WHITE PAPER

Analisi degli scenari di utilizzo principali per la segmentazione del software

Di John Grady, Senior Analyst di Enterprise Strategy Group

Gennaio 2023

Questo white paper di Enterprise Strategy Group è stato commissionato da Akamai e viene distribuito su licenza da TechTarget, Inc.

Sommario

Executive summary 3

L'approccio zero trust è sempre più diffuso, ma è fondamentale definire chiaramente le priorità 3

Attualmente la segmentazione del software è ancora sottoutilizzata come strumento di supporto del modello zero trust 5

Scenari di utilizzo principali per la segmentazione del softwaress 6

- Prevenzione delle minacce 7
- Promozione dell'efficienza nell'intera azienda 7
- Segmentazione zero trust 8

L'approccio di Akamai alla segmentazione del software 9

Conclusioni 10

Executive summary

Oggi l'approccio zero trust viene utilizzato ovunque nel settore della sicurezza informatica. Ciononostante, l'ampia portata dell'iniziativa e le opinioni discordanti sugli aspetti più importanti per la strategia hanno creato confusione in merito al punto di partenza e agli strumenti da utilizzare per garantire un supporto ottimale del framework. Anche se non esiste un singolo percorso per l'adozione dell'approccio zero trust, tale strategia dipende essenzialmente dalla comunicazione fra le varie entità e risorse, laddove sia espressamente consentita dalle policy, e questo sottolinea l'importanza della segmentazione del software.

Attualmente gli strumenti per la segmentazione del software non sono molto diffusi, ma si prevede un incremento significativo del loro utilizzo in seguito al riconoscimento dell'importanza critica di questo framework per l'approccio zero trust e della sua applicabilità a una vasta gamma di scenari di utilizzo. La segmentazione del software è utile a tutte le imprese che desiderano implementare un approccio zero trust allo scopo di prevenire le minacce, promuovere l'efficienza in tutto l'ambiente aziendale o adottare un approccio più moderno alla sicurezza in generale. In particolare, l'approccio di Akamai alla segmentazione del software, basato sul software e supportato dall'intelligenza artificiale, offre una visibilità granulare e consente di prevenire gli spostamenti laterali, bloccare gli attacchi ransomware e applicare i principi zero trust in modo coerente all'intero ambiente aziendale.

La segmentazione del software è utile a tutte le imprese che desiderano implementare un approccio zero trust allo scopo di prevenire le minacce, promuovere l'efficienza in tutto l'ambiente aziendale o adottare un approccio più moderno alla sicurezza in generale.

L'approccio zero trust è sempre più diffuso, ma è fondamentale definire chiaramente le priorità

