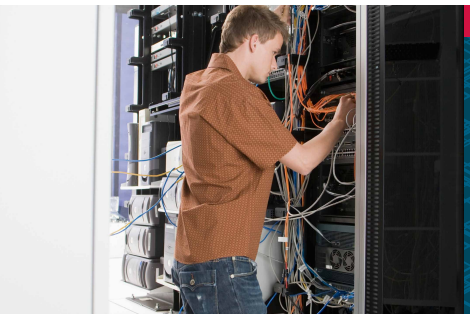

Amplia la virtualizzazione, mantieni la sicurezza

Decisioni di sicurezza importanti per le infrastrutture virtualizzate

La virtualizzazione diventa sempre più importante per i server e i desktop delle aziende; per questo i team IT devono essere in grado di supportare un numero sempre maggiore di utenti finali, maggiori carichi di lavoro, una diversificazione delle aree geografiche e allo stesso tempo essere pronti ai nuovi requisiti quali il provisioning "just in time" e il self service. McAfee® Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus) adatta i sistemi di sicurezza agli speciali requisiti tecnici e di gestione tipici della virtualizzazione. Consente di raggiungere in modo sicuro l'efficienza della virtualizzazione e allo stesso tempo di assicurare un'esperienza utente positiva.

Le tecnologie di virtualizzazione sono una delle principali priorità delle agende dei CIO nel 2012[1]. Tramite la scelta di strategie chiave quali il cloud computing, il principio bring-your-own-device e il consolidamento di server e centri dati, la virtualizzazione consente di raggiungere i due obiettivi di risparmio aziendale e flessibilità organizzativa. La virtualizzazione è fondamentale per raggiungere il successo. Tuttavia la virtualizzazione presenta delle sfide in termini operativi e di gestione del rischio distinte da quelle poste dalle tradizionali installazioni di sicurezza fisiche. La nuova modalità operativa della virtualizzazione richiede una nuova valutazione dei processi operativi, delle policy e delle decisioni di distribuzione rispetto ai sistemi di sicurezza tradizionali.

Colli di bottiglia delle prestazioni

Il problema più immediato riguarda le prestazioni di scansione. In una distribuzione tradizionale, ogni sistema, desktop o server, esegue le soluzioni anti-malware in locale ed effettua una scansione all'accesso oppure in base a una pianificazione per garantire che l'host non venga infettato. Questo modello basato sui singoli nodi è troppo esigente in termini di risorse per gli ambienti virtuali. Nel caso di eventi chiamati "scan storms", le operazioni di scansione possono arrivare a consumare tutte le risorse di elaborazione e memoria disponibili dell'hypervisor e impedire agli utenti di aprire nuove sessioni. In passato, molti amministratori decidevano di disattivare la scansione o ignorare gli aggiornamenti software pur di mantenere le prestazioni.

Tuttavia, gli ambienti virtualizzati sono diventati la piattaforma aziendale di maggior successo e per questo rappresentano la nuova frontiera per i criminali informatici che sfruttano le vulnerabilità di configurazione e di software. Senza una scansione della sicurezza corrente e attiva, le infrastrutture virtualizzate sono un terreno fertile per gli aggressori e i ladri di dati.

Software di sicurezza obsoleti

Il primo obiettivo di un criminale è un'immagine in esecuzione senza una soluzione anti-malware oppure con una soluzione non aggiornata. È necessario aggiornare il software di sicurezza sulle immagini in esecuzione, su quelle offline e sui modelli di immagine (o immagini gold). L'unica arma per difendersi efficacemente dagli aggressori consiste nell'aggiornare costantemente le funzioni di sicurezza dei sistemi e i contenuti anti-malware.

Quando si espande un'infrastruttura desktop virtualizzata (VDI), si può arrivare a supportare migliaia di macchine virtuali (VM) che vengono fornite e dismesse ogni giorno; in questo contesto la manutenzione della sicurezza è meno prevedibile. Sebbene sia possibile impostare i server fisici in continua esecuzione in modo da effettuare gli aggiornamenti di sicurezza in orari di poco traffico, per gli utenti desktop gli aggiornamenti di sicurezza devono basarsi sui flussi di lavoro dinamici delle VM. Anche qualora sia possibile archiviare offline e rendere inattive le immagini live durante la notte o per alcune ore, gli utenti si aspettano di poter accedere istantaneamente ai loro sistemi virtualizzati, senza ritardi nell'avvio dovuto a operazioni di scansione.

