# McAfee MVISION Insights

## A primeira capacidade de segurança de endpoint que reforça dinamicamente a sua postura de segurança para que você possa ficar à frente dos adversários

A evolução e o ritmo das ameaças cibernéticas são um perigo constante e um ponto de estresse para as organizações. As empresas reagiram aumentando seus orçamentos de segurança em meio a uma escassez de qualificações nessa área, mas ainda não conseguem se manter ao nível de adversários modernos que atualizam constantemente seu arsenal de ferramentas, táticas e técnicas. As opções atuais são de inteligência compartimentada, exigindo intervenção humana e manual. Estas podem lidar com ameaças imediatas, mas a quantidade crescente e as nuances dos ataques cibernéticos bombardeiam constantemente as equipes de segurança, forçando-as a uma postura reativa. Uma plataforma de inteligência sobre ameaças (TIP) pode oferecer um oceano de dados sobre ameaças, mas requer integração manual e ciclos de análise, o que limita a capacidade de ação e correção. O gerenciamento de vulnerabilidades pode oferecer recomendações quanto a vulnerabilidades existentes e seus níveis de gravidade, mas proporciona insights limitados sobre como a sua postura de segurança pode ou não se defender contra as ameaças atuais do mundo real.

A solução é o McAfee® MVISION Insights, com uma inteligência em tempo real que viabiliza ações proativas. Uma inteligência abrangente, depurada e analisada por inteligência artificial e seres humanos, permite priorizar quais ameaças e campanhas têm mais chances de visar a sua organização. O MVISION Insights prevê exatamente como uma ameaça afetaria a sua segurança geral, além de prescrever exatamente o que você precisa fazer para otimizar a sua postura de segurança.

### Principais vantagens

- **Inteligência sobre risco coletada de um bilhão de sensores:** identifique proativamente projetos de ameaça fora do seu perímetro, de uma fonte confiável. Priorize projetos de ameaça segundo o mercado vertical, a geografia e a sua postura de segurança de endpoint corporativa
- **Identifique campanhas de ameaças antes de um ataque e priorize o seu nível de risco em um único console:** obtenha inteligência decisiva sobre uma ameaça e sobre o quão eficaz será a sua postura de segurança de endpoint contra ela, incluindo recomendações de correção
- **Reduza o tempo médio entre detecção e resolução:** simplifique os fluxos de trabalho para acelerar a implementação de proteções adicionais. Avalie a sua postura de segurança de endpoint atual com mudanças decisivas necessárias e reduza o tempo de resposta de meses para horas

Conecte-se conosco

## Transforme a sua segurança para se tornar mais proativo

O MVISION Insights oferece novas capacidades, incorporadas na experiência da plataforma de gerenciamento da McAfee®, que simplificam e se alinham exclusivamente com as operações contra riscos e ameaças para aprimorar preemptivamente as contramedidas defensivas e reduzir os tempos de resposta, ao mesmo tempo que utilizam menos recursos. A inteligência sobre riscos coletada de um bilhão de sensores capacita a sua empresa com os insights necessários para priorizar as defesas. Detecção, correção, resposta preemptiva acelerada e redução significativa do risco são conseguidas com um único console.

Estratégias reativas de defesa cibernética desempenham sua função como um componente crítico de defesa cibernética, mas estão limitadas a lidar com fatos consumados e "apagar incêndios". Os adversários estão utilizando ferramentas de nova geração para elaborar campanhas voltadas contra defesas tradicionais, testando produtos de segurança reativos para ver quais técnicas atravessam seus escudos. As organizações precisam lidar com todo o ciclo de vida do ataque, antes e depois de serem atingidas.

## Ciclo de vida do ataque


Figura 1. O ciclo de vida de um ataque típico.

No final das contas, inteligência e insights decisivos viabilizam a melhor postura de segurança cibernética possível contra as ameaças mais prováveis e aumentam a confiança nas suas defesas. Veja como o McAfee MVISION Insights consegue isso:

- **Ajuda a reduzir os pontos cegos e melhora a conscientização situacional:** você sabe exatamente o quão eficazes serão as suas defesas, antes delas serem atingidas. O MVISION Insights rastreia e prioriza proativamente as ameaças locais e globais previstas para atingir a sua empresa.