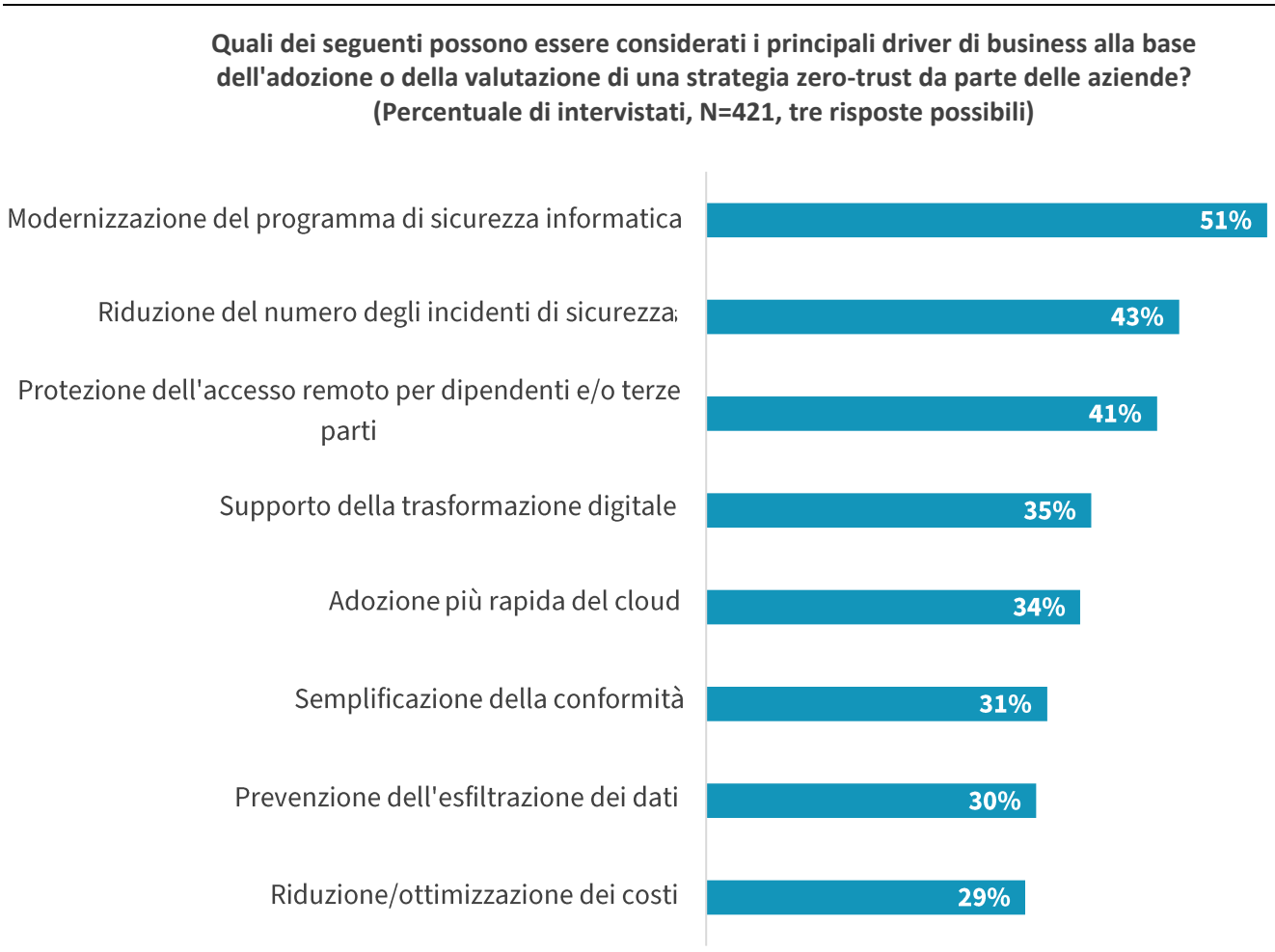
Il trasferimento delle risorse nel cloud, l'affermazione dei modelli di business digitali e una base di utenti sempre più distribuita non fanno che aumentare la complessità degli ambienti aziendali. Questi cambiamenti rendono intrinsecamente più difficile il lavoro del team di sicurezza informatica, perché gli hacker cercano di intrufolarsi nelle falle dei sistemi di difesa per sferrare attacchi ransomware, impossessarsi dei dati dei clienti o esfiltrare informazioni sensibili di proprietà intellettuale. Purtroppo, di fronte a queste realtà, gli approcci tradizionali alla sicurezza incentrati su controlli troppo permissivi basati sul perimetro non sono più sufficienti, e i team di sicurezza si vedono costretti a riconsiderare le loro strategie. Come se non bastasse, di fronte ad attacchi sempre più numerosi e sofisticati, i team di sicurezza non riescono più a gestire e creare le patch necessarie a contrastare tutte le potenziali minacce.

Questo panorama ha spinto molte organizzazioni verso lo zero trust. Anche se non sono una novità, le strategie zero trust hanno attirato l'interesse delle aziende fornendo uno strumento per l'adozione di un approccio alla sicurezza informatica più dinamico, meno permissivo e basato in misura maggiore sul rischio. L'approccio zero trust elimina il concetto di fiducia implicita in tutto l'ambiente, imponendo la convalida continua di ogni singola interazione digitale, in modo da aumentare notevolmente la probabilità che le risorse, gli utenti e i dispositivi rimangano sicuri e disponibili. Tuttavia, il vasto campo di applicazione dell'approccio zero trust, abbinato a definizioni e punti di vista spesso contrastanti, ha creato confusione, impedendo alle aziende di identificare chiaramente il punto di partenza.

