Akamai

WHITE PAPER

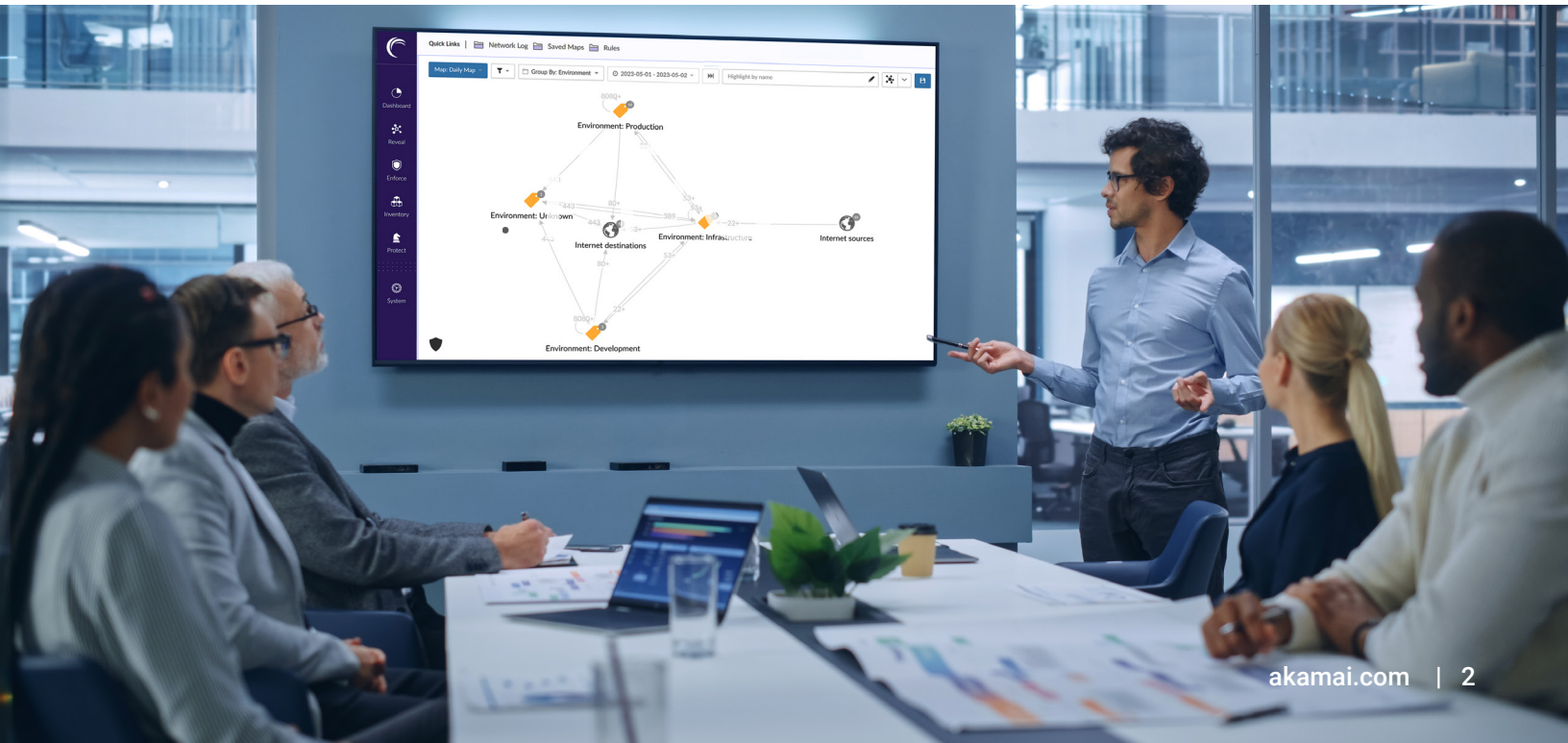
Segmentazione definita dal software per gli operatori dei data center

