente o número de falsos positivos e geram descrições exatas e detalhadas das ocorrências
- Políticas personalizáveis permitem a adaptação a qualquer ambiente

Flexível

- Gerencia até 10 mil agentes com um único gerenciador
- Gerenciamento opcional pelo McAfee ePolicy Orchestrator® 3.5
- A instalação e as atualizações imperceptíveis sem reinicialização ou intervenção do usuário final eliminam a possibilidade de violação de políticas
- A reação automática a ocorrências de segurança e a ausência de uma interface local para o usuário impedem que os usuários finais permitam violações acidentalmente

Prevenção de invasões para notebooks e desktops

Como funciona o McAfee Enterecept

Cada agente Enterecept vem com modelos predefinidos de políticas totalmente configurados, oferecendo proteção sem necessidade de outras configurações. Os agentes também possuem poderosos recursos de personalização que permitem aos profissionais de segurança criar e ajustar políticas específicas para seus ambientes e reduzir o número de falsos positivos.

O agente examina chamadas específicas ao sistema e chamadas à API (ambas usadas por todos os aplicativos para solicitar serviços do sistema operacional). Ele compara de maneira rápida e eficiente suas regras de comportamento e características de ataques conhecidos com várias informações sobre cada chamada (por exemplo, o processo que fez a chamada, o contexto de segurança no qual o processo é executado, o recurso acessado, etc.). Então, o agente bloqueia todas as chamadas de comportamentos ou programas mal-intencionados.

Os agentes acessam automaticamente atualizações criptografadas e autenticadas no sistema de gerenciamento, garantindo que cada um deles tenha as políticas e as características de ataques mais recentes.



O Enterecept garante a disponibilidade, a integridade e o sigilo de sistemas portáteis e desktops.

Recursos

Prevenção de Ataques Desconhecidos — O Enterecept evita ataques novos e nunca vistos, por meio das suas poderosas regras de comportamento que não precisam de atualização para bloquear os ataques desconhecidos. Essa abordagem comportamental fiscaliza o comportamento correto do SO e dos aplicativos, além de bloquear novos ataques que violam políticas.

Prevenção da Exploração de “Buffer Overflow” — Uma tecnologia patenteada impede a execução de programas como resultado de um “Buffer Overflow”, que é a maior fonte de vulnerabilidades de segurança de sistemas.

Prevenção de Ataques Conhecidos — Detecta e bloqueia explorações conhecidas e impede que sejam causados danos aos sistemas, comparando a atividade com o seu amplo banco de dados de ataques conhecidos, automaticamente atualizado, além de apresentar uma análise pericial detalhada.

Firewall de Sistema — Bloqueia o tráfego que entra e sai do sistema, por meio de um filtro de pacotes altamente individualizado e do firewall. Ele pode bloquear o tráfego que entra e sai do sistema, de acordo com a porta, o protocolo e o endereço IP.

Proteção de Recursos — Protege os sistemas contra comprometimentos, bloqueando seus recursos essenciais (arquivos, configurações, chaves de registro, serviços, etc.), impedindo até mesmo que usuários com direitos administrativos ignorem as políticas de segurança.

Invisível para os Usuários Finais — Os agentes são completamente invisíveis para os usuários finais, não exigindo nenhuma interação durante a instalação, as atualizações ou para reagir a ocorrências de segurança.

Controle Local de Acesso — Bloqueie o acesso a unidades de memória USB, unidades de disquete, etc.

Blindagem/Envolvimento de Aplicativos — A blindagem impede a invasão e o uso inadequado dos recursos do Internet Explorer e do Microsoft Outlook (arquivos, usuários, registro, etc.). O envolvimento impede que esses aplicativos realizem atividades mal-intencionadas fora do seu comportamento normal (por exemplo, acessar dados de outros aplicativos).

Políticas Ágeis de Prevenção Passo a Passo Prontas para Uso — Um console intuitivo de gerenciamento permite que as empresas transfiram agentes por meio de níveis cada vez mais altos de sensibilidade, alterando, assim, a sua postura de segurança passo a passo. O resultado é um nível quase zero de falsos positivos e pouquíssimos ajustes no longo prazo.

Gerenciamento Centralizado — O sistema de gerenciamento permite que as empresas fiscalizem configurações de segurança entre aplicativos, grupos de usuários e agentes para reduzir o custo de instalação e manutenção.

Sistema necessário

Windows (apenas para as versões do SO em inglês, francês e alemão)

- Windows XP SP2, Windows 2000 Workstation, ou Windows NT 4 Workstation

McAfee PrimeSupport

O programa McAfee PrimeSupport® é essencial para aproveitar ao máximo o seu investimento nas Soluções de Proteção de Sistemas e Redes da McAfee.

A equipe PrimeSupport da McAfee possui todos os recursos certos e está pronta para levar a você a solução de serviços de que você precisa. Entre os recursos do PrimeSupport estão: autorização de acesso a todas as versões de manutenção e atualizações de produtos disponíveis, acesso a uma ampla variedade de outros recursos de auto-atendimento remoto, suporte telefônico ao vivo que pode ser acessado 24/7/365, gerentes de conta de suporte designados disponíveis, além de uma ampla variedade de soluções de suporte de software e hardware que adaptáveis às suas necessidades.

McAfee, Inc. 3965 Freedom Circle, Santa Clara, CA 95054, 888.847.8766, www.mcafee.com

Os produtos da McAfee® denotam anos de experiência e compromisso com a satisfação do cliente. A equipe McAfee PrimeSupport® de atenciosos e altamente qualificados técnicos de suporte oferece soluções sob medida e assistência técnica detalhada na gestão do sucesso de projetos essenciais — tudo isso com níveis de serviço que atendem às necessidades de cada empresa cliente. A McAfee Research, líder mundial em sistemas de informação e pesquisa de segurança, continua na vanguarda da inovação no desenvolvimento e refino de todas as nossas tecnologias.

McAfee, Enterecept, ePolicy Orchestrator e PrimeSupport são marcas comerciais, registradas ou não, da McAfee, Inc. e/ou das suas afiliadas nos EUA e/ou em outros países. A cor vermelha usada em relação à segurança é marca distintiva dos produtos que levam a marca McAfee. Todas as outras marcas comerciais, registradas ou não, mencionadas neste documento pertencem exclusivamente aos seus respectivos titulares. © 2004 McAfee, Inc. Todos os direitos reservados. 1-sps-ent-dta-001-1204