



McAfee System Protection Solutions

Soluções de Gerenciamento Seguro de Conteúdo

Índice

Resumo Executivo	3
Panorama	3
Desafios ao Gerenciamento Seguro de Conteúdo	3
Soluções Flexíveis de Gerenciamento de Conteúdo	4
Soluções para o Gateway de Internet	5
Soluções para o Servidor de Aplicativos	6
Solução de Serviços Gerenciados	7
Segurança em Vários Níveis	8
Conclusão	8
McAfee PrimeSupport	9

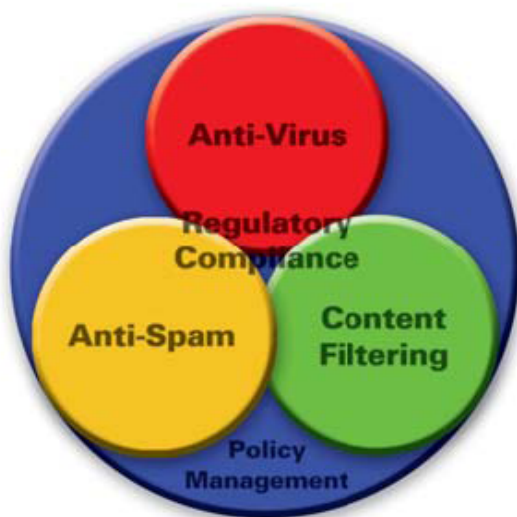
Resumo Executivo

Proteger o conteúdo que entra e sai das empresas é essencial nos ambientes de rede multifacetados de hoje. É fundamental assegurar que a sua empresa conte com uma proteção abrangente contra conteúdos inadequados, mal-intencionados ou virais, e que você siga as políticas de segurança da empresa, cumprindo, ao mesmo tempo, as normas de privacidade definidas pelo ramo e pela empresa.

Panorama

As Soluções de Gerenciamento Seguro de Conteúdo da McAfee® oferecem tecnologia integrada e flexível para que empresas de pequeno, médio e grande porte utilizem os recursos da maneira mais eficiente, aumentem a produtividade e evitem o comprometimento das políticas definidas pelo ramo e pela empresa. Com as melhores tecnologias antivírus, anti-spam e de proteção de conteúdo, as Soluções de Gerenciamento Seguro de Conteúdo da McAfee estão ligadas ao que há de melhor no mercado em gerenciamento e aplicação de políticas, garantindo que você tenha a flexibilidade de gerenciamento necessária.

Instaladas no gateway de Internet ou em servidores de e-mail ou de colaboração, as Soluções da McAfee levam a estratégia Protection-in-Depth™ a todos os aplicativos líderes de mercado associados, além de appliances com hardware e software integrados que permitem o controle, o gerenciamento e a compreensão do seu tráfego de Internet.



Funções de gerenciamento necessárias para proteger o conteúdo de Internet e e-mail de uma empresa.

Desafios ao Gerenciamento Seguro de Conteúdo

Antivírus

Vivemos em um mundo cada vez mais conectado, e as ameaças evoluíram muito na última década a uma velocidade alarmante. O impacto sobre as empresas aumentou em um ritmo incrível. Identificar as áreas de vulnerabilidade que colocam em risco sua empresa e seus negócios não é uma tarefa fácil em termos de conhecimento e recursos necessários.

Não apenas os incidentes de vírus estão aumentando, mas a gravidade desses incidentes e o custo associado à sua recuperação também estão crescendo.

- Segundo a 8ª Pesquisa Anual de Predominância de Vírus de Computador do ICSA Labs em 2002, os pesquisados foram solicitados a identificar os meios de infecção dos seus incidentes, desastres ou encontros mais recentes, e 86% indicaram o e-mail como a principal fonte.
- Segundo a Computer Economics, o vírus Nimda custou às empresas US\$ 635 milhões em limpeza e perda de produtividade em 2001.

Os vírus e worms que se disseminam por meio de e-mails podem infectar toda a sua rede em questão de minutos, interrompendo as comunicações com seus clientes e parceiros, além de interromper a comunicação e a colaboração dentro da empresa. Esses vírus exploram os recursos automatizados de criação de scripts dos aplicativos de e-mail, que são flexíveis e ricos em recursos, para gerar inundações de mensagens de e-mail que ocupam os servidores e entopem as caixas de entrada.