Una combinazione di risorse

I centri dati aggiungono un ulteriore livello di complessità al processo. La combinazione di risorse server, di storage e di rete consente il massimo utilizzo; questa unione, tuttavia, ha due implicazioni. Per prima cosa, in termini di sicurezza, si perdono i vantaggi dati dalla separazione fisica dei database, dei server applicazioni, dei server web e degli altri software. L'isolamento delle strutture fisiche rendeva dura la vita di autori di malware e hacker che desideravano espandersi. Per compensare questa maggior debolezza dei sistemi virtualizzati, è necessario pensare a sistemi di sicurezza più robusti.

L'altra implicazione è legata alla necessità di cambiare i processi di gestione; infatti mentre in precedenza le funzioni di server, storage e rete erano distinte, con la virtualizzazione, queste tre funzioni vengono gestite con un'unica console di gestione. Mentre prima, per queste risorse, esistevano amministratori e policy distinte, ora devono coesistere in un unico ambiente procedurale e con policy unitarie, spesso gestite da un solo amministratore della virtualizzazione, un vero "super utente". In questo contesto, i processi e gli avvisi devono competere per acquisire la visibilità a livello di gestione e le policy potrebbero richiedere un'opera di normalizzazione. Gli amministratori devono trovare dei modi per collaborare in modo operativo.

"Grazie a McAfee MOVE AntiVirus (AV), McKesson gode di una protezione completa e coerente degli ambienti virtuali contro il codice nocivo. In un contesto di adozione continua di nuove tecnologie legate in particolar modo al cloud computing, l'implementazione di McAfee MOVE [AntiVirus] AV ci consente di proteggere ulteriormente il nostro ambiente virtuale. La soluzione semplifica le operazioni di dimensionamento e distribuzione e garantisce lo stesso livello di protezione per tutti i sistemi."

Patrick Enyart
Senior Director
McKesson Information Security

Varietà di fornitori

Per questi cambiamenti, in molte organizzazioni vi è un'ulteriore complessità legata alla varietà dei fornitori. I diversi fornitori di soluzioni per la virtualizzazione hanno punti di forza diversi e molte aziende desiderano utilizzare più fonti per i software fondamentali. Il risultato è che la distribuzione potrebbe includere diversi hypervisor. Per questo è necessario, da un lato, proteggere le immagini e realizzare dei rapporti sulla conformità e, dall'altro, adeguarsi alle diverse specificità delle singole offerte.

Conformità

A tutti questi problemi se ne affiancano altri, legati alla conformità. È necessario dimostrare che i sistemi virtualizzati soddisfano i requisiti di conformità precedentemente (e spesso correntemente) imposti ai sistemi fisici. Le normative odierne prevedono una manutenzione regolare delle soluzioni anti-malware. Ad esempio la legge sulla privacy del Massachusetts (201 CMR 17:00) richiede "Versioni ragionevolmente aggiornate del software agent per la sicurezza dei sistemi; questi devono includere una protezione contro il malware e patch e definizioni virus ragionevolmente aggiornate oppure una versione di tale software per la quale sia ancora disponibile l'aggiornamento tramite patch e definizioni virus aggiornate; è altresì richiesto che il software in questione sia impostato in modo da ricevere i più recenti aggiornamenti della sicurezza su base regolare."

Nel contesto di un paesaggio delle minacce dinamico, tutti questi problemi diventano delle preoccupazioni pratiche nelle operazioni di sicurezza giornaliere dei sistemi virtualizzati. I modelli di sicurezza tradizionali del mondo fisico devono essere estesi o sostituiti da modelli di sicurezza ottimizzati per il mondo della virtualizzazione.

