Suggerimenti tecnici

10 suggerimenti per rendere più sicura la distribuzione di VMware Horizon

La salvaguardia dell'IT nell'era della virtualizzazione

Stimolate dai vantaggi della business mobility, le organizzazioni IT sono comprensibilmente desiderose di abbandonare le limitazioni dell'architettura legacy e optare per la libertà del desktop di nuova generazione. Con la trasformazione del desktop consentita da VMware® Horizon®, gli utenti finali possono ora contare sulla flessibilità di accesso ad applicazioni e desktop virtualizzati mediante una singola piattaforma.

Ma questa nuova dimensione della flessibilità degli utenti, che comprende funzionalità mirate come i servizi BYOD (Bring Your Own Device), pone nuovi problemi di sicurezza IT. Un accesso più articolato e frequente richiede maggiore vigilanza per garantire la sicurezza dei dati. E in un'area in cui la sicurezza dell'IT aziendale richiede già particolare attenzione (il numero di incidenti sta aumentando a un tasso di crescita annuale composto del 66%, con un costo per violazione pari a 5,9 milioni di dollari USA[1]) occorre essere certi che la trasformazione del desktop sia efficiente e sicura.

CHE COS'È VMWARE HORIZON?

VMware Horizon estende la potenza della virtualizzazione di applicazioni e desktop, che vengono resi disponibili agli utenti finali in versioni virtualizzate tramite una singola piattaforma. Questi servizi per applicazioni e desktop, che comprendono applicazioni RDS in hosting e applicazioni pacchettizzate VMware ThinApp®, sono tutti accessibili da un'unica area di lavoro unificata, estesa a dispositivi, supporti, ubicazioni e connessioni. Per ulteriori informazioni su Horizon, visitare vmware.com/go/horizon.

La virtualizzazione del desktop impone di ripensare la sicurezza IT

Mentre la trasformazione del desktop porta con sé una serie di vantaggi per gli utenti finali e le organizzazioni IT, ovvero risparmio sulle spese operative, gestione semplificata, maggiore produttività degli utenti finali, alta disponibilità e riduzione delle spese di capitale, è importante comprendere i problemi che comporta per i responsabili IT.

- Grazie alla distribuzione in tempo reale di desktop e applicazioni, la trasformazione del desktop consente agli amministratori IT di rendere rapidamente operativi nuovi utenti offrendo in pochi secondi "desktop stateless" effettivi. Come scalare orizzontalmente le distribuzioni in modo rapido senza perdere la visibilità o il controllo della rete?

- È possibile che l'organizzazione fornisca servizi per migliaia o addirittura centinaia di migliaia di utenti in postazioni ubicate accanto all'infrastruttura mission critical. Se i desktop virtuali sono compromessi, la violazione potrebbe risultare costosa.

- L'attività "est-ovest", il traffico interno tra server o desktop, può rendere l'organizzazione vulnerabile. Le azioni da parte di utenti finali attendibili possono rappresentare minacce per la rete, come le e-mail infette da virus o una navigazione su Internet su un sito non sicuro.

Alla luce di queste considerazioni sulla sicurezza, riportiamo 10 suggerimenti tecnici per rendere più sicura la distribuzione di Horizon:

1 Usare immagini gold

Con un'"immagine gold", un template per desktop virtuali, i team IT possono personalizzare i desktop virtuali in modo che gli utenti vedano soltanto le attività rilevanti per le loro esigenze aziendali. Di conseguenza, l'IT può concentrarsi sulla preservazione della purezza dell'immagine gold custodita in sicurezza nel data center. Se un desktop virtuale viene compromesso, l'IT può intervenire per eliminare l'immagine e ridistribuire un nuovo desktop.

