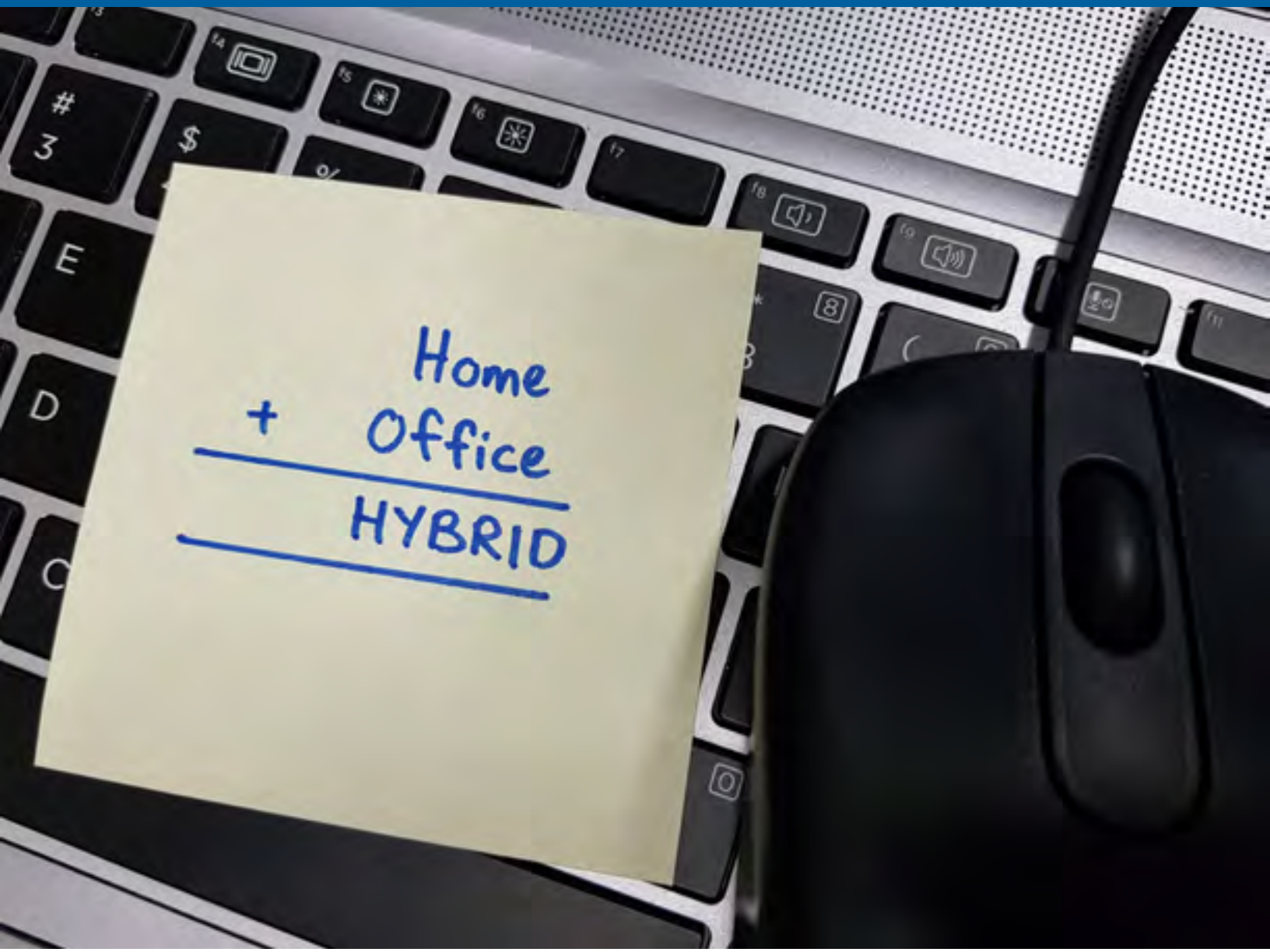
Proteggere la forza lavoro flessibile con un approccio zero trust

Scopri in che modo una metodologia zero trust è in grado di proteggere più efficacemente il tuo ambiente di lavoro flessibile



UN REPORT DI RICERCA DI HMG STRATEGY SUPPORTATO DA ZSCALER

HMG STRATEGY

zscaler™

RIEPILOGO

A marzo del 2020 il mondo è cambiato, e i CISO e i team addetti alla sicurezza delle informazioni si sono trovati ad affrontare una serie di nuove sfide. Milioni di dipendenti hanno iniziato improvvisamente a lavorare da casa, e l'idea che le organizzazioni avessero un perimetro definito da difendere è stata abbandonata per sempre.

