McAfee MVISION Insights

Il primo modulo per la protezione degli endpoint in grado di rafforzare dinamicamente il tuo livello di sicurezza per essere sempre un passo avanti ai criminali informatici.

L'evoluzione e il ritmo delle minacce informatiche rappresentano un pericolo e una fonte costante di tensione per le aziende. A fronte della carenza di competenze in materia di sicurezza, le aziende hanno risposto incrementando i budget dedicati alla sicurezza. Ciononostante, ancora non riescono a sostenere il ritmo imposto da criminali informatici che aggiornano costantemente il loro arsenale di strumenti, tattiche e tecniche. Le attuali opzioni di informazioni sulle minacce sono molto spesso isolate e richiedono un intervento manuale. Sono in grado di affrontare le minacce immediate, ma il crescente numero e la varietà di attacchi informatici mettono costantemente sulla difensiva i team della sicurezza. Una piattaforma di informazioni sulle minacce informatiche può offrire un ampio data lake sulle minacce, ma richiede un'integrazione e cicli di analisi manuali, che ne limita le possibilità di fruizione immediata e di applicazione delle misure correttive. Una soluzione di gestione delle vulnerabilità è in grado di identificare le vulnerabilità esistenti e la loro gravità, ma offre informazioni limitate quando si tratta di determinare se il tuo attuale livello di sicurezza può o meno proteggerti contro le minacce reali attualmente in circolazione.

La soluzione è McAfee® MVISION Insights, uno strumento di informazioni sulle minacce informatiche in tempo reale che ti permette di agire in modo proattivo. Condensate e analizzate dall'intelligenza artificiale e da esperti, queste informazioni sulle minacce informatiche complete permettono di prioritizzare le minacce e le campagne d'attacco al fine di identificare quelle che hanno maggiori possibilità di colpire la tua azienda. McAfee MVISION Insights prevede con precisione l'impatto di una minaccia sulla tua protezione complessiva, oltre a indicarti la procedura da seguire per ottimizzare il tuo livello di sicurezza.

Vantaggi principali

- **Informazioni sui rischi raccolte da un miliardo di sensori:** identifica in modo proattivo le minacce previste al di fuori del tuo perimetro attraverso una fonte approvata. Assegna le priorità alle minacce previste per settore, area geografica e livello di protezione degli endpoint aziendali.
- **Identificazione delle campagne prima dell'attacco e prioritizzazione del livello di rischio da un'unica console:** ottieni informazioni fruibili su una minaccia e sull'efficacia della protezione dei tuoi endpoint a tal proposito, incluse le raccomandazioni sulle misure correttive da applicare.
- **Riduzione del tempo medio tra il rilevamento e la risoluzione:** ottimizza i flussi di lavoro per accelerare l'implementazione di ulteriori misure di protezione. Valuta il livello di protezione attuale dei tuoi endpoint grazie a delle contromisure raccomandate e accelera i tempi di risposta (da diversi mesi a poche ore).

Seguici

La necessità di un approccio più proattivo

MVISION Insights offre nuove funzionalità integrate nella piattaforma di gestione McAfee® che si allineano perfettamente con la gestione dei rischi e delle minacce e la supportano per migliorare le contromisure difensive e accelerare i tempi di risposta utilizzando meno risorse. Le informazioni sui rischi raccolte di dati acquisiti da un miliardo di sensori forniscono alla tua azienda le conoscenze necessarie per assegnare le priorità alle difese. Una moltitudine di compiti, tra cui rilevamento, applicazione di misure correttive, tempi di risposta delle azioni preventive accelerati e una significativa riduzione del rischio, possono essere eseguiti da un'unica console.

Le strategie di difesa informatica reattive svolgono un ruolo importante ma spesso sono in ritardo rispetto alle tecniche utilizzate dai criminali informatici e di solito si limitano a rispondere alle emergenze. I criminali informatici utilizzano strumenti di nuova generazione per sviluppare campagne concepite per sfidare le difese tradizionali e stanno testando i prodotti di sicurezza reattivi per identificare le tecniche in grado di penetrare tali difese. Le aziende devono disporre di una soluzione in grado di coprire l'intero ciclo di vita dell'attacco, prima e dopo essere state colpite.

Ciclo di vita di un attacco

Figura 1. Ciclo di vita classico di un attacco.

