



McAfee System Protection Solutions

## Gestão Eficiente de Soluções Antivírus e de Segurança para Pequenas Empresas

## Índice

Introdução – Tamanho importa?	3
Por que é importante gerenciar uma política de segurança?	3
O que significa “gerenciar”?	3
Se não for fácil de usar, não vai ser usado	3
Mantendo a atualização – O critério mais importante da segurança bem-sucedida	4
Camadas de proteção	4
A estratégia Protection-in-Depth da McAfee	4
Capacidade de planejar uma reação de segurança	5
Capacidade de reação	5
Disposição para investir	5
O panorama de gerenciamento da McAfee – três formas de gerenciar	5
Opções de gestão de segurança da McAfee	6
McAfee PrimeSupport	8
Resumo	8

## Introdução — Tamanho importa?

Quando se trata de defender redes contra vírus, hackers e outras ameaças, existem apenas duas categorias de usuários — os que possuem uma política de segurança de TI definida, implementada e gerenciada, e aqueles que não possuem.

Há boas razões pelas quais muitas empresas não possuem uma política de segurança de TI. Elas contam com mão-de-obra de segurança de TI limitada, e os recursos que possuem dedicam-se a conduzir suas operações comerciais. Em sua maioria, são empresas de pequeno e médio porte, e elas precisam de ajuda para lutar de maneira eficiente contra o esmagador número de ameaças que atacam suas redes. A maioria das grandes empresas certamente conta com equipes de TI e especialistas em segurança. A maioria das empresas de menor porte não conta com isso.

Mas em vez de dar atenção ao porte da empresa, é mais útil perguntar sobre a capacidade do usuário de reagir a uma ameaça à segurança. Assim, outra maneira de enxergar a necessidade de soluções de segurança é examinar a medida em que o cliente é capaz de definir, implementar e distribuir uma política de segurança. Ser especialista ou analfabeto em segurança. Existe ou não mão-de-obra especializada em segurança?

### Procura-se — Equipe de TI

Procuramos um super-homem para lidar instantaneamente com 50 mil ameaças à segurança ou mais. Você cuidará de aplicativos essenciais em todos os PCs e servidores. Ambiente sob constante ataque de terroristas cibernéticos. A proteção precisa ser atualizada semanalmente, mensalmente, ou imediatamente. Deve ser capaz de trabalhar com orçamentos apertados. Os relatórios diários ao CIO precisam apresentar 95% ou mais de usuários em conformidade com a política. Elimine a ameaça e entre os benefícios estarão folgas aos fins-de-semana. Pizza grátis aos domingos.

Vamos parar imediatamente e perguntar: *O que é uma política de segurança?* O mais simples é definir quais parâmetros de configuração devem ser aplicados ao mecanismo de atualização do firewall ou do antivírus para garantir que, em geral, o usuário esteja protegido e atualizado. O mais complexo é estabelecer regras sistemáticas divulgadas que valham para todos os aspectos do sistema de TI e da distribuição de dados, definir aplicativos aprovados pela empresa, controle de acesso e autenticação na rede, fornecedores aprovados, grupos ou domínios de usuários, as configurações de qualquer número de diferentes camadas de segurança, e assim por diante.

Se uma empresa precisa parar e perguntar *“O que é uma política de segurança?”*, o porte dessa empresa não faz diferença; ela não conseguirá implementar com sucesso uma solução de segurança que exija definições de gestão de políticas de segurança de TI plenamente desenvolvidas.

## Por que é importante gerenciar uma política de segurança?

Uma das dificuldades enfrentadas por qualquer empresa ao gerenciar a segurança dos seus sistemas e garantir proteção completa é que, para fiscalizar o cumprimento das políticas, o administrador precisa saber se há algum problema com a conformidade dos sistemas da empresa antes que eles possam ser colocados em conformidade.

Um único computador sem proteção adequadamente gerenciada pode constituir uma ameaça para toda a rede. Isso significa que conhecer todos os sistemas conectados à rede é essencial para proteger a empresa com sucesso.

