Akamai

WHITE PAPER

La nuova concezione dei firewall

Un convincente caso economico per la segmentazione basata su software

Analisi riassuntiva

Perché i team di rete e sicurezza si affidano ancora ai firewall legacy per eseguire la segmentazione della rete interna? Con la proliferazione di applicazioni e segmenti protetti da policy, le appliance firewall fisiche si stanno dimostrando troppo complesse, poco flessibili e semplicemente inefficaci per affrontare le sfide di sicurezza degli odierni ambienti cloud ibridi sempre più dinamici. E sono molto più costose di quanto i team possano prevedere. A parte gli elevatissimi costi iniziali di firewall e hardware, vi sono molti costi significativi a valle dovuti alla gestione di progetti, manodopera, manutenzione e al rischio molto reale di un'esposizione prolungata delle risorse a causa dei lunghi tempi di implementazione. Se le aziende moderne vogliono sfruttare i vantaggi di un modello DevOps flessibile, una rapida implementazione delle applicazioni e del cloud, deve esserci un modo migliore per proteggere le risorse critiche con la segmentazione. Ora c'è: la segmentazione basata su software. È più facile, più veloce, più efficace e, come dimostrerà chiaramente questo documento, offre una sicurezza ottimale a un costo totale di proprietà molto inferiore rispetto ai tradizionali metodi di segmentazione.

Introduzione

Sono tre le tendenze che oggi contribuiscono a determinare la necessità di uno strumento più granulare per segmentare le reti e le singole risorse. In primo luogo, un modello DevOps flessibile e altri modelli di delivery rapida stanno privilegiando l'implementazione accelerata delle applicazioni in produzione. Ciò richiede inevitabilmente la creazione di zone più sicure con policy più precise. In secondo luogo, quando le organizzazioni migrano al cloud e adottano infrastrutture IT ibride, spesso migrano le applicazioni in ambienti diversi, il che aumenta il traffico intersegmento in tutta la loro rete. E in terzo luogo, la rapida proliferazione di applicazioni dovuta allo sviluppo flessibile sta creando una superficie di attacco sempre maggiore che gli hacker possono prendere di mira.

I firewall per la segmentazione: hanno fatto il loro tempo

Date queste condizioni, una forte dipendenza da VLAN e firewall per scopi di segmentazione sta diventando insostenibile. Da un punto di vista puramente tecnico, la configurazione di più installazioni VLAN e firewall in modo da tenere il passo con lo sviluppo delle applicazioni è complessa e ingombrante. È anche estremamente laboriosa, sottraendo troppi membri del team da progetti di sicurezza ad alta priorità. Il tempo di implementazione è un altro problema, che aumenta il rischio di esposizione e vulnerabilità prolungate delle risorse. E, soprattutto, è estremamente costosa da implementare, non solo a causa dei costi iniziali dei firewall e del nuovo hardware per supportare il traffico aggiuntivo, ma anche a causa dei costi associati alla gestione continua, alle modifiche e alla manutenzione delle installazioni.