In fin dei conti, le informazioni sulle minacce informatiche direttamente fruibili consentono di migliorare la tua sicurezza informatica applicando misure proattive contro le minacce più probabili e di essere più certo dello stato delle misure difensive dell'azienda. McAfee MVISION Insights adotta un approccio su tre fronti:

- **Riduzione delle zone d'ombra e miglioramento della consapevolezza della situazione:** sai esattamente la copertura offerta dalla tua soluzione di sicurezza prima che le minacce colpiscano la tua azienda. MVISION Insights tiene traccia e assegna le priorità proattivamente alle minacce locali e globali che potrebbero colpire la tua azienda.

MVISION Insights risponde alle domande sul rischio posto dagli endpoint

- Sei vulnerabile? Qual è il tuo livello di vulnerabilità?
- In che modo classifichi per priorità gli attacchi che potrebbero colpire la tua azienda? Come ne vieni a conoscenza? Qual è la tua procedura di ricerca?
- Come fai a sapere quali sono le minacce che non hanno colpito la tua azienda, ma che probabilmente lo faranno?
- Anche se avessi una piattaforma di informazioni sulle minacce (TIP), come assegneresti le priorità a tutti gli attacchi nel database TIP?
- Come vieni a conoscenza delle minacce che hanno colpito le aziende del tuo settore?
- Qual è la prevalenza di queste minacce nel tuo settore e nella tua area geografica?
- In che misura il tuo attuale sistema di protezione è in grado di contrastare queste minacce?
- Quanto ti fidi della tua protezione a fronte del panorama delle minacce e perché?

- **Analisi basata sull'apprendimento automatico:** questa funzionalità permette di stabilire l'efficacia del tuo livello di sicurezza specifico e ti comunica le misure preventive da applicare per bloccare in modo rapido e facile tali attacchi.
- **Identificazione automatica delle minacce globali che non avevi rilevato:** MVISION Insights sfrutta un enorme bacino di informazioni sulla sicurezza provenienti da oltre un miliardo di sensori.