Anti-spam

A evolução continua, e não se refere apenas a códigos mal-intencionados, tais como vírus, worms e cavalos de tróia. No mundo da troca de mensagens para colaboração, as ameaças estão se tornando mais diversificadas, invasivas e subversivas, e nem sempre têm por objetivo causar interrupções diretas na produtividade dos negócios, embora esse seja, muitas vezes, o efeito.

- Segundo a Gartner Research, as mensagens de spam custam às empresas dos EUA US\$ 1 bilhão por ano em termos de perda da produtividade.
- Segundo o Aberdeen Group, espera-se que a porcentagem de mensagens de spam que entopem as redes corporativas suba de 25% em 2002 para 50% em 2003.

O spam está sendo cada vez mais usado como um novo mecanismo de distribuição de cavalos de tróia e

virus. Já vimos a distribuição de backdoors por meio de spam, como foi o caso do Adware-Surfbar em setembro de 2003.

Com a crescente tendência das mensagens de *phishing*, o spam é criado para induzir o destinatário a revelar informações pessoais tais como números de cartão de crédito, informações bancárias, números de CPF e RG, senhas e outras informações sigilosas.

Anti-phishing

O McAfee SpamKiller® possui regras específicas que ajudam a identificar ataques de *phishing*, procurando certas características peculiares a esse tipo de ataque que possam estar presentes nas mensagens. Logo que são acionadas, essas regras recebem automaticamente uma pontuação geral de spam do SpamKiller, resultando, na maioria dos casos, no bloqueio das mensagens. Junto com o APWG (Anti-Phishing Working Group), a McAfee reuniu um detalhado banco de dados de ataques de *phishing*, utilizando o conhecimento sobre esses ataques para criar regras eficazes de filtragem.

Filtragem de Conteúdo

Muitas empresas estão começando a considerar o spam de conteúdo ofensivo como um problema jurídico, após o precedente criado na Chevron. Em 1996, a Chevron Corporation envolveu-se em um processo no valor de US\$ 2,2 milhões movido por funcionárias que se ofenderam com um e-mail contendo uma piada, intitulado “25 motivos pelos quais a cerveja é melhor que a mulher”. Da mesma forma, uma piada racista que circulou pela rede ofendeu alguns funcionários e levou a Morgan Stanley Dean Witter & Co. a enfrentar um processo no valor de US\$ 60 milhões.

- Relatórios do IDC, em junho de 2001, indicam que 48% dos empregadores que monitoram os funcionários afirmam que sua intenção é proteger-se contra vírus e contra a perda de informações; 21% monitoram os funcionários como uma forma de limitar a responsabilização legal.

Os empregadores sempre foram responsáveis pelos atos dos seus funcionários no local de trabalho. Entretanto, se uma empresa for capaz de demonstrar o devido cuidado no sentido de reduzir atividades inaceitáveis dos seus funcionários, isso poderá reduzir a possibilidade de responsabilização da empresa.

- Segundo o “The e-Policy Handbook”, de Nancy Flynn, 27% das empresas da lista FORTUNE 500 já precisaram se defender contra ações de assédio sexual cuja origem eram e-mails inadequados.

Gerenciar e proteger o conteúdo em um ambiente de troca de mensagens aumenta significativamente a produtividade dos funcionários.

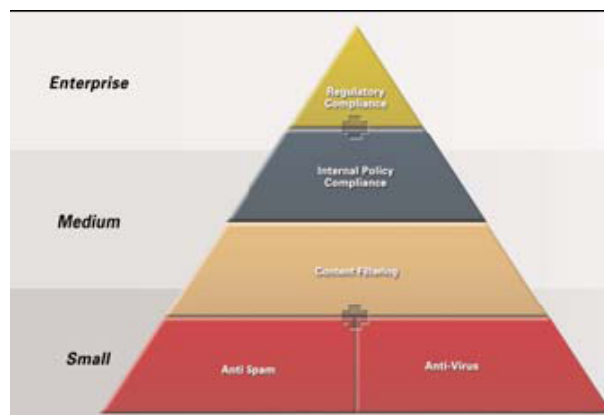
Cumprimento das Políticas Internas

Mais do que nunca, o trabalho do gerente de segurança ou de TI é um ato delicado de equilíbrio. De um lado estão as exigências dos negócios — gerenciar uma gama cada vez maior de dispositivos e localidades e atender às necessidades de um número cada vez maior de usuários móveis e funcionários que trabalham fora da empresa. DO outro lado estão as exigências de segurança — manter os sistemas atualizados e gerenciar os vários níveis de proteção e as ferramentas necessárias para combater as ameaças de hoje que estão em constante evolução.