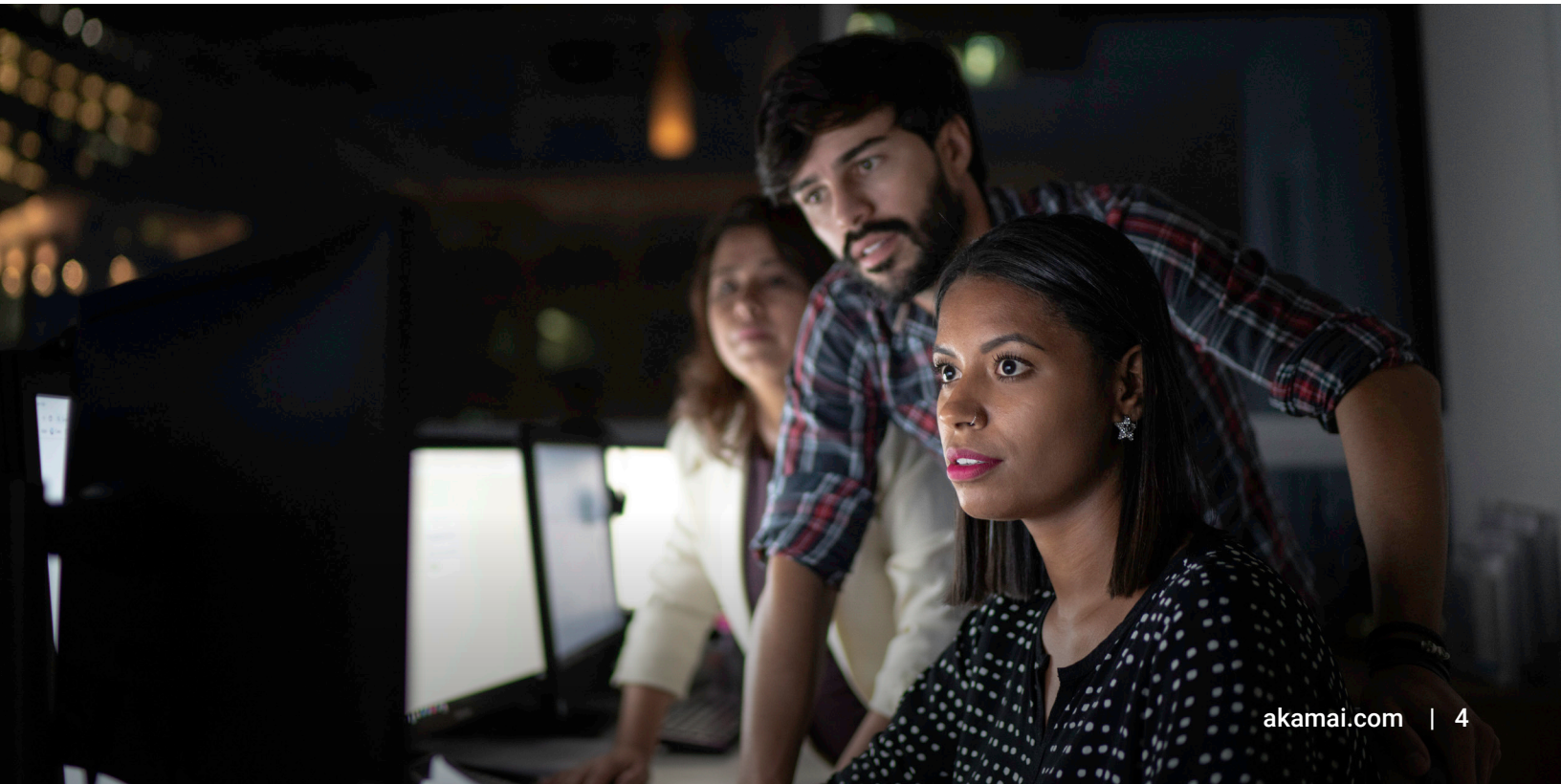
In poche parole, gli approcci tradizionali alla segmentazione della rete non sono più sufficienti. In particolare, poiché le organizzazioni cercano di trarre vantaggio da ambienti cloud e ibridi dinamici, l'affidamento a firewall interni per la sicurezza ne limita la flessibilità, la velocità di creazione e applicazione delle policy e la capacità di ridimensionare in modo sicuro le proprie operazioni. La necessità di un'alternativa di segmentazione moderna, semplificata, meno costosa e in definitiva più efficace ai firewall legacy non è mai stata così urgente. Adottate la segmentazione basata su software.

La necessità di un'alternativa di segmentazione moderna, semplificata, meno costosa e più efficace ai firewall legacy non è mai stata così urgente.

