E-BOOK

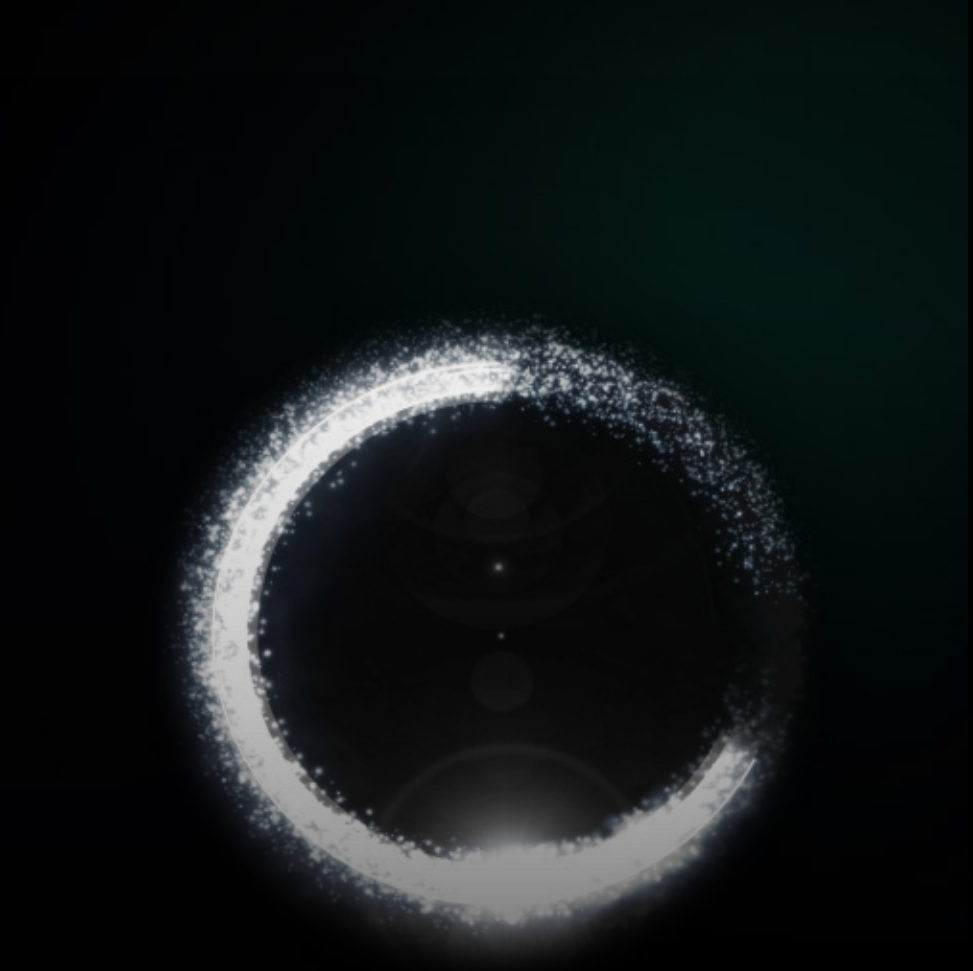
Le tre chiavi per la trasformazione attraverso l'approccio zero trust: **piattaforma, persone e processo**

INTRODUZIONE

La strada verso lo zero trust

La trasformazione digitale ha cambiato radicalmente il modo di operare delle aziende moderne. I **dipendenti passano molto più tempo su Internet, rispetto a quanto ne trascorrono sulla rete aziendale,** accedendo ad applicazioni e dati da qualsiasi luogo. I dati aziendali sensibili sono diventati più distribuiti, risiedono al di fuori del perimetro aziendale nelle applicazioni SaaS, come Microsoft 365, e nelle applicazioni private su AWS, Azure e Google Cloud Platform.