Portanto, ter uma política de segurança é bom. Ser capaz de gerenciá-la é *melhor* ainda.

Novas ameaças afetam empresas de todos os portes. Os fornecedores têm o dever de levar ferramentas de gerenciamento fáceis de usar às empresas de menor porte para que elas possam reagir às ameaças de maneira tão eficiente quanto as empresas maiores.

## O que significa “gerenciar”?

No contexto da segurança de TI, o termo “gerenciamento” refere-se à capacidade de fiscalizar a conformidade dos usuários, distribuir atualizações, gerar relatórios de status e de exceções, além de manter a rede em boas condições de segurança — a partir de um ponto central — controlada por uma ou mais pessoas autorizadas.

Muitas soluções de segurança contam com certo grau de autonomia de gerenciamento incorporado. Todos os bons aplicativos antivírus contam com um processo automatizado de atualização de arquivos de detecção de vírus. Mas mesmo em redes de pequeno porte, isso é demorado e, em última análise, é impossível garantir o cumprimento uniforme das políticas se cada sistema possui o seu próprio mecanismo independente de atualização, sem qualquer mecanismo centralizado de controle. Basta que um único usuário fora de controle altere as configurações de um único PC da rede para expor toda a rede a ataques.

Portanto, gerenciar significa ter o controle centralizado de informações e ações para regular o uso de grupos de PCs em toda a rede.

## Se não for fácil de usar, não vai ser usado

Para empresários extremamente pressionados e gerentes de TI não-especializados de empresas menores, a facilidade de uso é um fator importante, assim como a exigência de adaptação em um cenário de ameaças que muda constantemente.

O dilema dos fornecedores é como colocar as funções necessárias em uma solução de segurança, equilibrando a facilidade de instalação, distribuição e manutenção diária dessas funções. A capacidade de mudar, adaptar ou atualizar é fundamental para qualquer solução de segurança, e é isso que separa essas soluções de outras soluções para escritório amplamente utilizadas. Por sua própria natureza, o cenário de segurança está em constante mudança. Portanto, a facilidade de uso não deve significar *“fácil de instalar, mas reprovado no teste de mudanças”*.

No ramo de segurança de TI, em que as novas ameaças exigem que as soluções de segurança mudem constantemente, existe um aspecto fundamental na condução bem-sucedida de uma política de segurança — a *capacidade de mudar* — a capacidade das empresas de definir suas políticas de segurança e implementar uma solução que execute essas políticas e permita que a reação das ameaças se adapte ao longo do tempo.

A mudança é um acontecimento de processo difícil para a maioria dos usuários. Empresas de grande porte definem padrões de Ambiente Operacional Comum (COE) para tentar possibilitar a gestão previsível da sua infra-estrutura de TI. Mas definir um COE que impossibilite a implementação ágil de atualizações de aplicativos de segurança no atual cenário de ameaças mutantes é a receita do fracasso.

Para as pequenas empresas, o conceito de mudança é difícil por razões diferentes. Primeiro, a necessidade de mudança muitas vezes não é compreendida. Todos sabem que os vírus são maus, mas em que momento da semana de trabalho média do gerente de uma pequena empresa ele tem a chance de examinar a situação atual das ameaças e efetuar mudanças na política de segurança da rede? Como ele pode descobrir qual porta deve ser bloqueada para impedir que um novo worm se espalhe? O que significa quando a Microsoft® divulga uma nova vulnerabilidade?

Novas ameaças exploram vulnerabilidades na extremidade e na margem, onde a defesa padrão implementada é, provavelmente, a menos bem-preparada para dar conta da ameaça. Como é possível que você se defenda contra uma ameaça que ainda não foi descoberta? Mesmo que uma nova ameaça seja descoberta, como é possível saber o que fazer para combatê-la?

A segurança de TI é um ambiente em constante evolução no qual ameaças, como códigos mal-intencionados (vírus, worms, spywares) e explorações de vulnerabilidades (ataques de negação de serviço, hacking, furto de dados) sempre desafiam os fornecedores de segurança a criar ferramentas cada vez mais sofisticadas para detectá-las, impedi-las e afastá-las.