Complessità: il compito costoso di gestire i firewall

Prima di approfondire i vantaggi della segmentazione basata su software, è utile confrontarla con lo status quo. Man mano che un'azienda cresce, crescono anche il numero di applicazioni e la quantità di traffico dati associato, determinando la domanda di ulteriori segmenti di rete e policy di sicurezza più complesse. Se vi affidate a VLAN protette da firewall, ciascuna nuova rete implementata deve essere aggiunta a ogni porta trunk dello switch a cui è assegnato il traffico tra i segmenti. È necessario creare anche una sottorete IP per ogni nuova VLAN. È inoltre necessario creare un'interfaccia secondaria per il firewall. Infine, è necessario creare policy per il firewall. Ognuna di queste modifiche di solito richiede approvazioni, finestre di manutenzione e la possibilità di downtime, il che significa un aumento del rischio di interruzione della rete.

L'aggiunta di VLAN e firewall comporta un complesso processo in più fasi che coinvolge fino a cinque team, responsabili separatamente di gestione degli switch, instradamento, implementazione del firewall, server ESXi e creazione delle policy di sicurezza. Tutto ciò aumenta la durata dell'implementazione, espone l'organizzazione a rischi prolungati e determina un aumento dei costi di software, hardware e manodopera. Inoltre, dal punto di vista tecnico, si tratta di un lavoro ad alto rischio e a basso rendimento: molta complessità per un guadagno minimo, che sottrae tempo e risorse da altre attività di gestione del rischio ad alta priorità. Sfortunatamente, poche delle fasi del processo di gestione delle modifiche all'interno dell'ambiente VLAN protetto da firewall si prestano all'automazione.



Trovare la soluzione: segmentazione basata su software in tre semplici passaggi

La tecnologia del firewall perimetrale legacy semplicemente non è mai stata concepita per le esigenze più precise e limitate della larghezza di banda della segmentazione interna granulare. La segmentazione basata su software è emersa negli ultimi anni come un'alternativa praticabile, più veloce, più efficace e a basso costo per soddisfare la domanda di segmenti di rete più numerosi e più compatti negli ambienti dinamici di oggi. Fondamentale per l'implementazione della segmentazione basata su software è il concetto di "firewall distribuito", molto più agile e facile da gestire rispetto a un'appliance firewall di rete tradizionale.

> La segmentazione basata su software consente un'implementazione **10 o anche 20 volte più veloce** rispetto ai firewall tradizionali, con meno personale necessario e praticamente senza downtime o interruzioni.

Un esempio di soluzione di segmentazione basata su software leader del settore è Akamai Guardicore Segmentation. Rispetto al lungo, costoso e complesso processo di implementazione del firewall VLAN, la nostra soluzione di segmentazione basata su software richiede solo tre passaggi:

