

McAfee Entercept Management System

Gerenciamento de Nível Profissional para o McAfee Entercept Intrusion Prevention

O Desafio

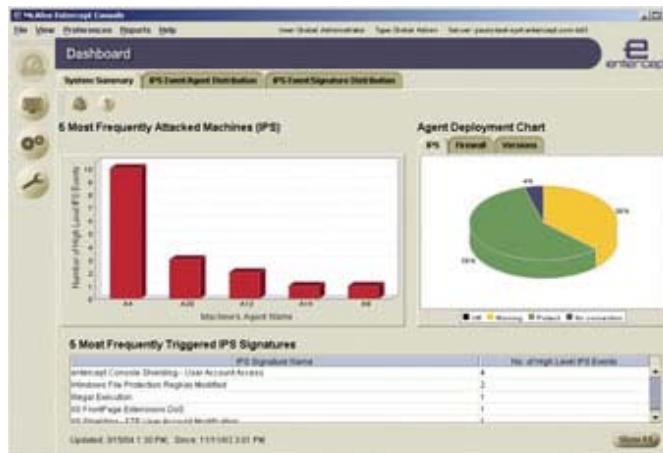
As empresas enfrentam a atemorizante tarefa de proteger as redes de hoje, que são geograficamente dispersas e heterogêneas. Elas precisam lidar com sofisticados ataques combinados que empregam vários vetores para penetrar na infra-estrutura de segurança. Elas também precisam cumprir exigências legais de proteção da integridade e do sigilo dos dados nos seus principais sistemas e aplicativos. Além disso, elas precisam documentar para a alta administração o valor dos seus investimentos em segurança.

As empresas precisam implementar um sistema de gestão de segurança que seja capaz de gerenciar com riqueza de recursos milhares de agentes, proporcionar proteção inigualável contra ameaças e reduzir o tempo necessário para administrar o sistema. O McAfee® Entercept® Intrusion Prevention é a solução mais abrangente, precisa e flexível de proteção contra ameaças do mercado, ajudando as empresas a reduzir os riscos, assegurar a disponibilidade dos negócios e reduzir o custo total de propriedade.

A solução Entercept

O Entercept Management System oferece gerenciamento amplo de nível corporativo para os agentes de prevenção de invasões do Entercept. O Sistema de Gerenciamento proporciona uma infra-estrutura de gerenciamento flexível, robusta e fácil de usar, capaz de controlar até 10,000 agentes por servidor de gerenciamento.

Todos os agentes Entercept (Desktop e Servidor) compartilham a mesma infra-estrutura de gerenciamento que o Sistema de Gerenciamento possui. **As** empresas podem aproveitar facilmente as configurações de segurança entre aplicativos, grupos de usuários e agentes para reduzir o custo de instalação e manutenção. Os administradores de segurança podem importar e exportar configurações entre vários servidores de gerenciamento, garantindo uma fiscalização uniforme das políticas. O Entercept protege várias plataformas (Windows, HP-UX e Solaris), proporcionando uma proteção uniforme e confiável contra invasões do host por meio do host para os ambientes de servidor heterogêneos de hoje.



O McAfee Entercept Management System possui um painel de controle resumido para exibir um panorama do status do sistema.

Como funciona o Entercept Management System

O Entercept Management System consiste em um servidor e um console de gerenciamento altamente flexíveis. O servidor de gerenciamento age como camada intermediária entre os agentes Entercept e o console, coordenando as comunicações e armazenando o banco de dados de ocorrências e configurações. Vários consoles em localidades geograficamente distribuídas podem conectar-se simultaneamente ao servidor de gerenciamento para administrar e monitorar os agentes.

Quando os agentes detectam e bloqueiam os ataques, eles enviam as respectivas informações ao servidor de gerenciamento Entercept. O servidor encaminha os respectivos dados para os consoles, além de armazená-los no banco de dados SQL central. O console agrega ocorrências semelhantes para reduzir o volume de dados brutos exibidos, apresentando um resumo da situação geral do sistema em um único painel de controle.

O Sistema de Gerenciamento possui um amplo conjunto de opções de reação e notificação, inclusive alertas por e-mail, por pager, capturas de SNMP, e disparo de um processo. O console se comunica com os agentes por meio de canais criptografados e autenticados. O Entercept Management System fiscaliza ativamente as políticas de segurança da empresa com a sua premiada tecnologia de prevenção de invasões, bloqueando ataques e, ao mesmo tempo, oferecendo recursos inigualáveis de geração de relatórios e análise de dados.

Benefícios

Abrangente

- Reduz a criticidade da distribuição de patches contra novas ameaças
- Bloqueia ataques conhecidos e desconhecidos
- protege a integridade e a privacidade de dados confidenciais
- Fiscalização ativa e automática de políticas, sem precisar da intervenção do usuário final
- Protege sistemas Windows, Solaris e HP-UX com uma premiada tecnologia patenteada
- Blindagem/Envolvimento de Aplicativos — A blindagem impede a invasão e o uso inadequado de recursos de servidores de Web, de banco de dados e de aplicativos de desktop (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).

Preciso

- Uma poderosa combinação de regras de comportamento, arquivos de características e firewall de sistema oferece proteção contra ataques tais como explorações de estouro de buffer e reduz o número de falsos positivos
- Assistentes criam regras e características personalizadas que se adaptam a qualquer ambiente
- A ausência de interação do usuário final elimina as chamadas à central de suporte de TI
- A pesquisa, a filtragem e o agrupamento permitem que os administradores identifiquem tendências e descubram possíveis ameaças

Flexível

- Gerencie milhares de agentes com um único gerenciador
- Distribuição e monitoramento de agentes por meio do McAfee ePolicy Orchestrator[®] 3.5 (opcional)
- Aproveita configurações entre aplicativos, grupos de usuários ou agentes
- Instalação/atualização imperceptíveis, sem a necessidade de reiniciar a máquina
- A agregação de ocorrências consolida ocorrências repetidas em um único item no console
- A trilha de auditoria do console registra todas as alterações de configuração feitas pelos administradores
- Níveis personalizáveis de proteção, do registro ao bloqueio.

Sistema Necessário

Configuração Recomendada

Servidor de Gerenciamento

- Pentium IV de 1,5GHz ou melhor
- 1GB de RAM
- 20GB de espaço livre no disco rígido
- Windows Server 2003
- Windows 2000 Server ou Advanced Server (SP 2 ou posterior)
- SQL Server 2000 (SP 2 ou posterior)
- Endereço IP estático
- Nenhum outro aplicativo instalado
- Portas TCP 443 e 5005 disponíveis (a 443 é usada se nada for definido em contrário, mas ela pode ser alterada)

Console

- Pentium III de 800MHz ou melhor
- 256MB de RAM
- 100MB de espaço livre no disco rígido
- Windows XP SP 2
- Windows 2000 Professional, Server ou Advanced Server
- Windows NT 4 Server ou Workstation, SP 6a

McAfee PrimeSupport

A McAfee tem adotado a estratégia de fornecer tecnologia de primeira classe para cada tipo de aplicação de gestão de desempenho — mas a Estratégia Protection-in-Depth™ é mais que apenas distribuir e implementar as melhores soluções hoje. A prevenção é, com certeza, a prioridade número um, mas, inevitavelmente, você precisará reagir a algum problema!

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-ent-mgt-003-1204