



Soluções McAfee System Protection

Dez coisas que empresas de pequeno e médio porte precisam saber para manter um ambiente tecnológico seguro

Proteção tecnológica total é essencial para empresas de todos os portes





O que você deve saber? Ter uma SMB (Empresa de Pequeno ou Médio Porte)* significa dar conta de 100% dos seus próprios problemas de TI. A maioria das empresas de pequeno e médio porte sofrem carência de informações sobre como proteger sua empresa contra *vírus*, *hackers* e *spam*. Sabemos, por experiência própria, que as empresas de pequeno e médio porte estão enfrentando os mesmos desafios e necessidades.

Desafios

- Equipe de TI e conhecimento sobre a segurança interna limitados
- Os donos de empresas estão cada vez mais cientes das ameaças de *vírus* e *hackers*
- Orçamento limitado para segurança tecnológica

Necessidades

- Soluções de segurança comprovada. Fáceis de instalar e de manter atualizadas
- Soluções acessíveis e econômicas
- Proteção *proativa* do patrimônio da empresa, bem como: *arquivos*, *aplicativos* e *dados de clientes*
- Tempo de atividade e disponibilidade máximos da rede, do servidor e dos recursos de desktop



Algumas coisas que você precisa saber para proteger sua empresa

Nº1

Soluções para SMB não devem ser versões reduzidas das soluções para grandes empresas.

Uma mesma solução não serve para todas. Uma solução que serve para uma empresa global não é ideal para uma SMB. A sua empresa precisa de uma solução comprovada, criada com as suas necessidades em mente, tais como: tamanho, orçamento e desafios.

Aumentar a segurança de TI é um elemento essencial para a estratégia tecnológica de toda SMB.

Tentar gerenciar a sua empresa em era de sofisticadas ameaças virtuais sem uma segurança central ideal é o mesmo que dirigir um carro *sem seguro*—é preciso estar protegido todos os dias!

- Certifique-se de que suas soluções de segurança dão conta das vulnerabilidades da sua empresa
- Compreenda e implemente todos os recursos das suas soluções de segurança
- Mantenha-se informado sobre ameaças de segurança novas ou mutantes que possam vir a afetar sua empresa

Nº2

Uma boa proteção não precisa ser complicada.

Você precisa de uma solução simples de instalar e fácil de manter atualizada. O seu tempo deve ser dedicado ao sucesso da sua empresa, e não à proteção constante da rede.

- Crie ao menos uma política de segurança para a sua empresa treinando seus funcionários para aplicá-la corretamente
- Obtenha os *patches* de segurança mais recentes. Estes proporcionam a você a proteção mais atualizada
- Assine boletins informativos de segurança, notificações de atualização de *software*, *AVERT™ Virus News*, etc.
- Estabeleça práticas para o bom gerenciamento de senhas e contas

- Se não as estiver usando, desative-as!

Nº3

A proteção da segurança deve ser *proativa*, e não *reativa*.

O segredo é encontrar uma solução de segurança *proativa* que faça muito mais do que apenas detectar e reagir aos vírus.

A solução correta monitora constantemente toda a sua rede, gerencia políticas de segurança em todos os níveis e toma medidas para mantê-lo protegido contra *vírus* de última geração.

- Seu *software* de segurança deve ser fácil de gerenciar e de manter-se atualizado
- O sistema deve alertá-lo sobre problemas de segurança e ajudá-lo a resolvê-los facilmente
- O software de segurança deve ter um console de gerenciamento de fácil compreensão, até mesmo para os membros da equipe que não tenham conhecimento técnico

Nº4

Soluções econômicas não precisam significar proteção de baixa qualidade.

Nem sempre as empresas de pequeno e médio porte podem arcar com uma equipe de TI especializada, ou gastar o tempo e os recursos destinados a questões prioritárias críticas aos negócios para garantir a segurança da rede.

- A solução ideal se ajusta aos seus limites orçamentários sem sacrificar a qualidade da proteção
- Adquira uma *firewall* de perímetro
- Instale e use um *antivírus* para *desktop*. Procure soluções *proativas* na identificação e exclusão de vírus conhecidos e desconhecidos
- Proteção para *desktop* e servidor. Estabeleça critérios que protejam seus dados e aplicativos críticos aos negócios
- Conte com várias camadas de proteção: *antivírus*, *firewalls*, proteção de *email*, *anti-spam*, serviços gerenciados, e outros.





Nº5

Os usuários são os piores inimigos deles mesmos—sua rede está cada vez mais vulnerável.

