McAfee ePolicy Orchestrator

Ispirazione e potenziamento per i professionisti della sicurezza

La gestione della protezione richiede complicate manovre fra strumenti e dati. Ciò rappresenta un vantaggio per gli avversari, che hanno più tempo per sfruttare le lacune fra gli strumenti e provocare così danni più gravi. Il personale della sicurezza informatica è limitato e perciò deve essere messo nelle condizioni di orchestrare semplicemente ambienti complessi.

La tua aziende ha bisogno di rispondere rapidamente alle minacce su qualsiasi tipo di dispositivo per ridurre al minimo i danni, mentre per la gestione è necessaria dimostrare l'efficacia della protezione. La piattaforma di gestione McAfee® ePolicy Orchestrator® (McAfee ePO™), disponibile sia in locale sia nel cloud, elimina le lungaggini e i potenziali errori umani, aiutando i responsabili della sicurezza a rispondere più rapidamente e con maggiore efficacia.

Protezione fondamentale

Partiamo dalle cose indispensabili. Alla base di qualsiasi architettura di sicurezza c'è la capacità di monitorare e controllare l'integrità di dispositivi e sistemi. Le normative del settore, come Center for Internet Security (CIS) Controls™ e Benchmarks e National Institute of Standards Technology (NIST) SP 800-53, obbligano a monitorare e controllare le infrastrutture di sicurezza informatica. La console McAfee ePO permette di ottenere una visibilità critica e di impostare e applicare automaticamente le policy per garantire un comportamento di sicurezza corretto in azienda. Elimina la complessità data dall'orchestrare multipli prodotti grazie alla gestione e imposizione delle policy nell'intera impresa da una singola console. Questa essenziale capacità di gestione della protezione è fondamentale per la conformità della tua sicurezza informatica.

Vantaggi principali

- Gestione centralizzata apprezzata nel settore, co un unico esclusivo pannello di controllo che semplifica il lavoro, disponibile nel cloud o in locale.
- Flussi di lavoro automatizzati che semplificano le attività amministrative e aumentano l'efficienza
- Piattaforma aperta e completa che integra McAfee e più di 150 soluzioni di terze parti per dare risposte più rapide e più accurate
- Gestione comune della sicurezza per la più grande quota di dispositivi sul mercato
- Sfrutta e potenzia i controlli nativi nei sistemi operativi come Windows Defender
- Scalabile a centinaia di migliaia di dispositivi, con copertura dal dispositivo al cloud

Seguici su

Gestione avanzata e collaudata della protezione. Di più: semplificata

Oltre 36.000 aziende ed enti si affidano alla console McAfee ePO per gestire la sicurezza, ottimizzare e automatizzare i processi di conformità e incrementare la visibilità complessiva su dispositivi, reti e operazioni di sicurezza. Le grandi imprese si affidano all'architettura altamente scalabile della console McAfee ePO, che permette loro di gestire centinaia di migliaia di nodi da un singolo pannello di controllo integrato. Questa visualizzazione aiuta a ordinare per priorità le attività legate ai rischi. Inoltre riepiloga la tua condizione di sicurezza, nell'intero spazio digitale, in un'unica veste grafica entro la nuova area di lavoro della protezione.

Per avere ulteriori informazioni gli amministratori possono approfondire specifici eventi. La visione riepilogativa riduce i tempi di creazione dei report e razionalizza i dati a portata di mano. Elimina inoltre i potenziali errori, anche se sono necessari interventi manuali. La console McAfee ePO fornisce all'amministratore della sicurezza aziendale l'opportunità di semplificare la manutenzione delle policy, acquisire informazioni sulle minacce di terze parti sfruttando Data Exchange Layer (DXL), la nostra struttura di messaggistica leader del settore e integrare le policy in senso bidirezionale fra una serie di prodotti. Queste efficienze operative tagliano l'impegno richiesto da processi e condivisione dei dati, consentendo una risposta più rapida e più precisa.

