WHITE PAPER

Un piano per la creazione di un'architettura Zero Trust

Sommario

Introduzione

Nel 2009 Forrester Research iniziò a promuovere il concetto di Zero Trust, avvertendo le organizzazioni che era giunto il momento di rivedere la tradizionale pratica di concedere l'accesso senza restrizioni a qualunque utente o applicazione che varcasse il perimetro di rete. Al contrario, ogni dispositivo, utente e flusso di rete doveva essere verificato prima di concedere un accesso completo. Nel corso degli anni, l'urgenza di adottare il concetto Zero Trust non ha fatto che aumentare, grazie a molti fattori.

Oggi, le aziende continuano ad adottare il lavoro ibrido, pertanto i dipendenti lavorano ovunque grazie ai programmi BYOD con cui possono accedere alle applicazioni e alle risorse aziendali tramite dispositivi gestiti o meno. Le applicazioni possono trovarsi ovunque: nel cloud, on-premise e in ambienti ibridi. A causa di questi cambiamenti, il perimetro della rete non esiste più. Gli attacchi ransomware sono diventati più frequenti e sofisticati, dando più possibilità agli autori di attacchi di violare le difese e aumentare i costi una volta effettuata la violazione. Il costo medio di una violazione di dati negli Stati Uniti ha raggiunto la cifra record a livello globale di 9,36 milioni di dollari, secondo il rapporto IBM 2024 sul costo delle violazioni di dati. Inoltre, l'aumento del numero di dispositivi connessi alla rete, come i dispositivi IoT (Internet of Things), e gli ulteriori requisiti per l'accesso di partner e clienti alla rete sono fattori che hanno contribuito a espandere notevolmente la superficie di attacco di un'azienda.

In questo panorama di cybersicurezza in continua evoluzione, i fornitori di software per la rete e la sicurezza si affrettano a marchiare i loro prodotti come Zero Trust o a lanciare nuovi prodotti, mentre consulenti e analisti coniano nuovi acronimi e definizioni di mercato. Ciò lascia ai team di sicurezza la fatica di dover spiegare questi concetti a volte complessi e prendere decisioni di acquisto in grado di porre le basi per passare a una strategia Zero Trust.

Questo white paper è studiato per offrire ai team di sicurezza un piano che consenta di effettuare investimenti in tecnologie Zero Trust, identificando il punto di partenza e delineando i fattori distintivi più importanti.

Le app cloud per il lavoro ibrido fanno crollare il paradigma di sicurezza della rete

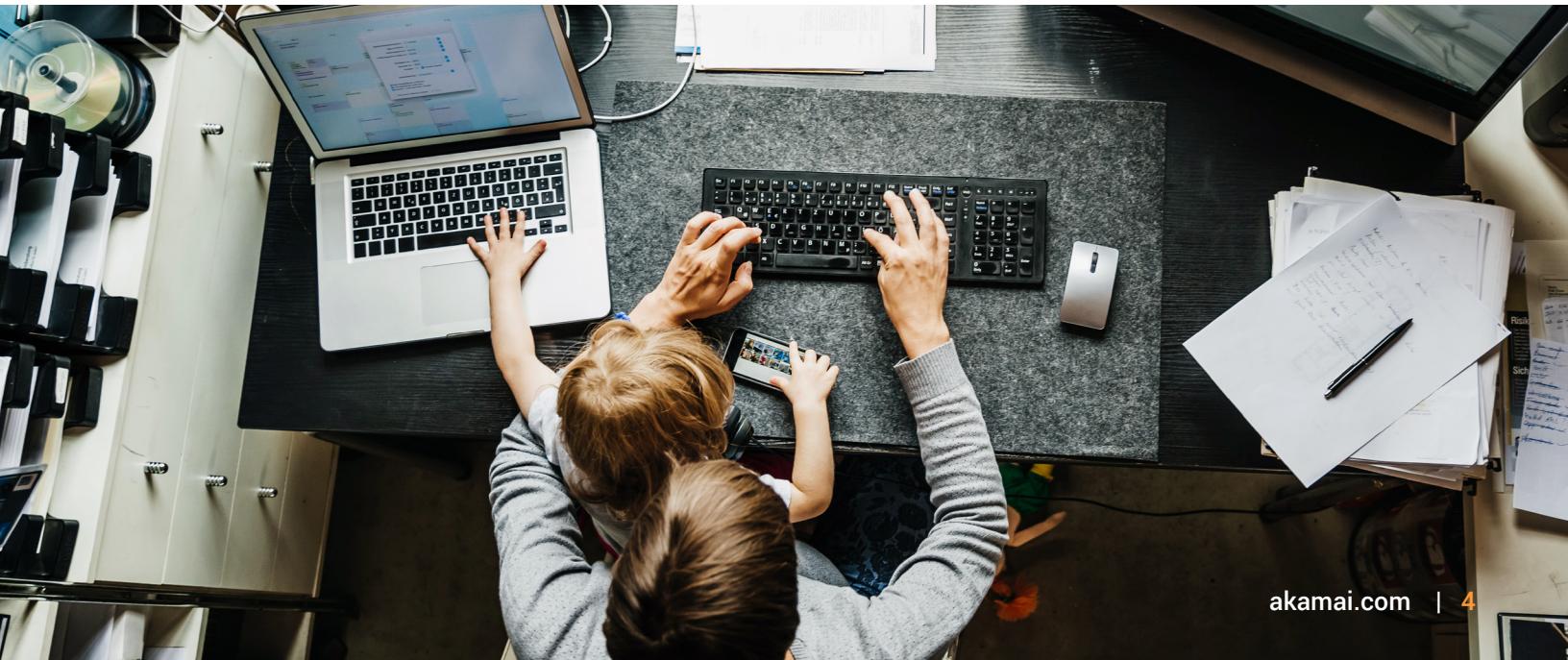
L'orario, il modo e il luogo in cui le persone lavorano oggi vanno ben oltre le quattro mura dell'ufficio.

Di conseguenza, il perimetro della rete non esiste più, almeno non in una forma riconoscibile. Gli utenti si trovano molto spesso al di là del proverbiale fossato e non al suo interno. Inoltre, stanno proliferando le applicazioni utilizzate come soluzioni SaaS (Software-as-a-Service) e le implementazioni multicloud. Considerando la presenza di minacce avanzate e persistenti, è molto probabile che si possa inavvertitamente concedere a utenti malintenzionati un accesso completo alle risorse più preziose, una volta che sono riusciti a entrare nella rete. Se non disponete di un programma Zero Trust completo, gli utenti malintenzionati, una volta entrati, avranno carta bianca.

Non si tratta meramente di una teoria, ma di una situazione dimostrata dall'ampia e costosa quantità di violazioni dei dati negli ultimi anni, la maggior parte delle quali si è verificata in seguito ad un abuso di fiducia all'interno del perimetro di rete.

Nel frattempo, le applicazioni progettate per l'utilizzo all'interno di un perimetro di rete spesso dispongono dei profili di sicurezza più scadenti. Dopo tutto, se foste sviluppatori che immaginano che solo i dipendenti autorizzati e in buona fede sono quelli che effettivamente accedono al sistema, sareste prudenti tanto quanto i codificatori di oggi, che sanno bene che vasti eserciti di hacker cercheranno di sfruttare la vulnerabilità delle loro applicazioni basate su Internet?

