McAfee ePolicy Orchestrator

Inspirando e capacitando o profissional de segurança

O gerenciamento de segurança requer malabarismos incômodos entre ferramentas e dados, frequentemente com visibilidade limitada sobre ameaças externas. Isso dá ao adversário a vantagem de ter mais tempo para explorar brechas ainda não identificadas entre as ferramentas, com o objetivo de causar mais danos. A mão de obra da segurança cibernética é limitada e precisa ser aparelhada para orquestrar, de maneira simples, ambientes de segurança cibernética complexos. É preciso ser menos reativo e se tornar mais proativo para se manter à frente dos adversários.

A sua organização precisa responder rapidamente a ameaças em qualquer tipo de dispositivo para minimizar os danos e quando a gerência exigir provas da eficácia da segurança. A plataforma de gerenciamento McAfee® ePolicy Orchestrator® (McAfee ePO™) — disponível no local e por meio da nuvem (com dois modelos à sua escolha: SaaS ou IaaS) — ajuda a eliminar o trabalho demorado e o potencial de erro humano. Ela também ajuda os responsáveis pelo gerenciamento da segurança a responder proativamente, mais rapidamente e com mais eficácia. Uma exclusividade do console do McAfee ePO é o McAfee® MVISION Insights, primeira tecnologia a priorizar ameaças e campanhas proativamente antes que você seja atingido, prever se as suas contramedidas serão eficazes e prescrever exatamente o que você precisa fazer caso não sejam, tudo ao mesmo tempo.

Segurança fundamental

Comecemos pelos itens indispensáveis. No centro de qualquer arquitetura de segurança está a capacidade de monitorar e controlar a integridade de dispositivos e sistemas. Padrões do setor, como o Controls e o Benchmarks do Center for Internet Security (CIS) e os controles de segurança e privacidade do National Institute of Standards Technology (NIST) SP 800-53, destacam a necessidade de monitorar e controlar infraestruturas de segurança. O console do McAfee ePO

Principais vantagens

- Gerenciamento centralizado aclamado pelo setor, com um exclusivo painel integrado para mais simplicidade — disponível pela nuvem ou no local
- Inteligência decisiva e proativa para você se manter à frente dos adversários
- Fluxos de trabalho automatizados para simplificar tarefas administrativas e obter mais eficiência
- Plataforma aberta e abrangente que integra soluções da McAfee e de mais 150 outros fornecedores para respostas mais rápidas e mais precisas
- Gerenciamento de segurança comum para a maior parte dos dispositivos do mercado
- Aproveitamento e aprimoramento de controles nativos existentes em sistemas operacionais, como o Windows Defender
- Capacidade de expansão para centenas de milhares de dispositivos, com cobertura do dispositivo à nuvem

Conecte-se conosco

permite obter visibilidade crítica e ajuda a estabelecer e impôr automaticamente políticas para garantir uma postura de segurança saudável por toda a sua empresa. Ele elimina a complexidade da orquestração de múltiplos produtos por meio de gerenciamento e imposição de políticas para toda a empresa através de um único console. A extensão do MVISION Insights oferece recomendações proativas de fortalecimento, além de inteligência decisiva. Essa capacidade de gerenciamento de segurança essencial é fundamental para a sua conformidade de segurança de TI.

Gerenciamento de segurança avançado e comprovado — simplificado

Mais de 36.000 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 dispositivos, redes e operações de segurança. As grandes corporações contam com a arquitetura altamente expansível do console do McAfee ePO, que as permite gerenciar centenas de milhares de nós a partir de um único painel integrado. Essa visualização de dashboard ajuda a priorizar riscos e oferece um resumo da sua postura de segurança, para todo o seu território digital, em uma única visualização gráfica dentro de um novo espaço de trabalho de proteção. Além disso, com o MVISION Insights, você obtém uma visualização proativa e única das ameaças externas previstas que importam para a sua organização e orientações preemptivas sobre o que é preciso fazer. Isso leva a sua segurança de endpoint a ser mais proativa e menos reativa, facilitando o gerenciamento da segurança. Finalmente, temos uma área de recursos de segurança, onde as mais recentes informações e pesquisas sobre ameaças são disponibilizadas imediatamente.

Os administradores podem se aprofundar no detalhamento de eventos específicos para obter insights adicionais. Essa visualização resumida reduz o tempo necessário para criar e racionalizar os dados à disposição, além de eliminar a possibilidade de erro, mesmo se alguma intervenção manual for necessária. O console do McAfee ePO simplifica a manutenção de políticas para administradores de segurança corporativa. Além disso, ele obtém de terceiros inteligência sobre ameaças, aproveitando o Data Exchange Layer (DXL), nossa estrutura de mensagens, líder do setor. Ele também integra políticas bidirecionalmente com uma gama de produtos. Essas eficiências operacionais reduzem a sobrecarga do compartilhamento de dados e processos, viabilizando uma resposta mais rápida e mais precisa.

