Akamai

WHITE PAPER

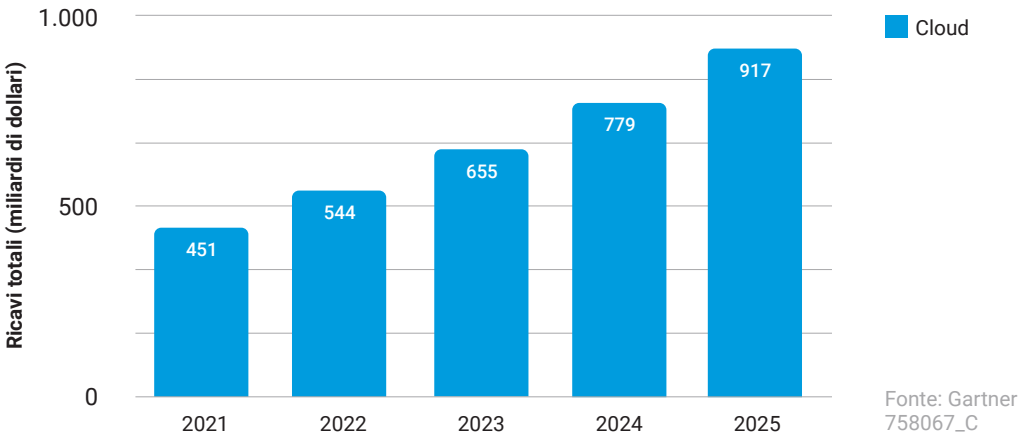
Facilitare il percorso verso la microsegmentazione

Una guida alla strategia per l'implementazione della microsegmentazione nei cloud ibridi.

Un maggior numero di cloud in previsione

La migrazione di grandi quantità di dati e di elaborazione dei dati nel cloud o, più precisamente, su più cloud, è senza dubbio il cambiamento più grande del computing aziendale nell'ultimo decennio. Sempre più organizzazioni stanno passando a cloud pubblici e, in genere, ad architetture di data center ibrido pubblico-privato Allo stesso tempo, stanno sfruttando l'infrastruttura come servizio (IaaS) alla ricerca di una sempre maggiore flessibilità. La società di analisi tecnologiche Gartner prevede che entro il 2025, poco più della metà di tutta la spesa IT nei segmenti di mercato interessati sarà passata dalle soluzioni tradizionali al cloud pubblico, rispetto al 41% nel 2022, e si prevede che la spesa dei ricavi totali per il cloud pubblico supererà 900 miliardi di dollari entro il 2025.[1]

La distinzione tra "cloud" e "multicloud" non è semplice. Sempre più spesso le aziende adottano piattaforme e fornitori di servizi multicloud. Una cosa è chiara: l'idea di un data center aziendale come spazio fisico unico e sicuro sta ormai diventando obsoleta. I data center moderni sono sempre più una combinazione eterogenea di ambienti e tecnologie di server fisici, macchine virtuali e container situati in strutture locali, cloud privati e fornitori IaaS di cloud pubblico. E queste installazioni disparate non sono statiche: le organizzazioni spostano costantemente dati e carichi di lavoro tra i vari ambienti on-premise e cloud a seconda dei livelli di traffico e delle esigenze di elaborazione



Previsioni sui ricavi dei servizi cloud pubblici a livello mondiale (in miliardi)

La maggiore complessità comporta nuove vulnerabilità e amplia le superfici di attacco

I clienti del cloud beneficiano sicuramente della maggiore flessibilità, elasticità e scalabilità offerte dai servizi IaaS: questi vantaggi sono una parte importante di ciò che rende il cloud così attraente. I compromessi che richiede, tuttavia, sono un notevole aumento della complessità di gestione, una perdita di visibilità del carico di lavoro tra gli ambienti e, di conseguenza, un panorama di cybersicurezza non mappata. Collaborare con più fornitori di servizi cloud significa che i team di sicurezza devono affrontare standard e capacità di sicurezza molto diversi. Gli strumenti di sicurezza tradizionali progettati per server ed endpoint locali semplicemente non sono in grado di gestire la scala e la complessità del cloud. Gli strumenti più recenti forniti dai fornitori IaaS possono essere efficaci nell'ambiente del provider, ma sono poco utili in un'infrastruttura multi-provider.