Valutare le priorità aziendali e i risultati auspicati consente di circoscrivere l'obiettivo e determinare più facilmente il contesto ottimale per l'avvio di un'iniziativa zero trust. I driver di business che spingono le aziende ad adottare un approccio zero trust sono numerosi (Figura 1).[1] L'obiettivo più comune è costituito dalla modernizzazione della sicurezza informatica, menzionata dal 51% degli intervistati. Questa mentalità è stata incentivata dal governo federale statunitense, attraverso una serie di ordini esecutivi sulla sicurezza informatica emanati dall'amministrazione Biden, che ha inserito l'architettura zero trust fra i requisiti della modernizzazione. Anche se non erano rivolti direttamente al settore privato, questi ordini possono comunque fornire un'indicazione anche ai team di sicurezza che non operano nella pubblica amministrazione. Gli altri obiettivi strategici dell'approccio zero trust includono il supporto della trasformazione digitale (35%) e un'adozione più rapida del cloud (34%). Questi driver sottolineano il fatto che, in molte aziende, il team di sicurezza deve contribuire alla crescita del business, anziché limitarsi alla semplice protezione degli asset. Anche gli obiettivi più strategici, come la riduzione degli incidenti di sicurezza (43%), la protezione dell'accesso remoto (41%), la semplificazione della conformità (31%) e la prevenzione dell'esfiltrazione dei dati (30%), sono molto comuni.

L'approccio zero trust ha lo scopo di garantire la comunicazione fra le varie entità e risorse solo se espressamente consentito dalle policy.

Figura 1. Driver per l'adozione di un approccio zero trust



Fonte: Enterprise Strategy Group, una divisione di TechTarget, Inc.

[1] Fonte: Risultati del sondaggio *The State of Zero Trust Security Strategies* di Enterprise Strategy Group, maggio 2021.

In alcuni casi, circoscrivendo in modo più preciso l'obiettivo del progetto zero trust, è possibile aiutare il team di sicurezza a identificare gli strumenti necessari per supportare la strategia. Se ad esempio si punta a migliorare la sicurezza dell'accesso remoto per dipendenti e terze parti, in molti casi si finisce per adottare una soluzione di accesso alla rete zero trust (ZTNA, Zero Trust Network Access). In questo scenario possono entrare in gioco anche gli strumenti di gestione delle identità, come l'autenticazione a più fattori (MFA, MultiFactor Authentication). Tuttavia, alcuni driver possono lasciare un ampio margine di interpretazione sui requisiti tecnologici e, nonostante la restrizione dell'ambito, molte aziende continuano a concentrarsi su molteplici obiettivi. In questi casi, è importante identificare strumenti e procedure che consentano di supportare una vasta gamma di scenari di utilizzo e risultati.

Attualmente la segmentazione del software è ancora sottoutilizzata come strumento di supporto del modello zero trust

Anche se non esiste un singolo percorso per l'adozione dell'approccio zero trust, in ultima analisi la strategia ha lo scopo di garantire la comunicazione fra le varie entità e risorse solo se espressamente consentito dalle policy. Questo significa che la filosofia zero trust delle aziende dovrebbe essere incentrata sulla possibilità di garantire una segmentazione appropriata degli asset, allo scopo di limitare gli effetti degli attacchi riusciti. Ciò è applicabile sia agli obiettivi di vasta portata, come la modernizzazione della sicurezza informatica, sia a quelli più mirati, come la prevenzione dell'esfiltrazione dei dati.