O centro de suporte permite acesso fácil a informações sobre produtos McAfee e oferece uma visão geral das condições do servidor McAfee ePO nos ambientes dos usuários. Ele está disponível para o console do McAfee ePO no local e para o console do McAfee ePO no Amazon Web Services (AWS). Você pode receber suporte e notificações de produtos proativamente, pesquisar os repositórios de conteúdo da McAfee e acessar recursos do tipo “melhores práticas” e “como fazer”, de dentro do console do McAfee ePO. Você também pode gerenciar o estado da infraestrutura do McAfee ePO verificando facilmente suas condições e obter recomendações de como melhorar essas condições.

Analistas do setor apontam o software McAfee ePO como a razão pela qual os clientes adotam a McAfee e permanecem com ela.

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

Organizações com plataformas integradas
- 78% sofreram menos que cinco violações no ano passado
- 80% descobriram ameaças em oito horas

Organizações sem plataformas integradas
- Somente 55% sofreram menos que cinco violações no ano passado
- Somente 54% descobriram ameaças em oito horas

(Fonte: 2016 Penn Schoen Berland)

A eficiência da plataforma aberta contra a dispersão

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, tornando ainda maior a vantagem operacional de uma experiência de gerenciamento unificado, da instalação à geração de relatórios. Mais da metade das organizações estima uma melhoria superior a 20% com a integração de ferramentas de segurança (fonte: pesquisa de 2018 da MSI).

A McAfee acolhe essas exigências com uma abordagem de plataforma aberta para o gerenciamento da segurança que permite consolidar o que está disperso, com proteção para todos os seus ativos, suporte para inteligência contra ameaças, gerenciamento de dados de código aberto e integração de produtos de terceiros. A McAfee oferece controle centralizado para fins de conformidade e gerenciamento em uma variedade de produtos de segurança. Os analistas podem 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.

Nossa plataforma aberta oferece uma variedade de abordagens de integração (scripts, APIs, ausência de API e o mínimo de esforço com a estrutura de comunicação de código aberto DXL), permitindo que você escolha a abordagem que melhor atenda as suas necessidades, sem excesso de personalização ou serviços. Através do programa McAfee® Security Innovation Alliance, nós aceleramos o desenvolvimento de produtos de segurança interoperáveis, simplificamos a integração desses produtos com ambientes de usuário complexos e oferecemos um ecossistema de segurança verdadeiramente integrado e conectado para maximizar o valor dos investimentos existentes em segurança dos usuários. O programa McAfee Security Innovation Alliance tem atualmente mais de 150 integrações com parceiros.

Além disso, a estrutura de comunicações do DXL conecta e otimiza ações de segurança de produtos de vários fornecedores, bem como soluções desenvolvidas internamente e soluções de código aberto. Com a integração entre Cisco pxGrid e DXL, você pode ter acesso a quaisquer dados de 50 tecnologias de segurança adicionais. O console do McAfee ePO é um componente fundamental para o gerenciamento de nossa sólida plataforma aberta.

Ampla segurança de dispositivos: gerencie as ferramentas de segurança nativas

A plataforma expansível do McAfee ePO gerencia vários dispositivos, incluindo aqueles que possuem controles nativos. A McAfee aprimora e cogerencia a segurança já incorporada no Microsoft Windows 10 para proporcionar uma proteção otimizada, além de possibilitar que as organizações aproveitem as capacidades nativas do sistema da Microsoft. O console do McAfee ePO gerencia o McAfee® MVISION Endpoint, que combina capacidades de autoaprendizagem

Poupe tempo

Segundo uma pesquisa recente (2018) da MSI, os consumidores acreditam que podem economizar até 20% de seu tempo caso suas ferramentas de segurança sejam integradas.

O valor da integração

- Aumenta a eficácia de ferramentas e processos: 61%
- Reduz a complexidade e o trabalho manual, permitindo que os profissionais de segurança se concentrem nas tarefas que exigem pensamento crítico: 61%
- Melhora a visibilidade ao mostrar os dados em padrões e em contexto: 58%
- Simplifica os fluxos de trabalho para uma resposta mais rápida: 57%

(*Fonte: pesquisa de 2018 da MSI)*

avançadas e especificamente ajustadas para a segurança nativa do sistema operacional da Microsoft, além de evitar o custo e a complexidade adicional de um console de gerenciamento a mais. O software McAfee ePO proporciona uma experiência de gerenciamento comum com políticas compartilhadas para dispositivos com Microsoft Windows 10 e todos os dispositivos existentes em uma corporação heterogênea para assegurar consistência e simplicidade.

