PRESENTAZIONE DELLA SOLUZIONE A CURA DI IDC

Il valore di business delle soluzioni SDN per la sicurezza del data center

Sponsorizzato da: Cisco

Pete Lindstrom
Matthew Marden
Richard L. Villars

May 2015

Panoramica

I CTO, i CIO e gli architetti delle applicazioni devono poter accedere a infrastrutture di data center in grado di gestire la varietà delle offerte di contenuti, i Big Data e l'analisi e le funzioni di archiviazione associate ai sistemi di interazione e analisi dai quali essi dipendono, per servire meglio i clienti e migliorare i risultati del business. Devono potenziare i data center esistenti, accelerare la realizzazione di nuovi data center in nuove aree geografiche e sfruttare al meglio i data center avanzati progettati, costruiti e gestiti dai provider di servizi. IDC definisce questa trasformazione di aziende e data center come il passaggio alla terza piattaforma.

Oggi praticamente tutte le innovazioni del business sono basate sulla terza piattaforma, con centinaia di migliaia, e addirittura milioni, di soluzioni e servizi di grande valore, in grado di trasformare i mercati e l'esperienza dell'utente finale. Il cambiamento interessa tutti gli elementi del reparto IT, tra cui approvvigionamento, progettazione, operazioni, sviluppo e gestione a lungo termine di dati e risorse. Questo nuovo mondo del data center è più dinamico, utilizza i dati in modo maggiormente intensivo e comporta ulteriori rischi per l'azienda che vanno affrontati e superati. Di conseguenza, l'architettura di rete di nuova generazione assume un'importanza vitale.

Questo nuovo modello architetturale deve gestire le limitazioni tecnologiche e operative delle tradizionali architetture di rete e soddisfare le esigenze del data center relativamente ai carichi di lavoro della terza piattaforma. Ad esempio, il Software-Defined Networking (SDN), che consente la separazione del piano di controllo della rete dal piano di inoltro dei dati, è stato concepito come uno strumento in grado di fornire alla rete l'agilità e la flessibilità di cui le aziende hanno bisogno per realizzare gli ambienti di cloud computing.

Cisco Application Centric Infrastructure (ACI) mira a soddisfare l'esigenza degli operatori di data center per quanto riguarda provisioning automatizzato, gestione programmatica e orchestrazione completa. Invece di separare il piano di controllo dal piano dei dati, ACI applica un modello di policy studiato per soddisfare i requisiti applicativi e automatizzare l'implementazione nella rete, a prescindere dal fatto che le applicazioni siano virtualizzate o meno. Cisco definisce questo approccio "modello di gestione dichiarativo". Esso comporta la cooperazione volontaria di persone o agenti che rendono note le proprie intenzioni mediante impegni reciproci. Le intenzioni sono astratte, ad esempio, la policy di un'applicazione dichiara i propri requisiti e l'infrastruttura sottostante (ad esempio gli switch del data center) interpreta il modo in cui soddisfare al meglio tali requisiti in base alle sue capacità intrinseche.

Un'altra opzione di networking per il cloud computing è OpenStack, che comprende un framework predefinito, denominato Neutron, per offrire ai clienti i servizi di rete, e include anche una serie di API northbound e southbound. Il modello di networking OpenStack è dotato di un'architettura modulare, la quale offre a ciascun cliente la flessibilità di selezionare un back-end idoneo per le proprie esigenze. Alcuni clienti iniziano con l'implementazione di riferimento predefinita, ma successivamente adottano estensioni create dai fornitori per soddisfare i propri scenari di utilizzo e le esigenze di networking.

Fattori determinanti della trasformazione del data center

Molti fattori esterni hanno un impatto diretto o indiretto sulle operazioni e gli investimenti dei data center. Si tratta di fattori di mercato, sociali, culturali, politici e tecnologici.