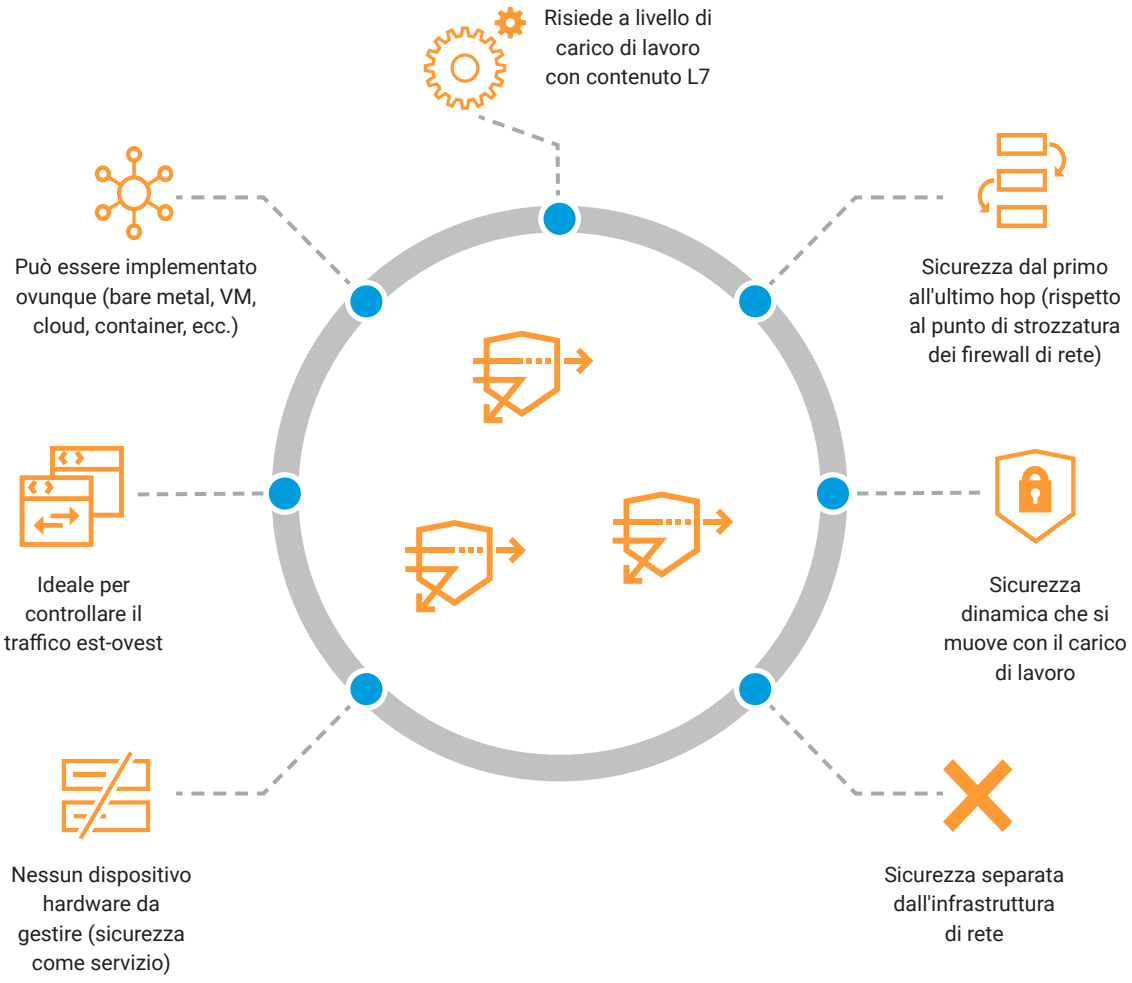
1. **Identificazione ed etichettatura delle risorse:** uno dei principali ostacoli incontrati durante il tradizionale processo di implementazione dei firewall è la mancanza di visibilità delle risorse che devono essere protette. Akamai Guardicore Segmentation include una funzionalità di visualizzazione che consente agli operatori di identificare ed etichettare tutte le applicazioni e le relative dipendenze in esecuzione nell'infrastruttura di un'organizzazione.

2. **Visualizzazione e raggruppamento per etichetta:** una volta ottenuta la visibilità contestuale, gli operatori possono quindi organizzare le applicazioni in gruppi logici in base alle etichette e mappare le relative dipendenze. Il nostro processo di etichettatura è molto flessibile e consente di raggruppare le applicazioni in base al proprio contesto aziendale, utilizzando una terminologia già nota.

3. **Creazione di policy:** gli operatori possono quindi creare policy di sicurezza granulari che determinano quali applicazioni sono autorizzate a comunicare tra loro in base ai flussi effettivamente osservati. I modelli di policy predefiniti per i casi di utilizzo comuni semplificano ulteriormente il processo. Le applicazioni e i workflow risultano così ben segmentati, indipendentemente da dove si trovano all'interno dell'ambiente.

La segmentazione basata su software è 10 o anche 20 volte più veloce da implementare rispetto al firewall tradizionale, con meno personale necessario e praticamente senza downtime o interruzioni. Inoltre, una volta avviato il processo di visualizzazione e segmentazione, potete facilmente suddividere ulteriormente la vostra rete o aggiungere diverse policy basate su etichette, automatizzare i processi, risolvere gli incidenti di sicurezza e apportare modifiche rapide in risposta ai requisiti aziendali o normativi.

