McAfee ePolicy Orchestrator

Ottieni, visualizza, condividi e sfrutta le informazioni relative alla sicurezza da una postazione centralizzata

Per gestire la sicurezza bisogna faticosamente destreggiarsi tra strumenti e dati. Ciò da un vantaggio all'avversario, che dispone di maggior tempo per sfruttare la lacuna non rilevata tra gli strumenti e causare danni. Inoltre, la forza lavoro dedicata alla sicurezza informatica è limitata e deve essere potenziata per gestire la complessità della cybersecurity. La piattaforma di gestione McAfee® ePolicy Orchestrator® (McAfee ePO™) elimina l'attività dispendiosa in termini di tempo e con potenziale errore umano e stimola i responsabili a gestire la sicurezza in modo più rapido e con maggiore efficacia.

Sicurezza essenziale

Partiamo dalle basi. Fondamentale per qualsiasi architettura di sicurezza è la capacità di monitorare e controllare lo stato di endpoint e sistemi. Standard di settore come i controlli di sicurezza e privacy del Center for Internet Security **(CIS)** Controls and National Institute of Standards Technology **(NIST) SP 800-53** li definiscono un must. 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. La gestione e l'applicazione delle policy ta i prodotti di sicurezza per l'intera azienda vengono eseguite da un'unica console, eliminando la complessità legata alla gestione di più prodotti. Questa sicurezza essenziale è fondamentale per la conformità della sicurezza IT dell'azienda.

Comprovata gestione avanzata della sicurezza

Oltre 30.000 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 endpoint, rete e operazioni di sicurezza. Le grandi aziende si affidano all'architettura altamente scalabile della console McAfee ePO, che permette loro di gestire centinaia e migliaia di nodi da un'unica console. La console McAfee ePO offre a un amministratore della sicurezza aziendale l'opportunità di semplificare la manutenzione delle policy, acquisire intelligence sulle minacce di terze parti sfruttando Data Exchange Layer (DXL) e integrare le policy in modo bidirezionale con una serie di prodotti. Queste efficienze operative riducono il processo e il sovraccarico dato dalla condivisione dei dati, consentendo una risposta più rapida e precisa.

Seguici su

L'efficienza ha la meglio sull'espansione incontrollata

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. McAfee abbraccia questi requisiti con un approccio alla gestione della sicurezza sintetizzato nell'espressione "Together is power" che permette di consolidare l'espansione incontrollata di strumenti proteggendo al tempo stesso la mole di risorse, supportando l'intelligence delle minacce, gestendo i dati open source e integrando i prodotti di terze parti. McAfee fornisce funzioni di comando e controllo centralizzati per la conformità e la gestione per una serie di prodotti di sicurezza. È possibile muoversi rapidamente tra i prodotti per trovare i dati critici e agire in base alla policy necessaria. 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.

Un elenco d'esempio di prodotti gestiti da McAfee ePO

Prodotti McAfee	Prodotti di terze parti
McAfee Endpoint Protection (prevenzione delle minacce, firewall, controllo del web)	Guidance Software: enCase Enterprise
McAfee Drive Encryption	Avecto: Privilege Guard
McAfee File and Removable Media Protection	AccessData: AccesData Enterprise
McAfee Active Response	Autonomic Software: Power Manager, Patch Manager
McAfee Management for Optimized Virtual Environments (McAfee MOVE)	Xerox MFP
McAfee Data Loss Prevention (McAfee DLP)	DXL
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	

Esempi di caso d'utilizzo: come la console McAfee ePO crea una gestione centralizzata dei prodotti di sicurezza

Prodotto e tecnologia	Esempio di caso d'utilizzo: gestione centralizzata	Vantaggi
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 eseguito attraverso un'interfaccia di gestione comune.	Rapido contenimento di un endpoint dannoso
McAfee ePO McAfee DLP 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 policyxper la perdita dei dati