Per gli operatori di data center multi-tenant, la segmentazione degli ambienti informatici non è solo importante, ma è fondamentale per il loro modello operativo. Prima di tutto, la loro infrastruttura va separata dagli ambienti dei clienti per consentire la condivisione di alcune risorse e impedire l'accesso ad altre risorse. In secondo luogo, va evitata la "contaminazione crociata" tra gli ambienti dei loro clienti, sia accidentale che dannosa, inclusa la prevenzione di violazioni o infezioni da malware che dall'ambiente di un cliente possono diffondersi all'ambiente di altri clienti. Infine, all'interno delle applicazioni operative proprietarie, è richiesto un buon livello di separazione per limitare l'impatto di una potenziale violazione. Analizzando approfonditamente le reti operative dei provider di data center, esistono tre scenari in cui la segmentazione, se realizzata in modo efficiente, può migliorare significativamente la sicurezza e ridurre i costi.

1. **Separare le reti operative** (DCIM, BMS, ecc.) dalla rete aziendale (sistemi interni del fornitore, inclusa la fatturazione) e dalle reti dei clienti

2. **Ridurre il rischio di movimenti laterali all'interno della rete operativa,** che presenta molti sistemi a cui è difficile applicare patch e introduce rischi, se non adeguatamente segmentata

3. **Creare una connettività efficiente e sicura tra le reti per i clienti**, come la DMZ, in cui risiede il portale personalizzato, che necessita di un accesso sicuro ai dati provenienti dalle reti operative (ad esempio, per la lettura dello stato di alimentazione) e dalle reti aziendali (per la lettura delle informazioni di fatturazione)



Oggi, queste soluzioni vengono gestite tramite strutture di rete molto complesse, lente da implementare e inefficienti, VLAN, reti intermedie, ecc. L'implementazione di una soluzione definita dal software, senza basarsi su configurazioni di rete complesse, consentirà di ridurre notevolmente i costi e di introdurre un controllo più rigoroso e solido sulla connettività.

Inoltre, i clienti si sforzano di implementare e mantenere un solido livello di segmentazione all'interno delle loro applicazioni (ospitate oppure on-premise), il che rappresenta per gli operatori dei data center un'importante opportunità di sfruttare le loro competenze interne in materia di segmentazione, i loro strumenti e i loro modelli operativi al fine di offrire ai loro clienti servizi gestiti e di incrementare notevolmente i profitti grazie all'utilizzo della segmentazione. Inoltre, grazie alla capacità di estendere le policy di sicurezza alle sedi dei clienti con la metodologia, gli strumenti e i processi più appropriati, gli operatori dei data center saranno in grado di ottenere accesso e visibilità sulle applicazioni non ospitate per accelerare la loro migrazione sicura verso il data center ospitato, contribuendo così a migliorare le principali attività aziendali.

Equifax: lo scenario peggiore

Se vi state chiedendo "qual è la cosa peggiore che potrebbe accadere" con una segmentazione dell'ambiente debole, inefficace o inesistente, la violazione di Equifax del 2017, molto pubblicizzata, è un ottimo esempio storico. La violazione ha portato alla compromissione di 143 milioni di dati personali altamente sensibili di soggetti americani. Secondo l'indagine del Government Accountability Office (GAO) degli Stati Uniti, i criminali si sono inizialmente introdotti nel portale di risoluzione delle controversie dei clienti del gigantesco istituto di credito sfruttando una vulnerabilità, nota come CVE 2017-5638, nel framework web Apache Struts. Una volta all'interno, hanno sostanzialmente avuto libero accesso ai sistemi dell'azienda per 76 giorni. Il rapporto del GAO attribuisce questa libertà di movimento laterale alla mancanza di segmentazione, che ha permesso un facile accesso ai database a piacimento; una superficie di attacco praticamente illimitata.