Vantaggi del firewall distribuito



Case study: Una grande produttore alimentare ottiene un risparmio dell'85% con la segmentazione

Un importante produttore di prodotti a base di carne di maiale statunitense doveva segmentare 45 applicazioni con una media di cinque server per applicazione, distribuiti in due sedi. L'obiettivo dell'azienda era quello di eliminare le sue reti semplici, con un'interruzione minima del servizio, e applicare policy il più rapidamente possibile.

Dopo aver esaminato le alternative, l'azienda ha scelto la soluzione di segmentazione basata su software di Akamai. Sebbene la velocità e la semplicità di implementazione abbiano influito sulla decisione, il fattore decisivo è stata un'analisi che mostrava un risparmio di oltre 900.000 dollari (o dell'85%) in un periodo di tre anni, rispetto alla protezione delle VLAN con un fornitore leader di firewall. In particolare:

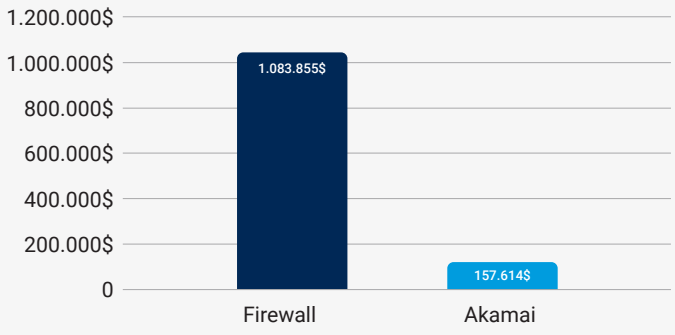
- il costo della licenza di Akamai Guardicore Segmentation era inferiore del 55% rispetto al costo dell'hardware per l'implementazione di un firewall VLAN.
- Il costo di manodopera, basato su un'ipotesi di 2.000 dollari a settimana, con Akamai era inferiore del 93% rispetto a un progetto VLAN con una durata molto più lunga.

Inoltre, Akamai ha soddisfatto l'esigenza del cliente di implementare rapidamente le policy, proteggendo 45 applicazioni senza interruzioni in sole sei settimane.

TCO del firewall*
1.083.855$

TCO di Akamai*
157.614$
-926.241$

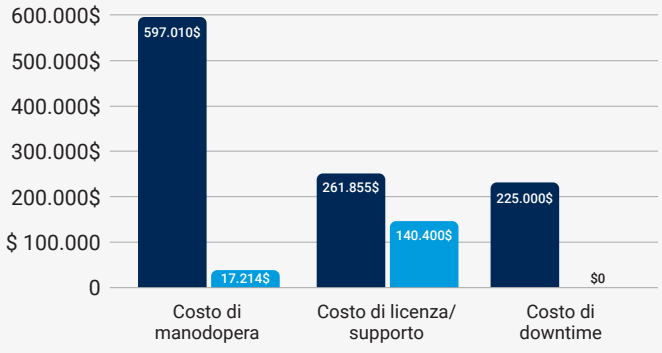
* Costo su un periodo di 3 anni



Costo di manodopera Akamai*
17.214$
-579.796$

Costo di licenza/supporto Akamai*
140.400$
-121.455$

Costo di downtime Akamai*
$0
-255.000$



In buona sostanza

La segmentazione basata su software offre tre vantaggi principali rispetto ai tradizionali metodi firewall:

Riduzione dei rischi più efficace: consentendo una rapida segmentazione delle applicazioni a un livello molto granulare, la segmentazione basata su software si traduce in una superficie di attacco notevolmente ridotta. Sfruttando i principi Zero Trust, che richiedono un'autenticazione rigorosa di qualsiasi utente, dispositivo o applicazione che tenti di accedere a una risorsa di rete, la segmentazione basata su software contrasta il movimento laterale delle minacce all'interno del data center o dell'ambiente di rete. Ciò mitiga ulteriormente l'impatto delle violazioni dei dati, impedendo agli autori di attacchi di acquisire il controllo dei processi anche se sono riusciti ad aggirare i sistemi di difesa perimetrali. Consente inoltre alle aziende di ottenere più rapidamente la conformità alle normative che richiedono il distinto isolamento delle applicazioni critiche e sensibili dal traffico di rete generale.