Ottimizzazione delle operazioni con McAfee MOVE

Quando, diversi anni fa, McAfee cominciò a lavorare con la comunità della virtualizzazione, questi problemi operativi cominciavano già ad emergere. Abbiamo risposto con una tecnologia specializzata in grado di integrare le nostre migliori capacità in fatto di sicurezza all'interno delle distribuzioni di server e desktop virtualizzati. McAfee MOVE AntiVirus offre la sicurezza e la protezione contro il malware senza compromettere le prestazioni. In questo modo è possibile sfruttare al massimo il valore della tecnologia della virtualizzazione e allo stesso tempo garantire la produttività dell'utente e la sicurezza del sistema operativo guest nella VM.

La nostra soluzione flessibile consente di scegliere il modello di distribuzione preferito: un modello in grado di funzionare su diverse piattaforme di virtualizzazione oppure un'opzione senza agent che sfrutta le API VMware vShield. Entrambe le opzioni sfruttano al massimo il sistema anti-malware McAfee leader del settore[2]. Inoltre, le prevenzione delle intrusioni e la sicurezza delle applicazioni web favoriscono una protezione extra contro gli attacchi.

Scansioni comode e solo se necessarie

McAfee MOVE AntiVirus libera le risorse dell'hypervisor per destinarle ad altre funzioni e allo stesso tempo garantisce l'esecuzione di scansioni aggiornate secondo quanto previsto dalla policy. Le scansioni, la manutenzione delle configurazioni e l'aggiornamento delle firme .DAT vengono effettuate da un'appliance fisica o virtuale rafforzata, che consente all'hypervisor di dedicarsi esclusivamente al supporto delle immagini guest.

L'integrazione di McAfee MOVE AntiVirus nel software di gestione della virtualizzazione consente di evitare le "scan storms" causate da un numero elevato di immagini che richiedono contemporaneamente il provisioning e la scansione. Inoltre, McAfee MOVE AntiVirus for Virtual Servers è in grado di pianificare in modo intelligente delle scansioni basate sulla disponibilità delle risorse e dell'hypervisor. Per effettuare la scansione delle VM attive, non è necessario metterle offline. Tuttavia, quando le immagini vengono messe offline, McAfee è in grado di sottoporle a scansione e aggiornarle per mantenerle pronte all'uso.

Applicazione dei più recenti aggiornamenti

McAfee MOVE AntiVirus protegge le VM utilizzando lo stesso motore McAfee VirusScan® utilizzato per i nostri prodotti antivirus per sistemi fisici leader del settore. Per mantenere le scansioni il più possibile aggiornate senza rallentare le prestazioni, l'appliance scarica e applica le firme più aggiornate su Offload Scan Server, invece che sulle singole VM. Quando dei file sconosciuti sembrano sospetti, McAfee MOVE AntiVirus consulta il servizio McAfee Global Threat Intelligence™.

Oltre alla scansione anti-malware, McAfee MOVE AntiVirus for Virtual Desktops comprende un firewall desktop e una protezione avanzata della memoria per limitare le attività dannose e preservare l'integrità dei file. Per consentire agli utenti di evitare i siti web rischiosi, che potrebbero introdurre del malware sull'immagine, McAfee include, per l'uso del web, anche degli avvisi di web reputation e dei controlli basati sulle policy. L'azione combinata di questi strumenti riduce la superficie soggetta agli attacchi dei sistemi virtualizzati. Per avere la massima protezione, è possibile includere anche altri strumenti come la whitelist delle applicazioni, che impedisce alle applicazioni indesiderate e al malware di interrompere le operazioni.

Sicurezza in rete

La virtualizzazione cambia anche il modo in cui le organizzazioni devono considerare la sicurezza in rete. Quando si virtualizza un'infrastruttura fisica, sono necessarie delle nuove strategie per creare e mantenere i confini della sicurezza in assenza di partizioni fisiche. Un altro problema è la portabilità delle VM e l'impatto sulle policy di sicurezza di rete. Le organizzazioni devono poter applicare una sicurezza di rete coerente indipendentemente dalla posizione fisica delle applicazioni e dei server virtualizzati.

McAfee offre una sicurezza di rete integrata per gli ambienti fisici e virtuali. McAfee Network Security Platform include l'ispezione nativa degli ambienti virtuali grazie alla completa integrazione con l'API per la sicurezza di rete di VMware vShield. Questo consente di ispezionare il traffico e di imporre delle policy sulle VM e tra le VM, indipendentemente dalla loro posizione fisica. Inoltre, l'accesso nativo agli strumenti VMware vCenter consente di integrare la sicurezza di rete trasversalmente agli ambienti virtuali.

