Família McAfee Endpoint Threat Defense and Response

Detecte malware de dia zero, proteja o paciente zero e combata ataques avançados

A escalada na sofisticação das ameaças cibernéticas requer uma nova geração de proteção para endpoints. Ameaças avançadas e o risco crescente de vulnerabilidades desconhecidas estão fazendo com que as organizações reúnam soluções de segurança sobrepostas e desconectadas que proporcionam visibilidade limitada e complexidade maior. A McAfee resolve esse problema com o McAfee® Endpoint Threat Defense e com o McAfee Endpoint Threat Defense and Response. Ambas as soluções aproveitam análises estáticas e comportamentais e sintetizam inteligência para proteger, detectar, corrigir e se adaptar para combater ameaças emergentes. Componentes de segurança unificados atuam como um só através de uma abordagem aberta e integrada, com compartilhamento de visibilidade e inteligência contra ameaças e fluxos de trabalho simplificados. Segurança conectada e análises forenses decisivas contra ameaças proporcionam uma infraestrutura segura para condenar ameaças com rapidez e eficiência, ficando à frente de atacantes potenciais.

Acabe com o malware de dia zero, o greyware e o ransomware

Fique à frente das ameaças emergentes com análises estáticas e dinâmicas de ameaças que aproveitam informações aprimoradas de reputação e comportamentais para detectar possíveis explorações. Aplique inteligência sintetizada com o McAfee Threat Intelligence Exchange para bloquear e conter ameaças imediatamente e atualizar instantaneamente a reputação das ameaças para prevenir ataques futuros.

Principais vantagens

- Detecte, proteja e corrija enquanto adapta proativamente suas defesas contra malware de dia zero, greyware e ransomware
- Proteja com mais eficiência utilizando reputações dinâmicas, análise comportamental e autoaprendizagem
- Minimize o impacto sobre usuários e aplicativos corporativos confiáveis com uma proteção aprimorada
- Responda a mais ameaças e as corrija mais rapidamente com uma inteligência sobre ameaças compartilhada pelo seu ecossistema de segurança
- Simplifique a investigação e a correção de incidentes com fluxos de trabalho unificados e um console único para gerenciamento através do software McAfee® ePolicy Orchestrator® (McAfee ePO™)

O McAfee Endpoint Threat Defense e o McAfee Endpoint Threat Defense and Response acabam com o malware de dia zero identificando similaridades entre os comportamentos maliciosos exibidos e os extensivos modelos de ameaças do Real Protect utilizando uma consulta em nuvem (com data centers hospedados nos Estados Unidos). Essa técnica de classificação comportamental é utilizada para erradicar ameaças ao vivo que possam ter passado por outras defesas de software de segurança. Ela proporciona uma inteligência contra ameaças decisiva através do software McAfee ePolicy Orchestrator, viabilizando descobertas de dia zero e correções em tempo real. A classificação comportamental evolui automaticamente por meio de autoaprendizagem dinâmica, proporcionando máxima proteção e eficiência e limitando a exposição da segurança.

Reduza a quantidade de eventos e resolva as ameaças mais rapidamente

Concentre-se no que é mais importante reduzindo a quantidade de eventos de segurança, condenando mais ameaças automaticamente, compartilhando inteligência e utilizando alertas proativos para definir respostas automáticas. Reduza o trabalho necessário para investigar e resolver ameaças com fluxos de trabalho simplificados que resolvem eventos mais rapidamente e expandem a capacidade da segurança enquanto aumentam a proteção por toda a sua organização.

Componentes conectados automaticamente compartilham valiosas informações de segurança por meio do McAfee Data Exchange Layer. O McAfee Threat Intelligence Exchange permite sintetizar uma inteligência abrangente contra ameaças em todo o seu ecossistema, incluindo o McAfee Global Threat Intelligence e outras fontes de terceiros, e compartilhar imediatamente informações sobre ameaças para adaptar automaticamente a sua proteção.