Il problema è come raggiungere questo tipo di segmentazione nel modo più efficace, efficiente ed economico. Storicamente, gli operatori si sono affidati ai firewall o alle VLAN tradizionali per separare gli ambienti all'interno di un'architettura multi-tenant o multi-utente. L'implementazione e il mantenimento di tali misure, tuttavia, sono in genere ardui, altamente manuali e dispendiosi in termini di tempo e denaro. Inoltre, queste tecniche non sono affatto ineccepibili e possono lasciare esposta una superficie di attacco molto grande. L'efficacia delle soluzioni progettate per la difesa perimetrale è particolarmente problematica all'interno dei data center, soprattutto perché la maggior parte di questi ambienti include una varietà di macchine virtuali, hypervisor, container e, persino, componenti nel cloud, oltre al fatto che i carichi di lavoro accelerano e rallentano automaticamente in modo dinamico. Un'altra nota importante è rappresentata dal fatto che la segmentazione con le VLAN richiede il downtime di un'applicazione, il che può risultare un intoppo per i controlli operativi critici.

Per tutti questi motivi, gli operatori di ambienti condivisi stanno maggiormente adottando moderne tecniche di segmentazione definite dal software, tra cui la microsegmentazione. I progressi delle tecnologie di microsegmentazione l'hanno resa un'opzione fattibile per tutti i tipi di aziende e, probabilmente, la scelta ottimale per passare ad un modello di sicurezza Zero Trust. Altrettanto importante è il fatto che, con gli strumenti giusti e una pianificazione oculata, l'implementazione della microsegmentazione può risultare più rapida e facile rispetto ai metodi menzionati sopra, nonché più semplice in termini di gestione e manutenzione. Infatti, test condotti recentemente hanno dimostrato che la microsegmentazione può ridurre i tempi di implementazione fino a 30 volte rispetto ai firewall tradizionali. Un altro vantaggio cruciale: con la segmentazione definita dal software, non sono necessarie modifiche alla rete né sono richiesti tempi di downtime delle applicazioni. Questi risparmi in termini di tempo e di efficienza si traducono in costi significativamente inferiori per tutto il processo di implementazione.

Le insidie insite negli approcci convenzionali

Per comprendere i vantaggi offerti dalla segmentazione definita dal software o dalla microsegmentazione, è utile, a fini comparativi, esaminare alcuni degli svantaggi e dei limiti delle tecniche standard utilizzate sia on-premise che nel cloud. Questi metodi possono includere una combinazione di firewall fisici o virtualizzati e configurazioni di rete come le VLAN. In generale, questi metodi richiedono risorse e lavoro in quantità. La creazione di policy di sicurezza è un processo laborioso. Le aggiunte e le modifiche devono essere eseguite manualmente, il che rallenta l'efficienza operativa e aumenta il rischio di vulnerabilità.

I firewall interni, in particolare, sono costosi da acquistare e complessi da configurare. Inoltre, interferiscono con il normale flusso del traffico, alterando gli schemi e creando "hairpinning" tortuosi che finiscono per ostacolare le prestazioni del sistema. Come il settore sta imparando, i firewall non sono destinati alla segmentazione all'interno del data center: alcuni fornitori ammetteranno prontamente che i firewall semplicemente non sono la scelta migliore.

Una delle sfide più ardue quando si cerca di introdurre la segmentazione in un ambiente di produzione esistente e funzionante è che, per usare i metodi tradizionali, è necessario il downtime delle applicazioni. Il downtime è costoso. Può avvenire solo in finestre temporali specifiche e spesso non è assolutamente possibile.

Un'altra sfida degna di nota è che la creazione di una segmentazione interna richiede una buona conoscenza delle dipendenze est-ovest delle applicazioni. Questa conoscenza è solitamente inesistente. Senza un modo semplice per mappare le dipendenze delle applicazioni, è estremamente difficile e rischioso separare un ambiente brownfield.

Perché la segmentazione definita dal software è più efficace

Efficienza operativa, migliore sicurezza: la segmentazione definita dal software supera le inefficienze intrinseche delle tecniche tradizionali e, cosa forse più importante, garantisce una maggiore sicurezza per gli ambienti multi-utente. Come suggerisce il nome, la segmentazione definita dal software prende il concetto di segmentazione della rete e lo implementa senza bisogno di modificare l'infrastruttura. Implica la creazione di policy di sicurezza relative a singole applicazioni o ad applicazioni raggruppate logicamente, indipendentemente da dove risiedono nel data center ibrido. Queste policy indicano quali applicazioni possono o meno comunicare tra loro: un vero e proprio approccio Zero Trust.