Dashboard MVISION Insights

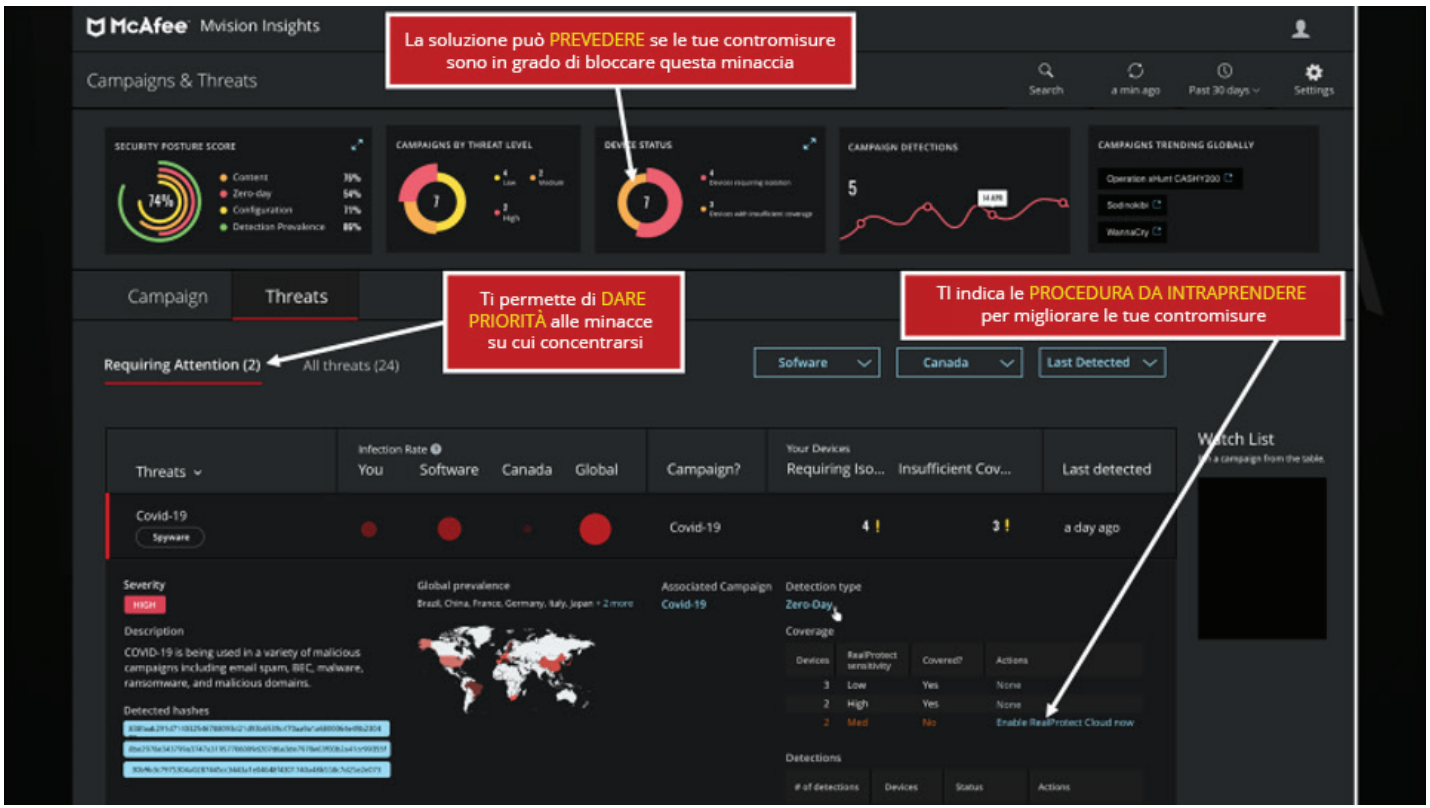

Figura 2. Esempio di una dashboard MVISION Insights.