## O MVISION Insights oferece respostas para questões relacionadas ao risco em endpoints

- Você está correndo risco? Qual é o seu nível de exposição?
- Como você prioriza os ataques que podem atingir a sua organização? Como você aprende sobre eles? Qual é o seu processo de pesquisa?
- Como você determina quais ameaças podem atingir a sua organização, embora ainda não tenham atingido?
- Mesmo que você tivesse uma TIP, como priorizaria todos os ataques dentro do banco de dados da TIP?
- Como determinar quais ameaças atingiram seus pares?
- Qual é a predominância no seu setor e região?
- O quão eficiente é a sua postura de segurança atual contra essa ameaça?
- Qual é o seu nível de confiança diante do cenário de ameaças como um todo e por quê?

- **Análises de autoaprendizagem:** essa capacidade permite determinar qual seria o desempenho da sua postura de segurança específica e, em seguida, prescreve ações de proteção preemptivas que podem ser implementadas com rapidez e facilidade para bloquear esses ataques.
- **Identifica automaticamente ameaças globais que passariam despercebidas:** o MVISION Insights faz uso de um imenso reservatório de inteligência de segurança, obtido de mais de um bilhão de sensores.

## Dashboard do MVISION Insights


Figura 2. Exemplo de dashboard do MVISION Insights.

