McAfee Server Security Suite Advanced

Protezione avanzata dei server con whitelisting per distribuzioni fisiche, virtuali e cloud

Vantaggi principali

- Individua tutti i server fisici e virtuali, inclusi quelli nel cloud con un unico riquadro di gestione da una console centrale.
- Combina le tecniche di blacklisting e whitelisting per proteggere i server fisici e virtuali dal malware.
  - Fornisce whitelisting dinamico per proteggere dalle minacce sconosciute assicurando che gli host siano mantenuti al sicuro evitando che le applicazioni indesiderate vengano eseguite tramite McAfee Application Control for Servers.
  - Rileva costantemente le modifiche a livello di sistema, nei siti distribuiti e remoti, per aiutare a soddisfare i requisiti di conformità.

Il centro dati ha vissuto un'importante fase di transizione negli ultimi anni relativamente alle soluzioni di archiviazione, server, reti e applicazioni che fornisce. La natura diversificata del centro dati e la rapida evoluzione verso il cloud computing richiede nuove modalità per la protezione di questo ambiente. La sfida per il dipartimento IT aziendale e per i professionisti della sicurezza è di creare una posizione di sicurezza unificata e solida per gli ambienti fisici, virtualizzati e cloud per aiutare a garantire agilità e convenienza. McAfee® Server Security Suite Advanced - parte dell'offerta di prodotto Intel® Security - offre il più completo sistema di protezione e gestione di server per le distribuzioni fisiche, virtuali e nel cloud, con la sicurezza aggiuntiva data dal whitelisting e dal controllo delle modifiche, che aiutano a mantenere la conformità.

Individua tutti i carichi di lavoro

Spesso individuare tutti i carichi di lavoro e quindi applicare le policy di sicurezza appropriate nelle distribuzioni fisiche, virtuali e cloud, si rivela un compito difficile. La gestione è semplice grazie a report di analisi che permettono di rilevare gli endpoint non protetti e stabilire la conformità di sicurezza. Tramite connettori per il software McAfee® ePolicy Orchestrator® (McAfee ePO™), McAfee Server Security Suite Advanced permette di individuare tutti i server fisici e virtuali inclusi quelli nel cloud pubblico e privato. La soluzione include anche McAfee Data Center Connector for VMware vSphere, Amazon AWS, OpenStack e Microsoft Azure. Insieme consentono di monitorare tutti i computer virtuali sia in sede che fuori sede e applicare policy di sicurezza granulari che assicurano uno stato di sicurezza efficace. Le dashboard forniscono una fotografia dello stato della sicurezza tra cui la protezione della memoria del sistema operativo, le relazioni tra l'host hypervisor e il computer virtuale, la sede in cui il computer virtuale è dislocato e altro ancora.

Protezione dei server

McAfee Server Security Suite Advanced offre la protezione più completa per i server, che siano fisici, virtualizzati o nel cloud. Inoltre, offre funzioni di change control e una combinazione unica di tecnologie di protezione blacklisting e whitelisting ineguagliate nel settore.

Vantaggi principali (continua)

- Offre protezione ottimizzata per la virtualizzazione per un impatto minimo sulle prestazioni con McAfee MOVE AntiVirus.
- Fornisce visibilità totale sullo stato di sicurezza di tutti i computer virtuali nel cloud pubblico e privato tramite McAfee Data Center Connector for VMware vSphere, Amazon Web Services, OpenStack e Microsoft Azure.

McAfee Server Security Suite Advanced include McAfee Application Contro for Servers, una soluzione di whitelisting che consente l'esecuzione del solo software autorizzato sui server. Questa soluzione di whitelisting gestita centralmente utilizza un modello di sicurezza dinamico e funzioni di sicurezza innovative che bloccano le applicazioni non autorizzate e contrastano le minacce avanzate persistenti senza richiedere un'impegnativa gestione di elenchi. Il whitelisting riduce significativamente l'impatto sulle prestazioni dell'host proteggendo contro le minacce senza gli aggiornamenti delle firme.

Parte della protezione fondamentale per i server, la suite offre soluzioni antimalware tradizionali per i server Microsoft Windows e Linux, compreso il software McAfee VirusScan® Enterprise, classificato al primo posto da NSS Labs per gli exploit zero-day e gli attacchi di evasione. In aggiunta all'antimalware tradizionale, la suite offre una soluzione a parte, specializzata per gli ambienti virtuali. McAfee Management for Optimized Virtual Environments (MOVE) AntiVirus ottimizza la tecnologia antivirus per gli ambienti virtualizzati, minimizzando l'impatto sulle prestazioni anche per ambienti di grandi dimensioni e fornendo supporto per tutti i principali hypervisor. McAfee MOVE AntiVirus è disponibile in modalità agentless, come opzione ottimizzata per ambienti VMware o multipiattaforma e può essere distribuita per ambienti KVM, Microsoft Hyper-V, VMware e Xen basati su hypervisor.

