Resumo da Solução

Monitore continuamente. Reaja com rapidez.

O McAfee® Active Response otimiza a detecção e a correção de ataques direcionados avançados.

Em todos os dias do ano passado, 2.803.036 registros de dados foram perdidos ou roubados devido a uma violação de dados e as pesquisas indicam que os números continuam aumentando em um ritmo alarmante. No ano passado, houve um total de 1.540 casos de violações de dados, um aumento de 46% em relação ao ano anterior[1]. A maioria das organizações que se preocupam com a segurança percebem rapidamente que as soluções tradicionais para endpoints, que são configuradas uma vez e "esquecidas" em seguida, não são capazes de proteger contra a enxurrada de ataques direcionados avançados (ATAs, do inglês "advanced targeted attacks") e ataques de dia zero. As equipes de segurança precisam de visibilidade ininterrupta da atividade dos endpoints em vez de alertas gerados pelos produtos de segurança depois que o problema já ocorreu. Uma solução de detecção e resposta de endpoints (EDR, do inglês "endpoint detection and response") é um complemento fundamental para as defesas atuais. Segundo a Gartner, "as organizações que investem em ferramentas de EDR estão deliberadamente abandonando a mentalidade de 'resposta a incidentes' e adotando uma abordagem de 'monitoramento contínuo' em busca de incidentes que, como se sabe, ocorrem com frequência[2]".

A proteção insuficiente da maioria das soluções para endpoints

Em vez de adotar uma abordagem proativa, a maioria das equipes de resposta a incidentes atualmente utiliza uma metodologia reativa. Muitas vezes, as ameaças são descobertas somente depois que os danos já ocorreram. Após driblar suas defesas, os ATAs permanecem instalados de forma oculta por um período prolongado, podendo proliferar-se por toda a sua infraestrutura até provocar uma violação.

As soluções tradicionais para endpoints, com antivírus com base em assinaturas, prevenção de perda de dados, prevenção de intrusão nos hosts e outros recursos básicos. oferecem uma visibilidade limitada do que realmente está ocorrendo nos seus endpoints em toda a sua infraestrutura. Isso acontece principalmente quando várias ferramentas de diferentes fornecedores estão implementadas. Essa abordagem fragmentada torna a busca e a análise da atividade de ameaças uma tarefa difícil e cara. As equipes de segurança sempre dependeram de varreduras programadas para ter uma visão da postura de segurança da empresa, mas essas verificações ocasionais estão longe de ser suficientes, principalmente quando se considera que mais de 307 novas ameaças surgem a cada minuto (mais de cinco por segundo), segundo o *Relatório de ameaças de novembro de 2014* do McAfee Labs.[3] Além da abundância de malwares de dia zero, as varreduras programadas não identificam ameaças multivetoriais inativas que podem ter se infiltrado na sua infraestrutura sem ser detectadas, esperando o momento certo de atacar.

intel Security

Resumo da Solução

Em geral, as equipes de segurança não conseguem manter-se informadas da atividade maliciosa porque os recursos são escassos, os profissionais têm tempo limitado e os processos inflexíveis de resposta a incidentes não são suficientes para lidar com ataques de grandes proporções. À medida que cada vez mais endpoints são incorporados à infraestrutura (laptops, desktops, dispositivos móveis e servidores), a TI tem o desafio de gerenciar esses sistemas, oferecer a segurança adequada e coletar informações sobre as ameaças.

