McAfee Server Security Suite Advanced

Sicurezza completa per distribuzioni fisiche, virtuali e cloud con whitelisting e controllo delle modifiche.

Nell'attuale ambiente IT complesso, è sempre più difficile proteggere nuovi server e carichi di lavoro cloud da minacce sempre più sofisticate senza un approccio olistico. McAfee® Server Security Suite Advanced offre protezione continua e coerente su distribuzioni fisiche, virtuali e in cloud pubblico. La protezione completa include antivirus di base, protezione firewall, prevenzione delle intrusioni, whitelisting per proteggere dalle minacce zero-day e controllo delle modifiche per soddisfare i requisiti normativi per la conformità. La protezione avanzata riduce al minimo l'impatto sulle prestazioni per i server fisici e virtuali e scala automaticamente con i carichi di lavoro cloud dinamici.

Rilevamento e controllo istantanei

Tenere traccia delle lacune di sicurezza all'interno di un data center ibrido in continua espansione non è un compito difficile, grazie a Cloud Workload Discovery per cloud ibrido, una funzionalità fondamentale di McAfee Server Security Suite Advanced. Coprendo VMware, OpenStack, Amazon Web Services (AWS) e Microsoft Azure, Cloud Workload Discovery per cloud ibridi fornisce visibilità end-to-end su tutti i carichi di lavoro e le loro piattaforme. Informazioni approfondite sui controlli di sicurezza deboli, le impostazioni di crittografia e i firewall non sicuri, oltre agli indicatori di compromissione, come il traffico sospetto, portano a un più rapido rilevamento. Il software McAfee® ePolicy Orchestrator® (McAfee ePO™) o gli strumenti DevOps permettono un rapido processo di remediation.

La sicurezza cloud può essere complessa poiché sono presenti molti diversi carichi di lavoro cloud con profili di rischio e requisiti di sicurezza unici. La valutazione basata su policy di Cloud Workload Discovery semplifica il confronto di quali controlli di sicurezza richiedono questi diversi carichi di lavoro, rispetto a quelli di cui effettivamente dispongono, per garantire protezione e conformità adeguate. Una volta individuati i rischi per la sicurezza, è possibile procedere a completare la protezione con pochi semplici clic.

L'integrazione di Cloud Workload Discovery con la console di gestione di McAfee ePO offre alle aziende un controllo efficace per implementare soluzioni sicure in ambienti fisici, virtuali e cloud. Grazie a questa integrazione, gli amministratori della sicurezza possono

Vantaggi principali

- Unifica la gestione della sicurezza tra endpoint, reti, dati e soluzioni di conformità di McAfee e soluzioni di terze parti attraverso il software McAfee ePO.
- Fornisce visibilità approfondita, valutazione del rischio e remediation attraverso Cloud Workload Discovery per cloud ibrido.
- Combina blacklisting e prevenzione delle intrusioni con whitelisting avanzato e controllo delle modifiche per proteggere i server fisici e virtuali dal malware.
  - Protegge da minacce sconosciute bloccando l'esecuzione di applicazioni indesiderate.
  - Rileva costantemente le modifiche a livello di sistema, nei siti distribuiti e remoti, per aiutare a soddisfare i requisiti di conformità.
- Blocca le minacce sconosciute zero-day in pochi secondi utilizzando i dati locali sulla reputazione combinati con le analisi della sandbox.
- Offre sicurezza fisica e virtuale ottimizzata con un impatto minimo sulle prestazioni.

utilizzare un'unica piattaforma di gestione con flussi di lavoro semplificati per indirizzare gli avvisi sulle minacce e applicare le policy, riducendo i tempi di identificazione e risoluzione dei problemi di sicurezza.

McAfee Server Security Suite Advanced assicura che gli ambienti cloud dinamici che supportano DevOps non vadano a sacrificare la sicurezza a favore dell'agilità. La nostra sicurezza si adatta in modo flessibile ai carichi di lavoro del cloud in modo da assicurare protezione costante. Con il provisioning flessibile nei cloud privati, i server di scansione offline possono essere aggiunti o rimossi automaticamente dal pool di risorse quando i carichi di lavoro vengono aumentati o ridotti. Per i carichi di lavoro AWS e Azure, gli utenti possono configurare la sicurezza a livello di modello in modo da scalare automaticamente quando cambiano i carichi di lavoro.

Protezione completa

McAfee Server Security Suite Advanced offre la protezione più completa per i server, che siano fisici, virtuali o nel cloud. Inoltre, la sua protezione contro gli attacchi di overflow del buffer della memoria su sistemi Windows a 32 e 64 bit, unitamente a una combinazione unica di blacklisting, whitelisting e controllo delle modifiche, non ha pari nel settore. La suite include:

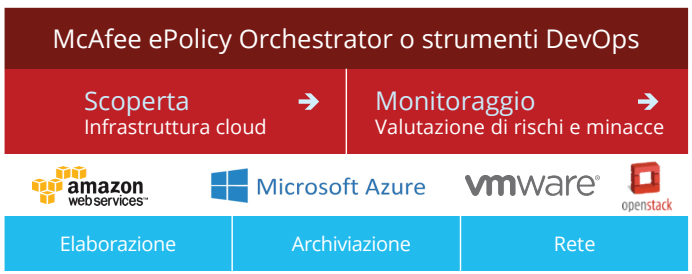

Figura 1. Ricava un vantaggio sostenibile con Cloud Workload Discovery.