La soluzione a queste sfide nel mercato è il modello Zero Trust.



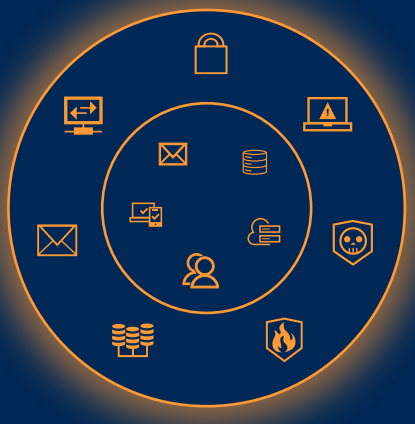
Un'architettura di sicurezza Zero Trust

Il principio alla base del modello Zero Trust è piuttosto semplice, ma molto potente: l'attendibilità non è un attributo che dipende dalla posizione. Non ci si dovrebbe fidare di qualcosa semplicemente perché si trova dietro al firewall aziendale. Al contrario, ogni azione, a prescindere da dove essa si verifichi, deve essere considerata attendibile soltanto se è stata esplicitamente consentita. In definitiva, può accadere soltanto ciò che deve accadere. Le organizzazioni non devono più fidarsi implicitamente delle azioni non necessarie. Ad esempio, il fatto di concedere a tutti gli utenti del proprio gruppo contabile accesso al sistema finanziario, quando in realtà basta concederlo a pochi, crea un rischio e non un valore.

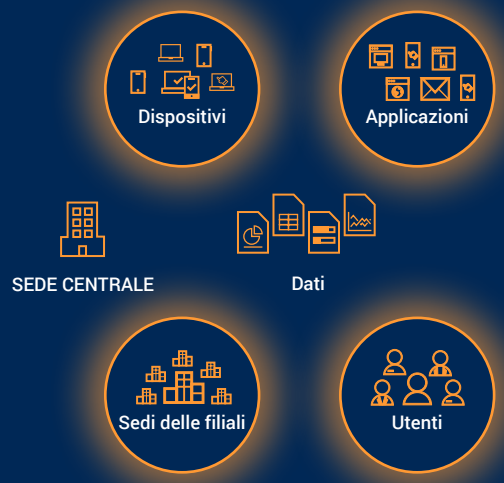
Il metodo per provare l'attendibilità di questi componenti è basato su un potente sistema di autenticazione e autorizzazione e i sistemi non devono trasferire i dati finché non viene stabilita tale attendibilità. Inoltre, andrebbero eseguite operazioni di analisi e registrazione per verificare i comportamenti e si dovrebbe restare sempre vigili riguardo a eventuali segnali che indicano violazioni di qualsiasi tipo.

Questo fondamentale cambio mette fine a una cospicua quantità di compromessi a cui abbiamo assistito nell'ultimo decennio. Gli utenti malintenzionati non riusciranno più a sfruttare i punti deboli del vostro perimetro e quindi ad accedere alle applicazioni e ai dati sensibili una volta che hanno superato il fossato. Ora non esiste più alcun fossato. Esistono solo le applicazioni e gli utenti, ciascuno dei quali deve autenticarsi reciprocamente e verificare l'autorizzazione prima di poter effettuare un accesso.

Architettura di sicurezza tradizionale



Realtà moderna



Come fa un'organizzazione a creare un'architettura Zero Trust?

Per prima cosa, tutte le aziende devono definire una strategia per il proprio panorama attuale e determinare se e quando avranno la necessità di assumere nuovi talenti per la propria forza lavoro. Sarebbe possibile dedicare un intero saggio a questo importante passaggio della procedura, ma i prodotti che effettivamente possono aiutare a realizzare una strategia Zero Trust dovrebbero basarsi sul raggiungimento di tre obiettivi.

1

Non fidarsi di nessuno e verificare continuamente.

Il concetto "Non fidarsi di nessuno e verificare continuamente" è molto più complesso di ciò che sembra in teoria. Eliminare semplicemente l'accesso a tutti i sistemi e a tutti i dati, significa blindare la rete. La vera sfida è verificare continuamente, senza creare gravi interruzioni delle attività, in particolar modo perché la maggior parte dei sistemi è progettata sulla base di una fiducia implicita. Dovete disporre di un ampio livello di visibilità e controllo su tutti i tipi di accesso, nonché di metodi semplici e pratici per applicare e mantenere le policy appropriate.

2

Una volta effettuata la verifica, bisogna fornire un accesso minimo.

In un ambiente Zero Trust, una volta verificato un utente, è necessario concedergli l'accesso soltanto a ciò che gli compete in base al suo ruolo.

3

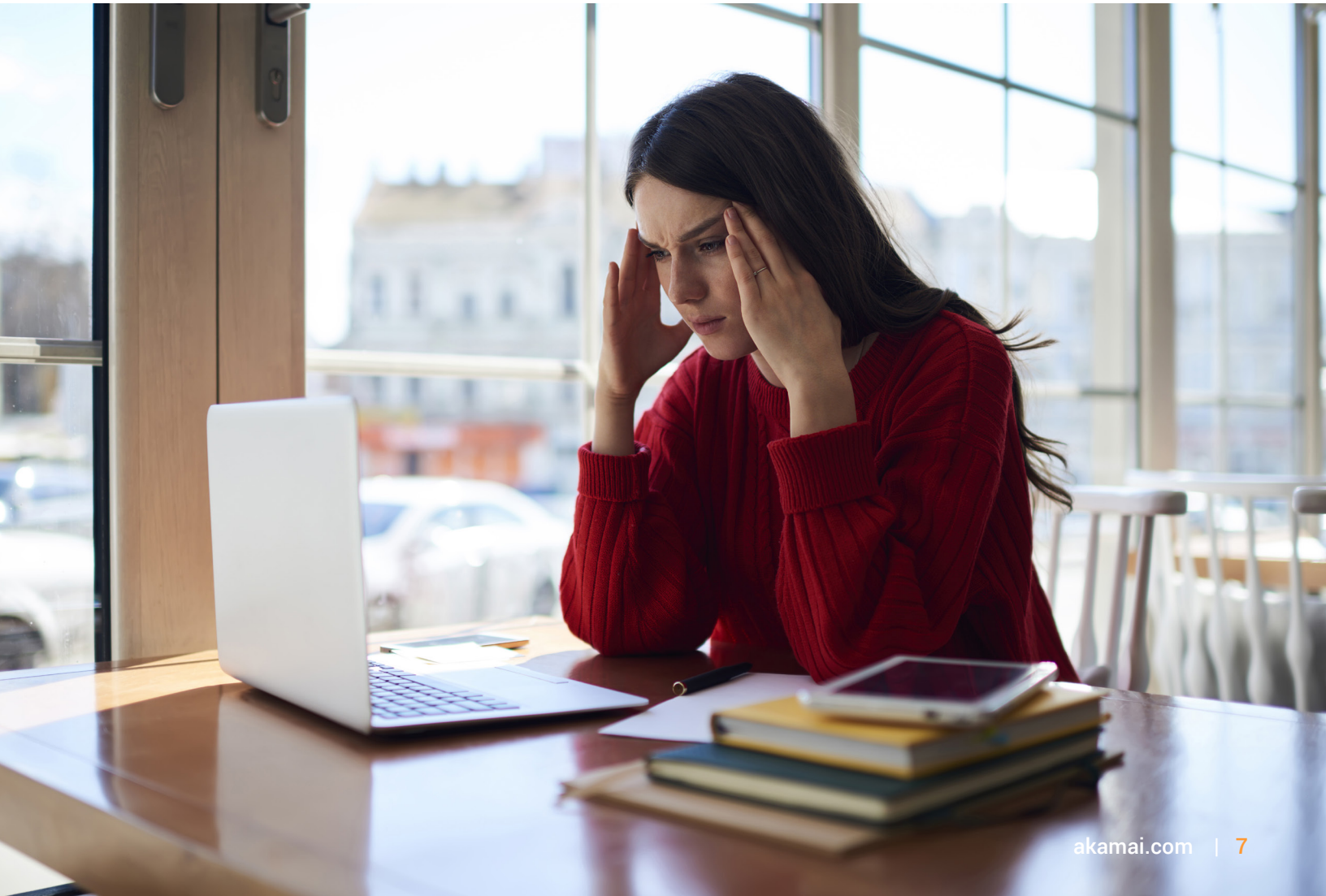
Monitoraggio costante delle minacce.