Velocità per una strategia di sicurezza ottimale: in breve, la segmentazione basata su software aumenta il vostro livello di protezione, consentendo più rapidamente ai team di sicurezza di stare al passo con l'implementazione delle applicazioni del modello DevOps flessibile e di garantire che ogni applicazione in produzione sia adeguatamente protetta. Significa anche l'impiego di meno risorse, tecniche o umane, in progetti di segmentazione per lunghi periodi. I team possono concentrare il proprio tempo su altre importanti iniziative.

Costo totale di proprietà notevolmente inferiore: questo è il vero fattore decisivo e probabilmente il vantaggio più significativo dal punto di vista aziendale. La segmentazione basata su software può essere ottenuta con una spesa in conto capitale (CapEx) molto inferiore per una soluzione software rispetto all'acquisto di appliance firewall e hardware aggiuntivo. Inoltre, assicura anche minori spese operative (OpEx) nel tempo in termini di risparmio di manodopera e risorse per la manutenzione e la gestione continue.

Solo in base a queste misure, in un confronto affiancato tra la segmentazione basata su software e una soluzione firewall per 10 segmenti applicativi, l'approccio di Akamai ha dimostrato di offrire un potenziale risparmio totale dell'85%, pari a circa 1 milione di dollari.

Naturalmente, anche se ci si può aspettare di ottenere risparmi misurabili nella prima settimana di implementazione, il costo totale di proprietà (TCO) è molto più significativo del semplice prezzo di acquisto anticipato o dei costi vivi continui. Anche se i vantaggi completi in termini di prezzo possono non essere immediatamente evidenti, la segmentazione basata su software produce risparmi sostanziali eliminando virtualmente il downtime e l'interruzione del servizio. Inoltre, le imprese eviteranno perdite finanziarie derivanti da violazioni dei dati, nonché sanzioni in caso di non conformità. E riducono notevolmente il rischio di danni alla reputazione e perdita di profitti a seguito di una violazione. I team e le risorse IT possono essere ridistribuiti dalla gestione delle modifiche al firewall a progetti più produttivi. Tutti questi fattori di costo contribuiscono a un TCO inferiore e a una redditività più solida per chi opta per una soluzione di segmentazione basata su software.

Case study: una grande banca globale, che deve affrontare sanzioni di conformità, si rivolge ad Akamai Guardicore Segmentation

A seguito di una verifica che ha rilevato rischi per la sicurezza nelle sue reti semplici e di fronte a un corpus di nuove normative che richiedono una segmentazione più rigorosa, un importante istituto finanziario europeo ha avviato un progetto di segmentazione utilizzando VLAN e regole firewall. Questo progetto si stava protraendo notevolmente, richiedendo l'attenzione di più parti interessate e team, causando downtime della produzione e ambiguità delle policy. Di conseguenza, la banca stava pagando sanzioni a causa della mancata conformità, oltre ai costi di implementazione insostenibilmente elevati.

Il team IT ha cercato rapidamente soluzioni alternative ed è rimasto impressionato dal livello di automazione che Akamai poteva apportare alle sue operazioni di sicurezza. La banca ha implementato Akamai Guardicore Segmentation in più regioni e tipi di infrastrutture IT. Il completamento del progetto ha richiesto meno di tre mesi: è stato 10 volte più veloce di quanto inizialmente stimato con i metodi di segmentazione tradizionali. La banca non solo ha migliorato il proprio livello di sicurezza, ma ha anche soddisfatto i requisiti di conformità per oltre 10.000 risorse. La rapida implementazione ha comportato un'accelerazione della riduzione dei rischi, insieme a un notevole risparmio di costi e risorse interne.