Con la pandemia globale che andava avanti e la maggior parte dei team aziendali che continuava a lavorare da remoto, le architetture di rete esistenti hanno rivelato i propri limiti, perché non sono state più in grado di tutelare i dipendenti e le organizzazioni in un ambiente di lavoro altamente distribuito. Al contempo, anche la migrazione delle applicazioni, con il relativo passaggio dal data center alle piattaforme cloud e SaaS, è accelerata a un ritmo senza precedenti, e continua ancora oggi ad aumentare. Uno studio condotto da O'Reilly Media rivela che il 48% delle organizzazioni prevede di spostare il 50% o più delle proprie applicazioni sul cloud entro il 2022 [1].

Un'altra serie di difficoltà relative alla flessibilità della forza lavoro è rappresentata dall'aumento dei problemi di sicurezza associati ai dispositivi personali non gestiti impiegati negli uffici domestici. La continua dipendenza dalle reti private virtuali (VPN) ha esposto molte organizzazioni a rischi.

Questi sono solo alcuni dei motivi per cui la maggior parte dei CISO e dei responsabili della sicurezza aziendale sta adottando architetture zero trust moderne per rafforzare le proprie difese e tutelare l'intera organizzazione.

"Uno dei principali punti di forza di una metodologia zero trust consiste nella capacità di adattare i propri controlli di sicurezza in base ai livelli specifici di rischio e alla priorità assegnata a ciascun caso d'uso", afferma **Lisa Lorenzin**, Field CTO di Zscaler per le Americhe. *"Con una moderna soluzione zero trust, è possibile operare con il giusto livello di astrazione: per collegare un utente a un'app specifica, è possibile collocare i controlli inline, invece di collegare un endpoint alla rete"*.

Le aziende continuano a espandere la propria presenza digitale e a creare pool di prodotti e servizi digitali, e per tutelare tutti i livelli di questo modello di business è necessario adottare un'architettura zero trust. **Questo spiega perché, secondo una recente indagine condotta da HMG Strategy e Zscaler in cui sono stati intervistati 118 responsabili della sicurezza, il 61% dei CISO e degli addetti alla sicurezza aziendale ritiene che un modello di sicurezza zero trust sia l'approccio più efficace per proteggere l'ecosistema digitale di un'organizzazione**.

HMG Strategy ha avviato una collaborazione con Zscaler per comprendere meglio come è cambiato il panorama delle minacce da quando le aziende hanno adottato il lavoro flessibile, dove si trovano queste nuove vulnerabilità critiche, e per illustrare i vantaggi e le opportunità dell'implementazione di un'architettura zero trust. In questo approfondito report di ricerca, scoprirai:

- I principali rischi per la sicurezza e le sfide associate all'ambiente di lavoro flessibile
- Perché le architetture esistenti, oltre a comportare perdite economiche, sono inadeguate a tutelare l'azienda
- Esempi recenti di attacchi ransomware e di violazioni della sicurezza della rete
- L'urgente necessità di adottare un'architettura zero trust
- Esempi reali di aziende che stanno traendo vantaggio dall'adozione di un modello di sicurezza zero trust
- Suggerimenti per l'implementazione di un'architettura zero trust per supportare la forza lavoro flessibile

[1] *2021 Cloud Adoption Report, O'Reilly Media.*

Sappiamo cosa si intende davvero per zero trust

Quale tra le seguenti voci rappresenta una definizione accurata dei modelli di sicurezza zero trust?

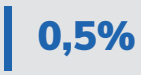
GRAFICO 1:

Lo zero trust è un framework per la sicurezza delle organizzazioni che operano nel mondo cloud e mobile; stabilisce che utenti e applicazioni non debbano essere ritenuti automaticamente attendibili ed elimina il concetto di perimetro di rete.

È un principio di sicurezza incentrato sulla concezione che le organizzazioni non debbano considerare attendibili le entità presenti all'interno o all'esterno del proprio perimetro di rete, e che debbano invece verificare chiunque tenti di connettersi ai propri sistemi, prima di concedere l'accesso.

