

# McAfee ePolicy Orchestrator

## Obtenha, visualize, compartilhe e tome decisões com base em insights de segurança, de maneira centralizada

O gerenciamento de segurança requer malabarismos incômodos entre ferramentas e dados. Isso dá ao adversário a vantagem de ter mais tempo para explorar brechas ainda não identificadas entre as ferramentas e causar danos. Além disso, a mão de obra da segurança cibernética é limitada e precisa ser instrumentalizada para gerenciar a complexidade da segurança cibernética. A plataforma de gerenciamento McAfee® ePolicy Orchestrator® (McAfee ePO™) elimina o trabalho demorado e potencialmente sujeito a erro humano e inspira os responsáveis a gerenciar a segurança com mais rapidez e eficácia.

### Segurança fundamental

Comece com os fundamentos. No centro de qualquer arquitetura de segurança está a capacidade de monitorar e controlar a saúde de endpoints e sistemas. Padrões industriais, como os controles do **CIS** (Center for Internet Security) e os controles de segurança e privacidade **SP 800-53 do NIST** (National Institute of Standards Technology), ressaltam essa necessidade. O console do McAfee ePO permite obter visibilidade crítica e estabelecer e impôr políticas automaticamente para garantir uma postura de segurança saudável por toda a sua empresa. O gerenciamento e a imposição de políticas nos produtos de segurança de toda a sua empresa é conseguido a partir de um único console, eliminando a complexidade do gerenciamento de vários produtos. Essa segurança essencial é fundamental para a sua conformidade de segurança de TI.

### Gerenciamento de segurança avançado e comprovado

Mais de 30.000 empresas e organizações contam com o console do McAfee ePO para gerenciar a segurança, simplificar e automatizar processos de conformidade e aumentar a visibilidade geral sobre endpoints, redes e operações de segurança. As empresas de grande porte contam com a arquitetura altamente expansível do console do McAfee ePO, que permite às grandes corporações gerenciar centenas e milhares de nós a partir de um único console. O console do McAfee ePO oferece ao administrador de segurança corporativa a oportunidade de simplificar a manutenção de políticas, incorporar inteligência contra ameaças de terceiros aproveitando o Data Exchange Layer (DXL) e integrar bidirecionalmente políticas com uma gama de produtos.

Conecte-se conosco



## DATA SHEET

Essas eficiências operacionais reduzem a sobrecarga do compartilhamento de dados e processos, possibilitando uma resposta mais rápida e mais precisa.

### Eficiência contra o espalhamento desordenado

Uma pesquisa da ESG mostra que 40% das organizações utilizam de 10 a 25 ferramentas, enquanto 30% utilizam de 26 a 50 ferramentas para gerenciar bilhões de novas ameaças e dispositivos. Essa diversidade de uso de produtos gera complexidade e multiplica a vantagem operacional de uma experiência de gerenciamento unificado, da instalação à geração de relatórios. A McAfee acolhe essas exigências com uma abordagem “Together is power” (juntos somos fortes) para o gerenciamento da segurança, que permite consolidar o espalhamento com proteção da amplitude dos seus ativos, suporte para inteligência contra ameaças, gerenciamento de dados de código aberto e integração de produtos de terceiros. A McAfee oferece comando e controle centralizados para fins de conformidade e gerenciamento em uma variedade de produtos de segurança. Você pode alternar rapidamente entre produtos para localizar os dados críticos e tomar as providências necessárias em termos de política. O console do McAfee ePO também permite investir em tecnologias de próxima geração e integrá-las com os ativos existentes dentro de uma mesma estrutura de trabalho.