Inoltre, anche in quest'era di virtualizzazione e in cui "tutto è definito dal software", la mentalità della sicurezza (e quindi la maggior parte degli investimenti) è ancora fondata sulla necessità percepita di bloccare gli attacchi specificamente nel punto di accesso. Ciò non vuol dire che le difese perimetrali non servano, sono ancora molto importanti per lo stack di sicurezza IT, ma non funzionano altrettanto bene quando il perimetro cambia costantemente. I dati e i carichi di lavoro si spostano tra cloud pubblici e privati e data center locali, e gli utenti che vi accedono lavorano sempre più da postazioni remote che possono disporre o meno dei controlli di sicurezza adeguati.

L'enorme numero di violazioni dei dati segnalate ogni anno è sufficiente per dirci che i criminali più scaltri riescono a superare le difese perimetrali praticamente a piacimento. E una volta all'interno, trovano una rete relativamente semplice in cui le risorse che risiedono all'interno del perimetro sono praticamente senza protezione. Nonostante tutta la flessibilità acquisita dalle organizzazioni, la maggiore complessità della gestione e della protezione delle infrastrutture multicloud ha moltiplicato in modo esponenziale la superficie di attacco; con pochi o nessun controllo sulla comunicazione, ogni singolo server diventa di per sé una superficie di attacco. Di conseguenza, gli autori di attacchi possono dedicare più tempo a muoversi lateralmente, senza essere rilevati, tra i carichi di lavoro del traffico est-ovest per trovare le risorse più critiche.

La segmentazione della rete è una pratica di sicurezza ben nota e consolidata, ma al giorno d'oggi può essere difficile da eseguire in infrastrutture IT dinamiche e su scala cloud, dove i carichi di lavoro comunicano e spesso migrano tra segmenti. I clienti del cloud aziendale sono giunti alla consapevolezza di dover segmentare ulteriormente le applicazioni e i carichi di lavoro per controllare rigorosamente i flussi di comunicazione in tempo reale e rilevare e contrastare le minacce all'interno del data center prima che possano causare danni. È necessaria una soluzione che riduca la complessità della sicurezza lavorando in modo coerente oltre i confini dell'infrastruttura per ridurre la superficie di attacco complessiva, consentendo ai team di sicurezza di rilevare più minacce più rapidamente e limitarne la diffusione.

È qui che entra in gioco la segmentazione.

Definizione della microsegmentazione

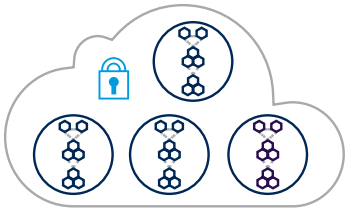
Gartner definisce la microsegmentazione come "il processo di implementazione dell'isolamento e della segmentazione per scopi di sicurezza all'interno del data center virtuale". Inoltre, la microsegmentazione "riduce il rischio di una diffusione laterale di attacchi avanzati nei data center aziendali e consente alle aziende di applicare policy di segmentazione coerenti tra carichi di lavoro on-premise e basati su cloud".[2]

La microsegmentazione in genere agisce impostando policy di sicurezza relative a singole applicazioni o gruppi di applicazioni, indipendentemente da dove risiedono nel data center ibrido. Queste policy determinano quali applicazioni e componenti possono e non possono comunicare tra loro. Pertanto, i tentativi di comunicazione non autorizzata sono un indicatore immediato di una minaccia. Nel migliore dei casi, le tecnologie di microsegmentazione sono indipendenti dall'infrastruttura, quindi le policy di sicurezza possono continuare a proteggere le rispettive applicazioni mentre si spostano tra gli ambienti cloud.

Aree di soluzione per la segmentazione

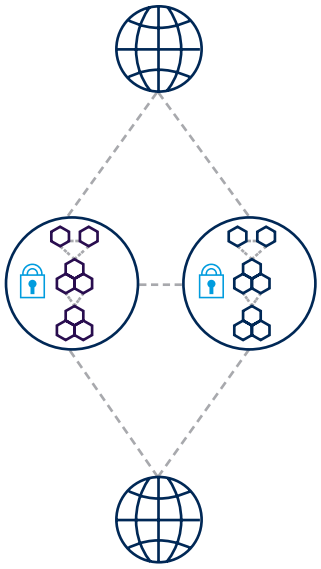
Segmentazione dell'infrastruttura

Proteggete il traffico delle applicazioni all'interno di una particolare infrastruttura.