Come sostiene la maggior parte degli esperti del settore, il modello Zero Trust è un esercizio continuo. I criminali adottano metodi di violazione dei sistemi di difesa sempre più sofisticati e le aziende devono monitorare, verificare e limitare continuamente gli accessi. Uno dei vantaggi apportati da un modello Zero Trust è il fatto di non concentrarsi sull'operato dei criminali, bensì sulle attività dell'azienda stessa. Adottando una policy Zero Trust, i criminali avranno più difficoltà a minare contemporaneamente tutte le attività dell'azienda. Idealmente, sarà possibile fermare ogni attacco lungo la catena. In tutto ciò è contemplata anche la possibilità di fermare gli attacchi non ancora concepiti. Non conta che si tratti o meno di un attacco zero-day perché il modello Zero Trust riuscirà a mitigarlo.

Il lato oscuro del modello Zero Trust

Tuttavia, quando un'organizzazione inizia ad implementare il modello Zero Trust, deve tenere conto anche del rovescio della medaglia che questa mancanza di fiducia e queste limitazioni di accesso comportano. Un aspetto fondamentale del modello Zero Trust è la limitazione dell'accesso, principalmente tramite la creazione di elenchi degli elementi consentiti. Questa pratica consiste nel decidere ciò che è consentito; tutto il resto viene negato per impostazione predefinita. Tuttavia, riducendo la capacità di un criminale di riuscire nel suo intento, aumentano le probabilità che un'azienda impedisca accidentalmente a qualcuno di svolgere il proprio lavoro. In alternativa, i ripetuti controlli su carichi di lavoro e dispositivi possono creare notevoli ritardi e frustrazioni. Una strategia Zero Trust che impedisce alle persone di svolgere il proprio lavoro in maniera efficace non è affatto una strategia.

Una potente strategia Zero Trust, pertanto, deve essere in grado di trovare un equilibrio tra sicurezza e accesso. Dovrà anche trovare un equilibrio tra ciò che è possibile effettivamente ottenere e le risorse del proprio team di sicurezza, sia in termini di budget che di personale.

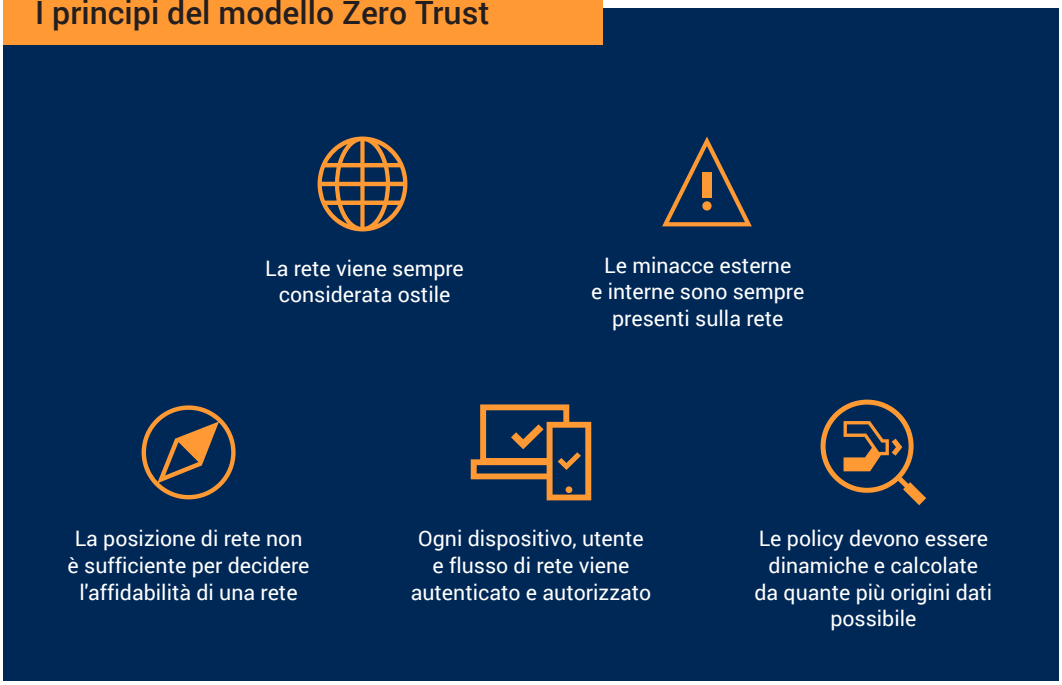


Elementi del modello Zero Trust

Sono passati 15 anni da quando Forrester ha delineato per la prima volta il concetto Zero Trust. Molte organizzazioni stanno cominciando soltanto adesso il proprio viaggio verso il modello Zero Trust, affrontando un mercato di prodotti software complesso. Da un lato, alcuni prodotti esistono da anni e offrono alcune delle funzioni dell'architettura Zero Trust, dall'altro sono stati lanciati altri nuovi prodotti e sono tantissimi i fornitori di software che si sono affrettati a ribrandizzare le loro soluzioni come "Zero Trust". Inoltre, come sostengono molti analisti e osservatori del settore, "il modello Zero Trust non è un prodotto, ma una strategia completa" e "il modello Zero Trust non è una destinazione, ma un viaggio". Eppure, queste affermazioni frequenti contribuiscono ben poco ad aiutare chi deve acquistare soluzioni tecnologiche Zero Trust e, anzi, possono provocare anche più confusione.

