McAfee Endpoint Security

Segurança específica para gerenciamento proativo de ameaças e controles de segurança comprovados

Segurança de endpoint: quais são as suas prioridades?

Nas empresas de hoje em dia, a segurança pode ser responsabilidade de uma única equipe ou de várias. No caso de organizações empresariais, costuma ser uma função compartilhada por diversas equipes, como as de administração de TI e de operações de segurança. Seja qual for a abordagem que melhor descreve o cargo que você desempenha na sua empresa, os resultados e capacidades esperados da sua plataforma de proteção de endpoint estão naturalmente relacionados ao que você considera mais importante.

A solução de endpoint da qual você depende deve corresponder às prioridades que mais importam para você. Independentemente do seu cargo, o McAfee® Endpoint Security corresponde às suas necessidades críticas específicas — da prevenção e caça a ameaças à adequação dos controles de segurança. Com as capacidades do McAfee® MVISION Insights, prioridades de ameaça específicas são oferecidas para se trabalhar antes que ocorra um ataque. A solução permite assegurar a disponibilidade dos sistemas para os usuários, encontrar mais oportunidades para automação e simplificar fluxos de trabalho complexos.

Assegure disponibilidade e visibilidade

O McAfee Endpoint Security permite aos clientes responder e gerenciar o ciclo de vida da defesa contra ameaças com defesas proativas e ferramentas de correção. A correção por reversão automática restaura os sistemas a um estado saudável para preservar a produtividade de usuários e administradores, economizando um tempo que, de outra forma, seria gasto na espera pela normalização do sistema, na recuperação ou na restauração de uma imagem em uma máquina infectada. Inteligência global contra ameaças e inteligência de eventos locais em tempo real são compartilhadas entre endpoints e o McAfee® MVISION EDR para coletar detalhes de eventos de ameaça, detectar e impedir as ameaças de evadir a detecção e mapear as ameaças à estrutura MITRE ATT&CK para investigação posterior. O gerenciamento é mantido simples por meio de um console de gerenciamento centralizado disponível em opções de distribuição local, SaaS ou de ambiente virtual. O MVISION Insights oferece visibilidade e controle exclusivos sobre possíveis ameaças prioritárias com alta probabilidade de ataque, além de determinar se a postura de segurança da organização será suficiente para proteger contra a ameaça. Isso assegura um alto nível de proteção contra uma ameaça crítica, derrotando o adversário antes que ele ataque.

Principais vantagens

- **Defesas avançadas para ameaças avançadas:** autoaprendizagem, defesa contra roubo de credenciais e correção por reversão complementam as capacidades básicas de segurança dos sistemas de desktop e servidor Windows
- **Sem complexidade adicional:** gerencie as tecnologias da McAfee, as políticas do Windows Defender Antivirus, o Defender Exploit Guard e as configurações do Windows Firewall utilizando uma única política e um único console