Uma justificativa importante para a aquisição de segurança tecnológica em empresas de pequeno e médio porte é o crescente número de opções para conectividade remota a aplicativos de missão crítica. Isso tornou as SMBs mais conscientes e vulneráveis ao acesso não autorizado. Com uma solução de *detecção de invasão proativa* e baseada na rede, você pode bloquear ataques à rede, barrando as ameaças antes que elas possam entrar.

- Proteger os usuários remotos é um grande desafio. Geralmente, eles utilizam conexões com pouca largura de banda, são inacessíveis aos administradores da rede e seu *antivírus* pode não estar atualizado

- A infecção por vírus pode ocorrer sempre que um documento ou arquivo executável for transferido pelo *FTP* ou pelos arquivos compartilhados do usuário.

- Ameaças internas (*funcionários, por exemplo*) estão entre as principais fontes de atividade mal-intencionada

- Uma defesa verdadeiramente sólida exige ampla proteção integrada que abrange toda a sua empresa, chegando ao *desktop*

- Use um *firewall* como o *McAfee® Desktop Firewall™*

Nº6

Sua caixa de entrada é um risco em potencial.

A *Gartner Research*** afirma: “A ameaça à segurança mais provável de acontecer com empresas de pequeno e médio porte é um vírus

chegando por *email*”.

O ideal é identificar regras específicas aos negócios para serem aplicadas aos *emails* que entrarem na rede—determinando o que é seguro e o que é uma ameaça potencial, o que chegará ao usuário final e o que ficará em quarentena.

- Crie para os usuários finais uma política de uso do *email*

- Não compartilhe seu endereço de *email*

- Não abra *emails* de origem desconhecida

- Não clique duas vezes nos anexos, (a menos que você saiba do que se trata) não abra nenhum arquivo com extensão dupla (*hello.txt.vbs, por exemplo*)

- Proteja-se contra a *spam* com soluções como o *McAfee Security SpamKiller® powered by McAfee SpamAssassin™*—uma *suíte* de ofertas para proteger sua empresa do *desktop* ao *gateway*

Nº7

Sua caixa de saída é um risco em potencial.

Mensagens contendo comentários ofensivos sobre raça, sexo, idade, orientação sexual, pornografia, crenças religiosas ou políticas, origem nacional ou deficiência física, deixam sua empresa legalmente vulnerável. O vazamento de informações confidenciais sobre a empresa, os clientes ou os parceiros também impõem despesas e penalidades. Enviar um *email* é como enviar um cartão postal, ou seja, muitas pessoas podem lê-lo no caminho.

- Crie para os usuários finais uma política de uso do *email*
- Proteja-se contra conteúdo inadequado adicionando automaticamente uma mensagem de isenção de responsabilidade a todos os

emails de saída

- Previna-se contra mensagens e arquivos inapropriados, não solicitados ou *hostis* por meio de filtragem de conteúdo
- McAfee GroupShield®—oferece proteção abrangente contra conteúdo inadequado para seus servidores de *email*

Nº8

As ameaças mistas de hoje chegam a você rapidamente, se replicando e inundando a sua rede.

Elas combinam os piores aspectos dos *worms, vírus e cavalos de Tróia*, sendo complementadas com sofisticadas técnicas de invasão. Provavelmente, você nunca saberá o que o acertou. Tais ameaças se espalham tão rapidamente que podem interromper as atividades comerciais em questão de minutos. O ataque *Nimda*, que causou um prejuízo de pelo menos \$600 milhões***, tinha quatro métodos de propagação. Estima-se que, no futuro, os vírus sejam ainda mais prejudiciais.

- Monitorar uma rede é um grande desafio. Por natureza, a rede deve ser acessível a vários usuários, executando vários aplicativos simultaneamente; o monitoramento de tais atividades exige tempo e recursos significativos, bem como um programa de monitoramento *proativo*—e *não reativo*

- Certifique-se de que seus funcionários conheçam os perigos dos vírus e de outros arquivos mal intencionados e como eles podem afetar os negócios

- Configure o *antivírus* para varrer *emails, downloads* da *Internet, disquetes*, unidades *Zip* e *CD-ROMs* antes do uso



Soluções McAfee System Protection criadas para a sua empresa

- **McAfee SAV (Active VirusScan Suite) Small Business Edition**
- **McAfee AVD (Active Virus Defense Suite) Small Business Edition**—Proteção antivírus premiada, integrada e econômica, que abrange toda a rede e oferece atualizações automáticas
- **McAfee WebShield® e250 e e500**—Hardware e software integrados, que barram os vírus antes que eles entrem na rede
- **McAfee VirusScan® ASaP**—O único serviço antivírus 24x7 gerenciado, atualizado automaticamente todos os dias
- **McAfee Desktop Firewall**—Impede que clientes enviem ou recebam ameaças hostis de aplicativos não autorizados na rede, oferecendo recursos de firewall (abrangentes para a rede e seus aplicativos), combinados com a tecnologia de detecção de invasão
- **McAfee VirusScan**—Software antivírus líder para *desktop* da McAfee
- **McAfee SpamKiller powered by McAfee SpamAssassin**—Vem pronto para usar, detectando 95% do *spam* e o “barrando” antes que chegue aos usuários finais

Nº9

Os usuários finais baixam softwares não relacionados ao trabalho.