Il processo di trasformazione digitale migliora l'agilità aziendale e il flusso delle informazioni, ma estende notevolmente la superficie di attacco ed espone l'azienda a nuove minacce. Le architetture di sicurezza tradizionali, incentrate sulla protezione della rete, non sono più efficaci in questa nuova realtà. La protezione dell'azienda e il mantenimento dei vantaggi della **trasformazione digitale richiedono la migrazione verso un modello di sicurezza zero trust fornito attraverso il cloud,** che sia il più vicino possibile a dove oggi si concentrano gli utenti e le risorse aziendali.



DEFINIZIONE

Che cosa è l'approccio zero trust?

Si sente parlare del concetto di zero trust da oltre un decennio, tuttavia c'è ancora molta confusione su cosa significhi realmente questo termine. Non si tratta semplicemente di una singola tecnologia.

Lo zero trust è un approccio olistico alla sicurezza delle organizzazioni moderne, basato sull'accesso a privilegi minimi e sul principio che **nessun utente o applicazione deve essere intrinsecamente ritenuto attendibile, appunto "zero trust" ossia attendibilità zero.** Si parte quindi dal presupposto che tutto sia ostile e **si stabilisce l'attendibilità solo in base all'identità e al contesto dell'utente,** impiegando policy volte al controllo degli accessi in ogni fase del percorso.

DEFINIZIONE

Lo zero trust nella pratica

L'approccio zero trust affronta le sfide più difficili che oggi riguardano la sicurezza, il networking e l'abilitazione dell'ambiente di lavoro moderno:

SICUREZZA

Prevenire le minacce informatiche:

L'approccio zero trust offre protezione dalle minacce informatiche, non solo per gli utenti, ma anche per i carichi di lavoro cloud, per i server e per le applicazioni SaaS.

Prevenire la perdita dei dati:

Lo zero trust fornisce un approccio olistico volto a garantire che i dati non possano essere divulgati o persi, sia accidentalmente che intenzionalmente, dagli utenti o dai carichi di lavoro cloud.

RETI

Semplificare la connettività di utenti e filiali:

L'approccio zero trust consente alle organizzazioni di trasformare le reti hub-and-spoke legacy, consentendo alle filiali e agli utenti da remoto di connettersi in modo sicuro a qualsiasi destinazione direttamente tramite Internet, indipendentemente da dove si connetta l'utente.

Garantire la sicurezza della connettività cloud:

Anziché estendere le tradizionali VPN da sito-a-sito al cloud, il che comporta il rischio di spostamenti laterali, lo zero trust consente ai carichi di lavoro di connettersi in modo sicuro ad altri carichi di lavoro.

IMPLEMENTARE L'AMBIENTE DI LAVORO MODERNO

Garantire la sicurezza del lavoro da qualsiasi luogo:

Una vera e propria soluzione zero trust dovrebbe consentire ai dipendenti di lavorare in modo sicuro e senza problemi da qualsiasi luogo, senza doversi preoccupare della rete o di dover o meno attivare una VPN.