É essencial garantir o cumprimento das políticas internas pela sua solução de Gerenciamento Seguro de Conteúdo. A visibilidade e a aplicação são fundamentais para assegurar que a sua proteção esteja atualizada e realmente proteja a sua empresa.

Cumprimento de Leis e Normas

O cumprimento de leis de privacidade tais como a HIPAA, a GLBA e a SEC continuam alimentando as preocupações das empresas em relação à segurança da troca de mensagens. A tecnologia de Gerenciamento Seguro de Conteúdo permite não apenas proteger a troca de mensagens nas empresas, como também ajuda a impedir o vazamento de informações, permitindo que as empresas estabeleçam políticas para proteger-se contra responsabilização legal. Os riscos da responsabilização legal são cada vez maiores devido a funcionários que baixam MP3s e DVDs inteiros para os recursos de armazenamento da empresa. Essas empresas têm a obrigação legal não apenas de assegurar que podem cumprir as leis e normas, mas também de se proteger juridicamente.



Distribuição das funções de gerenciamento seguro de conteúdo entre os segmentos de empresas de pequeno, médio e grande porte.

Soluções Flexíveis de Gerenciamento de Conteúdo

Uma empresa de pequeno, médio ou grande porte tem necessidades básicas diferentes em relação a

uma SCM (Solução de Gerenciamento Seguro de Conteúdo), e qualquer solução que se considere nessa área deverá ser capaz de acompanhar as necessidades da empresa. Para uma empresa de pequeno porte, os elementos mais comuns da SCM — filtragem antivírus e anti-spam — são os mais importantes, mas as pequenas empresas também precisam impedir a entrada de conteúdos inadequados. Empresas de médio porte têm as mesmas necessidades em relação à tecnologia antivírus e anti-spam, mas as necessidades relativas a essas tecnologias, bem como as que se referem à filtragem de conteúdo, estão ficando cada vez mais específicas e detalhadas. Isso ocorre porque as empresas de médio porte possuem políticas de segurança de troca de mensagens de negócios que precisam ser aplicadas e cumpridas. Exemplos de políticas de segurança de troca de mensagens: a necessidade de opções específicas de quarentena para indivíduos quando se trata de spam, permitir que apenas determinados tipos de arquivos entrem na sua empresa, ou abranger grupos específicos de pessoas. Em resumo, uma empresa precisa ser capaz de estabelecer regras de varredura para indivíduos ou grupos de usuários. As demandas das grandes empresas em relação ao cumprimento de políticas estão se tornando cada vez mais detalhadas devido à necessidade de cumprir políticas detalhadas de segurança interna ou leis que proíbem a saída de dados confidenciais das empresas. Qualquer solução de SCM que seja adquirida deve proporcionar à empresa a melhor tecnologia em cada uma das principais áreas — antivírus, anti-spam e filtragem de conteúdo — além de ser capaz de proporcionar controles detalhados de políticas para o tráfego enviado e recebido. Isso permite que a empresa cumpra todas as políticas de segurança de troca de mensagens. Outra vantagem de uma solução integrada é que a empresa reduzirá o seu TCO de gerenciamento e administração, tendo toda a tecnologia central de troca de mensagens disponível em uma única solução.

Soluções para o Gateway de Internet

Appliances McAfee

Os Appliances McAfee são a base das Soluções de Gerenciamento de Conteúdo da McAfee para *Gateway*. Os Appliances McAfee 3100, 3200 e 3300 estão disponíveis em três soluções físicas altamente flexíveis e instaláveis em rack. Utilizando tecnologia de PC testada e aprovada de alta disponibilidade e um robusto sistema operacional Linux, os Appliances são uma solução robusta e flexível para hospedar as Soluções de Software para Gerenciamento Seguro de Conteúdo da McAfee. Os Appliances da McAfee executam os programas McAfee WebShield® e

McAfee SpamKiller individualmente ou combinados em um único appliance.