- **Fattori di mercato:**
  - **"Everything as a service":** il cambiamento dei modelli per il finanziamento di risorse fisiche e digitali è alla base dell'evoluzione delle pratiche interne di gestione di budget, costi e investimenti.
  - **Digitalizzazione dei mercati:** la transizione dal modello di business fisico a quello digitale determina un notevole aumento dei volumi di dati, delle esigenze prestazionali e dei requisiti funzionali dell'IT.
  - **Complessità dei rapporti di business:** gli ecosistemi di partnership favoriscono la standardizzazione dell'interconnessione e la condivisione dei dati tra aziende e settori diversi.
- **Fattori sociali/culturali/politici:**
  - **Norme sull'utilizzo dei dati:** le opinioni personali e le politiche governative in materia di raccolta, conservazione e utilizzo di dati personali e proprietà intellettuale diventano instabili e frammentarie.
  - **Sfruttamento dei dati:** le nazioni, le aziende e il crimine organizzato sono tutti coinvolti nella guerra informatica.
  - **Interazione con i clienti:** i social media favoriscono l'interazione diretta cliente-azienda e cliente-cliente, che genera l'esigenza di avere informazioni sempre nuove e aggiornate.
- **Tecnologia:**
  - **IT modulare:** i modelli di servizi cloud, convergenti, definiti dal software e di iperscala cambiano le modalità di acquisto e gestione delle unità base dell'IT.
  - **Importanza dei dati:** i dati utilizzati per interagire con i clienti e ottenere informazioni preziose per il business vengono generati, raccolti e archiviati nei data center dei provider di servizi in misura sempre maggiore.
  - **IT variabile:** le esigenze di supporto IT per i progetti di mobilità e analisi dei dati a breve termine obbligano le aziende ad acquistare, implementare e re-implementare le risorse in tempi brevi e per periodi di tempo ridotti.

Il riallineamento e il ribilanciamento di data center e risorse IT stimolati da queste forze hanno importanti conseguenze anche per le attuali reti estese delle aziende. Le aziende dovranno cambiare i percorsi di connessione esistenti per collegare i data center interni alle strutture di terze parti. Devono anche occuparsi dei notevoli cambiamenti del volume di traffico e della variabilità del traffico stesso, in quanto le aziende hanno l'esigenza di spostare grandi volumi di informazioni tra molte sedi e con modelli meno prevedibili.

Il ruolo della sicurezza nel data center moderno

Un denominatore comune di questi fattori determinanti e dei cambiamenti dei carichi di lavoro dei data center è la necessità di maggiore agilità e flessibilità per la sicurezza del data center. In ciascun scenario di utilizzo, il concetto di sicurezza assume un significato diverso: integrità, fedeltà, visibilità, controllo del contenuto e dei dati. I reparti IT hanno bisogno di una piattaforma comune che possono utilizzare per impostare, reimpostare ed estendere in modo rapido e affidabile un'ampia gamma di funzioni di sicurezza all'interno dei data center e dell'intera azienda.

A livello di rete, le funzionalità di sicurezza integrate comprendono la capacità di monitoraggio (rilevamento delle intrusioni), la segmentazione in base alle policy (firewall) e la crittografia delle comunicazioni (rete privata virtuale). Tuttavia, spesso le imprese trattano le risorse dei data center come un'unità, senza fare alcuna distinzione tra i livelli di utilizzo e di rischio. Questo approccio consente alle imprese di collocare tutte le risorse in un'unica grande "zona" e di concentrare la protezione sui punti di ingresso/uscita perimetrali (talvolta definiti i punti di accesso "nord" e "sud" del data center).

Mano a mano che i data center si espandono e si evolvono fino a formare insiemi di risorse con caratteristiche diverse, fornendo funzioni differenti per linee di business, gruppi di utenti o tipi di piattaforme diversi, la sicurezza deve evolversi di pari passo, in modo da proteggere dalle minacce mirate queste risorse più dinamiche ed evolute. Le imprese devono valutare come condividere le risorse e come monitorare e crittografare le comunicazioni a un livello più granulare.