Esempi di integrazione

Prodotto e tecnologia	Casi di utilizzo integrato	Vantaggi
McAfee ePO McAfee Endpoint Security DXL Cisco Identity Service Engine (ISE) Cisco PxGrid	McAfee Endpoint Security contrassegna un host sospetto. La console McAfee ePO avvia scansioni aggiuntive. Il tutto viene comunicato a Cisco ISE tramite PxGrid e la tecnologia di scambio DXL (la console McAfee ePO). Cisco ISE può isolare il sistema finché non viene giudicato accettabile.	Maggiore protezione proattiva
Avecto Defendpoint McAfee ePO DXL McAfee Threat Intelligence Exchange	Distribuzione e gestione della soluzione per la gestione dei privilegi più avanzata del settore, Avecto Defendpoint, da McAfee ePO. Le modifiche alla configurazione di Avecto Defendpoint sono informate dai dati sulla reputazione delle applicazioni di McAfee Threat Intelligence Exchange.	Complessità ridotta Nessuna infrastruttura aggiuntiva, con riduzione del TCO Modifiche dell'accesso ai privilegi sulla base dell'intelligence delle minacce
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 sulle vulnerabilità vengono condivisi con la comunità di fornitori DXL.	Riduzione della complessità Ottieni una postura completa e affidabile e stabilisci le priorità delle azioni per ridurre al minimo i rischi da un'unica dashboard
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 con la comunità DXL.	Riduzione del tempo necessario al rilevamento Blocco e remediation degli attacchi

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 integrate	Aziende non integrate
Meno di 5 violazioni nello scorso anno	78%	55%
Minacce individuate in otto ore	80%	54%

2016 Penn Schoen Berland

Flussi di lavoro flessibili semplificano i processi

Il database McAfee ePO fornisce 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. È possibile definire come la console di McAfee ePO dovrebbe indirizzare avvisi e risposte di sicurezza in base al tipo e alla criticità degli eventi di sicurezza per l'ambiente, le policy e gli strumenti. 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. Utilizza la console McAfee ePO per attivare le azioni di remediation dai sistemi delle operazioni IT, come l'assegnazione di policy più severe. La possibilità di sfruttare le sue API (Application Programming Interface) web riduce lo sforzo manuale.

Casi di utilizzo comune

- 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 di McAfee ePO nei processi e nelle funzioni aziendali esistenti sfruttando il solido set di API per ottenere maggiori informazioni e accelerare i flussi di lavoro (per esempio, integrazione con sistemi di ticketing, applicazioni web o portali self-service).
- È possibile mantenere il livello di sicurezza distribuendo agent e soluzioni di sicurezza man mano che nuovi computer vengono aggiunti alla rete aziendale sincronizzando la console di McAfee ePO con Active Directory.

"La più potente piattaforma per la gestione degli endpoint oggi disponibile sul mercato, McAfee ePolicy Orchestrator, rappresenta lo strumento per la gestione primaria di tutti i prodotti di sicurezza dell'azienda e offre la potenza e la flessibilità che gli acquirenti aziendali desiderano. Le funzionalità di sicurezza sono ampie e strettamente integrate tramite un motore di policy comune e flusso di intelligence."

—Forrester Wave: Endpoint Security Suites (suite per la sicurezza degli endpoint), 2016

Rapidi processi di mitigazione e remediation

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 semplici notifiche o remediation approvate.

Casi di utilizzo comune 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 su eventi legati a client o minacce, come una policy per impedire comunicazioni esterne quando un host viene compromesso (questo negherebbe le attività di comando e controllo) o bloccare l'esportazione/trasferimento dei dati fino a quando l'amministratore non ha reimpostato la policy
- Etichettatura dei sistemi ed esecuzione di attività aggiuntive per la remediation, come le scansioni della memoria su richiesta quando vengono rilevate 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 dell'endpoint con policy più limitate