Proteja o paciente zero

Detecte e impeça que o malware de dia zero faça alterações maliciosas em sistemas de endpoint. A contenção dinâmica de aplicativos observa o comportamento do greyware e impede alterações maliciosas para efetivamente interromper as explorações antes que elas comecem. Proteja endpoints, dentro e fora das redes, e contenha comportamentos maliciosos com uma proteção invisível para os usuários.

Operacionalize processos de segurança para dimensionamento e adaptação

A imposição de políticas, a investigação de incidentes e a correção são simplificadas através do software McAfee ePO, um console de gerenciamento unificado que proporciona visibilidade sobre todos os sistemas para que você possa determinar prontamente a postura de segurança dos endpoints e ativar a proteção em tempo real. Reduza o trabalho de monitoramento, pesquisa e resposta com fluxos de trabalho unificados e correção com um só clique em um único endpoint ou em toda a infraestrutura. Com o McAfee Endpoint Threat Defense e o McAfee Endpoint Threat Defense and Response, aproveite a autoaprendizagem automatizada para atualizar os modelos de classificação de comportamento e compartilhar instantaneamente a inteligência contra ameaças por todos os componentes de segurança para que eles possam atuar como um sistema único e unificado contra as ameaças emergentes. Previna ataques futuros e aproveite reações predefinidas para conter ameaças potenciais e para que você possa liberar a sua equipe e deixá-la se concentrar em outras prioridades do gerenciamento de segurança.

Revele, priorize e remedie ataques avançados

O McAfee Endpoint Threat Defense and Response ajuda a determinar a origem, o alcance e o impacto de um ataque. Ele utiliza a tecnologia McAfee Active Response para proporcionar visibilidade ao vivo e histórica sobre os endpoints da sua infraestrutura. Indicadores de ataque são identificados e priorizados com um contexto sólido para viabilizar respostas mais rápidas.

Persiga proativamente as ameaças, com precisão, velocidade e agilidade, para eliminar as que estejam se propagando ativamente, que estejam à espreita ou que tenham apagado seus rastros para evitar detecções.

Visibilidade e controle orientados por conhecimento identificam onde as ameaças estão tentando estabelecer uma presença e permitem que os responsáveis pela resposta a incidentes façam contenções e correções imediatas, reduzindo a exposição de meses para minutos, ou até mesmo milissegundos.

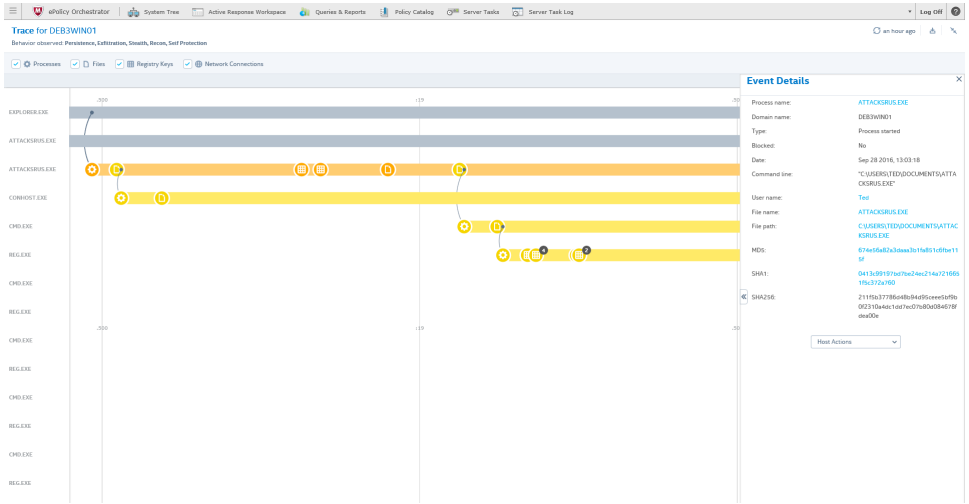

Figura 1. O cenário de ameaças rastreia a origem e o comportamento de incidentes suspeitos para acelerar a resposta a incidentes.