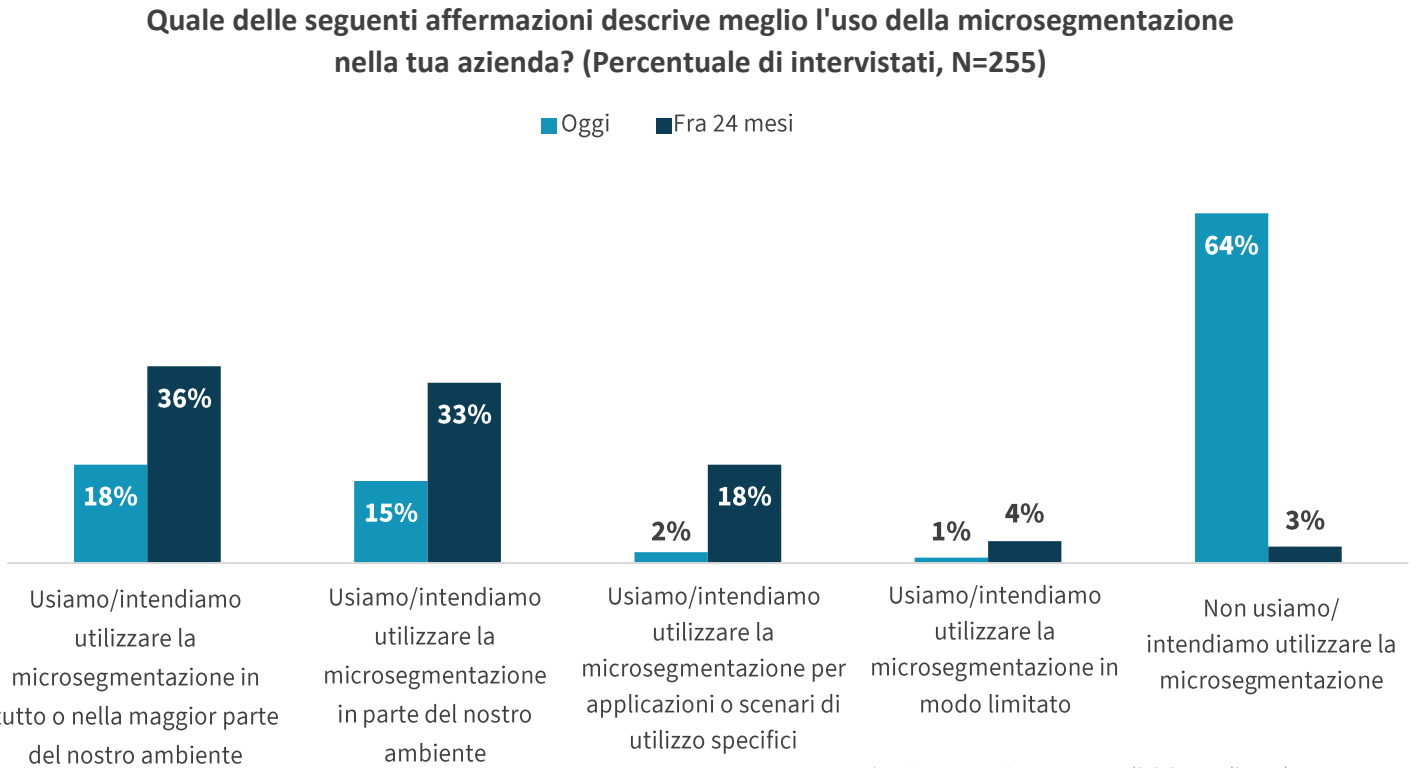
Negli ambienti di oggi, tuttavia, una segmentazione grossolana non è sufficiente, e per proteggere adeguatamente gli asset aziendali occorre una segmentazione più granulare del software. Le moderne architetture applicative dipendono spesso da carichi di lavoro distribuiti su diverse istanze server e, in alcuni casi, fra molteplici ambienti cloud. La segmentazione delle risorse basata sulla posizione è ormai obsoleta, perché non consente di gestire le problematiche a cui si trovano attualmente di fronte i team di sicurezza.

Le aziende sono sempre state riluttanti ad adottare gli strumenti di segmentazione del software. Una ricerca condotta dalla divisione Enterprise Strategy Group (ESG) di TechTarget dimostra che, per il 28% delle aziende, la segmentazione del software è troppo complessa. Tuttavia, questo è dovuto soprattutto al fatto che i team di sicurezza non utilizzano strumenti adatti allo scopo. Nello specifico, dalla ricerca ESG emerge che il 55% delle aziende utilizza strumenti basati sull'infrastruttura, come i firewall, per la segmentazione del software, mentre solamente l'8% usa strumenti basati sull'host.[2] I firewall non consentono di applicare le policy granulari necessarie per una segmentazione efficace del software. Inoltre, tali strumenti offrono solo una visibilità limitata sui carichi di lavoro applicativi, e difficilmente riescono a gestire tutti gli aspetti di un ambiente che include sia risorse on-premise che cloud.

Tutto ciò ha finito per limitare l'utilizzo della segmentazione del software. Nonostante la sua importanza critica per l'approccio zero trust, secondo la ricerca di ESG oggi solo il 36% delle aziende usa la segmentazione del software (Figura 2). Per fortuna molte aziende riconoscono che si tratta di una grave lacuna nel loro sistema di difesa. Di conseguenza, il 91% degli intervistati prevede di utilizzare la segmentazione del software nei prossimi 24 mesi.[3] Sostanzialmente, la segmentazione del software consolida e amplifica i principali vantaggi dell'approccio zero trust, proteggendo le reti fisiche, virtuali e cloud dalle minacce sia interne che esterne, e dovrebbe costituire un componente chiave di qualunque strategia zero trust.