Consistência através de fluxos de trabalho automatizados

O console 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. A pesquisa da MSI, contratada pela McAfee em 2018, revelou que as organizações, ao automatizar tarefas repetíveis ou repetitivas, esperam economizar aproximadamente 25% do tempo despendido.

Com o software McAfee ePO, você pode distribuir e impor políticas de segurança facilmente a partir de uma visualização única clicando ao longo de algumas etapas lógicas que se sucedem. A visualização de painel único oferece contextos relevantes conforme você percorre tarefas e vê cada etapa e como ela se relaciona com as demais etapas. Isso reduz a complexidade e minimiza a possibilidade de erros. Você pode definir 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. Você pode utilizar o console do McAfee ePO para desencadear ações de correção a serem executadas 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. Você tem a opção de exigir um processo de aprovação antes que uma política nova ou atualizada seja implementada, reduzindo o risco de algum erro e assegurando um controle de qualidade.

Um fluxo de trabalho automatizado e claramente proativo revela-se no MVISION Insights. Na visualização comum, campanhas e ameaças externas e desconhecidas são indicadas automaticamente e priorizadas desde o dashboard do MVISION Insights com base em inteligência geográfica e setorial. Isso constitui uma avaliação preditiva, indicando se a postura de segurança atual é suficiente para deter a ameaça. O mais importante é que ações específicas são sugeridas, como atualizar o .DAT ou isolar.

"O (software) McAfee ePO é **um dos precursores da automação e orquestração de segurança integrada.** ...os profissionais de segurança de hoje exigem o poder do (software McAfee) ePO tradicional, mas na forma de uma experiência simplificada que os torne eficientes e eficazes... como um espaço de trabalho oferecido como SaaS, o MVISION combina análises, eventos e gerenciamento de políticas de uma maneira que empresas médias e grandes podem assimilar."

— Frank Dickinson, vice-presidente de pesquisa de produtos de segurança da IDC

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.
- Seja proativo e obtenha insights decisivos sobre ameaças previstas, sua atuação no seu setor ou região, se podem ser evitadas com a sua postura de segurança atual e, caso não possam, o que deve ser feito, tudo isso aproveitando o MVISION Insights.
- 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, o console do McAfee ePO integra-se com sistemas de emissão de tíquetes, aplicativos Web e portais de autoatendimento.
- Mantenha a sua postura de segurança ao distribuir soluções de segurança por autoaprendizagem ou agentes conforme novas máquinas são acrescentadas à sua rede corporativa, bastando sincronizar o console do McAfee ePO com o Microsoft Active Directory.

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 console 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

- Notifique administradores quanto a novas ameaças, atualizações falhas ou erros de alta prioridade, por e-mail ou SMS, com base em limiares predeterminados.
- Aplique políticas com base em eventos de cliente ou de ameaça, por exemplo, para prevenir comunicações externas caso um host possa estar comprometido (impossibilitando atividades de comando e controle) ou bloquear o vazamento de dados ou a transferência para fora até que o administrador redefina a política.
- Marque sistemas e execute tarefas adicionais para correção, como varreduras de memória solicitadas quando ameaças forem detectadas.
- Acione 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.
- Coloque automaticamente em quarentena uma carga de trabalho ou contêiner (qualquer dispositivo) com políticas mais restritivas.

"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

Gerenciamento de segurança baseado na nuvem

As organizações precisam simplificar e acelerar a distribuição de soluções contra ameaças avançadas. Muitas estão vendo o valor, em termos de eficiência, do gerenciamento de segurança baseado na nuvem ao eliminar o custo e a manutenção de uma infraestrutura no local. O console do McAfee ePO pode ser implementado pela nuvem, de qualquer lugar e a qualquer momento, por meio de duas opções de distribuição alternativas: software McAfee ePO no AWS ou McAfee® MVISION ePO™. Ambas as opções podem ser colocadas em funcionamento em menos de uma hora.

- O software McAfee ePO no AWS permite que as organizações aproveitem muitos serviços nativos do AWS, como autodimensionamento e o Amazon RDS, eliminando a necessidade de adquirir e gerenciar um banco de dados separado. Isso permite que os administradores se concentrem em tarefas críticas de segurança, e não na infraestrutura. O software McAfee ePO no AWS gerencia o McAfee® Endpoint Security, o McAfee® Data Loss Prevention, o McAfee® Cloud Workload Security, o DXL e soluções de terceiros que podem ser integradas ao software McAfee ePO.
- O MVISION ePO baseia-se nas vantagens do McAfee ePO como oferta de software como serviço (SaaS). Isso simplifica consideravelmente o gerenciamento da plataforma, possibilitando que você cuide das tarefas críticas de segurança. As atualizações da plataforma são transparentes, com um modelo de entrega contínua. A segurança dos dispositivos é distribuída automaticamente por toda a empresa assim que o seu agente é distribuído, eliminando o trabalho manual de instalar ou atualizar a segurança em cada dispositivo e assegurando uma imposição mais forte contra ameaças. Isso permite às empresas gerenciar o McAfee MVISION Endpoint e o DXL de um único console e de qualquer lugar.