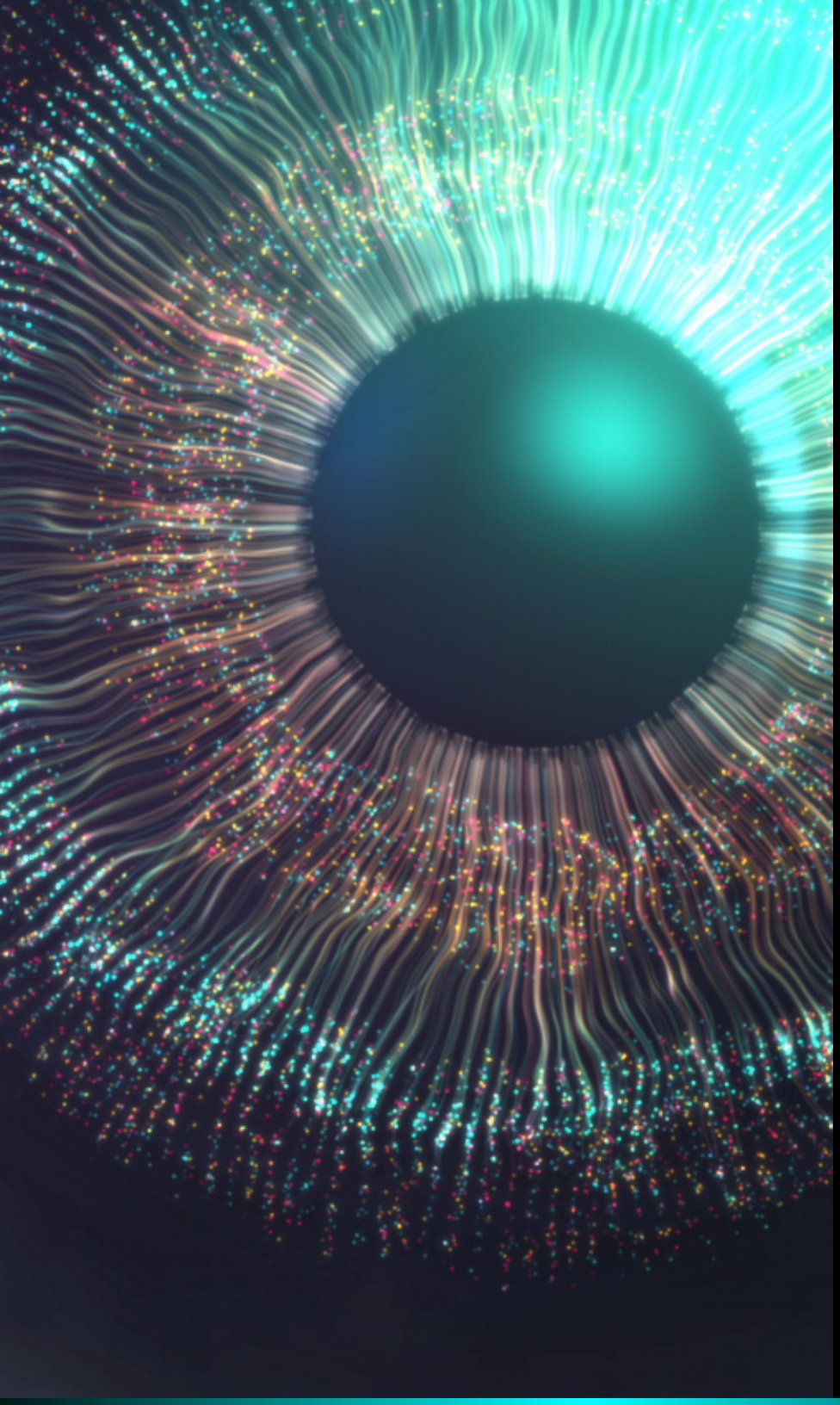
Ottimizzare le esperienze utente:

Assicurando la comprensione dell'esperienza di ogni dipendente per ogni applicazione, lo zero trust consente alle organizzazioni di fornire un'esperienza utente ottimale.

Pianificazione del successo dell'approccio zero trust

Mano a mano che Internet diventa la nuova rete aziendale, lo zero trust fornisce il percorso per **un accesso rapido, senza interruzioni e sicuro** sull'intero ecosistema aziendale.

Tuttavia, l'implementazione di un modello di sicurezza zero trust non è solo una funzione dell'IT, in quanto influisce su tutte le aree dell'azienda e va oltre i confini tradizionali dell'organizzazione. Implementare con successo l'approccio zero trust richiede una strategia mirata che affronti le sfide ed evidenzi le opportunità tra **persone, processi e piattaforme tecnologiche.** →



LE BASI DELL'APPROCCIO ZERO TRUST

Piattaforma

Lo zero trust non riguarda semplicemente una singola tecnologia, come l'identità o la segmentazione delle applicazioni; si tratta di una strategia, **una base su cui costruire il proprio ecosistema di sicurezza.** Questo approccio collega in modo sicuro gli utenti alle applicazioni utilizzando policy aziendali su Internet e ha al centro una piattaforma tecnologica zero trust guidata da tre principi chiave:

