SCHEDA TECNICA

McAfee Security Suite for Virtual Desktop Infrastructure

La sicurezza di cui hai bisogno con un impatto minimo sulle prestazioni

L'adozione di desktop virtuali è già una realtà, ma è necessario incorporare nella soluzione una sicurezza efficace per i desktop in modo da proteggere l'azienda senza problemi di prestazioni o legati alla densità server desiderata. Gli antivirus tradizionali non funzionano molto bene all'interno di un'infrastruttura virtualizzata. La risposta? McAfee® Security Suite for Virtual Desktop Infrastructure (VDI), che offre protezione completa ottimizzata per i desktop virtuali.

McAfee Security Suite for VDI fornisce protezione antimalware ottimizzata per la virtualizzazione, whitelisting per proteggere dalla minacce zero-day, protezione dalle intrusioni desktop e protezione dei dati. Inoltre, segnala agli utenti i siti web pericolosi e/o li blocca.

Architettura di scansione ottimizzata

La natura dinamica dei computer desktop richiede un'attenzione particolare. Le immagini devono essere mantenute libere dal malware quando sono offline e sottoposte a scansione senza indugi quando gli utenti avviano una sessione. Tuttavia l'antimalware non è l'unico servizio ad avviarsi e, dato che spesso gli utenti lavorano in gruppi, nei momenti di punta si creano delle vere e proprie "tempeste antivirus" che consumano tutte le risorse e impediscono agli utenti di ottenere una sessione.

Per eliminare ritardi e colli di bottiglia delle scansioni, McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) sposta il carico costituito da scansioni, configurazioni e operazioni di aggiornamento dei file .DAT, dalle singole immagini ospiti a un'appliance virtuale rafforzata/server di analisi offload. Costruisce e mantiene una cache globale dei file esaminati per assicurare che, quando un file viene sottoposto a scansione risultando pulito, i computer virtuali (VM) che vi accedono successivamente non debbano attendere un'altra scansione. L'allocazione delle risorse di memoria per ogni VM diminuisce e può essere restituita all'insieme delle risorse per un utilizzo più efficiente. La pianificazione intelligente delle scansioni su richiesta fa in modo che le scansioni non interferiscano con le prestazioni dell'hypervisor.

Gestione dettagliata delle policy

La console di McAfee® ePolicy Orchestrator® (McAfee ePO™) permette di configurare le policy e i controlli di McAfee MOVE AntiVirus. I dati dei computer desktop virtuali possono essere aggregati con i dati provenienti da altri sistemi, tramite dashboard e report unificati.

Vantaggi principali

- Offre funzionalità di discovery e visibilità con il software McAfee ePO e Cloud Workload Discovery.
- Fornisce una combinazione unica di blacklisting e whitelisting per proteggere i desktop virtuali dal malware.
- Ottimizza la protezione della virtualizzazione per un impatto minimo sulle prestazioni.
- Aggiunge la protezione del web e contro le intrusioni con protezione della memoria e delle applicazioni web.
- Sfrutta il software McAfee ePO per ottenere una visibilità a colpo d'occhio, controllo e reportistica degli endpoint.
- Permette la distribuzione flessibile agentless e multi-piattaforma.
- Supporta il provisioning flessibile di scanner offline per scalare su richiesta (multi-piattaforma).
- Si integra con le informazioni locali sulla reputazione per una risposta alle minacce più rapida (multi-piattaforma).

Gli amministratori possono configurare una policy unica per computer VM, gruppo di risorse, cluster o centro dati tramite Cloud Workload Discovery per cloud privati, adattando le loro esigenze di sicurezza in modo specifico alla conformazione del centro dati.

Distribuzione senza agent per Vmware

McAfee MOVE AntiVirus sfrutta VMware NSX o VMware vCNS per una migliore efficienza. Nelle distribuzioni agentless, questi usano l'hypervisor come una connessione ad alta velocità per consentire al computer virtuale di sicurezza (SVM) McAfee MOVE AntiVirus 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 componenti VMware SVM e 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 nostro software 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 di McAfee MOVE AntiVirus consente di monitorare lo stato di SVM all'interno di VMware vCenter e di essere avvisato se il computer SVM perde la connettività. Nel caso una VM venga infettata, il software McAfee ePO riceve i dati di questo evento con i dettagli della specifica VM coinvolta. La profonda integrazione con NSX sincronizza le policy create nel software 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 permette l'immediata quarantena dei computer virtuali attraverso il firewall VMware NSX.

Multi-piattaforma per tutti gli hypervisor

Nelle installazioni multi-piattaforma l'agent McAfee MOVE AntiVirus - un componente endpoint leggero - comunica a McAfee MOVE Offload Scan Server di gestire i processi antivirus per conto di ogni computer desktop virtuale. Un agent software McAfee ePO gestisce le policy e le scansioni. Inoltre, è possibile selezionare e sottoporre a scansione un'immagine che userai come master pulito. Quindi, un amministratore può pre-popolare le cache globali con immagini pulite per aiutare a fornire tempi di avvio più rapidi per i desktop virtuali.