### Exemplo de lista de produtos gerenciados pelo McAfee ePO

Produtos da McAfee	Produtos de terceiros
McAfee Endpoint Protection (prevenção de ameaças, firewall e controle de Web)	Guidance Software: enCase Enterprise
McAfee Drive Encryption	Avecto: Privilege Guard
McAfee File and Removable Media Protection	AccessData: AccessData Enterprise
McAfee Active Response	Autonomic Software: Power Manager, Patch Manager
McAfee Management for Optimized Virtual Environments (McAfee MOVE)	Xerox MFP
McAfee Data Loss Prevention (McAfee DLP)	DXL
McAfee Policy Auditor	
McAfee Enterprise Security Manager	
McAfee Threat Intelligence Exchange	
McAfee Application Control	
McAfee Cloud Workload Security	
McAfee Advanced Threat Defense	
McAfee Content Security Reporter	
McAfee Database Activity Monitoring	

## DATA SHEET

### Exemplos de casos de uso: como o console do McAfee ePO permite o gerenciamento centralizado de produtos de segurança

Produto e tecnologia	Exemplo de caso de uso de gerenciamento centralizado	Benefício
McAfee ePO McAfee Endpoint Security	O McAfee Endpoint Security descobre um arquivo malicioso conhecido em um endpoint. O console do McAfee ePO estabelece uma política mais rigorosa para o endpoint e o coloca em quarentena. Isso é feito em uma única interface de gerenciamento comum.	Contenção rápida de um endpoint comprometido
McAfee ePO McAfee DLP McAfee Enterprise Security Manager	O McAfee Enterprise Security Manager detecta um vazamento de dados significativo em um endpoint e o marca no console do McAfee ePO. O console do McAfee ePO aplica políticas de proteção contra perda de dados para bloquear os dados e avisa o usuário sobre a falta de conformidade.	Imposição automática da política contra perda de dados

### Exemplos de integração

Produto e tecnologia	Caso de uso integrado	Benefício
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	O McAfee Endpoint Security sinaliza um host suspeito. O console do McAfee ePO pode acionar varreduras adicionais. Isso é transmitido ao Cisco ISE via PxGrid e pelo intercâmbio DXL (o console do McAfee ePO). O Cisco ISE pode isolar o host até que ele seja considerado aceitável.	Maior proteção proativa
Avecto Defendpoint McAfee ePO DXL McAfee Threat Intelligence Exchange	Distribuição e gerenciamento da solução Avecto Defendpoint, líder em gerenciamento de privilégios, a partir do McAfee ePO. As alterações de configuração do Avecto Defendpoint são feitas com base em dados de reputação de aplicativos do McAfee Threat Intelligence Exchange.	Redução de complexidade Nenhuma infraestrutura adicional e redução do custo total de propriedade Alterações de acesso privilegiado tomadas com base na inteligência contra ameaças
Rapid7 Nexpose McAfee ePO DXL	O McAfee ePO compartilha a lista de ativos com o Nexpose. Isso permite que você compreenda a postura de risco a partir do console do McAfee ePO e possa definir a política de acordo com a necessidade. Dados de vulnerabilidade são compartilhados com a comunidade de fornecedores de DXL.	Redução da complexidade Obtenção de uma postura abrangente e confiável e priorização de ações para minimizar o risco a partir de um único dashboard
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	Essa integração viabiliza o compartilhamento bidirecional e em tempo real de inteligência entre a rede e endpoints. Os eventos são compartilhados com a comunidade de DXL.	Redução do tempo de detecção Bloqueio e correção dos ataques

## DATA SHEET

As organizações com plataformas integradas são melhor protegidas e obtêm respostas mais rápidas do que as que não dispõem de plataformas integradas.

	Organizações integradas	Organizações não integradas
Sofreram menos que cinco violações no ano passado	78%	55%
Descobriram ameaças em oito horas	80%	54%

2016 Penn Schoen Berland

### Fluxos de trabalho extensíveis simplificam processos

O banco de dados do McAfee ePO proporciona capacidades automatizadas e versáteis de gerenciamento para que você possa identificar, gerenciar e responder rapidamente a vulnerabilidades, mudanças nas posturas de segurança e ameaças conhecidas, a partir de um único console. Você define como o console do McAfee ePO deve direcionar alertas e respostas de segurança com base no tipo e na gravidade dos eventos de segurança para o seu ambiente e as suas políticas e ferramentas. Como suporte às operações de desenvolvimento e segurança, a plataforma do McAfee ePO permite criar fluxos de trabalho automatizados entre os seus sistemas de segurança e operações de TI para corrigir rapidamente os problemas. Use o console do McAfee ePO para desencadear ações de correção pelos seus sistemas de operações de TI, por exemplo, atribuir políticas mais rigorosas. O aproveitamento de suas interfaces de programação de aplicativos (APIs) para a Web reduz o trabalho manual.