1. Connettività basata su **identità e policy**
2. Rendere **le applicazioni invisibili**
3. **Architettura basata su proxy** per connettersi alle app e ispezionare il traffico

LE BASI DELL'APPROCCIO ZERO TRUST

Piattaforma

1 Connettività basata su identità e contesto

Le VPN e i firewall tradizionali mettono gli utenti in rete per consentirgli l'accesso alle applicazioni. Una volta sulla rete, l'attendibilità intrinseca concessa all'utente aumenta il rischio di movimento laterale da parte di minacce o aggressori. Al contrario, l'approccio zero trust utilizza identità e policy in base al contesto per connettere in modo sicuro gli utenti autenticati a una singola specifica applicazione autorizzata, in base a policy granulari di accesso e sicurezza, senza mai mettere gli utenti sulla rete aziendale. La limitazione dell'accesso previene i movimenti laterali e riduce i rischi aziendali. Inoltre, poiché nessuna risorsa di rete viene esposta a Internet, è possibile proteggersi da attacchi DDoS e mirati.

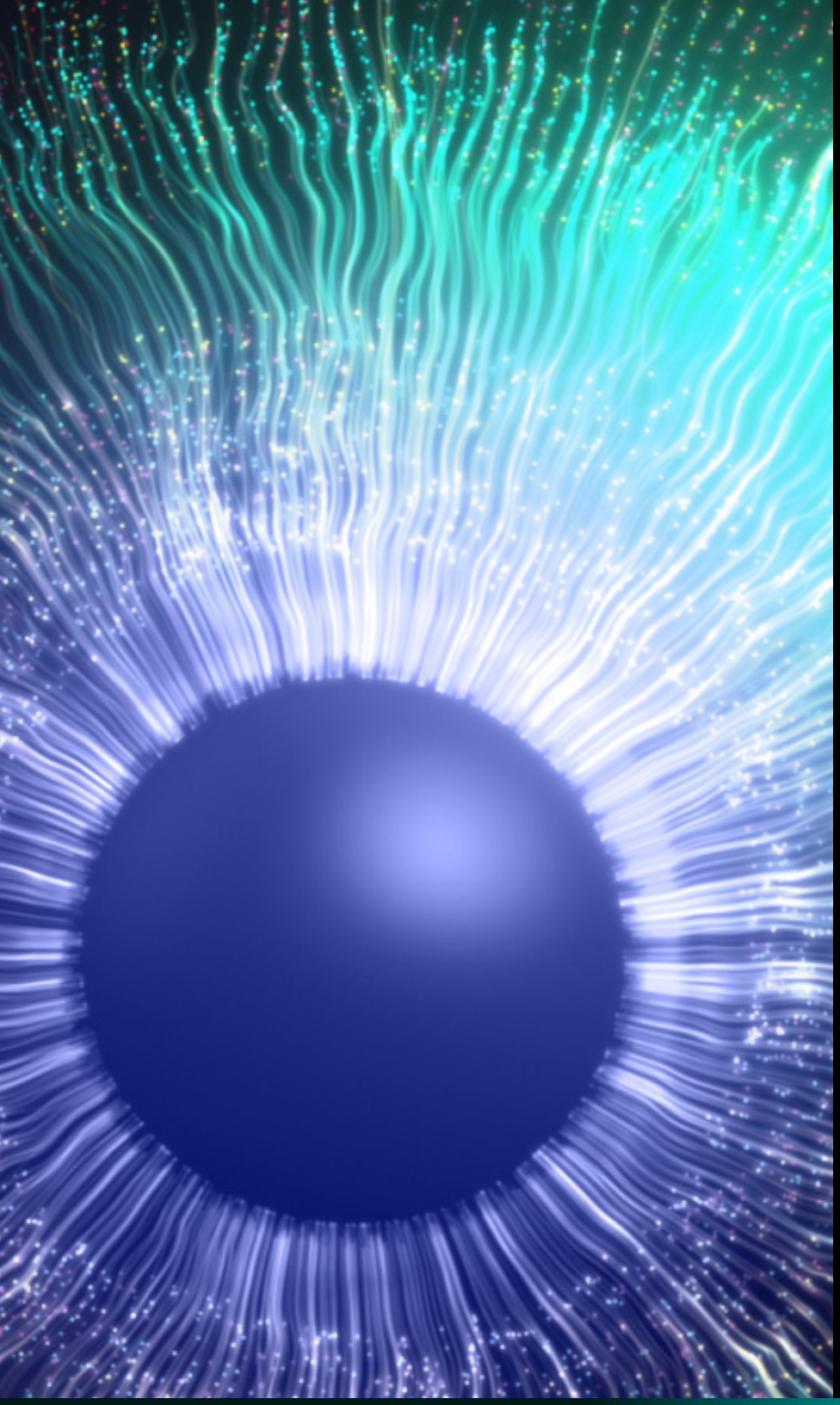
2 Rendere le applicazioni invisibili

La migrazione delle applicazioni verso il cloud espande notevolmente la superficie d'attacco. I firewall tradizionali pubblicano le app su Internet, il che significa che possono essere facilmente trovate da utenti e hacker. Un approccio zero trust consente di evitare di esporre la rete aziendale a Internet, nascondendo le identità di origine e offuscando gli indirizzi IP. Rendendo le app invisibili agli avversari e accessibili solo agli utenti autorizzati, la superficie di attacco viene ridotta e l'accesso alle applicazioni, tramite Internet, SaaS o cloud pubblici o privati, è sempre sicuro.

