McAfee Active Response

Detecção e resposta abrangentes para endpoints

Atualmente, as organizações que se preocupam com segurança enfrentam um cenário de ameaças que muda em um ritmo frenético. Ataques são criados e propagados em proporções nunca vistas. Ataques desenvolvidos especialmente visam determinadas organizações utilizando conhecimento específico para aprimorar sua eficácia e minimizar detecções. Os atacantes estão vencendo com mais frequência as tecnologias preventivas. As organizações com visão de futuro, portanto, exigem ferramentas integradas e fáceis de usar para poder detectar melhor a presença de atacantes e possibilitar investigações e correções rápidas. As melhores soluções de detecção e resposta aumentam a eficiência da segurança, até mesmo por capturar cada vez mais informações de um número crescente de sistemas. Ao oferecer prontamente capacidades superiores, interação automatizada com soluções existentes de gerenciamento de segurança e personalização pelo usuário, o McAfee® Active Response reduz consideravelmente a janela de oportunidade dos atacantes para causar danos aos seus ativos computacionais e marca corporativa.

Principais vantagens

- **Automatizado:** capture e monitore o contexto e o estado do sistema quanto a alterações que possam ser IoAs, localize componentes inertes de ataque e envie inteligência para equipes forenses, de operações e de análise
- **Adaptável:** ao ser alertado, você pode se ajustar a mudanças nas metodologias de ataque, automatizar a coleta de dados, os alertas e as respostas conforme os objetos de interesse, e personalizar a sua configuração conforme os fluxos de trabalho do cliente
- **Contínuo:** coletores persistentes ativam gatilhos quando eventos de ataque são detectados, alertando-o e aos seus sistemas quanto à atividade de ataque que você esteve observando

O cenário de ameaças em evolução

As empresas agora compreendem que podem ser invadidas por um atacante a qualquer momento e que precisam estar preparadas para lidar efetivamente com essas violações por meio de detecção antecipada de ataques, detecção de atividades em andamento ou descoberta de indicadores de ataque (IoAs). Essa compreensão vem acompanhada do entendimento de que novas tecnologias são necessárias para lidar com as brechas atuais em termos de visibilidade, descoberta, detecção e resposta.

Limitações das atuais abordagens de resposta a incidentes

Quando solicitados a investigar um incidente suspeito ou conhecido em toda uma organização, os responsáveis pela resposta a incidentes e administradores de segurança costumam ser limitados por dois fatores: tempo e escala. Embora uma grande quantidade de informações detalhadas seja coletada pelos sistemas e ferramentas existentes, leva-se muito tempo para coletar e analisar essas informações. Como a velocidade é um requisito crítico na coleta de dados, são feitas muitas concessões quanto à natureza dos dados coletados, bem como ao número de sistemas dos quais eles são coletados. Além disso, a própria magnitude dos dados coletados que precisam ser analisados para identificação de informações cruciais torna cada vez mais difícil esse processamento.

As ferramentas de resposta a incidentes mais frequentemente utilizadas são scripts criados pelos próprios responsáveis pela resposta a incidentes. Essas ferramentas constituem a base da coleta dos dados a serem utilizados

Requisitos de sistema

Hardware mínimo necessário
O servidor pode ser instalado em uma máquina virtual, se necessário.
Os requisitos de hardware mínimos recomendados para o servidor McAfee Active Response são os seguintes:

- 4 CPUs Intel® Xeon® X5675 de 3,07 GHz
- 8 GB de RAM
- 120 GB de SSD (disco de estado sólido)

Infraestrutura de serviços necessária
- McAfee® ePolicy Orchestrator® (McAfee ePO™) 5.1.1 ou posterior
- Extensão McAfee Agent 5.0 ou posterior
- Camada de negociação McAfee Data Exchange Layer 2.0.0.405 ou posterior

Navegadores da Web compatíveis
- Microsoft Internet Explorer 9 ou posterior
- Google Chrome 17 ou posterior
- Mozilla Firefox 10.0 ou posterior

Infraestrutura de cliente necessária
- McAfee Agent 5.0.0.2710 ou posterior para endpoints Linux
- McAfee Agent 5.0.0.2610 ou posterior para endpoints Microsoft Windows
- Clientes McAfee Data Exchange Layer 2.0.0.405 ou posterior em todos os endpoints gerenciados

em uma análise mais ampla. Esse conhecimento acumulado, juntamente com as ferramentas associadas, está bem amadurecido, mas seu aproveitamento na escala e na velocidade exigidas é limitado. Essa falta de capacidade de realizar uma investigação ao vivo de IoAs específicos em toda uma organização frequentemente leva os responsáveis a uma visão míope de seu trabalho de descoberta e resposta. Tipicamente, esse trabalho é restringido artificialmente para satisfazer exigências de prazo e isso pode contribuir para déficits significativos no processo de resposta a incidentes. Isso prejudica severamente os responsáveis, pois seu trabalho é limitado artificialmente devido às restrições das ferramentas atuais.

