Akamai

EBOOK

Superare i problemi di implementazione per proteggere i sistemi bancari più importanti

Rapporto sullo stato della segmentazione globale

Sommario

Introduzione

Proteggere il settore dei servizi finanziari ha sempre posto notevoli sfide per i team addetti alla sicurezza IT. Tuttavia, i criminali sempre più sofisticati ora combinano varie tecniche per lanciare minacce più grandi e più frequenti, mettendo i team addetti alla sicurezza nelle società di servizi finanziari sotto pressione come mai prima d'ora. Le società di servizi finanziari operano basandosi su una presenza digitale, pertanto una violazione riuscita può causare danni ingenti, se non irreparabili, alla reputazione e al fatturato.

Come dimostrano i risultati di questo rapporto, gli attacchi stanno avendo un impatto perfino maggiore, aumentando la pressione sui responsabili della sicurezza affinché scelgano le soluzioni giuste e mantengano l'intero ambiente sicuro, senza compromettere le performance complessive o rischiare di esporre enormi quantità di dati sensibili.

Gli intervistati che operano nelle società di servizi finanziari (in tutte le aree geografiche, inclusi Stati Uniti, America Latina, EMEA e APAC) concordano in modo schiacciante sull'efficacia della segmentazione per mantenere le risorse protette, ma i loro progressi complessivi nell'implementazione in applicazioni e risorse aziendali di importanza critica sono stati inferiori alle aspettative. L'ostacolo numero uno per le società di servizi finanziari è stato rappresentato dall'aumento dei colli di bottiglia, il che suggerisce che i team potrebbero aver reagito alle minacce senza avere il tempo o il supporto necessari per comprendere appieno e mitigare gli impatti sulle performance derivanti dai cambiamenti

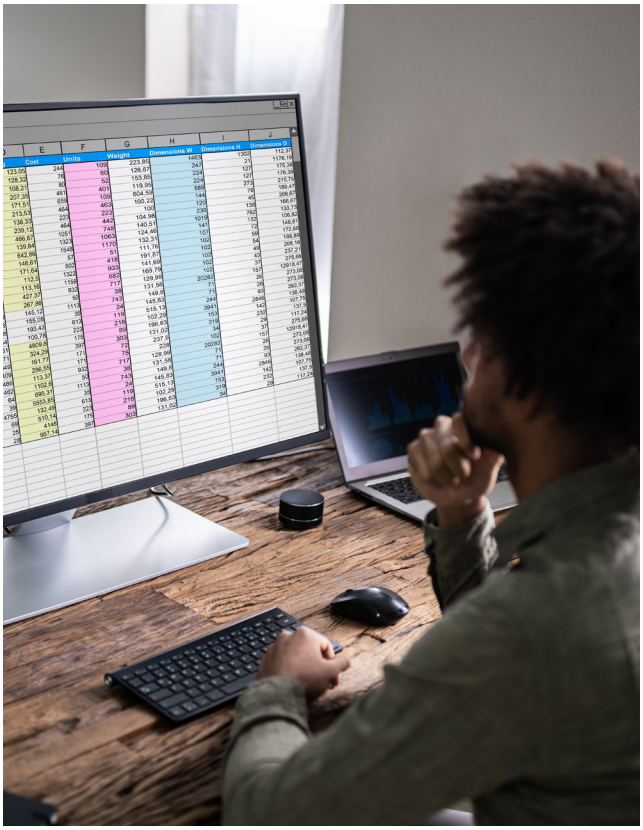
La buona notizia? La perseveranza dà i suoi frutti. La segmentazione ha dimostrato di avere un effetto trasformativo sulla difesa per coloro che hanno segmentato la maggior parte delle risorse critiche, consentendo loro di mitigare e contenere i ransomware 13 ore più velocemente rispetto a coloro che avevano segmentato solo una risorsa. Immaginate la differenza che fanno quelle 13 ore per il vostro team, i vostri clienti e la vostra reputazione.