Valutazione dei rischi

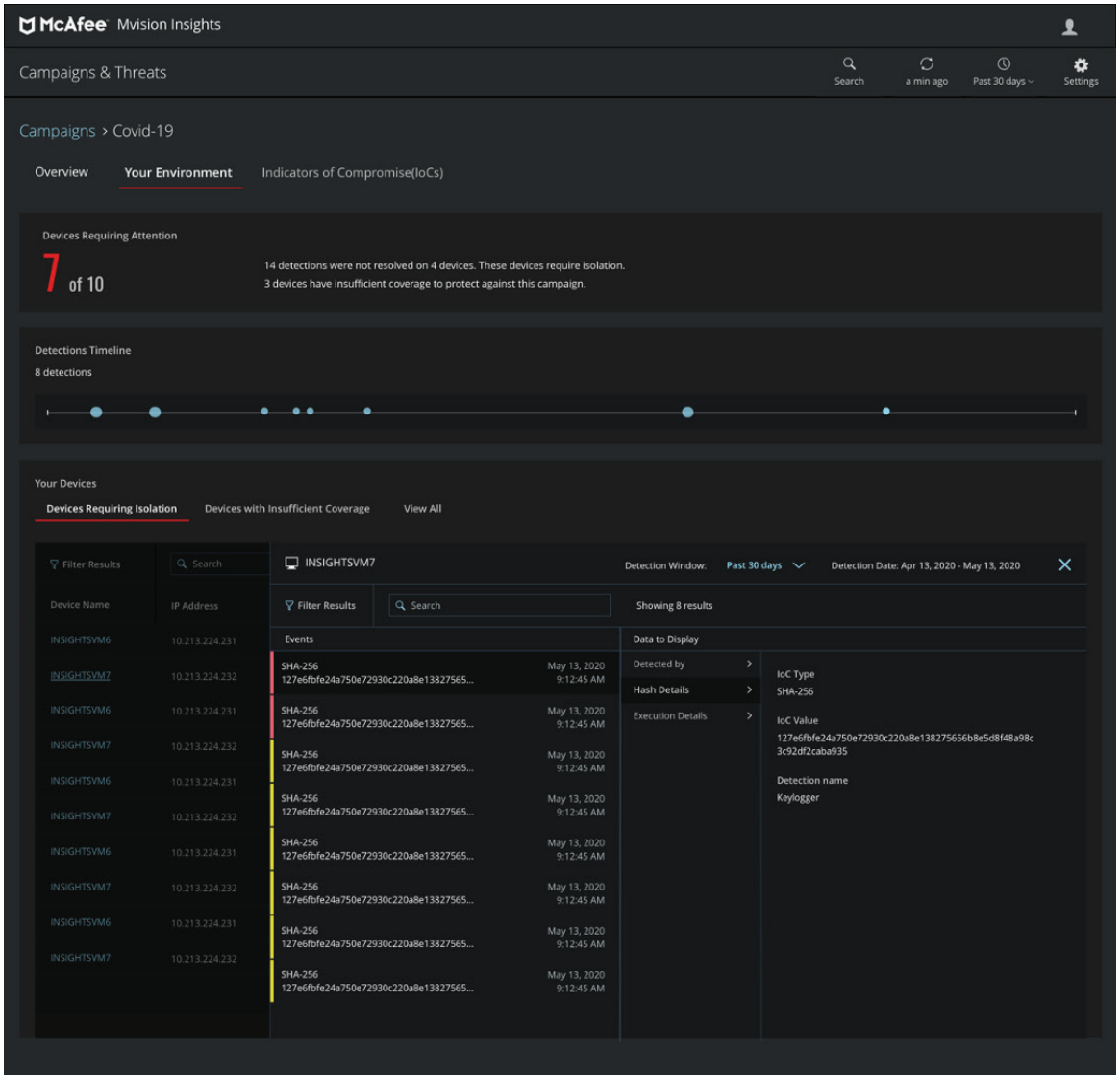

Figura 3. Identifica con precisione le vulnerabilità nel tuo ambiente per contrastare in modo proattivo le minacce.

Rilevamento e tempi di risposta accelerati in modo significativo

MVISION Insights aiuta la tua azienda a correggere e rafforzare la sicurezza del tuo ambiente unico, indicandoti la procedura da seguire e proponendoti azioni automatiche. L'automazione permette di contrastare gli attacchi esterni in modo più efficiente. La soluzione analizza e confronta automaticamente le minacce esterne e propone misure di protezione proattiva prima che attacchino.

- **Riduzione del tempo medio tra il rilevamento e la risoluzione da mesi a minuti:** la combinazione di uomo e macchina (deep learning e machine learning) e le capacità di analisi avanzata permettono di esaminare enormi volumi di dati per presentare informazioni direttamente fruibili. L'ampia capacità di rilevamento in modalità preventiva accelera i tempi di risposta e riduce in modo significativo il rischio.
- **Miglioramento del rapporto segnale-rumore per gli indicatori di minaccia:** le analisi avanzate migliorano il rilevamento delle minacce e l'interpretazione degli allarmi. La funzionalità di analisi delle minacce di MVISION Insights può passare facilmente a McAfee® MVISION EDR per cercare ulteriori contesti, come gli indicatori di compromissione (IoC), e ridurre i cicli d'indagine.
- **Le minacce vengono presentate in modo comprensibile e in base a priorità, insieme a suggerimenti relativamente alle misure da adottare:** un intervento guidato, basato su informazioni analizzate e prioritizzate, migliora l'efficienza anche dell'analista più inesperto. Dalla console integrata è possibile intervenire in modo rapido e semplice modificando le configurazioni, isolando i dispositivi infetti, aggiornando le policy o passando alla soluzione EDR (Endpoint Detection and Response).

Maggiore autonomia delle risorse SOC

I team di sicurezza sono sopraffatti dal volume di informazioni che devono esaminare per garantire la protezione del loro ambiente. La mancanza di tempo e risorse ostacola l'analisi delle minacce e delle difese. Indipendentemente dalle competenze degli analisti, la combinazione di uomo e macchina permette di estendere le capacità di analisi e di fare ordine tra enormi quantità di dati al fine di presentare delle informazioni direttamente fruibili. MVISION Insights permette alla tua azienda di superare la mancanza di competenze e offre al personale del centro SOC le informazioni necessarie per agire. I team di sicurezza sono meglio informati e possono così prendere decisioni migliori.

- La comprensione umana ottenuta grazie alle informazioni sulle minacce consente ai team di sicurezza di personalizzare e di rafforzare le difese di un'azienda per garantire una protezione ottimale senza la necessità di personale aggiuntivo o di acquisire nuove competenze. MVISION Insights alimenta MVISION EDR con dati più rilevanti per ridurre il ciclo di indagine e offre le competenze e le risorse necessarie per condurre delle ricerche. Gli analisti possono verificare in modo più rapido ed efficiente il rischio posto dall'incidente e la sua causa.
- La soluzione permette ai responsabili della sicurezza di ottenere il massimo dalle persone e dai prodotti, liberando gli analisti della sicurezza da compiti di routine e aiutando i membri del team meno esperti a migliorare. Le aziende possono ridurre il tempo dedicato alla gestione della sicurezza. I flussi di lavoro possono essere razionalizzati per accelerare l'implementazione di ulteriori misure di sicurezza.
- La soluzione automatizza preventivamente il rilevamento, la risposta e la protezione per le minacce prioritizzate da una singola console, evitando agli analisti di passare da un compito all'altro. MVISION Insights raccoglie e analizza i dati rilevanti e comunica le procedure da seguire in risposta alle minacce in un unico luogo facilmente accessibile per gli analisti della sicurezza.