3 Architettura basata su proxy per connettersi alle app e ispezionare il traffico

I firewall di nuova generazione hanno difficoltà a ispezionare il traffico criptato. Di conseguenza le organizzazioni, spesso, finiscono per aggirare l'ispezione del traffico criptato, aumentando il rischio di minacce informatiche e di perdita dei dati. Inoltre, i firewall utilizzano un approccio "passthrough", che consente a contenuti sconosciuti di raggiungere la destinazione prima che qualsiasi analisi venga completata. Se viene rilevata una minaccia, viene inviato un avviso, ma potrebbe essere troppo tardi. D'altro canto, una protezione efficace contro le minacce e una prevenzione completa contro la perdita dei dati richiedono un'architettura proxy progettata per ispezionare le sessioni SSL, analizzare il contenuto all'interno delle transazioni e prendere decisioni in tempo reale sulle policy e sulla sicurezza, prima di consentire al traffico di proseguire verso la destinazione. Inoltre, tutto questo deve essere eseguito su larga scala, senza influire sulle prestazioni, indipendentemente dal luogo in cui si connettono gli utenti.

Azione consigliata: valuta una piattaforma zero trust come **Zscaler Zero Trust Exchange™**



UN CAMBIAMENTO CULTURALE

Le persone

Il successo dell'adozione dello zero trust inizia con la piattaforma giusta, ma dipende dall'intento dell'organizzazione **di sviluppare nuove competenze e adottare una nuova mentalità culturale.** Dai leader IT, che si trovano di fronte alla necessità di trasformarsi in modo rapido e sicuro, ai professionisti IT di base, che implementano lo zero trust, tutti, dal team esecutivo agli utenti finali e all'ecosistema esteso devono essere inclusi per garantire il successo.