### Mantendo a atualização — o critério mais importante da segurança bem-sucedida

Muitas empresas se concentram principalmente no mecanismo de atualização do seu software antivírus. Esse é um aspecto essencial da manutenção de uma postura defensiva sólida, mas não basta por si mesmo. Uma postura defensiva sólida exige várias camadas de defesa, além da capacidade de controlar a implementação, o ritmo, a distribuição e as informações dessas camadas de defesa. Em resumo, a capacidade de gerenciar o software escolhido para a proteção contra vírus é essencial.

### Camadas de proteção

Para que possamos definir uma abordagem em vários níveis, a maior parte das redes pode ser dividida nas seguintes categorias:

- PCs, servidores de arquivos e outros dispositivos clientes
- Servidores de aplicativos, como servidores de e-mail ou servidores de portal
- Gateways externos de Internet

Em cada categoria, a McAfee conta com várias soluções específicas antivírus e de segurança, no intuito de fornecer ao cliente o que há de melhor em soluções para o nível de aplicativos. Isso não difere do objetivo de outros fabricantes, e o cliente se beneficia da natureza altamente competitiva do ramo e dos desafios lançados pelos criadores de programas mal-intencionados, em termos de inovação e aprimoramento constante de recursos para cada aplicativo.

### A estratégia Protection-in-Depth da McAfee

A McAfee® possui uma estratégia de reunir todas as suas soluções em uma estrutura única chamada Estratégia Protection-in-Depth™. Essa estratégia permite que os clientes tenham acesso a uma gama de produtos de segurança em vários níveis e para várias plataformas e possam impedir com sucesso as invasões, limitar o impacto dos ataques e reduzir o custo das operações de limpeza.

A implementação bem-sucedida de um sistema de defesa de segurança passa essencialmente pela gestão de políticas e da conformidade dos aplicativos. No mundo das pequenas empresas, isso se traduz na gestão antivírus.



Estratégia Protection-in-Depth da McAfee.

### Capacidade de planejar uma reação de segurança

Vírus, worms e outras formas de programas mal-intencionados não fazem distinção. Eles infectam ou se proliferam onde quer que exista uma oportunidade, através de vulnerabilidades comuns de engenharia social (usuários) ou de defesa de sistemas (profissionais de TI).

As pessoas e empresas mais afetadas são aquelas cujas defesas são as mais fracas. O fato de que os vírus são uma ameaça é claro para empresas de todos os portes e segmentos, mas os meios para fazer algo no sentido de defender-se contra os vírus com algo além de aplicativos antivírus básicos variam enormemente de acordo com as características da empresa ou do usuário.

Pequenas empresas tendem a contar com menos mão-de-obra especializada de TI e estão menos preparadas para estabelecer uma defesa bem-sucedida contra programas mal-intencionados ou invasões. Elas podem ter a capacidade técnica de implementar uma política de segurança de TI, mas não contam com os profissionais especializados para tanto.

Muitas vezes, os fabricantes do ramo de TI caracterizam seus clientes referindo-se ao seu porte como empresas, normalmente dividido em pequeno, médio ou grande. Isso não ajuda muito, especialmente quando se tenta relacionar as soluções de segurança com os clientes. Na realidade, há apenas dois tipos de clientes em termos de segurança — aqueles que contam com profissionais ou recursos de TI e aqueles que não contam — ou seja, especialistas em TI e analfabetos em TI.

### Capacidade de reação

*Todos os meus usuários estão protegidos?*

*Todos os meus usuários estão atualizados?*

Se a resposta a qualquer uma das perguntas acima for “eu não sei”, então temos um problema de gerenciamento. Existe uma falha no processo de gerenciamento que significa, muito provavelmente, que um ataque ou uma epidemia de vírus poderão atingir seus objetivos.

A questão toda é o gerenciamento de recursos. A incapacidade de gerenciar a conformidade dos usuários, o processo de atualização ou o processo de backup abre as portas para que o cliente sofra danos por meio de infecções ou invasões.