Informazioni migliori e più rilevanti

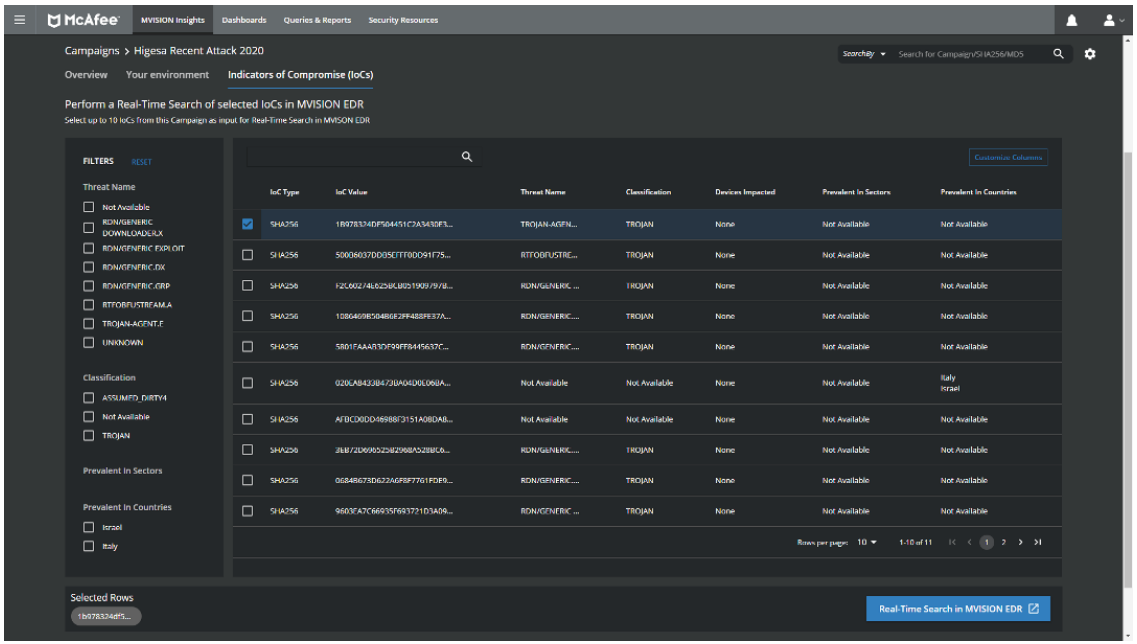

Figura 4. Approfitta di un'analisi più approfondita per comprendere meglio le minacce e stabilire la tua capacità di proteggere la tua azienda.

Requisiti di sistema di MVISION Insights

MVISION Insights è gestito dal software McAfee® ePolicy Orchestrator® (McAfee® ePO™) 5.10 (in locale e IaaS) e McAfee® MVISION ePO™ (SaaS). La soluzione è ottimizzata per l'utilizzo con la nostra più recente tecnologia di protezione degli endpoint: McAfee® Endpoint Security e McAfee® Agent. Per funzionare in modo efficace, MVISION Insights deve accettare i dati telemetrici di McAfee Endpoint Security.

Esempi di casi di utilizzo

Problema	Soluzione	Risultato
Sono sotto attacco? **È una nuova variante della campagna?**	▪ Valutazione delle minacce delle campagne conosciute ▪ Analisi retrospettiva di un determinato attacco ▪ Relazione comparativa sull'efficacia delle misure di protezione ▪ Analisi retrospettiva dell'attacco con gli indicatori di compromissione dell'utente	Rispondi alla domanda: Sono in pericolo?
La configurazione della mia soluzione di sicurezza è in grado di proteggermi?	▪ Controllo del livello di protezione locale	Valutazione dei mio livello di protezione attuale
Quali modifiche specifiche devo apportare per essere protetto?	▪ Controllo del livello di protezione locale	Suggerimenti prescrittivi sulle azioni da intraprendere
Le mie altre funzioni di sicurezza possono isolare la minaccia?	▪ Pubblicazione per isolare o contenere in altre funzioni di sicurezza	Invio delle azioni di contenimento ad altre funzioni di sicurezza per limitare ulteriormente il rischio (tramite DXL)

Ulteriori informazioni

Ulteriori informazioni sono disponibili sul sito mcafee.com/it.

McAfee

Via Fantoli 7
20138 Milano Italia
02 554171
www.mcafee.com/it