UN CAMBIAMENTO CULTURALE

Le persone

I leader IT

In qualità di leader IT, è necessario essere sia innovatori che strateghi. Il percorso dello zero trust richiede l'allineamento delle priorità aziendali e dell'IT, la suddivisione in silo e l'applicazione delle tecnologie e dell'architettura giuste per promuovere la trasformazione e raggiungere i risultati desiderati per il business. Durante il percorso verso l'approccio zero trust, si avrà bisogno di:

- **Comprendere le best practice e le strategie** per la trasformazione entrando in contatto con i colleghi e organizzando l'azienda per implementare tali cambiamenti
- **Aiutare i professionisti IT a sviluppare le competenze e le conoscenze** necessarie per passare con successo da un'architettura incentrata sulla rete a un'architettura zero trust
- Rendere lo zero trust **invisibile agli utenti finali**

Azione consigliata:
entra in contatto con innovatori che condividono la stessa ideologia sull'approccio zero trust e sulle best practice per la trasformazione digitale attraverso un forum come **Zero Trust REvolutionaries**

UN CAMBIAMENTO CULTURALE

Le persone

I professionisti IT

I team IT sono esperti in rete e sicurezza, abituati a lavorare sull'hardware e a definire policy sulla base di 30 anni di standard di rete e sicurezza IT. La migrazione all'approccio zero trust **influisce direttamente sui professionisti IT.** Molte delle competenze su cui hanno fatto affidamento in passato dovranno essere aggiornate e dovranno svilupparne di nuove per supportare la trasformazione digitale; il risultato sara' un impatto notevolmente maggiore sull'organizzazione e il disporre di un bagaglio di conoscenze molto più prezioso e orientato al futuro.

Il successo dipende dall'offerta di **formazione avanzata per consentire la transizione della forza lavoro IT,** un'offerta che garantisca la relativa comprensione dei nuovi processi aziendali, nonché delle best practice e delle procedure per l'utilizzo dei servizi zero trust. Allo stesso tempo, è possibile dimostrare in che modo l'approccio zero trust **consenta di risparmiare tempo** e di **offrire più valore** all'organizzazione.

Azione consigliata:
aiuta i professionisti IT a essere al passo con l'approccio zero trust, grazie a un programma di formazione certificato: Zscaler™ Zero Trust Academy