L'efficienza della piattaforma aperta contrasta la proliferazione

Una ricerca di ESG mostra che il 40% delle aziende utilizza da 10 a 25 strumenti, mentre il 30% utilizza da 26 a 50 strumenti per gestire miliardi di nuove minacce e dispositivi. La molteplicità di prodotti utilizzati crea complessità e moltiplica il vantaggio operativo di un'esperienza di gestione unificata, dall'installazione alla reportistica. Secondo più della metà delle aziende il miglioramento apportato dall'integrazione degli strumenti di sicurezza è stimabile in oltre il 20% (ricerca MSI 2018). McAfee abbraccia tali requisiti con una piattaforma aperta per la gestione della protezione, che consente di razionalizzare la proliferazione e di proteggere la vastità delle tue risorse. Supporta inoltre le informazioni sulle minacce, gestisce i dati open source e integra i prodotti di terze parti. McAfee offre un controllo centralizzato per la conformità e la gestione per una serie di prodotti di sicurezza. Gli analisti passano rapidamente da un prodotto all'altro per trovare i dati critici e prendere le necessarie azioni basate sulle policy. La console McAfee ePO consente inoltre di investire in tecnologie di nuova generazione e di integrarle con risorse esistenti all'interno di un unico framework.

La nostra piattaforma aperta offre vari metodi di integrazione (scripting, API, non API e un impegno minimo grazie al tessuto di messaggistica open source DXL). Ciò permette di scegliere l'approccio migliore per le tue esigenze, senza pesanti personalizzazioni o servizi. Tramite il programma McAfee® Security Innovation Alliance acceleriamo lo sviluppo di prodotti di sicurezza interoperabili,

Secondo gli analisti del settore, il software McAfee ePO è la ragione per cui i clienti adottano McAfee e restano con McAfee.

I vantaggi di una piattaforma integrata

Le aziende con piattaforme integrate sono meglio protette e ottengono tempi di risposta più rapidi rispetto alle loro controparti che non dispongono di una piattaforma integrata.

Aziende con piattaforme integrate

- Il 78% ha subito lo scorso anno meno di cinque violazioni.
- L'80% ha individuato le minacce entro otto ore.

Organizzazioni senza piattaforme integrate

- Solo il 55% ha subito lo scorso anno meno di cinque violazioni.
- Solo il 54% ha indivudato le minacce entro otto ore.

Fonte: Penn Schoen Berland 2016

ne semplifichiamo l'integrazione nei complessi ambienti dei clienti e creiamo un ecosistema di sicurezza connessa, veramente integrato, che massimizza il valore degli investimenti in sicurezza compiuti dai clienti. Il programma McAfee Security Innovation Alliance include oltre 150 integrazioni dei partner.

Inoltre, la struttura di comunicazione di Data Exchange Layer (DXL) collega e ottimizza le azioni di sicurezza tra prodotti di marche diverse, nonché tra le soluzioni sviluppate internamente e open source. Con l'integrazione di Cisco pxGrid e DXL hai accesso ai dati provenienti da altre 50 tecnologie di sicurezza. McAfee ePO è un componente fondamentale per la gestione della nostra robusta piattaforma aperta.

Sicurezza dei dispositivi ampliata: gestisci gli strumenti di sicurezza nativi

La piattaforma estendibile McAfee ePO gestisce svariati dispositivi, compresi quelli dotati di controlli nativi. McAfee migliora e co-gestisce la protezione già incorporata in Microsoft Windows 10 per ottimizzare la protezione, consentendo contemporaneamente alle aziende di trarre vantaggio dalle capacità native nei sistemi Microsoft. Il software McAfee ePO gestisce McAfee® MVISION Endpoint che combina avanzate capacità di apprendimento automatico, specificamente regolate per la protezione nativa nei sistemi operativi Microsoft, evitando al contempo di aumentare complessità e costi con un'ulteriore console di gestione. Il software McAfee ePO offre una gestione comune, con policy condivise per i dispositivi Microsoft Windows 10 e tutti i dispositivi dell'azienda eterogenea, per assicurare uniformità e semplicità.

