IBM Security Virtual Server Protection for VMware

Aumentate il livello di convenienza, conformità e sicurezza con le soluzioni ottimizzate per la sicurezza dei centri dati virtualizzati

In evidenza

- Garantisce la persistenza delle policy di sicurezza anche in caso di migrazione delle macchine virtuali da un server ESX all'altro
- Fornisce prevenzione delle intrusioni e firewall senza la necessità di un agent basato su host
- Identifica le attività di rootkit all'interno dell'OS guest
- Consente di controllare la proliferazione incontrollata di server virtuali e attenua i rischi introdotti da macchine virtuali non autorizzate
- Esegue monitoraggi e report sull'attività dell'infrastruttura virtuale, consentendo di ottenere la conformità con i requisiti di compliance
- Consente di abbattere i costi e ridurre il livello di complessità con funzionalità di protezione automatica dell'infrastruttura virtuale.

La virtualizzazione apporta notevoli vantaggi all'organizzazione IT, ma le soluzioni per la sicurezza esistenti non sono ottimizzate per l'utilizzo in ambienti virtuali. I processi e le tecnologie tradizionali per la sicurezza non sono in grado di proteggere in modo efficace i livelli aggiuntivi, compresi hypervisor, stack di gestione e rete virtuale. Di conseguenza, i server virtualizzati possono essere meno sicuri dei server fisici che sostituiscono e possono lasciare le organizzazioni esposte a rischi legati alla non conformità con la normativa in materia di compliance. Le organizzazioni devono assumere un approccio pienamente consapevole dei nuovi potenziali rischi e devono implementare i necessari controlli per la sicurezza. IBM Security Virtual Server Protection for VMware è una soluzione integrata per l'attenuazione delle minacce, progettata per consentire alle organizzazioni di sfruttare appieno i vantaggi della virtualizzazione del server proteggendo, al contempo, risorse virtualizzate di fondamentale importanza.

Firewall

IBM Security Virtual Server Protection for VMware offre la tecnologia firewall per consentire la segmentazione della rete virtuale e prevenire la comunicazione non autorizzata tra trust zones.

Prevenzione delle intrusioni trasparente

Le macchine virtuali (VM) possono essere configurate e implementate rapidamente, realizzando in tal modo un ambiente estremamente dinamico. La tecnologia leader sul mercato per la prevenzione delle intrusioni di IBM protegge le VM nel momento del collegamento online o dello spostamento all'interno del data centre.

Rilevamento automatico

Le reti virtuali possono anche introdurre gap di visibilità che rendono inefficaci tool e processi di rilevamento tradizionali. IBM Security Virtual Server Protection for VMware è in grado di eseguire il rilevamento automatico delle nuove VM. Questa funzionalità consente di aumentare il livello di sicurezza e visibilità all'interno dell'ambiente virtuale.

Rilevamento del rootkit da parte della VM

IBM Security Virtual Server Protection for VMware esegue ispezioni, in modo trasparente, delle VM per individuare l'installazione di rootkit. Questa soluzione integra le tradizionali funzionalità anti-malware identificando i rootkit, essendo immune dalle tecniche comunemente adottate dai rootkit per disabilitare gli agent basati su host.

Analisi del traffico tra VM

Il traffico di rete tra VM all'interno dello stesso server fisico non esce al di fuori della macchina, condizione che può creare un'area non visibile particolarmente allarmante tra VM di diversi livelli trust. Mentre i sistemi tradizionali di prevenzione delle intrusioni di host e rete non hanno visibilità del traffico tra VM, IBM Security Virtual Server Protection for VMware esegue il monitoraggio del traffico tra server virtuali per arrestare le minacce prima che impattino sull'ambiente.

Controllo di accessi alla rete virtuale

Le VM possono essere introdotte rapidamente nel data centre con un basso livello di supervisione e, di conseguenza, possono creare esposizioni a rischi in termini di sicurezza. IBM Security Virtual Server Protection for VMware esegue controlli di accessi alla rete virtuale con messa in quarantena o limitazione dell'accesso alla rete da parte di un server virtuale finché non viene convalidata la sicurezza della VM.

Auditing dell'infrastruttura virtuale

IBM Security Virtual Server Protection for VMware esegue report sull'attività di utenti privilegiati quali eventi VMotion, modifiche dello stato delle VM (avvio, arresto, pausa) e attività di login che possono ridurre il tempo di preparazione richiesto per supportare i controlli.

Tecnologia IBM Virtual Patch

La tecnologia IBM Virtual Patch protegge le vulnerabilità di sistemi operativi o applicazioni, consentendo alle organizzazioni di avviare cicli di patching prevedibili. Questo approccio può proteggere automaticamente le organizzazioni dalle vulnerabilità dei server virtuali a prescindere dalla rispettiva strategia di patching.

Sfruttare il potere del controllo della sicurezza a livello enterprise

Nonostante la continua espansione della virtualizzazione, le organizzazioni continuano ad assumere un approccio ibrido verso l'IT; per questo motivo server e connessioni in rete fisici continueranno ad esistere e richiedono protezione. IBM promuove l'assunzione di un approccio di difesa completo da parte del cliente nei confronti della sicurezza a livello enterprise-. La soluzione IBM Security Virtual Server Protection for VMware fornisce un livello di difesa-completo per l'infrastruttura virtuale, e rappresenta, al contempo, un livello appartenente ad una strategia per la sicurezza enterprise di più ampia portata. Con IBM, i clienti possono trarre vantaggio da una tecnologia per la sicurezza leader a livello mondiale, progettata per proteggere ogni singolo livello dell'ambiente IT. Facendo afferire reti, host, endpoint, applicazioni e sicurezza virtuale alla stessa tecnologia di base, le organizzazioni possono ottenere anche maggiore visibilità e controllo della sicurezza per mezzo di una soluzione efficiente e scalabile.

