SCHEDA TECNICA

McAfee MVISION Endpoint Detection and Response (MVISION EDR)

Potenza di rilevamento, analisi guidata e risposta alle minacce, semplificate.

Gli avversari si muovono in maniera occulta, camuffando le proprie azioni all'interno dei componenti affidabili già presenti nel tuo ambiente. Non sempre installano qualcosa di tangibile come il malware, ma sempre lasciano una traccia comportamentale. Endpoint detection and response (EDR) svolge un monitoraggio continuo, raccogliendo dei dati che forniscono la visibilità e il contesto necessari per rilevare e rispondere alle minacce. Tuttavia i metodi finora utilizzati scaricavano troppe informazioni sugli addetti alla sicurezza, già molto impegnati. McAfee® MVISION EDR aiuta a gestire l'alto volume di allarmi, consentendo ad analisti con qualsiasi livello di competenza di fare di più e di svolgere indagini più efficaci.

Rinforza, velocizza e semplifica il rilevamento e risposta per gli endpoint

MVISION EDR riduce il tempo medio necessario per rilevare e rispondere alle minacce, permettendo a tutti gli analisti di comprendere gli allarmi, analizzarli a fondo e reagire rapidamente. Le analisi avanzate ampliano il rilevamento e chiariscono gli allarmi. L'automazione e le analisi guidate dall'intelligenza artificiale (AI) permettono anche agli analisti inesperti di eseguire analisi di livello superiore, mentre quelli più anziani possono applicare le proprie capacità alla ricerca delle minacce, abbreviando i tempi di risposta.

Rileva e rispondi più velocemente alle minacce avanzate contro gli endpoint

Senza dati, contesto e analisi corrette, i sistemi EDR generano troppi allarmi oppure non vedono le minacce emergenti, sprecando tempo e risorse preziosi senza migliorare la sicurezza. MVISION EDR offre una raccolta dati sempre attiva e svariati motori analitici in tutte le fasi di rilevamento e indagine, per far emergere accuratamente i comportamenti sospetti, interpretare gli allarmi ed eseguire azioni informate.

- **Guadagna in contesto e visibilità:** le informazioni sugli eventi degli endpoint vengono inviate nel cloud, offrendo il contesto e la visibilità necessari per scoprire le minacce occulte. Le informazioni degli endpoint sono disponibili per l'ispezione immediata e la ricerca in tempo reale, oltre che per le ricerche cronologiche. Opzioni flessibili di conservazione dei dati supportano le svariate esigenze dei differenti gruppi e organizzazioni che svolgono le operazioni di sicurezza.

Vantaggi principali

- Rileva le minacce in modo pratico e con alta qualità, senza il rumore di fondo.
- Le analisi più rapide ti permettono di predisporre una difesa più resistente.
- Le indagini guidate dall'intelligenza artificiale offrono approfondimenti automatici sugli attacchi.
- Le aziende massimizzano l'efficacia del personale esistente.
- È una soluzione a bassa manutenzione, basata sul cloud.
- Semplifica le distribuzioni sfruttando il software McAfee ePO in sede oppure la soluzione MVISION ePO di tipo SaaS.
- Gli analisti possono concentrarsi sulla risposta strategica agli eventi senza il fardello delle attività amministrative.

Seguici

- **Scopri di più con le potenti analisi basate sul cloud:** i motori di analisi ispezionano le attività degli endpoint per scoprire un ampio spettro di comportamenti sospetti e rilevare quelle minacce (dal malware basato su file agli attacchi senza file) che sono sfuggite alle altre difese. La distribuzione basata sul cloud consente la rapida adozione dei nuovi motori e tecniche di analisi.
- **Pensa come un pirata informatico:** i risultati del rilevamento basato sui comportamenti vengono correlati al framework MITRE ATT&CK™, a supporto di un processo più uniforme per determinare la fase corrente di una minaccia, determinarne il rischio associato e dare priorità a una risposta.
- **Consulta i dati facilmente:** la classificazione degli allarmi aiuta gli analisti a capire la gravità di un rischio e a scegliere la risposta appropriata. È a questo punto che l'opzione flessibile di visualizzazione dei dati aiuta gli analisti con diversi livelli di esperienza a consultare i dati con facilità, per comprendere rapidamente perché un allarme è scattato e determinare il prossimo passaggio: chiusura, risposta o analisi.
- **Rispondi velocemente:** le risposte preconfigurate di MVISION EDR permettono un'azione immediata. Gli utenti possono facilmente contenere le minacce interrompendo un processo, mettendo in quarantena un computer ed eliminando i file. Gli analisti possono agire su un singolo endpoint oppure espandere la risposta all'intera sede con un solo clic.