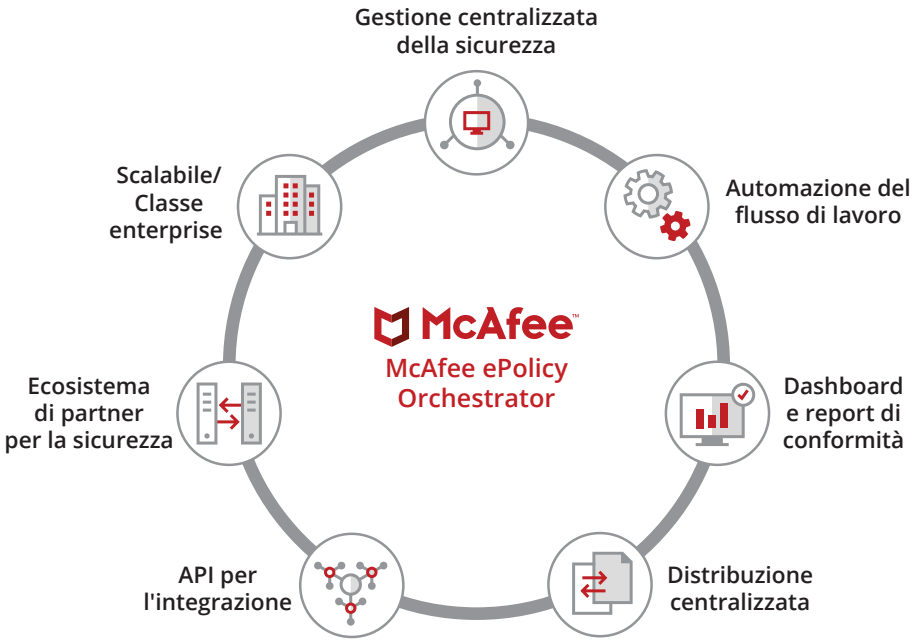

Figura 1. Gestione centralizzata della sicurezza utilizzando la console di McAfee ePO.

Protezione dell'azienda con la console McAfee ePO

Gestione centralizzata della sicurezza

- Un'unica caratteristica console per la gestione centralizzata e la visibilità su centinaia di migliaia di nodi in tutta l'azienda
- Una struttura aperta per un'ampia gestione della sicurezza dei sistemi protetti da McAfee e soluzioni di terze parti
- La piattaforma estensibile si integra con l'infrastruttura IT esistente sfruttandola per ridurre le problematiche operative

Tempi di risposta più rapidi in sicurezza

- Visualizzazioni complete e approfondimenti per indirizzare proattivamente le problematiche di sicurezza interne ed esterne
- Rapida distribuzione centralizzata di aggiornamenti e definizioni di sicurezza per garantire che gli endpoint siano protetti dalle minacce più recenti
- Tempi di risposta più rapidi tramite dashboard fruibili e funzionalità di query e reporting avanzate

Complessità ridotta e processi ottimizzati

- Capacità di attivarsi rapidamente tramite la configurazione guidata, flussi di lavoro di gestione delle policy automatizzati e dashboard predefinite
- Assegnazione di policy basata su tag per indirizzare in modo preciso l'applicazione di profili di sicurezza predefiniti a singoli o gruppi di sistemi sulla base dei ruoli aziendali o dello stato di rischio
- Funzionalità di catalogazione dei task e gestione automatizzata per ottimizzare i processi amministrativi e ridurre le spese operative
- Un singolo agent per gestire molteplici prodotti endpoint riduce il rischio di conflitti tra endpoint

Scalabilità per implementazioni enterprise

- Architettura di classe enterprise per supportare la gestione di centinaia di migliaia di dispositivi con un unico server
- Supportato e collaudato all'interno di ambienti IT eterogenei complessi
- Reportistica aziendale che aggrega una visione completa dello stato della sicurezza e della conformità

"Il software McAfee ePO si contraddistingue rispetto ad altre soluzioni. È un punto di accesso centralizzato per la nostra protezione degli 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, Information Security Engineer, Computer Sciences Corporation

McAfee Together is power.

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

McAfee, il logo McAfee, ePolicy Orchestrator e McAfee ePO sono marchi registrati o marchi di McAfee, LLC o sue filiali negli Stati Uniti e in altri Paesi. Altri marchi e denominazioni potrebbero essere rivendicati come proprietà di terzi. Copyright © 2017 McAfee, LLC. 3718_0118
GENNAIO 2018