Por que todos precisam do McAfee Active Response

Muito em breve, a tecnologia de EDR será um componente fundamental da estratégia e das práticas de segurança cibernética de todos os usuários. Como sugere o consultor de segurança John Reed Stark, "as ferramentas de EDR deixam as empresas mais aptas a detectar e reagir a ameaças externas e internas, aumentam sua velocidade e flexibilidade para conter ataques ou anormalidades futuras e ajudam a empresa a gerenciar as ameaças aos dados de forma mais eficaz em geral".[4]

O McAfee Active Response completa sua estratégia de segurança em camadas e reforça não só a proteção para endpoints, mas também sua postura de segurança em geral. Ele é um elemento fundamental de um conjunto abrangente de soluções, que inclui tecnologias essenciais de segurança de endpoints, como antivírus, controle de aplicativos, informações de ameaças locais e muito mais. Como parte da arquitetura integrada e conectada da Intel Security, o McAfee Active Response proporciona visibilidade e informações contínuas sobre a atividade de endpoints para ajudar sua equipe a agir com mais rapidez com a finalidade de resolver os problemas da forma mais favorável para sua empresa.

Os administradores, investigadores e profissionais responsáveis por tratar incidentes de segurança têm uma visão ininterrupta da atividade em toda a infraestrutura, podendo reagir adequadamente a ameaças que podem estar inativas esperando para atacar, que podem ter sido excluídas para evitar a detecção ou que podem estar se propagando por toda a sua rede. Gatilhos integrados personalizáveis auxiliam sua equipe de segurança a descobrir indicadores de ataque (IoAs, do inglês "indicators of attack") atuais e futuros e a considerar essas informações para agir com prontidão.

A eficiência da descoberta inteligente, a investigação e a análise detalhadas interativas em tempo real, os relatórios abrangentes, bem como as medidas e os alertas priorizados são utilizados pela plataforma de gerenciamento do McAfee® ePolicy Orchestrator® (McAfee ePO™). Através da plataforma do McAfee ePO, a Intel Security unifica o processo de **proteção, detecção e correção** transformando-o em um loop de feedback adaptável, que permite que a segurança evolua e aprenda em um ciclo iterativo, que melhora ao longo do tempo. O McAfee Active Response corresponde ao componente de **detecção** e **correção** desse ciclo de defesa contra ameaças, auxiliando as organizações a identificar os ataques com mais eficácia e a implementar medidas corretivas com rapidez. O software McAfee ePO oferece a escalabilidade, a extensibilidade e o monitoramento unificado contínuo de toda a sua infraestrutura. Ele também ajuda a manter os custos baixos, eliminando a necessidade de contratar profissionais técnicos e gestores para fins de administração.

McAfee Active Response

- Monitore continuamente alterações de estado e eventos críticos nos endpoints.
- Use coletores ininterruptos para localizar e visualizar todos os arquivos: executáveis e inativos.
- Defina interceptações que acionam respostas automáticas e personalizadas.
- Gerencie toda a solução em um único console.

Figura 1. Proteção automatizada, adaptável e contínua contra ATAs com o McAfee Active Response.

Resumo da Solução

O McAfee Active Response possui três componentes que são fundamentais para uma estratégia de EDR eficaz:

- **Automação:** Interceptações ou gatilhos podem ser configurados de acordo com diversos parâmetros. Eles instruem todos os endpoints do seu ambiente a procurar tipos específicos de IoAs. Quando determinado tipo de IoA é descoberto, os gatilhos automaticamente iniciam uma reação definida pelo usuário, como "reinicializar o sistema". Ao contrário de outras soluções de EDR, que apenas coletam informações continuamente, o McAfee Active Response aplica automaticamente uma lógica para acionar uma reação específica em determinadas condições.
- **Adaptabilidade:** Quando os administradores recebem um alerta, o McAfee Active Response adapta a resposta às metodologias específicas utilizadas pelo ataque em questão. É possível realizar pesquisas personalizadas ou padrão em toda a sua organização para desenvolver uma compreensão mais aprofundada dos IoAs e adaptar as medidas corretivas e os recursos adequados.
- **Monitoramento contínuo:** O McAfee Active Response atua de forma contínua. Os gatilhos acionam alarmes ou respostas quando os ataques ocorrem e é possível ajustá-los para monitorar os sistemas para de detectar atividades de ataque futuras.