Coerenza tramite flussi di lavoro automatizzati

Il software McAfee ePO offre funzionalità di gestione automatizzata flessibili, in modo da poter identificare, gestire e rispondere rapidamente alle vulnerabilità, alle modifiche nei comportamenti di sicurezza e alle minacce note da un'unica console. Secondo quanto rilevato dalla ricerca di MSI, commissionata da McAfee nel 2018, con l'automazione delle attività ripetitive o ripetibili le aziende prevedono di risparmiare circa il 25% di tempo al giorno. Con il software McAfee ePO puoi facilmente distribuire e imporre le policy di sicurezza da una singola visualizzazione, facendo clic su pochi passaggi logici sequenziali. Mentre svolgi le attività e vedi ciascun passaggio e il modo in cui si correla agli altri, il singolo pannello di controllo ti offre il contesto pertinente. Ciò riduce la complessità e minimizza la possibilità di errori. Puoi definire il modo in cui la console McAfee ePO deve dirigere avvisi e risposte di sicurezza, in base al tipo e alla criticità degli eventi di sicurezza per ambiente, policy e strumenti di cui disponi. Per supportare le operazioni di sviluppo e le operazioni di sicurezza, la piattaforma McAfee ePO consente di creare flussi di lavoro automatizzati tra i sistemi delle operazioni di sicurezza e IT per risolvere rapidamente i problemi. Puoi utiizzare la console McAfee ePO per avviare le azioni di remediation da parte dei sistemi delle operazioni informatiche, come l'assegnazione di policy più rigorose. La possibilità di sfruttare le sue API (Application Programming Interface) web riduce le attività manuali. Si ha la possibilità di richiedere un processo di approvazione prima che venga emessa una nuova policy o attività o un loro aggiornamento, riducendo così il rischio di un errore e garantendo il controllo della qualità.

Risparmio di tempo

La recente ricerca MSI del 2018 indica che i clienti stimano nel 20% il risparmio di tempo con l'integrazione degli strumenti di sicurezza.

Il valore dell'integrazione

- Aumenta l'efficacia di strumenti e processi: 61%
- Riduce la complessità e le attività manuali, consentendo ai professionisti della sicurezza di concentrarsi su quelle che richiedono un pensiero critico: 61%
- Migliora la visibilità mostrando tendenze e contesto dei dati: 58%
- Semplifica i flussi di lavoro per una risposta più rapida: 57%

Fonte: ricerca MSI 2018

Esempi di utilizzo comuni

- Risparmio di tempo ed eliminazione delle attività ridondanti e laboriose pianificando i report sulla conformità della sicurezza per soddisfare le esigenze di ogni soggetto interessato.
- Facile integrazione della console McAfee ePO nei processi e funzioni aziendali esistenti, grazie alla robusta serie di interfacce API (Application Program Interface) per ottenere maggiori informazioni e accelerare i flussi di lavoro. Per esempio, si integra con sistemi di gestione dei ticket, applicazioni web o portali di self-service.
- Mantenimento della condizione di sicurezza tramite la distribuzione di soluzioni con agent o basate sull'apprendimento automatico quando nuove macchine vengono aggiunte alla rete aziendale. La console McAfee ePO si sincronizza con Microsoft Active Directory.

Mitigazione e remediation rapide

La piattaforma McAfee ePO integra funzionalità avanzate per incrementare l'efficienza del personale preposto alla sicurezza quando deve mitigare una minaccia o apportare una modifica per ripristinare la conformità. La risposta automatica di McAfee ePO attiva un'azione sulla base di un evento che si verifica. Le azioni possono essere delle semplici notifiche oppure una remediation approvata.

Esempi di utilizzo comuni per la risposta automatica

- Notifica agli amministratori nuove minacce, aggiornamenti non riusciti o errori con priorità elevata tramite email o SMS in base a soglie predeterminate
- Applicazione di policy basate sul client o sugli eventi di minaccia, come una policy per prevenire le comunicazioni esterne quando un host potrebbe essere stato compromesso (per negare quindi le attività di controllo e comando) oppure il blocco del trafugamento dei dati o dei trasferimenti verso l'esterno, finché l'amministratore non ha ripristinato la policy.
- Contrassegno dei sistemi ed esecuzione di attività aggiuntive per la remediation, come le scansioni della memoria su richiesta quando vengono rilevate delle minacce.
- Attivazione di eseguibili registrati affinché eseguano script esterni e comandi del server, come la generazione di un ticket del service desk o l'integrazione in altri processi aziendali
- Messa in quarantena automatica del carico di lavoro o del container (qualsiasi dispositivo) con policy più restrittive.