2 Usare layer di sicurezza

In un ambiente virtualizzato, affrontare i rischi connessi alla sicurezza su più fronti è un approccio vincente. Con l'introduzione di ulteriori misure di sicurezza come l'applicazione di "white list" tramite VMware NSX™, è possibile approvare le applicazioni che vengono eseguite sulla rete. Questo meccanismo mantiene la rete sicura e gli utenti conformi, poiché le aziende si misurano con la realtà dello "shadow IT", in cui gli utenti finali e i responsabili della linea di business perseguono applicazioni e servizi aziendali al di fuori del dominio IT. È inoltre possibile preservare l'integrità delle applicazioni mediante metodi di distribuzione specifici, utilizzando strumenti come VMware App Volumes™.

1. PwC, "Managing cyber risks in an interconnected world", settembre 2014

INFORMAZIONI SU VMWARE APP VOLUMES

VMware App Volumes consente agli amministratori IT di distribuire applicazioni e dati a utenti o desktop in pochi secondi, secondo le esigenze. App Volumes consente di ridurre i costi di infrastruttura e gestione grazie all'utilizzo di volumi gestiti. Le applicazioni sono del tutto assimilabili, in termini di prestazioni, alle applicazioni installate a livello nativo e forniscono agli utenti finali un'esperienza ottimale in tutte le sessioni e per tutti i dispositivi.

I vantaggi comprendono:

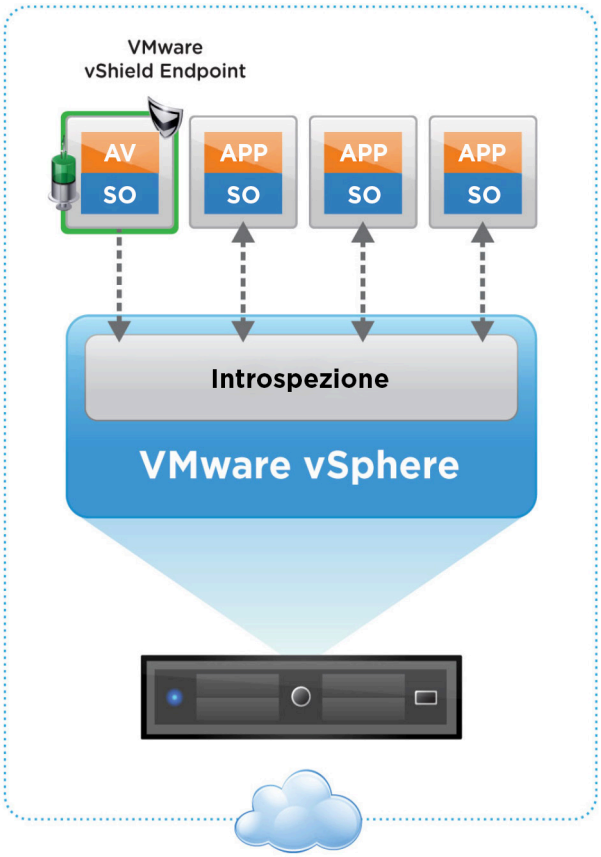
- Applicazioni gestite centralmente
- Facile distribuzione delle applicazioni
- Applicazioni distribuite per utente

Per ulteriori informazioni su App Volumes, visita https://www.vmware.com/it/products/appvolumes/.

3 Assicurare una sicurezza adeguata dei dispositivi endpoint

Investendo in funzionalità hardware e software, è possibile rafforzare la sicurezza dei dispositivi di endpoint Horizon. Ad esempio, se un dispositivo viene perso o rubato, le funzionalità basate su hardware, come Trusted Platform Module (TPM), consentono l'autenticazione sulla piattaforma senza necessità di avvio del dispositivo. Inoltre, garantiscono che le definizioni antivirus e il software anti-malware siano aggiornati e che il firewall del dispositivo di endpoint sia aggiornato e attivo.

È noto che alcuni amministratori IT eludono procedure antivirus per i loro desktop virtuali per ridurre l'impatto sulla memoria, sulla CPU e sui dischi. Ma i danni causati da un virus su un desktop virtuale possono essere altrettanto gravi di quelli provocati da un virus su un desktop fisico, soprattutto se si trascura di aggiornare regolarmente le macchine virtuali (VM). VMware vShield Endpoint™ trasferisce il carico di lavoro del software di elaborazione degli agenti antivirus e anti-malware dalle VM a un'appliance virtuale sicura e questo può rappresentare un'alternativa eccellente.



