DATA SHEET

McAfee MVISION Endpoint Detection and Response (MVISION EDR)

Recursos simplificados e poderosos para detecção, investigação guiada e resposta a ameaças

Os adversários agem furtivamente — camuflando suas ações dentro dos componentes mais confiáveis já existentes no seu ambiente. Eles nem sempre instalam algo substancial como malware, mas sempre deixam um rastro comportamental. A detecção e resposta para endpoints (EDR) monitora e coleta dados continuamente para proporcionar a visibilidade e o contexto necessários para detectar e responder a ameaças. No entanto, as abordagens atuais frequentemente sobrecarregam com excesso de informação equipes de segurança já assoberbadas. O McAfee® MVISION EDR ajuda a gerenciar o grande volume de alertas, capacitando analistas de todos os níveis de qualificação a fazer mais e a investigar com mais eficácia. Uma exclusividade do MVISION EDR é o McAfee® MVISION Insights[1], primeira tecnologia a priorizar ameaças proativamente *antes* que você seja atingido, prever se as suas contramedidas serão eficazes e prescrever exatamente o que você precisa fazer caso não sejam eficazes, tudo isso simultaneamente.

Fortaleça, acelere e simplifique a EDR

O MVISION EDR reduz o tempo médio necessário para detectar e responder a ameaças ao possibilitar que todos os analistas compreendam os alertas, investiguem-os completamente e respondam rapidamente. Análises avançadas ampliam o escopo das detecções e permitem interpretar corretamente os alertas. Investigações orientadas por inteligência artificial (IA) e automação capacitam até os analistas menos experientes a analisar em um nível mais alto, liberando os seus analistas seniores para aplicar seus conhecimentos na caça a ameaças e na redução do tempo de resposta.

Detecte ameaças avançadas no endpoint e responda mais rapidamente

Sem os dados, contexto e análises certos, os sistemas EDR geram alertas em demasia ou não acusam ameaças emergentes, desperdiçando tempo e recursos preciosos sem aprimorar a segurança. O MVISION EDR oferece coleta de dados contínua e vários mecanismos de análise ao longo dos estágios de detecção e investigação para ajudar a revelar comportamentos suspeitos com precisão, permitir a compreensão de alertas e contextualizar ações.

Principais vantagens

- Detecção de ameaças decisiva e de alta qualidade, sem falsos alertas
- Insights proativos sobre ameaças antes dos ataques
- Análises mais rápidas permitem que você monte uma defesa mais resiliente
- Investigações orientadas por IA proporcionam aos analistas insights sobre o ataque gerados por máquina
- As organizações podem maximizar a produtividade de suas equipes existentes
- É uma solução de nuvem que exige pouca manutenção
- Simplifique as distribuições aproveitando o software McAfee ePO existente no local ou o MVISON ePO baseado em SaaS
- Os analistas podem se concentrar na resposta estratégica a incidentes sem sobrecarga administrativa