Il risultato: la segmentazione mostra nel complesso lenti progressi, ma coloro che hanno perseverato hanno ridotto enormemente il rischio.

La segmentazione va bene. La microsegmentazione è ancora meglio.

La segmentazione è un approccio architetturale che divide una rete in segmenti più piccoli per migliorare le performance e la sicurezza.

La microsegmentazione è una tecnica di sicurezza che vi consente di dividere in modo logico una rete in segmenti separati fino al livello dei singoli carichi di lavoro. È possibile quindi definire i controlli di sicurezza e la delivery di servizi per ogni singolo segmento.



Gli attacchi ransomware continuano ad aumentare, così come il loro impatto

Il numero di attacchi ransomware nelle società di servizi finanziari (riusciti o meno) è quasi raddoppiato negli ultimi due anni, passando da una media di 43 nel 2021 a 62 nel 2023. Nonostante la reputazione del settore per le solide misure di sicurezza adottate, queste cifre sottolineano una vulnerabilità critica che non può essere trascurata. È evidente che il settore dei servizi finanziari non è immune alla minaccia dei ransomware e trascurare il rischio non è un'opzione da considerare.

Le società di servizi finanziari nell'APAC sono state prese di mira, in media, con il numero più alto di attacchi ransomware (73), mentre in America Latina si è registrato il numero più basso di attacchi (48, Figura 1).

Numero medio di attacchi ransomware sferrati contro il settore dei servizi finanziari negli ultimi 12 mesi per area geografica

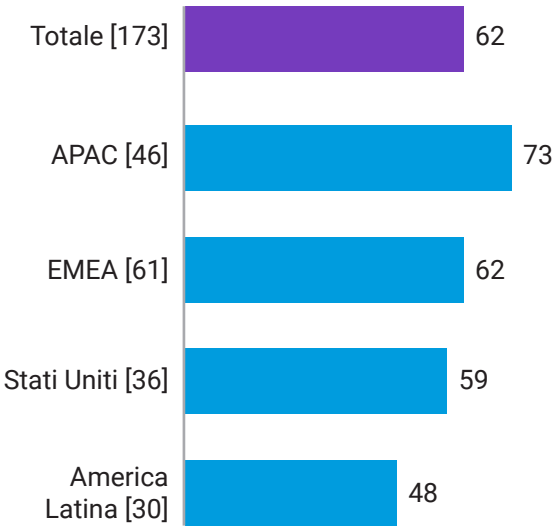


Figura 1. Quanti attacchi ransomware hanno colpito la vostra organizzazione negli ultimi 12 mesi (indipendentemente dal fatto che siano andati a buon fine)? Il grafico mostra il numero medio di attacchi negli ultimi 12 mesi, suddivisi per area geografica (mostrati i numeri di base) (dati relativi solo al settore dei servizi finanziari).

Poiché la maggior parte delle società di servizi finanziari opera a livello globale, l'aumento del numero di attacchi mirati nell'APAC potrebbe derivare dalla percezione degli hacker che gli obiettivi dell'APAC offrano rendimenti più elevati. Tuttavia, ciò non implica che le società di servizi finanziari di altre aree geografiche siano più sicure, ma solo che potrebbero avere maggiori probabilità di subire attacchi laterali originati altrove.

Inoltre, gli intervistati in America Latina sono più propensi ad affermare che la loro società di servizi finanziari ha segmentato più di due risorse, seguiti dagli intervistati nell'APAC. Ciò dimostra che le società di servizi finanziari nell'APAC potrebbero tentare di aumentare la loro segmentazione alla luce del numero di attacchi ransomware con cui vengono prese di mira.

