McAfee Advanced Threat Defense

Detecção de ataques direcionados avançados

O McAfee® Advanced Threat Defense permite que as organizações detectem os ataques direcionados avançados e convertam as informações sobre ameaças em ação e proteção imediatas. Diferentemente da sandbox (área restrita) tradicional, estão incluídas capacidades adicionais de inspeção que ampliam a detecção e expõem ameaças evasivas. Uma forte integração entre soluções de segurança — da rede ao endpoint — permite o compartilhamento instantâneo de informações sobre ameaças por todo o ambiente, aprimorando a proteção e a investigação. Opções de distribuição flexíveis proporcionam suporte para qualquer rede.

Nossa tecnologia transformou o ato de detecção ao associar os recursos de análise de malware avançado às defesas existentes — do perímetro da rede até o endpoint — e ao compartilhar informações sobre ameaças com todo o ambiente de TI. Ao compartilhar informações sobre ameaças entre os sistemas de gerenciamento, rede e endpoint, nossas soluções interrompem imediatamente as comunicações de comando e controle, colocam sistemas comprometidos em quarentena, bloqueiam instâncias adicionais da mesma ameaça ou de ameaças semelhantes, determinam onde podem ter ocorrido danos e tomam as providências necessárias.

McAfee Advanced Threat Defense: detecção de ameaças avançadas

O McAfee Advanced Threat Defense detecta o malware furtivo e de dia zero de hoje com uma abordagem inovadora e em camadas. Ele combina mecanismos estáticos de baixo impacto, como assinaturas antivírus, reputação e emulação em tempo real, com análises dinâmicas (sandboxing) para investigar o comportamento real. A investigação prossegue com análises profundas de código estático que inspecionam atributos de arquivo e conjuntos de instruções para determinar comportamentos intencionais ou evasivos, além de estabelecer se há semelhança com famílias de malware conhecidas. Como etapa final na análise, o McAfee Advanced Threat Defense procura

Principais diferenciais do McAfee Advanced Threat Defense

Integração completa com as soluções da McAfee

- Elimina a brecha que separa a localização da contenção e da proteção por toda a organização
- Otimiza fluxos de trabalho para agilizar a resposta e a correção

Recursos eficazes de análise

- Emprega uma descompactação sólida para obter análises melhores e mais completas
- Combina análises profundas de código estático, análises dinâmicas e autoaprendizagem para proporcionar uma detecção mais precisa, com dados de análise inigualáveis

especificamente por indicadores maliciosos que tenham sido identificados por autoaprendizagem através de uma rede neural profunda. No conjunto, isso tudo representa a proteção de segurança contra malware avançado mais forte do mercado, efetivamente estabelecendo um equilíbrio entre desempenho e a necessidade de inspeção profunda. Embora métodos de menor intensidade analítica, como assinaturas e emulação em tempo real, favoreçam o desempenho ao capturar malware conhecido, o acréscimo de análise profunda de código estático e insights obtidos por autoaprendizagem ao recurso de sandboxing estende a proteção contra ameaças altamente evasivas e camufladas. Indicadores maliciosos que podem não ser executados em um ambiente dinâmico podem ser identificados por meio de descompactação, análise profunda de código estático e insights de autoaprendizagem.

Os criadores de malware usam a compactação para alterar a composição do código ou ocultá-lo para impedir sua detecção. A maioria dos produtos não consegue descompactar corretamente todo o código executável original (fonte) para análise. O McAfee Advanced Threat Defense inclui recursos abrangentes de descompactação que removem a ocultação, expondo o código executável original. Ele permite que a análise profunda de código estático examine além dos atributos de alto nível do arquivo para encontrar anomalias, analisando atributos e conjuntos de instruções para determinar o comportamento pretendido.

Juntas, a análise profunda de código estático, a autoaprendizagem e a análise dinâmica proporcionam uma avaliação completa e detalhada do malware suspeito. Os resultados inigualáveis dessas análises são usados na geração de relatórios resumidos que proporcionam ampla compreensão e priorização de ações, além de relatórios mais detalhados que fornecem dados analíticos de qualidade sobre o malware.

Proteção aprimorada

Encontrar o malware avançado é importante. Mas se a única coisa que uma solução pode fazer é gerar um relatório ou um alerta, os administradores continuarão tendo uma quantidade imensa de trabalho e a rede permanecerá desprotegida.