Alguns clientes simplesmente não são capazes de reagir. Isso não significa que eles sejam maus clientes, mas simplesmente que eles precisam de ajuda para reagir. Muitas vezes, eles simplesmente não sabem que precisam reagir.

### Disposição para investir

De um jeito ou de outro, tudo se resume em investimento — assim como todas as decisões gerenciais — ou se investe

em recursos próprios ou se delega a tarefa para um fornecedor externo. Investimentos desse tipo sempre precisarão se enquadrar em restrições, mas é possível obter grandes retornos até mesmo de investimentos modestos.

No ramo de segurança de TI, todos os clientes têm a seu favor um cenário extremamente competitivo de fornecedores, pois eles lutam para fazer melhor pelos seus clientes e, é claro, conquistar clientes dos outros fornecedores.

Não é apenas o preço que beneficia o cliente. A riqueza de funções, a facilidade de uso e a qualidade do suporte também são aspectos essenciais de uma solução, e cada nova versão vem com alguma novidade para o usuário.

### O panorama de gerenciamento da McAfee — três formas de gerenciar

A gama de opções de gerenciamento da McAfee permite que as empresas decidam se investirão em ferramentas que possam ser gerenciadas sem intervenção — mais adequadas para empresas que contam com alguma ou bastante mão-de-obra especializada em TI — ou se é melhor delegar a dor de cabeça às soluções gerenciadas de serviços especialmente reunidas pela McAfee e dedicar seu tempo a administrar os negócios enquanto a McAfee administra a política de segurança.

1. Processo de gerenciamento terceirizado
2. Simplificado, gerenciamento sem intervenção
3. Grande porte, gerenciamento sem intervenção

O objetivo é garantir, independentemente da abundância ou da escassez de profissionais ou recursos de segurança de TI do cliente, que o cliente tenha a certeza de que suas defesas estarão em um estado de prontidão ideal.

A principal diferença entre o simples e o sofisticado é a gama de outras opções de gerenciamento disponíveis. O parâmetro básico é a capacidade de manter ao menos um conjunto válido de configurações de segurança (política) para que o aplicativo antivírus, o firewall e a solução de prevenção contra invasões estejam sempre funcionando para todos os usuários a qualquer momento.

Em um mundo ideal, todas as ameaças podem ser gerenciadas por uma única solução, de uma forma adequada a todos os tipos de usuários. Mas não vivemos em um mundo ideal. A experiência da McAfee com empresas que usam o ePolicy Orchestrator® para gerenciar uma infra-estrutura de grande porte é que não existe um “tamanho único”. Empresas menores precisam de um conjunto diferentes de parâmetros para atingir 98% das mesmas metas, mas com uma estrutura simplificada de políticas. Há vários anos, a McAfee vem operando suas soluções gerenciadas antivírus e de firewall para auxiliar empresas menores a atingir essa meta e, há pouco tempo, lançou um console de gerenciamento dedicado para pequenas e médias empresas, o McAfee ProtectionPilot™, para empresas que preferem gerenciar por si mesmas sua instalação antivírus.

## Opções de gestão de segurança da McAfee

### Delegue o processo de gerenciamento

- **Serviços Gerenciados da McAfee** — Os Serviços Gerenciados da McAfee oferecem soluções antivírus automáticas e sempre ativas que são gerenciadas 24 horas por dia pelos especialistas da McAfee.
  - **Público-alvo** — Empresas que não possuem a mão-de-obra ou não querem gerenciar suas configurações de antivírus ou de firewall; provavelmente, entre 2 e mais de 100 usuários.
- **Necessidades do cliente**
  - o Simplicidade de instalação
  - o Atualizações automáticas
  - o Geração simples de relatórios por um painel de controle
  - o Política única de segurança

A maior vantagem de implementar um dos serviços gerenciados da McAfee é a transferência das decisões de gerenciamento para um corpo de especialistas. Para muitas empresas menores, o serviço McAfee Managed VirusScan® é uma solução antivírus imperceptível e eficiente que é atualizada automaticamente pelo menos uma vez por semana, ou com maior frequência, conforme a situação exija. O usuário não precisa tomar nenhuma decisão sobre o nível de risco de uma determinada ameaça. A McAfee cuida de todas as decisões sobre atualização. Entretanto, o usuário é capaz de ver a situação de conformidade de todos os usuários pela interface gráfica do painel de controle.



