

# McAfee ePolicy Orchestrator 3.5

## Gerencie Centralmente a Sua Segurança de Sistemas

Os sistemas conectados em rede precisam de vigilância constante contra ameaças e ataques — que estão sempre por aí, testando as defesas e sondando os pontos fracos. Por causa disso, o trabalho do administrador é um delicado ato de equilíbrio. De um lado estão as exigências dos negócios — gerenciar um variado e cada vez maior número de dispositivos, bem como atender às necessidades de um número crescente de usuários móveis. Do outro lado estão as exigências de segurança — manter os seus sistemas em conformidade e gerenciar vários níveis de proteção de última geração e as ferramentas necessárias para combater as ameaças de hoje que estão em constante evolução.

É essencial poder ver completamente a segurança do seu sistema e fiscalizar o que já está implementado. Em última análise, cada uma dessas exigências é constante e igual. Basta um escorregão, e todo o seu universo pode ser atirado em completo desequilíbrio.

O McAfee® ePolicy Orchestrator® 3.5 (ePO™) é a solução de gerenciamento de segurança de sistemas líder de mercado — proporcionando uma defesa preventiva coordenada contra ameaças e ataques à empresa. Como núcleo das soluções de Proteção de Sistemas da McAfee, os administradores podem reduzir o risco dos sistemas desprotegidos e não-conformes, manter a proteção atualizada, configurar e fiscalizar políticas de proteção e monitorar o status de segurança, 24/7, a partir de um único console centralizado que realmente pode ser estendido a toda a empresa.

### Reduza o risco dos sistemas desprotegidos e não-conformes

A redução dos pontos fracos atacáveis deve ser uma das principais prioridades de todas as equipes de segurança. Um único sistema desconhecido que não possui uma proteção gerenciada adequada representa uma ameaça considerável a toda a rede — constante reinfeção por ameaças conhecidas, a introdução de novas vulnerabilidades, alvos potenciais de ameaças, ou pontos de propagação, tudo isso são os sintomas e os riscos de se ter sistemas desprotegidos. Portanto, o conhecimento de todos os sistemas que se conectam à rede é essencial para a proteção bem-sucedida da empresa.

O problema dos sistemas desprotegidos é ainda mais agravado pelo fato de que, na maioria das redes, o único requisito de entrada é o acesso físico. Contratados, funcionários terceirizados, visitantes de salas de conferência, ou simplesmente sistemas esquecidos, todos têm a mesma oportunidade de se conectar à rede corporativa e representar, sem intenção, uma ameaça considerável à integridade e à disponibilidade da rede.

O ePO 3.5 tem uma abordagem exclusiva de redução dos riscos de sistemas desprotegidos e não-conformes. Utilizando sensores distribuídos, o ePO 3.5 monitora passivamente a rede em busca de qualquer conexão de LAN, determinando rapidamente se elas estão sendo gerenciadas pelo ePO 3.5 e reagindo, de acordo com diversas políticas, a sistemas desprotegidos que não estão gerenciados pelo ePO 3.5. Por intermédio da identificação ágil dos sistemas não-gerenciados, os administradores podem melhorar consideravelmente a conformidade de segurança dos sistemas e reduzir o ponto fraco representado por sistemas desprotegidos e não-conformes.

### Monitore a segurança do sistema 24/7

Os serviços integrados de notificação e os relatórios gráficos do ePO 3.5 proporcionam a visibilidade ininterrupta necessária ao monitoramento eficiente da segurança do sistema, à avaliação do status da sua política e à descoberta dos pontos fracos da sua rede.

Informações instantâneas e preventivas são fundamentais para um profissional de segurança, especialmente no monitoramento da conformidade e da atividade de ameaças. O ePO 3.5 conta com alertas e notificação integrados em relação a conformidade, atividade de ameaças e sistemas desprotegidos. Os limites, definidos pelo administrador, permitem o envio de alertas críticos a pessoas específicas por meio de e-mail, SMS, pager alfanumérico ou capturas de SNMP. Os alertas avisam sobre atividades de ameaças, níveis de conformidade do antivírus e detecção de sistemas desprotegidos.