UN CAMBIAMENTO CULTURALE

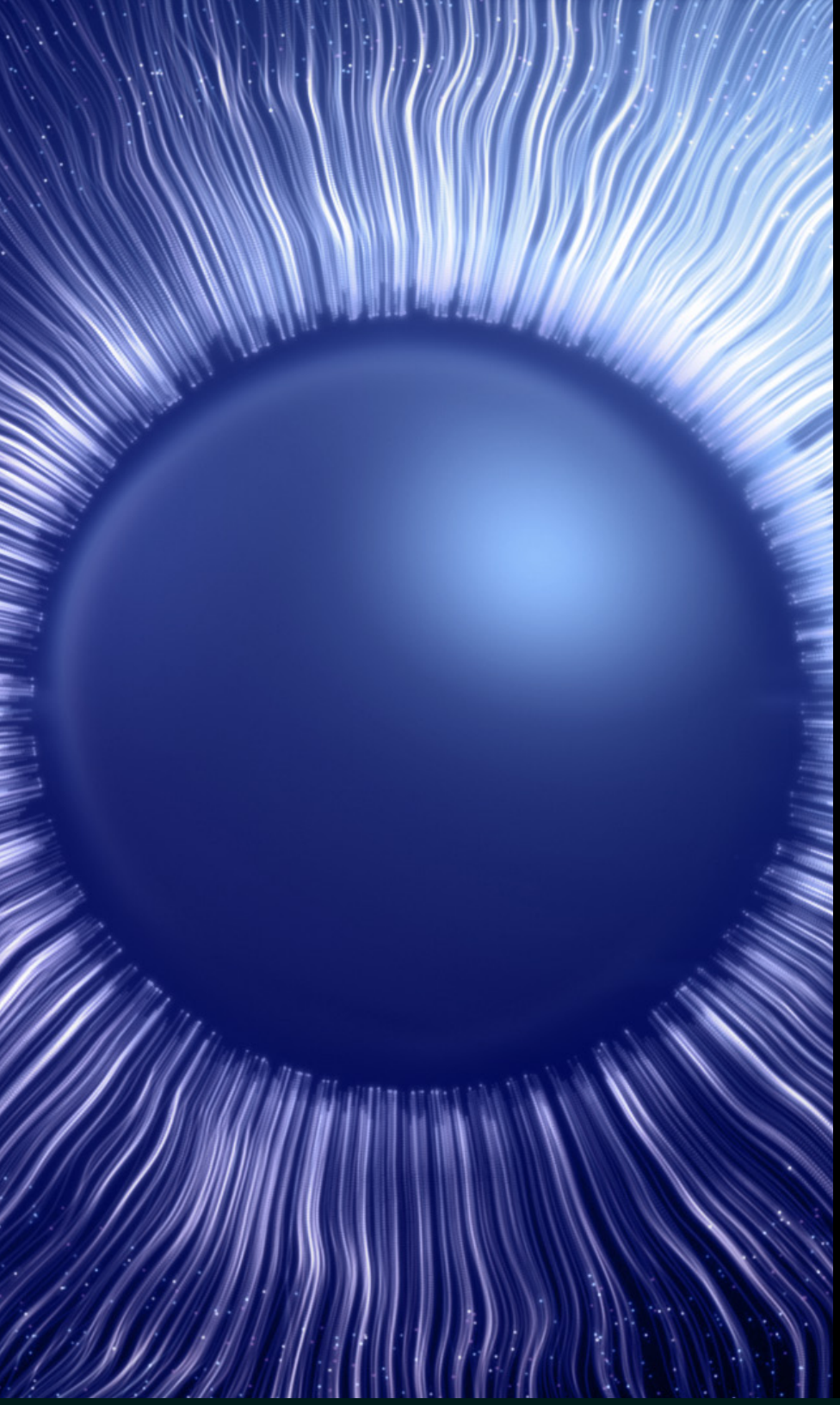
Le persone

Gli utenti

Se impostato correttamente, l'approccio zero trust è un fattore abilitante invisibile per gli utenti finali, il che consente ai dipendenti di lavorare da qualsiasi luogo e da qualsiasi dispositivo. Dato che l'accesso zero trust si basa sempre su policy di identità e aziendali, e il servizio cloud connette automaticamente gli utenti alle applicazioni tramite il percorso di accesso più rapido, la posizione fisica dell'utente non è più importante. Un utente che lavora in ufficio gode della **medesima esperienza di accesso veloce e coerente** rispetto a quando lavora da casa o da qualsiasi luogo.

Allo stesso tempo, una soluzione zero trust solida consente alle organizzazioni di **ridurre drasticamente i rischi senza bloccare l'accesso degli utenti** alle applicazioni. Ad esempio, la tecnologia di isolamento del browser cloud può fornire un accesso sicuro ai contenuti attivi offrendo pagine web sotto forma di pixel rese in un ambiente isolato, senza influire sull'esperienza utente. Può inoltre essere sfruttata per limitare la possibilità di copiare e incollare i dati, impedire il download di file o confinare i download nel contenitore di isolamento, per proteggere i dispositivi endpoint da ransomware e altre minacce sofisticate. In questo modo, lo zero trust sfrutta la tecnologia per limitare i rischi in base al contesto.

Azione consigliata:
utilizza architetture zero trust che includono strumenti che garantiscono agli utenti un'esperienza ottimale, come **Zscaler Digital Experience**



UN PERCORSO PROGRAMMATICO

Il processo

Quali sono i passaggi per la configurazione dello zero trust e come è possibile accelerare la trasformazione del business? Sapere da dove cominciare può essere la parte più complessa di questo percorso, ma non deve essere necessariamente così. L'approccio zero trust inizia con una piattaforma e deve estendersi per **comprendere dati, persone, dispositivi e carichi di lavoro.**

Pertanto, le integrazioni solide dei prodotti con il provider di identità, la soluzione per la sicurezza degli endpoint e la soluzione SIEM sono elementi essenziali nel quadro dell'approccio zero trust, per poter aggiungere ulteriore contesto e semplificare l'adozione.