Uma sólida integração entre o McAfee Advanced Threat Defense e os dispositivos de segurança — do perímetro da rede até o endpoint — permite ações imediatas dos dispositivos de segurança integrados quando o McAfee Advanced Threat Defense determina que um arquivo é malicioso. Essa integração automatizada e poderosa entre detectar e proteger é crucial.

O McAfee Advanced Threat Defense pode ser integrado de diversas formas: diretamente com determinadas soluções de segurança, através do McAfee Threat Intelligence Exchange ou através do McAfee Advanced Threat Defense Email Connector.

A integração direta permite que as soluções de segurança da McAfee ajam imediatamente em relação aos arquivos condenados pelo McAfee Advanced Threat Defense. Elas podem incorporar imediatamente as informações de ameaças aos processos existentes de imposição de política e bloquear a entrada de instâncias adicionais do mesmo arquivo ou de arquivos semelhantes na rede.

Distribuição flexível e centralizada

- Reduza os custos com uma distribuição centralizada e compatível com diversos protocolos
- Opções de distribuição flexíveis proporcionam suporte para qualquer rede

Soluções integradas

- McAfee Active Response
- McAfee Advanced Threat Defense Email Connector
- McAfee Enterprise Security Manager
- McAfee ePolicy Orchestrator®
- McAfee Network Security Platform
- McAfee Threat Intelligence Exchange
  - McAfee Application Control
  - McAfee Endpoint Protection
  - McAfee Security for Email Servers
  - McAfee Server Security
- McAfee Web Gateway

As condenações do McAfee Advanced Threat Defense são exibidas nos dashboards e logs dos produtos integrados, como se toda a análise tivesse sido concluída internamente, simplificando os fluxos de trabalho e permitindo que os administradores gerenciem os alertas de forma eficiente ao trabalhar a partir de uma única interface.

A integração com o McAfee Threat Intelligence Exchange estende os recursos do McAfee Advanced Threat Defense para defesas adicionais, incluindo o McAfee Endpoint Protection, e permite o acesso de diversas soluções de segurança integradas aos resultados da análise e aos indicadores de comprometimento. Se um arquivo é condenado pelo McAfee Advanced Threat Defense, o McAfee Threat Intelligence Exchange imediatamente publica as informações sobre a ameaça através de uma atualização de reputação, disponível para todas as contramedidas integradas dentro da organização.

Os endpoints ativados pelo McAfee Threat Intelligence Exchange podem bloquear as instalações de malware "paciente zero" e oferecer proteção proativa se o arquivo aparecer posteriormente. Os gateways ativados pelo McAfee Threat Intelligence Exchange podem impedir que o arquivo entre na organização. Além disso, os endpoints ativados pelo McAfee Threat Intelligence Exchange continuam a receber atualizações de condenação de arquivo quando estão fora da rede, eliminando os pontos cegos da entrega de carga fora de banda.

O McAfee Advanced Threat Defense Email Connector possibilita que o McAfee Advanced Threat Defense receba anexos de e-mail de um gateway de e-mail para análise. O McAfee Advanced Threat Defense analisa os arquivos dos anexos e retorna um veredito ao gateway de encaminhamento de e-mail, dentro do cabeçalho da mensagem. O gateway de e-mail pode, então, realizar ações com base na política, como excluir o anexo ou colocá-lo em quarentena, evitando que o malware infecte e se espalhe pela rede interna. Para uma detecção aprimorada no servidor de e-mail, o McAfee Advanced Threat Defense integra-se com o McAfee Security for Email Servers através do McAfee Threat Intelligence Exchange.

Localização e correção de sistemas comprometidos

Para corrigir um ataque, as organizações precisam de visibilidade abrangente com informações decisivas e priorizadas para tomar melhores decisões e reagir de forma apropriada. As soluções McAfee trabalham juntas para oferecer às organizações exatamente o que elas necessitam.

O McAfee Enterprise Security Manager assimila e correlaciona informações detalhadas sobre a reputação de arquivos e eventos de execução do McAfee Advanced Threat Defense e de outros sistemas de segurança para apresentar alertas avançados e históricos sobre informações de segurança aprimorada, priorização de riscos e percepção situacional em tempo real.