Além disso, localizar sistemas não-conformes, rastrear uma epidemia até a sua fonte, ou determinar a eficácia das políticas de segurança não requerem nenhum esforço com a ampla gama de mais de 40 relatórios predefinidos do ePO 3.5. Desde resumos executivos de segurança em uma página até informações detalhadas sobre a política antivírus e a atividade de vírus, sobre a política de firewall de desktop, as vulnerabilidades do sistema e as políticas anti-spam e de filtragem de conteúdo, todas as informações estão nas suas mãos. A personalização dos relatórios de acordo com as suas necessidades específicas também é muito fácil. Os administradores podem escolher entre vários tipos de gráficos imprimíveis e exportáveis, inclusive gráficos tridimensionais de barra, "pizza", de linha e tabelas. O ePO 3.5 é integrado à tecnologia Crystal Reports da Business Objects® e ao servidor Microsoft® MSDE/SQL para equilibrar simplicidade e riqueza de recursos, atendendo às necessidades de empresas de qualquer porte.

### Fiscalize a Conformidade da Proteção e as Atualizações

Um dos aspectos mais difíceis do gerenciamento preventivo de uma política de segurança é manter todos os sistemas com as proteções mais recentes. O ePO 3.5 garante a conformidade de toda a empresa por meio da fiscalização automática de políticas, impedindo que os sistemas saiam de conformidade e que os usuários finais alterem configurações ou desativem proteções essenciais.

O ePO 3.5 é fundamental para a gestão eficiente do processo de atualização. As atualizações podem ser programadas pelos administradores para serem realizadas a intervalos regulares, podendo ser estabelecidas por sistema ou por grupo, além de outros métodos definidos pelo administrador. Ele usa um projeto inteligente de repositórios distribuídos que tira totalmente do servidor a carga das atualizações, distribuindo

as atualizações por toda a rede, mantendo o tráfego da rede em níveis baixos e a velocidade em níveis altos. Além disso, ele é abrangente, capaz de distribuir atualizações de todos os DATs, *engines*, *service packs*, *hotfixes* e patches da McAfee.

## Avalie preventivamente a atualização dos patches da Microsoft

Com o ePO 3.5, tomar medidas preventivas de redução das vulnerabilidades do sistema e medir a eficácia da distribuição dos seus patches são tarefas simples e diretas. O System Compliance Profiler (SCP) é um componente que integra o ePO 3.5, permitindo que os profissionais de segurança avaliem rapidamente a conformidade dos sistemas de toda a empresa, inclusive a presença de patches de segurança essenciais da Microsoft. O estabelecimento de perfis é baseado em regras, que podem ser personalizadas pelo administrador, em modelos baixados da McAfee, pesquisando um arquivo, um serviço, uma chave de registro ou uma referência a um determinado patch da Microsoft. A *tomada de impressões digitais* da Microsoft (que utiliza códigos de *hash MD5*) também está disponível para garantir a absoluta integridade dos patches de segurança da Microsoft e para impedir a falsificação de patches. A criticidade da conformidade é estabelecida pelo administrador, sendo facilmente monitorada na forma de relatórios gráficos detalhados de conformidade.

## Reaja rapidamente a epidemias

Para reagir com eficiência a epidemias o ePO 3.5 é fundamental, proporcionando aos administradores os meios para adequar uma reação a uma ameaça específica. Em emergências nas quais você precisa de atualização imediata em todas as suas máquinas, o servidor pode exigir que todos os agentes *atualizem já* e aplicar a alteração em toda a rede. Por outro lado, a epidemia pode exigir que a política seja alterada no firewall do sistema, ou pode exigir apenas uma atualização de política no gateway. Com o ePO 3.5, a sua reação será imediata e concentradíssima na tarefa em questão.

A Atualização Global Expressa garante uma atualização rápida em toda a empresa — até 50 mil sistemas em no máximo uma hora — todos verificados com os poderosos recursos de geração de relatórios do ePO 3.5. A distribuição pela rede global garante o uso eficiente da largura de banda, aumentando muito a capacidade de reagir a ameaças novas e que surgiram recentemente.