Il data center moderno deve valutare come implementare i propri sistemi di rilevamento e prevenzione delle intrusioni, così come la segmentazione dei firewall, per determinare i casi in cui occorre implementare nuovamente i controlli esistenti e se sia necessario aggiungere nuove funzionalità per gestire le comunicazioni a "est" e a "ovest" che avvengono tra server e altre risorse. Parte integrante di questo approccio è individuare gli insiemi di risorse più piccoli, tipicamente a livello di applicazione, ma non solo, e introdurre un numero maggiore di funzioni di monitoraggio e controlli di policy per gestire il traffico tra le applicazioni.

Con l'implementazione nel data center di ulteriori controlli, le funzionalità di gestione centralizzata diventano un'esigenza imprescindibile. La posizione delle risorse da proteggere e il modo in cui vengono utilizzate sono sempre più dinamici, pertanto le funzioni di sicurezza devono adattarsi alle nuove architetture.

Questa presentazione della soluzione a cura di IDC è basata sulle ricerche svolte da IDC tra gli utenti dei prodotti di sicurezza dei data center. Lo studio quantifica i possibili vantaggi a livello di business, tra cui un aumento della produttività del 33,5% per quanto riguarda le operazioni del personale addetto alla sicurezza IT, una riduzione dell'80,7% delle interruzioni non pianificate dei servizi a causa di violazioni e minacce, nonché un'implementazione della sicurezza più veloce del 63,8% per nuove applicazioni e servizi. Su base annuale, per un'azienda con 1.000 utenti, ciò comporta un miglioramento dell'affidabilità pari a 48.700 dollari, un aumento dell'efficienza del personale IT pari a 71.700 dollari e un aumento dei tempi di produzione, reso possibile dal miglioramento delle operazioni, pari a 92.600 dollari.

I vantaggi per il business delle soluzioni di sicurezza per i data center di nuova generazione

Le soluzioni di sicurezza per i data center di nuova generazione devono consentire alle aziende di massimizzare il valore di business dei propri investimenti in tali data center. Per apportare valore, le soluzioni di sicurezza devono essere integrate, basate su policy, solide, flessibili e scalabili. Le soluzioni di sicurezza ben progettate, ben implementate e che rispondono a questi requisiti creano valore poiché consentono di risparmiare tempo e risorse per la gestione e il provisioning, riducono l'impatto delle minacce su operatività e business e non ostacolano la capacità del data center di supportare e dare impulso all'azienda. Di conseguenza, queste soluzioni di sicurezza offrono le seguenti caratteristiche per supportare i data center di nuova generazione.

- **Sono integrate per aumentare l'efficienza e ridurre i rischi.** I prodotti di sicurezza che si integrano sia con le soluzioni che supportano i tradizionali ambienti di data center dell'azienda che con gli altri prodotti di sicurezza utilizzati nell'ambiente dei data center di nuova generazione permettono di risparmiare tempo e ridurre i rischi. Con l'integrazione si riduce al minimo il tempo che i team addetti alla sicurezza devono dedicare a ridefinire le policy, si eliminano i costi e le inefficienze degli ambienti IT isolati e si riduce il tempo di esposizione di applicazioni e servizi a potenziali minacce per la sicurezza.
- **Sono semplici per alleggerire il carico gestionale.** I prodotti di sicurezza nei data center di nuova generazione sono utilizzati in ambienti basati su automazione e orchestrazione. Per essere compatibili con tali ambienti devono basarsi su policy per consentirne il provisioning come servizio. In questo modo, non solo è supportata l'architettura globale dei data center di nuova generazione, ma aumenta anche la produttività del personale addetto alla sicurezza IT, che può ridurre il tempo dedicato all'amministrazione e alla gestione delle impostazioni, della configurazione e delle implementazioni della sicurezza.
- **Offrono funzionalità solide, per ridurre al minimo l'impatto delle minacce per la sicurezza.** I prodotti di sicurezza nei data center di nuova generazione devono fornire funzionalità di sicurezza complete, che garantiscano la copertura di tutto il traffico in entrata, in uscita e all'interno del data center. Le aziende possono così ridurre al minimo l'impatto delle minacce sugli utenti e sul business, migliorando la produttività e riducendo al minimo le interruzioni delle attività.
- **Sono flessibili e scalabili per supportare il business tramite le applicazioni.** I data center di nuova generazione sono configurati per facilitare le operazioni aziendali accelerando i cicli di sviluppo delle applicazioni e alleggerendo il carico gestionale delle applicazioni. Al fine di raggiungere questo obiettivo, i prodotti di sicurezza devono essere implementabili a seconda delle necessità e nel minor tempo possibile, per ridurre il time-to-market di applicazioni e servizi.