[2] Fonte: Risultati completi del sondaggio *Network Security Trends in Hybrid Cloud Environments* di Enterprise Strategy Group, dicembre 2021.
[3] Ibid.

Figura 2. Adozione della segmentazione del software



Fonte: Enterprise Strategy Group, una divisione di TechTarget, Inc.

Scenari di utilizzo principali per la segmentazione del softwaress

La segmentazione del software è ampiamente applicabile a una vasta gamma di scenari di utilizzo dell'approccio zero trust, un vantaggio che in questo momento viene sottolineato più che mai. Innanzitutto e soprattutto, la segmentazione del software fornisce un ottimo punto di partenza per un percorso zero trust, perché consente di proteggere gli asset più critici per l'azienda, soprattutto se la soluzione adottata garantisce una visibilità altamente granulare sulle relazioni che legano carichi di lavoro ed entità. In qualunque iniziativa zero trust è fondamentale sviluppare una baseline dei flussi di traffico e delle dipendenze, per cominciare a eliminare la fiducia implicita senza interferire con il business. Questo approccio permette ai team di sicurezza di proteggere velocemente gli asset più critici per limitare gli effetti di una potenziale violazione mentre l'implementazione dell'approccio zero trust è ancora in corso. Sapendo di poter contare su questa garanzia, i team di sicurezza possono concentrarsi su alcuni degli altri scenari di utilizzo supportati dalla segmentazione del software.

Prevenzione delle minacce

L'approccio zero trust è un framework di sicurezza, e la sicurezza ha lo scopo di proteggere l'azienda dalle minacce informatiche. Proprio per questo, alcuni dei principali scenari di utilizzo della segmentazione del software sono incentrati sulla prevenzione delle minacce e sulla limitazione dei relativi effetti per le risorse aziendali. Nello specifico:

- Isolamento degli asset critici. Nel decidere le priorità di protezione, i team di sicurezza devono soppesare e bilanciare il rischio. Le applicazioni di alto valore che contengono informazioni dei clienti regolamentate, proprietà intellettuale o altri dati sensibili dovrebbero ricevere più attenzione e beneficiare di controlli di sicurezza più efficaci, a causa del potenziale impatto della compromissione di tali sistemi. La segmentazione del software consente ai team di sicurezza di garantire che tali applicazioni, e i carichi di lavoro da cui sono formate, sono completamente separati dal resto dell'infrastruttura.
- Limitazione degli spostamenti laterali. Un principio poco valorizzato dell'approccio zero trust è costituito dalla "presunzione di vulnerabilità", che consiste nel presupporre che gli avversari abbiano già ottenuto l'accesso alla rete aziendale. Infatti, a causa della proliferazione di endpoint tradizionali, server, risorse cloud e persino dispositivi intelligenti, le intrusioni sono inevitabili. Di conseguenza la segmentazione del software consente di limitare il raggio d'azione di un potenziale attacco, impedendo agli hacker di spostarsi lateralmente nella rete.

Protezione dal ransomware

I continui attacchi ransomware e i relativi effetti hanno portato il problema all'attenzione dei dirigenti, se non addirittura del Consiglio di amministrazione delle imprese. Se per prepararsi a un attacco ransomware sono necessari ottimi livelli di protezione dei dati e una capacità adeguata di rispondere agli incidenti, oltre a un sistema di sicurezza affidabile, la segmentazione del software aiuta le aziende a mettersi nella posizione ideale per contrastarlo. Durante un attacco, gli hacker si concentrano sui sistemi e sulle informazioni sensibili solo dopo essersi introdotti nell'ambiente e aver dedicato un po' di tempo all'identificazione degli obiettivi. Se si utilizza la segmentazione del software per isolare gli asset critici e limitare gli spostamenti laterali, gli hacker hanno meno libertà di movimento all'interno dell'ambiente. Inoltre, quando viene rilevato un attacco ransomware, un'azienda che utilizza la segmentazione del software può chiudere velocemente i canali di comunicazione utilizzati dagli hacker e isolare i server infetti, in modo da prevenire l'ulteriore propagazione dell'attacco.

