McAfee Advanced Threat Defense

Detectar malware avançado

O McAfee® Advanced Threat Defense permite que as organizações detectem malware avançado e evasivo e convertam 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 e à investigação — 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 pelo ecossistema, as soluções de segurança integradas trabalham juntas interrompendo imediatamente as comunicações de comando e controle, colocando em quarentena os sistemas comprometidos, bloqueando instâncias adicionais da mesma ameaça ou de ameaças semelhantes, determinando qual foi o impacto, investigando e tomando providências.

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 de análise 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.

Principais diferenciais do McAfee Advanced Threat Defense

Ampla integração de soluções

- Integração com as soluções existentes da McAfee, gateways de e-mail de terceiros e outros produtos compatíveis com padrões abertos
- Elimina a lacuna entre localização da ameaça e sua contenção e proteção por toda a organização
- Otimiza fluxos de trabalho para agilizar a resposta e a correção
- Viabiliza a automação

Recursos eficazes de análise

- Combina análises profundas de código estático, análises dinâmicas e autoaprendizagem para proporcionar uma detecção mais precisa, com dados de análise inigualáveis
- Recursos avançados apoiam o SOC e viabilizam as investigações

Conecte-se conosco

Como etapa final na análise, o McAfee Advanced Threat Defense procura 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 o malware mais facilmente identificável, o acréscimo da análise profunda de código estático e de insights obtidos por autoaprendizagem ao recurso de sandboxing amplia a detecção de ameaças altamente camufladas e evasivas. 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

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.

Uma integração direta permite que as soluções de segurança atuem 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

- Reduz 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
- Bro Network Security Monitor
- TAXII (Trusted Automated eXchange of Indicator Information)

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 para todos os gateways e-mail ativos 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. Um modo off-line permite que e-mails com anexos sejam entregues ao usuário final enquanto são examinados pelo McAfee Advanced Threat Defense. O gateway de e-mail não espera por um veredito quanto ao anexo. Os administradores visualizam os resultados da varredura de anexos através do McAfee Advanced Threat Defense ou do McAfee Threat Intelligence Exchange. 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.

Compartilhamento de ameaças para aprimorar e automatizar a investigação

Para investigar e corrigir um ataque, as organizações precisam de visibilidade abrangente com informações decisivas para tomar melhores decisões e reagir de forma apropriada. O McAfee Advanced Threat Defense produz uma inteligência sobre ameaças profunda que é facilmente compartilhada por todo o seu ambiente

para aprimorar e automatizar as investigações. O suporte às interfaces de programação de aplicativos (APIs) REST e Data Exchange Layer (DXL) propicia integrações com outros produtos e padrões de compartilhamento de ameaças amplamente utilizados, como o Structured Threat Information eXpression (STIX) / Trusted Automated eXchange of Indicator Information (TAXII), e viabiliza ainda mais a criação, suporte e expansão de um ecossistema de segurança colaborativo por parte das organizações.

Dentro de um ecossistema McAfee, 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 oferecer visualizações avançadas de alertas 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. 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. A eficiência dos analistas é incrementada quando esses relatórios detalhados são visualizados a partir de um mesmo espaço de trabalho dentro do McAfee Active Response.

Capacidades avançadas como suporte à investigação

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:** fornecem informações críticas para a investigação, incluindo mapeamento MITRE ATT&CK™, decodificação de código de máquina (disassembly), descargas de memória, diagramas de chamadas de funções gráficas, informações sobre arquivos incorporados ou inseridos, logs de API do usuário e informações PCAP. Cronogramas de ameaças ajudam na visualização das etapas de execução dos ataques.
- **Integração com o Bro Network Security Monitor:** distribua o sensor Bro em um segmento de rede suspeito para monitorar e capturar o tráfego e encaminhar arquivos ao McAfee Advanced Threat Defense para inspeção.

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 em um formato virtual, com suporte para nuvem tanto privada quanto pública e disponibilidade no Azure Marketplace.

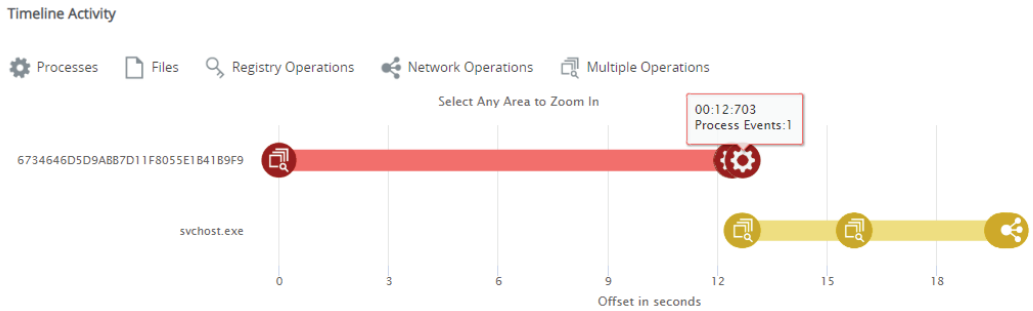

Figura 1. A exibição de atividades em uma linha de tempo permite visualizar as etapas de execução da ameaça analisada.

