RESUMO DE SOLUÇÃO

Uma abordagem mais simples para a segurança de endpoint

Como desenvolver uma defesa unificada para proteger cada endpoint — do dispositivo à nuvem

A segurança cibernética está diante de um dilema: enquanto a quantidade, o nível de sofisticação e o impacto financeiro das violações continuam sua escalada, a disponibilidade de analistas qualificados está menor do que nunca.

Agora há uma maneira de resolver os problemas complexos de segurança enfrentados pela sua empresa, fazendo mais em menos tempo e com menos recursos. O portfólio de proteção de endpoint da McAfee emprega análises e autoaprendizagem para atingir um grau de eficácia líder no setor, além de oferecer a flexibilidade de conectar nossas soluções a produtos de mais de 150 outros fornecedores. Conforme trabalhamos para unificar proteção de dados e defesa contra ameaças do dispositivo à nuvem, estamos construindo um futuro no qual a segurança é um sistema integrado — mais simples, mais inteligente e mais amplo do que tudo o que existia até então.

Principais vantagens

- Defenda seus endpoits com prevenção de explorações, firewall, controle de Web e autoaprendizagem.
- Proteja dispositivos iOS e Android contra phishing, ataques de dia zero e perda de dados, em tempo real, mesmo estando off-line.
- Recursos poderosos para detecção, investigação e resposta — simplificados com investigações orientadas por inteligência artificial.
- Autoaprendizagem, defesa contra roubo de credenciais e correção por reversão complementam as capacidades básicas de segurança do sistema operacional.
- Simplifique e acelere a sua segurança com gerenciamento em um único painel.
- Escolha gerenciamento baseado em SaaS com o MVISION ePO ou gerenciamento no local com o McAfee® ePO™.

Conecte-se conosco

Como a quantidade, o nível de sofisticação e o impacto financeiro das violações continuam a crescer, as empresas se encontram em uma encruzilhada. Elas devem continuar contando apenas com soluções antivírus tradicionais, sabendo que isso as deixa vulneráveis a ameaças modernas, como ransomware e redes de bots? Ou devem agregar uma "solução" de múltiplos fornecedores que ofereça melhor proteção contra ameaças, mas que também retarde processos, reduza o desempenho das máquinas e cause indisponibilidades significativas? Felizmente, com o portfólio de proteção de endpoint da McAfee, as empresas não precisam mais escolher entre defesa contra ameaças e agilidade operacional.

McAfee Endpoint Security

Gerenciamento central e análise compartilhada

Essa plataforma de proteção de endpoint com gerenciamento centralizado utiliza um único agente para múltiplas tecnologias, incluindo proteção contra ameaças, firewall, controle de Web, prevenção adaptável contra ameaças e mais — tudo isso desenvolvido para simplificar ambientes complexos.

Ao contrário do software antivírus tradicional, o McAfee Endpoint Security aproveita conexões entre endpoints locais e o McAfee® Global Threat Intelligence na nuvem para detectar ameaças de dia zero quase em tempo real. Assim que uma ameaça é identificada, onde quer que seja, ela pode ser identificada em qualquer lugar. A combinação de informações e análises compartilhadas com capacidades de proteção contra explorações avançadas permite ao McAfee Endpoint Security atingir uma taxa de proteção 25% maior contra ameaças de dia zero do que o McAfee® VirusScan® Enterprise. Em testes independentes, o McAfee Endpoint Security obteve uma taxa de êxito geral de 99,98% — sem falsos positivos.

Manutenção automatizada e correção eficiente

Com o McAfee Endpoint Security, você pode se beneficiar com recursos aprimorados de automação e autoaprendizagem. A classificação comportamental por autoaprendizagem da plataforma detecta ameaças de dia zero quase em tempo real, viabilizando uma inteligência decisiva contra ameaças. Além disso, ela evolui automaticamente com o tempo, identificando novos comportamentos e adicionando regras para identificar ataques futuros.