Poiché non esiste un solo prodotto in grado di fornire ad un'azienda il sistema Zero Trust e poiché ogni singola organizzazione presenta diverse priorità e vulnerabilità, il punto di partenza sarà diverso per ogni azienda. Eppure, grazie alle innovazioni tecnologiche e alla concentrazione del settore, le aziende ora possono ottenere gli strumenti necessari a implementare una policy Zero Trust da un'unica origine. Anche le società di analisi stanno cominciando a capirlo.

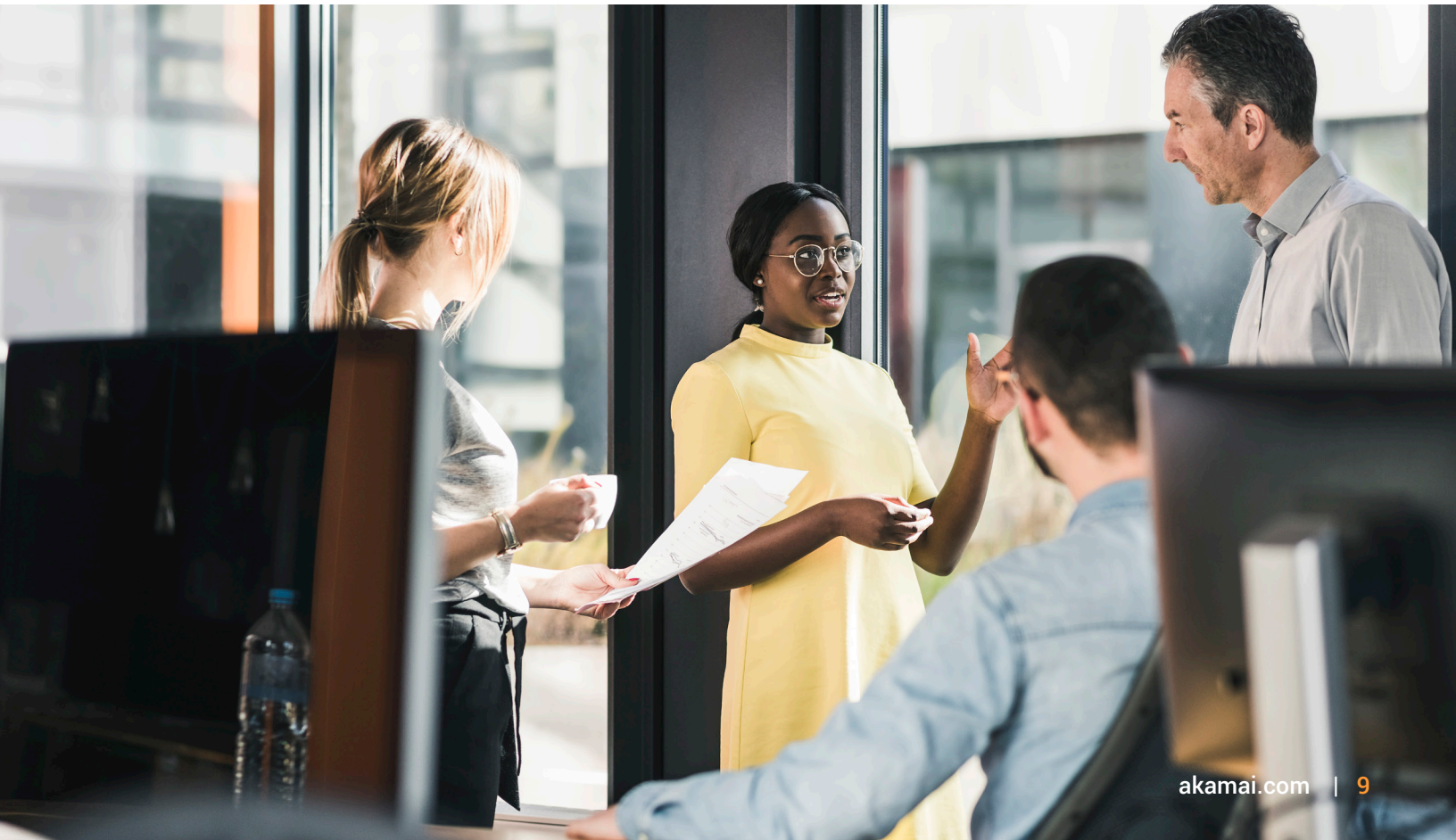
I principi del modello Zero Trust



Gartner monitora ciò che viene definito SSE (Secure Service Edge), una combinazione di soluzioni SWG (Secure Web Gateway), CASB (Cloud Access Security Broker) e ZTNA (Zero Trust Network Access). Nel suo rapporto Quali sono le strategie pratiche per implementare il modello Zero Trust?, Gartner include anche la microsegmentazione (definita come segmentazione da carico a carico), consigliando alle organizzazioni che intendono passare a un'implementazione pratica di concentrarsi su due progetti fondamentali: la segmentazione da utente ad applicazione (ZTNA) e la segmentazione da carico a carico (segmentazione basata sull'identità).

Allo stesso modo, IDC analizza l'accesso sicuro e la segmentazione del modello Zero Trust, definendo il tutto come una panoramica completa delle tecnologie, esistenti ed emergenti, utilizzate per proteggere i sistemi informatici, le risorse e i dati attraverso la segmentazione logica, il controllo degli accessi e il rilevamento delle minacce.

Tuttavia, unire questi sistemi separati in un'unica strategia coesa diventa una sfida notevole. Quali sono gli elementi fondamentali che dovrebbero cercare CIO, CISO e altri professionisti della sicurezza quando creano un'architettura Zero Trust che funziona per la propria organizzazione?



Zero Trust Network Access

A volte confuso con l'approccio generale al modello Zero Trust, ZTNA è una parte fondamentale dello stack tecnologico. L'accesso sicuro è il passo iniziale fondamentale in un qualsiasi sistema Zero Trust. Sfortunatamente, come molti elementi del processo, diventa subito più complesso di ciò che sembra. L'accesso sicuro non è una decisione binaria. Fornire il giusto livello di accesso all'applicazione giusta, per l'utente giusto e al momento giusto è diventato molto più complesso, a causa della natura più ampiamente distribuita degli utenti e delle applicazioni. In effetti, la stessa definizione di utente adesso potrebbe riferirsi non soltanto ai dipendenti, ma anche a clienti, fornitori e partner. Nel frattempo, le applicazioni possono inglobare app legacy, SaaS o app mobili e richiedere l'accesso a e da data center, Internet o ambienti cloud.

Un'efficace soluzione ZTNA verificherà l'identità dell'utente e l'integrità del suo dispositivo, facendo in modo che possa accedere alle applicazioni necessarie, a prescindere dalla sua posizione, riducendo, così, la possibile superficie di attacco e migliorando flessibilità e monitoraggio. Per fornire l'accesso, le organizzazioni si sono affidate per decenni a VPN (Virtual Private Network) supportate da provider di identità. Queste VPN, progettate per un'epoca diversa, non bastano più a gestire il numero e l'ambito in cui opera la forza lavoro distribuita di oggi. La soluzione ZTNA si è evoluta diventando molto di più che un sostituto delle VPN e adesso concede accessi non soltanto in base alla verifica dell'identità degli utenti e del loro dispositivo, ma anche di attributi come ora e data, geolocalizzazione e comportamento dei dispositivi, al fine di garantire il livello adeguato di fiducia.