Conecte-se conosco

- **Obtenha contexto e visibilidade:** as informações dos eventos de endpoint são transmitidas para a nuvem, proporcionando o contexto e a visibilidade necessários para revelar ameaças ocultas. As informações dos endpoints ficam disponíveis para inspeção imediata e pesquisa em tempo real, além de pesquisas históricas. Opções flexíveis de retenção de dados atendem às necessidades variadas de diversas organizações e equipes de operações de segurança.
- **Obtenha contexto novo e proativo com o MVISION Insights:** notificações no dashboard ou alertas por e-mail sobre campanhas priorizadas, definidos pela equipe de especialistas do McAfee® Advanced Threat Research. São oferecidas não só informações sobre campanhas, mas também avaliações locais de sistemas que podem estar comprometidos, previsões de possíveis impactos à sua plataforma de proteção de endpoint e orientações prescritivas para evitar violações nas contramedidas. Isso permite que o analista fique à frente dos adversários, antes que estes ataquem. Diferentemente de testes de penetração com exercícios para equipes vermelha e azul, com pouco tempo e recursos é possível priorizar, prever e prescrever. Esses três Ps são automatizados e enviados à nossa equipe em caso de ameaças antes do ataque. O que costumava levar semanas, agora leva minutos. Isso muda a atuação da equipe do SOC, de sempre reativa para proativa.
- **Revele mais com análises poderosas baseadas em nuvem:** mecanismos analíticos inspecionam a atividade de endpoint para revelar um amplo espectro de comportamentos suspeitos e detectar ameaças — desde malware baseado em arquivo a ataques sem arquivo — que tenham passado por outras defesas de segurança. A distribuição baseada em nuvem possibilita a adoção rápida de novas técnicas e mecanismos analíticos.
- **Pense como um criminoso cibernético:** os resultados da detecção com base em comportamento são mapeados na estrutura MITRE ATT&CK™, apoiando um processo mais consistente para determinar a fase de uma ameaça e seu risco associado e para priorizar uma resposta.
- **Navegue facilmente:** a hierarquização dos alertas ajuda ainda mais os analistas a compreender a gravidade do risco e a resposta apropriada. A flexibilidade de exibição e visualização de dados nesse estágio ajuda analistas de diversos níveis de experiência a navegar facilmente pelos dados para compreender rapidamente por que um alerta foi acionado e determinar as etapas seguintes: ignorar, responder ou investigar.
- **Responda com rapidez:** as respostas predefinidas do MVISION EDR possibilitam uma ação imediata. Os usuários podem conter facilmente as ameaças encerrando um processo, colocando uma máquina em quarentena e excluindo arquivos. Os analistas podem atuar em um único endpoint ou estender a resposta por todo o ambiente com um único clique.

Investigação orientada por IA

Em caso de resposta imediata a um alerta de incidente cuja causa raiz não seja óbvia (como frequentemente não é), os analistas de segurança precisam sair da solução EDR e investigar para compreender realmente todos os aspectos de uma ameaça ou campanha complexa e o risco associado. As soluções de EDR costumam "permitir" a investigação fornecendo dados brutos, contexto e funções de pesquisa, mas não prescindem de analistas qualificados para realizar as consultas e análises. Analistas experientes frequentemente não têm tempo para validar e investigar muitos alertas, ao passo que analistas inexperientes talvez não saibam por onde começar.

Com o MVISION EDR, analistas de qualquer nível podem dar um passo adiante e investigar. Em vez de simplesmente possibilitar uma investigação com dados e funcionalidade de pesquisa, o MVISION EDR orienta a investigação.

- **Guias de investigação dinâmica:** construídos pela combinação da experiência e do conhecimento de investigadores forenses da McAfee e inteligência artificial (IA), os guias de investigação multiplicam forças no processo de investigação e exploram paralelamente muitas hipóteses, atingindo velocidade e precisão máximas. Diferentemente de roteiros que automatizam tarefas em scripts para ameaças conhecidas, os guias de investigação ajustam-se dinamicamente ao caso em questão, combinando diversos dados e estratégias de investigação. O MVISION EDR pergunta e responde questões automaticamente para provar ou descartar as hipóteses. O MVISION EDR coleta, resume e exibe automaticamente evidências de múltiplas fontes e realiza interações conforme a investigação evolui.
- **Ampla coleta de dados e relevância local:** o mecanismo de investigação respaldado por inteligência artificial reúne e processa anomalias e sequências de eventos complexos — de endpoints, de sistemas de gerenciamento de eventos e informações de segurança (SIEM), de dados proativos do MVISION Insights e do software McAfee® ePolicy Orchestrator® (McAfee ePO™) — para ajudar na compreensão dos alertas. O MVISION EDR compara as evidências com as atividades normais conhecidas de cada organização e com fontes de inteligência sobre ameaças para aprimorar a relevância local e reduzir os falsos positivos relacionados a atividades normais. As investigações podem se originar de alertas do SIEM ou do MVISION EDR.
- **Visualizações diferentes para usuários diferentes:** a exibição flexível de dados aplica a ótica apropriada para usuários com níveis de experiência diferentes, de modo que todos os analistas possam compreender rapidamente como as anomalias e eventos estão conectados sem a necessidade de alternar entre múltiplas telas.