### Casos de uso comuns

- Poupe tempo e elimine tarefas redundantes ou trabalhosas agendando relatórios de conformidade de segurança conforme as necessidades de cada parte interessada.
- Integre facilmente o console do McAfee ePO nos seus processos e funções empresariais existentes aproveitando seu conjunto robusto de APIs para obter mais insights e acelerar os fluxos de trabalho (por exemplo, integrando-se com sistemas de emissão de tíquetes, aplicativos Web ou portais de autoatendimento).
- Mantenha a sua postura de segurança ao distribuir soluções de segurança e agentes conforme novas máquinas são acrescentadas à sua rede corporativa, bastando sincronizar o console do McAfee ePO com o Active Directory.

---

“O produto McAfee ePolicy Orchestrator é a plataforma de gerenciamento de endpoints mais poderosa do mercado atualmente e é a ferramenta de gerenciamento de base para todos os produtos de segurança da empresa, oferecendo o poder e a flexibilidade desejados pelos compradores corporativos. As capacidades de segurança são amplas e fortemente integradas por meio de um fluxo de inteligência e um mecanismo de políticas comuns.”

— Forrester Wave: Endpoint Security Suites 2016 (pacotes de segurança de endpoint)

---

### Mitigação e correção rápidas

A plataforma do McAfee ePO possui capacidades avançadas para aumentar a eficiência da equipe de operações de segurança quando esta resolve uma ameaça ou faz alguma alteração para restaurar a conformidade. As respostas automáticas do McAfee ePO podem desencadear uma ação com base em um evento ocorrido. As ações podem ser meras notificações ou correções aprovadas.

### Casos de uso comuns para resposta automática

- Notificação de administradores quanto a novas ameaças, atualizações falhas ou erros de alta prioridade via e-mail ou SMS com base em limiares predeterminados
- Aplicação de políticas com base em eventos de cliente ou ameaça, por exemplo, para prevenir comunicações externas caso um host possa estar comprometido (o que impede atividades de comando e controle) ou bloquear o vazamento de dados ou a transferência para fora até que o administrador redefina a política
- Marcação de sistemas e execução de tarefas adicionais para remediação, como varreduras de memória solicitadas quando ameaças são detectadas
- Acionamento de executáveis registrados para executar scripts externos e comandos de servidor, por exemplo, para gerar um tíquete de suporte ou para integração em outros processos corporativos
- Colocação automática do endpoint em quarentena com políticas mais restritas