## Avaliações de risco

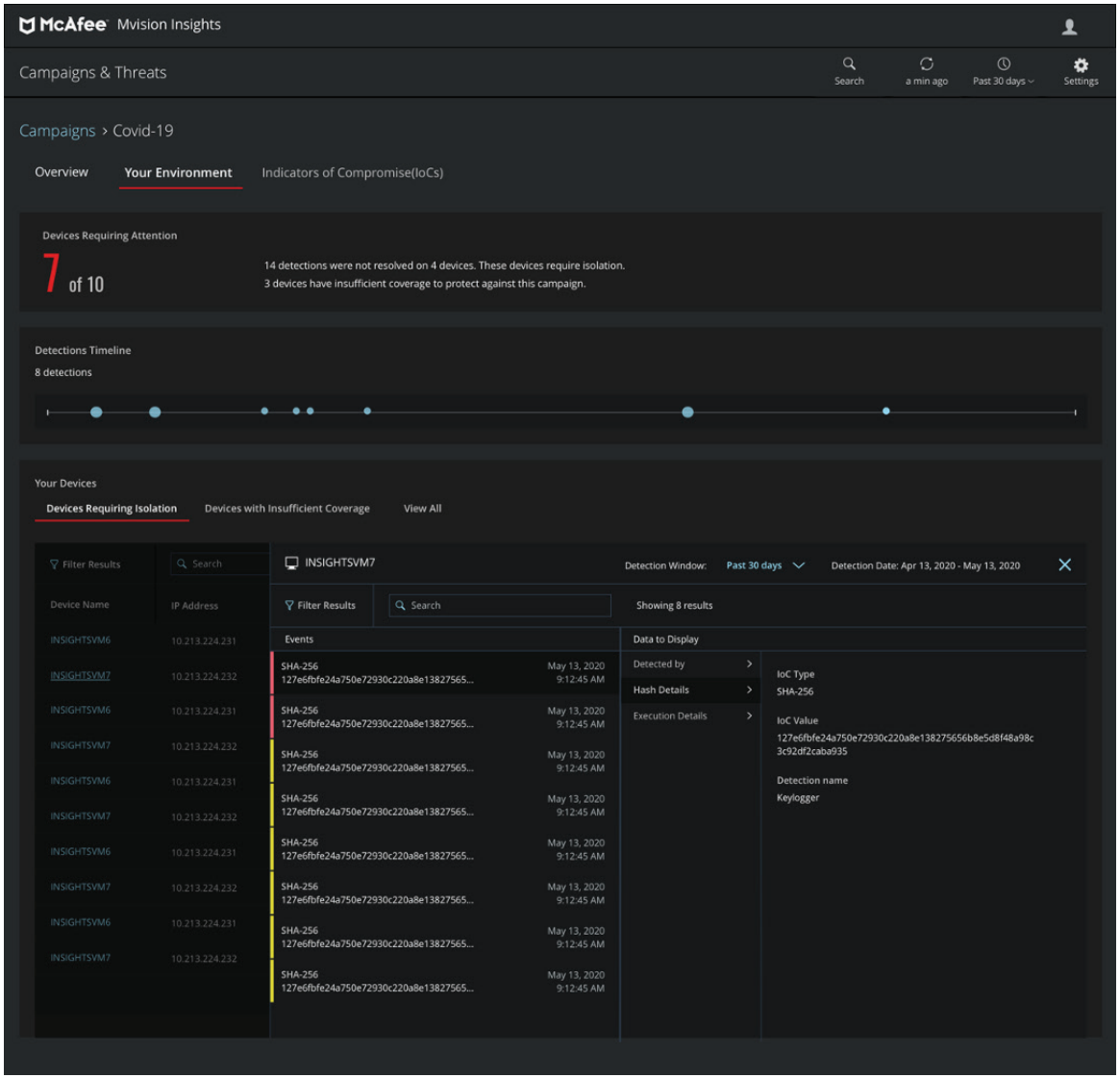


Figura 3. Saiba o que exige atenção no seu ambiente para combater proativamente a ameaça.

## Reduza significativamente os tempos de detecção e resposta

O MVISION Insights ajuda a sua empresa a dar o próximo passo proativo crítico para mudar e corrigir o seu ambiente específico com ações automatizadas e orientações prescritivas. A automação aumenta a eficácia contra ataques externos ao analisar e comparar automaticamente as ameaças externas e defender proativamente contra elas antes do ataque.

- **Reduza o tempo médio necessário para detecção e resolução, de meses para minutos:** com a colaboração homem-máquina (aprendizagem profunda e autoaprendizagem), as capacidades avançadas de análise são expandidas, o que possibilita investigar quantidades enormes de dados e apresentar informações de inteligência decisivas. Capacidades expandidas de detecção aceleram preemptivamente a resposta e reduzem significativamente o risco.
- **Melhore a relação sinal/ruído dos indicadores de ameaças:** a análise avançada expande a detecção e interpreta melhor os alertas. A análise de ameaças do MVISION Insights pode recorrer facilmente ao McAfee® MVISION EDR para buscar contexto adicional, como indicadores de comprometimento (IoCs) e reduzir os ciclos de investigação.
- **As ameaças são apresentadas a você de uma forma compreensível, com priorização e possibilidade de execução de ações:** a resposta orientada com base em insights e inteligência analisada e priorizada capacita até mesmo analistas novatos. Do console integrado, responda com rapidez e facilidade fazendo alterações nas suas configurações, isolando dispositivos infectados, atualizando a política ou alternando para detecção e resposta em endpoint (EDR).

## Capacite os recursos do SOC

As equipes de segurança estão sobrecarregadas com o imenso volume de informações que devem analisar para proteger seus ambientes. Tempo e recursos limitados inibem a análise de ameaças e as defesas. Com a parceria homem-máquina, as capacidades analíticas são expandidas — não importando o nível de capacitação dos analistas — para perscrutar enormes quantidades de dados e apresentá-las como informações decisivas. O MVISION Insights permite que a sua empresa enfrente a falta de qualificações e capacite as funções do SOC. As equipes de segurança ficam melhor informadas, para que possam tomar decisões melhores.

- Os insights humanos obtidos pelo uso da inteligência fornecida sobre os dados permitem que as equipes de segurança personalizem e maximizem as defesas corporativas para uma proteção otimizada, sem exigir aumento do tamanho ou das qualificações da equipe, nem depender de um alto nível de qualificação. O MVISION Insights oferece insights mais significativos para o MVISION EDR, reduzindo a duração do ciclo de investigação e proporcionando o conhecimento e os recursos necessários para a realização das investigações. Os analistas podem verificar o risco do incidente e a causa-raiz com mais velocidade e eficiência.

- Ajuda os diretores de segurança (CSOs) a obter o máximo de suas equipes e de seus produtos ao livrar os analistas de segurança das tarefas corriqueiras e ajudando até mesmo os integrantes mais novatos da equipe a se tornarem mais eficientes. As organizações podem conseguir uma redução nas horas despendidas no gerenciamento da segurança. Os fluxos de trabalho podem ser simplificados para acelerar proteções adicionais.
- Automatiza preemptivamente a detecção, a resposta e as defesas contra ameaças priorizadas em um único console, reduzindo a necessidade dos analistas de alternar entre tarefas. O MVISION Insights acumula e analisa elementos de dados relevantes com orientação decisiva em um único lugar, colocando tudo ao alcance dos analistas de segurança quando necessário.