UN PERCORSO PROGRAMMATICO

Il processo

Alla luce della necessità di integrazione, consigliamo una **piattaforma zero trust e un ecosistema di partner della tecnologia** che forniscano i seguenti strumenti per creare un progetto informato e potenziare l'adozione dello zero trust:

- **Progetti della soluzione,** che forniscano le architetture di riferimento dei casi d'uso
- **Guide alla progettazione,** che condividano i principi di progettazione e le best practice di integrazione
- **Guide all'implementazione,** che forniscano una linea guida alla configurazione durante l'attivazione delle integrazioni per la prova di valore (PoV) e l'implementazione della produzione

L'implementazione di una soluzione olistica zero trust diventa molto più semplice con il progetto giusto. Cerca i fornitori con architetture di riferimento convalidate congiuntamente, progettate per affrontare un insieme specifico di casi d'uso, e con una guida prescrittiva alla progettazione dedicata agli architetti della sicurezza sull'utilizzo integrato di queste piattaforme sulla base delle best practice.

Tali linee guida forniscono un framework più strutturato che semplifica l'implementazione, garantisce operazioni efficienti e la migliore esperienza utente e consente l'applicazione di una sicurezza ottimale. Tutto ciò permetterà di accelerare l'adozione dello zero trust in tutta l'organizzazione.

Azione consigliata: sfrutta le soluzioni con integrazioni approfondite dei partner che forniscono progetti convalidati, come quelli presenti **nell'ecosistema zero trust di Zscaler.**

Sfrutta appieno le opportunità offerte dallo zero trust

La trasformazione digitale rende le aziende più agili ed efficienti, ma richiede di ripensare le architetture di rete e di sicurezza. L'approccio zero trust fornisce **le basi per le organizzazioni cloud-first, per accelerare la trasformazione digitale** e dare ai dipendenti la possibilità di lavorare in modo produttivo e sicuro da qualsiasi luogo. All'inizio del percorso verso lo zero trust, lo sviluppo di una strategia che integri la piattaforma, le persone e i processi giusti contribuirà a garantirne il successo.

È bene individuare una piattaforma che utilizzi policy di identità e aziendali per stabilire l'attendibilità e connettere gli utenti alle risorse senza inserirli nella rete aziendale. È bene proteggere le applicazioni rendendole invisibili agli avversari e accessibili solo agli utenti autorizzati e usare un'architettura proxy, non un firewall passthrough, per proteggere i dati e garantire un'efficace protezione dalle minacce informatiche.

È bene entrare in contatto con i propri colleghi per acquisire le best practice e le strategie alla base della trasformazione, allineare l'organizzazione per adottare una nuova mentalità culturale e sviluppare le competenze necessarie per implementare e gestire un'architettura zero trust, garantendo al contempo che lo zero trust sia invisibile e senza soluzione di continuità per gli utenti finali. Tutto questo diventa più facile con il progetto giusto. È possibile sfruttare **una piattaforma zero trust tramite integrazioni solide dei partner che forniscono architetture di riferimento convalidate congiuntamente e linee guida prescrittive per la progettazione** per l'utilizzo integrato di queste piattaforme.

Tenendo a mente questi elementi, sarà possibile **sfruttare appieno le opportunità offerte dallo zero trust, accelerare la trasformazione digitale e rendere l'IT un vero fattore di abilitazione aziendale.**

Esplora gli innumerevoli vantaggi di **una vera piattaforma zero trust.**

Inizia il tuo percoso

zscaler™

©2021 Zscaler, Inc. Tutti i diritti riservati.Zscaler™ e Zero Trust Exchange™ sono (i) marchi commerciali o marchi di servizio registrati o (ii) marchi commerciali o marchi di servizio di Zscaler, Inc. negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi commerciali sono di proprietà dei rispettivi proprietari.