Appliances McAfee WebShield

Nos multifacetados ambientes de rede de hoje, é essencial assegurar que o conteúdo que entra e sai da empresa atenda às políticas corporativas de segurança e às leis que tratam da privacidade. As Soluções de Gerenciamento Seguro de Conteúdo da McAfee utilizam uma tecnologia integrada e flexível que permite a empresas de qualquer porte otimizar seus recursos, aumentar a produtividade e impedir o comprometimento das suas políticas de segurança. Com tecnologias de primeira classe contra vírus, spam e de proteção de conteúdo, as Soluções de Gerenciamento Seguro de Conteúdo da McAfee permitem que você controle, gereencie e compreenda o seu tráfego de Internet.

Os Appliances McAfee WebShield são uma solução do tipo “configure e esqueça” para o gateway de Internet, efetuando varredura no tráfego de entrada e saída dos protocolos SMTP, HTTP, FTP e POP3. Os Appliances são incomparáveis em termos de desempenho, detecção e limpeza de vírus, e proteção contra e-mails indesejáveis na forma de spam e conteúdos inconvenientes. Podem ser usados por empresas de qualquer porte.

Appliances McAfee SpamKiller

Os Appliances McAfee SpamKiller oferecem proteção anti-spam e filtragem de conteúdo líderes de mercado em um único appliance que integra hardware e software. O SpamKiller proporciona uma taxa de detecção de spam de 95%, sem qualquer ajuste. A principal tecnologia dos appliances SpamKiller é o engine McAfee SpamAssassin™, que atua por meio de um sistema de classificação, atribuindo notas aos e-mails de acordo com uma série de testes. O SpamAssassin utiliza um sistema de pontuação baseado em um amplo conjunto de regras para determinar se um e-mail específico é um spam. Centenas de regras são aplicadas a cada e-mail, e cada regra tem uma pontuação negativa ou positiva associada a ela. Regras com pontuação negativa indicam atributos de mensagens legítimas, e regras com pontuação positiva indicam atributos de mensagens não-solicitadas. Quando combinadas, essas pontuações individuais dão a cada e-mail uma *classificação geral de spam*. Utilizando o processo subjacente de conjuntos regras predefinidas, os appliances SpamKiller verificam cada e-mail recebido, empregando diferentes métodos de detecção.

- **Análise de Integridade** — O SpamKiller examina o cabeçalho, o layout e a organização de cada e-mail, identificando as características do spam.

- **Detecção Heurística** — Usada para identificar mensagens como provável spam. A detecção heurística utiliza uma série de testes internos para determinar a probabilidade de uma mensagem ser realmente um spam. Cada teste atribui uma nota para ajudar a reduzir os falsos positivos.
- **Filtragem de Conteúdo** — Essa função pode ser usada para ajudar a identificar palavras ou expressões-chave em uma mensagem que possam indicar que se trata de um spam.
- **Suporte a Blacklists e Whitelists** — Blacklists definidas pelo administrador, que bloqueiam domínios conhecidos pelo administrador como remetentes de spam; além de whitelists definidas pelo administrador, que sempre permitem a entrada de mensagens provenientes de domínios especificados pelo administrador.
- **Utilização de Listas de Bloqueio de DNS** — Os appliances WebShield permitem o uso de listas de bloqueio por DNS para a identificação de remetentes conhecidos de spam.
- **Filtragem Bayesiana** — Com a tecnologia de filtragem bayesiana, a solução SpamKiller é capaz de assimilar o que é e o que não é spam para uma determinada empresa, proporcionando uma detecção de spam verdadeiramente inteligente.

Soluções para o Servidor de Aplicativos

McAfee SecurityShield for Microsoft ISA Server

Com funções e desempenho incomparáveis de antivírus, anti-spam e filtragem de conteúdo, o McAfee SecurityShield™ não tem rival na proteção do Microsoft® ISA Server 2000 e 2004.

Reconhecendo originalmente os protocolos SMTP, HTTP e FTP, a proteção dos principais protocolos de tráfego de e-mail de Web e de Internet está garantida. Filtre o tráfego que entra e sai da empresa ou, em empresas que usam o Microsoft ISA Server internamente, entre departamentos ou áreas da empresa. Com o McAfee SecurityShield, você tem o que há de melhor em tecnologia antivírus, com a filtragem antivírus de primeira classe da McAfee. O SecurityShield pode reparar, bloquear ou colocar em quarentena automaticamente o tráfego infectado, impedindo que códigos mal-intencionados entrem ou saiam da empresa por meio dos protocolos SMTP, HTTP e FTP.