Coloro che hanno segmentato più di due risorse/aree per area geografica nel settore dei servizi finanziari

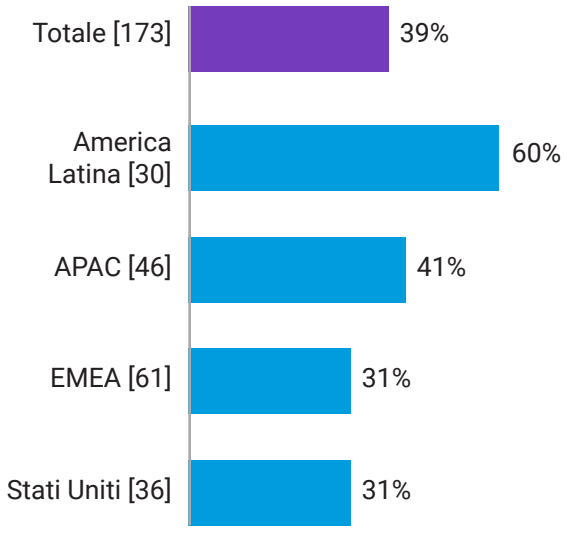


Figura 2. Per ognuna delle seguenti misure di sicurezza IT, quali sono le risorse eventualmente coperte? Il grafico mostra le risposte per la sola misura di sicurezza della segmentazione e le percentuali che utilizzano la segmentazione per proteggere le risorse chiave, suddivise per area geografica (mostrati i numeri di base) (dati relativi solo al settore dei servizi finanziari).

Gli attacchi ransomware non solo sono più frequenti nel 2023 rispetto al 2021, ma hanno anche un impatto maggiore (Figura 3): i nostri intervistati indicano un incremento dei tempi di downtime della rete e della perdita di dati, che aumentano entrambi notevolmente la pressione esercitata sui team addetti alla sicurezza. Si è osservato anche un aumento nella percentuale degli intervistati che segnalano premi assicurativi più alti, particolarmente da parte degli intervistati negli Stati Uniti (56%) a dimostrare il livello di rischio in cui possono incorrere le società di servizi finanziari, che spesso conservano i dati non solo sugli utenti, ma anche sulle loro aziende.

Vediamo l'effetto di questa pressione anche in termini di strategia: la percentuale di società di servizi finanziari che aggiornano continuamente le strategie o le policy di cybersicurezza è passata dal 3% nel 2021 al 18% nel 2023, in risposta non solo ai ransomware, ma anche ad una superficie di attacco in costante evoluzione. La distribuzione della forza lavoro e la migrazione di applicazioni e dati nel cloud sono solo due dei fattori che influenzano quotidianamente la strategia di sicurezza.