Indagini guidate dall'AI

Se la risposta immediata a un allarme e la causa alla radice dell'evento non sono così ovvie (come spesso accade), gli analisti della sicurezza devono svolgere un'indagine al di fuori della soluzione EDR per capire veramente tutte le sfaccettature di una minaccia o campagna complessa e il rischio associato. Le tradizionali soluzioni EDR "consentono" un'indagine offrendo dati grezzi, contesto e funzioni di ricerca, ma necessitano comunque di analisti esperti per lo svolgimento delle attività di investigazione e analisi. Spesso gli analisti esperti non hanno il tempo di convalidare e indagare l'elevato numero di allarmi, mentre quelli inesperti non sanno a volte dove cominciare.

Con MVISION EDR gli analisti di qualsiasi livello possono compiere il passo successivo e indagare. Anziché limitarsi a consentire un'indagine con le funzionalità e i dati di ricerca, MVISION EDR guida l'analisi stessa.

- **Guide dinamiche all'indagine:** compilate combinando l'esperienza e le competenze degli investigatori forensi di McAfee con l'intelligenza artificiale, le guide all'indagine moltiplicano la forza del processo di indagine e valutano molte ipotesi in parallelo per massimizzare velocità e accuratezza. A differenza delle attività automatizzate negli script e mirate alle minacce note, le guide all'indagine si adattano in maniera dinamica allo specifico caso, combinando differenti dati e strategie di indagine. MVISION EDR genera automaticamente domande e risposte per provare o smentire le ipotesi. Sempre automaticamente, MVISION EDR raccoglie, riepiloga e visualizza le prove provenienti da numerose fonti per poi ripetere il processo con l'evoluzione dell'indagine.

- **Ampia raccolta dati e rilevanza locale:** il motore di indagine basato sull'AI raccoglie ed elabora artefatti e complesse sequenze di eventi provenienti dagli endpoint, dai sistemi SIEM (Security Information and Event Management, gestione degli eventi e delle informazioni di sicurezza) e dal software McAfee® ePolicy Orchestrator® (McAfee ePO™) per agevolare l'interpretazione degli allarmi. MVISION EDR confronta le prove con le attività normali note per ciascuna organizzazione e con le fonti di informazioni sulle minacce per migliorare la rilevanza locale e ridurre i falsi positivi. Le indagini possono partire sia dagli allarmi di MVISION EDR che del SIEM.
- **Viste differenti per utenti differenti:** la visualizzazione flessibile dei dati si adatta ai diversi livelli di esperienza degli utenti, così tutti gli analisti possono capire velocemente in che modo artefatti ed eventi sono correlati, senza dover consultare numerose schermate.
- **Indagini antiphishing:** MVISION EDR si inserisce facilmente nei processi di indagine antiphishing delle operazioni di sicurezza. Le email sospette possono essere inviate a MVISION EDR per l'ispezione e, se le ritiene ostili, MVISION EDR determina rapidamente quali computer in tutta l'organizzazione possono esserne stati colpiti.

MVISION EDR riduce le competenze e il lavoro necessari per lo svolgimento delle indagini e aumenta la velocità con la quale gli analisti possono determinare il rischio di un evento e la sua causa originaria. A livello organizzativo i vantaggi sono molteplici. Ciascun analista può essere più efficiente, un maggior numero di casi può essere smaltito dagli analisti giovani, mentre quelli più anziani possono svolgere attività di maggior valore.