Considerazioni chiave per l'acquisto di soluzioni Zero Trust Network Access

Mentre le aziende iniziano a sostituire le vecchie VPN con soluzioni di gestione delle identità più sofisticate, ci sono una serie di aree da considerare. Le soluzioni più avanzate di oggi devono unire gestione delle identità e degli accessi, sicurezza delle applicazioni, autenticazione multifattore (MFA) e Single Sign-On: il tutto con visibilità e controllo della gestione, in un'unica interfaccia. Le organizzazioni che desiderano adottare modelli Zero Trust dovrebbero cercare soluzioni in grado di gestire le esigenze attuali e future, così da eseguire un rapido onboarding dei dipendenti in caso di fusione o acquisizione di altre aziende, favorire la manifattura o la produzione in diversi mercati o aree geografiche, aggiungere e rimuovere facilmente i collaboratori per adattarsi alle mutevoli esigenze aziendali e spostare le applicazioni sul cloud in modo conveniente e senza compromessi in termini sicurezza.

Le organizzazioni dovrebbero cercare soluzioni in grado di integrarsi direttamente nelle infrastrutture di identità esistenti, persino se includono più directory e provider di servizi di identità. Ciò consente una rapida implementazione del servizio ZTNA, evitando di modificare l'infrastruttura o l'architettura di identità esistenti.

Scegliere l'edge

Tra i prodotti sul mercato esiste anche un elemento distintivo significativo che i team che si occupano di prendere decisioni sull'acquisto del sistema Zero Trust potrebbero non prendere in considerazione, mentre dovrebbero assolutamente farlo. Le soluzioni che vengono combinate con piattaforme cloud edge possono offrire ulteriori vantaggi, agendo come un proxy basato sulle identità, che posiziona la connettività sulla piattaforma edge, garantendo che tutti i processi di autenticazione vengano svolti sull'edge, lontano dal data center. Sebbene alcune aziende adottino architetture proxy di accesso eseguite nella DMZ, ciò non consente di sfruttare la capacità del cloud di assorbire meglio attacchi, fornire larghezza di banda per la memorizzazione nella cache e garantire la scalabilità automatica, in base alle necessità.

Un proxy basato sulle identità realizzato nel cloud può scalare on demand, eseguire risorse pesanti per la CPU e assorbire gli attacchi. Inoltre, si trova su un indirizzo IP privato non direttamente raggiungibile da Internet. Le attività che richiedono livelli elevati di performance e sicurezza vengono svolte in prossimità dell'edge, più vicino all'utente finale. Inoltre, il percorso di ingresso sensibile all'applicazione avviene su un tunnel di applicazioni inverso, il che rimuove efficacemente la visibilità dell'IP del perimetro e riduce il rischio di attacchi volumetrici.

> **Le soluzioni che vengono combinate con piattaforme cloud edge possono offrire ulteriori vantaggi, agendo come un proxy basato sulle identità.**

Considerazioni sull'autenticazione multifattore nell'ambito della creazione di un piano Zero Trust

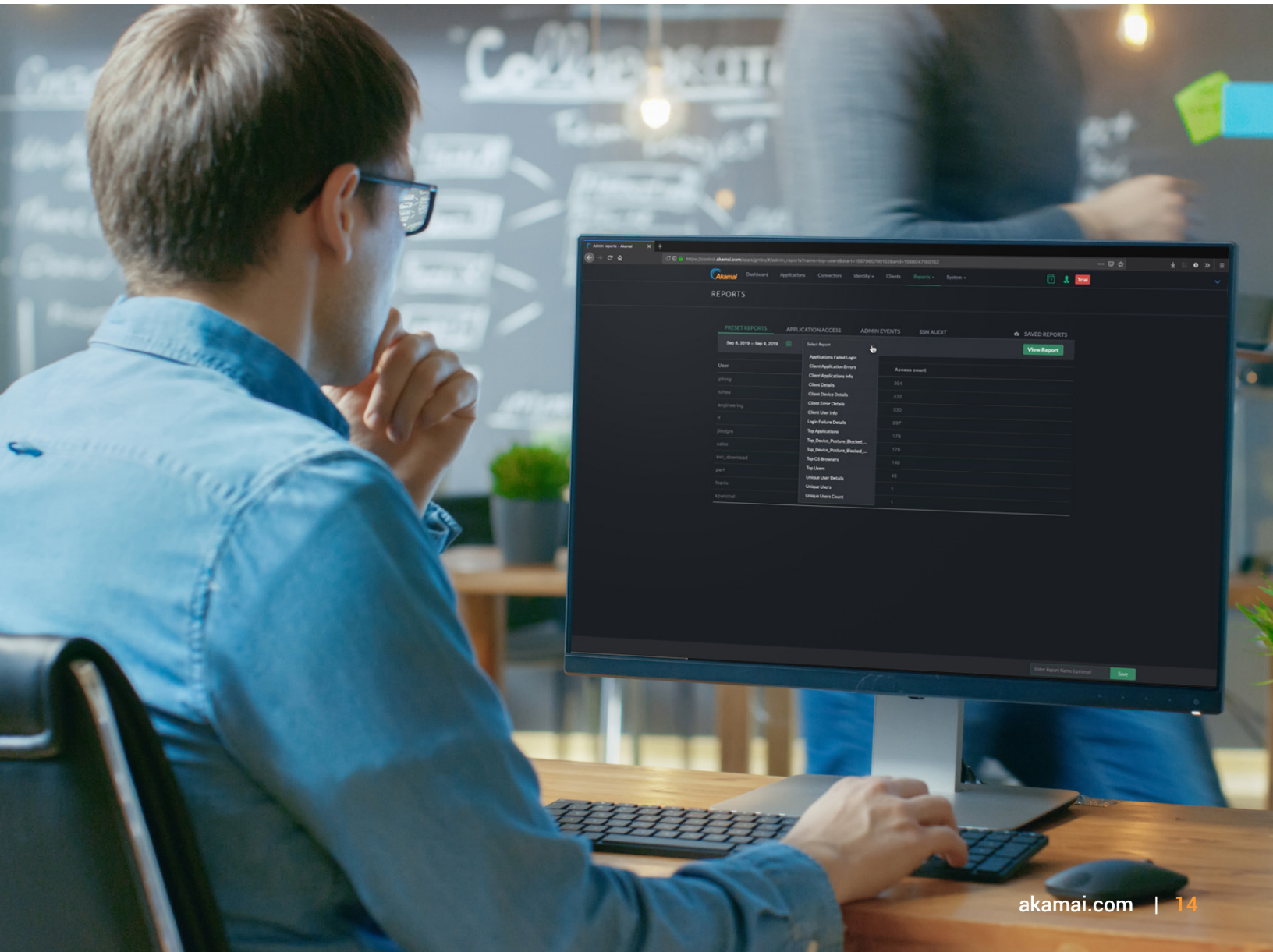
Con la diffusione del lavoro ibrido e la necessità di garantire un accesso più ampio, la maggior parte delle organizzazioni ha già adottato l'autenticazione MFA e ha implementato un qualche tipo di soluzione. È importante riconoscere, tuttavia, che la combinazione di accesso a livello aziendale ed MFA offre un valore maggiore rispetto a quello fornito dalla somma delle parti. L'MFA è fondamentale per il concetto di fiducia, perché non richiede soltanto una password. È necessaria una seconda verifica per evitare di subire attacchi in una delle aree di fiducia più comunemente colpite da violazioni. È importante anche ricordare che non tutte le soluzioni MFA sono uguali.