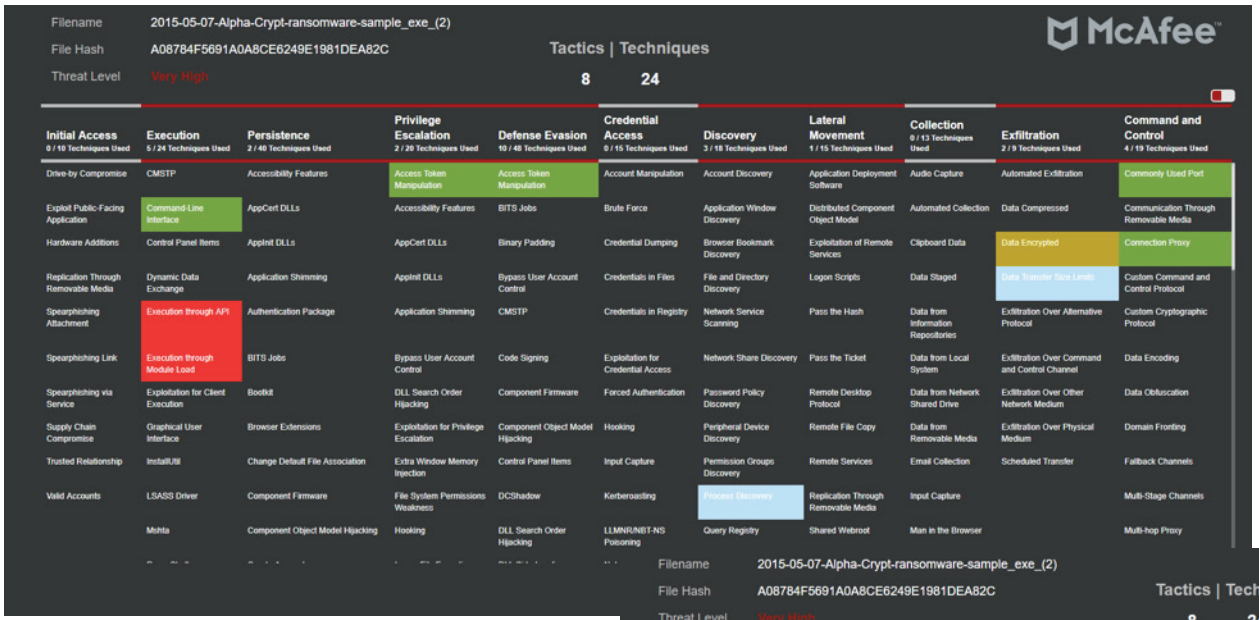

Figura 2. Mapa de resultados da estrutura MITRE ATT&CK™.

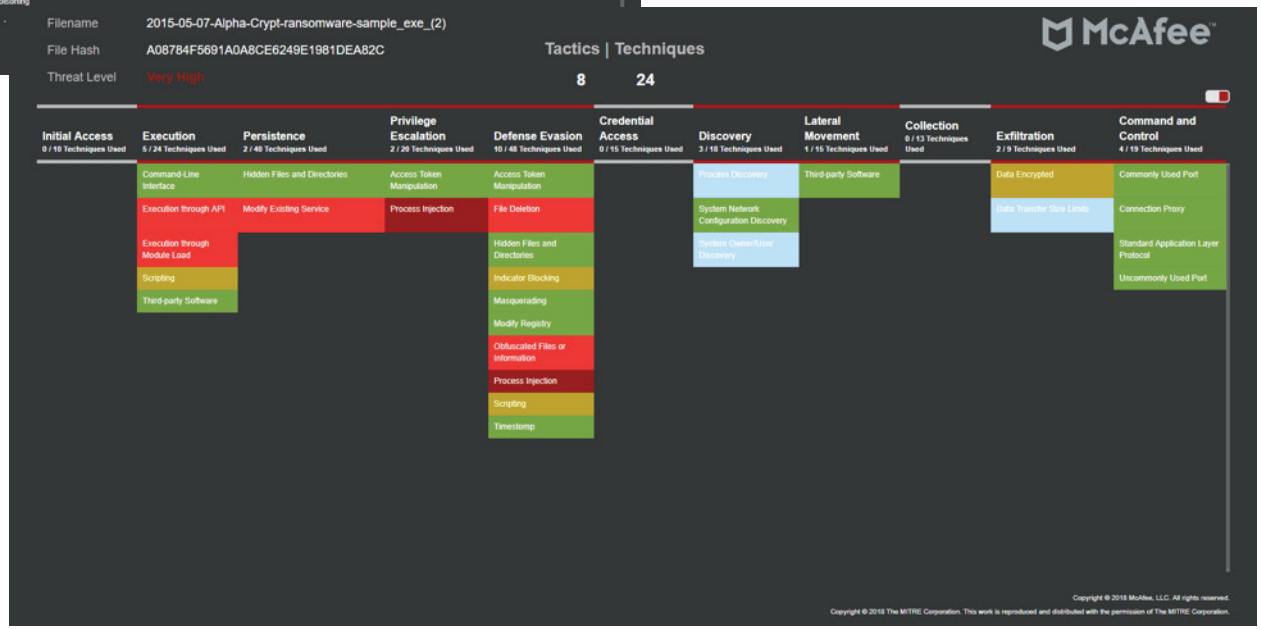

Figura 3. Uma visualização filtrada dos resultados exibidos na figura 2 permite ver detalhes sobre as técnicas identificadas.

Especificações do McAfee Advanced Threat Defense		
Formato físico	ATD-3200 1U para montagem em rack	ATD-6200 1U para montagem em rack
Formato virtual	v1008 ESXi 5.5, 6.0, 6.5, 6.7 Hyper-V Windows Server 2012 R2, Windows Server 2016	
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 (emulação e análise comportamental), análise dinâmica (sandboxing), análise profunda de código, regras YARA personalizadas, autoaprendizagem	
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)	

Saiba mais

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

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