Nessuna modifica manuale o tempi di downtime: la segmentazione definita dal software non richiede alcuna modifica alla rete e nessuna creazione di VLAN, il che si traduce in risparmi operativi significativi. Inoltre, non richiede downtime delle applicazioni o modifiche dovute alla migrazione su una nuova VLAN. Si tratta di un aspetto importante. In molte applicazioni per le quali il downtime è molto costoso o impossibile, è l'unico modo per fornire questa misura di sicurezza cruciale.

Ampia visibilità: inoltre, le soluzioni di segmentazione avanzate definite dal software, progettate per affrontare le sfide della segmentazione del traffico est-ovest, forniscono uno strumento di visibilità integrato che aiuta a identificare i confini dei segmenti e le dipendenze delle applicazioni. Ciò si traduce in un processo efficiente ed elimina gli errori operativi durante la creazione delle policy.

Automazione di policy e controlli: la segmentazione definita dal software consente inoltre di applicare le policy in modo dinamico, così che man mano che i carichi di lavoro aumentano o diminuiscono, vengono attribuiti automaticamente alla policy corretta. Ciò consente un notevole risparmio di risorse, eliminando la necessità di spostamenti, aggiunte o modifiche manuali.

Indipendenza dall'infrastruttura: un vantaggio fondamentale della segmentazione definita dal software è l'indipendenza dall'infrastruttura. Lo stesso strumento fornisce visibilità e segmentazione su qualsiasi infrastruttura: bare metal, virtualizzata, PaaS, cloud, container, ecc. Il tutto da un'unica posizione e con un unico flusso di lavoro. Ciò si traduce in una notevole libertà operativa, grazie alla quale è possibile raggiungere gli standard di sicurezza senza alcun vincolo dettato dalla scelta dell'infrastruttura sottostante.

Maggiori ricavi, migliori rapporti: l'aspetto più importante è che tutto ciò introduce un'opportunità significativa per gli operatori dei data center. Mentre gestiscono e forniscono la segmentazione interna, possono anche sfruttare la formazione, gli strumenti e i processi per offrire un servizio gestito indispensabile ai propri clienti, gestendo la segmentazione non solo per le applicazioni ospitate, ma anche per le applicazioni presenti nelle sedi dei clienti o nel cloud, il tutto da un'unica posizione. Ciò si traduce non solo in un potenziale di ricavo aggiuntivo, ma crea anche una maggiore dipendenza dall'operatore, con conseguenti relazioni più lunghe e profitti più elevati.

Perché Akamai

Per ottenere questi vantaggi, una soluzione di segmentazione definita dal software deve soddisfare una serie di criteri essenziali. Deve consentire una visibilità profonda, a livello di processo, di tutte le applicazioni in esecuzione nell'ambiente informatico e la capacità di mappare tutti i flussi di dati tra di esse. Inoltre, la flessibilità di etichettare correttamente le risorse per la creazione di policy e di modificare automaticamente le etichette in base all'autoscala dei carichi di lavoro è la chiave per un'implementazione e una gestione efficienti. La soluzione deve, poi, essere indipendente dalla piattaforma e dall'infrastruttura. Le policy devono essere in grado di seguire le rispettive applicazioni e di funzionare in modo coerente in più ambienti. Infine, la soluzione deve consentire un modello operativo automatizzato e semplificato per la creazione, la gestione e l'applicazione delle policy.

Solo Akamai Guardicore Segmentation soddisfa tutti questi criteri. La segmentazione definita dal software è la nostra funzionalità principale. La soluzione fornisce una visualizzazione grafica senza precedenti di tutte le risorse dell'ambiente e delle loro dipendenze, che si tratti di bare metal, macchine virtuali, cloud pubblico, container o dispositivi IoT. Questa profonda visibilità accelera notevolmente il processo di identificazione, raggruppamento e creazione di policy di sicurezza relative a microsegmenti di applicazioni.

Per altre informazioni, visitate il sito akamai.com/guardicore.