Segmentazione delle applicazioni

Proteggete il traffico tra applicazioni e reti esterne.



Microsegmentazione

Regole che proteggono il traffico all'interno delle applicazioni con contesto aggiuntivo come l'attribuzione a livello di processo.

2 Gartner, "Technology Insight for Microsegmentation", marzo 2017; "Hype Cycle for Cloud Security 2017", luglio 2017

Il caso della microsegmentazione

I data center dinamici di oggi richiedono alle aziende di spostare la propria attenzione dalla prevenzione delle intrusioni e la gestione degli accessi ai carichi di lavoro e alle applicazioni stesse. E sembra che ciò stia accadendo a un ritmo accelerato. Già nel 2017, Gartner ha iniziato a notare una tendenza verso "una maggiore attenzione alla protezione del carico di lavoro dei server da minacce mirate avanzate che aggirano il perimetro tradizionale e la protezione basata su firme. In genere, questi attacchi hanno un movente economico e prendono di mira i carichi di lavoro di server e applicazioni al fine di accedere a dati sensibili o transazioni".[3]

Un fattore determinante della microsegmentazione è la necessità di proteggere le applicazioni e i carichi di lavoro mission-critical. Ciò può sembrare semplicemente una questione di interesse personale o una buona pratica aziendale, ma in molti casi è anche imposto dalle policy di sicurezza e dai requisiti normativi.

I team di sicurezza devono trovare modi per ridurre la superficie di attacco in espansione all'interno dei data center, il che significa ridurre la vulnerabilità dei server che eseguono applicazioni. Le tecniche di autenticazione tradizionali, come il blocco delle firme o l'inserimento negli elenchi di elementi consentiti delle applicazioni, vengono aggirate troppo facilmente dai criminali sofisticati. La microsegmentazione consente ai team di impostare e applicare policy di accesso e comunicazione rigorose e granulari. Dovrebbe inoltre migliorare la visibilità dei flussi delle applicazioni e consentire ai team di valutare meglio il proprio sistema di sicurezza.

La microsegmentazione è necessaria?

Rispondere ad alcune semplici domande vi aiuterà ad accertare se necessitate della di microsegmentazione.

- Operate in un settore regolamentato o dovete rispettare le normative che regolano la sicurezza dei dati e delle transazioni?
- Disponete di un'infrastruttura ibrida con carichi di lavoro che si estendono su più cloud?
- State eseguendo applicazioni in macchine virtuali o container?
- Percepite una perdita di visibilità e controllo dei carichi di lavoro?
- Siete in grado di determinare in qualsiasi momento se è presente una minaccia o se è in corso un attacco nel vostro data center?
- Potete controllare la sicurezza della vostra infrastruttura da "un'unica posizione"?

I quattro principali ostacoli sul percorso

Se gli esperti di sicurezza concordano generalmente sulla necessità della microsegmentazione nei data center dinamici di oggi, perché è considerato così difficile implementarla in modo efficiente e con successo? Le organizzazioni che tentano di implementare la microsegmentazione utilizzando strumenti convenzionali generalmente incontrano quattro ostacoli principali:

1. **Mancanza di visibilità**
   È probabilmente il primo ostacolo che incontrerete: è impossibile proteggere quello che non vedete. La microsegmentazione riguarda la protezione di singoli e gruppi di applicazioni e processi di workflow. I team di sicurezza necessitano di visibilità sugli effettivi flussi di traffico est-ovest per comprenderli nel contesto. La maggior parte degli strumenti non offrono tale livello di profondità.

2. **Mancanza di supporto multicloud ibrido**
   Le policy di sicurezza di microsegmentazione devono essere in grado di adattarsi facilmente agli ambienti on-premise e cloud pubblici e seguire gli spostamenti dei carichi di lavoro. Gli strumenti progettati per funzionare in un ambiente specifico sono inefficaci negli ambienti ibridi.