Caratteristiche e vantaggi

Potenziamento della sicurezza dinamica ovunque siano implementate le VM:

- Prevenzione delle intrusioni senza agent e firewall per assicurare il massimo livello di difesa e sicurezza-
- Isolamento del carico di lavoro a livello di rete
- Rilevamento automatico di VM non visibili ai tool di rilevamento tradizionali
- Identificazione trasparente di attività di rootkit all'interno delle VM
- Messa in quarantena di VM potenzialmente non sicure finché la loro sicurezza non viene convalidata
- Monitoraggio dell'attività dell'infrastruttura virtuale.

Accelerazione e semplificazione del controllo per la verifica della conformità PCI DSS (Payment Card Industry Data Security Standard) e conseguimento della compliance con funzionalità di sicurezza e reporting personalizzate per l'infrastruttura virtuale:

- Funzionalità di segmentazione della rete virtuale per separare i server virtuali che rientrano nella portata della Peripheral Controller Interface (PCI)
- La protezione automatica garantisce l'attuazione dei controlli di sicurezza anche negli ambienti più dinamici.

Consente di ridurre costi e complessità rispetto all'utilizzo di soluzioni di sicurezza fisiche in infrastrutture virtuali con funzionalità di protezione automatiche:

- Riduzione del carico di lavoro dell'amministratore del sistema con funzionalità di protezione, rilevamento e valutazione automatica
- Utilizzo della tecnologia IBM Virtual Patch per la protezione automatica delle vulnerabilità sui server virtuali a prescindere dalla strategia di patching.

Potenziare l'efficienza con IBM Security SiteProtector System

IBM Security SiteProtector System offre una soluzione più semplice e conveniente per gestire la sicurezza e garantire la compliance con le normative, fornendo la gestione centralizzata del controllo delle policy di sicurezza, analisi, messaggi di allarme e reporting per la vostra organizzazione con il supporto di VMware ESX. Progettato per la massima semplicità e flessibilità, SiteProtector System è in grado di fornire attività centralizzate di configurazione, gestione, analisi e reporting.

Migliorare la sicurezza virtuale grazie alla ricerca condotta da IBM X-Force

L'eccellenza di IBM in materia di sicurezza è resa possibile grazie al team di fama mondiale X-Force. La straordinaria intelligence del team X-Force viene trasmessa alle soluzioni di sicurezza di IBM. Che si tratti di applicativi 1U o componenti software installate su una VM, le soluzioni di IBM sono tutte supportate dalla stessa intelligence per la sicurezza e prevenzione delle minacce, messa a punto dal team X-Force. Il team X-Force è uno dei gruppi di ricerca in materia di sicurezza commerciale più noti e da più tempo affermati al mondo. Questo gruppo di esperti leader in materia di sicurezza è impegnato nella conduzione di ricerche e valutazioni su questioni legate a vulnerabilità e sicurezza, così come nello sviluppo di tecnologia di valutazione e intervento per i prodotti di sicurezza IBM, nonché in attività di divulgazione al pubblico di tematiche inerenti le minacce Internet emergenti. Oltre a fornire aggiornamenti sui contenuti in tema di sicurezza ai prodotti di sicurezza IBM, il team X-Force offre anche il servizio di analisi IBM X-Force Threat Analysis Service (XFTAS). Il servizio XFTAS offre informazioni mirate su un'ampia gamma di minacce che possono colpire la rete per mezzo di analisi dettagliate delle condizioni delle minacce a livello globale.

Perché IBM?

La soluzione IBM Security Virtual Server Protection for VMware è stata creata ad hoc-per proteggere il centro dati virtuale, che costituisce il nucleo centrale dell'infrastruttura, senza ridurre l'efficienza o la performance del sistema. Oltre alla massima protezione, IBM Security Virtual Server Protection for VMware consente al cliente di adempiere agli standard di compliance, limitando l'accesso a dati di fondamentale importanza contenuti nelle VM ed eseguendo una tracciatura dell'accesso da parte degli utenti. IBM offre una gamma completa di soluzioni per la sicurezza – comprese tecnologie all'avanguardia per la protezione dell'ambiente fisico di server, endpoint, network core, applicazioni e molto altro ancora. Con IBM, la sicurezza virtuale può essere gestita a livello centrale in parallelo con la tecnologia IT per la sicurezza esistente, per consentire ai clienti maggiore efficienza e scalabilità. IBM apporta una sicurezza completa, end-to-end (E2E) alla virtualizzazione, consentendo al cliente di realizzare, più rapidamente, i vantaggi offerti dalla tecnologia di virtualizzazione.

Requisiti	
Piattaforma	server X86 con VMware vSphere 4

Ulteriori informazioni

Per ulteriori informazioni su IBM Security Virtual Server Protection for VMware, contattate il rappresentante IBM o il Business Partner IBM locale, o visitate i seguenti siti:
ibm.com/tivoli/security

IBM Italia S.p.A.
Circonvallazione Idroscalo
20090 Segrate (MI)
Italia

La home page IBM è disponibile all'indirizzo **ibm.com**

WGD03008-ITIT-00