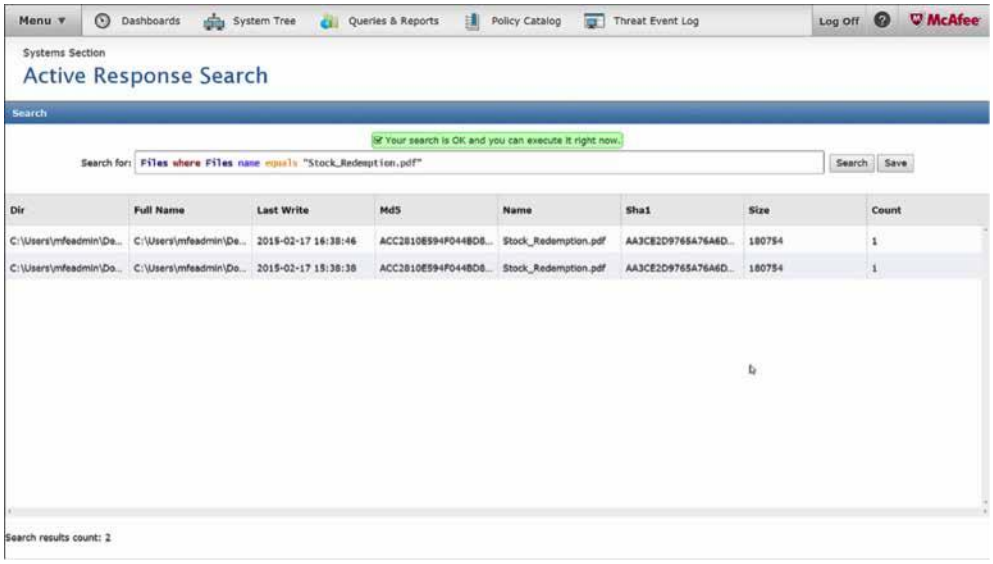

Figura 2. Resultados da pesquisa do McAfee Active Response.

A coleta de dados precisos revela o potencial de violação.
Os coletores são um componente essencial do McAfee Active Response. Os recursos integrados de pesquisa proporcionam aos usuários uma visibilidade aprofundada dos sistemas, permitindo descobrir e visualizar dados úteis que dão pistas sobre malwares à espreita ou atividades suspeitas. Os coletores são como detetives aptos a investigar além do óbvio, examinando executáveis de programas, processos em execução, bem como arquivos e objetos inativos ou excluídos.

Os coletores do McAfee Active Response oferecem ampla capacidade de configuração, adaptabilidade e precisão. Você tem a opção de usar o catálogo predefinido ou de criar e importar seus próprios scripts utilizando o McAfee Data Exchange Layer para executá-los. Em seguida, você pode realizar pesquisas em fontes de dados tradicionais ou em "buracos negros" (onde os pacotes de dados podem ser destruídos ou descartados sem seu conhecimento) para encontrar a combinação exata de características que correspondem aos IoAs que pretende rastrear.