3. **Motori di policy non flessibili**
   Come notato in precedenza, i data center di oggi non sono statici. Nemmeno le misure di sicurezza possono esserlo: la mentalità di una "configurazione univoca" non basterà più. Purtroppo, gli strumenti esistenti dei provider di servizi cloud non consentono la flessibilità necessaria per definire, testare e perfezionare costantemente le regole. Questo problema è aggravato dalle infrastrutture ibride che richiedono più strumenti per policy.

4. **Nessuna integrazione con controlli complementari**
   Se eseguita correttamente, la microsegmentazione non riguarda solo la protezione dei processi, ma anche il blocco degli attacchi. Tuttavia, gli strumenti di microsegmentazione a funzione singola in genere non includono funzionalità di rilevamento delle violazioni, lasciando all'utente il compito di integrare gli strumenti e farli interagire in modo efficace. Questo approccio basato su più strumenti comporta un alto rischio di fallimento.

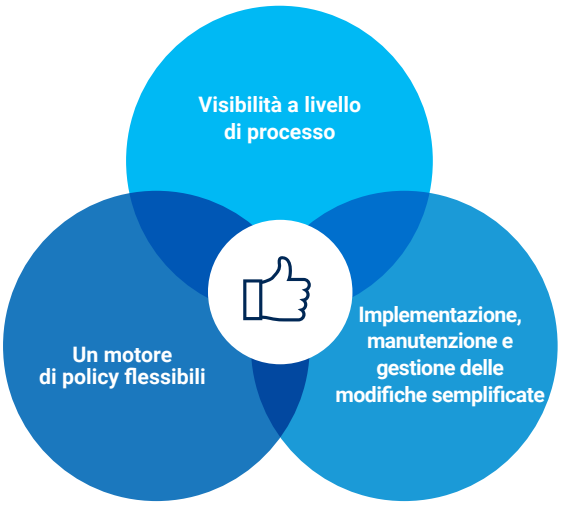
I progetti inefficaci sono la norma, non l'eccezione

Considerati questi ostacoli, non c'è da sorprendersi se la maggior parte dei progetti di microsegmentazione tendono a soffrire a causa di cicli di implementazione, costi di attivazione e risorse fiscali pesanti e, per finire, incapacità di raggiungere gli obiettivi. Le organizzazioni spesso hanno difficoltà a capire cosa deve essere segmentato (a causa della mancanza di visibilità) e a decidere il grado di segmentazione è necessario. Potrebbero passare mesi a creare fogli di calcolo con regole complesse per le comunicazioni a livello di processo, non cogliendo le opportunità per raggruppare le applicazioni e razionalizzare le policy. Troppo spesso, propendono per una "segmentazione eccessiva", impostando troppe policy distinte, con una conseguente eccessiva complessità della sicurezza, che è esattamente ciò che stanno cercando di superare. Come ha osservato Gartner, "...sarà necessario rivedere la progettazione iniziale di più del 70% dei progetti di segmentazione a causa dell'eccessiva segmentazione".[4]

L'eccessiva segmentazione corre il rischio di rallentare le applicazioni e, in ultima analisi, le attività aziendali. Ma si rischia di eccedere nel senso opposto, verso una segmentazione insufficiente, e finire per compromettere la vostra strategia di sicurezza.

Strategia per un percorso di microsegmentazione di successo

Il percorso per implementare la microsegmentazione non è lineare: il rilevamento, la comprensione e il controllo dei flussi delle applicazioni nel vostro ambiente ha numerosi risvolti. I team di sicurezza necessitano di flessibilità quando sviluppano policy di sicurezza per integrare costantemente nuove modifiche o aggiunte senza interrompere le applicazioni. Molte soluzioni offrono motori di creazione di policy non flessibili, costringendo i team di sicurezza a implementare regole incomplete o inefficaci prima che siano pronte.



Molto semplicemente, un'implementazione di successo è quella che supera o elude i quattro ostacoli principali, evitando un'eccessiva complessità e riducendo il rischio di una segmentazione insufficiente o eccessiva consentendo un approccio graduale. Ciò significa disporre di una soluzione che soddisfi questi requisiti:

- **Visibilità a livello di processi:** i team devono essere in grado di rilevare, raccogliere e normalizzare tutti i flussi est-ovest e nord-sud; disporre di strumenti che consentono il rilevamento automatico delle applicazioni e la comprensione dei relativi requisiti di comunicazione; e avere la possibilità di filtrare più attributi dell'applicazione per facilitare l'etichettatura e il raggruppamento di risorse che possono condividere policy.

