SCHEDA TECNICA

McAfee Management for Optimized Virtual Environments AntiVirus

Sicurezza per il cloud privato senza sacrificare le prestazioni

Gli antivirus tradizionali non vanno molto d'accordo con le infrastrutture virtualizzate. McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) offre una protezione avanzata e ottimizzata contro il malware per desktop e server virtualizzati. Può essere implementato su molteplici hypervisor oppure si può scegliere un'opzione senza agent, ottimizzata per VMware NSX o VMware vCNS. In entrambi i casi, si ottiene la massima sicurezza per il rilevamento e il contenimento immediato delle minacce con un impatto minimo sulle prestazioni del computer virtuale (VM). McAfee MOVE AntiVirus ottimizza la protezione antimalware per le distribuzioni virtualizzate liberando risorse dall'hypervisor, mentre assicura che le scansioni di sicurezza aggiornate siano eseguite secondo le policy.

Controllo ottimizzato delle scansioni

La natura dinamica dei computer desktop ospiti e dei server virtuali richiede un'attenzione particolare. Le immagini devono essere libere da malware quando gli utenti avviano una sessione. Questo può essere difficile, dal momento che gli utenti spesso iniziano a lavorare in gruppo, causando nei momenti di punta delle vere e proprie "tempeste antivirus" che consumano le risorse e impediscono agli utenti di ottenere una sessione.

Per eliminare ritardi e colli di bottiglia delle scansioni, McAfee MOVE Antivirus sposta il carico costituito da scansioni, configurazioni e operazioni di aggiornamento dei file .DAT, dalle singole immagini ospiti a un server di scansione offload. Creiamo e manteniamo una cache globale dei file esaminati per assicurare che, quando un file viene sottoposto a scansione risultando pulito, le VM che vi accedono successivamente non debbano attendere un'altra scansione. L'allocazione delle risorse di memoria per ogni VM diminuisce e può essere rimessa a disposizione dell'insieme delle risorse per un utilizzo più efficiente.

McAfee MOVE AntiVirus permette a policy separate per la scansione all'accesso e on demand di abilitare l'esecuzione di sicurezza ottimizzata. Per esempio, gli amministratori possono presupporre un ragionevole livello di rischio per le scansioni all'accesso in tempo

Vantaggi principali

- **Scansione offload del malware:** protezione istantanea con basso impatto su memoria ed elaborazione.
- **Evita che si scateni una tempesta antivirus:** le opzioni includono scansioni in accesso e on demand.
- **Permette un'implementazione flessibile:** multi-piattaforma (tutti i principali hypervisor, VM Windows) o senza agent (VM VMware, Windows e Linux).
- **Migliora l'ottimizzazione delle risorse:** provisioning flessibile degli scanner offline con notifica degli eventi (multi-piattaforma).
- **Blocca le minacce zero-day sconosciute in pochi secondi:** intelligence sulla reputazione locale combinata con le analisi comportamentali all'interno di una sandbox (multi-piattaforma, modulo aggiuntivo venduto separatamente).
- **Sfrutta la console McAfee® ePolicy Orchestrator® (McAfee ePO™):** visibilità e controllo end-to-end per distribuzioni fisiche, virtuali e nel cloud.

reale al fine di evitare che le prestazioni vengano compromesse e quindi utilizzare la scansione su richiesta con policy più severe in esecuzione in un momento successivo quando l'impatto è minore.

Visibilità end-to-end completa per tutti i cloud

Una scarsa visibilità complica l'implementazione di policy di sicurezza corrette per gli ambienti virtualizzati. McAfee Cloud Workload Discovery per cloud privati, che copre VMware e OpenStack, fornisce una visione completa di tutti i data center virtuali e inserisce le proprietà principali come server, hypervisor e VM all'interno della console McAfee ePO. Una volta che gli amministratori ottengono visibilità sullo stato di sicurezza di tutte le VM e possono monitorare le relazioni tra hypervisor e VM quasi in tempo reale, la protezione del centro dati virtuali risulta notevolmente semplificata. Una dashboard personalizzabile mostra lo stato delle scansioni di sicurezza, visioni d'insieme di sintesi e dati cronologici della sicurezza relativi alle risorse.