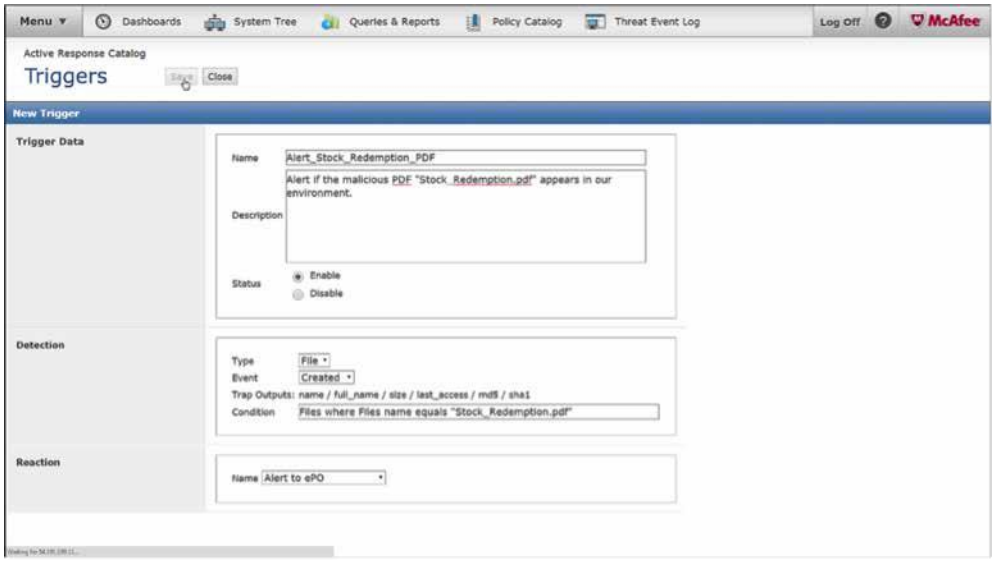

Figura 3. Configuração de um gatilho e definição de uma reação no McAfee Active Response.

Gatilhos e reações oferecem uma resposta automatizada e contínua.
Com apenas um conjunto de instruções, os gatilhos auxiliam a monitorar continuamente e a reagir a eventos de segurança ou a mudanças de estado hoje e no futuro. Depois que você define o conjunto de possíveis comportamentos de ataque ou os detalhes que deseja monitorar, basta configurar um gatilho para gerar automaticamente um alerta ou executar uma reação quando esses IoAs forem detectados. Com uma única etapa simples, sua equipe de segurança pode detectar e corrigir ameaças emergentes com eficiência e eficácia. A Gartner recomenda esse tipo de recurso de EDR em seu relatório de 2015, *Best Practices for Detecting and Mitigating Advanced Persistent Threats (Práticas recomendadas para detectar e reduzir as ameaças persistentes avançadas):* "…recursos de resposta automática a detecções de ameaças com o uso de soluções de EDR, tais como eliminação de processos, exclusão de arquivos ou limpeza da memória, com a finalidade de evitar a perda de dados e deter uma 'cadeia de destruição' ativa."[5]

McAfee Active Response na arquitetura da Intel Security

A estrutura da Intel Security unifica e integra vários produtos, serviços e soluções de parceiros para reduzir os riscos de segurança de forma centralizada, eficiente e eficaz. Ela ajuda a reagir com mais rapidez quando ATAs ameaçam seu ambiente. No núcleo da arquitetura integrada e conectada da Intel Security, está a plataforma de gerenciamento do McAfee ePO, que você utiliza para implementar e gerenciar o McAfee Active Response. Como o McAfee Active Response é diretamente integrado à plataforma de gerenciamento do McAfee ePO, ele funciona perfeitamente com outras tecnologias avançadas da Intel Security, incluindo o McAfee Threat Intelligence Exchange, os McAfee Complete Endpoint Protection Suites e o McAfee Enterprise Security Manager.

Como funciona.

Depois que o cliente do McAfee Active Response é instalado no endpoint, ele se integra ao McAfee Agent e preenche um cache de hash de arquivo, um cache de fluxo de rede e um cache do Registro. Esses caches são atualizados instantânea e continuamente, sempre que ocorre atividade de endpoints. O coletor sempre ativo registra o tipo de informações determinadas pelas suas instruções sobre os arquivos maliciosos (até mesmo se eles estiverem inativos) ou sobre a atividade suspeita. Esses dados são armazenados e indexados localmente no endpoint e em seguida exibidos na interface do software McAfee ePO. Não há necessidade de um appliance de armazenamento de dados separado ou de armazenamento em nuvem. A coleta persistente ocorre em segundo plano de forma lenta, evitando picos de consumo de recursos no endpoint. Os usuários podem continuar trabalhando sem interrupções.

Se você receber um alerta de um produto de segurança ou quiser encontrar uma ameaça recém-descoberta da qual acabou de tomar conhecimento por meio de informações compartilhadas, poderá fazer uma busca de forma bastante semelhante a uma pesquisa do Google. Quando os administradores iniciam uma pesquisa na plataforma de gerenciamento do McAfee ePO, o cliente do McAfee Active Response examina os caches. Os resultados levam de 10 a 20 segundos para serem exibidos oferecendo uma visão precisa do estado atual do seu ambiente em tempo real.