Impatto dei ransomware/attacchi informatici sulle società di servizi finanziari

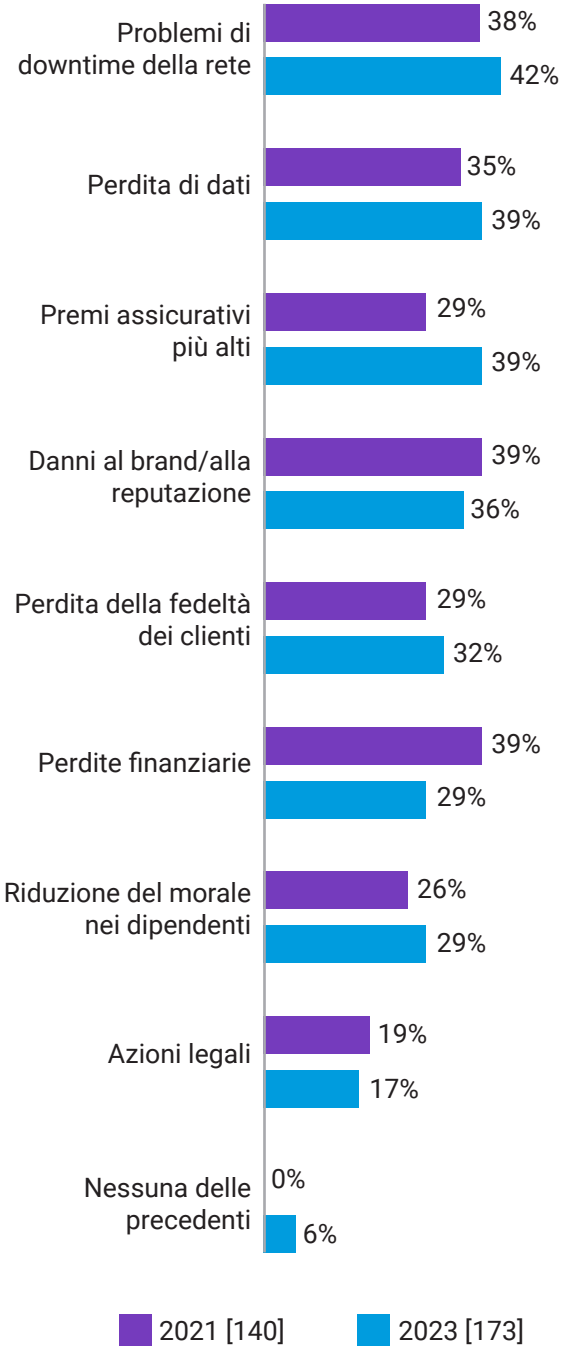


Figura 3. Quando è stato rilevato in precedenza un ransomware o un altro attacco informatico, quali dei seguenti impatti ha avuto sulla vostra organizzazione? Il grafico mostra le dimensioni di base per anno, suddivise per dati cronologici, e non mostra tutte le opzioni di risposta (dati relativi solo al settore dei servizi finanziari).

La segmentazione è la pietra miliare del modello Zero Trust

I nostri intervistati che operano nel settore dei servizi finanziari concordano sull'importanza della segmentazione nel garantire la sicurezza delle loro organizzazioni e, in particolare, nell'affrontare i malware: il 66% di essi afferma che la segmentazione è estremamente importante e il 92% ritiene che sia fondamentale per contribuire a contrastare gli attacchi più devastanti.

Inoltre, la segmentazione contribuisce in modo determinante all'adozione di un sistema Zero Trust. Quando si è citato il motivo per cui un'organizzazione ha avviato un progetto di segmentazione, la risposta più comune è stata quella di promuovere il sistema Zero Trust: quasi tutti gli intervistati che hanno adottato la segmentazione stanno implementando o hanno già implementato un sistema di sicurezza Zero Trust (99%), anche se meno della metà di essi (47%) segnala che il proprio sistema Zero Trust è finalizzato e definito e, pertanto, può essere considerato ad un livello avanzato.

La maggioranza degli intervistati che operano nelle società di servizi finanziari aspira a spingersi oltre e a implementare la microsegmentazione, che protegge i carichi di lavoro delle applicazioni a livello granulare: l'88% dichiara che la microsegmentazione è almeno una priorità elevata, mentre il 39% la indica come priorità assoluta. Gli intervistati dell'America Latina sono i più propensi a considerare la microsegmentazione come una priorità assoluta (50%) rispetto agli intervistati dell'area EMEA (31%), che sono i meno propensi al riguardo. Il fatto che gli intervistati dell'America Latina siano più propensi a segnalare la microsegmentazione come una priorità assoluta si riflette nelle loro performance (Figura 1) a indicare che le organizzazioni che danno priorità alla microsegmentazione possono aspettarsi di trarne benefici.

Inoltre, il 99% dei responsabili decisionali IT in questo settore riferiscono che la microsegmentazione è stata adottata almeno da una minoranza del loro settore, sottolineando che si tratta di una soluzione di cui quasi tutti hanno un'ampia consapevolezza.

Perseverare produce risultati trasformativi

La dura realtà è che, nonostante in larga parte concordino sul fatto che la segmentazione sia la chiave per fermare gli attacchi, l'implementazione della segmentazione è stata lenta, forse più di quanto ci si aspettasse. Solo il 39% delle società di servizi finanziari ha segmentato più di due delle aree aziendali più importanti nel 2023 (rispetto al 26% nel 2021), mentre il 45% ha avviato l'ultimo progetto di segmentazione della rete almeno due anni fa, il che suggerisce uno stallo.