Considerare tutto come non attendibile, sempre

Nessuna delle precedenti



Fonte: studio "Understanding Zero Trust – Safeguarding the Hybrid Workforce" di HMG Strategy e Zscaler condotto intervistando 118 esperti, tra cui CISO e responsabili senior della sicurezza informatica

Lo zero trust è una strategia di sicurezza informatica in cui le policy di sicurezza vengono applicate non in base alla presunta attendibilità, ma bensì al contesto, che viene stabilito attraverso controlli degli accessi a privilegi minimi e l'autenticazione rigorosa dell'utente. Un'architettura zero trust ottimizzata si traduce in un'infrastruttura di rete più semplice, una migliore esperienza utente e una difesa più efficiente dalle minacce informatiche.

"Uno dei principali punti di forza di una metodologia zero trust consiste nella possibilità di adattare i controlli di sicurezza in base a specifici livelli di rischio e alla priorità assegnata a ciascun caso d'uso".

LISA LORENZIN
Field CTO, Americhe
Zscaler

Come affrontare le principali sfide per la sicurezza derivanti da un'ambiente di lavoro flessibile

Sebbene il lavoro da remoto e i problemi di sicurezza delle reti domestiche non protette e dei dispositivi personali non gestiti siano presenti ormai da anni, il drastico passaggio delle aziende al lavoro da remoto a partire da marzo del 2020 ha ampliato in modo esponenziale il livello di digitalizzazione di tutte le organizzazioni, e di conseguenza le loro vulnerabilità, tra cui la superficie di attacco.

La maggior parte dei dipendenti non ha dimestichezza con la sicurezza della rete o i passaggi necessari per proteggere sé stessi o i dati sensibili dei clienti e proprietari. Gli utenti si collegano ai servizi attraverso i firewall e le VPN della rete aziendale pensando di essere al sicuro, ma in realtà la sicurezza della rete basata sul perimetro li espone a potenziali rischi.

Inoltre, sebbene alcuni team di sicurezza conducano simulazioni di attacchi phishing per aiutare i dipendenti a comprendere e riconoscere meglio questo tipo di campagne, un livello di rischio rimane per molte organizzazioni. Questo spiega perché, secondo il report del 2021 sui rischi delle VPN di Zscaler, il 72% dei dirigenti teme che le VPN possano compromettere la capacità dell'IT di preservare la sicurezza degli ambienti aziendali.

Le vulnerabilità delle VPN

La continua dipendenza dall'uso di VPN per tutelare dipendenti e dati aziendali sensibili lascia le aziende esposte su diversi fronti.

Lorenzin sottolinea tre principali problematiche delle VPN:

1. Ogni gateway VPN ha un listener in entrata che lo rende una superficie di attacco esposta.
2. Il gateway VPN diventa quindi un punto di attracco che viene sfruttato dagli hacker per lanciare altri attacchi più sofisticati.
3. La natura di una VPN è intrinsecamente aperta, e questo costringe i team di sicurezza a bloccare esplicitamente i dipendenti negando loro l'accesso alle applicazioni e ai sistemi se non sono o non dovrebbero essere autorizzati ad accedervi.

Il catastrofico attacco informatico a Colonial Pipeline del 2021 è stato lanciato tramite una VPN legacy che non prevedeva l'autenticazione a più fattori degli utenti. Questo attacco rappresenta un classico esempio di movimento laterale da parte di un criminale informatico che si è potuto muovere indisturbato attraverso la rete di un'organizzazione. Dopo aver rubato le credenziali VPN di un utente, l'aggressore è riuscito ad accedere alla rete di Colonial Pipeline, a spostarsi lateralmente e ad accedere alle applicazioni finanziarie critiche per rubare i dati sensibili e richiedere un riscatto.

L'attacco ha interrotto temporaneamente la fornitura di carburante a gran parte della costa orientale e dell'area meridionale degli Stati Uniti, e all'azienda è stato richiesto di pagare un riscatto di 4,4 milioni di dollari in Bitcoin.

Tra le altre aziende colpite da ransomware e da altri attacchi informatici resi possibili dal lavoro flessibile c'è Brenntag, un distributore tedesco di prodotti chimici che, in questo caso, si è trovato a pagare un riscatto di 4,4 milioni di dollari in Bitcoin al gruppo ransomware Darkside, dopo che quest'ultimo ha criptato i dispositivi sulla rete nordamericana di Brenntag e rubato i file non criptati.