## Insights mais profundos

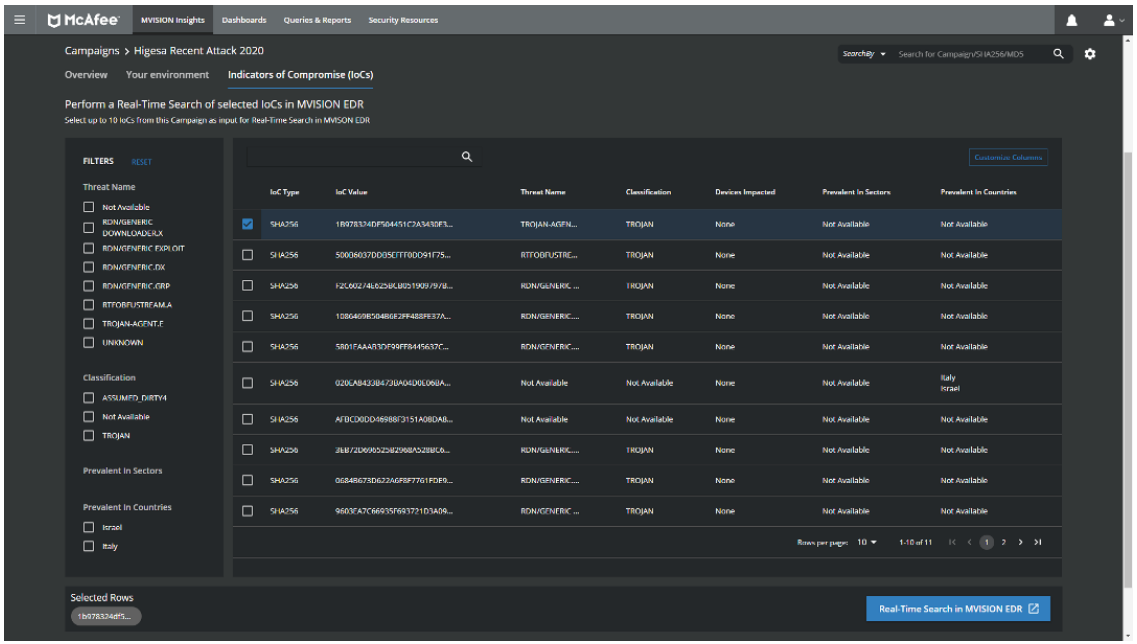


Figura 4. Investigue mais a fundo para compreender os eventos de ameaça e determinar a sua capacidade de defender a sua organização.

## Requisitos do MVISION Insights

O MVISION Insights é gerenciado pelo software McAfee® ePolicy Orchestrator® (McAfee® ePO™) 5.10 (no local e IaaS) e pelo McAfee® MVISION ePO™ (SaaS). Ele é otimizado para uso com nossa mais recente tecnologia de proteção de endpoint: o McAfee® Endpoint Security e o McAfee® Agent. O MVISION Insights requer adesão à telemetria do McAfee Endpoint Security para funcionar devidamente.

## Exemplos de casos de uso

| Problema | Solução | Resultado |
|---|---|---|
| **Estou sendo visado?**<br>**Esta é uma nova variante de campanha?** | ▪ Avaliação de ameaça de campanha conhecida<br>▪ Análise retrospectiva de ataque específico<br>▪ Relatório comparativo de eficácia da proteção<br>▪ Análise retrospectiva de ataque a IoC do usuário | Responder a pergunta: estou correndo risco? |
| **Minha configuração de proteção atual pode me proteger?** | ▪ Verificação da postura de proteção local | Avaliar minha postura de segurança atual |
| **O que devo mudar, especificamente, para estar protegido?** | ▪ Verificação da postura de proteção local | Orientação prescritiva sobre o que fazer |
| **Minhas outras funções de segurança podem ser isoladas?** | ▪ Publicar ações de isolamento ou contenção para outras funções de segurança | Enviar ações de contenção para outras funções de segurança com o objetivo de reduzir o risco (via DXL) |

## Learn More

Para obter mais informações, visite www.mcafee.com/br.

McAfee

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