I dati giusti, al momento giusto, per l'attività in corso

In aggiunta alle indagini guidate, analisti e cacciatori di minacce possono usare le potenti capacità di ricerca e raccolta dati di MVISION EDR per ampliare le indagini ed esaminare approfonditamente i diversi sistemi.

- **Ricerche cronologiche:** l'esaustiva e sempre attiva raccolta dati invia le informazioni degli eventi da tutti i sistemi monitorati al cloud. Gli analisti possono consultare questi dati centralizzati, a prescindere dallo stato online od offline di ciascun endpoint, per trovare gli indicatori di compromissione (IoC) e gli indicatori di attacco (IoA) eventualmente presenti insieme ai file eliminati.
- **Ricerca in tempo reale:** per le indagini attive sugli eventi, la ricerca in tempo reale raggiunge gli endpoint in tutto l'ambiente e li interroga rapidamente per avere informazioni aggiornate al momento. La sintassi flessibile consente svariate capacità di ricerca nelle workstation, da interrogazioni semplici sulle applicazioni installate a ricerche più complesse che restituiscono un maggior numero di dati, come l'identificazione di un utente al momento di un evento, l'esecuzione da riga di comando e il momento di avvio di un'applicazione sospetta. Questa capacità scala facilmente le interrogazioni in tutta l'impresa, fino a decine di migliaia di computer.

- **Raccolta dati su richiesta:** a supporto delle indagini e su richiesta, MVISION EDR scatta un'istantanea dell'endpoint, acquisendo una visualizzazione completa dei processi attivi, delle connessioni di rete, dei servizi e degli elementi in esecuzione automatica. MVISION EDR fornisce il livello di gravità associato oltre a informazioni aggiuntive, come hash, reputazione e il processo 'parent'/servizio/utente che ha eseguito un file sospetto. Abilitate da uno strumento di raccolta dati non persistente, le istantanee possono essere scattate sia nei sistemi monitorati che in quelli non monitorati.

La collaborazione amplia la visibilità, aumenta l'efficienza operativa e migliora i risultati

MVISION EDR è un componente fondamentale di un ecosistema di sicurezza integrato. Amplia le capacità di protezione degli endpoint ed espande la visibilità, supportando i flussi di lavoro e i processi degli addetti alla sicurezza per ridurre il tempo medio di rilevamento e risposta e aumentare l'efficienza operativa.

- **Correla i dati da tutta l'azienda per la visibilità completa:** la collaborazione e la facile integrazione con fonti di dati oltre gli endpoint sono essenziali per colmare le lacune dei dati e indagare minacce che presentano molte sfaccettature. La stretta integrazione con le soluzioni di gestione degli eventi e delle informazioni di sicurezza (SIEM), come McAfee® Enterprise Security Manager o i prodotti di terze parti, consente a MVISION EDR di ampliare le capacità di indagine e approfondimento correlando gli artefatti negli endpoint con le informazioni della rete e altri dati raccolti dal SIEM.
- **Supporto della collaborazione e dei flussi di lavoro nel team:** MVISION EDR si inserisce negli attuali processi delle operazioni di sicurezza e supporta la collaborazione condividendo i dati delle indagini e gli aggiornamenti tramite le piattaforme di risposta agli eventi.
- **Distribuzione semplice e scalabile:** MVISION EDR è disponibile come applicazione SaaS. La gestione con il software McAfee ePO, la piattaforma di gestione centralizzata della sicurezza più avanzata del settore, semplifica la distribuzione e la manutenzione continua di MVISION EDR e dell'intera infrastruttura di sicurezza. Ora disponibile sia in sede sia nel cloud, il software McAfee ePO offre una flessibilità gestionale che si adatta alle più svariate esigenze delle aziende.

Per informazioni su MVISION EDR, contatta il tuo rappresentante McAfee oppure visita www.mcafee.com/enterprise/it-it/solutions/mvision.html.