Nel valutare soluzioni MFA come parte di una strategia Zero Trust, le organizzazioni devono cercare soluzioni con le seguenti caratteristiche:

- Integrazione con la gestione delle identità e l'accesso aziendale
- Conformità a FIDO2, per garantire che le credenziali utente siano decentralizzate, isolate e crittografate sui dispositivi personali degli utenti, un aspetto particolarmente importante nella difesa da attacchi di phishing
- Possibilità di verificare gli utenti tramite lo smartphone, senza affidarsi a chiavi fisiche

Microsegmentazione

Non esiste la perfezione nel modello Zero Trust. Inevitabilmente, ci saranno falle che gli autori di attacchi più ostinati possono trovare e sfruttare. Un approccio completo al modello Zero Trust, pertanto, richiederà la microsegmentazione. Oggi, la maggior parte delle reti ha pochi segmenti o non ne ha affatto. Infatti, in genere le organizzazioni proteggevano le proprie applicazioni più importanti con i firewall, ma ciò può rivelarsi difficile per varie ragioni. I firewall in pratica necessitano dell'applicazione di policy di rete, il che crea un punto di strozzatura. Servono connessioni di rete per oltrepassare un firewall, cosa che spesso diventa molto costosa, non è consapevole dei rischi del traffico di rete moderno ed è estremamente difficile da cambiare. Le organizzazioni, invece, stanno adottando la microsegmentazione basata su software, che semplifica molti di questi processi ad alto carico di lavoro.



Elementi distintivi nella microsegmentazione

Nonostante sia un requisito importante di qualunque iniziativa Zero Trust, la microsegmentazione è stata spesso tenuta separata dalle soluzioni ZTNA principali. E, anche se la microsegmentazione viene venduta sia dai provider di piattaforme di sicurezza che come soluzione autonoma, esistono alcune differenze importanti che gli acquirenti devono comprendere.

Dove posso distribuirla? Le soluzioni di microsegmentazione realizzate come strumenti di rete anziché con un approccio incentrato sulla sicurezza e quelle studiate per sistemi on-premise dovrebbero allertare i potenziali acquirenti. Gli strumenti di oggi dovrebbero essere distribuiti nel cloud, in ambienti on-premise, su dispositivi (compresi quelli sui quali non è possibile installare agenti) e tra container in ambienti ibridi. In genere tutto questo richiede un software basato su cloud. Se una soluzione di microsegmentazione protegge soltanto l'80% dell'ambiente, non basta.

Quanta visibilità fornisce? Nonostante le soluzioni di microsegmentazione limitino gli accessi, troppe limitazioni possono interrompere i processi aziendali e portare a ricevere richiami da parte del COO. La microsegmentazione necessita di una comprensione approfondita dell'ambiente. Quali server possono accedere a quali server? È possibile definire delle policy tra un cluster Kubernetes e un Windows Server 2008? Tanti strumenti non dispongono di agenti risalenti al 2008 oppure così avanzati da imporre policy su Kubernetes. Un software di microsegmentazione deve essere in grado di gestire questa specie di complessità per distribuire il modello Zero Trust in maniera efficace.

Inoltre, chi acquista software di microsegmentazione deve considerare la granularità delle policy supportate dal prodotto. La maggior parte dei sistemi applicherà policy a livello di applicazione su porte e processi. Prodotti più sofisticati possono applicare policy a livello dei microservizi. Ad esempio, gli autori di attacchi possono utilizzare alcuni dei servizi di svchost, come l'utilità di pianificazione, per spostarsi lateralmente all'interno della rete. Tuttavia, le aziende non possono bloccare completamente svchost, perché fa troppe cose importanti. In questo caso, una soluzione di microsegmentazione che imponga una policy a livello dei microservizi può fare la differenza.

Quanto è difficile da implementare? La facilità con la quale si esprime la policy necessaria al momento e, non meno importante, le esigenze future sono aspetti fondamentali per una qualsiasi soluzione di microsegmentazione. Che ci si trovi in una fase di pianificazione o di fronte a una minaccia all'ambiente da isolare, è bene assicurarsi che il motore in cui stiamo investendo sia in grado di supportare entrambi gli scenari.

Partire con un elenco di elementi consentiti in un progetto di microsegmentazione può essere intimidatorio per i team addetti alla sicurezza; negare per errore l'accesso a un'applicazione o un servizio in realtà necessari implica notevoli rischi. Una soluzione di microsegmentazione sofisticata dovrebbe contenere modelli di elenchi di elementi non consentiti implementabili dai team in maniera semplice e rapida, per ottenere dei risultati immediati per il progetto. Una volta ottenuto questo, le organizzazioni possono continuare il proprio percorso verso una protezione completa, fatta di elenchi di elementi consentiti, che includa funzionalità accurate di mappatura di dipendenze e inventario contestuale.

> **Le soluzioni di microsegmentazione realizzate come strumenti di rete anziché con un approccio incentrato sulla sicurezza e quelle studiate per sistemi on-premise dovrebbero allertare i potenziali acquirenti.**

Firewall DNS

In un ambiente Zero Trust, non si tratta solo di non fidarsi delle persone, ma anche di Internet stesso. I dipendenti hanno necessità di accedere a Internet e, man mano che si diffondono SaaS e applicazioni mobili, servizi cloud, lavoro ibrido e dispositivi IoT, si amplia contestualmente anche la superficie di attacco di un'organizzazione. Pertanto, diventa sempre più difficile proteggere l'azienda e gli utenti da minacce come i malware, i ransomware, il phishing e l'esfiltrazione dei dati. Le organizzazioni hanno risorse limitate per la gestione delle complessità relative ai punti di controllo per la sicurezza e delle lacune nella sicurezza nelle soluzioni tradizionali già esistenti in sede.

L'applicazione di un modello Zero Trust tra una persona e Internet richiede un firewall DNS, che diventa una funzionalità centrale di qualsiasi progetto Zero Trust.

Requisiti di base Zero Trust degli investimenti nei firewall DNS

Sebbene siano apparentemente semplici, esistono dei requisiti che gli acquirenti di prodotti tecnologici devono considerare quando investono in un firewall DNS. Molte organizzazioni hanno implementato i loro firewall DNS on-premise, ma adesso devono estendere questo tipo di protezione agli utenti, ovunque si trovino. Come avviene per la gestione delle identità, i provider che dispongono di potenti piattaforme edge, in genere, hanno un livello di sicurezza DNS maggiore, grazie all'intelligence sulle minacce ricavata dalla piattaforma estesa. I responsabili decisionali dovrebbero prendere attentamente in considerazione questi requisiti fondamentali.