Sebbene i criminali informatici attacchino le aziende di ogni settore e dimensione, secondo le stime di Accenture nel report "The Cost of Cybercrime", il 57% di tutti gli attacchi informatici viene sferrato contro le imprese. Secondo un altro report di Accenture, "How Aligning Security and the Business Creates Cyber Resilience", il numero medio di attacchi per azienda è aumentato di ben il 31% nel 2021 rispetto al 2020. Al contempo, il costo medio di una violazione dei dati per azienda è risultato di 3,86 milioni di dollari, una somma che include i periodi di inattività delle aziende, i pagamenti dei riscatti e i relativi costi per la bonifica, le attività legali e altre spese.

Come adottare un approccio migliore e più conveniente

L'adozione di un'architettura zero trust, oltre a proteggere da costose violazioni, è anche in grado di offrire alle aziende una riduzione della complessità, un'esperienza utente migliore e una protezione dati di livello superiore, il tutto eliminando la superficie di attacco.

Sanmina, fornitore leader di soluzioni di produzione integrate, che serve i segmenti in rapida crescita del mercato globale dei servizi di produzione elettronica, ne è un esempio lampante. Sebbene l'azienda avesse adottato i principi dello zero trust e avesse iniziato a riprogettare i propri sistemi durante la sua trasformazione cloud per supportare le pratiche di produzione avanzate dell'Industria 4.0, il team di sicurezza dell'azienda si è reso conto da subito che non era possibile raggiungere appieno un modello zero trust utilizzando la tecnologia VPN tradizionale.

"Avevamo bisogno di una soluzione di accesso adeguata al mondo moderno e senza perimetro", spiega **Matt Ramberg**, Vice President of Information Security di Sanmina.

Come per molte altre aziende, la forza lavoro di Sanmina, composta da oltre 35.000 persone, lavorava sempre più in modalità mobile e da remoto, in particolare dopo la pandemia di COVID-19; questa situazione ha reso prioritaria l'adozione di un modello zero trust.

"Ogni giorno, diverse migliaia di persone lavorano da remoto e hanno bisogno di accedere a decine di migliaia di risorse", afferma Ramberg. *"L'utilizzo delle VPN era una pratica obsoleta che in realtà incrementava i rischi legati alla sicurezza informatica generando superfici di attacco"*.

Dopo aver valutato diverse opzioni, Sanmina ha deciso di estendere le capacità della piattaforma Zscaler Zero Trust Exchange™ già adottata con l'integrazione di Zscaler Private Access™ (ZPA).

Elemento fondamentale di Zero Trust Exchange, ZPA collega gli utenti e i dispositivi alle applicazioni, anziché alla rete. A differenza di firewall e VPN,[2] che creano backdoor che consentono l'ingresso delle minacce, Zero Trust Exchange rende gli utenti e le applicazioni invisibili alle minacce esterne, prevenendo al contempo il movimento laterale e consentendo alle aziende di limitare l'accesso degli utenti collegandoli solo alle applicazioni di cui hanno bisogno, senza mai collocarli sulla rete aziendale.

> ***"Avevamo bisogno di una soluzione di accesso adeguata al mondo moderno e senza perimetro".***
>
> **MATT RAMBERG**
> *Vice President of Information Security*
> **Sanmina**

[2] *I cinque principali rischi dei firewall perimetrali e l'unico modo per superarli tutti - Zscaler*

La decisione di Sanmina di adottare Zero Trust Exchange ha prodotto molti vantaggi. A differenza di quanto accadeva con le VPN, grazie a Zero Trust Exchange, il team responsabile della sicurezza informatica dell'azienda è ora in grado di controllare e proteggere in modo granulare tutto il traffico tra utenti e applicazioni, tutelando al contempo le applicazioni interne dalle vulnerabilità legate alla sicurezza.

Inoltre, gli indici di redditività del capitale investito da Sanmina per l'adozione di Zero Trust Exchange sono incrementati rapidamente. Rispetto a quanto accadeva con firewall e VPN, gli utenti aziendali ora godono di un accesso più rapido e senza interruzioni alle applicazioni pubbliche e private.