Durante um ataque, os administradores podem ver rapidamente onde estão ocorrendo infecções e por quanto tempo os endpoints ficaram expostos, o que os permite compreender a ameaça e reagir mais prontamente. O recurso Real Protect pode corrigir os endpoints atacados, restaurando-os ao estado mais recente de bom funcionamento para prevenir infecções imediatamente e reduzir o trabalho do administrador. A contenção dinâmica de aplicativos constitui uma defesa adicional contra ransomware e greyware ao permitir isolar o "paciente zero".

A combinação da plataforma McAfee ePO com o McAfee Endpoint Security proporciona grande visibilidade, incrementa a produtividade da TI, simplifica as operações, unifica a segurança e reduz custos. Essas e outras eficiências permitiram às equipes de segurança cibernética que migraram para o McAfee Endpoint Security economizar até 40 horas por semana em gerenciamento.

Principais vantagens do McAfee Endpoint Security

- Detecta ameaças de dia zero quase em tempo real
- Atualiza continuamente o mecanismo antimalware
- Permite comunicação entre antivírus, prevenção de explorações, firewall e controle de Web
- Restaura o endpoint ao estado mais recente de bom funcionamento
- Detém aplicativos e processos maliciosos nos endpoints mesmo quando estes se encontram off-line
- Prioriza alertas com uma "reprodução" dos eventos do ataque
- Proporciona caça e resposta a incidentes, integradas e fáceis de usar
- Torna a resposta a incidentes fácil como um clique

A produtividade dos funcionários também é preservada: as varreduras levam apenas alguns segundos e só ocorrem quando o dispositivo está ocioso, sendo retomadas prontamente após uma reinicialização ou desligamento. O melhor de tudo é que o McAfee Endpoint Security é leve e não requer uma conexão com a nuvem, para que os usuários sejam defendidos mesmo quando estão off-line.

McAfee MVISION EDR

Um departamento de TI médio gerencia milhares de endpoints — sejam desktops, servidores, celulares, relógios de pulso inteligentes ou dispositivos IoT. As soluções de EDR atuais desovam informações demais em cima de equipes de segurança já assoberbadas e que dependem de analistas veteranos para investigar ameaças. Essa abordagem não se mostrou eficaz ou expansível, especialmente quando agravada pelas restrições de largura de banda e pela falta de qualificações de hoje em dia.

O MVISION EDR começa onde as tecnologias antivírus e soluções tradicionais de EDR terminam. A solução integrada de segurança de endpoint ajuda a gerenciar um grande volume de alertas, monitorando e coletando dados de atividade de endpoint que possam indicar uma ameaça e proporcionando a visibilidade e o contexto necessários. Ao analisar os dados para identificar padrões de ameaça, suas capacidades de análise e resposta automatizada de IA descartam ou detém as ameaças e notificam o pessoal de segurança, enquanto ferramentas forenses e analíticas pesquisam as ameaças identificadas e procuram atividades suspeitas.

Um nível mais alto com investigação orientada por inteligência artificial (IA)

As soluções de EDR costumam "viabilizar" a investigação fornecendo dados brutos, contexto e funções de pesquisa, mas não prescindem de analistas qualificados para realizar as consultas e análises. O MVISION EDR, por outro lado, orienta a investigação, reduzindo a experiência e o trabalho necessários para a realização das investigações. Ele também permite que os analistas determinem o risco e a causa raiz do incidente mais rapidamente

A investigação orientada por IA coleta e processa automaticamente quantidades imensas de dados de diversas fontes, incluindo a origem e o alvo do ataque, bem como o aparente padrão de ataque. Em seguida, assim como um analista veterano orientaria um analista menos inexperiente no decorrer de uma perícia, a IA apresenta automaticamente uma ou mais hipóteses relacionadas aos alertas e coleta, resume e mostra visualmente evidências de múltiplas fontes conforme as investigações evoluem. Com base nas evidências, o MVISION EDR utiliza essas hipóteses para formular e ajudar a responder questões pertinentes que orientarão a investigação, enquanto os analistas deliberam se devem continuar com mais questões e coleta de dados, encerrar o caso ou escalar o caso.

Isso ajuda os analistas a aumentar seu nível de qualificação, o que os torna mais aptos a gerenciar um grande volume de alertas, reduzir o tempo da investigação e aumentar a veracidade das investigações. Com analistas ainda novatos podendo analisar ameaças, os analistas mais experientes ficam livres para aplicar seus conhecimentos à caça de ameaças e à redução dos tempos de resposta.