Para empresas que querem a melhor defesa contra o spam, existe o SpamKiller for SecurityShield.

O SpamKiller atribui notas aos e-mails de acordo com uma série de testes internos, proporcionando uma

detecção extremamente precisa, sem a necessidade de qualquer outro ajuste. Ele oferece cinco níveis de proteção contra spam:

- **Análise de Integridade** — O cabeçalho, o layout e a empresa remetente de cada mensagem são examinados para identificar as características que são comuns a todas as mensagens de spam.
- **Detecção Heurística** — Por meio de vários testes internos, o SpamKiller determina a probabilidade de uma mensagem ser um spam; cada teste atribui uma nota para ajudar a reduzir os falsos positivos.
- **Filtragem de Conteúdo** — Podem ser inseridas palavras ou expressões-chave que possam estar presentes em e-mails indicando que se tratam de spam.
- **Blacklists e Whitelists** — As blacklists são listas de remetentes conhecidos de spam, e as whitelists são remetentes conhecidos de mensagens que podem ser classificadas como spam, mas contêm informações que você deseja receber. Além das blacklists e whitelists definidas pelo administrador, os usuários podem definir suas listas pessoais, permitindo ainda mais personalização e precisão.
- **Filtragem Bayesiana** — Com a tecnologia de filtragem bayesiana, a solução SpamKiller é capaz de assimilar o que é e o que não é spam para uma determinada empresa, proporcionando uma detecção de spam verdadeiramente inteligente.

McAfee GroupShield para Servidores de E-mail

O McAfee GroupShield® para Servidores de E-mail oferece uma proteção abrangente contra ameaças que chegam por e-mail, tais como vírus e conteúdos inadequados, além de conter um módulo complementar opcional anti-spam para servidores Microsoft Exchange 5.5, 2000, 2003 e Lotus Domino 5 ou posteriores. Como um componente das soluções de gerenciamento seguro de conteúdo para servidores de aplicativos, o GroupShield pode identificar e impedir a entrada e a circulação de mensagens ou arquivos hostis no seu ambiente de servidor de e-mail. Apenas o GroupShield se integra com o McAfee ePolicy Orchestrator® (ePO™) para permitir que os administradores gerenciem as políticas e gerem relatórios gráficos de maneira centralizada. O McAfee SpamKiller atua como um complemento opcional do GroupShield, proporcionando recursos anti-spam inigualáveis como parte de uma solução simples e integrada de segurança de e-mail. Finalmente, o McAfee Outbreak Manager oferece uma defesa eficiente e proativa contra o envio de e-mails em massa (que tornaria inúteis outras soluções de segurança).

Como todos os produtos antivírus da McAfee, o GroupShield utiliza o premiado engine de varredura da McAfee. Sempre reconhecido por organizações independentes de teste como tecnologia líder mundial em detecção e limpeza de vírus, o engine bloqueia todos os tipos de vírus e códigos mal-intencionados, inclusive vírus de macro, cavalos de tróia, worms da Internet, vírus avançados de 32 bits e até mesmo objetos ActiveX e Java hostis. A McAfee tem um invejável currículo em testes independentes por proporcionar detecção e limpeza eficientes.

O McAfee GroupShield conta com o AutoUpdate, que permite o download automático dos mais recentes arquivos de definição de vírus (DAT) por meio de FTP ou de compartilhamento de arquivos da rede. Essa função automatizada do servidor assegura que você sempre estará atualizado com os últimos arquivos DAT da McAfee.