- **Investigação de phishing:** o MVISION EDR conecta-se facilmente a fluxos de trabalho de investigação de phishing em operações de segurança. Os e-mails suspeitos podem seguir para o MVISION EDR para inspeção. Caso eles sejam considerados maliciosos, o MVISION EDR pode determinar rapidamente quais máquinas da organização podem ter sido afetadas.

O MVISION EDR reduz o conhecimento e o trabalho necessários para realizar investigações, além de aumentar a velocidade com a qual os analistas podem determinar o risco do incidente e sua causa raiz. Em nível organizacional, as vantagens são inúmeras. Cada analista pode ser mais eficiente, mais casos podem ser delegados a analistas juniores e os analistas seniores podem investir seu tempo em atividades de maior valor.

Os dados certos — no momento certo — para a tarefa em questão

Além da investigação orientada, analistas e caçadores de ameaças podem utilizar as capacidades poderosas de pesquisa e coleta de dados do MVISION EDR e os dados proativos do MVISION Insights para expandir consultas e examinar detalhadamente os sistemas e correlações entre sistemas.

- **Pesquisa histórica:** a coleta de dados abrangente e contínua encaminha informações sobre eventos de endpoint de todos os sistemas monitorados para a nuvem. Os analistas podem pesquisar esses dados centralizados — independentemente de cada endpoint estar on-line ou off-line — para localizar indicadores de comprometimento (IoCs) e indicadores de ataque (IoAs) que possam estar presentes juntamente com os arquivos excluídos.
- **Pesquisa em tempo real:** para consultas de incidentes ativos, a pesquisa em tempo real busca endpoints de todo o ambiente para obter rapidamente as informações mais recentes. Uma sintaxe versátil possibilita uma gama de capacidades, desde consultas simples, como procurar aplicativos instalados nas estações de trabalho, até pesquisas mais complexas que retornem mais dados da estação de trabalho, como identificar um usuário no momento do evento, uma execução de linha de comando e o momento em que o aplicativo suspeito foi iniciado. Essa capacidade pode estender facilmente as consultas a toda a corporação, abrangendo milhares de máquinas.

- **Coleta de dados solicitada:** para amparar as investigações, o MVISION EDR pode obter um instantâneo de um endpoint sob solicitação, capturando uma visualização abrangente de processos ativos, conexões de rede, serviços e entradas de execução automática. O MVISION EDR informa a gravidade associada e informações adicionais, como hash, reputação e o usuário/serviço/processo principal que executou o arquivo suspeito. Através de uma ferramenta de coleta de dados não persistente, instantâneos podem ser capturados tanto em sistemas monitorados quanto não monitorados.
- **Campanhas em destaque:** ataques orquestrados e direcionados (com base em região ou setor) são apontados pelo MVISION Insights, identificando IOCs a serem procurados proativamente com o EDR. Isso capacita o analista a fazer buscas proativas antes que os ataques ocorram.

A colaboração expande a visibilidade, aumenta a eficiência operacional e melhora os resultados

O MVISION EDR é um componente fundamental em um ecossistema integrado de segurança. Ele estende as capacidades de proteção de endpoint e expande a visibilidade enquanto auxilia os fluxos de trabalho e processos da equipe de segurança, contribuindo para reduzir o tempo médio necessário para detectar e responder e aumentando a eficiência operacional.

- **Correlacione dados de toda a empresa para total visibilidade:** a colaboração e a fácil integração com fontes de dados além do endpoint é fundamental para fechar lacunas de dados em investigações de ameaças multifacetadas. Uma forte integração com soluções de gerenciamento de eventos e informações de segurança (SIEM) como o McAfee® Enterprise Security Manager ou produtos de terceiros permite ao MVISION EDR expandir capacidades de investigação e insights ao correlacionar anomalias de endpoint com informações de rede e outros dados coletados pelo SIEM.