Conecte-se conosco

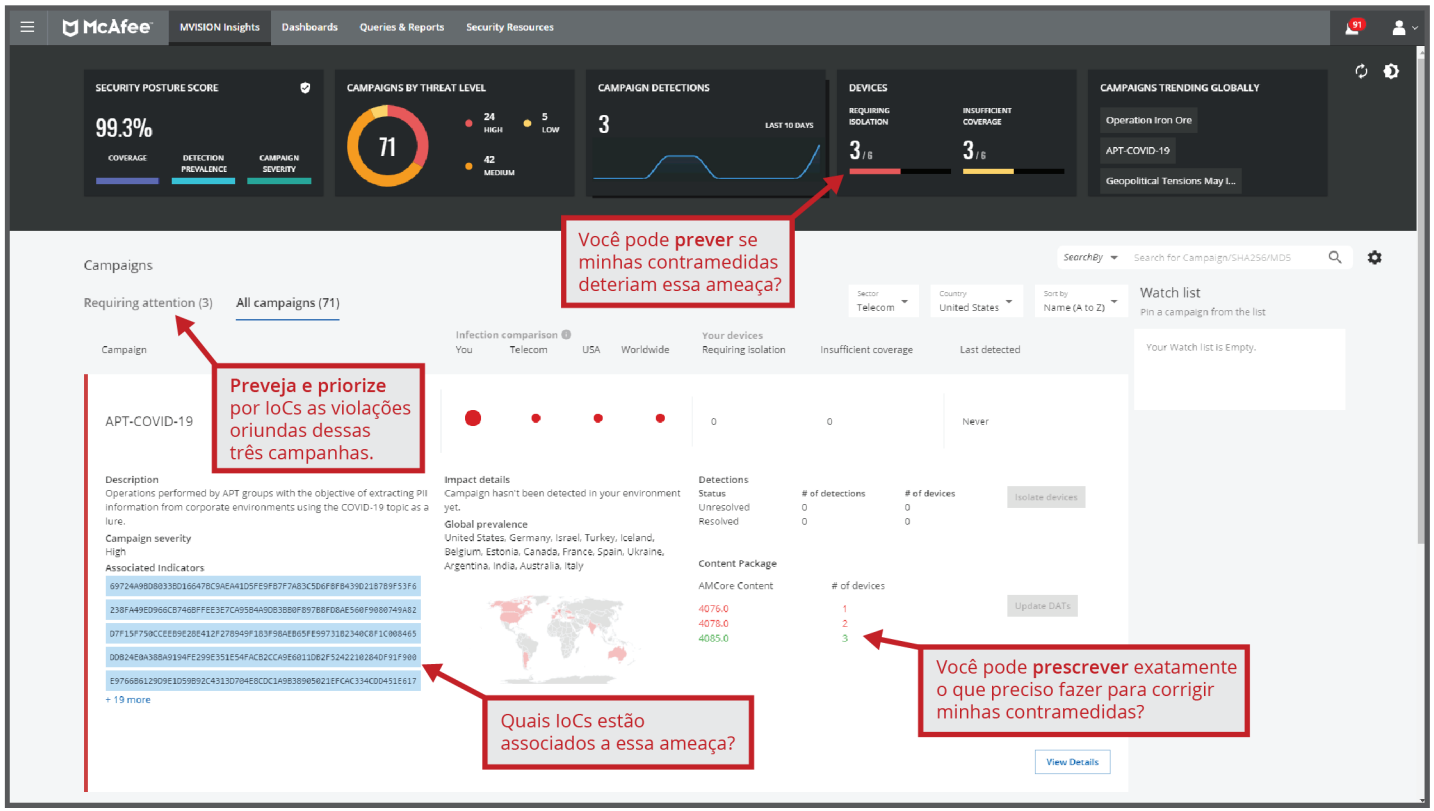

Figura 1. Dashboard do MVISION Insights. (O MVISION Insights requer a telemetria do McAfee Endpoint Security (opcional) para funcionar adequadamente.)

Ao utilizar o MVISION Insights, as organizações recebem alertas e notificações sobre possíveis ameaças priorizadas com maiores chances de ataque com base no setor e na região. Além disso, o MVISION Insights oferece uma avaliação local da postura de segurança e das possibilidades de proteção contra a ameaça em questão.

Ele também identifica endpoints vulneráveis à ameaça e oferece uma orientação prescritiva sobre o que atualizar. Isso aumenta os esforços proativos para manter a dianteira em relação a adversários propensos a atacar.

Principais vantagens

- **MVISION Insights:** responda imediatamente a possíveis campanhas ativas (as quais são priorizadas dependendo de estarem visando o seu setor ou suas geografias) utilizando uma solução líder em inteligência de segurança decisiva prontamente disponível. O MVISION Insights prevê quais endpoints carecem de proteção contra as campanhas e oferece orientação prescritiva sobre o que fazer para melhorar a detecção. Esta é a única solução de segurança de endpoint capaz de priorizar, prever e prescrever ações simultaneamente

O McAfee Endpoint Security coleta insights sobre ameaças de múltiplas camadas de engajamento, utilizando um único agente de software para eliminar redundâncias causadas por múltiplos produtos separados.

O resultado é uma abordagem integrada de segurança que elimina a correlação manual de ameaças.