McAfee SpamKiller para Servidores de E-mail

O McAfee SpamKiller para Servidores de E-mail oferece proteção abrangente contra spam e conteúdos inadequados para servidores Microsoft Exchange 5.5, 2000, 2003 e para o Lotus Domino 5 ou posteriores. Disponível como um componente autônomo ou em combinação com o McAfee GroupShield, o SpamKiller para Servidores de E-mail proporciona detecção e desempenho incomparáveis contra o spam, e não tem rival na proteção de servidores de e-mail. Projetado para operar com alto desempenho, o SpamKiller pode ajudar a reduzir os custos associados ao spam, varrendo as mensagens assim que elas chegam ao servidor de e-mail. Após passar pela varredura, o spam pode ser colocado em quarentena em uma pasta de lixo eletrônico no servidor, ou na pasta de lixo eletrônico do usuário. Detectando o spam, você impede que seus usuários precisem lidar com mensagens indesejáveis, ajudando-os a aumentar sua produtividade. A principal tecnologia dos appliances SpamKiller é o engine McAfee SpamAssassin, que funciona por meio de um sistema de classificação que atribui notas aos e-mails de acordo com uma série de testes. O SpamAssassin utiliza um sistema de pontuação baseado em um amplo conjunto de regras para determinar se uma mensagem específica é um spam. Centenas de regras são aplicadas a cada mensagem, e cada regra possui uma pontuação negativa ou positiva associada a ela. Regras com pontuação negativa indicam atributos de mensagens legítimas, e regras com pontuação positiva indicam atributos de mensagens não-solicitadas. Quando combinadas, essas pontuações individuais dão a cada e-mail uma *classificação geral de spam*.

Utilizando o processo subjacente de conjuntos de regras predefinidas, os appliances SpamKiller verificam cada

e-mail recebido, empregando diferentes métodos de detecção.

- **Análise de Integridade** — O SpamKiller examina o cabeçalho, o layout e a organização de cada e-mail, identificando as características comuns do spam.
- **Detecção Heurística** — Usada para identificar mensagens como provável spam. A detecção heurística utiliza uma série de testes internos para determinar a probabilidade de uma mensagem ser realmente um spam. Cada teste atribui uma nota para ajudar a reduzir os falsos positivos.
- **Filtragem de Conteúdo** — Essa função pode ser usada para ajudar a identificar palavras ou expressões-chave em uma mensagem que possam indicar que se trata de um spam.
- **Suporte a Blacklists e Whitelists** — Blacklists definidas pelo administrador, que bloqueiam domínios conhecidos pelo administrador como remetentes de spam; além de whitelists definidas pelo administrador, que sempre permitem a entrada de mensagens provenientes de domínios especificados pelo administrador.
- **Filtragem Bayesiana** — Com a tecnologia de filtragem bayesiana, a solução SpamKiller é capaz de assimilar o que é e o que não é spam para uma determinada empresa, proporcionando uma detecção de spam verdadeiramente inteligente.

McAfee PortalShield for Microsoft SharePoint Server

O McAfee PortalShield™ for Microsoft SharePoint é segurança de conteúdo para todos os documentos, arquivos, conteúdo da Web e repositórios de documentos. Com o PortalShield, os usuários do Microsoft SharePoint podem acessar, encontrar e compartilhar com segurança as informações de que precisam para serem produtivos profissionalmente, independentemente da localização física das informações na rede. Os recursos do PortalShield vão além das soluções tradicionais de segurança antivírus e de conteúdo para proteger os servidores Microsoft SharePoint, detectando, limpando e eliminando vírus, e procurando conteúdo proibido dentro dos documentos armazenados nos espaços de trabalho do SharePoint.

Com um único pacote de software que oferece varredura antivírus abrangente de todos os documentos, arquivos, conteúdos da Web e repositórios de documentos em máquinas que executam o SharePoint Portal Server, o PortalShield atende à necessidade das pequenas, médias e grandes empresas em relação à implementação de

tecnologias antivírus abrangentes que sejam flexíveis e gerenciáveis, ajudando as empresas a reduzir sua vulnerabilidade a ataques contra conteúdos e dados confidenciais.

Solução de Serviços Gerenciados

McAfee Managed Mail Protection

O McAfee Managed Mail Protection oferece proteção abrangente de e-mail contra spam, vírus, além de filtragem de conteúdo, tudo isso como um serviço gerenciado. O Managed Mail Protection varre os e-mails SMTP enviados e recebidos, que são encaminhados à McAfee para detecção e limpeza prévias de spam e vírus antes de entrar ou sair do gateway, sem os altos custos e os inconvenientes normalmente associados à segurança de e-mail. Junto com a abrangente varredura de e-mails “na nuvem” (in the cloud), o McAfee Managed Mail Protection também oferece — gratuitamente — acesso a um portal seguro na Web para exibir relatórios de visibilidade de status de e-mail e estatísticas de velocidade, além de personalizar as políticas de e-mail, aumentando a flexibilidade da sua segurança de e-mail. Delegue sua administração de segurança de e-mail à McAfee para ter uma *proteção automática sempre ativa* — de modo que você possa voltar a se concentrar nos seus negócios.