Gestione completa

McAfee MOVE AntiVirus utilizza lo stesso ambiente di gestione di McAfee ePolicy Orchestrator® (McAfee ePO™) già noto agli amministratori che utilizzano gli endpoint, le informazioni e gli strumenti di sicurezza di rete fisici McAfee. Nel contesto di un unico sistema di console e policy, ogni amministratore può creare dei dashboard personalizzati per monitorare i dati che gli interessano e creare dei rapporti su specifiche risorse, anche se prevedono una combinazione di host fisici e virtuali e una combinazione di endpoint e server. Il supporto dei ruoli rende più semplice abbinare la sicurezza al mondo dell'amministrazione collaborativa dei centri di dati virtualizzati. Il software McAfee ePO, inoltre, integra oltre 100 altri prodotti dei partner McAfee Security Innovation Alliance e consente quindi al reparto IT di ottimizzare i flussi di lavoro sull'intera infrastruttura IT.

Standardizzazione e specializzazione

La scelta di un'implementazione basata su agent o di una multipiattaforma implica la capacità di supportare le relazioni con fornitori correnti e futuri. La soluzione multipiattaforma utilizza un agent leggero per ogni immagine guest per gestire policy e scansioni e sfrutta un server di scansione offload per le scansioni all'accesso. Questo approccio consente di combinare gli hypervisor Citrix, Microsoft e VMware per ottenere una maggiore flessibilità o per agevolare la presenza di comunità di utenti diversificate.

La nostra alternativa senza agent si integra strettamente con VMware per sfruttare gli investimenti fatti in tecnologie hypervisor. McAfee MOVE AntiVirus si serve di VMware vShield Endpoint per effettuare la scansione delle macchine virtuali dall'esterno delle immagini guest, senza la necessità di un software McAfee all'interno dell'immagine stessa. Grazie a VMware vMotion, le VM sottoposte a scansione possono migrare da un host all'altro senza impatto per l'utente o per i sistemi di scansione. L'integrazione tra il software McAfee ePO e vCenter ottimizza il monitoraggio e la gestione degli incidenti.

Conformità continua

La comune piattaforma McAfee ePO permette di avere delle policy coerenti sia sui sistemi fisici che su quelli virtuali. Per garantire i processi di conformità, è possibile creare una vista di verifica dei dati pertinenti e realizzare dei rapporti ad hoc o pianificati specifici per le diverse normative.

Un passo in avanti

È ora possibile abbinare la sicurezza ai requisiti di virtualizzazione. McAfee ha ottimizzato la protezione anti-malware e degli endpoint in modo che possa essere attivata dall'interno e dall'esterno della struttura e dei processi necessari all'efficienza della virtualizzazione. Le scansioni non intralciano le operazioni degli utenti attivi, mentre i processi del software di sicurezza e dell'aggiornamento delle firme rispettano la natura delle immagini server e desktop che prevede fasi online e fasi offline.

Il nostro design flessibile consente di scegliere qualsiasi fornitore e allo stesso tempo di garantire gli standard di sicurezza e conformità. McAfee consente di sfruttare tutti i vantaggi della virtualizzazione senza esporre dati e utenti agli attacchi dei criminali informatici moderni. I nostri investimenti finalizzati all'integrazione e all'ottimizzazione della nostra ampia gamma di prodotti sono costanti e consentono alle aziende di distribuire i più robusti sistemi di sicurezza con la massima efficienza per tutto il tempo necessario ad espandere l'uso della virtualizzazione.

Per ulteriori informazioni su McAfee MOVE AntiVirus, visitare il sito www.mcafee.com/it/solutions/virtualization/virtualization.aspx oppure contattare il proprio rappresentante o rivenditore McAfee di zona.

McAfee
An Intel Company

McAfee Srl
via Fantoli, 7
20138 Milano
Italia
(+39) 02 554171
www.mcafee.com/it

[1] http://www.informationweek.com/news/storage/virtualization/232400150
[2] http://www.av-comparatives.org/images/stories/test/ondret/avc_od_aug2011.pdf