Detecção e resposta abrangentes para endpoints

O McAfee Active Response proporciona detecção de ameaças avançadas à segurança e resposta às mesmas continuamente, para ajudar os profissionais de segurança a monitorar a postura de segurança, melhorar a detecção de ameaças e expandir as capacidades de resposta a incidentes por meio de descoberta antecipada, análise detalhada, investigação forense, relatórios abrangentes e ações e alertas priorizados. Otimizado para satisfazer rígidos critérios de detecção e resposta (EDR) em endpoints, o McAfee Active Response utiliza coletores predefinidos e personalizáveis pelo usuário para pesquisar profundamente todos os sistemas e encontrar não apenas IoAs presentes em processos sendo executados, mas também que possam estar inertes ou que tenham sido excluídos. Além disso, o McAfee Active Response não só permite aos usuários procurar por um IoA no presente, mas também alertar e agir conforme os objetivos da segurança por meio de instruções vinculadas a gatilhos, caso o IoA venha a ocorrer no futuro.

O McAfee Active Response é prova da eficácia da arquitetura de segurança integrada da Intel Security, desenvolvida para resolver mais ameaças, mais rapidamente e com menos recursos em um mundo mais complexo.
O McAfee Active Response oferece visibilidade contínua e insights poderosos sobre os seus endpoints para que você possa identificar violações mais rapidamente. Ele oferece as ferramentas de que você necessita para corrigir problemas mais rapidamente e da maneira mais adequada aos seus negócios. Todo esse poder é gerenciado por meio do software McAfee® ePolicy Orchestrator® (McAfee ePO™), aproveitando o McAfee Data Exchange Layer — isso proporciona escalabilidade e extensibilidade unificadas, sem a necessidade de aumento da equipe para administrar o produto.

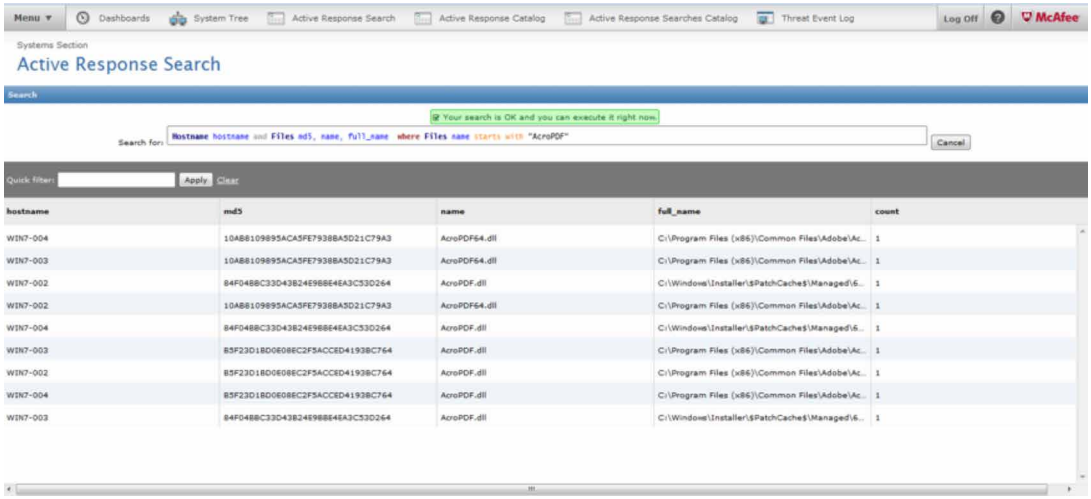

Figura 1. Interface de usuário para pesquisa do McAfee Active Response.