Principais vantagens do McAfee MVISION EDR

- Detecção de ameaças decisiva e de alta qualidade, sem falsos alertas
- Análise mais rápida para uma defesa mais resiliente
- Investigações orientadas por IA proporcionam insights sobre o ataque gerados por máquina
- Capacidade de maximizar o impacto da equipe existente
- Solução de nuvem que exige pouca manutenção
- Aproveite o aclamado gerenciamento de segurança em console único do MVISION ePO (baseado em SaaS) ou do McAfee ePO (no local ou baseado em IaaS)
- Os analistas podem se concentrar na resposta estratégica a incidentes sem sobrecarga administrativa

Uma identificação mais rápida leva a uma resposta mais rápida

Os analistas também podem utilizar as capacidades de pequisa profunda e de coleta de dados contínua para expandir as consultas e examinar detalhadamente os sistemas e os relacionamentos entre os sistemas. O MVISION EDR pode capturar um instantâneo dos processos ativos, conexões, serviços e entradas de execução automática de um endpoint, possibilitando inspeção imediata, pesquisa em tempo real e pesquisas históricas. Esses dados também são enviados em fluxo para a nuvem, viabilizando a adoção rápida de novas técnicas e mecanismos de análise, enquanto resultados de detecção com base em comportamentos são mapeados dentro da estrutura MITRE ATTACK, o que proporciona um processo mais consistente para determinar a fase e o risco de uma ameaça e priorizar uma resposta.

Os insights e as capacidades de investigação do MVISION EDR são ainda mais expandidos por meio de integração com soluções de gerenciamento de eventos e informações de segurança (SIEM), como o McAfee® Enterprise Security Manager ou produtos de terceiros. Isso permite uma correlação entre anomalias em endpoints e informações de rede e outros dados coletados pelo SIEM.

McAfee MVISION Endpoint

O MVISION Endpoint proporciona capacidades aprimoradas de detecção e correção para clientes que desejam reforçar sua proteção de endpoint. Desenvolvido especificamente para complementar as defesas nativas do sistema operacional (SO), ele incrementa o firewall e a prevenção de explorações nativos dos ambientes Windows 10 e Windows Server 2016 e 2019 detectando ameaças sofisticadas que passam despercebidas pelo Microsoft Defender.

Uam estratégia de endpoint mais inteligente

Ao contrário de alternativas limitadas a uma única forma de análise por autoaprendizagem, o MVISION Endpoint pode realizar análises estáticas, comportamentais e de malware sem arquivo para uma proteção contra ameaças mais forte e com menos falsos positivos. Ele utiliza autoaprendizagem comportamental para identificar ameaças por seus comportamentos reais, condenando arquivos que compartilhem recursos com outros exemplares de malware. Ele também conta com correção por reversão aprimorada, possibilitando restaurar um sistema atingido por ransomware ao estado mais recente de bom funcionamento.

Defesa com base em nuvem, com um console único

O melhor de tudo é que o MVISION Endpoint proporciona uma experiência de gerenciamento unificada. Em vez de duplicar o gerenciamento de políticas, ele permite que as configurações do Windows Defender Antivirus, do Exploit Guard e do Windows Firewall e as políticas dos produtos McAfee sejam gerenciadas de forma centralizada. Ao distribuir o McAfee MVISION Endpoint juntamente com o McAfee ePO ou o MVISION ePO, você obtém uma defesa realmente integrada através de um painel único.

Principais vantagens do McAfee MVISION Endpoint

- Gerenciamento centralizado para Windows 10 e Windows Server 2016 e 2019
- Defesas avançadas com ou sem arquivo e comportamentais por autoaprendizagem
- Menor custo total de propriedade (TCO) e simplificação dos fluxos de trabalho
- Defesa contra roubo de credenciais e correção por reversão
- Gerenciamento das tecnologias da McAfee e da Microsoft com política única e console único

Principais vantagens do McAfee MVISION Mobile

- Oferece proteção em tempo real no próprio dispositivo
- Detecta ameaças móveis e protege contra ataques de dia zero
- Destaca riscos à privacidade para informar aos usuários os perigos associados a cada aplicativo específico

O McAfee ePO e o MVISION ePO também oferecem capacidades de integração com produtos de terceiros, agregando contramedidas adicionais ao console para reforçar e personalizar ainda mais a sua segurança.