Ispezione del DNS. I provider dovrebbero poter fornire ispezioni in tempo reale di tutti i domini, con un'intelligence sulle minacce sofisticata, e bloccare automaticamente i domini dannosi. Le soluzioni devono agire anche su tutte le porte e su tutti i protocolli, per conferire protezione dal malware che non utilizza protocolli e porte web standard. La qualità di un'ispezione DNS può variare ampiamente da un provider all'altro e gli acquirenti dovrebbero cercare quelli con esperienza di mercato e storie di successo dei clienti consolidate.

Protezione per tutti i dispositivi. I provider devono disporre di agenti per i dispositivi utilizzati all'interno e all'esterno della rete, come laptop, smartphone e tablet.

Onboarding DNS flessibile. I provider devono disporre di più metodi per inoltrare le richieste DNS al firewall DNS allo scopo di fornire la massima flessibilità e coprire tutti i casi di utilizzo.

Identificazione e blocco dei tentativi di esfiltrazione del DNS. L'esfiltrazione del DNS, specialmente le sue varianti a bassa velocità effettiva, possono consentire ai criminali di esfiltrare i dati desiderati tramite il canale DNS. Scegliete provider in grado di fornire sistemi di rilevamento dei tentativi di esfiltrazione del DNS online e offline sulla base di algoritmi proprietari.

Monitoraggio delle minacce

L'ultima parte della tecnologia Zero Trust fondamentale è il monitoraggio delle minacce. Nonostante il presupposto del modello Zero Trust sia che non ci si deve fidare di nulla in maniera implicita, le organizzazioni devono restare vigili per scoprire gli attacchi in corso e quelli emergenti, nonché i potenziali rischi (come le configurazioni errate oppure i diritti di accesso eccessivamente permissivi). Quando i team di sicurezza valutano i software disponibili sul mercato, dovrebbero riflettere su queste tre considerazioni utili a un monitoraggio delle minacce efficace.

Considerazioni chiave

Algoritmi efficaci
Gli algoritmi avanzati, che si sono dimostrati efficaci in fatto di anomalie nelle attività degli utenti e della rete, di analisi dei file eseguibili, di analisi dei registri e molto altro, dovrebbero far parte di qualsiasi servizio di monitoraggio delle minacce.

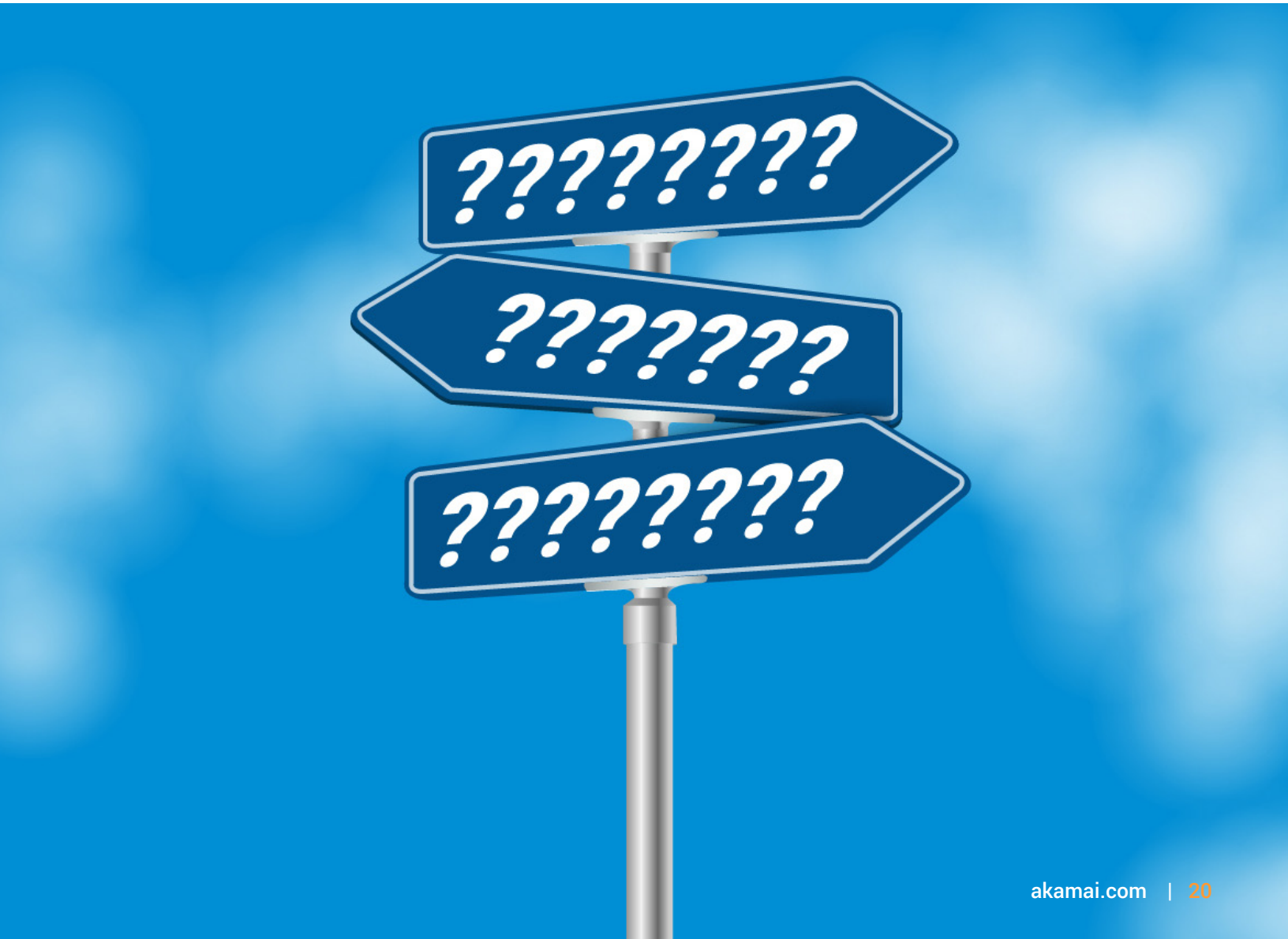
Potente rilevamento dei segnali
Nonostante il software e l'intelligenza artificiale siano strumenti essenziali per il monitoraggio delle minacce, i responsabili decisionali in fatto di Zero Trust dovrebbero comunque tener conto delle competenze interne dei fornitori con i quali lavorano. I servizi di monitoraggio delle minacce devono poter separare i segnali buoni da quelli cattivi, al fine di evitare un eccessivo numero di avvisi e offrire notifiche immediate di incidenti. Le organizzazioni devono aspettarsi anche dei resoconti periodici, contenenti le analisi di tutte le campagne di alto profilo.

