McAfee Cloud Threat Detection

Aprimore facilmente as proteções da Intel Security para condenar malware avançado e expor ameaças evasivas

Uma variedade das mais recentes análises —incluindo autoaprendizagem — identifica malware e converte condenações em ações, atualizando as proteções para frustrar ataques semelhantes no futuro.

Principais vantagens:

- Reduza o risco das ameaças desconhecidas que prejudicam os seus negócios
- Aproveite o Big Data e o poder da auto-aprendizagem
- Otimize seus investimentos em segurança
- Simplifique a distribuição de análises de ameaças avançadas

As organizações enfrentam uma batalha desigual contra um malware inteligente que continua evadindo defesas tradicionais. Soluções avançadas de detecção ajudam, mas podem ser complexas e caras quando há limitações em recursos e equipe de segurança. A maioria delas não se integra na infraestrutura de proteção e, portanto, deixa a janela de vulnerabilidade aumentar enquanto os responsáveis pela resposta a incidentes tomam suas providências.

O que se precisa? Uma detecção avançada e econômica, que seja bem simples de distribuir e de usar: o McAfee® Cloud Threat Detection. Esse serviço novo e conveniente complementa soluções existentes da Intel® Security para condenar malware avançado e expor ameaças evasivas. Como uma oferta de nuvem, ele permite que você aproveite facilmente o imenso poder computacional que opera uma variedade das mais recentes técnicas de análise. Você pode aprimorar a detecção e otimizar os investimentos em segurança existentes.

Detecção integrada com proteção

As soluções da Intel Security constituem a sua primeira linha de defesa, filtrando o malware conhecido e o malware provável utilizando ferramentas avançadas, como emulação e reputação. Porém, quando não têm certeza de que um arquivo é malicioso, elas podem recorrer à nuvem para uma análise mais completa.

Máquinas versus malware emergente e evasivo

Com o Cloud Threat Detection, mecanismos de análise estática trabalham para extrair detalhes dos arquivos. Uma cobertura abrangente de tipos de arquivo proporciona o tão necessário contexto para os chamados arquivos “grey” (em situação indefinida), efetivamente identificando tanto arquivos maliciosos quanto limpos. Além disso, utiliza-se análise comportamental, pois o arquivo também é executado em um ambiente de área restrita (sandbox). Tudo o que o malware faz é registrado, examinado e avaliado quanto à existência de intenção maliciosa. O arquivo gerou alguma pasta aleatória, gravou um novo arquivo nela e excluiu o arquivo original? Ele disfarçou algum acesso a URLs desconhecidos ou suspeitos em meio ao tráfego com sites conhecidos, como Google, Amazon ou Facebook? Estes são apenas alguns exemplos de comportamentos que o serviço McAfee Cloud Threat Detection pode usar para classificar um arquivo desconhecido. Esses processos também revelam os metadados,

intel Security

URLs, nomes de arquivo, localizações de pastas e outras coisas que informamos aos clientes para que estes possam investigar e verificar se outras máquinas foram comprometidas.

Autoaprendizagem supervisionada

Gerenciada e otimizada pelo McAfee Labs, cada etapa do ciclo de análise é assistida pelo poder de grandes cérebros, do Big Data e da autoaprendizagem. Insights de mais de 25 anos de dados e dois bilhões de arquivos foram utilizados para desenvolver e treinar extensivos modelos de classificação em nosso sistema Big Data na nuvem. Pesquisas ativas e a constante interpretação dos resultados das inspeções alimentam uma autoaprendizagem contínua para que esses modelos evoluam de acordo com as mudanças nas técnicas e comportamentos do malware e conforme os avanços em pesquisa.

Foco na precisão

Nossa experiência nos ensinou que falsos negativos ou falsos positivos podem ser prejudiciais e caros. Por isso, os sistemas que utilizamos incluem verificações e comparações com certificados de assinatura e com os arquivos de sistema mais críticos para assegurar que as condenações sejam rápidas, mas confiáveis. Enquanto uma análise avançada detecta ameaças emergentes, fazemos uma referência cruzada e associamos anomalias de malware e atributos contextuais e comportamentais para minimizar falsos positivos. Essa é uma das vantagens marcantes de nossa combinação de análise em nuvem e amplos recursos antimalware.

Detecção em ação

Para cada veredito, o McAfee Cloud Threat Detection notifica o sistema de origem, o qual impõe uma política, como colocar em quarentena uma máquina ou ativar a proteção para frustrar ataques semelhantes. IoCs (indicadores de comprometimento) detalhados estão disponíveis para investigações adicionais e para os insights necessários para correção e recuperação pós-ataque. As condenações também atualizam reputações no McAfee Global Threat Intelligence (GTI) para acelerar a proteção para todas as organizações com soluções compatíveis com o GTI.

Atuação rápida, economia e facilidade para pequenos negócios

Como em um serviço com base em nuvem, você simplesmente digita uma chave compartilhada criptografada a partir do seu produto McAfee integrado, de maneira que o provisionamento é rápido. Se você tem sistemas distribuídos, não há necessidade de mover o tráfego para um data center; basta enviá-lo para a nuvem. Nossos especialistas se encarregam da manutenção contínua e implementam atualizações e upgrades de forma transparente. Em vez de despesas de capital antecipadas, preços de assinatura com base em volume eliminam as barreiras de custo para a adesão.

Saiba mais em **www.mcafee.com/br/products/cloud-threat-detection.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