Infine, è possibile rafforzare ulteriormente la sicurezza dei dispositivi endpoint mediante soluzioni di terze parti. Soluzioni come Trend Micro Deep Security offrono caratteristiche avanzate, tra cui anti-malware, IDS/IPS, monitoraggio dell'integrità, filtraggio degli URL e installazione di patch. Estese funzionalità di sicurezza vengono eseguite a livello hypervisor e forniscono una protezione immediata al momento in cui viene attivato un nuovo desktop virtuale. Inoltre, la sicurezza segue automaticamente l'endpoint in qualsiasi posizione nel data center.

INFORMAZIONI SU VMWARE VSHIELD ENDPOINT

VMware vShield Endpoint rafforza la sicurezza per le macchine virtuali, migliorando al contempo le prestazioni per la protezione degli endpoint per ordini di grandezza. vShield Endpoint è ideato per sfruttare gli investimenti esistenti, consentendo ai clienti di gestire le policy antivirus e anti-malware per ambienti virtualizzati con le stesse interfacce di gestione utilizzate per proteggere gli ambienti fisici. La soluzione si integra con i prodotti dei seguenti vendor: Trend Micro, Intel Security, Symantec, Sophos e Kaspersky.

4 Implementare policy di gruppo e policy estese

Quando si verifica una violazione in un endpoint, ad esempio quando in un dispositivo manca un aggiornamento del software antivirus o antimalware, le policy di gruppo possono contribuire a deviare il pericolo. Con una policy di gruppo è possibile inoltre assicurare coerenza tra i desktop virtuali, disattivare i servizi non necessari all'utente e vietare l'accesso a determinate aree del desktop o della rete. Le impostazioni delle policy impediscono agli utenti di apportare modifiche che potrebbero esporre il desktop a vulnerabilità.

Si consiglia l'utilizzo di VMware User Environment Manager™, una soluzione di gestione dell'ambiente utente potente, semplice e scalabile che aiuta l'IT nella gestione delle applicazioni e degli utenti, nonché nell'impostazione di policy dinamiche. Con le impostazioni di policy e applicazioni che seguono gli utenti in tutti i dispositivi e in qualsiasi ubicazione e l'accesso gestito in base all'ingresso degli utenti tramite desktop interno o dispositivo esterno, le operation IT quotidiane sono più efficienti e sicure.

Inoltre, utilizzando i file del template di amministrazione (ADM) delle policy di gruppo di Horizon, che estende la policy di gruppo di Active Directory, è possibile gestire le informazioni da e verso il desktop, ad esempio disattivare gli appunti.

5 Garantire un'architettura adeguata

Con Horizon, la distribuzione sicura richiede particolare attenzione alla configurazione di firewall e zona demilitarizzata, nonché alla separazione di pool di desktop. Per iniziare, collocare un firewall tra la rete del data center e la rete dell'ufficio. Se si utilizzano LAN o firewall virtuali per segmentare i server dai desktop, accertarsi che l'ambiente VDI sia sul lato desktop del firewall.

Per garantire sicurezza per gli utenti remoti, collocare il server di sicurezza o il punto di accesso nella zona demilitarizzata. In questo modo si offre agli utenti un punto di connessione senza consentire l'accesso diretto alla rete. E per una funzione gateway, prendere in considerazione i vantaggi di Access Point su un server di sicurezza. Ad esempio, con Access Point si implementerà una macchina virtuale con sicurezza potenziata, bloccata e preconfigurata basata su Linux, non solo software in esecuzione su un sistema operativo Windows a fine generico. È inoltre possibile collegare Access Point a un singolo View Connection Server o collegarlo tramite un'unità di bilanciamento del carico a più View Connection Server per una maggiore disponibilità.