Detalhes de ameaças que exijam investigações adicionais sobem automaticamente nas prioridades dos responsáveis pela resposta a incidentes. Os dados sobre eventos de ameaça são apresentados em um formato simples e de fácil visualização por meio do Story Graph, que mostra detalhes da ameaça e permite aos administradores aprofundar facilmente o detalhamento e investigar as origens dos malfeitores.

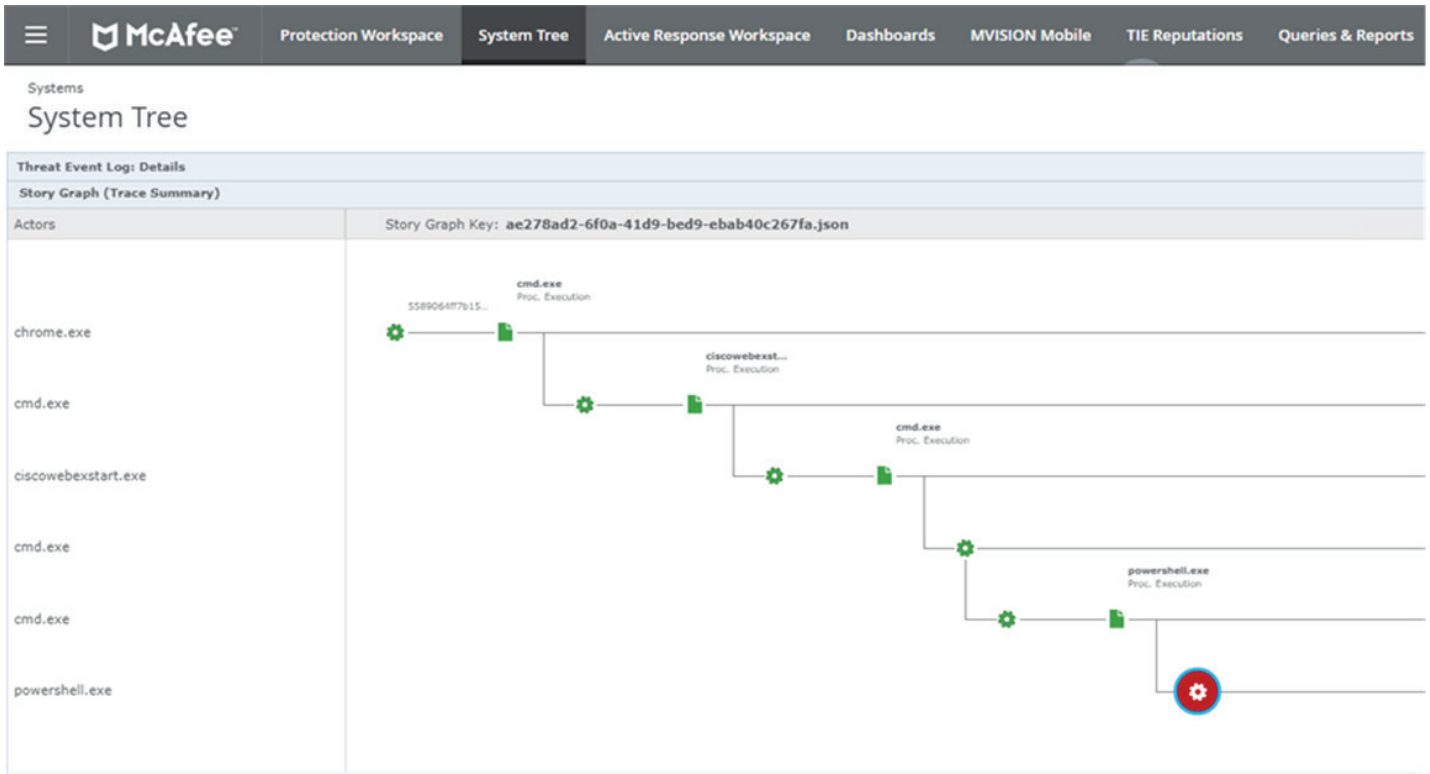

Figura 2. Story Graph.