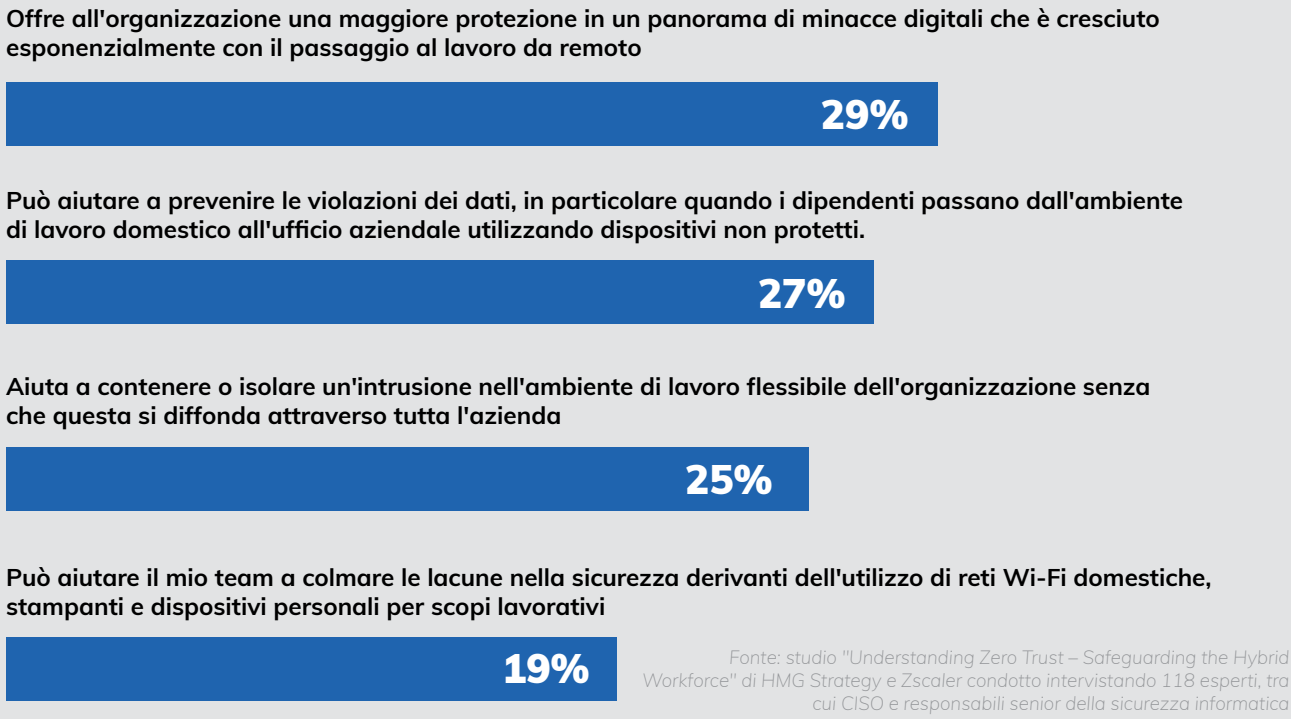
Inoltre, le spese per l'amministrazione IT si sono ridotte drasticamente, in quanto non è più necessario acquistare, configurare, gestire e aggiornare firewall, VPN e web gateway tradizionali. *"Avevamo diversi dispositivi fisici distribuiti in tutto il mondo, e ognuno di essi richiedeva configurazioni, regole, patch, aggiornamenti e contratti di manutenzione individuali"*, afferma Ramberg.

L'adozione di un'architettura zero trust da parte di Sanmina ha aiutato il produttore ad ampliare in modo sicuro l'utilizzo delle tecnologie dell'Industria 4.0, a ridurre i costi per l'amministrazione IT e ad accelerare i processi di fusione e acquisizione per incrementare l'agilità dell'azienda, migliorando al contempo l'esperienza utente. Nella prossima sezione di questo report, analizzeremo perché vi è un'urgente necessità di adottare questa metodologia di sicurezza dall'efficacia comprovata, e forniremo esempi di altre organizzazioni di alto livello che stanno traendo vantaggio da questa transizione.

Potenziare la sicurezza con lo zero trust

Quali sono i principali vantaggi per la sicurezza derivanti dall'adozione di un modello di sicurezza zero trust in un ambiente di lavoro flessibile?

GRAFICO 2:



Fonte: studio "Understanding Zero Trust – Safeguarding the Hybrid Workforce" di HMG Strategy e Zscaler condotto intervistando 118 esperti, tra cui CISO e responsabili senior della sicurezza informatica

Come indicato dai CISO e dai responsabili della sicurezza informatica, il principale vantaggio derivante dall'applicazione di un modello di sicurezza zero trust a un ambiente di lavoro flessibile consiste nel maggiore livello di protezione che offre per rispondere a un panorama di minacce digitali che è aumentato in modo esponenziale con il passaggio al modello di lavoro da remoto.