- Rilevamento delle minacce e risposta. In caso di attacco, il tempo gioca un ruolo chiave. Gli strumenti di segmentazione del software possono aiutare i team di sicurezza a rispondere in modo rapido ed efficace, identificando tempestivamente i possibili canali di propagazione dell'attacco sulla base delle relazioni fra le applicazioni, bloccando le porte utilizzate dagli hacker durante l'attacco e mettendo velocemente in quarantena i sistemi interessati, per isolarli dal resto della rete. Inoltre, in questo modo l'attacco viene contenuto presso il punto di accesso iniziale.

Promozione dell'efficienza nell'intera azienda

Oggi, oltre ad adempiere alla propria mansione principale di proteggere l'ambiente, i team di sicurezza devono anche evitare di interferire in qualsiasi modo con l'efficienza del business. Inoltre, quando il team di sicurezza riesce effettivamente ad aiutare i colleghi, genera un vantaggio per l'intera azienda, che può manifestarsi in diversi modi. I più comuni includono:

- Supporto dell'adozione del cloud. La transizione al cloud non è certo una novità, ma i problemi di sicurezza rimangono la preoccupazione principale nella maggior parte delle aziende. In molti casi ciò è dovuto alla scarsa familiarità con i controlli di sicurezza nativi delle piattaforme Infrastructure-as-a-Service, mentre in altri dipende dall'approccio incoerente alla sicurezza riscontrato in molti ambienti di cloud ibrido. La segmentazione del software offre alle aziende un livello di sicurezza superiore, perché i controlli possono essere applicati a tutti gli aspetti dell'ambiente, garantendo una coerenza superiore negli scenari di cloud ibrido.

- Supporto della modernizzazione delle applicazioni. Oltre a quella del cloud, sta accelerando anche l'adozione delle moderne architetture applicative, come quelle basate su container. Questi modelli consentono ai team applicativi di progettare, creare e implementare le applicazioni con una velocità senza precedenti. Gli strumenti capaci di garantire la protezione di queste risorse, senza limitare la velocità di sviluppo, influiscono positivamente sul business, mentre gli strumenti di segmentazione del software che forniscono visibilità sui flussi di traffico negli ambienti container e applicano automaticamente le policy di segmentazione, a mano a mano che i container vengono attivati o spostati, possono aiutare i team di sviluppo a garantire la sicurezza delle loro applicazioni.

- Semplificazione della conformità. I problemi di conformità alle normative sottraggono sempre più tempo, denaro e attenzione alle risorse aziendali. Garantendo il massimo isolamento dei rischi per la sicurezza, al fine di limitare potenziali problemi come la violazione della riservatezza dei dati o una fuga di informazioni personali, è possibile rendere questo processo molto meno oneroso. La segmentazione del software assicura l'isolamento dei sistemi regolamentati dal resto dell'ambiente, alleviando il carico di lavoro dei team di sicurezza.

Segmentazione zero trust

Uno degli aspetti più interessanti della segmentazione del software è costituito dalla possibilità di fornire vantaggi immediati all'azienda, se applicata a scenari di utilizzo estremamente mirati. Molte aziende sono attratte dalla possibilità di creare elenchi di esclusione, isolare le applicazioni critiche, segmentare l'ambiente e utilizzare altre policy meno complicate che forniscono valore in modo rapido e relativamente semplice. Ben poche imprese, sempre che ce ne siano, implementano in un singolo passaggio una strategia completa di segmentazione del software in tutto l'ambiente aziendale. Tuttavia, a mano a mano che la segmentazione del software si diffonde nell'ambiente, nel contesto di un'iniziativa zero trust, molte aziende cominciano ad adottare un approccio di segmentazione zero trust. Questo permette di combinare gli scenari di utilizzo e i vantaggi illustrati in precedenza, garantendo alle aziende una visibilità completa e granulare sui flussi di traffico, proteggendo gli asset più sensibili, prevenendo gli spostamenti laterali e rispondendo tempestivamente alle minacce, il tutto supportando il business in modo ottimale. Anche se non costituisce il punto di partenza di molti progetti di segmentazione del software, questo approccio può essere visto come un obiettivo da raggiungere in un secondo momento.