Anche se l'antivirus è fondamentale per la sicurezza, per proteggersi dalle minacce avanzate possono servire delle soluzioni aggiuntive. McAfee Host Intrusion Prevention protegge l'azienda dalle minacce di sicurezza complesse che potrebbero altrimenti essere involontariamente introdotte o autorizzate.

Crescere nel cloud

Nel momento in cui ci si espande nel cloud, diventa sempre più difficile assicurare l'applicazione di policy di sicurezza appropriate ai carichi di lavoro recenti. McAfee affronta tali sfide rilevando automaticamente i computer virtuali in esecuzione e quelli bloccati forniti nel cloud pubblico e privato. Per abilitare tale processo, è sufficiente registrare un account cloud pubblico nella piattaforma McAfee ePO. I computer virtuali possono poi essere protetti automaticamente con policy di sicurezza adeguate. Inoltre, la dashboard McAfee per la protezione del centro dati offre visibilità totale dello stato di protezione e degli eventi di sicurezza nei cloud pubblici e privati.

Ottimizzazione dei server, ottimizzazione dell'azienda

L'enorme potenziale della virtualizzazione e del cloud computing può essere sfruttato appieno solo se essi vengono protetti a sufficienza. McAfee offre soluzioni per la protezione dei server che non ostacolerà le opzioni di crescita man mano che le aziende progrediscono. Fisica, virtualizzata o nel cloud: McAfee offre una suite di soluzioni per mantenere i server protetti mantenendo la flessibilità. McAfee Server Security Suite Advanced offre la protezione dei server fisici, virtuali e nel cloud con soluzioni avanzate che stabiliscono e mantengono una solida condizione di sicurezza all'interno dell'organizzazione.

Approfondisci i benefici offerti da McAfee Server Security Suite Advanced: **http://www.mcafee.com/it/products/server-security-suite-advanced.aspx**.

Funzionalità	A che cosa serve
Whitelisting delle applicazioni	• Riduce in modo significativo l'impatto sulle prestazioni dell'host rispetto al tradizionale controllo della sicurezza degli endpoint. • Protegge contro minacce zero-day e 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.
Controllo delle modifiche	• Previene eventuali manomissioni bloccando le modifiche non autorizzate ai file di sistema critici, directory e configurazioni, facendo risparmiare tempo agli amministratori per attività di troubleshooting relativamente alle violazioni di sicurezza. • Segue e convalida ogni tentativo di modifica in tempo reale sul server, applicando le policy per il controllo delle modifiche in base a intervalli di tempo, origine o ticket approvati. • Questo controllo continuo riduce al minimo l'impatto delle modifiche ad hoc o non autorizzate.
Gestione da un'unica console	• Gestione da un singolo pannello di server fisici e virtuali, compresi quelli che si trovano nel cloud privato e pubblico, per una maggior visibilità sulla sicurezza. • Semplifica gli aspetti operativi e richiede minor tempo allo staff amministrativo. • Riduce i costi per l'hardware grazie al minor ingombro dei server.
Protezione essenziale per il server	• Protezione antimalware per i server fisici classificata al primo posto da NSS Labs[1] contro gli exploit zero-day e gli attacchi evasivi. • Host Intrusion Prevention protegge le aziende dalle minacce di sicurezza complesse che potrebbero altrimenti essere involontariamente introdotte o autorizzate.
Protezione della virtualizzazione	• Sicurezza ottimizzata dei carichi di lavoro distribuiti sulle infrastrutture virtuali senza compromettere le prestazioni e l'utilizzo delle risorse. • Protezione per molteplici hypervisor nel centro dati per uno stato di sicurezza comune per tutte le tipologie di hypervisor utilizzate. • Distribuzione agentless ottimizzata per ambienti basati su VMware per aiutare a fornire ottime prestazioni e densità VM.
Piena visibilità dei computer virtuali sul cloud pubblico e privato	• Rileva sia i server fisici che gli hypervisor e i computer virtuali in ambienti VMware vSphere, Amazon AWS, OpenStack e Microsoft Azure per una piena visibilità su ciò che deve essere protetto. • Rileva quando vengono introdotti i computer virtuali in modo da poterli proteggere automaticamente con policy di sicurezza per garantire uno stato di sicurezza adeguato per tali computer virtuali.

1. NSS Labs, Inc., Protection & Evasion Test (Test sulla protezione e le evasioni di NSS Labs, Inc.), 2013

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