L'urgente necessità di adottare un modello zero trust

Il volume crescente di dipendenti che stanno facendo ritorno in azienda o che dividono il proprio tempo lavorando dall'ufficio e da remoto ha ampliato la superficie di attacco ed espone l'impronta digitale delle aziende a ulteriori vulnerabilità e sfide che i CISO e i team responsabili della sicurezza devono affrontare.

Il costante passaggio dei dipendenti tra il lavoro in ufficio e da remoto impiegando dispositivi non protetti apre la porta a una maggiore probabilità di violazioni dei dati e ad altri tipi di attacchi lanciati da criminali informatici e da aggressori associati a Stati-nazione. Questo è uno dei principali motivi per cui i responsabili della sicurezza intervistati durante l'indagine condotta da HMG Strategy e Zscaler hanno deciso di adottare un'architettura zero trust.

"Che sia dall'ufficio di casa, da una caffetteria, da un ufficio aziendale, con il computer portatile o tramite un Desktop as a Service con base cloud, gli utenti hanno comunque bisogno di accedere alle stesse risorse e di usufruire della stessa protezione per il traffico in uscita", afferma Lorenzin. *"Lo zero trust è l'approccio migliore, perché permette di avere policy e visibilità centralizzate e uniformi senza affidarsi a una moltitudine di prodotti singoli che potrebbero non essere coordinati tra loro e non offrire visibilità e controllo"*, aggiunge.

Careem protegge l'espansione della sua forza lavoro globale che opera prevalentemente da remoto

Un modello di sicurezza zero trust è diventato la scelta più ovvia per **Careem**, il principale fornitore di servizi di noleggio auto con autista del Medio Oriente.

Quando è stata fondata nel 2012, Careem utilizzava il tradizionale approccio alla sicurezza informatica a castello e fossato. Negli ultimi anni, l'azienda di Dubai è cresciuta in modo esponenziale in tutto il Medio Oriente e nel Nord Africa con una forza lavoro che opera prevalentemente da remoto, e i dirigenti hanno capito che il modello di sicurezza tradizionale adottato stava ostacolando la sua rapida crescita.

"Con il nostro business destinato a quadruplicare, ci siamo resi conto che la nostra infrastruttura di sicurezza legacy rappresentava un notevole spreco di risorse e ci impediva di reclutare efficacemente i lavoratori e di raggiungere i nostri obiettivi aziendali", spiega **Peeyush Patel**, CIO e CISO di Careem. *"Avevamo bisogno di modernizzare il nostro intero approccio alla sicurezza"*.

Per favorire il modello di sviluppo della sua app con base cloud, la forza lavoro operante prevalentemente da remoto e l'esplosivo trend di crescita del suo business, Careem ha deciso di sostituire la sua infrastruttura di sicurezza tradizionale, composta da oltre cinquanta firewall e decine di dispositivi VPN, con un approccio zero trust supportato dalla piattaforma Zscaler Zero Trust Exchange.

"La piattaforma Zero Trust Exchange è stata la scelta più naturale per poter dare vita a un modello SSE (Security Service Edge) zero trust e proteggere i nostri dati, i nostri dipendenti e i nostri clienti", spiega Patel.

Per snellire e semplificare la sua infrastruttura di sicurezza, Careem ha adottato più servizi all'interno di Zero Trust Exchange. Inizialmente, Careem ha distribuito Zscaler Internet Access™ (ZIA) per proteggere l'accesso alle applicazioni SaaS e a Internet, Zscaler Private Access (ZPA) per proteggere l'accesso alle applicazioni private di Careem nell'infrastruttura cloud pubblica e all'interno del suo data center, e Zscaler Digital Experience (ZDX) per rilevare e risolvere proattivamente i problemi di accesso prima che colpissero gli utenti.

All'interno della piattaforma, Careem utilizza anche un CASB (Cloud Access Security Broker) per tutelare i dati inattivi analizzando le applicazioni SaaS e gli ambienti IaaS, e la tecnologia di DLP (Data Loss Prevention) cloud per supportare la conformità alle normative quando vengono gestiti i dati personali sensibili sul cloud.

Una volta distribuita la piattaforma Zero Trust Exchange, Careem ha subito ottenuto agilità, produttività e vantaggi per tutta l'azienda, a partire dall'eliminazione della frustrazione e dei costi legati alla sicurezza della rete.

