McAfee Security Suite for Virtual Desktop Infrastructure

La sicurezza di cui hai bisogno, la flessibilità che meriti

L'adozione di desktop virtuali (VDI) 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 VDI, che offre protezione completa ottimizzata per i desktop virtuali.

Vantaggi principali

- Rilevamento e visibilità per gli ambienti VMware vSphere con il software McAfee ePO e McAfee Data Center Connector for VMware vSphere. L'esclusiva combinazione di blacklist e whitelist protegge dal malware i server fisici e virtuali.
- Protezione ottimizzata della virtualizzazione per un impatto minimo sulle prestazioni.
- Protegge da minacce sconosciute bloccando l'esecuzione di applicazioni indesiderate sui desktop virtuali.
- Aggiunge la protezione del web e contro le intrusioni con protezione firewall desktop, della memoria e delle applicazioni web.
- Sfrutta il software McAfee ePO per ottenere una visibilità a colpo d'occhio, controllo e reportistica degli endpoint.

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 evita che possano accedervi.

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 (MOVE) AntiVirus sposta il carico costituito da scansioni, configurazioni e operazioni di aggiornamento dei file. DAT, dalle singole immagini ospiti a una appliance virtuale rafforzata/offload scan server.

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 del software McAfee® ePolicy Orchestrator® (McAfee ePO™) permette di configurare le policy e i controlli del comportamento 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. Gli amministratori possono configurare una policy unica per computer VM, gruppo di risorse, cluster o centro dati tramite McAfee Data Center Connector, adattando le loro esigenze di sicurezza in modo specifico alla conformazione del centro dati.

intel Security

Configurazione di McAfee Security Suite for VDI

McAfee MOVE Anti-Virus for Virtual Desktops (VDI)

- McAfee MOVE AntiVirus
  - Distribuzione con molteplici hypervisor
  - Distribuzione agentless
- McAfee Data Center Connector for vSphere
- Software McAfee VirusScan® Enterprise for Windows
- Software McAfee VirusScan Enterprise for Linux
- McAfee Host Intrusion Prevention System
- McAfee Application Control for Desktops
- Tecnologia McAfee SiteAdvisor® Enterprise
- Software McAfee ePolicy Orchestrator

La distribuzione agentless sfrutta VMware vShield per garantire efficienza

Nelle distribuzioni agentless, VMware vShield Endpoint usa l'hypervisor come una connessione ad alta velocità per consentire McAfee MOVE AntiVirus Security Virtual Appliance di esaminare i computer virtuali dall'esterno dell'immagine ospite. Mentre esegue la scansione, la SVA ordina a vShield di memorizzare nella cache i file autorizzati e di cancellare, negare l'accesso oppure mettere in quarantena i file dannosi.

Dopo l'installazione e la configurazione della SVA e dei necessari componenti di vShield sui server ESX, insieme all'installazione del driver di vShield sulle VM ospiti, ogni immagine viene automaticamente protetta nel momento in cui viene creata. Non è necessario installare il software McAfee su ogni client VM. La nostra implementazione, che tiene conto di vMotion, implica il fatto che tutti i computer virtuali dell'azienda possono essere spostati da un host all'altro ed essere protetti da SVA sull'host di destinazione, senza alcun impatto sulle scansioni o sull'esperienza dell'utente. L'integrazione McAfee consente di monitorare lo stato di SVA all'interno di vCenter e di essere avvisato se SVA 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.

Molteplici hypervisor per standard e comodità

Nelle installazioni con molteplici hypervisor l'agent McAfee MOVE AntiVirus - un componente endpoint leggero - comunica a 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 funzioni di scansione. 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, impostabili nella console software McAfee ePO, oppure si possono gestire le VM come gruppo.

Per saperne di più

Le soluzioni McAfee ti mettono a disposizione tutta la protezione di cui necessiti, con la flessibilità che meriti. Visita il sito **www.mcafee.com/it/products/data-center-security-suite-for-vdi.aspx**.

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. • Possibilità di distribuzioni agentless e con molteplici hypervisor: distribuzione per ambienti di virtualizzazione di diversi fornitori (VMware, Citrix, Hyper-V). • La distribuzione agentless ottimizzata per VMware aiuta a fornire ottime prestazioni e densità VM. Nessuna necessità di installare/aggiornare gli agent McAfee su ogni desktop virtuale: in questo modo si riduce la complessità e viene notevolmente migliorata la fruibilità.
Protezione fondamentale degli endpoint	• Protezione antivirus per i server fisici classificata al primo posto da NSS Labs contro gli exploit zero-day e gli attacchi evasivi. • 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.
Piena visibilità dei computer virtuali nel cloud privato	• Rileva automaticamente i computer virtuali nel cloud privato (VMware vSphere).
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 da un singolo pannello di computer fisici e virtuali, compresi quelli che si trovano nei cloud privati e pubblici, per una maggior visibilità sulla sicurezza. • Semplifica i processi operativi e richiede minor tempo allo staff amministrativo. • Riduce i costi per l'hardware grazie al minor ingombro dei server.

McAfee. Part of Intel Security.
Via Fantoli 7
20138 Milano
Italia
(+39) 02 554171
www.intelsecurity.com