Personale competente
I team devono comprendere persone appartenenti a vari tipi di ambienti, come quello offensivo, di risposta agli incidenti e del data science, e devono essere disponibili 24 ore al giorno, 7 giorni su 7. Si tratta di un ambito in cui i provider di delivery dei contenuti possono apportare notevoli vantaggi. Le informazioni derivanti dal monitoraggio di centinaia di terabyte al secondo contribuiscono all'ottenimento di una prospettiva unica per qualsiasi rilevamento dei segnali.

Da dove iniziare?

Un'iniziativa Zero Trust non è mai completa, perciò quando si analizzano i requisiti software, hardware e di assunzione, spesso la domanda principale che bisogna farsi è: "Da quale tecnologia inizio?".

Come spesso succede, la risposta dipenderà dalle specifiche esigenze di un'azienda, dalle valutazioni del rischio e dai relativi punti di forza e debolezza. Per molti osservatori del settore, la risposta è iniziare con l'implementazione di ZTNA. Infatti, proteggere l'organizzazione dal traffico nord-sud dannoso può essere un punto di partenza prudente. Eppure, esiste anche chi è convinto che un approccio est-ovest con la microsegmentazione, nello specifico una microsegmentazione definita dal software, sia la strada migliore.



Quando iniziare dalla microsegmentazione

Se, come molti esperti, pensate anche voi che la difesa perfetta non esista e che prima o poi subirete un attacco, allora volete essere in grado di proteggere almeno le vostre risorse più preziose. La microsegmentazione offre proprio questo. Una delle ragioni per le quali le organizzazioni potrebbero esitare a partire con la microsegmentazione è la percezione della complessità.

Per prima cosa, la microsegmentazione non è un approccio di tipo "tutto o niente". Come il modello Zero Trust stesso, può essere effettuata per gradi. Le organizzazioni possono iniziare identificando le loro risorse più preziose. Concentratevi su ciò che è fondamentale. Assicuratevi che se qualcuno entra nel vostro sistema non riesca a bloccare totalmente le vostre attività. L'importanza di una risorsa può basarsi sui dati al suo interno oppure sul livello di protezione esistente.

In molti casi, scegliete una soluzione di microsegmentazione in grado di proteggere i vostri sistemi legacy, in cui, spesso, vengono eseguite applicazioni business-critical e che sono particolarmente vulnerabili. Alcune soluzioni di microsegmentazione non supportano la protezione dei sistemi legacy.

In secondo luogo, la microsegmentazione definita dal software rimuove molte delle complessità percepite. Non sarà necessario gestire degli hardware o tempestare di telefonate gli architetti di rete e della sicurezza. Basterà implementare il software, abbassando, così, notevolmente le barriere di accesso.

Una volta avviata l'iniziativa di microsegmentazione, i primi vantaggi saranno chiari e potranno dare una spinta in avanti al resto del progetto. Ad esempio, si creerà una fonte di verità su tutto ciò che succede nel proprio ambiente. È possibile ottenerla subito, senza dover applicare delle policy e, una volta fatto, sarà possibile capire benissimo il funzionamento dei flussi. Inoltre, quando un'organizzazione inizia a isolare le applicazioni, è possibile proteggere in maniera rapida e semplice le applicazioni critiche, in modo tale che comunichino esclusivamente tramite porte e processi specifici.

In alternativa, un risultato immediato può essere individuare policy specifiche in base alle minacce. Le piattaforme di microsegmentazione sofisticate conterranno un elenco di elementi non consentiti integrato. Ciò significa che sarà possibile creare rapidamente una policy per fermare le connessioni superflue tra servizi desktop remoti e Internet. Le organizzazioni, ad esempio, possono isolare rapidamente il tipo di vulnerabilità che ha causato l'attacco Colonial Pipeline.

Qualunque sia il punto di partenza, la chiave per avviare un qualsiasi percorso Zero Trust è l'equilibrio: un'eccellente gestione delle identità con una segmentazione scarsa o una protezione dagli accessi web scadente non contribuiscono a realizzare un sistema di sicurezza efficace.

Piattaforma e strumenti specializzati a confronto

Come avviene con molte decisioni in fatto di tecnologia, l'acquisto di software Zero Trust spesso si riduce al dover scegliere tra singoli strumenti specializzati e una piattaforma che unisca più componenti disparati. L'impatto del modello Zero Trust sui team di sicurezza, gli integratori, gli architetti e gli analisti, nonché l'esigenza degli stessi di gestire policy su diverse console, diversi agenti e integrazioni multiple, fanno della piattaforma un'offerta allettante. Ciò è particolarmente vero nell'ambito di un mercato del lavoro ristretto, in cui scarseggiano professionisti della cybersicurezza competenti. Gestire soluzioni da parte di più fornitori può aumentare significativamente i costi del personale, poiché soluzioni che non comunicano tra loro in maniera efficace creano falsi positivi, che diventano un peso per gli utenti finali e possono richiedere ulteriore assistenza e formazione.

Inoltre, in termini di assistenza e negoziazioni contrattuali, avere a che fare con una persona soltanto può essere un buon motivo per scegliere l'implementazione di un modello Zero Trust con un fornitore di piattaforme.

Idealmente, dovreste scegliere un solo provider con un approccio flessibile, che sia in grado di offrire una piattaforma completa per il modello Zero Trust insieme a singoli prodotti mirati. Questa flessibilità rende più semplice adottare il modello Zero Trust oltre ad usufruire dei vantaggi offerti da un solo provider.

> **Una delle ragioni per le quali le organizzazioni potrebbero esitare a partire con la microsegmentazione è la percezione della complessità.**

Riesame degli elementi del modello Zero Trust

Conoscere i vostri utenti. Assicurarsi che siano verificati.

Proteggere le vostre risorse. Autenticare/autorizzare tutte le transazioni.

Proteggere i vostri utenti. Impedire al malware di infettare gli utenti.

Conclusione

In definitiva, la maggior parte delle organizzazioni che desiderano proteggersi dagli attacchi informatici riconoscono quanto sia necessario iniziare a passare tempestivamente a un'architettura Zero Trust. Molte hanno già iniziato il proprio percorso per gradi oppure più velocemente, in risposta all'aumento dello smart working. Eppure, man mano che gli attacchi diventano più sofisticati, che le superfici di attacco si allargano e che sempre più utenti richiedono l'accesso da remoto, l'esigenza di avere un portfolio completo di soluzioni che funzionino insieme non fa che crescere.

Per dettagli su elementi specifici dell'approccio di Akamai al modello Zero Trust, visitate il sito akamai.com/zerotrust o parlate con uno dei nostri esperti.

Informazioni sulla sicurezza Akamai

Akamai Security protegge le applicazioni che danno impulso alle vostre attività aziendali e rafforzano le interazioni, senza compromettere le performance o le customer experience. Tramite la scalabilità della nostra piattaforma globale e la visibilità delle minacce, possiamo unire le nostre forze per prevenire, rilevare e mitigare le minacce affinché voi possiate rafforzare la fiducia nel brand e realizzare la vostra visione. Per ulteriori informazioni sulle soluzioni di cloud computing, sicurezza e delivery dei contenuti di Akamai, visitate il sito akamai.com o akamai.com/blog e seguite Akamai Technologies su X (in precedenza Twitter) e LinkedIn. Data di pubblicazione: 10/24.