La lentezza delle implementazioni è spiegata più chiaramente dai principali ostacoli incontrati dagli intervistati: aumento dei colli di bottiglia delle performance (41%), mancanza di competenze/esperienza nella segmentazione (39%) e requisiti di conformità (35%). Vale la pena notare che, sebbene la mancanza di risorse o esperienza sia una delle ragioni principali del ritardo nei progetti di segmentazione, una carenza di talenti si avverte nell'intero settore della cybersicurezza e, con i cambiamenti che avvengono così rapidamente in questo settore, è normale rilevare lacune di competenze.

Tuttavia, se suddivisi per area geografica (Figura 4), gli ostacoli che con maggiore probabilità si incontreranno sono diversi tra loro a indicare che alcuni problemi possono essere determinati tanto quanto, se non di più, da condizioni locali (ad esempio, mancanza di competenze negli Stati Uniti, problemi di conformità nell'APAC) anziché da questioni globali.

Nonostante i lenti progressi, i tassi di segmentazione stanno gradualmente aumentando. La percentuale di organizzazioni con applicazioni/dati business-critical (nonché server) segmentati è aumentata fino al 17% dal 2021 al 2023. Questi aumenti superano gli incrementi medi complessivi che sono stati osservati in tutti i settori (rispettivamente, 12% e 8%) a indicare che i reparti IT delle società di servizi finanziari sono in qualche modo più capaci della maggior parte delle aziende ad affrontare gli ostacoli incontrati, probabilmente per il fatto che i summenzionati requisiti di conformità generalmente rigidi richiedono un livello di sicurezza sempre più elevato. Tuttavia, un altro motivo potrebbe essere anche collegato ai premi assicurativi più alti che le società di servizi finanziari devono affrontare: infatti, le compagnie assicurative potrebbero imporre ai propri clienti di affrontare determinati problemi il più rapidamente possibile.

Ostacoli incontrati durante la segmentazione della rete nel settore dei servizi finanziari (primi tre per area geografica)

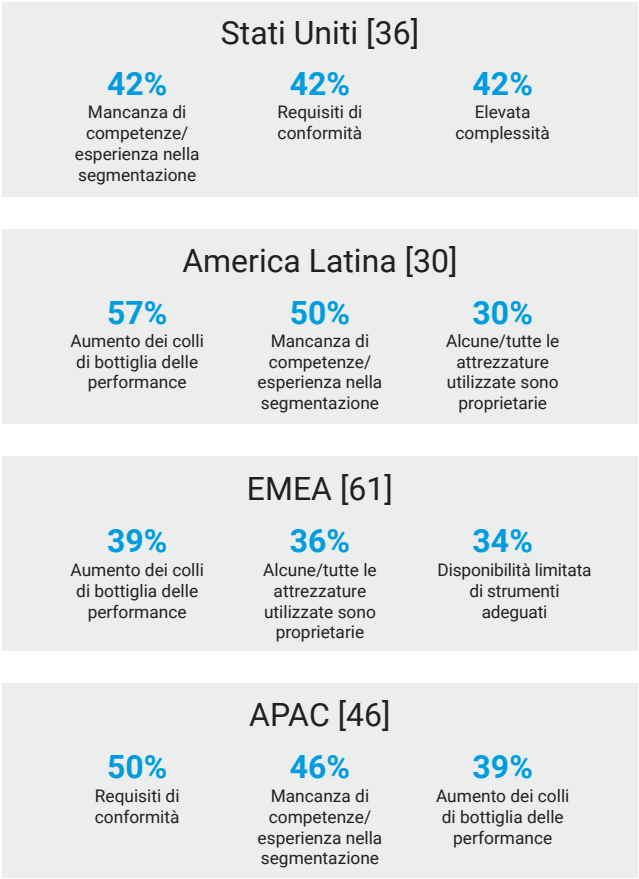


Figura 4. Quali eventuali problemi la vostra organizzazione ha incontrato/prevede di incontrare durante la segmentazione della rete? Il grafico mostra le dimensioni di base per area geografica, riportando solo coloro che a un certo punto hanno segmentato la rete, con le prime tre risposte selezionate per area geografica (dati relativi solo al settore dei servizi finanziari).