McAfee Server Security Suite Essentials e McAfee Server Security Suite Advanced estendono la visibilità e il controllo per i cloud pubblici e i server fisici Amazon Web Services (AWS) e Microsoft Azure.

Gestione dettagliata delle policy

La familiare console di McAfee ePO permette di configurare le policy e i controlli di McAfee MOVE AntiVirus. È possibile eseguire il rollup dei dati virtuali con i dati dei sistemi fisici e dei cloud pubblici per fornire dashboard e report unificati. Gli amministratori possono configurare una policy unica per computer VM, cluster o centro dati tramite McAfee Cloud Workload Discovery, adattando la sicurezza in modo specifico alla conformazione del centro dati.

Funzioni aggiuntive McAfee MOVE AntiVirus

Gestione e visibilità:

- Pianifica istantaneamente una scansione su richiesta su un computer VM o un gruppo di computer VM.
- Migliora la precisione del processo di scansione con scansioni on demand mirate.
- Distribuisci automaticamente uno scanner offload su ogni hypervisor attraverso l'integrazione con VMware NSX Service Composer.
- Rimani aggiornato sulle problematiche con dashboard, report e avvisi via email.

Distribuzione e configurazione semplificate:

- Distribuisci e configura uno scanner offload su molteplici hypervisor (senza agent).
- Ripristina file in quarantena utilizzando la console McAfee ePO (multi-piattaforma).
- Diagnostica dettagliata per l'ottimizzazione delle prestazioni dell'antivirus.
- Gestione omogenea delle policy senza agent e multi-piattaforma.

Opzione senza agent per ambienti VMware

McAfee MOVE AntiVirus sfrutta VMware NSX o VMware vCNS per una migliore efficienza. Nelle distribuzioni

Configurazioni di McAfee MOVE AntiVirus

McAfee MOVE AntiVirus for Virtual Servers

- McAfee MOVE AntiVirus:
  - Distribuzione multi-piattaforma
  - Distribuzione senza agent
- Cloud Workload Discovery per cloud privati (VMware e OpenStack)
- Software McAfee ePO

McAfee MOVE AntiVirus for Virtual Desktops

- McAfee MOVE AntiVirus:
  - Distribuzione multi-piattaforma
  - Distribuzione senza agent
- Cloud Workload Discovery per cloud privato, per VMware e OpenStack
- McAfee Host Intrusion Prevention System
- McAfee SiteAdvisor® Enterprise
- Protezione della memoria e delle applicazioni web
- Software McAfee ePO

senza agent, questi usano l'hypervisor come una connessione ad alta velocità per consentire a McAfee MOVE AntiVirus Security Virtual Machine (SVM) di esaminare i computer virtuali dall'esterno dell'immagine ospite. Mentre esegue la scansione, il computer SVM ordina a VMware NSX o VMware vCNS di memorizzare nella cache i file autorizzati e di cancellare, negare l'accesso oppure mettere in quarantena i file dannosi.

Una volta installati e configurati i computer SVM e i componenti VMware NSX o VMware vCNS sui server VMware ESX, oltre ad installare il drive endpoint di VMware NSX o VMware vCNS sui computer virtuali ospiti, ogni immagine viene automaticamente protetta senza installare il software McAfee su ogni computer virtuale client. La nostra implementazione, che tiene conto di vMotion, implica il fatto che i computer virtuali dell'azienda possono essere spostati da un host all'altro ed essere protetti da SVM sull'host di destinazione, senza alcun impatto sulle scansioni o sull'esperienza dell'utente.

L'integrazione dei prodotti McAfee con VMware vCNS consente di monitorare lo stato del computer SVM all'interno di VMware vCenter e di essere avvisato se il computer SVM perde la connettività. Nel caso una VM venga infettata, la console McAfee ePO riceve i dati di questo evento con i dettagli della specifica VM coinvolta. La profonda integrazione con VMware NSX sincronizza le policy create nella console McAfee ePO e le regole assegnate in VMware NSX. Contrassegnando i computer vulnerabili che non dispongono di una protezione contro il malware o i computer infettati da malware è possibile avviare l'immediata quarantena dei computer virtuali attraverso il firewall VMware NSX.

