Akamai

# Come sfatare i 7 miti sulla microsegmentazione

Può sembrare controintuitivo pensare in piccolo quando si scala in grande, ma ci sono numerosi falsi miti sulle moderne soluzioni di microsegmentazione.

Pensate che riscontrerete downtime della rete o difficoltà a rendere operativa una distribuzione definita dal software? Riflettete. Ecco cosa è importante per la granularità.

Mito numero 1

# La mia soluzione EDR è sufficiente per bloccare gli attacchi ransomware

Il rilevamento e la risposta degli endpoint (EDR) e la segmentazione affrontano entrambi gli attacchi ransomware, ma in fasi diverse della kill chain e in modi diversi. Le soluzioni EDR mirano a rilevare la presenza di ransomware in esecuzione sui dispositivi o sugli endpoint che stanno controllando. Se la tecnologia EDR rileva un ransomware, può distruggere il processo, mettere in quarantena il dispositivo e spesso risolvere eventuali problemi di crittografia che si sono verificati. EDR e segmentazione sono complementari: se EDR non rileva il ransomware, le soluzioni di segmentazione suddividono la rete in compartimenti isolati per limitare il movimento laterale (est-ovest) di un attacco. Con il ransomware, è necessario il movimento laterale affinché gli autori di attacchi abbiano successo. La segmentazione garantirà che gli attacchi che sono riusciti ad avanzare oltre l'endpoint alla fine raggiungano un ostacolo, limitando la zona di impatto di un'infezione iniziale. Ulteriori informazioni sulle differenze tra EDR e segmentazione.

**1 ora e 42 minuti**

è il tempo medio impiegato da un autore di attacchi per iniziare a muoversi lateralmente all'interno della rete una volta ottenuto un punto d'accesso iniziale

(Microsoft Digital Defense Report 2022)

Mito numero 2

# Sto già eseguendo la segmentazione

La segmentazione non è un concetto nuovo, è solo diventata più sofisticata. Per decenni, le organizzazioni hanno utilizzato un mosaico di VLAN, firewall interni, ACL e gruppi di sicurezza per segmentare i propri ambienti. Ma questi metodi legacy non si sono evoluti per soddisfare le complesse esigenze delle moderne infrastrutture ibride e multicloud, creando lacune difensive e punti ciechi a causa della sottosegmentazione.

Ad esempio, i firewall legacy non mappano o valutano le dipendenze del workflow, rendendo difficile identificare le segmentazioni per applicazioni, carichi di lavoro o utenti. Le aziende sono quindi costrette a implementare policy di segmentazione ad ampio raggio che sono eccessivamente permissive e possono facilmente *e rapidamente* comportare pericolose configurazioni errate che sono difficili e scomode da risolvere.

Con la microsegmentazione, le organizzazioni possono segmentare e applicare fino al livello 7, ben oltre ciò che è possibile fare con i tradizionali strumenti di segmentazione.

Riduzione dei costi di

**2,0 milioni di dollari**

per l'aggiornamento dei firewall entro tre anni

(Forrester TEI)

Mito numero 3

# La microsegmentazione è troppo difficile da rendere operativa

La microsegmentazione moderna è pronta per gli eventi aziendali più importanti, ora più che mai.

Akamai Guardicore Segmentation consente di raggiungere la massima efficienza operativa tramite l'uso di un'unica soluzione basata su software per la segmentazione, la visibilità, la creazione di policy e l'applicazione in tutti gli ambienti, dal data center e cloud alle risorse basate su container. Al momento dell'implementazione, Akamai Guardicore Segmentation crea una mappa visiva dinamica dell'intera infrastruttura IT che consente ai team di sicurezza di visualizzare l'attività fino al livello del singolo processo, sia in tempo reale che su base cronologica. Queste informazioni dettagliate sul comportamento dell'applicazione possono quindi essere utilizzate per creare rapidamente policy di microsegmentazione granulari tramite un'interfaccia visiva intuitiva. Le regole di negazione globali, l'isolamento delle applicazioni critiche e la capacità di segmentare immediatamente ambienti di grandi dimensioni si traducono in un rapido time-to-value e in una riduzione dei rischi.

Con i metodi di segmentazione legacy, manca la visibilità persino per sapere da dove iniziare.

↑95%

di aumento della produttività SecOps

(Forrester TEI)

Mito numero 4

# Microsegmentazione significa downtime delle applicazioni e della rete

Con gli approcci tradizionali alla segmentazione, le applicazioni vengono spesso spostate tra sottoreti o VLAN, causando downtime e interrompendo la continuità operativa. I tecnici di rete e gli amministratori dei firewall devono pianificare downtime programmati, il controllo delle modifiche o le finestre di manutenzione, aumentando il tempo necessario per distribuire nuovi servizi o aggiornamenti delle applicazioni. Peggio ancora, questi ritardi possono comportare un aumento del rischio dovuto all'esposizione e alla vulnerabilità delle risorse.

La segmentazione definita dal software, d'altra parte, scollega la sicurezza dall'infrastruttura e dai sistemi operativi sottostanti in modo che la segmentazione possa essere eseguita in modo indipendente, senza toccare la rete o l'applicazione. Se si verifica un evento, invece di isolare completamente i computer interessati, viene bloccato solo il vettore di attacco, limitando l'impatto negativo sull'azienda.

La microsegmentazione può anche essere implementata in modalità di avviso per consentire di testare le policy in ambienti di produzione live senza il rischio di downtime. Conclusione: le moderne soluzioni di segmentazione non dovrebbero comportare una scelta tra una migliore sicurezza e la flessibilità aziendale.