Capacidades da família McAfee Endpoint Threat Defense and Response

Componente	Vantagem	Benefícios para o cliente	Diferenciação	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Contenção dinâmica de aplicativos[1]	Protege o paciente zero evitando que o greyware faça alterações maliciosas em endpoints, tanto dentro quanto fora da rede.	▪ Viabilize a análise de ameaças em potencial sem sacrificar o paciente zero. ▪ Aumente a proteção sem afetar os usuários ou os aplicativos confiáveis. ▪ Reduza o tempo do encontro à contenção, com o mínimo de intervenção manual. ▪ Proteja o paciente zero e, ao mesmo tempo, preserve a produtividade do endpoint e isole a rede da infecção.	▪ Parte integrante da infraestrutura da McAfee para máxima proteção e eficiência. ▪ Trabalha com ou sem uma conexão com a Internet e não requer interação ou análise externa. ▪ Transparente para o usuário. ▪ O modo de observação proporciona visibilidade instantânea sobre as ameaças ao expor comportamentos de exploração dentro do ambiente.	√	√
Real Protect	Aplica classificação de comportamento por autoaprendizagem para bloquear malware de dia zero antes que este seja executado e interrompe ameaças ao vivo que tenham escapado de detecções anteriores.	▪ Acabe facilmente com mais malware de dia zero, incluindo objetos de difícil detecção, como ransomware. ▪ Desmascare, analise e corrija ameaças automaticamente, sem a exigência de intervenção manual. ▪ Adapte as defesas utilizando classificação automatizada e uma infraestrutura de segurança conectada.	▪ Análises comportamentais dinâmicas e estáticas proporcionam melhor proteção do que abordagens de um só estágio. ▪ Detecta malware que só pode ser encontrado por meio de análise comportamental dinâmica. ▪ Uma integração avançada compartilha atualizações de reputação em tempo real e aumenta a eficácia da segurança para todos os componentes de segurança.	√	√