Coloro che hanno segmentato sei aree aziendali critiche hanno ridotto notevolmente il rischio

La protezione e la segmentazione di un maggior numero di risorse rendono immediatamente più sicure le società di servizi finanziari. I team addetti alla sicurezza sono maggiormente in grado di identificare gli attacchi e possono rispondere in modo molto più efficace. L'implementazione di strategie di segmentazione non appropriate o non definite correttamente aumenta solo la vulnerabilità, ma, se eseguita correttamente, la segmentazione migliora la resilienza informatica e impedisce agli attacchi informatici di causare importanti interruzioni aziendali, evitando che i ransomware e le violazioni possano diffondersi ai sistemi e ai dati critici.

I nostri risultati mostrano che, dopo una violazione, il recupero avviene 13 ore più velocemente con la segmentazione.
Facciamo due calcoli: per le società di servizi finanziari che hanno implementato la segmentazione in sei aree mission-critical, sono necessarie, in media, tre ore per bloccare completamente un attacco ransomware. Per coloro che hanno implementato la segmentazione su una sola risorsa, sono necessarie 16 ore.

Allo stesso modo, la segmentazione consente di risparmiare 11 ore di contenimento del movimento laterale.
Per coloro che hanno implementato la segmentazione in tutte e sei le aree mission-critical, sono necessarie in media tre ore per limitare in modo significativo gli spostamenti laterali di un attacco ransomware. Per coloro che hanno implementato la segmentazione su una sola risorsa, sono necessarie in media 14 ore.

Considerate la differenza per il vostro team, i danni al brand e i costi sostenuti durante queste 11 - 13 ore, a seconda dei casi.

Per contrastare un attacco

3 ore

Il tempo necessario, in media, per bloccare completamente un attacco ransomware, per coloro che hanno segmentato tutte e sei le risorse aziendali. Per coloro che hanno segmentato una sola risorsa: **16 ore**

Per limitare il movimento

3 ore

Il tempo necessario, in media, per limitare in modo significativo il movimento laterale di un attacco ransomware, per coloro che hanno segmentato tutte e sei le risorse aziendali. Per coloro che hanno segmentato una sola risorsa: **14 ore**

In che modo una soluzione di microsegmentazione basata su software aiuta a risolvere le sfide

Le società di servizi finanziari cercano di potenziare la scalabilità, sfruttare gli investimenti esistenti, ottimizzare i costi e migliorare l'agilità e la flessibilità mediante la migrazione sul cloud dei carichi di lavoro, spesso integrando i data center on-premise con i cloud pubblici o privati. Le soluzioni di segmentazione definita dal software, come Akamai Guardicore Segmentation, sono emerse come un approccio alla sicurezza a livello applicativo più flessibile, funzionale e conveniente, velocizzando notevolmente l'implementazione, semplificando la manutenzione e mitigando le minacce in modo efficace. Poiché questo metodo è più rapido e semplice da implementare rispetto agli approcci basati su infrastrutture come firewall e VLAN, consente alle società di servizi finanziari di raggiungere una sicurezza su larga scala e di soddisfare, al tempo stesso, le crescenti richieste aziendali, offrendo customer experience innovative con tecnologie all'avanguardia. Inoltre, è perfettamente compatibile con diversi sistemi e ambienti, fornendo una gestione e un controllo centralizzati, dai server bare metal alle implementazioni multicloud e ai sistemi legacy. Pertanto, offre una soluzione unificata per visualizzare e controllare le connessioni nell'intero ambiente, indipendentemente dalla loro posizione fisica.

