VMware NSX for Horizon

IN BREVE

VMware NSX™ for Horizon® rende la rete VDI semplice e veloce. Gli amministratori IT sono in grado di creare in pochi secondi policy che seguono dinamicamente i desktop virtuali, evitando i lunghi processi di provisioning della rete. Estendendo la policy di sicurezza dal data center al desktop e alle applicazioni, questa soluzione congiunta fornisce inoltre una piattaforma estensibile che si integra con le soluzioni di sicurezza leader del settore.

VANTAGGI

- Maggiore sicurezza per i desktop virtuali ubicati nel data center insieme ad altri carichi di lavoro.
- Semplificazione e velocizzazione dell'amministrazione della policy di rete e sicurezza degli utenti basata su raggruppamenti logici, ruoli o tag.
- Associazione automatica della policy a un desktop al momento della sua creazione. La policy segue la VM indipendentemente dall'infrastruttura sottostante.
- Integrazione con soluzioni leader del settore per antivirus, malware, prevenzione delle intrusioni e servizi di sicurezza di nuova generazione.

Rete e sicurezza per applicazioni e desktop virtuali: rapidità, semplicità ed estensibilità

Molte aziende ricorrono alla virtualizzazione di desktop e applicazioni per migliorare la sicurezza del client-computing e offrire soluzioni di Enterprise Mobility di livello superiore. La centralizzazione di desktop e applicazioni consente di proteggere i dati inattivi, impedire l'accesso non autorizzato alle applicazioni e fornire un processo più efficiente per il patching, la gestione e l'aggiornamento delle immagini dati.

Tuttavia, con la virtualizzazione di desktop e applicazioni, nuovi problemi di sicurezza possono sorgere alle spalle firewall del data center, dove si trovano centinaia o addirittura migliaia di desktop. Questi desktop sono adiacenti ai carichi di lavoro mission critical e ai desktop di altri utenti, esponendoli al pericolo di malware e altri attacchi che possono spostarsi dal desktop al server, mettendo a rischio una superficie di attacco molto più estesa nel data center. Le minacce "est-ovest" oggi interessano molti clienti, in particolare le aziende con requisiti severi di sicurezza e conformità.

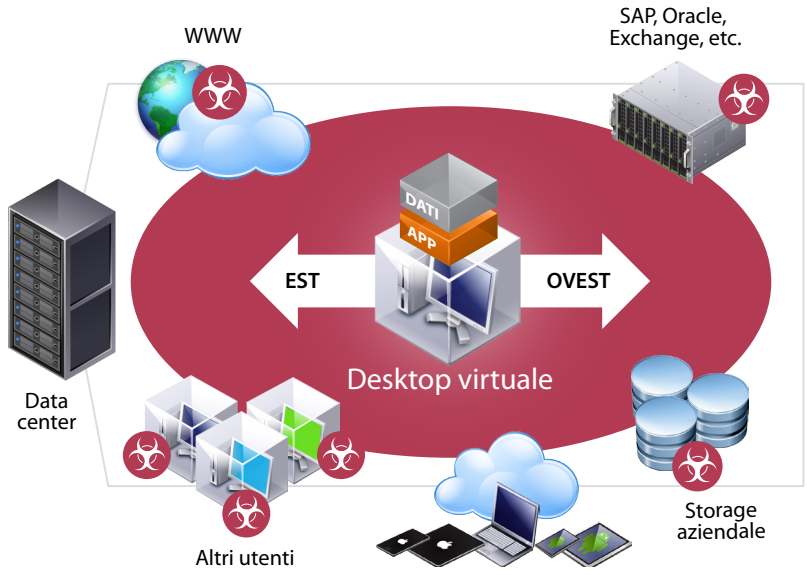

Figura 1: Problematiche di sicurezza inerenti al traffico est-ovest del data center

Le aziende che desiderano amministrare una policy di rete e sicurezza che segua in modo persistente utenti e carichi di lavoro solitamente hanno effettuato importanti investimenti in un'architettura incentrata sull'hardware, costosa in termini di spese di capitale, complessa da gestire e lenta da adattare all'ambiente aziendale dinamico.

VMware NSX for Horizon

VMware NSX for Horizon protegge in modo efficace il traffico est-ovest del data center, garantendo allo stesso tempo all'IT una gestione rapida e semplice della policy di rete e sicurezza che segue dinamicamente le applicazioni e i desktop virtuali degli utenti finali ovunque, su qualsiasi infrastruttura e dispositivo.