Gestione della sicurezza, basata sul cloud

Le aziende hanno bisogno di semplificare e accelerare la distribuzione delle soluzioni contro le minacce avanzate. Molti vedono l'efficienza di gestire la sicurezza nel cloud, eliminando il costo e la manutenzione di un'infrastruttura in sito. Il software McAfee ePO può essere impleentato da qualunque luogo e in qualsiasi momento tramite il cloud, con due opzioni di distribuzione alternative: software McAfee ePO su Amazon Web Services (AWS) oppure McAfee MVISION ePO. Entrambe le opzioni possono essere rese operative in meno di un'ora.

"McAfee ePO è uno dei progenitori dell'automazione e dell'orchestrazione integrata della sicurezza. ...gli odierni professionisti della sicurezza richiedono la classica potenza di ePO, ma fornita come un'esperienza semplificata, in modo da contribuire alla loro efficienza ed efficacia ... come spazio di lavoro distribuito in SaaS, MVISION riunisce analisi, gestione delle policy ed eventi in modo che il settore enterprise e il midmarket possano adattarvisi."

—Frank Dickinson, vice presidente della ricerca, prodotti di sicurezza, IDC

- Il software McAfee ePO su AWS consente alle aziende di sfruttare molti servizi nativi in AWS, come la scalabilità automatica e Amazon RDS, eliminando la necessità di acquistare e gestire un database separato. Ciò permette agli amministratori di concentrarsi sulle attività critiche per la sicurezza, non sull'infrastruttura. Il software McAfee ePO su AWS gestisce McAfee® Endpoint Security, McAfee® Data Loss Prevention, McAfee® Cloud Workload Security, Data Exchange Layer e le soluzioni di terze parti che sono integrate in McAfee ePO.
- McAfee® MVISION ePO si basa sui vantaggi di McAfee ePO come offerta Software-as-a-Service (SaaS). Questo semplifica drasticamente la gestione della piattaforma, consentendoti di eseguire le attività critiche per la sicurezza. Gli aggiornamenti della piattaforma sono trasparenti, con un modello di invio continuo. La protezione dei dispositivi viene distribuita automaticamente in tutta l'impresa dopo la distribuzione del tuo agent, eliminando le installazioni e gli aggiornamenti manuali per ciascun dispositivo e assicurando una protezione più solida contro le minacce. Ciò consente alle aziende di gestire McAfee MVISION Endpoint e Data Exchange Layer da una singola console, ovunque. McAfee MVISION ePO consente ai dispositivi di fornire approfondimenti essenziali per la gestione degli eventi e delle informazioni di sicurezza (SIEM), assicurando che i dati pertinenti siano a portata degli analisti per migliorare la ricerca delle minacce e la remediation.

Prodotti McAfee gestiti da McAfee ePO

Prodotti McAfee*
McAfee® Endpoint Protection (prevenzione delle minacce, firewall, controllo del web)
McAfee MVISION Endpoint che fa da complemento a Windows Defender con la protezione delle minacce avanzate
McAfee® MVISION Mobile
McAfee® Drive Encryption
McAfee® File and Removable Media Protection
McAfee® Active Response
McAfee® Management for Optimized Virtual Environments (McAfee MOVE)
McAfee Data Loss Prevention (McAfee DLP)
McAfee® Policy Auditor
McAfee® Enterprise Security Manager
McAfee® Threat Intelligence Exchange
McAfee® Application Control
McAfee® Cloud Workload Security
McAfee® Advanced Threat Defense
McAfee® Content Security Reporter
McAfee® Database Activity Monitoring
Data Exchange Layer (DXL)

**Per McAfee ePO in locale*

Distribuzioni flessibili

Distribuzione	Vantaggio principale
McAfee ePO in locale	Pieno controllo dei dati e delle funzionalità
McAfee ePO su AWS	Elimina la necessità di manutenzione dell'hardware di una soluzione in locale
McAfee MVISION ePO ePO Software-as-a-Service*	Offerta SaaS multitenant che rimuove tutta la manutenzione e gli upgrade dell'infrastruttura

**Non tutta la capacità ePO è disponibile in McAfee MVISION ePO*

"Il software McAfee ePO si contraddistingue rispetto ad altre soluzioni. Si tratta di una soluzione completa per la protezione dei nostri endpoint. Posso vedere tutto ciò che devo vedere per tutti i prodotti McAfee da un unico riquadro di visualizzazione. Le dashboard di facile utilizzo e le funzionalità integrate rendono tutto - visibilità, reporting, distribuzione, aggiornamento, manutenzione, processo decisionale - molto più semplice."