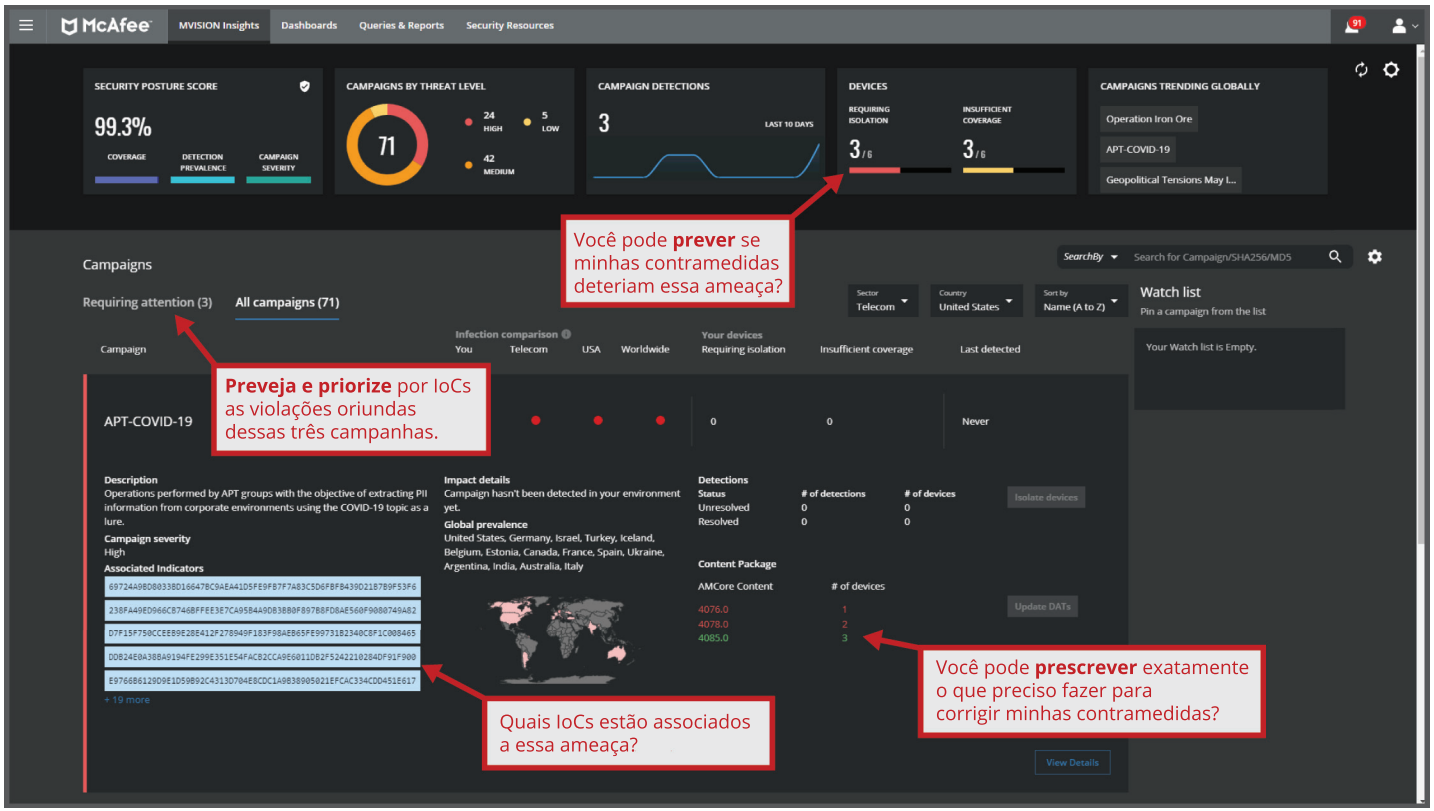

Figura 1. Dashboard do MVISION Insights: o MVISION Insights aponta automaticamente as ameaças que importam e oferece orientações sobre o que fazer, antes que o ataque ocorra. Ele oferece insights de EDR adicionais para esclarecer e acelerar o trabalho de investigação.