- **Un motore di policy flessibili:** dovreste essere in grado di progettare contemporaneamente best practice e regole di conformità di alto livello per segmenti di grandi dimensioni e regole più granulari per i microsegmenti. La soluzione dovrebbe consentire di passare gradualmente dalla segnalazione all'applicazione delle norme. E dovrebbe consentirvi di definire policy che funzionino su tutte le piattaforme, i dispositivi e i cloud.

- **Implementazione, manutenzione e gestione delle modifiche semplificate:** Il sistema dovrebbe semplificare l'implementazione, la manutenzione e la modifica delle regole secondo necessità. Dovrebbe includere funzionalità di rilevamento delle violazioni e di risposta agli incidenti integrate. Infine, le policy dovrebbero essere sufficientemente ben definite da poterle integrare negli strumenti di implementazione automatizzata (CI/CD) per ogni nuova applicazione lanciata.

Funzionalità della soluzione ideale

Naturalmente, sul mercato sono disponibili molti strumenti di microsegmentazione, e non tutti rendono facile seguire questo percorso. Per garantire un'implementazione più semplice e di maggior successo, assicuratevi di scegliere una soluzione con queste funzionalità:

- **Rilevamento automatico delle applicazioni**, con visibilità completa a livello di processo per server bare metal, macchine virtuali e container

- La possibilità di definire **query affidabili ed estese** per creare etichette contestuali e gruppi di oggetti

- Un **motore di policy flessibili** con una progettazione intelligente delle regole che aiuta a perfezionare, rafforzare e mantenere le policy

- Una **funzionalità di rilevamento delle violazioni** multi-metodo integrata per individuare più minacce più rapidamente e limitarne la diffusione

- **Supporto di un'infrastruttura ibrida**: un'unica piattaforma che funziona con qualsiasi infrastruttura: data center, cloud pubblici e privati e altro ancora

Una soluzione con queste funzionalità principali agevolerà il vostro percorso verso un'implementazione della microsegmentazione di successo, vi consentirà di superare gli ostacoli e le complessità noti e vi preparerà a sfruttare tutti i vantaggi aziendali di un'infrastruttura cloud ibrida flessibile senza sacrificare la sicurezza.

I data center ibridi, le piattaforme multicloud e IaaS offrono alle organizzazioni maggiore flessibilità, scalabilità e agilità rispetto a quanto sarebbe possibile in un data center on-premise "chiuso". Ma aumentano anche l'esposizione e la vulnerabilità delle applicazioni e dei carichi di lavoro (le risorse effettive prese di mira dagli attacchi informatici). Sebbene la microsegmentazione sia ampiamente considerata una best practice per proteggere i carichi di lavoro nel cloud, le aziende hanno difficoltà ad attuarla in modo appropriato. La buona notizia è che non dovete fare tutto in una volta. Le soluzioni avanzate di oggi, abbinate a un approccio a fasi e graduale, rendono molto più semplice il percorso verso l'implementazione della microsegmentazione, che garantisce una migliore sicurezza per le risorse più importanti della vostra organizzazione.

Ulteriori informazioni sull'implementazione della microsegmentazione sono disponibili sul sito akamai.com/guardicore

1 "Gartner afferma che le aziende che operano nei principali segmenti di mercato spenderanno più della metà dei loro budget IT per il cloud entro il 2025". Gartner, 9 febbraio 2022.

2 Heiser Jay. "Hype Cycle for Cloud Security, 2017". Gartner, 17 luglio 2017.

3 MacDonald Neil. "Guida di settore per le piattaforme di protezione dei carichi di lavoro nel cloud". Gartner, 22 marzo 2017.

4 Young Greg. "Best practice sulla segmentazione di rete per la sicurezza". Gartner, 28 luglio 2016.

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 ed evolvere la vostra strategia di sicurezza per favorire il modello Zero Trust, bloccare i ransomware, proteggere app e API o contrastare gli attacchi DDoS, offrendovi la sicurezza necessaria per concentrarvi costantemente sull'innovazione, sull'espansione e sulla trasformazione di tutto il possibile. 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.