Compatível com todas as plataformas de e-mail (Exchange, Outlook, Lotus), o Managed Mail Protection não exige a contratação de mais profissionais nem a compra de mais hardware e software para gerenciar as operações diárias de e-mail, reduzindo o custo total de propriedade da segurança de e-mail. O Managed Mail Protection é um serviço gerenciado de segurança que não é instalado nem fica residente no PC. Basta que um registro de MX (Intercâmbio de E-mail) de uma empresa seja redirecionado por meio dos servidores da McAfee para que o tráfego de e-mail passe rapidamente pela varredura com facilidade — antes de entrar ou sair da sua rede — com atraso de menos de um segundo no trânsito. O Managed Mail Protection ajuda as empresas a se proteger contra as mensagens que consomem tempo ou contra conteúdos inadequados, sem aumentar a carga de trabalho do sobrecarregado pessoal de TI ou da rede existente.

Como parte das Soluções de Gerenciamento Seguro de Conteúdo da McAfee, o Managed Mail Protection proporciona uma tecnologia integrada e flexível, garantindo que as comunicações de uma empresa por e-mail fiquem limpas e protegidas. A aplicação de políticas seguras de conteúdo com o Managed Mail Protection protege automaticamente suas comunicações essenciais e, ao mesmo tempo, otimiza

os recursos, aumenta a produtividade e impede o comprometimento de políticas internas. Com o Managed Mail Protection, um único serviço de segurança oferece vários níveis de proteção gerenciada com a confiável tecnologia da McAfee.

Segurança em Vários Níveis

Como o perímetro está se tornando uma área cada vez mais incerta, as empresas não podem mais pressupor que os servidores que ficam por trás das defesas de gateway estejam totalmente protegidos. Mediante um número cada vez maior de servidores de aplicativos, tais como portais de Web ou servidores de troca de mensagens para colaboração, expostos à Internet, muitas vezes nos esquecemos de que ainda é grande a possibilidade de vazamento de informações ou de ataques. As Soluções de Gerenciamento Seguro de Conteúdo da McAfee são projetadas para adequar-se a todos os níveis da rede, no gateway e nos seus principais servidores de aplicativos.

A prática recomendada para qualquer empresa é aplicar proteção abrangente e amplitude de proteção. A sua empresa precisa de proteção abrangente para se defender contra ameaças, tais como vírus, worms, spams e conteúdos inadequados e, ao mesmo tempo, cumprir exigências legais e aplicar as políticas internas. Além disso, as empresas necessitam de proteção no gateway e nos servidores de e-mail e de aplicativos.

As únicas soluções que comprovadamente oferecem proteção ampla em vários níveis e combina vários métodos de detecção com proteção em todos os níveis do ambiente perimetral são as Soluções de Gerenciamento Seguro de Conteúdo da McAfee.

Para Que Proteger o Gateway de Internet?

Sendo o primeiro ponto de entrada, o gateway de Internet tem a vantagem de ser um ponto único de proteção para toda a estrutura da empresa. Os appliances McAfee instalados no gateway de Internet protegem o e-mail contra códigos mal-intencionados, tais como vírus, além de conteúdos inadequados em mensagens e spam. O tráfego da Web é protegido contra códigos mal-intencionados, inclusive usuários com contas de Webmails pessoais. Cuidando do spam no gateway, o espaço de armazenamento na rede e a largura de banda são economizados pelo bloqueio das mensagens antes que elas entrem no ambiente de e-mail da empresa.

Com menos dispositivos para gerenciar e manter, os appliances da McAfee que executam o WebShield e o SpamKiller reduzem o custo total de propriedade e aumentam a capacidade de reação a epidemias, com a capacidade de atualização rápida. Como um

funil principal de segurança para o relato de incidentes de segurança na rede, fica fácil ter uma visão ampla da atividade do gateway. Visto que o McAfee WebShield e o SpamKiller residem nos appliances projetados com um sistema operacional robusto baseado no Linux, os appliances reduzem o risco de inatividade da rede devido à manutenção de patches de segurança normalmente associada aos ambientes operacionais mais utilizados.

Por que Proteger os Servidores de Aplicativos?