## Proteja os usuários móveis

Com o ePO 3.5, *funcionário móvel* não precisa ser uma expressão assustadora para a equipe de segurança. Fiscalizando as políticas mesmo quando o laptop não está conectado à rede, e aplicando as atualizações sempre que uma conexão à Internet for detectada, o ePO 3.5 gerencia de maneira eficaz a sua infra-estrutura não-gerenciável. E como os usuários móveis e remotos exigem mais flexibilidade, o ePO 3.5 distribui a eles automaticamente as atualizações a partir do repositório mais próximo e que consome menos largura de banda, permitindo, além disso, atualizações adiáveis e reiniciáveis. Em última análise, o ePO 3.5 garante que os seus usuários remotos e móveis fiquem tão bem protegidos e sejam tão fáceis de gerenciar quanto os que se conectam pela rede local.

## Facilidade de gerenciamento de toda a empresa

Os produtos da McAfee® denotam anos de experiência e compromisso com a satisfação do cliente. A equipe McAfee PrimeSupport® de técnicos de suporte atenciosos e altamente qualificados oferece soluções sob medida e assistência técnica detalhada para gerenciar o sucesso de projetos essenciais — tudo com níveis de serviço que atendem às necessidades de cada um dos nossos clientes. A McAfee Research, líder mundial em pesquisa de sistemas de informação e segurança, continua na vanguarda da inovação no desenvolvimento e no refinamento de todas as nossas tecnologias.

McAfee, ePolicy Orchestrator, ePO, e PrimeSupport são marcas comerciais, registradas ou não, da McAfee, Inc. e/ou de suas afiliadas nos EUA e/ou em outros países. A cor vermelha usada para identificar a segurança é traço distintivo 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 Network Associates Technology, Inc. Todos os direitos reservados.

O ePO 3.5 foi criado levando em conta a flexibilidade para a empresa, gerenciando até 250 mil usuários por servidor, podendo ser operado facilmente em qualquer lugar, por intermédio de um console remoto, poupando à sua empresa os custos de mais hardware e gerenciamento. As políticas que abrangem todos os níveis de proteção contra ameaças — da frequência de atualizações até as configurações do firewall pessoal, a avaliação de patches, os tipos de arquivos que devem ser varridos, as configurações de varredura heurística — podem ser definidas de maneira centralizada por máquina ou por grupo, sendo totalmente personalizáveis pelo administrador. Todas elas são fiscalizadas automaticamente para garantir uma proteção sólida.

Precisa gerenciar a proteção em mais de um idioma? Sem problema. Quer gerenciar produtos antivírus que você já possui além dos atuais aplicativos de segurança? Fácil. Precisa que administradores diferentes gerenciem partes diferentes da sua rede? Está feito. Tem servidores de arquivos Windows®, Linux e NetWare? Moleza. Quer integração com o Microsoft Active Directory? Sem problema. Quer incluir firewalls de sistema e prevenção de invasões? Simples. O ePO 3.5 cuida de tudo isso com facilidade.

## Integração com investimentos essenciais em infra-estrutura

Projetado levando em conta a eficiência administrativa, o ePO 3.5 se concentra no aproveitamento de investimentos essenciais no Microsoft Active Directory (AD), garantindo a simplicidade do controle de modificações e a uniformidade de diretórios em toda a empresa. A integração com o Microsoft AD permite a importação programada de sistemas do AD para o diretório do ePO 3.5, além de, quando for o caso, permitir o espelhamento de agrupamentos do AD no diretório do ePO 3.5.

## Reduza os custos operacionais e de infra-estrutura

O ePO 3.5 ajuda você a consolidar os seus fornecedores de segurança, integra-se à sua infra-estrutura de rede e segurança e reduz os custos operacionais e de capital, por meio de uma única abordagem centralizada de gestão da segurança de sistemas.

## Duas perguntas importantes

Na luta contra os códigos mal-intencionados, há muitas perguntas que você pode fazer, mas somente duas é que importam: *Estamos protegidos? e: Estamos infectados?* O ePO 3.5 pode responder a ambas — garantindo que a sua proteção esteja pronta, com a verificação e exibição dos seus pontos de conexão.

## Requisitos do sistema

Para obter informações sobre os requisitos do sistema, consulte a *data sheet* de Requisitos do Sistema.