Defesas integradas contra ameaças avançadas automatizam e aceleram a resposta

Defesas adicionais contra ameaças avançadas, como a contenção dinâmica de aplicativos (DAC), também estão disponíveis como parte da estrutura integrada do McAfee Endpoint Security para ajudar as organizações a se defenderem contra as ameaças avançadas mais recentes.[1] Por exemplo, a DAC analisa e toma providências contra greyware e outros tipos de malware emergente, contendo-os para evitar infecções.

Uma outra tecnologia contra ameaças avançadas é o Real Protect, que utiliza classificação de comportamentos por autoaprendizagem para detectar malware de dia zero e melhorar a detecção. A classificação sem assinatura é realizada na nuvem e ocupa pouco espaço no cliente, enquanto proporciona uma detecção quase em tempo real. Insights decisivos são fornecidos e podem ser utilizados para criar indicadores de ataque (IoAs) e indicadores de comprometimento (IoCs). Isso pode ser particularmente útil para detecção de movimentação lateral, descoberta de pacientes zero, atribuição a perpetradores de ameaças, investigações forenses e correção. O Real Protect também acelera análises futuras ao fazer com que a classificação de comportamentos evolua automaticamente para identificação de comportamentos e acréscimo de regras para identificar futuros ataques semelhantes utilizando recursos tanto estáticos quanto em tempo de execução.

Finalmente, para evitar infecções imediatamente e reduzir o tempo exigido dos administradores de segurança de TI, o cliente corrige o endpoint já condenado restaurando-o ao estado mais recente de bom funcionamento.

Proteção inteligente para endpoints que permite saber o que os atacantes estão fazendo agora

Uma inteligência melhor leva a resultados melhores. O McAfee Endpoint Security compartilha suas observações em tempo real com as múltiplas tecnologias de defesa de endpoint conectadas à sua estrutura para colaborar e acelerar a identificação de comportamentos suspeitos, propiciar uma melhor coordenação das defesas e oferecer uma proteção melhor contra ataques direcionados e ameaças de dia zero. Insights como hash de arquivo, URL de origem, AMSI e eventos de PowerShell são rastreados e compartilhados não apenas com outras defesas, mas também com o cliente e com interfaces de gerenciamento para ajudar os usuários a compreender os ataques e a proporcionar análises forenses sobre ameaças decisivas aos administradores.

Além disso, a tecnologia McAfee® Threat Intelligence Exchange capacita defesas adaptáveis a colaborar com outras soluções da McAfee, inclusive gateways, áreas restritas (sandboxes) e nossa solução de gerenciamento de eventos e informações de segurança (SIEM). A coleta e a distribuição de inteligência local, comunitária e global sobre segurança reduz o tempo decorrido entre ataque, descoberta e contenção, de semanas ou meses para milissegundos.

Combinada com o McAfee® Global Threat Intelligence (McAfee GTI), a estrutura do McAfee Endpoint Security aproveita a nuvem para monitorar e agir com base em todo o espectro de ameaças novas e emergentes em tempo real e em todos os vetores: arquivos, Web, mensagens e rede. O sistema de gerenciamento e a base instalada de endpoints são aprimorados com inteligência global e localizada contra ameaças para combater instantaneamente o malware desconhecido e direcionado. Ações automáticas contra aplicativos e processos suspeitos desencadeiam rapidamente respostas contra formas novas e emergentes de ataque, além de informar outras defesas e a comunidade global.

Os usuários do DAC e do Real Protect obtêm insights sobre ameaças mais avançadas e sobre seus comportamentos característicos. Por exemplo, o DAC fornece informações sobre aplicativos contidos e sobre o tipo de acesso que eles tentam obter, como ao Registro ou à memória.

Para organizações interessadas em coletar insights sobre ameaças em processos de endpoint para caçar malware e equipar os responsáveis pela resposta a incidentes, o Real Protect oferece insights sobre os comportamentos considerados maliciosos e classifica as ameaças. Esses insights podem ser particularmente úteis para revelar tentativas de evasão de detecção feitas por malware baseado em arquivo através de técnicas como compactação, criptografia ou uso indevido de aplicativos legítimos.