La distribuzione di McAfee MOVE Antivirus senza agent con VMware vCNS e VMware NSX avviene simultaneamente, rendendo estremamente semplice e omogenea la transizione a VMware NSX per i clienti di VMware vCNS.

Multi-piattaforma per tutti i principali hypervisor

Nelle installazioni multi-piattaforma, tra cui vSphere, Hyper-V, KVM e XenServer, l'agent McAfee MOVE AntiVirus - un componente endpoint leggero - comunica al computer SVM di gestire i processi antivirus per conto di ogni VM. L'agent di McAfee MOVE AntiVirus mantiene una cache locale e gestisce le policy e le funzioni di scansione. Puoi selezionare e sottoporre a scansione un'immagine che userai come master pulito. Il pre-popolamento della cache locale con immagini pulite velocizza al massimo il tempo di avvio del computer virtuale.

Quando un utente accede a un file, McAfee MOVE Offload Scan Server esegue una scansione all'accesso, inviando una risposta alla VM. Gli utenti vengono avvisati di eventuali problemi tramite una segnalazione pop-up e possono quindi cancellare, negare l'accesso o mettere in quarantena i file pericolosi.

Poiché le richieste di scansione variano all'interno delle implementazioni multi-piattaforma, è possibile aggiungere o rimuovere automaticamente SVM dal gruppo di risorse per ridimensionare o incrementare la potenza, per una scalabilità illimitata e un utilizzo efficiente delle risorse. Le segnalazioni di eventi aiutano agli amministratori a comprendere i trend di utilizzo degli SVM per ottimizzare la gestione delle risorse.

Nelle distribuzioni multi-piattaforma, McAfee MOVE AntiVirus può migliorare le informazioni globali sulla reputazione provenienti da McAfee Global Threat Intelligence (McAfee GTI) con i dati locali di McAfee Threat Intelligence Exchange, un modulo aggiuntivo venduto separatamente, per identificare immediatamente e combattere il sempre crescente numero di elementi di malware unici. Utilizzando McAfee Threat Intelligence Exchange, McAfee MOVE AntiVirus si coordina con McAfee Advanced Threat Defense per analizzare dinamicamente il comportamento di applicazioni sconosciute in una sandbox e immunizzare automaticamente tutti gli endpoint dal malware appena rilevato. L'integrazione di McAfee MOVE AntiVirus con McAfee Network Security Platform attraverso McAfee Threat Intelligence Exchange fornisce un approccio multi-livello alla sicurezza per una protezione unificata perimetrale e dei computer virtuali.

Gestione unificata delle policy per distribuzioni senza agent e multi-piattaforma

Molte aziende potrebbero voler sfruttare la capacità di McAfee MOVE AntiVirus di supportare distribuzioni sia senza agent che multi-piattaforma. McAfee MOVE AntiVirus offre agli amministratori della sicurezza la capacità di definire e gestire policy di sicurezza coerenti utilizzando un punto di estensione nella console McAfee ePO in modo che la gestione di tali diversi metodi sia semplice e omogenea.

Per saperne di più

Le soluzioni McAfee ti armano di tutta la protezione di cui necessiti, con la flessibilità che meriti.

Maggiori informazioni sono disponibili all'indirizzo **www.mcafee.com/it/products/move-anti-virus.aspx**.

Architettura	Distribuzione multi-piattaforma	Distribuzione senza agent
Supporto hypervisor/piattaforma	Tutti i principali hypervisor, inclusi VMware, Citrix, Hyper-V e KVM.	VMware
Piattaforma di scansione	Windows 2008, Windows 2012 R2, Windows Server 2016	Linux Ubuntu 16.04
Scalabilità della distribuzione	Un SVM protegge i computer virtuali da molteplici hypervisor. È possibile effettuare il provisioning dei computer SVM in modo flessibile.	Un computer SVM per host ESX.
Comunicazioni con le VM	Sulla rete	Sull'hypervisor
Protezione dei computer virtuali	Windows	Windows e Linux

McAfee
Together is power.

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