- O MVISION EDR faz uso do contexto proativo sobre novas ameaças externas fornecido pelo MVISION Insights, acelerando os trabalhos de investigação e correção.
- O MVISION Insights avisa sobre possíveis campanhas que são priorizadas dependendo de estarem visando o seu setor ou geografia.

Ele prevê quais endpoints carecem de proteção contra as campanhas e diz o que fazer para melhorar a detecção. Ele também informa ao analista a operação de ataque da campanha e o objetivo do ataque, além de oferecer recomendações estratégicas e corretivas através de contramedidas. O MVISION Insights oferece um conjunto completo de IoCs a serem pesquisados

proativamente com o MVISION EDR. Os analistas podem executar pesquisas ou buscas proativas com outras ferramentas.

  - Caso a telemetria do MVISION Insights revele que você pode ter sido afetado por uma campanha, ele oferece a opção elegante de alternar do MVISION Insights para o MVISION EDR. Os analistas encarregam-se dos IoCs em questão, poupando o tempo e o trabalho de copiar e colar manualmente as informações de IoC. Um conjunto completo de IoCs de campanha é fornecido com cada campanha, acelerando bastante a investigação de possíveis violações.

- **Fluxos de trabalho e colaboração com a equipe de suporte:** o MVISION EDR conecta-se às operações de segurança atuais e viabiliza a colaboração ao compartilhar dados de investigações e atualizações por plataformas de resposta a incidentes de segurança.
- **Distribuição simples e expansível:** o MVISION EDR está disponível na forma de um aplicativo SaaS. O gerenciamento com o software McAfee ePO — plataforma centralizada de gerenciamento de segurança mais destacada do setor — simplifica a distribuição e a manutenção cotidiana do MVISION EDR e de toda a sua infraestrutura de segurança. Agora disponível tanto no local quanto na nuvem, o software McAfee ePO oferece flexibilidade de gerenciamento, adequando-se a diversas necessidades organizacionais.

Para obter informações sobre o MVISION EDR, entre em contato com um representante da McAfee ou visite www.mcafee.com/enterprise/pt-br/about/mvision.html.

Precisa de detecção e correção gerenciadas de endpoints?

Detecção e resposta gerenciadas (MDR) são serviços de segurança cibernética terceirizados, desenvolvidos para proteger os seus dados e ativos, mesmo quando uma ameaça passa despercebida por controles de segurança comuns da organização.

Uma plataforma de segurança de MDR é considerada um controle de segurança permanente avançado que costuma incluir uma variedade de atividades fundamentais de segurança, incluindo segurança gerenciada na nuvem para organizações que não podem manter um centro de operações de segurança (SOC) próprio. Os serviços de MDR combinam análise avançada, inteligência contra ameaças e conhecimento humano na investigação e resposta a incidentes implementada em nível de host e de rede. Os parceiros McAfee Service Provider certificados oferecem monitoramento contínuo de alertas críticos, caça a ameaças gerenciada, investigações avançadas e interrupção de ameaças para melhorar significativamente o trabalho de detecção e resposta a ameaças da organização.

Saiba mais sobre o MDR com tecnologia da McAfee em www.mcafee.com/MDR.

1. O MVISION Insights requer a telemetria do McAfee Endpoint Security (opcional) para funcionar adequadamente. Caso não queira fornecer essa telemetria, você não deve escolher este produto, pois não poderá aproveitar tudo que ele oferece.