—Christopher Sacharok, Tecnico della sicurezza informatica, Computer Sciences Corporation

Esempi di utilizzo: come la console McAfee ePO permette la gestione centralizzata della protezione

Prodotto e tecnologia	Caso di utilizzo	Vantaggio
McAfee MVISION ePO McAfee MVISION Endpoint Microsoft Windows 10	Il software McAfee MVISION ePO gestisce McAfee MVISION Endpoint, che potenzia i controlli nativi in Microsoft Windows 10 con una protezione avanzata. Puoi facilmente scoprire e gestire le minacce avanzate grazie alla piattaforma di gestione comune e alle policy coerenti per Microsoft Windows e McAfee Endpoint Security.	Migliore protezione per i controlli nativi in Microsoft Windows e gestione collaudata più efficiente.
McAfee ePO McAfee Endpoint Security	McAfee Endpoint Security individua un file dannoso noto su un endpoint. La console McAfee ePO imposta una policy più rigorosa sull'endpoint per metterlo in quarantena. Il tutto viene eseguito attraverso un'interfaccia di gestione comune.	Rapido contenimento degli endpoint infetti
McAfee ePO McAfee Data Loss Prevention McAfee Enterprise Security Manager	McAfee Enterprise Security Manager rileva un'esfiltrazione significativa di dati su un endpoint e lo contrassegna all'interno della console McAfee ePO. La console McAfee ePO applica policy di protezione dalla perdita di dati per bloccare i dati e informare l'utente che non è conforme.	Applicazione automatica della policy per la perdita dei dati

Esempi di integrazione

Prodotto e tecnologia	Casi di utilizzo integrato	Vantaggio
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	McAfee Endpoint Security contrassegna un host sospetto. La console McAfee ePO può avviare delle scansioni aggiuntive. Il tutto viene comunicato a Cisco ISE tramite PxGrid e la tecnologia di scambio DXL (tramite la console McAfee ePO). Cisco ISE può isolare il sistema finché non viene giudicato accettabile.	Maggiore protezione proattiva
Rapid7 Nexpose McAfee ePO DXL	McAfee ePO condivide l'elenco delle risorse con Nexpose. Ciò consente di acquisire una comprensione dello stato di rischio dalla console di McAfee ePO e permette di impostare la policy di conseguenza. I dati della vulnerabilità vengono condivisi con la comunità di fornitori DXL.	▪ Complessità ridotta ▪ Un'unica dashboard offre una visione esaustiva e affidabile della condizione e assegna priorità alle azioni per ridurre al minimo i rischi
Check Point NGTX Check Point NGTP McAfee ePO DXL McAfee Active Response McAfee Enterprise Security Manager	Questa integrazione semplifica la condivisione di intelligence bi-direzionale e in tempo reale tra la rete e gli endpoint. Gli eventi vengono condivisi anche con la comunità DXL. Check Point Anti-Bot software blade blocca il traffico di comando e controllo (C&C) e avvisa il software McAfee ePO, oltre alle altre soluzioni di sicurezza di terze parti integrate, tramite argomenti DXL comuni. Con queste informazioni, McAfee avvia immediatamente il relativo flusso di lavoro della remediation per i dispositivi endpoint. Check Point e McAfee possono inoltre rilevare e prevenire gli attacchi zero-day e convertirli in attacchi noti, a prescindere dal fatto che provengano dalla rete o da un endpoint. Scambiando in tempo reale informazioni critiche per la missione aziendale, l'integrazione consente ai nostri rispettivi prodotti di rilevare, bloccare e neutralizzare le minacce in modo automatizzato.	▪ Riduzione del tempo necessario al rilevamento ▪ Blocco e remediation degli attacchi

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