Um desempenho sólido e eficaz ajuda você a reagir a tempo

Defesas inteligentes são de pouco valor quando obstruem os usuários com varreduras lentas, levam muito tempo para serem instaladas ou são complicadas de gerenciar. O McAfee Endpoint Security preserva a produtividade dos usuários com uma camada de serviço comum e com nosso mecanismo antimalware principal que ajuda a reduzir a quantidade de recursos e energia exigidos pelo sistema do usuário. As varreduras de endpoint não afetam a produtividade do usuário porque só ocorrem quando o dispositivo está ocioso, sendo retomadas prontamente após uma reinicialização ou desligamento.

Um processo de varredura adaptável também ajuda a reduzir as exigências de CPU ao aprender quais processos e origens são confiáveis e, com isso, concentrar recursos somente naqueles que parecem suspeitos ou que se originam de fontes desconhecidas. O McAfee Endpoint Security possui um firewall integrado que utiliza o McAfee GTI para proteger endpoints contra redes de bots, ataques de negação de serviços distribuída (DDoS), ameaças persistentes avançadas e conexões perigosas na Web.

Alivie a pressão com menos complexidade e mais sustentabilidade

O rápido crescimento de produtos de segurança com sobreposição de funcionalidade e consoles de gerenciamento separados dificultou para muitos depreender uma imagem clara dos ataques potenciais. O McAfee Endpoint Security proporciona uma proteção sólida e de longo prazo, graças à sua estrutura aberta e expansível que atua como base para centralização de soluções de endpoint atuais e futuras. Essa estrutura aproveita o Data Exchange Layer para uma colaboração entre tecnologias, com os investimentos existentes em segurança. Sua arquitetura integrada coordena-se perfeitamente com outros produtos da McAfee, reduzindo ainda mais as lacunas de segurança, o isolamento de tecnologias e as redundâncias, além de melhorar a produtividade ao reduzir os custos operacionais e a complexidade do gerenciamento.

O software McAfee® ePolicy Orchestrator® (McAfee ePO™) pode reduzir ainda mais a complexidade ao proporcionar um painel único para monitoração, distribuição e gerenciamento de endpoints. Visualizações personalizáveis e fluxos de trabalho decisivos em linguagem compreensível constituem ferramentas para determinação rápida da postura de segurança, localização de infecções e redução do impacto das ameaças por meio da colocação de sistemas em quarentena, término de processos maliciosos ou bloqueio de vazamentos de dados. Ele também oferece um local único para gerenciar cada endpoint, outras capacidades da McAfee e mais de 130 soluções de segurança de terceiros.

Recurso	Por que você precisa dele
Detecção e resposta proativa a ameaças (MVISION Insights)	▪ Detecta possíveis ameaças, preditiva e preemptivamente, com base no seu setor e na sua região. ▪ Avalia localmente a postura de segurança contra a ameaça em potencial e oferece orientações sobre como melhorar a defesa. ▪ Fique à frente dos adversários estabelecendo proteções antes que o ataque aconteça.
Real Protect	▪ Sua classificação comportamental por autoaprendizagem detecta ameaças de dia zero quase em tempo real, viabilizando uma inteligência decisiva contra ameaças. ▪ Evolui automaticamente com o tempo, identificando novos comportamentos e adicionando regras para identificar ataques futuros.
Proteção de endpoint para ataques direcionados	▪ A proteção de endpoint reduz a lacuna entre localização e contenção, de dias para milissegundos. ▪ O McAfee Threat Intelligence Exchange coleta inteligência de diversas fontes, possibilitando que os componentes de segurança se comuniquem instantaneamente uns com os outros sobre ataques avançados emergentes e de múltiplas fases. ▪ O registro de eventos de Powershell e AMSI revela ataques sem arquivo e baseados em script e ajuda a proteger contra os mesmos.
Varredura inteligente e adaptável	▪ O desempenho e a produtividade são aprimorados contornando-se a varredura de processos confiáveis e priorizando-se processos e aplicativos suspeitos. ▪ A varredura comportamental adaptável monitora, visa e escala a ocorrência conforme exigido pela atividade suspeita.
Correção por reversão	▪ A correção por reversão reverte automaticamente alterações feitas pelo malware e retorna os sistemas ao seu último bom estado conhecido, preservando a produtividade dos usuários.
Segurança de Web proativa	▪ A segurança de Web proativa garante uma navegação segura com proteção de Web e filtragem para endpoints.
Contenção dinâmica de aplicativos	▪ A contenção dinâmica de aplicativos (DAC) defende contra ransomware e greyware e protege o “paciente zero”. [2]
Bloqueia ataques de redes hostis	▪ O firewall integrado utiliza pontuações de reputação baseadas no McAfee GTI para proteger endpoints contra redes de bots, DDoS, ameaças persistentes avançadas e conexões de Web suspeitas. ▪ A proteção por firewall só permite tráfego de saída durante a inicialização do sistema, protegendo endpoints quando estes não estão na rede corporativa.
Story Graph	▪ Os administradores podem ver rapidamente onde estão as infecções, por que elas estão ocorrendo e a duração da exposição para compreender a ameaça e reagir mais rapidamente.
Gerenciamento centralizado (plataforma McAfee ePO) com múltiplas opções de distribuição	▪ Um autêntico gerenciamento centralizado proporciona mais visibilidade, simplifica as operações, incrementa a produtividade da TI, unifica a segurança e reduz os custos.
Estrutura de segurança de endpoint aberta e expansível	▪ Sua arquitetura integrada permite que as defesas de endpoint colaborem e se comuniquem para uma defesa mais forte. ▪ Isso resulta em custos operacionais mais baixos devido à eliminação de redundâncias e da otimização de processos. ▪ A integração perfeita com outros produtos da McAfee e de terceiros reduz as lacunas da proteção.