Proporcionar aos usuários finais privilégios para *download* em máquinas do local de trabalho podem deixar sua rede vulnerável a um ataque viral. Bloquear PCs com uma configuração segura, implementando um *firewall* em cada máquina, permitirá exposição mínima a aplicativos prejudiciais.

- Se seu funcionário não precisa de software para fins comerciais legítimos, não permita que ele seja carregado no computador
- Estabeleça políticas claras na empresa sobre o *download* de *música, pornografia, salas de bate-papo* ou *jogos*

Nº10

Você e a sua empresa são a espinha dorsal da economia.

Sua empresa e outras semelhantes impulsionam a economia nacional. Na verdade, as empresas de pequeno e médio porte formam a maioria das empresas dos EUA. O que difere a sua empresa das grandes corporações é que *a sua pode ser mais receptiva e flexível a mudanças tecnológicas*. Você tem a vantagem do *controle*, da *velocidade* e da *agilidade* ao seu lado quando toma decisões sobre tecnologia. Ao adaptar-se prontamente a mudanças na tecnologia e implementar as melhores práticas, você pode tornar-se inovadora no seu ramo.

- De acordo com um estudo da *Giga Information Group*†, o investimento nas Soluções *McAfee Network Protection* proporcionou às empresas um *ROI* positivo de até 145% em um período de três anos. O estudo revelou que as empresas que *usam o appliance* de prevenção contra invasão da *McAfee* economizaram 23% em custos de capital, 41% em custos operacionais e 33% em benefícios comerciais, de modo que a solução “é paga” em quatro meses.
- Aumente a segurança da empresa para aumentar sua lucratividade geral. Ter uma rede segura diminui suas chances de ser infectado por um vírus, assegura que você se mantenha em operação e que não haja inatividade do sistema interferindo em suas transações comerciais
- Você não precisa ser especialista em operações de rede para implementar medidas de segurança na rede da sua empresa. *Appliances* de segurança viáveis e efetivos estão disponíveis por meio de revendedores treinados para prestar consultoria e instalar o sistema necessário com o objetivo de proteger a sua empresa

* Considerando que empresas de pequeno porte tenham 100 funcionários ou menos, e empresas de médio porte, de 101 a 999 funcionários.

** Fonte: Computer Economics, Inc., uma empresa de pesquisa independente, em Carlsbad, Califórnia, que atende a 82% das empresas Fortune 500.

*** Fonte: Computer Economics, Inc., 4 de janeiro de 2003.

† Fonte: Giga Information Group (subsidiária da Forrester Research)—“The Total Economic Impact of IntruVert’s IntruShield® Intrusion Detection and Prevention” (O impacto econômico total dos recursos de detecção e prevenção do IntruShield® da IntruVert), maio de 2003.



McAfee Security 3965 Freedom Circle, Santa Clara, CA 95054. 888.VIRUSNO (888.847.8766)

Os produtos da Network Associates® contam com o respaldo de anos de experiência e comprometimento com a satisfação do cliente. Os membros da equipe da PrimeSupport® são técnicos de suporte atenciosos e altamente qualificados, os quais fornecem soluções personalizadas, oferecendo assistência técnica abrangente para o gerenciamento do sucesso de projetos de missão crítica, tudo com a qualidade de serviço que atende às necessidades de todas as empresas nossas clientes. A McAfee® Research, líder mundial em segurança e sistemas de informação, continua inovando no desenvolvimento e refinamento de todas as nossas tecnologias.

Network Associates, McAfee, AVERT, GroupShield, SpamKiller, powered by SpamAssassin, Desktop Firewall, Protection-in-Depth, IntruShield, WebShield, VirusScan e PrimeSupport são marcas comerciais, registradas ou não, da Network Associates, Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. Os produtos que levam a marca Sniffer são produzidos apenas pela Network Associates, Inc. Todas as outras marcas comerciais, registradas ou não, mencionadas neste documento pertencem exclusivamente a seus respectivos proprietários. ©2004 Networks Associates Technology, Inc. Todos os direitos reservados. 4-sps-smb-002-0204