La separazione di pool di desktop è consigliabile quando i desktop devono essere separati dal resto dell'organizzazione, come i desktop per le risorse umane, i collaboratori esterni o gli sviluppatori. L'uso di VMware NSX come add-on per la piattaforma VMware vSphere® può aiutarvi a effettuare la separazione.

6 Usare autenticazione multifattore e pass-through

Essendo compatibile con soluzioni di autenticazione multifattore leader, come RSA SecurID, VASCO DIGIPASS, SMS Passcode e SafeNet, Horizon offre la base per la sicurezza del desktop. Horizon funziona con tecnologia di autenticazione pass-through, in cui gli utenti immettono le credenziali due volte o accedono al desktop con un account distinto.

Inoltre, prendere in considerazione l'uso di VMware Identity Manager™. Questa soluzione di gestione delle identità offre accesso condizionale e accesso Single Sign-on (SSO), semplificando la business mobility e consentendo un'esperienza d'uso unificata su tutti i dispositivi senza compromettere la sicurezza dell'ambiente.

7 Proteggere le periferiche

Le unità esterne possono introdurre virus dannosi o consentire agli utenti persino il furto di proprietà intellettuale. Con Horizon è possibile adottare misure per proteggere i dati in modo che non possano essere copiati nei dispositivi di storage portatili locali, quali USB e stampanti non protette. Inoltre, quando la funzionalità di reindirizzamento dell'unità client è installata sul desktop virtuale, gli utenti sono in grado di accedere "da remoto" ai file archiviati sul proprio PC locale. Compressione e crittografia vengono richiamate durante il trasferimento dei file dall'endpoint al desktop virtuale.

8 Effettuare manutenzione/scansioni periodiche

Occuparsi della sicurezza in modo approfondito significa anche dedicare attenzione alla manutenzione. Per tenersi al riparto da potenziali violazioni, adottare le seguenti misure:

- Aggiornare il software con funzionalità anti-virus e anti-malware che informano il personale appropriato di attacchi imminenti.
- Definire una policy accettabile per ricomporre o aggiornare regolarmente i desktop di Horizon per rendere possibile l'introduzione di patch di sicurezza, patch e aggiornamenti di applicazioni e l'effettuazione di aggiornamenti del sistema operativo.
- Applicare regolarmente patch e aggiornamenti della sicurezza, non solo per il sistema operativo ma anche per le applicazioni nell'"immagine gold".
- Eseguire scansioni periodiche delle porte sui firewall principali e secondari, per garantire che la policy del firewall sia correttamente attuata e non consenta l'accesso non autorizzato alla zona demilitarizzata.
- Condurre un'analisi del modello di traffico per comprendere che tipo di traffico sia consentito all'interno dei firewall e della zona demilitarizzata e monitorare il firewall per individuare porte inutilizzate.
- Effettuare controlli regolari. Ad esempio, controllare regolarmente la configurazione dell'unità di bilanciamento del carico e il firewall per accertarsi che non vengano effettuati accessi non autorizzati.
- Quando si applicano patch e aggiornamenti, aggiornare prima l'immagine parent, testarla e distribuirla rapidamente e in modo affidabile su tutti i desktop virtuali.

L'IMPORTANZA DELL'AGGIORNAMENTO: INCREMENTO DELLA SICUREZZA E DELLE PRESTAZIONI

Aggiornando i desktop virtuali al momento della disconnessione, ciascun utente dispone sempre di un desktop pulito e funzionale. Oltre alla sicurezza derivante dall'eliminazione di potenziali virus e malware dal desktop virtuale, l'utente successivo potrà contare sulla stessa facilità d'uso e su un miglioramento delle prestazioni.

9 Proteggere la rete

La combinazione di VMware NSX e Horizon offre il quadro di riferimento per l'automazione e la microsegmentazione. Con VMware NSX è possibile fornire un firewall distribuito per porta, che consente di controllare il tipo di traffico che un desktop può ricevere e l'origine e la destinazione del traffico proveniente dal desktop. È inoltre possibile creare zone per isolare i collaboratori esterni e proteggere la rete dalla navigazione su Web ad alto rischio.