Relatório do McAfee Managed VirusScan.

- **Simplificado, gerenciamento sem intervenção (com o McAfee ProtectionPilot)**
  - **Público-alvo** — Pequenas e médias empresas que desejam gerenciar suas próprias defesas antivírus, mas que contam com pouca mão-de-obra especializada em segurança de TI ou que possuem uma política simples de segurança de TI; normalmente, são empresas que possuem de 25 a 250 usuários
- **Necessidades do cliente**
  - o Simplicidade de implementação
  - o Configuração e gestão de tarefas com orientação
  - o Aplicação automática de atualizações
  - o Geração simples de relatórios por um painel de controle
  - o Capacidade de controlar e personalizar a política de segurança

O ProtectionPilot é uma ferramenta de gerenciamento centralizado de segurança que permite uma abordagem simples e proativa da implementação e do gerenciamento contínuo da proteção antivírus, para administradores de rede que gerenciam até 500 computadores. O assistente de instalação garante a simplicidade e a clareza do caminho até a proteção, e as atualizações automáticas começam imediatamente.

Para empresas que contam com alguma mão-de-obra especializada de TI, o ProtectionPilot apresenta opções de tarefas que são intuitivas e guiadas por assistentes, permitindo que os administradores implementem e gerenciem uma política de segurança fiscalizada automaticamente para seus usuários. Essa forma de defesa gerenciada sem intervenção é viável e eficiente para empresas com pouca mão-de-obra especializada de TI, pois todo o etos de facilidade de uso do projeto do ProtectionPilot conta com o respaldo de anos de experiência em oferecer facilidade de gerenciamento para empresas de grande porte. O resultado é uma ampla gama de funções de controle e informação de antivírus que atendem às necessidades dos clientes, sem comprometer o rigor da conformidade em toda a rede.

Onde outros fornecedores esperam que o usuário se arraste por intermináveis relatórios, a McAfee facilita a visão de problemas de conformidade pelo painel de controle de relatórios. Quando são incluídos novos computadores, a McAfee facilita o trabalho, permitindo que eles sejam arrastados para dentro do domínio gerenciado. Quando usuários fora de controle ou colegas bem-intencionados decidem *ajustar* as opções de varredura antivírus, o ProtectionPilot automaticamente impõe a configuração correta novamente ao sistema do usuário. Quando a McAfee publica um conjunto atualizado de arquivos de características de detecção de vírus (DAT), o ProtectionPilot os acessa automaticamente e atualiza todos os usuários da rede.

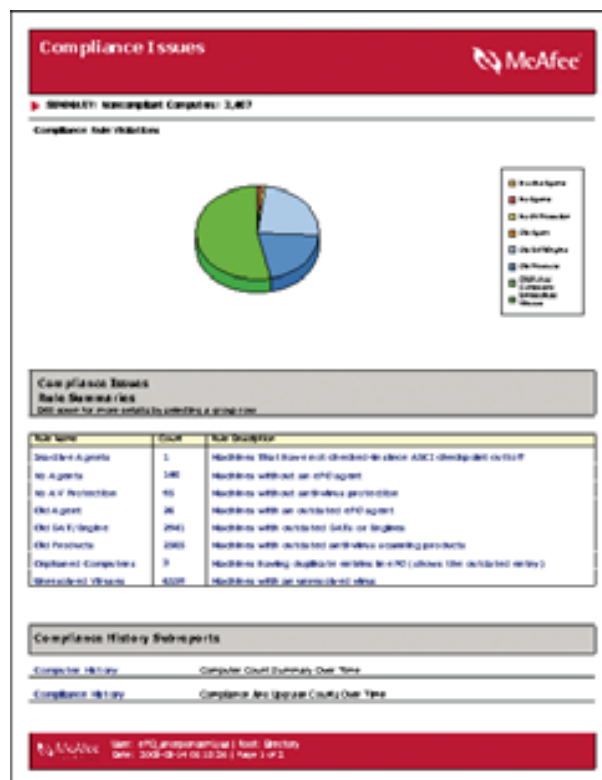


Painel de controle do McAfee ProtectionPilot.