Com dados de indicadores de comprometimento do McAfee Advanced Threat Defense, o McAfee Enterprise Security Manager examina retroativamente seis meses à procura de indícios dessas anomalias nos dados de qualquer rede ou sistema que tenham sido retidos. Isso pode revelar sistemas que tenham se comunicado previamente com fontes de malware recém-identificadas. O McAfee Enterprise Security Manager fornece um entendimento claro do risco para que ações corretivas imediatas — interativas ou automatizadas — sejam tomadas. A sólida integração com o McAfee Endpoint Protection, o McAfee Threat Intelligence Exchange e o McAfee Active Response otimiza a resposta e a eficiência das operações de segurança com visibilidade e ação, como a emissão de novas configurações, implementação de novas políticas, remoção de arquivos e distribuição de atualizações de software que podem mitigar o risco de forma proativa. Uma ação informada pode ser facilmente executada quando endpoints infectados da rede são automaticamente identificados pelo McAfee Active Response e listados nos relatórios do McAfee Advanced Threat Defense.

Distribuição

Opções de distribuição flexíveis de análises de ameaças avançadas proporcionam suporte para qualquer rede. O McAfee Advanced Threat Defense está disponível como um appliance no local ou de forma virtual. Em qualquer formato, ele atua como um recurso compartilhado entre múltiplas soluções da McAfee, dimensionando-se economicamente e reduzindo custos.

Os centros de operações de segurança e os analistas de malware também podem usar o McAfee Advanced Threat Defense para investigações.

O McAfee Advanced Threat Defense oferece diversas capacidades avançadas, incluindo:

- Suporte configurável para sistemas operacionais e aplicativos: adeque imagens de análise com variáveis de ambiente selecionadas para validar ameaças e apoiar as investigações.
- Modo interativo com o usuário: permite que os analistas interajam diretamente com amostras de malware.
- Amplos recursos de descompactação: diminuem o tempo de investigação de dias para minutos.
- Caminho lógico completo: permite uma análise de amostras mais profunda ao forçar a execução de caminhos lógicos adicionais que ficam latentes em ambientes de área restrita (sandbox) típicos.
- Envio de amostras para múltiplos ambientes virtuais: acelera a investigação ao determinar quais variáveis de ambiente são necessárias para a execução do arquivo.
- Relatórios detalhados de resultados de desmontagem de código, descargas de memória, diagramas de chamadas de funções gráficas, informações sobre arquivos incorporados ou inseridos, logs de API do usuário e informações PCAP: proporcionam informações críticas para as investigações dos analistas.

Para obter informações ou começar uma avaliação do McAfee Advanced Threat Defense, entre em contato com seu representante ou visite **www.mcafee.com/br/products/advanced-threat-defense.aspx**.

Especificações do McAfee Advanced Threat Defense		
Formato físico	ATD-3100 1U para montagem em rack	ATD-6100 1U para montagem em rack
Formato virtual	v1008, v1016, v3032, v6064 ESXi 5.5, 6.0	v1008, v1016, v3032, v6064 ESXi 5.5, 6.0
Detecção		
Tipos de amostra de arquivo compatíveis	Arquivos PE, Adobe, Microsoft Office, de imagem, compactados, Java, Android Application Package e URLs	
Métodos de análise	McAfee Anti-Malware Engine, reputação no McAfee GTI (arquivo/URL/IP), Gateway Anti-Malware (emulacão e análise comportamental), análise dinâmica (sandboxing), análise profunda de código, regras YARA personalizadas, autoaprendizagem: rede neural profunda	
Sistemas operacionais compatíveis	Windows 10 (64 bits), Windows 8.1 (64 bits), Windows 8 (32 bits/64 bits), Windows 7 (32 bits/64 bits), Windows XP (32 bits/64 bits), Windows Server 2016, Windows Server 2012, Windows Server 2012 R2, Windows Server 2008, Windows Server 2003, Android O suporte para o sistema operacional Windows está disponível em todos os idiomas.	
Formatos de saída	STIX, OpenIOC, XML, JSON, HTML, PDF, texto	
Métodos de envio	Integrações com produtos individuais, APIs RESTful, envio manual e McAfee Advanced Threat Defense Email Connector (SMTP)	

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