- **McAfee Application Control for Servers:** questa soluzione di whitelisting permette l'esecuzione sui server solo di software autorizzato per proteggere contro malware sconosciuto e zero-day e minacce avanzate. Questa soluzione di whitelisting gestita utilizza un modello di attendibilità dinamico per eliminare una gestione degli elenchi dispendiosa in termini di tempo.
- **McAfee Change Control for Servers:** fornisce un rilevamento costante delle modifiche a livello di sistema tra sedi distribuite e remote per assicurare la conformità con leggi e normative, come Sarbanes-Oxley e Payment Card Industry Data Security Standard (PCI DSS).
- **McAfee Endpoint Security - Prevenzione contro le minacce:** parte di una struttura collaborativa estendibile che protegge i server Microsoft Windows e Linux dagli exploit zero-day e dagli attacchi avanzati.
- **McAfee Management for Optimized Virtual Environments AntiVirus (McAfee MOVE AntiVirus):** questa soluzione antimalware è progettata specificamente per gli ambienti virtuali. È disponibile come opzione ottimizzata senza agent per VMware NSX e VMware vCNS e come opzione multi-piattaforma che può essere distribuita per tutti i principali hypervisor, tra cui Microsoft Hyper-V, VMware, KVM e Xen.

- **McAfee Host Intrusion Prevention for Server:** protegge le aziende da minacce alla sicurezza complesse monitorando il comportamento del codice sul server, analizzando gli eventi per rilevare l'attività sospetta.
- **McAfee Endpoint Security - Firewall:** controlla il traffico di rete e internet e intercetta le comunicazioni sospette.

McAfee Server Security Suite Advanced può migliorare le informazioni globali sulla reputazione di 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, le soluzioni nella suite si coordinano con McAfee Advanced Threat Defense per analizzare dinamicamente il comportamento di applicazioni sconosciute in una sandbox e immunizzare tutti gli endpoint da malware appena rilevato.

McAfee collabora con Rapid7 per la gestione delle vulnerabilità. La soluzione Nexpose di Rapid7 individua e classifica le vulnerabilità e conferma quando viene posto rimedio alle violazioni.

Impatto minimo sulle prestazioni

Sebbene la sicurezza sia prioritaria per la maggior parte delle aziende, alcune sono riluttanti a procedere con la protezione dei server a causa delle preoccupazioni relative al suo impatto sulle prestazioni. McAfee Server Security Suite Advanced permette di proteggere i server fisici e virtuali senza sacrificare le prestazioni anche quando si effettua una scansione del malware.

A differenza di molti prodotti antimalware, McAfee Endpoint Security e McAfee MOVE AntiVirus non richiedono risorse di elaborazione particolarmente importanti. McAfee Endpoint Security fornisce scansioni rapide e ottimizza il suo utilizzo della CPU e della memoria offrendo una protezione migliore di altri prodotti antimalware. McAfee MOVE AntiVirus scarica la scansione del malware dai computer virtuali per una protezione istantanea con un basso impatto su memoria ed elaborazione. Policy separate per le scansioni all'accesso e on demand permettono un maggior controllo dell'ottimizzazione delle prestazioni e della sicurezza.

Ottimizzazione della sicurezza 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, virtuale o nel cloud: offriamo una suite di soluzioni per mantenere i server e i carichi di lavoro cloud protetti in ambienti sempre più dinamici.

SCHEDA TECNICA

Funzionalità	A che cosa serve
Gestione da un'unica console	▪ 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 gli aspetti operativi e richiede minor tempo allo staff amministrativo.
Rilevamento e controllo istantanei	▪ Individua i server fisici e ottieni una visione completa dei carichi di lavoro e delle piattaforme VMware vSphere, OpenStack, AWS e Microsoft Azure. ▪ Assicurati di essere sempre protetto con una protezione che scala in modo flessibile in base ai tuoi carichi di lavoro cloud dinamici.
Protezione della virtualizzazione	▪ Ottimizza la sicurezza dei carichi di lavoro distribuiti sulle infrastrutture virtuali senza compromettere le prestazioni e l'utilizzo delle risorse. ▪ Scegli una distribuzione multi-piattaforma (tutti i principali hypervisor) o senza agent per VMware NSX e VMware vCNS per fornire prestazioni eccezionali e densità del computer virtuale.
La sicurezza del cloud pubblico	▪ Verifica la sicurezza della piattaforma, comprese le impostazioni di firewall e crittografia, per AWS e Microsoft Azure. ▪ Assicura protezione completa con visibilità sulle minacce di traffico e rete per AWS.
Whitelisting delle applicazioni	▪ Riduci in modo significativo l'impatto sulle prestazioni dell'host rispetto al tradizionale controllo della sicurezza dei server. ▪ Difenditi contro le minacce persistenti avanzate e zero-day (APT) senza aggiornamenti delle firme, per una protezione più rapida. ▪ Riduci l'overhead operativo grazie al whitelisting dinamico.
Controllo delle modifiche	▪ Previeni eventuali manomissioni bloccando le modifiche non autorizzate a file di sistema critici, directory e configurazioni, facendo così risparmiare tempo agli amministratori nelle attività di risoluzione delle violazioni. ▪ Segui 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 di modifica approvati.
Protezione essenziale per il server	▪ Implementa protezione anti-malware che tutela da exploit zero-day e attacchi avanzati. ▪ Salvaguarda dalle minacce complesse alla sicurezza che potrebbero altrimenti essere introdotte involontariamente o autorizzate con McAfee Host Intrusion Prevention System.
Intelligence sulla reputazione locale	▪ Blocca le minacce sconosciute zero-day in pochi secondi attraverso l'integrazione con McAfee Threat Intelligence Exchange (un modulo aggiuntivo venduto separatamente).

Ulteriori informazioni

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

McAfee Together is power.

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