L'approccio di Akamai alla segmentazione del software

La soluzione Akamai Guardicore Segmentation è un approccio alla segmentazione del software basato sul software, espressamente concepito per impedire ai vettori di minaccia di effettuare spostamenti laterali all'interno dell'ambiente digitale.

È importante ricordare che oltre alla segmentazione del software, che costituisce un aspetto chiave dell'approccio zero trust, esistono anche altri componenti fondamentali, che richiedono tecnologie diverse per supportare le attività di rilevamento delle minacce, con la relativa risposta, la gestione delle identità, la sicurezza dei dati e molto altro ancora. La valutazione, la selezione e la collaborazione con i fornitori di tecnologie richiedono un processo metodico e attento ai dettagli, che può fare la differenza tra il raggiungimento degli obiettivi di sicurezza informatica dell'azienda e la creazione di un'infrastruttura che rischia di assorbire gran parte delle risorse di tempo, denaro e forza lavoro. Di conseguenza, scegliendo strumenti di segmentazione del software capaci di offrire una vasta gamma di integrazioni e funzionalità per la condivisione dei segnali, è possibile sviluppare una strategia zero trust che va oltre la semplice segmentazione del software, riducendo anche la complessità operativa.

Akamai, protagonista storico del mercato delle infrastrutture di rete, ha integrato la segmentazione del software e l'approccio zero trust come elementi di base del suo portafoglio di soluzioni. La profonda conoscenza dei requisiti delle infrastrutture aziendali, sia per gli ambienti on-premise che per gli ambienti cloud, ha permesso ad Akamai di specializzarsi nell'individuazione e nella risoluzione dei potenziali problemi di sicurezza informatica.

Akamai Guardicore Segmentation è un approccio alla segmentazione del software basato sul software, espressamente concepito per impedire ai vettori di minaccia di effettuare spostamenti laterali all'interno dell'ambiente digitale. Sfrutta la visibilità granulare per applicare i principi zero trust a livello di rete, permettendo alle aziende di visualizzare le attività e gli spostamenti all'interno degli ambienti fisici e virtuali. Questo framework di segmentazione basato sull'intelligenza artificiale si avvale di modelli integrati allo scopo di rilevare e bloccare le intrusioni, come il ransomware, gli attacchi basati sugli endpoint e gli attacchi mirati contro la forza lavoro remota. Può essere utilizzato su piattaforme di ogni tipo, inclusi i server bare-metal, le macchine virtuali, i container, i dispositivi IoT e le istanze cloud.

Akamai Guardicore Segmentation raccoglie dati esaustivi sull'infrastruttura sottostante utilizzando vari metodi, come sensori basati su agente, raccolta dei dati attraverso la rete, log dei flussi nei cloud privati virtuali e integrazioni che promuovono le funzionalità agentless. La mappatura dinamica offre agli amministratori una visione end-to-end sulle attività, con una granularità inferiore. Sfruttando l'esperienza di Akamai con gli ambienti di rete aziendali, la soluzione Akamai Guardicore Segmentation è stata espressamente concepita per garantire scalabilità e prestazioni coerenti, identificando ed evitando le cause dei colli di bottiglia del traffico.

Conclusioni

La segmentazione del software non è una tecnologia nuova. In realtà, quando è stata introdotta, probabilmente i tempi non erano ancora maturi. Ma non finiremo mai di sottolineare l'importanza della segmentazione del software per la protezione dei moderni ambienti multi-cloud ibridi e, nello specifico, per l'operazionalizzazione delle strategie zero trust. La segmentazione del software garantisce i livelli di flessibilità, agilità ed efficienza necessari per adottare un approccio zero trust in moltissimi scenari di utilizzo mission-critical e business-critical, proteggendo tutti i componenti, dall'infrastruttura cruciale alla proprietà intellettuale, fino alle identità e alle credenziali. Per la sua esperienza nel campo delle infrastrutture di rete, della segmentazione e della segmentazione del software, Akamai è un ottimo candidato per aiutare le aziende a pianificare, realizzare, implementare e gestire un'infrastruttura protetta, basata sugli strumenti e sugli approcci di segmentazione del software.

Enterprise Strategy Group by TechTarget

Enterprise Strategy Group è un'azienda di analisi, ricerca e strategia tecnologica integrate che fornisce intelligence di mercato, informazioni preziose e servizi per contenuti di go-to-market alla comunità IT globale.

www.esg-global.com contact@esg-global.com 508.482.0188