Come facilita la distribuzione

La microsegmentazione genera innanzitutto una visualizzazione interattiva di tutte le connessioni che vengono effettuate nell'ambiente, un elemento fondamentale per superare i principali ostacoli all'implementazione. Inoltre, noi di Akamai abbiamo integrato nella nostra soluzione dei modi attivi per affrontare i colli di bottiglia delle performance e i requisiti di conformità.

I colli di bottiglia delle performance non derivano necessariamente da uno sforzo tecnico del sistema causato da una soluzione di segmentazione, ma da colli di bottiglia della forza lavoro causati dalla necessità di segmentare manualmente le aree aziendali e di risolvere manualmente i problemi che interessano tali aree quando si verificano. Akamai si adopera per risolvere questo problema (e l'ostacolo numero uno all'implementazione, ossia la mancanza di competenze) riducendo la necessità di eseguire la segmentazione manualmente e offrendo un supporto tecnico e servizi professionali di alto livello. I nostri esperti di segmentazione collaborano con voi durante l'intero processo di implementazione per garantire il raggiungimento degli obiettivi di segmentazione nel vostro ambiente IT esclusivo.

Il supporto all'implementazione deriva anche dalla soluzione stessa: le raccomandazioni di policy basate sull'intelligenza artificiale e i modelli di policy già pronti per i casi d'uso più comuni fanno risparmiare tempo e clic, semplificano il flusso di lavoro, riducono il tempo complessivo di implementazione delle policy e prevengono le configurazioni errate dovute a errori umani. Per uno dei nostri clienti, siamo stati in grado di realizzare un progetto di segmentazione granulare che avrebbe richiesto due anni e oltre un milione di dollari di costi totali in sole sei settimane con un solo tecnico, riducendo il costo complessivo del progetto dell'85%, dimostrando che la segmentazione granulare può essere implementata in modo rapido e semplice, senza subire colli di bottiglia.

Come la microsegmentazione facilita la conformità

Molti dei nostri clienti utilizzano la nostra soluzione per garantire e attestare la conformità a una serie di mandati di conformità, come PCI-DSS, SWIFT, Sarbanes-Oxley, GDPR, DORA e molti altri. Questi mandati normativi, di solito, richiedono che i dati in questione siano separati dagli altri sistemi dell'ambiente. Sebbene ciò possa essere proibitivo utilizzando firewall e VLAN, la nostra soluzione basata su software consente di creare segmenti specifici per i dati in questione e di applicare regole di comunicazione su chi può o non può accedere a tali dati. Utilizzando la nostra mappa visiva con visualizzazioni quasi in tempo reale e storiche, potete attestare la vostra conformità a questi mandati dimostrando fisicamente che i dati in questione non sono accessibili a utenti e computer non autorizzati.

Perseverare con la soluzione e il supporto giusti per trasformare la strategia di sicurezza

La segmentazione può risultare complessa. Tuttavia, come dimostra questo rapporto, chi riesce a implementarla in modo efficace vede migliorare la sicurezza della rete, incrementare le performance della rete e la conformità e semplificare la gestione della rete. Una segmentazione adeguata limita il movimento laterale delle minacce e consente di reagire più rapidamente durante una violazione attiva. E dopo una violazione, le operazioni di ripristino sono più sicure e richiedono meno tempo.

Scegliere una soluzione progettata per superare le sfide comuni all'implementazione della segmentazione, e collaborare con esperti del settore durante il percorso, vi mette nella migliore posizione possibile per trasformare la vostra strategia di sicurezza. Inoltre, più aree aziendali segmentate, più fate progredire la vostra architettura Zero Trust, riducendo il rischio attuale e garantendo una difesa di prima linea contro i vettori di minaccia futuri.