Esse agente extremamente leve é mais rápido, mais simples e mais robusto que ferramentas de segurança tradicionais. Com atualizações entregues automaticamente ao cliente, você nunca terá de se perguntar se ele está atualizado — e com seu baixo consumo de recursos e desempenho equilibrado, o impacto sobre o usuário é mantido ao mínimo, preservando a produtividade.

McAfee MVISION Mobile

O McAfee MVISION Mobile detecta ameaças e vulnerabilidades em dispositivos Apple iOS e Android, nas redes às quais estes se encontram conectados e nos aplicativos que os usuários instalaram. Sua integração com nossa plataforma avançada de gerenciamento central corporativo, o software McAfee ePO, permite que você gerencie dispositivos móveis como qualquer outro endpoint. Como componente integrado do McAfee® Device Security, o MVISION Mobile estende a visibilidade e o controle dos seus ativos móveis utilizando o mesmo console único que abrange todos os seus dispositivos gerenciados pela McAfee.

Mais inteligente e mais vigilante

Diferentemente das soluções de segurança móvel baseadas em nuvem que dependem de análise de aplicativos em área restrita (sandbox) ou tunelamento de tráfego, o MVISION Mobile situa-se diretamente nos dispositivos móveis para proporcionar uma proteção contínua, não importando como o dispositivo está conectado: pela rede corporativa, por um ponto de acesso público, pela operadora de celular ou mesmo sem conexão alguma.

O MVISION Mobile utiliza algoritmos de autoaprendizagem alimentados por bilhões de pontos de dados de milhões de dispositivos para identificar ameaças e ataques atuais ou iminentes. Eles analisam desvios em relação ao comportamento normal dos dispositivos e fazem determinações sobre indicadores de comprometimento para identificar precisamente ataques avançados baseados em dispositivo, aplicativo e rede — incluindo ataques nunca vistos antes. Uma inteligência de aplicativo abrangente reduz os riscos à segurança e à privacidade e, com isso, as possibilidades de perda de dados. Notificações de proteção de rede, desenvolvidas para permitir que você e seus funcionários saibam se o respectivo dispositivo está se conectando a uma rede insegura ou comprometida, enfatizam a prevenção dos ataques antes que estes comecem.

McAfee MVISION ePO

O McAfee MVISION ePO, aclamado no setor, foi desenvolvido para gerenciar as soluções da McAfee e aprimorar os controles de segurança nativos incorporados nos sistemas operacionais. Essa versão SaaS global, multilocatária e corporativa do comprovado e exclusivo software McAfee ePO permite gerenciar a segurança, configurar e impor políticas automaticamente, simplificar e automatizar processos

- Acelera a resposta por meio de uma inteligência sobre ameaças móveis decisiva e de nível corporativo
- Permite que os funcionários trabalhem em qualquer lugar, em qualquer horário e em qualquer dispositivo, graças aos controles de conformidade
- Detecta links nocivos encontrados em mensagens de texto, aplicativos de redes sociais e e-mails por meio da proteção contra phishing
- Integra-se com soluções de gerenciamento de mobilidade corporativa (EMM), mas também funciona em cenários com dispositivos trazidos pelos usuários (BYOD)
- Permite que as equipes de resposta a incidentes aproveitem dados forenses detalhados sobre ameaças para análise e ação, de maneira a prevenir que um dispositivo comprometido cause uma epidemia

de conformidade e aumentar a visibilidade. Ele oferece expansibilidade para centenas de milhares de dispositivos, incluindo os que possuem controles nativos, com cobertura do dispositivo à nuvem — tudo isso sem a complexidade de manter uma arquitetura no local.