O MVISION ePO permite que os seus dispositivos proporcionem insights críticos para a sua solução de gerenciamento de eventos e informações de segurança (SIEM), assegurando que os dados relevantes estejam à disposição dos seus analistas para aprimorar o trabalho de caça e neutralização de ameaças. Além disso, os atuais usuários do software McAfee ePO, tanto no local quanto em nuvem híbrida, agora podem migrar para o MVISION ePO com rapidez e facilidade e aproveitar plenamente as várias eficiências e vantagens de uma plataforma de gerenciamento de segurança baseada em SaaS.

Produtos da McAfee gerenciados pelo software McAfee ePO

Produtos da McAfee*
McAfee® Endpoint Protection (prevenção de ameaças, firewall e controle de Web)
O McAfee® MVISION Endpoint complementa o Microsoft Defender com proteção contra ameaças avançadas
McAfee® MVISION Mobile
McAfee® MVISION Insights
McAfee® Drive Encryption
McAfee® File and Removable Media Protection
McAfee® Active Response
McAfee® Management for Optimized Virtual Environments (McAfee® MOVE)
McAfee® Data Loss Prevention (McAfee® DLP)
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 Exchange Layer (DXL)

**Para o software McAfee ePO no local.*

Distribuições flexíveis

Distribuição	Principal vantagem
McAfee ePO no local	Total controle dos dados e do conjunto de recursos
McAfee ePO em AWS	Elimina a necessidade da manutenção de hardware exigida por uma solução no local
McAfee® MVISION ePO Software como serviço (SaaS)*	Oferta de SaaS multilocatário para eliminar toda a manutenção de infraestrutura e upgrades

**Nem todas as capacidades do software McAfee ePO estão disponíveis no McAfee MVISION ePO.*

Casos de uso: como o console do McAfee ePO permite um gerenciamento centralizado da segurança

Produto e tecnologia	Caso de uso	Benefício
MVISION ePO MVISION Endpoint Microsoft Windows 10	O software McAfee MVISION ePO gerencia o McAfee MVISION Endpoint, que complementa os controles nativos do Microsoft Windows 10 com proteção avançada. Você pode descobrir e gerenciar ameaças avançadas facilmente com uma plataforma de gerenciamento comum e políticas consistentes entre o Microsoft Windows e o McAfee Endpoint Security.	Melhor proteção para os controles nativos do Microsoft Windows e gerenciamento comprovadamente mais eficiente
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 dos endpoints comprometidos
McAfee ePO McAfee Data Loss Prevention 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
McAfee ePO MVISION ePO McAfee Endpoint McAfee MVISION EDR McAfee MVISION Insights	O McAfee MVISION Insights oferece informações decisivas sobre ameaças externas previstas e priorizadas. O MVISION Insights recorre ao McAfee® MVISION EDR para oferecer indicadores de comprometimento (IoCs), pesquisando para determinar se eles existem no ambiente sendo investigado. Caso afirmativo, são disponibilizadas informações detalhadas sobre uma campanha relacionada e instruções sobre o que fazer.	Aceleração de investigações e resoluções

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 (por meio do console do McAfee ePO). O Cisco ISE pode isolar o host até que ele seja considerado aceitável.	Maior proteção proativa
Rapid7 Nexpose McAfee ePO DXL	O McAfee ePO compartilha a lista de ativos com o Nexpose. Isso permite que você compreenda a sua postura de risco a partir do console do McAfee ePO e defina 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 do DXL. O blade de software Anti-Bot da Check Point bloqueia o tráfego de comando e controle (C&C) e alerta o software McAfee ePO, bem como outras soluções de segurança de terceiros integradas sobre tópicos de DXL comuns. Com essa inteligência, a McAfee inicia automaticamente um fluxo de trabalho de correção relevante para dispositivos endpoint. A Check Point e a McAfee também podem detectar e prevenir ataques de dia zero e convertê-los em ataques conhecidos, independentemente dos ataques se originarem da rede ou do endpoint. Ao trocar informações de missão crítica em tempo real, a integração permite a nossos respectivos produtos detectar, bloquear e neutralizar ameaças de maneira automatizada.	▪ Redução do tempo de detecção ▪ Bloqueio e correção dos ataques

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