- Grande porte, gerenciamento sem intervenção (com o ePolicy Orchestrator)
  - Público-alvo — Empresas de médio a grande porte que desejam implementar um console abrangente e flexível de gerenciamento de políticas de segurança e antivírus; adequado para empresas de médio a grande porte.
- Necessidades do cliente
  - o Capacidade de centralização da distribuição
  - o Transmissões de pacotes com economia de largura de banda
  - o Repositórios distribuídos
  - o Estruturas hierárquicas de geração de relatórios
  - o Vários domínios gerenciados
  - o Detecção de sistemas fora de controle
  - o Estabelecimento do perfil de conformidade dos sistemas
  - o Relatórios personalizáveis de conformidade e infecção
  - o Vários idiomas permitidos em um único domínio
  - o Aceitação de aplicativos de vários fabricantes

O ePolicy Orchestrator é a solução líder de mercado em gestão de segurança de sistemas, oferecendo à empresa uma defesa coordenada e proativa contra ameaças e ataques. Permitindo um gerenciamento abrangente e incomparável da segurança dos sistemas ao menor custo de propriedade, ele garante a conformidade com a política de segurança de sistemas e a eficiência da proteção dos computadores, evitando as dispendiosas interrupções de negócios causadas por infecções de programas mal-intencionados e outros ataques. Com o eixo central da McAfee System Protection Solutions, os administradores podem tomar a iniciativa de reduzir o risco de sistemas fora de controle e não-conformes, manter a proteção atualizada, configurar e fiscalizar as políticas de proteção, além de monitorar o status de segurança, 24 horas por dia, 7 dias por semana, com um único console centralizado e verdadeiramente flexível para acompanhar qualquer tamanho de infra-estrutura.

Há mais de quatro anos, o ePolicy Orchestrator estabeleceu-se como console líder em conformidade de sistemas e gestão de segurança no ramo de segurança de TI. Muitos fabricantes possuem recursos de registro de eventos ou geração de relatórios, mas poucos permitem que se tomem medidas para executar ações corretivas em uma gama tão grande de aplicativos, afetando muito pouco a velocidade da rede e apresentando tanta flexibilidade.



Relatório do McAfee ePolicy Orchestrator.

A abordagem de painel de controle do ProtectionPilot é substituída por um ambiente gráfico completo, comandado por menus, de geração de relatórios. Os usuários fora de controle são identificados, enquanto diferentes políticas de segurança podem ser definidas e aplicadas a uma ampla gama de grupos de usuários e domínios. O ePolicy Orchestrator coloca o responsável pela segurança de TI no controle da implementação da política de segurança da empresa, permitindo que seja atingida uma conformidade demonstrável.

### McAfee PrimeSupport

A McAfee tem adotado a estratégia de fornecer tecnologia de primeira classe para cada tipo de aplicativo de gestão de desempenho e segurança — mas, hoje, a Estratégia Protection-in-Depth é mais do que apenas distribuir e implementar as melhores soluções. 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 suíte 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.

### Resumo

Uma política simples de segurança que seja fácil de gerenciar será sempre mais eficiente que uma política sofisticada que seja impossível de gerenciar. Talvez o fato mais importante seja que uma política de segurança simples é muito melhor que nenhuma. Os clientes podem recorrer à McAfee para encontrar soluções de gerenciamento de políticas em ambas as extremidades do espectro, de acordo com a sua capacidade de gerenciamento ou com as necessidades da sua infraestrutura de TI. As opções de gestão de segurança da McAfee permitem que os clientes implementem as políticas de segurança de TI mais eficientes e apropriadas. Isso significa que eles podem manter o controle da segurança das suas redes, sem forçar sua equipe de TI além do limite. A McAfee significa opções de gerenciamento.