Segurança aliada à simplicidade

O plataforma expansível do McAfee ePO proporciona uma experiência de gerenciamento comum com políticas compartilhadas para todos os dispositivos, incluindo dispositivos com Windows 10, em toda uma corporação heterogênea, assegurando consistência e simplicidade. O MVISION ePO oferece visibilidade em um painel único, permitindo eliminar a complexidade da orquestração de múltiplos produtos. Com capacidades de gerenciamento ágeis e automatizadas, os usuários podem identificar, gerenciar e responder rapidamente a vulnerabilidades, mudanças na postura de segurança e ameaças conhecidas — estando em qualquer lugar, através de um navegador. Nesse painel, políticas de segurança podem ser distribuídas e impostas por toda a corporação com apenas alguns passos.

O espaço de trabalho da proteção oferece um resumo de todo o seu terreno digital em uma única visualização gráfica, permitindo aos administradores priorizar riscos e detalhar eventos específicos para maiores insights. Essa visualização resumida reduz o tempo necessário para criar relatórios e racionalizar os dados à disposição, além de eliminar a possibilidade de erro que existe quando alguma intervenção manual é necessária. Ao reunir gerenciamento de risco e análise de incidentes, ela permite que os seus dispositivos forneçam insights cruciais para o seu SIEM, colocando informações críticas ao seu alcance para um melhor trabalho de caça e correção de ameaças.

Eficiência adicional

Segundo o Magic Quadrant de proteção de endpoint da Gartner, o software McAfee ePO é o motivo pelo qual muitas organizações compram da McAfee e permanecem com ela. Com essa tecnologia comprovada agora disponível no formato SaaS, as empresas podem se beneficiar ainda mais ao possibilitar que seus profissionais de segurança se concentrem exclusivamente no monitoramento e controle de todos os dispositivos. Além de eliminar a configuração e a manutenção associadas a uma infraestrutura de segurança no local, o MVISION ePO também automatiza a distribuição da segurança de dispositivo pela empresa e proporciona atualizações contínuas e transparentes, oferecendo estabilidade e poupando tempo. Com capacidades avançadas para aumentar a eficiência da equipe de operações de segurança quando esta neutraliza uma ameaça ou faz alguma alteração para restaurar a conformidade, é possível obter uma economia de tempo ainda maior.

Para descobrir se o MVISION ePO é indicado para a sua empresa, clique aqui e faça uma avaliação gratuita.

Principais vantagens do McAfee MVISION ePO

- Gerenciamento centralizado aclamado no setor
- Visibilidade e controle simples e unificados, de qualquer lugar
- Eliminação da complexidade associada à manutenção de uma plataforma de segurança no local
- Uma visão comum que reúne gerenciamento de risco e análise de incidentes
- Plataforma abrangente que gerencia produtos da McAfee e controles nativos em sistemas operacionais
- Fluxos de trabalho automatizados para funções administrativas eficientes
- Investigação e correção simplificadas de incidentes
- Gerenciamento de segurança comum para a maior parte dos dispositivos no mercado
- Expansibilidade de centenas a milhares de dispositivos
- Cobertura do dispositivo à nuvem

ESTUDOS DE CASO

MGM Resorts International
20.000 nós em 20 resorts no mundo todo

- **Desafios:** incapacidade de neutralizar riscos e bloquear ataques de dia zero; necessidade de compreender padrões de ataque complexos e proporcionar disponibilidade permanente para aplicativos críticos; incapacidade de reduzir despesas nas operações de segurança e ainda se manter atualizada
- **Soluções:** McAfee® Enterprise Security Manager, McAfee® Investigator, MVISION EDR, McAfee® Web Gateway, McAfee Endpoint Security, McAfee Data Loss Prevention, DXL e McAfee® Professional Services
- **Resultados:** menos tempo para conter, investigar e corrigir ameaças e melhoria das qualificações da equipe de operações de segurança

Atrius Health
Mais de 65.000 usuários em 9.000 endpoints distribuídos por mais de 29 localizações

- **Desafios:** proteger contra ransomware e phishing; acelerar a detecção e a resposta; manter a organização protegida sem obstruir o crescimento das empresas
- **Soluções:** McAfee Enterprise Security Manager e McAfee Endpoint Security
- **Resultados:** economia operacional; contratação de vários funcionários em expediente integral evitada; menos tempo necessário para detecção e resposta; melhor segurança para ambientes virtuais