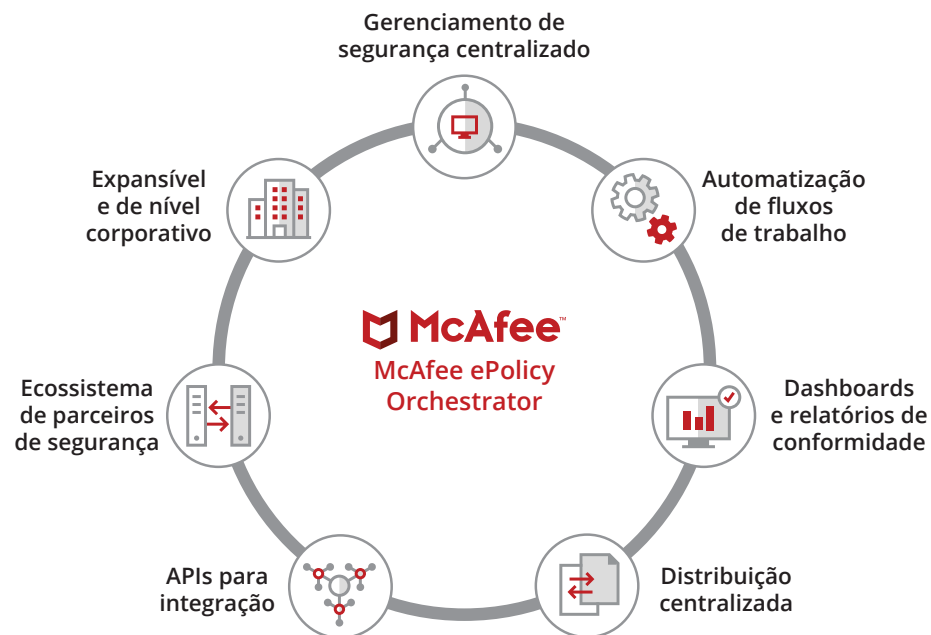


Figura 1. Gerenciamento centralizado de segurança utilizando o console do McAfee ePO.

### Proteção por toda a sua organização com o console do McAfee ePO

#### Segurança com gerenciamento centralizado

- Console único para gerenciamento centralizado e visibilidade sobre centenas de milhares de nós por toda a empresa
- Estrutura de trabalho aberta para amplo gerenciamento de segurança em sistemas protegidos pela McAfee e por soluções de terceiros
- Plataforma expansível que se integra à sua infraestrutura de TI existente, aproveitando-a para reduzir o atrito operacional

#### Acelere a resposta com confiança

- Visualizações e insights abrangentes para lidar proativamente com problemas de segurança internos e externos
- Distribuição imediata e centralizada de definições e atualizações de segurança para assegurar que os endpoints sejam protegidos contra as ameaças mais recentes
- Menores tempos de resposta por meio de dashboards decisivos e capacidades avançadas de geração de relatórios e consultas

### Reduza a complexidade e simplifique os processos

- Possibilidade de começar a usar imediatamente, com configuração orientada, fluxos de trabalho de gerenciamento de políticas automatizados e dashboards predefinidos
- Atribuição de políticas com base em “tags” para direcionar precisamente a aplicação de perfis de segurança predefinidos a sistemas individuais ou a grupos de sistemas com base em suas funções na empresa ou no status de risco
- Capacidades de gerenciamento automatizado e catálogo de tarefas para simplificar processos administrativos e reduzir a sobrecarga
- Um agente único para gerenciar vários produtos de endpoint reduz o risco de conflitos nos endpoints

#### Dimensione para distribuições corporativas

- Arquitetura de classe corporativa, com suporte para o gerenciamento de centenas de milhares de dispositivos com um único servidor
- Compatível e comprovado em ambientes de TI complexos e heterogêneos
- Relatórios corporativos que agregam uma visualização abrangente da sua postura de segurança e da sua conformidade

---

“O software McAfee ePO destaca-se na comparação com outras soluções. Ele é um ponto central para nossa proteção de endpoints. Posso ver tudo o que preciso ver, em todos os nossos produtos McAfee, a partir de um único painel. Seus dashboards fáceis de usar e sua funcionalidade incorporada tornam tudo — visibilidade, geração de relatórios, distribuição, atualização, manutenção, tomada de decisões — muito mais fácil.”

— Christopher Sacharok, engenheiro de segurança da informação, Computer Sciences Corporation

---



Av. Nações Unidas, 8.501 – 16º andar  
Pinheiros – São Paulo – SP  
CEP 05425-070, Brasil  
+(11) 3711-8200  
[www.mcafee.com/br](http://www.mcafee.com/br)

McAfee e o logotipo da McAfee, ePolicy Orchestrator e McAfee ePO são marcas comerciais ou marcas registradas da McAfee, LLC ou de suas afiliadas nos EUA e em outros países. Outros nomes e marcas podem ser propriedade de terceiros. Copyright © 2017 McAfee, LLC. 3718\_0118 JANEIRO DE 2018