Cisco Application Centric Infrastructure

Le reti SDN separano le funzioni del piano di controllo dalle funzioni del piano dati e spesso sono definite in termini strettamente tecnici. La sicurezza definita dal software si basa sui principi e sull'architettura di base di SDN, ma ne espande la potenzialità grazie alla capacità di integrazione in più ambienti. L'approccio "hub-and-spoke" di SDN associa un controller, in cui le policy di sicurezza sono definite e valutate, ai nodi che implementano le policy. Il tutto dinamicamente e in tempo reale. Usare un linguaggio di policy astratto rispetto al livello dell'applicazione consente di implementare i criteri applicabili nei nodi appropriati, il che assicura flessibilità e allineamento rispetto ai componenti dell'applicazione in uso. Ne consegue un'architettura più efficace dal punto di vista della sicurezza e più facile da gestire in modo efficiente.

Cisco Application Centric Infrastructure consente di soddisfare le esigenze di un moderno data center a livello di dati e sicurezza. Tale infrastruttura è gestita da un controller centrale, l'APIC. Esso controlla tutti i dispositivi di sicurezza del data center, sia fisici che virtuali, in modo tale che essi possano essere gestiti accuratamente e allineati alle risorse da proteggere. Tale controller è in grado di definire e gestire i dispositivi di sicurezza e di rete Cisco, supporta un ecosistema di fornitori di soluzioni di sicurezza di terze parti e integra ulteriori funzionalità per assicurare supporto aggiuntivo.

Grazie alla sua capacità di sfruttare l'architettura di sicurezza esistente di un'azienda, Cisco ACI consente alle imprese di preservare l'investimento esistente in controlli di sicurezza fisica, aggiungendo al tempo stesso altri controlli funzionali nei sistemi hardware o virtuali, per proteggere le comunicazioni est-ovest, sempre più importanti. Per gestire le risorse dinamiche di un'impresa moderna, le policy possono essere create, abbinate in base a un profilo di applicazione e quindi distribuite all'interno di un ambiente. In tal modo, quando le risorse vengono spostate, con esse si sposta anche la policy corretta.

Per le aziende che hanno già effettuato un investimento significativo nelle soluzioni di sicurezza Cisco e che hanno già predisposto una serie ben definita di policy di sicurezza, ACI consente di far evolvere l'architettura del data center, piuttosto che modificarla radicalmente. Allo stesso tempo, questa infrastruttura può soddisfare le nuove esigenze delle architetture virtualizzate e distribuite per garantire all'impresa che il livello di sicurezza sia sempre quello più appropriato.

Quantificare i vantaggi per il business delle soluzioni di sicurezza per i data center di nuova generazione

La tabella 1 indica le metriche relative al valore di business ottenibile dalle aziende che utilizzano le soluzioni di sicurezza nei data center di nuova generazione, in base alle ricerche IDC in corso.

La figura 1 mostra il valore annuo dell'aumento della produttività del personale IT e degli utenti relativamente all'utilizzo delle soluzioni di sicurezza nei data center di nuova generazione per un'azienda con 1.000 utenti.