"I nostri colleghi erano molto insoddisfatti dell'accesso tramite VPN", ha dichiarato Patel. *"L'adozione della piattaforma e di ZPA non solo ha eliminato queste lamentele, ma ha migliorato notevolmente l'esperienza complessiva degli utenti, con un corrispondente aumento del Net Promoter Score (NPS) del 70% tra i nostri colleghi e CSR".*

Inoltre, Careem ha registrato un notevole risparmio di risorse, che ha potuto quindi reinvestire nelle sue attività di sviluppo. *"Semplificando l'accesso alle applicazioni di ingegneria, abbiamo recuperato circa 20.000 ore di sviluppo all'anno", ha dichiarato* Patel. *"Abbiamo quindi riorientato queste risorse verso la creazione di valore per l'azienda".*

L'esperienza di Careem rivela che un approccio zero trust non solo fornisce controlli e misure di sicurezza più efficaci negli ambienti di lavoro flessibili, ma offre anche maggiore agilità, produttività e risparmi sui costi. Nella sezione finale di questo report condivideremo i suggerimenti per distribuire un'architettura zero trust e tutelare al meglio la forza lavoro flessibile delle aziende.

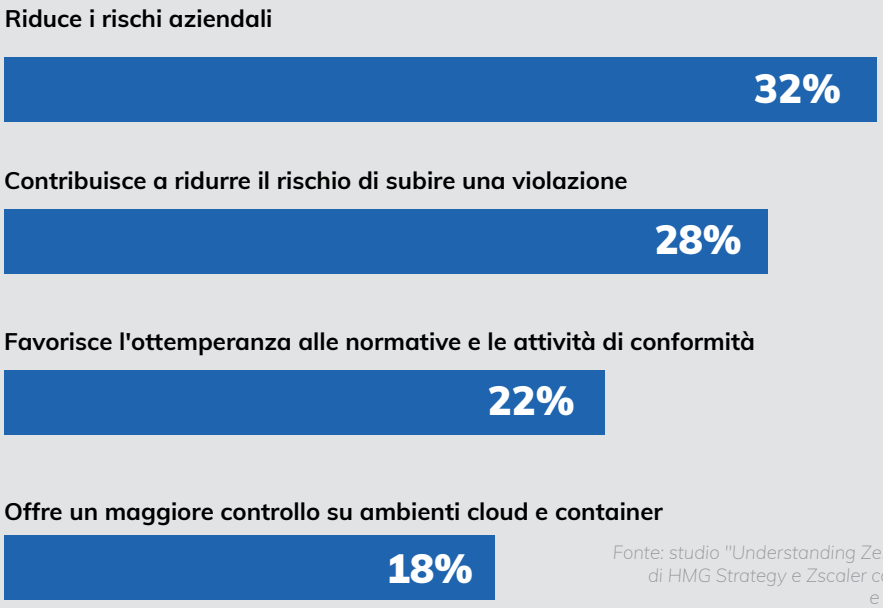
"La piattaforma Zero Trust Exchange è stata la scelta più naturale per poter creare un modello SSE (Security Service Edge) zero trust e proteggere i nostri dati, i nostri dipendenti e i nostri clienti".

PEEYUSH PATEL
CIO e CISO
Careem

I vantaggi dello zero trust: riduzione del rischio e maggiore controllo

Quali sono i principali vantaggi aziendali e operativi derivanti dall'adozione di un modello di sicurezza zero trust?

GRAFICO 3:



Fonte: studio "Understanding Zero Trust – Safeguarding the Hybrid Workforce" di HMG Strategy e Zscaler condotto intervistando 118 esperti, tra cui CISO e responsabili senior della sicurezza informatica

I VANTAGGI AZIENDALI E OPERATIVI DI UN MODELLO ZERO TRUST

I vantaggi aziendali e operativi che Sanmina, Careem e altre aziende hanno ottenuto grazie all'adozione di un approccio zero trust, sono in linea con le esperienze che Lorenzin ha riscontrato con altri clienti di Zscaler.

"L'utilizzo di un modello zero trust offre quattro principali vantaggi", spiega Lorenzin. "**Il primo è rappresentato dalla flessibilità e dalla resilienza** date dalla distribuzione rapida e dalla capacità di adattarsi rapidamente ai cambiamenti man mano che l'organizzazione si evolve".