Figura 2: NSX for Horizon offre rapidità, semplicità ed estensibilità per la rete e la sicurezza VDI

Con questa soluzione, le aziende possono trarre vantaggio dalla semplicità e dalla rapidità della rete e della sicurezza VDI. Gli amministratori IT sono in grado di creare in pochi secondi policy che seguono dinamicamente i desktop virtuali, evitando i lunghi processi di provisioning della rete.

Estendendo la policy di sicurezza dal data center a desktop e applicazioni, questa soluzione fornisce anche una piattaforma estensibile in grado di integrarsi nell'ecosistema VMware di partner per la sicurezza leader del settore, per fornire ai clienti un livello di sicurezza superiore per la protezione dell'intero desktop.

Funzionamento

VMware NSX for Horizon migliora la sicurezza della virtualizzazione dei desktop e contribuisce a risolvere le problematiche correlate alle minacce est-ovest, consentendo agli amministratori di definire la policy centralmente. La policy viene poi distribuita sul layer dell'hypervisor in ogni host vSphere e associata automaticamente a ogni desktop virtuale al momento della creazione del desktop stesso. Per proteggere i desktop virtuali e i carichi di lavoro adiacenti nel data center, VMware NSX implementa la "microsegmentazione", assegnando o ogni desktop la propria difesa perimetrale. Questa "sicurezza a comparti stagni" utilizza le funzionalità di firewall virtuale distribuito di VMware NSX per controllare il traffico da e verso ogni VM, impedendo l'accesso non autorizzato a desktop e carichi di lavoro adiacenti. Se il desktop virtuale viene spostato da un host a quello successivo o nel data center, la policy lo segue automaticamente.

Funzionalità e vantaggi

VMware NSX for Horizon rende la rete VDI semplice e veloce con una policy di sicurezza che segue dinamicamente gli utenti finali nell'infrastruttura e su qualsiasi dispositivo, ovunque.

Rete VDI semplice e veloce

Con VMware NSX for Horizon, gli amministratori possono creare, modificare e gestione le policy di sicurezza per tutti i desktop virtuali con pochi semplici clic. Le policy di sicurezza possono essere associate rapidamente a gruppi di utenti per velocizzare l'implementazione dei desktop virtuali. Grazie alla possibilità di distribuire funzioni di rete virtualizzate (come switch, routing, firewall e bilanciamento del carico), gli amministratori possono creare reti virtuali per VDI senza la complessità correlata a LAN virtuali, ACL o sintassi di configurazione dell'hardware.

Policy automatizzata che segue dinamicamente utenti finali e desktop

Gli amministratori possono impostare policy che si adattano dinamicamente all'ambiente di elaborazione dell'utente finale, con servizi di sicurezza di rete associati all'utente in base a ruolo, raggruppamento logico, sistema operativo desktop e altri fattori, indipendentemente dall'infrastruttura di rete sottostante. La policy gestita centralmente viene collegata automaticamente a ogni VM desktop al momento della creazione del desktop stesso e segue in modo persistente il desktop virtuale nel data center, offrendo alle aziende scalabilità in assoluta sicurezza.

Piattaforma per una sicurezza avanzata

VMware NSX offre una piattaforma estensibile che può essere integrata con le funzionalità leader del settore offerte da un consolidato ecosistema di partner per la sicurezza. Aggiungendo dinamicamente servizi, la sicurezza dei desktop virtuali può essere estesa dal data center al desktop e all'applicazione. Questo ecosistema di partner, di cui fanno parte tra l'altro Trend Micro, Intel Security e Palo Alto Networks, offre soluzioni per la protezione di sistema operativo, browser, e-mail e altro, con antivirus, malware, prevenzione delle intrusioni e servizi di sicurezza di nuova generazione.

Ulteriori informazioni

Sul sito web VMware e su Twitter sono disponibili ulteriori informazioni su Horizon e VMware NSX.

Risorse su VMware Horizon

Web: http://www.vmware.com/it/products/horizon-view

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

Twitter: @VMwareHorizon

Risorse su VMware NSX

Web: http://www.vmware.com/it/products/nsx/

Blog: http://blogs.vmware.com/networkvirtualization/

Twitter: @VMwareNSX

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