Os servidores de aplicativos, entre eles os servidores de e-mail e de colaboração (Microsoft Exchange, Lotus Domino), e os portais de Web (Microsoft SharePoint) representam dificuldades únicas para a proteção. Sempre que uma mensagem é enviada ou recebida, ou que se escreve uma nova solicitação de calendário ou outro item, como um arquivo ou documento, a mensagem fica armazenada em um banco de dados ou em outro repositório de informações. Se a mensagem contiver uma ameaça, ela será armazenada e estará pronta para infectar ou propagar-se assim que for lida por outro usuário. Nem as soluções antivírus para PC nem as soluções antivírus para o gateway são capazes, sem auxílio, de varrer esses tipos de repositórios ou bancos de dados; portanto, eles se tornam portos seguros de onde podem ser lançadas futuras infecções contra a empresa hospedeira ou seus clientes e parceiros. Além disso, as mensagens podem ser encaminhadas do servidor de troca de mensagens para outro destinatário sem sequer passar pela varredura no cliente ou passar pelo gateway de Internet. As mensagens podem ser transmitidas internamente sem sequer deixar a rede por meio do gateway de Internet.

A proteção no nível do servidor de aplicativos possibilita um nível maior de personalização de políticas para usuários/grupos, além de permitir que os administradores protejam o tráfego interno de e-mail, além do tráfego externo (que inclui o envio de materiais inadequados dentro da empresa).

Conclusão

As soluções de gerenciamento seguro de conteúdo residem em dois "postos avançados" no perímetro — o gateway de Internet e o servidor de aplicativos (área de e-mail ou de troca de mensagens de colaboração).

Dar conta das atuais ameaças, do cumprimento das políticas internas e das exigências legais significa assegurar que todas as áreas da sua empresa estejam cobertas. O gateway de Internet, sendo o primeiro ponto de entrada na estrutura da empresa, permite a implementação de soluções que podem ser distribuídas por toda a rede de maneira mais fácil e rápida. Entretanto, devido ao seu amplo alcance, as soluções de gateway são incapazes de penetrar nos servidores de e-mail e de colaboração devido à natureza do seu funcionamento. Os ambientes de e-mail ou de colaboração apresentam dificuldades ligeiramente diferentes quando se trata de proteger o ambiente. Esses servidores são vulneráveis aos ataques tradicionais de rede e transportados por e-mail, permitindo a hospedagem de ameaças por longos períodos, contribuindo, muitas vezes, para a reinfecção da rede. Se os servidores forem deixados sem verificação, eles também hospedarão uma grande parte das comunicações internas que não passam pelo gateway de Internet. Para proteger esses ambientes, as soluções de gerenciamento seguro de conteúdo precisam residir na plataforma do ambiente de e-mail ou de colaboração.

Simplificando, para proteger realmente o tráfego de mensagens que entram e saem da sua empresa, a instalação de soluções de gerenciamento seguro de conteúdo no gateway de Internet, nos servidores de e-mail e em todos os servidores de aplicativos é obrigatória. Escolher uma solução de gerenciamento seguro de conteúdo de um fornecedor como a McAfee, que pode oferecer uma tecnologia integrada de primeira classe, ajudará muito, com uma interface única de gerenciamento para controlar as políticas em diversas áreas de funcionalidade, além de

relatórios unificados de vários recursos do gerenciamento seguro de conteúdo. A McAfee também pode fornecer uma ampla variedade de soluções para cobrir toda a sua rede, permitindo que você tenha os mesmos componentes tecnológicos premiados instalados em diferentes pontos de entrada na rede – essencial para atender às necessidades de uma defesa de mensagens em vários níveis.

McAfee PrimeSupport

A McAfee tem adotado a estratégia de fornecer tecnologia de primeira classe a cada tipo de aplicação de gerenciamento de segurança desempenho e — mas a Estratégia Protection-in-Depth é mais que apenas distribuir e implementar as melhores soluções hoje. Certamente a prevenção é a prioridade número um, porém, 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 precisa. Entre os recursos do PrimeSupport estão: autorização de acesso a todas as versões de manutenção e atualizações de produtos disponíveis, acesso a uma grande 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 diversas 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®, com seus 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, Protection-in-Depth, WebShield, SpamKiller, SpamAssassin, SecurityShield, GroupShield, ePolicy Orchestrator, ePO, PortalShield, 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 Networks Associates Technology, Inc. Todos os direitos reservados. 6-sps-scm-001-1004