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 un allarme a comparsa e i file possono essere spostati in quarantena in attesa di una decisione in merito. Ogni computer virtuale è configurabile con specifiche policy univoche, che possono essere impostate nella console McAfee ePO, oppure si possono gestire i desktop virtuali come gruppo.

Configurazione di McAfee Security Suite for VDI

- McAfee MOVE AntiVirus
  - Distribuzione multipiattaforma
  - Distribuzione agentless
- Cloud Workload Discovery per cloud privati (VMware e OpenStack)
- McAfee VirusScan® Enterprise for Windows
- McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention for Desktops
- McAfee Application Control for Desktops
- Tecnologia McAfee SiteAdvisor® Enterprise
- McAfee ePolicy Orchestrator

Poiché i carichi di lavoro vengono aumentati o ridotti nelle implementazioni multi-piattaforma, è possibile aggiungere o rimuovere automaticamente SVM dal gruppo di risorse per ridimensionare o incrementare la potenza, con 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.

McAfee MOVE AntiVirus nelle distribuzioni multi-piattaforma può migliorare le informazioni globali sulla reputazione di McAfee Global Threat Intelligence 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. Inoltre, immunizza tutti i desktop virtuali da malware appena rilevato.

Funzione	A che cosa serve
Protezione della virtualizzazione	▪ Migliora la sicurezza dei carichi di lavoro distribuiti sulle infrastrutture desktop virtuali senza compromettere le prestazioni e l'utilizzo delle risorse. ▪ La distribuzione agentless ottimizzata per VMware aiuta a fornire ottime prestazioni e densità VM. Nessuna necessità di installare/aggiornare i nostri agent su ogni desktop virtuale: in questo modo si riduce la complessità e viene notevolmente migliorata la fruibilità. ▪ La distribuzione multi-piattaforma per tutti gli hypervisor supporta il provisioning flessibile degli scanner offline per scalare su richiesta e si integra con le informazioni locali sulla reputazione per una risposta più rapida alle minacce.
Protezione fondamentale degli endpoint	▪ La protezione antivirus di McAfee effettua scansioni più rapide, utilizza meno memoria e richiede meno cicli della CPU proteggendo meglio rispetto ad altri prodotti. ▪ La prevenzione delle intrusioni su host protegge le aziende dalle minacce di sicurezza complesse che potrebbero altrimenti essere involontariamente introdotte o autorizzate. ▪ McAfee SiteAdvisor® Enterprise impedisce agli utenti di interagire con siti web pericolosi e permette la personalizzazione delle policy per limitare l'accesso a siti web potenzialmente dannosi, assicurando così la conformità con le policy.
Whitelisting delle applicazioni	▪ Riduce in modo significativo l'impatto sulle prestazioni dell'host rispetto ai tradizionali controlli di sicurezza degli endpoint. ▪ Protegge contro minacce persistenti avanzate e zero-day (APT) senza aggiornamenti delle firme, per una protezione più rapida. ▪ Il whitelisting dinamico richiede un impiego di risorse operativo minore rispetto alle tecniche di whitelisting legacy.

SCHEDA TECNICA

Funzione	A che cosa serve
Cloud Workload Discovery	▪ Fornisce piena visibilità dei carichi di lavoro su cloud privato e le piattaforme alla base per identificare i controlli di sicurezza non efficaci
Protezione di file e dispositivi rimovibili (crittografia)	▪ La crittografia è semplicissima e meno pericolosa da distribuire grazie alla protezione di file e media rimovibili. ▪ Prestazioni native sugli host crittografati tramite l'implementazione ottimizzata della tecnologia Intel® AES-NI. ▪ Offre crittografia di file e cartelle in modo automatico, trasparente e basato su policy e crittografia di media rimovibili (drive USB, CD, DVD). ▪ Permette agli utenti di crittografare i media USB rimovibili e di trasferire le informazioni in modo sicuro. ▪ Permette di accedere in modo sicuro ai dati presenti in cartelle di rete condivise.
Gestione centralizzata tramite il software McAfee ePO	▪ Gestione centralizzata di distribuzioni fisiche, virtuali e in cloud per un miglior controllo della sicurezza, tra cui gestione delle policy, distribuzione, visibilità e gestione della sicurezza su tutte le piattaforme. ▪ Semplifica i processi operativi e richiede minor tempo allo staff amministrativo. ▪ Riduce i costi per l'hardware grazie al minor ingombro dei server.

Per saperne di più

Le soluzioni McAfee ti armano di tutta la protezione di cui necessiti, con un impatto minimo sulle prestazioni. Visita il sito **www.mcafee.com/it/products/data-center-security-suite-for-vdi.aspx**.

McAfee
Together is power.

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