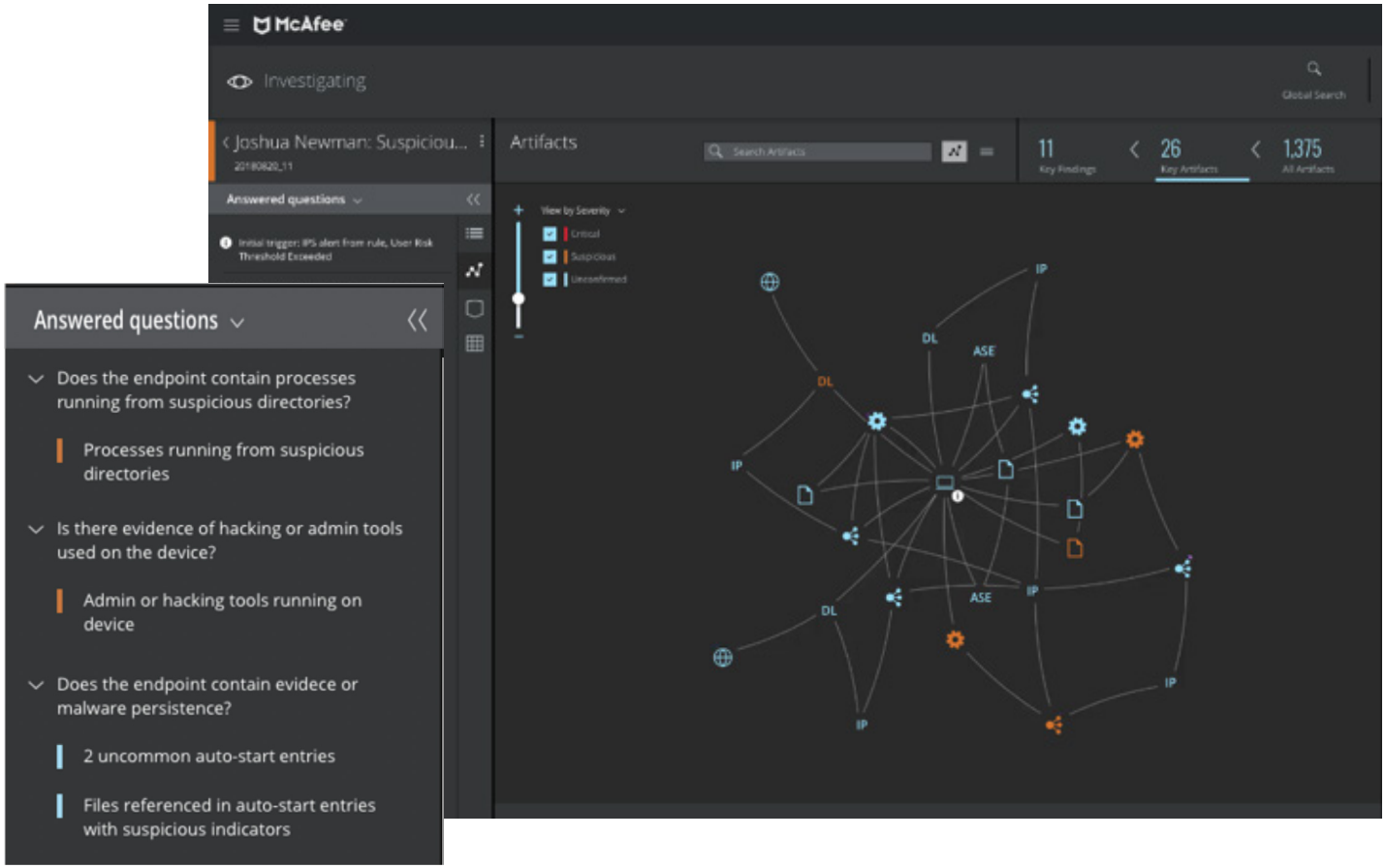

Figura 1. MVISION EDR indaga per te. Raccoglie automaticamente gli artefatti e ti presenta i risultati più importanti. La visualizzazione mostra le relazioni e velocizza la comprensione degli analisti. MVISION EDR genera automaticamente le giuste domande e risposte per provare o smentire le ipotesi.

McAfee
Together is power.

Via Fantoli, 7
20138 Milano
Italy
(+39) 02 554171
www.mcafee.com/it