Una grande banca globale

Obiettivo del progetto:

separazione di Dev/Prod/UAT

Ambito del progetto:

1. Limitazione del traffico tra gli ambienti di produzione e non di produzione
2. Tempestività di isolamento delle app

Segmentazione tradizionale

- Progressi estremamente lenti
- Errori di verifica, multe ed errori di produzione
- Interruzioni della produzione dovute a downtime dell'applicazione

Tempo: 2 anni con firewall/VLAN

Impatto di Akamai

- 10.000 risorse non conformi segmentate
- Zero downtime delle applicazioni
- Implementazione 10 volte più rapida
- Attività manuali ridotte con DevOps

Tempo: 6 mesi
Personale: 3 architetti

Conclusione: sommate tutto questo

I firewall non sono obsoleti. Hanno sicuramente un ruolo da svolgere nella protezione del perimetro della rete. Ma negli ambienti dinamici di oggi, il perimetro è diventato un concetto in qualche modo amorfo. Per raggiungere il necessario equilibrio tra sicurezza e flessibilità, le organizzazioni devono essere in grado di proteggere le proprie risorse digitali non solo a livello di rete L4, ma anche a livello di applicazione L7, in particolare i singoli processi. E i firewall non sono solo inadatti a tale scopo, ma in realtà ostacolano il progresso. Tentare una segmentazione granulare con i firewall comporta un elevatissimo impiego di risorse: umane, tecniche e finanziarie.

Rispetto ai firewall, la segmentazione basata su software ha dimostrato di ridurre notevolmente i rischi per la sicurezza e il time-to-value complessivo con un TCO notevolmente inferiore rispetto agli approcci tradizionali, il che si traduce in un maggiore ROI ottenuto più rapidamente. Non si tratta di una visione futuristica: la segmentazione basata su software è praticabile e sta attualmente offrendo questi vantaggi alle organizzazioni in un'ampia gamma di settori.

Uno studio sull'evoluzione dell'IT

La storia della tecnologia è una storia di costante miglioramento, semplificazione e riduzione dei costi. La segmentazione non fa eccezione.

Considerate l'esempio dello storage, che in appena due decenni si è evoluto da floppy disk a unità flash, quindi NAS (Network Attached Storage) e infine lo storage nel cloud. O il runtime di calcolo, che si è evoluto dai server alle macchine virtuali, dal cloud computing ai container e, infine, al computing senza server. In ogni caso, i fattori chiave sono stati il risparmio sui costi e una maggiore flessibilità. E, naturalmente, i rapidi progressi tecnologici lo hanno reso possibile.

L'evoluzione della segmentazione, dalle appliance firewall fisiche ai firewall distribuiti basati su software e astratti dalla rete, segue un percorso analogo. E i fattori determinanti sono gli stessi: costi ridotti e maggiore flessibilità (ovvero velocità di implementazione), con conseguente miglioramento continuo dell'efficacia delle policy di sicurezza, grazie a un approccio più granulare che supporta il modello Zero Trust.

È ora che i team di rete e sicurezza adottino un nuovo modello per la protezione con la segmentazione, come hanno chiaramente fatto in altri settori tecnologici. Il firewall fisico per la segmentazione ha lo stesso destino del floppy disk.

Volete vedere la nostra soluzione in azione?
Richiedete subito una demo: akamai.com/guardicore

Akamai protegge l'experience dei vostri clienti, dipendenti, sistemi e dati aiutandovi ad integrare la sicurezza in tutti i vostri prodotti, ovunque vengano creati e distribuiti La visibilità della nostra piattaforma sulle minacce globali ci aiuta ad adattare e a migliorare la vostra strategia di sicurezza (per favorire l'adozione del modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS), offrendovi la sicurezza necessaria per concentrarvi sull'innovazione, sull'espansione e sulla trasformazione dell'azienda in modo continuativo. Per ulteriori informazioni sulle soluzioni per la sicurezza, il computing e la delivery di Akamai, visitate il sito akamai.com e akamai.com/blog o seguite Akamai Technologies su Twitter e LinkedIn. Data di pubblicazione: 05/23.