

McAfee Enterecept Standard Multi-Platform Server Agent

Prevenção de Invasões para Sistemas Críticos

O Desafio

O número de novas vulnerabilidades e a velocidade com a qual os ataques podem comprometer sistemas críticos aumentam a cada ano, aumentando os riscos à disponibilidade, à integridade e ao sigilo dos sistemas. Infelizmente, os produtos antivírus e de IDS de host 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 legislativas para garantir a privacidade de dados confidenciais e controlar o acesso a sistemas e aplicativos.

Para proteger preventivamente os sistemas contra os sofisticados ataques de hoje, as empresas precisam implementar uma prevenção contra invasões que conte com vários níveis de proteção. O McAfee® Enterecept® é a solução de prevenção contra invasões mais abrangente, precisa e flexível 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

Os Agentes Multiplataforma Padrão Enterecept protegem os sistemas contra ataques conhecidos e desconhecidos, com uma premiada tecnologia patenteada. Cada agente gerenciado de forma centralizada utiliza uma poderosa combinação de tecnologias de prevenção de invasões para bloquear ataques com precisão inigualável:

- Regras de comportamento protegem contra ataques desconhecidos dirigidos a novas vulnerabilidades — sem precisar de atualizações
- Os arquivos de características protegem o host, identificando com precisão tráfegos hostis conhecidos, reduzindo consideravelmente o número de falsos positivos
- O firewall de sistema (apenas nas versões para Windows®) controla o acesso a sistema e aplicativos, bloqueando o tráfego que entra ou sai do sistema, de acordo com o endereço IP, o protocolo ou a porta.

Benefícios

Abrangente

- Bloqueia ataques desconhecidos sem qualquer atualização, reduzindo significativamente a criticidade da distribuição de patches contra novas ameaças
- Tecnologias complementares protegem a disponibilidade, a integridade e o sigilo de servidores e dados
- A prevenção de invasões mais o firewall de sistema blindam os aplicativos essenciais contra ataques



O McAfee Enterecept utiliza regras de comportamento, arquivos de características e um firewall de sistema para prevenir ataques conhecidos e desconhecidos.

Preciso

- O *Trusted Applications* permite que as empresas eliminem o risco de falsos positivos de aplicativos essenciais
- Os arquivos de características contêm descrições específicas detalhadas de eventos
- Políticas previamente configuradas que podem ser personalizadas reduzem o número de falsos positivos e liberam valiosos recursos humanos de segurança

Flexível

- Gerencia até 10 mil agentes com um único gerenciador
- Gerenciamento opcional pelo McAfee ePolicy Orchestrator® 3.5
- Instalação e atualização imperceptíveis, sem reinicialização, garantindo uma proteção contínua
- Níveis personalizáveis de proteção, do registro ao bloqueio

Como funciona o McAfee Enterecept

Cada agente vem com um modelo predefinido de políticas totalmente configurado, 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 personalizadas específicas para seus ambientes e reduzir o número de falsos positivos.

O agente examina chamadas específicas ao sistema e às APIs, usadas por todos os aplicativos para solicitar serviços ao 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.

O console de gerenciamento do Enterecept apresenta um resumo panorâmico das ameaças e da situação do sistema.

Recursos

Prevenção de Ataques Desconhecidos — O Enterecept evita ataques novos e nunca vistos, através das suas poderosas regras de comportamento. As regras de comportamento fiscalizam o comportamento adequado do sistema operacional e de aplicativos e bloqueiam novos ataques que violem as políticas, sem qualquer necessidade de atualizações.

Prevenção da Exploração de Estouro de Buffer — Uma tecnologia patenteada impede a execução de programas como resultado de um estouro de buffer. Os agentes protegem servidores críticos contra essas perigosas explorações, que são a maior fonte de vulnerabilidades de segurança dos servidores.

Prevenção de Ataques Conhecidos — Bloqueia explorações conhecidas e impede que sejam causados danos aos servidores, comparando a atividade com o seu amplo banco de dados de ataques conhecidos. Os agentes acessam automaticamente as atualizações de novas características de ataques.

Proteção de Recursos — Protege a disponibilidade, a integridade e o sigilo dos sistemas, bloqueando seus recursos essenciais (arquivos, configurações, chaves de registro, serviços, etc.).

Firewall de Sistema (Apenas nas versões para Windows) — Bloqueia o tráfego de rede que entra e sai do sistema, através 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.

Blindagem/Envelopamento de Servidores de Web e de Banco de Dados — A blindagem impede a invasão e o uso inadequado de recursos de aplicativos essenciais (arquivos, usuários, registro, etc.). O envelopamento impede que o aplicativo protegido realize atividades mal-intencionadas fora do seu comportamento normal (por exemplo, acessar dados de outros aplicativos).

Proteção de HTTP e SQL — A proteção de HTTP bloqueia ataques dirigidos contra servidores de Web Apache, Sun ou Microsoft®, através de um exclusivo mecanismo de desmembramento de HTTP. A proteção de SQL protege servidores SQL 2000 contra técnicas de injeção de SQL, através de um exclusivo mecanismo de consulta de SQL.

Distribuição e Monitoramento pelo McAfee ePO™ 3.5 — Opções de instalação, atualização e monitoramento de agentes.

Sistema Necessário

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

- Windows Server 2003
- Windows XP SP2
- Windows 2000 Server e Advanced Server
- Windows NT 4 Server ou Enterprise Server, SP 6A
- Microsoft SQL Server 2000
- Microsoft IIS 4, 5 e 6

Sun

- Solaris 7, 8 e 9 (kernels de 32 e 64 bits)
- Sun ONE/iPlanet 3.6, 4.0, 4.1 e 6.0

HP-UX

- HP-UX II.0, Ili (PA-RISC de 64 bits)

Apache

- Apache 1.3.6 e posteriores, 2.0.42 e posteriores

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 gama 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 gama de soluções de suporte de software e hardware que podem ser adaptadas 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-ese-005-1204