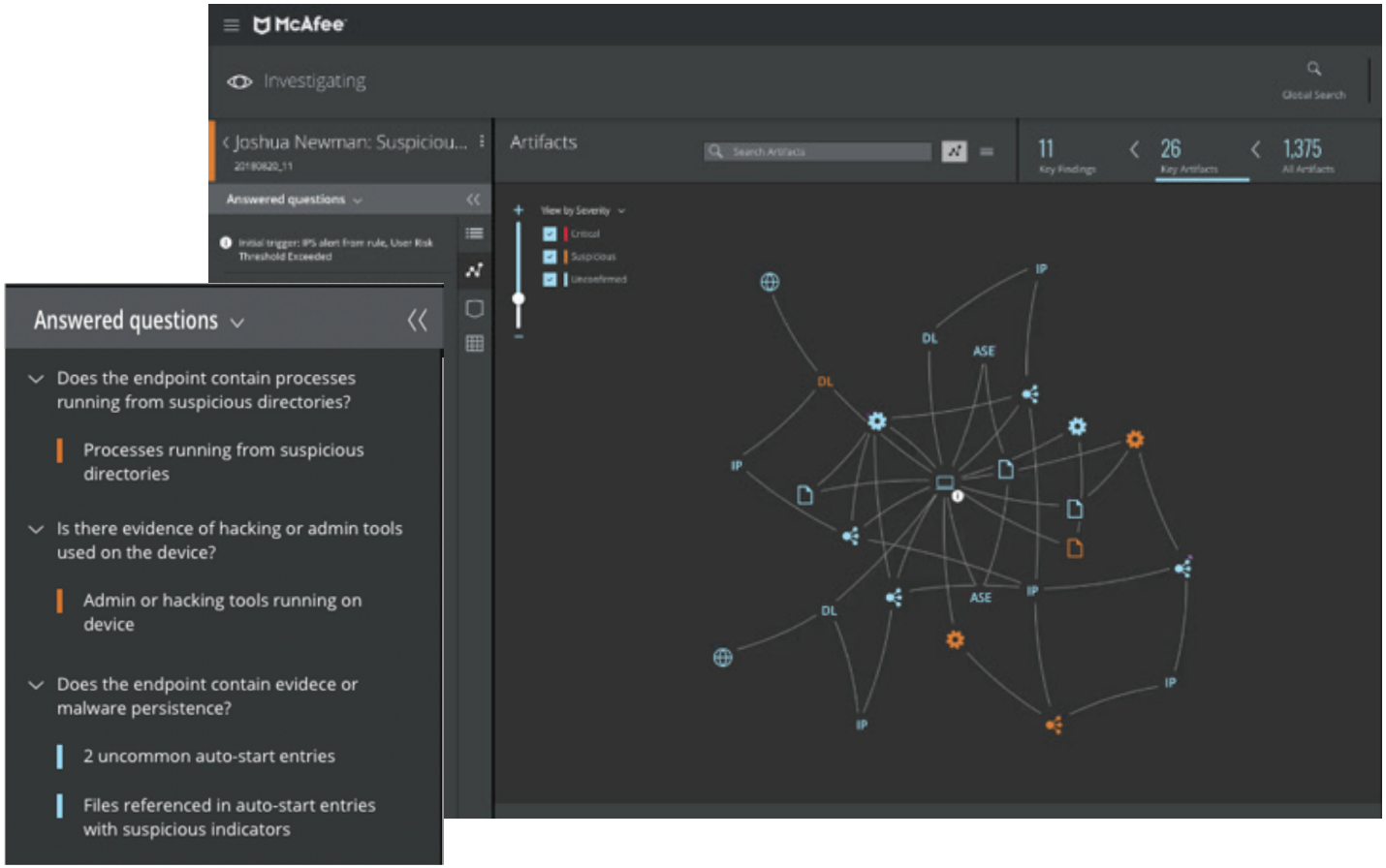

Figura 2. O MVISION EDR investiga para você. Ele coleta anomalias automaticamente e apresenta as principais descobertas. A visualização exibe relações e velocidades que os analistas entendem. O MVISION EDR pergunta e responde as questões certas para provar ou descartar as hipóteses.