Mito numero 5

# La microsegmentazione non copre il mio ambiente IoT o OT

Sapevate che i criteri Zero Trust possono essere applicati per i dispositivi IoT e OT che non sono in grado di eseguire software di sicurezza basati su host?

Le nostre funzionalità di segmentazione senza agenti colmano le lacune difensive tra i dispositivi che non possono eseguire agenti per eliminare i punti ciechi di visibilità, come gli endpoint isolati. Questa copertura estesa è particolarmente critica per gli ambienti sanitari, retail e di produzione con molti dispositivi IoT connessi alla rete (e vulnerabili) e sistemi OT legacy. L'integrazione della segmentazione senza agenti nella vostra infrastruttura di rete consente il rilevamento automatico di nuovi dispositivi, il fingerprinting e l'applicazione delle policy per aiutare a mitigare i rischi, accelerando al contempo il passaggio al modello Zero Trust a livello aziendale.

Mito numero 6

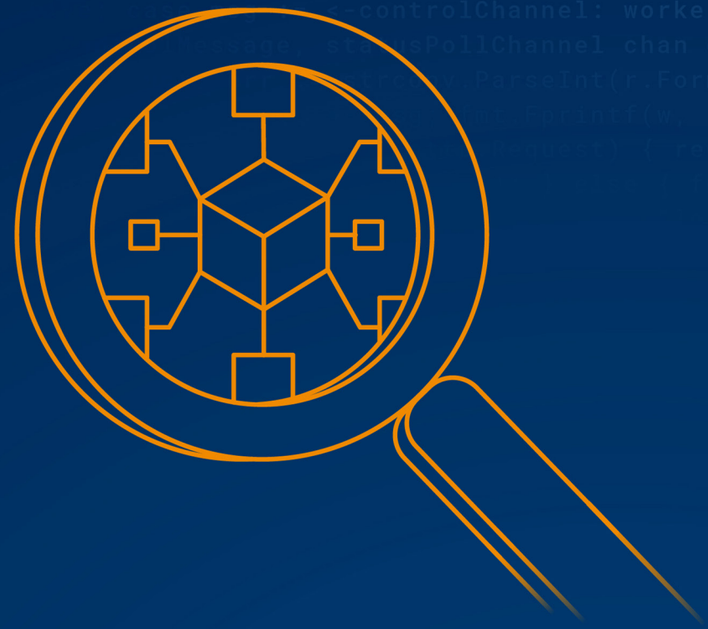
# Un agente di microsegmentazione causa una latenza eccessiva

Uno dei più grandi falsi miti sulla microsegmentazione è la maggiore latenza.

In realtà, l'utilizzo di policy di segmentazione distribuite basate su software invece di forzare tutto il traffico attraverso specifici punti di strozzatura del firewall elimina i colli di bottiglia della rete. Per sua natura, l'agente Akamai Guardicore è altamente ottimizzato per funzionare con Linux, Unix, il sistema operativo Windows e MacOS e non consuma risorse sostanziali.

E poiché l'agente non è in linea, non esegue un'ispezione approfondita dei pacchetti che può aumentare la latenza.

Invece, l'agente Akamai Guardicore acquisisce informazioni minime dall'intestazione del pacchetto per formare una visione completa dell'ambiente del cliente. Se state cercando velocità *e* performance, *potete* ottenere entrambe.



Mito numero 7

# Microsegmentazione significa assumere FTE introvabili

Con i CISO che sentono la pressione di "fare di più con meno", le soluzioni di sicurezza devono sollevare l'onere dagli addetti alla sicurezza, non consumare ulteriormente le scarse risorse interne.

I metodi di segmentazione tradizionali come la gestione di firewall e VLAN comportano processi complessi e in più passaggi che coinvolgono molti team, responsabili separatamente di commutazione, routing, implementazione del firewall e creazione di policy di sicurezza. L'implementazione di un firewall legacy può richiedere in media da 14 a 22 settimane. Tutto ciò si aggiunge alle tempistiche del progetto, sottoponendo l'organizzazione a significativi costi di manodopera e spese generali operative.

Al contrario, la soluzione definita dal software di Akamai richiede in media due settimane per l'implementazione e un solo dipendente a tempo pieno. E aggiungendo Akamai Hunt, il nostro servizio gestito di ricerca delle minacce, vi faremo risparmiare tempo e risorse monitorando il vostro ambiente per rilevare attacchi emergenti, movimenti laterali e comportamenti di attacco anomali.

Al giorno d'oggi, i talenti informatici sono difficile da assumere e ancora più difficili da trattenere. È ora che i sistemi di difesa lavorino a favore, *e non contro*, la vostra organizzazione.

Statistiche principali

106%

ROI assicurato fino a ~106% entro 12 mesi

(Forrester TEI)

# Il contributo di Akamai

Akamai Guardicore Segmentation è una soluzione di microsegmentazione basata su software che fornisce il modo più semplice, rapido e intuitivo per applicare i principi del modello Zero Trust. La soluzione vi consente di prevenire il movimento laterale dannoso nella vostra rete tramite precise policy di segmentazione, la visualizzazione dell'attività svolta nel vostro ambiente IT e avvisi sulla sicurezza della rete. Akamai Guardicore Segmentation supporta i vostri data center, ambienti multicloud ed endpoint. È più facile da distribuire rispetto agli approcci di segmentazione dell'infrastruttura e vi offre una visibilità e un controllo impareggiabili sulla vostra rete.

Scoprite in che modo Akamai Guardicore Segmentation offre protezione granulare, visibilità approfondita e applicazione coerente delle policy di sicurezza su larga scala per proteggere i vostri dati più sensibili.