Tabela 1. Principais recursos e por que você precisa deles.

Fique à frente das ameaças cibernéticas

O McAfee Endpoint Security oferece o que os profissionais de segurança de hoje precisam para superar as vantagens dos atacantes: defesas inteligentes e colaborativas, somadas a uma estrutura que simplifica ambientes complexos. Com um desempenho sólido e eficiente e uma eficácia na detecção de ameaças que é comprovada por testes de terceiros, as organizações podem proteger seus usuários, aumentar a produtividade e ter tranquilidade.

A McAfee, líder do mercado de segurança de endpoint, oferece uma gama completa de soluções que produzem defesa em profundidade e defesa proativa ao combinar proteções poderosas com gerenciamento eficiente, capacitando as equipes de segurança a resolver ameaças mais rapidamente e com menos recursos.

Migração facilitada

Ambientes com as versões atuais do software McAfee ePO, do McAfee VirusScan® Enterprise e do McAfee® Agent podem aproveitar nossa ferramenta de migração automática para migrar suas políticas existentes para o McAfee Endpoint Security em aproximadamente 20 minutos ou menos.[3]

Você terá as seguintes vantagens com o McAfee Endpoint Security:

- Varreduras de usuário com impacto zero para mais produtividade dos usuários
- Dados forenses mais sólidos mapeados no Story Graph para insights instantâneos e investigações simplificadas que ajudam você a reforçar as suas políticas
- Correção por reversão para desfazer automaticamente as alterações feitas pelo malware e preservar a saúde dos sistemas
- Insights proativos sobre ameaças em potencial priorizadas e orientações prescritivas sobre como ajustar as suas contramedidas contra as ameaças com o MVISION Insights
- Menos agentes para gerenciar e menos varreduras desnecessárias para reduzir interações
- Defesas colaborativas que trabalham juntas para derrotar ameaças avançadas
- Uma estrutura da próxima geração, pronta para se conectar a outras soluções de detecção e resposta (EDR) para endpoints contra ameaças avançadas

Saiba Mais

Para saber mais sobre o McAfee Endpoint Security, visite-nos clicando aqui.

Para saber mais sobre como o McAfee Endpoint Security complementa o portfólio de produtos da McAfee, visite:

- MVISION Endpoint
- Família de produtos MVISION
- McAfee Threat Intelligence Exchange
- MVISION EDR
- McAfee ePolicy Orchestrator
- MVISION Insights

1. Disponível com a maioria dos pacotes para endpoint da McAfee. Para obter detalhes, consulte um representante de vendas.
2. Ibid.
3. O tempo de migração depende do seu ambiente e das suas políticas existentes.

McAfee

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