Sistemas operacionais de cliente compatíveis

- Microsoft Windows
  - Windows 8.0, básico, 32 e 64 bits
  - Windows 8.1, básico, U1; 32 e 64 bits
  - Windows Server 2012, básico, R2; U1; 64 bits
  - Windows Server 2008 R2 Enterprise, SP1, 64 bits
  - Windows Server 2008 R2 Standard, SP1, 64 bits
  - Windows 7 Enterprise, até SP1; 32 e 64 bits
  - Windows 7 Professional, até SP1; 32 e 64 bits
- CentOS 6.5, 32 bits
- RedHat 6.5, 32 bits

Recurso	Vantagem	Vantagens para o cliente	Diferenciação
Coletores	Os coletores permitem que os usuários localizem e visualizem dados de seus sistemas.	Os coletores oferecem capacidades de pesquisa para examinar profundamente os sistemas. Eles proporcionam visibilidade sobre possíveis ataques ou violações críticas para coleta e visualização de dados desses sistemas. Utilizando qualquer uma dentre várias linguagens comuns de script, os usuários podem personalizar facilmente seus próprios coletores e respostas, oferecendo o máximo em configurabilidade e adaptabilidade.	O McAfee Active Response vai além de arquivos executáveis ou em execução, examinando código que possa estar inerte ou que tenha sido excluído em uma tentativa de encobrir os rastros do atacante. O McAfee Active Response pode pesquisar arquivos, o fluxo de rede, o Registro e o mapeamento de processos.
Gatilhos	Os gatilhos permitem que um profissional de segurança monitore continuamente um evento crítico ou uma mudança de estado com um determinado conjunto de instruções, tanto no presente quanto no futuro.	Ações são iniciadas por um gatilho definido previamente, gerando um evento ou executando respostas. O McAfee Active Response tem a capacidade de fazer mais do que meras "espiadas" estáticas, estando em um modo contínuo de resposta.	O McAfee Active Response pode ver hoje as ameaças e desencadear ações para ameaças que possam vir amanhã.
Reações	As reações proporcionam ações pré-configuradas e personalizáveis como resultado de determinadas condições do gatilho, permitindo caçar e eliminar ameaças.	As reações permitem que os usuários executem ações, como procurar arquivos que tenham sido excluídos do sistema por hash de arquivo (MD5 e SHA1), ver se algum host está ativamente conectado a um endereço IP ou se esteve previamente, ou procurar um arquivo malicioso não baseado em PE que não tenha sido acessado ou detonado no sistema (busca por um PDF malicioso em um sistema no qual ele tenha sido copiado para o sistema de arquivos, mas não executado).	O McAfee Active Response é pré-configurado para agir sobre os resultados das pesquisas e acomoda ações personalizadas prescritas pelo usuário para satisfazer necessidades específicas definidas pelo mesmo.
Gerenciamento centralizado com o software McAfee ePO	O ambiente de console único proporciona gerenciamento e automação abrangentes.	Os administradores podem aproveitar o software McAfee ePO como parte da arquitetura de segurança integrada da Intel Security para acionar respostas automatizadas a gatilhos e pesquisas, e para responder a ameaças e corrigi-las. A gerenciabilidade em um único painel oferece mais visibilidade sobre a segurança, sem um fardo administrativo adicional. Isso simplifica os aspectos operacionais e reduz o investimento de tempo da equipe administrativa.	Gerenciamento e ação por meio de um único console são um nítido fator de diferenciação. Utilizando um único console, nós protegemos de maneira exclusiva uma variedade de plataformas com um conjunto poderoso de controles de segurança, incluindo o McAfee Active Response.
Arquitetura de segurança integrada	Aproveita a camada de intercâmbio de dados para simplificar a comunicação com outros produtos da McAfee, parte da Intel Security.	Como parte da arquitetura de segurança integrada da Intel Security, o McAfee Active Response reduz os riscos, o tempo de resposta, a sobrecarga de trabalho e os custos operacionais da equipe através dos conceitos inovadores, dos processos otimizados e das recomendações práticas da plataforma.	

Saiba mais sobre as vantagens do McAfee Active Response em **www.mcafee.com/br/products/active-response.aspx**.

McAfee. Part of Intel Security.
Av. das Nações Unidas, 8.501 - 16° andar
CEP 05425-070 - São Paulo - SP - Brasil
Telefone: +55 (11) 3711-8200
Fax: +55 (11) 3711-8286
www.intelsecurity.com