Florida International University
55.000 estudantes e 15.000 funcionários em dois campi principais e campi satélites em outros países

- **Desafios:** necessidade de permitir a liberdade do BYOD, mas ainda assim proteger o ambiente contra ameaças; evitar que os estudantes introduzam malware no ambiente acidentalmente; manter visibilidade ampla
- **Soluções:** McAfee Enterprise Security Manager e McAfee Endpoint Security
- **Resultados:** contenção mais rápida de ataques ou arquivos suspeitos; postura geral de segurança mais forte sem a necessidade de aumentar a equipe; proteção de endpoint mais robusta com o mínimo de impacto sobre os usuários; facilidade de gerenciamento e visibilidade sobre toda a empresa

Banco Delta
400 endpoints.

- **Desafios:** reduzir a sobrecarga do gerenciamento de segurança; construir uma defesa forte para proteção contra ataques sofisticados; planejar uma estratégia de segurança para o futuro, incluindo migração para a nuvem
- **Soluções:** plataforma McAfee ePO, McAfee Enterprise Security Manager e McAfee Endpoint Security
- **Resultados:** redução perceptível de infecções e de comportamentos potencialmente comprometedores por parte dos usuários

Seguradora dos EUA
6.000 desktops e 2.000 servidores distribuídos em 12 localizações

- **Desafios:** incapacidade de proteger dados pessoais confidenciais dos clientes; desejo de oferecer uma segurança de ponta sem comprometer a experiência do cliente
- **Soluções:** McAfee Endpoint Security, McAfee Data Loss Prevention e McAfee Web Gateway
- **Resultados:** os picos de utilização da CPU foram reduzidos de 95% para 30% ou 35% e varreduras que antes levavam vários dias agora levam horas; muitas horas economizadas para engenheiros de segurança cibernética; maior produtividade, tanto de usuários finais quanto das operações de segurança; melhor postura de segurança

Grande banco multinacional (região EMEA)
45.000 endpoints em mais de 40 países e dois centros de dados

- **Desafios:** incapacidade de proteger a organização contra ransomware e ameaças de dia zero ou bloquear ameaças causadas pelos comportamentos dos usuários; desejo de melhorar a eficiência do gerenciamento da segurança
- **Soluções:** McAfee Endpoint Security, plataforma McAfee ePO e McAfee Web Gateway
- **Resultados:** uma protecão de endpoint aprimorada, que captura mais malware e defende melhor contra ameaças de dia zero; menos tempo para proteção utilizando soluções integradas de segurança que compartilham informações sobre ameaças quase em tempo real, economia de tempo operacional em decorrência de uma administração de segurança mais fácil e menos incidentes

Grandes ganhos

McAfee Endpoint Security

- Ganhador de prata na categoria de segurança de endpoint do prêmio Cybersecurity Excellence Awards
- Prêmio de produto corporativo aprovado pela AV-Comparatives
- AV-TEST: a McAfee atingiu um placar de usabilidade perfeito

MVISION Endpoint

- Ganhador de prata na categoria de segurança de endpoint do prêmio Cybersecurity Excellence Awards de 2019
- Prêmio de inovador técnico de segurança de endpoint em 2018

MVISION Mobile

- Ganhador de prata na categoria de segurança móvel do prêmio Cybersecurity Excellence Awards de 2019

Endpoints atendidos pela McAfee

- 622 milhões de endpoints no total
- 97 milhões de endpoints corporativos
- 525 milhões de endpoints de consumidores
- 69.000 clientes corporativos
- 7.000 funcionários
- 189 países
- 80% das empresas Fortune 100
- 75% das empresas Fortune 500
- 64% das empresas Global 2000
- 87% dos maiores bancos do mundo
- 54% dos 50 maiores varejistas
- Mais de 1.550 patentes de segurança em todo o mundo

"O McAfee ePO é um dos precursores da orquestração e automação de segurança integradas... os profissionais de segurança de hoje exigem o poder do [McAfee] ePO tradicional, mas na forma de uma experiência simplificada que os torne eficientes e eficazes... como um espaço de trabalho oferecido por 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

McAfee
Together is power.

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