DATA SHEET DA FAMÍLIA DE SOLUÇÕES

Componente	Vantagem	Benefícios para o cliente	Diferenciação	McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
McAfee Threat Intelligence Exchange	Conecta os componentes da segurança para compartilhar insights contextuais e proporcionar visibilidade e controle por toda a organização para uma proteção adaptável contra as ameaças.	▪ Viabilize a identificação de ameaças no paciente zero e o compartilhamento instantâneo pelo sistema de segurança para prevenir a próxima infecção. ▪ Reduza o custo total de propriedade e operacionalize com eficiência a segurança de endpoint. ▪ Conecte os componentes da segurança para criar uma proteção de loop fechado, transformando tecnologias de segurança independentes em um único sistema coordenado.	▪ Sintetize canais do McAfee Global Threat Intelligence, informações de terceiros e inteligência local. ▪ Defina o que é e o que não é confiável com inteligência local ou de terceiros. ▪ Conecte instantaneamente informações sobre reputação de ameaças entre produtos de endpoint, Web, rede e nuvem. ▪ Extraia relatórios decisivos e detalhados de inteligência contra ameaças para adaptar as defesas.	√	√
McAfee Data Exchange Layer	Conecta a segurança para integrar e simplificar a comunicação com produtos da McAfee e de terceiros.	▪ Reduza o risco e o tempo de resposta. ▪ Reduza a sobrecarga e os custos da equipe operacional. ▪ Otimize processos e recomendações práticas.	▪ Compartilhe informações sobre ameaças entre todos os produtos de segurança. ▪ Compartilhe instantaneamente insights sobre ameaças do tipo “paciente zero” com todos os outros endpoints para prevenir infecções e atualizar a proteção.	√	√
McAfee ePO Management Platform	Um painel unificado para um gerenciamento altamente expansível, flexível e automatizado das políticas de segurança para identificar e responder a questões de segurança.	▪ Unifique e simplifique os fluxos de trabalho de segurança para obter eficiências comprovadas. ▪ Visibilidade em painel unificado sobre todos os sistemas para determinar prontamente a postura de segurança e a proteção em tempo real. ▪ Distribua e gerencie rapidamente a proteção da McAfee com imposição de políticas personalizadas. ▪ Reduza o tempo do insight à resposta com consultas, dashboards e respostas dinâmicas e automatizadas.	▪ Controle granular, custos mais baixos e um gerenciamento de segurança operacional mais rápido através de um console único. ▪ Dashboards de arrastar e soltar proporcionam mais visibilidade em tempo real por todo o ecossistema. ▪ Kits de desenvolvimento de software (SDKs) de plataforma aberta facilitam a adoção rápida de futuras inovações em segurança.	√	√
McAfee Active Response	Visibilidade proativa sobre ameaças, linhas de tempo, caçada ao vivo e histórica, e detecção, com a capacidade de realizar ações imediatas e adaptar a proteção.	▪ Pesquise rapidamente dados de ameaças ao vivo e históricas para determinar todo o alcance do ataque, acelerar as investigações e reduzir o tempo de resposta. ▪ Automatize as respostas às ameaças e ofereça proteção ao vivo, sem intervenção manual. ▪ Priorize ameaças de alta prioridade. ▪ Use monitoramento contínuo e coletores personalizáveis para procurar profundamente indicadores de ataque que não apenas estejam em execução ou adormecidos, mas que possam até já ter sido excluídos.	▪ Visibilidade instantânea sobre tentativas de exploração desconhecidas e comportamentos arriscados em execução no ambiente que não tenham sido detectados por tecnologias de proteção. ▪ Investigue a linha de tempo dos eventos em cada endpoint com pesquisa ao vivo integrada por todos os endpoints para caçar ameaças. ▪ Ação de um só clique para proteger, corrigir e adaptar, concentrando múltiplas ferramentas e etapas em uma única operação.		√

Especificações

McAfee Endpoint Threat Defense	McAfee Endpoint Threat Defense and Response
Plataformas compatíveis:	**Plataformas compatíveis:**
▪ Microsoft Windows: 7, To Go, 8, 8.1, 10, 10 November, 10 Anniversary	▪ Microsoft Windows: 7, 8, 8.1, 10, 10 Anniversary
▪ Mac OSX versão 10.5 ou posterior	▪ RedHat 6.5
▪ Linux: RHEL, SUSE, CentOS, OEL, Amazon Linux e Ubuntu nas versões mais recentes	▪ CentOS 6.5
Servidores:	▪ Windows Server 2008, 2012, 2016
▪ Windows Server (2003 SP2 ou posterior, 2008 SP2 ou posterior, 2012), Windows Server 2016	
▪ Windows Embedded (Standard 2009, Point of Service 1.1 SP3 ou posterior)	
▪ Citrix Xen Guest	
▪ Citrix XenApp 5.0 ou posterior	

1. O McAfee Endpoint Threat Defense and Response inclui data centers hospedados nos EUA que são utilizados para validar a autenticação do cliente, verificar reputações de arquivos e armazenar dados relevantes para detecção e busca de arquivos suspeitos. Embora não seja obrigatório, a tecnologia de contenção dinâmica de aplicativos funciona melhor com uma conexão com a nuvem. As capacidades McAfee Active Response, de contenção dinâmica de aplicativos e Real Protect dos produtos exigem acesso à nuvem e suporte ativo, e estão sujeitas aos termos e condições do serviço de nuvem.

Learn More

Saiba mais sobre as vantagens do McAfee Endpoint Threat Defense em **www.mcafee.com/br/products/endpoint-threat-defense.aspx.**

Saiba mais sobre as vantagens do McAfee Endpoint Threat Defense and Response em **www.mcafee.com/br/products/endpoint-threat-defense-response.aspx.**

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