Con la microsegmentazione, ciascuna macchina virtuale è dotata di una difesa perimetrale specifica. Un firewall distribuito monitora il traffico di origine e destinazione di ciascuna VM, eliminando gli accessi non autorizzati e assicurandosi che le minacce non si infiltrino nel data center. È possibile automatizzare il provisioning della sicurezza e microsegmentare i carichi di lavoro, consentendo di scalare più rapidamente e in modo più sicuro e incrementando al contempo le prestazioni del desktop virtuale.

10 Limitare l'esposizione soltanto alle strette necessità

Non lasciare mai spazi che sia possibile sfruttare: questo fa riflettere sull'importanza della granularità delle autorizzazioni. Nell'ambiente predefinito, le applicazioni possono avere accesso ad altre applicazioni. Ad esempio, con un malware, un'applicazione potrebbe sovrascrivere la memoria di un'altra applicazione in esecuzione. Questo può provocare danni significativi, in quanto tutte le aree alle quali ha accesso l'applicazione vengono compromesse. Con la virtualizzazione delle applicazioni tramite VMware ThinApp, ciascuna applicazione dispone di un sandbox nel sistema operativo virtuale (VOS) all'interno del quale agire. Di conseguenza, le applicazioni non riescono più a vedersi tra loro o a vedere i propri file e alcune sezioni del sistema operativo possono anche essere isolate dall'applicazione. Di conseguenza, è possibile limitare l'ambito di una possibile infezione e consentire l'eliminazione di tale infezione in caso di violazione.

CONSIDERAZIONI SULLA SICUREZZA OVVIE, MA A VOLTE TRASCURATE:

- Laddove possibile, evitare di concedere diritti di amministrazione agli utenti.
- Gestire la sicurezza dei desktop virtuali con le stesse procedure destinate a quella dei desktop tradizionali, mediante applicazioni anti-virus, applicazione delle policy e strumenti di blocco.
- Sostituire i certificati autofirmati predefiniti per la protezione dei canali SSL con quello generato da un'autorità di certificazione convalidata, per ridurre gli attacchi man-in-the-middle.
- Quando gli utenti utilizzano un secondo desktop virtuale per scopi di accesso remoto o telelavoro, limitare la loro capacità di accedere ai dati sensibili.
- Monitorare i picchi di traffico con VMware vRealize® Operations Manager™.
- Per la distribuzione esterna, distribuire server di sicurezza o server Access Point nella zona demilitarizzata.

Conclusioni

Nonostante tutte le promesse di flessibilità e di efficienza di gestione per gli utenti finali, la trasformazione del desktop di per sé non renderà più sicura l'organizzazione IT. Al contrario, come illustrato, essa può esporre l'organizzazione a problemi di sicurezza più significativi se non è proattiva. Seguendo e mettendo in atto adeguatamente i suggerimenti riportati in questo documento, è possibile incrementare la sicurezza della rete fornendo al contempo tutti i vantaggi per l'IT che la trasformazione del desktop promette.

Ora è possibile provare Horizon gratuitamente grazie a un Hands-on Lab. Puoi attivarlo nel tuo browser in pochi minuti, senza necessità di installazione. Registrazione: https://www.vmware.com/horizon-hol-labs.

Seguici online

Blog: https://blogs.vmware.com/euc

Twitter: @vmwarehorizon

Facebook: https://www.facebook.com/vmwarehorizon

vmware®

VMware, Inc. 3401 Hillview Avenue Palo Alto CA 94304 USA Tel. 877-486-9273 Fax 650-427-5001 www.vmware.com
VMware, Inc. - Via Spadolini, 5 - Edificio A - 20141 Milano - Tel.: (+39) 02 3041 2700 Fax: (+39) 02 3041 2701 www.vmware.it