Risultati per area geografica

La segmentazione e la microsegmentazione sono considerate più importanti nell'area EMEA e negli Stati Uniti che in America Latina: i responsabili decisionali della sicurezza IT nell'area EMEA (70%) e negli Stati Uniti (60%) sono più propensi ad affermare che la segmentazione della rete è estremamente importante per garantire la sicurezza delle loro organizzazioni rispetto a quelli in America Latina (57%).

Gli intervistati dell'America Latina sono più propensi ad affermare che la microsegmentazione è la priorità assoluta: (50%) rispetto alle controparti negli Stati Uniti (42%), nell'APAC (41%) e nell'area EMEA (31%).

Gli intervistati dell'area EMEA sono più propensi ad affermare di non aver effettuato alcuna segmentazione: gli intervistati dell'area EMEA sono più propensi ad affermare di non aver segmentato alcuna risorsa business-critical (7%) rispetto a tutte le altre aree geografiche, in cui è stata eseguita una segmentazione parziale.

Gli intervistati dell'America Latina sono i più propensi ad affermare di aver compiuto i migliori progressi nella segmentazione: le società di servizi finanziari dell'America Latina sono più propense ad affermare di aver segmentato più di due risorse business-critical (60%) rispetto a quelle dell'APAC (41%), dell'area EMEA (31%) e degli Stati Uniti (31%).

Le organizzazioni in tutte le aree geografiche devono affrontare alcune sfide: il 98% degli intervistati nell'APAC afferma di aver incontrato problemi durante la segmentazione della rete e una percentuale simile ha affermato lo stesso negli Stati Uniti (97%), mentre le percentuali sono state leggermente inferiori nell'area EMEA (89%) e in America Latina (87%).

Le società di servizi finanziari in America Latina sono molto più avanti nel processo di implementazione del sistema di sicurezza Zero Trust: gli intervistati in America Latina sono molto più propensi a dichiarare che l'implementazione del loro sistema Zero Trust è pienamente completa e definita (57%) rispetto a quelli dell'area EMEA (47%) e dell'APAC (41%).

Il nostro gruppo di sondaggio

Per lo studio di ricerca completo, abbiamo intervistato 1.200 responsabili decisionali del settore IT e della sicurezza in 10 paesi allo scopo di misurare i progressi compiuti dalle organizzazioni in termini di protezione dei loro ambienti, focalizzandoci sul ruolo della segmentazione.

Agli intervistati sono state poste domande sui loro sistemi di sicurezza IT e sulle strategie di segmentazione adottate, nonché sulle minacce che le loro organizzazioni si sono trovate ad affrontare nel 2023. Dai dati e dai risultati emersi, possiamo comprendere come le strategie di sicurezza siano cambiate a partire dal 2021 e le aree che ancora necessitano di miglioramenti.

Hanno partecipato al sondaggio intervistati che lavorano in tutto il mondo, inclusi Stati Uniti, India, Messico, Brasile, Regno Unito, Francia, Germania, Cina, Giappone e Australia, all'interno di aziende che impiegano oltre 1.000 dipendenti e operano in vari settori e industrie.

Per gli scopi di questo rapporto, abbiamo analizzato 173 intervistati (nel 2023) e 140 intervistati (nel 2021) che operano nel settore dei servizi finanziari.

Scoprite ulteriori informazioni su Akamai Guardicore Segmentation

A sostegno e protezione della vita online c'è sempre Akamai. Le principali aziende al mondo scelgono Akamai per creare, offrire e proteggere le loro experience digitali, aiutando miliardi di persone a vivere, lavorare e giocare ogni giorno. 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 di Akamai per i servizi finanziari, visitate il sito akamai.com/finserv o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 05/24.

Vanson Bourne è un'azienda indipendente specializzata in ricerche di mercato per il settore tecnologico. La sua reputazione di azienda in grado di offrire analisi solide e credibili si basa su principi di ricerca rigorosi e sulla capacità di raccogliere le opinioni di responsabili decisionali senior in tutti i ruoli tecnici e commerciali, in tutti i settori e in tutti i principali mercati. Per altre informazioni, visitate il sito www.vansonbourne.com.