TABELLA 1

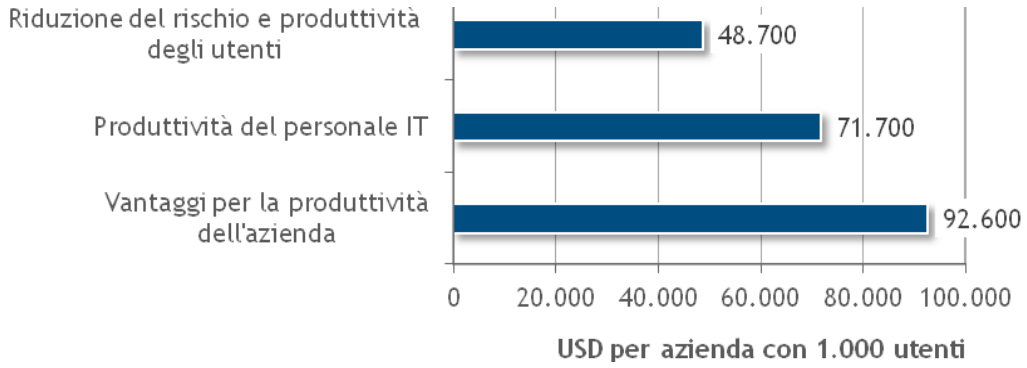
Miglioramenti derivanti dall'utilizzo di prodotti per la sicurezza nei data center di nuova generazione

	(%)
Vantaggi per la produttività del personale IT	
Riduzione dei tempi di gestione della sicurezza	33,5
Aumento delle minacce per la sicurezza identificate proattivamente	50,9
Riduzione dei tempi di risposta alle minacce per la sicurezza	82,1
Vantaggi per la riduzione del rischio e la produttività degli utenti	
Riduzione delle interruzioni non pianificate dei servizi	80,7
Vantaggi per la produttività dell'azienda	
Riduzione dei tempi di implementazione della sicurezza	63,8

Fonte: IDC, 2015

FIGURA 1

Vantaggi annui tipici per un'azienda con 1.000 utenti che utilizza soluzioni di sicurezza per i data center di nuova generazione



Fonte: IDC, 2015

Appendice: metodologia

IDC ha raccolto i dati utilizzati in questo documento tramite i sondaggi che conduce ogni anno presso le aziende che utilizzano soluzioni di sicurezza per i propri data center. I risultati del valore di business sono stati normalizzati esprimendoli in termini di vantaggi in dollari per un'azienda media con un reparto IT che supporta 1.000 utenti finali. Per quantificare i vantaggi relativi alle operazioni del personale IT, IDC ha moltiplicato i risparmi di tempo e le efficienze per uno stipendio lordo medio annuo di 100.000 USD, mentre per quantificare i risparmi di tempo e la maggior produttività per gli altri dipendenti non appartenenti al reparto IT ha utilizzato uno stipendio lordo medio annuo di 70.000 USD.

Informazioni su IDC

International Data Corporation (IDC) è un'azienda leader a livello mondiale per le ricerche di mercato, i servizi di consulenza e gli eventi per i mercati delle telecomunicazioni, dell'IT e dei prodotti tecnologici di consumo. IDC offre supporto ai professionisti IT, ai vertici aziendali e alla comunità degli investitori per l'acquisto di tecnologia e per la definizione delle strategie aziendali. Oltre 1.100 analisti di IDC offrono servizi di consulenza a livello locale, regionale e mondiale sulle tendenze e sulle opportunità delle tecnologie e del settore in oltre 110 paesi in tutto il mondo. Da più di 50 anni IDC fornisce informazioni strategiche per supportare i clienti a realizzare i propri obiettivi aziendali. IDC è una società controllata da IDG, l'azienda leader mondiale nel settore degli eventi, della ricerca e delle comunicazioni in materia di tecnologia.

Sede principale

5 Speen Street
Framingham, MA 01701
Stati Uniti
508.872.8200
Twitter: @IDC
idc-insights-community.com
www.idc.com