Em seguida, os gatilhos e as reações entram em ação. Os gatilhos funcionam como sentinelas, monitorando continuamente os endpoints em busca de IoAs. Se determinado IoA for detectado, o gatilho será acionado e responderá automaticamente com uma reação, que pode ser personalizada de acordo com seus objetivos específicos. Reações comuns incluem enviar um alerta, excluir um arquivo nocivo, eliminar um processo malicioso ou realizar uma análise pericial mais detalhada.

O McAfee Active Response em ação

Nada melhor do que casos de uso reais para enfatizar a importância da solução de EDR. Veja a seguir alguns exemplos de como o McAfee Active Response pode auxiliar a detectar e reagir a ameaças em diferentes situações.

"Minas explosivas" não detonadas

Como mencionado, o McAfee Active Response atua em conjunto com o McAfee Threat Intelligence Exchange, que permite o compartilhamento de dados relevantes sobre ameaças em tempo real entre os componentes de segurança da arquitetura da Intel Security, permitindo que eles atuem como uma infraestrutura de segurança colaborativa unificada. O McAfee Threat Intelligence Exchange ajuda a bloquear arquivos "indefinidos", desconhecidos ou emergentes, que conseguem passar pelo antivírus. Ele oferece maior visibilidade e maior controle sobre esses tipos de arquivos e identifica onde a tentativa de execução ou a execução real do arquivo ocorre. Em seguida, o McAfee Threat Intelligence Exchange envia o primeiro alerta para o McAfee Data Exchange Layer. A partir daí, as equipes de segurança podem usar o McAfee Active Response para consultar o hash de arquivo no ambiente e determinar se "minas explosivas" inativas foram instaladas em algum outro lugar. Todas essas atividades são realizadas com rapidez e eficiência pela plataforma de gerenciamento do McAfee ePO.

Malwares ocultos em documentos

Cada vez mais ameaças de dia zero ou códigos utilizados para distribuir malware são inseridos em documentos, como arquivos .ZIP, arquivos de imagem, .PDFs, arquivos do Adobe Flash ou arquivos .PNG. Esses ataques ocultos geralmente não podem ser detectados por antivírus comuns. Você pode usar o McAfee Active Response para realizar uma pesquisa desses tipos de arquivos de acordo com determinados atributos. Por exemplo, digamos que um arquivo de documento suspeito apareceu no laptop do seu assistente. Sua equipe pode usar o McAfee Active Response para definir um gatilho, que vigiará esse tipo de arquivo em todos os endpoints da organização e o excluirá antes que ele gere danos.

Saiba mais

Automatizado, adaptável e contínuo, o McAfee Active Response é um componente fundamental da abordagem integrada da Intel Security para derrotar ATAs cada vez mais numerosos e complexos com rapidez e eficácia no panorama de ameaças atual. Para saber mais sobre como o McAfee Active Response complementa o portfólio atual de produtos da Intel Security, acesse:

- **McAfee Active Response**
- **McAfee ePolicy Orchestrator**
- **McAfee Threat Intelligence Exchange**
- **McAfee Complete Endpoint Protection Suites**

1. **http://breachlevelindex.com/pdf/Breach-Level-Index-Annual-Report-2014.pdf**
2. **https://www.gartner.com/doc/2738017/market-guide-endpoint-detection-response**
3. **http://www.mcafee.com/us/about/news/2014/q4/20141209-01.aspx**
4. **http://www.cybersecuritydocket.com/2015/05/08/edr-the-future-of-cybersecurity-and-incident-response/**
5. **https://www.gartner.com/doc/2589029/best-practices-mitigating-advanced-persistent**

McAfee. Parte de Intel Security.
2821 Mission College Boulevard Santa Clara, CA 95054
888 847 8766
www.intelsecurity.com