"Il secondo vantaggio consiste nell'incremento della sicurezza", dichiara Lorenzin. "Ciò include la capacità di rimuovere la superficie di attacco esterna e i mezzi per ridurre e potenzialmente eliminare il movimento laterale non autorizzato".

Il terzo è il miglioramento dell'esperienza utente, che fornisce un accesso più rapido, più semplice e più uniforme alle applicazioni.

Il quarto principale vantaggio consiste nella riduzione dei costi.

"È possibile eliminare il CapEx (spese in conto capitale) non solo per i molteplici gateway VPN distribuiti in tutto il mondo, ma anche per gli stack di apparecchi e funzionalità (bilanciamento del carico, firewall DMZ, protezione da DDoS) associati a quei gateway VPN", afferma Lorenzin.

I quattro vantaggi di un'architettura zero trust

Inizia il tuo viaggio verso lo zero trust

Per i CISO e i responsabili della sicurezza che stanno per intraprendere il proprio viaggio verso lo zero trust, un buon punto di partenza consiste nell'identificare un caso d'uso definito e semplice a cui applicare i principi dello zero trust, determinare quali sono i controlli che l'organizzazione ha già implementato, e infine applicare il modello zero trust allo stesso caso d'uso per dimostrarne i vantaggi.

"Individua un caso d'uso che sia potenzialmente a basso impatto. Concediti la possibilità di provare qualcosa di nuovo. Non partire dal problema più difficile da affrontare", consiglia Lorenzin.

A partire da qui, i responsabili della sicurezza possono comunicare al CEO e al consiglio di amministrazione cos'è un'architettura zero trust e spiegare loro che si tratta di un modello progettato per ridurre i rischi, supportare il business e fornire all'azienda maggiore flessibilità e agilità rispetto ai tradizionali approcci alla sicurezza incentrati sulla rete. L'uso di analogie può aiutare a definire meglio l'approccio zero trust e a renderlo di facile comprensione anche per i membri meno esperti del consiglio di amministrazione.

I responsabili della sicurezza possono quindi mostrare i successi ottenuti con il progetto pilota per dimostrare il valore di un approccio zero trust e favorire l'ottenimento di investimenti a supporto dell'adozione di questa strategia.

È inoltre utile raccogliere feedback e spunti di riflessione da altri professionisti in merito alle loro esperienze con le distribuzioni zero trust. Tra i forum più noti per ottenere questo tipo di informazioni indichiamo CXO REvolutionaries Forum. Queste interazioni possono anche fornire dei suggerimenti per trovare un partner zero trust di fiducia in grado di offrire la piattaforma più adatta per affrontare ogni singolo caso d'uso prioritario per l'organizzazione e la capacità di raggiungere i propri obiettivi strategici legati allo zero trust.

"Approfitta dalle conoscenze delle community del settore interagendo con chi ha intrapreso questo percorso da molto più tempo di te", spiega Lorenzin.

Come abbiamo dimostrato, adottare un'architettura zero trust non è solo opportuno, ma è di vitale importanza per tutelare la forza lavoro flessibile e il business digitale, e tutti gli sforzi necessari per intraprendere questa transizione saranno senza dubbio ripagati.

Informazioni su HMG Strategy

HMG Strategy è la principale piattaforma digitale al mondo che mette in contatto i dirigenti del settore tecnologico per ripensare l'impresa e rimodellare il mondo del business. Le CIO e CISO Executive Leadership Series regionali e virtuali, i libri e il Digital Resource Center che abbiamo realizzato offrono approfondimenti di ricerca unici di CIO, CISO, CTO e dirigenti esperti del settore tecnologico su temi come leadership, innovazione, trasformazione e crescita professionale.

La rete globale di HMG Strategy è composta da oltre 400.000 dirigenti IT, esperti di settore e leader di alto livello riconosciuti in tutto il mondo.

Per saperne di più sui 7 pilastri dell'affidabilità del modello di business unico di HMG Strategy, fai clic qui.

HMG Strategy: la piattaforma digitale numero 1 e più accreditata che mette in contatto i dirigenti del settore tecnologico per ripensare l'impresa e rimodellare il mondo del business.

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita di dati, grazie alla connessione sicura di utenti, dispositivi e applicazioni, in qualsiasi luogo. Distribuita in più di 150 data center a livello globale, Zero Trust Exchange, basata su SASE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su zscaler.it o seguici su Twitter @zscaler.