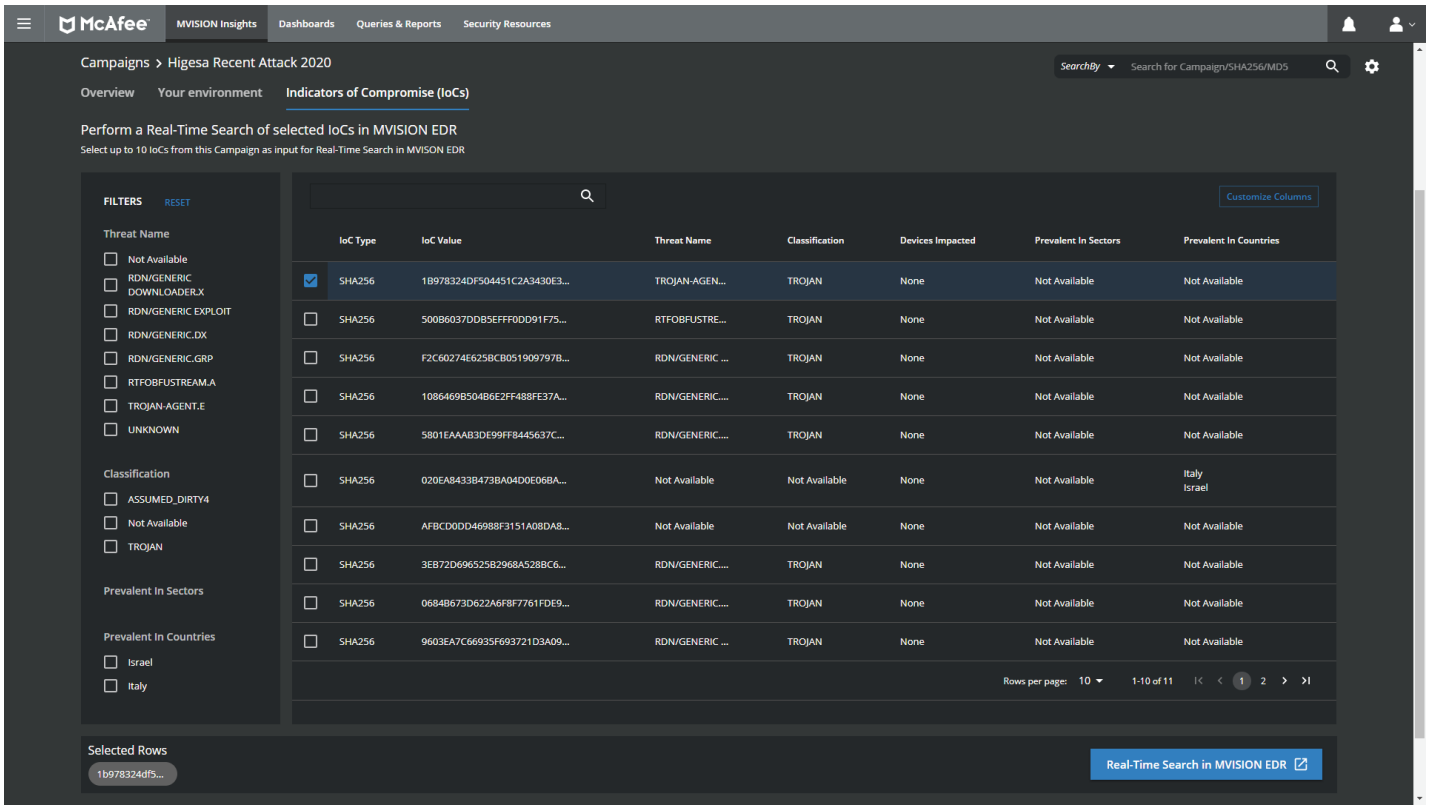

Figura 3. O MVISON Insights oferece IoCs de uma ameaça de alta prioridade, com a opção de pesquisar no EDR.

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