Progetto per il rientro in ufficio: come modernizzare gli ambienti di lavoro con lo zero trust

WHITE PAPER

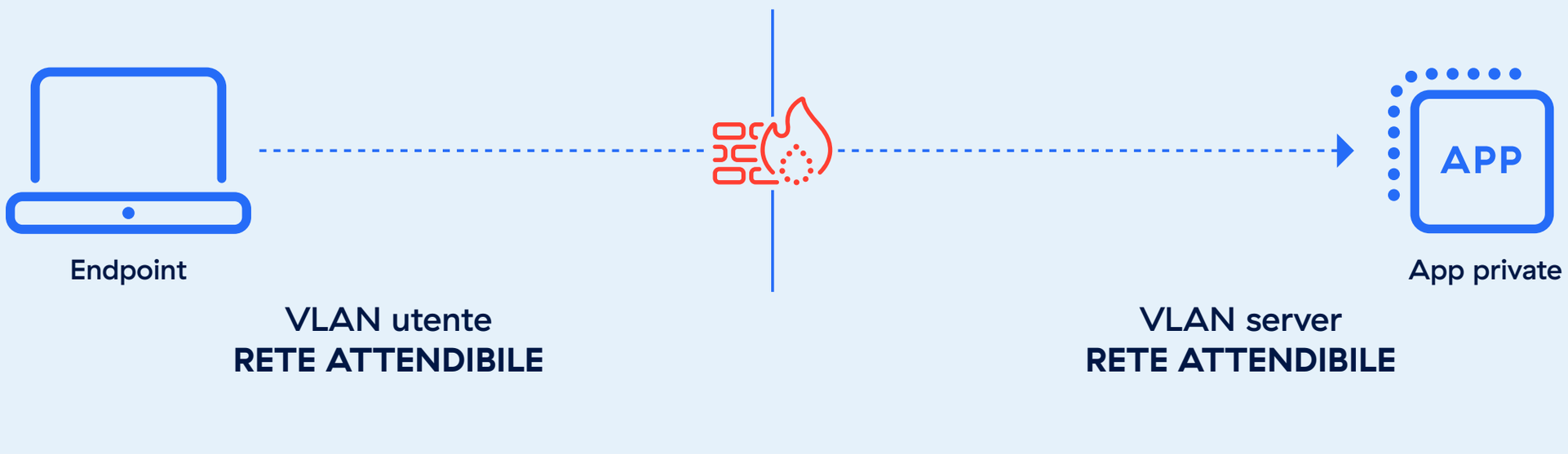
Il rientro in ufficio non sarà un ritorno al passato. I dipendenti rientreranno in ufficio, ma le applicazioni e i dati no. Anni di lavoro da remoto e ibrido hanno incrementato nei dipendenti la dipendenza e la familiarità con le applicazioni con base cloud e quando rientreranno in ufficio si aspettano la stessa affidabilità e reattività dell'IT, se non maggiore. Tornare a un approccio basato sul "facciamo come abbiamo sempre fatto" non soddisferà queste aspettative.

La migrazione delle applicazioni e dei dati verso il cloud richiede un nuovo approccio alla sicurezza on-premise, che non comprometta la produttività. Lo zero trust, inizialmente adottato per supportare il lavoro sicuro da remoto, offre gli stessi vantaggi anche al personale on-premise e dovrebbe essere considerato un fattore chiave per gli ambienti di lavoro moderni.

Sicurezza tradizionale in ufficio: l'attendibilità è gestita da barriere fisiche

In passato, le reti aziendali erano progettate come delle fortezze, in cui si dava per scontato che tutti gli utenti o i dispositivi operanti all'interno dei confini fisici degli uffici fossero attendibili, delineando così il cosiddetto "perimetro" di sicurezza. Questo modello era adatto quando i sistemi degli uffici erano statici e tutti erano collegati alla stessa infrastruttura.

Nel modello di sicurezza della rete tradizionale, basato sul perimetro, una connessione a un ufficio dell'ente colloca il dispositivo della workstation sulla rete attendibile:



Nel modello tradizionale, la connessione alla rete implicava l'accesso a tutte le applicazioni, risorse e dati disponibili sulla rete. Per contribuire ad attenuare la preoccupazione che un utente o dispositivo non autorizzato riesca a connettersi alla rete attendibile, è possibile implementare uno strumento come un Network Access Control (NAC) per controllare l'accesso alla rete, ad esempio per impedire a un dispositivo non attendibile di connettersi a meno che non disponga di un certificato rilasciato dall'infrastruttura PKI dell'ente.

Si tratta di un buon passo avanti, ma risulta comunque inefficiente rispetto a un modello di sicurezza basato sulla segmentazione e sull'accesso a privilegi minimi, questo perché l'approccio basato sulla rete attendibile è caratterizzato da:

- Accesso esteso e illimitato
- Controlli limitati e granulari
- Vulnerabilità della rete interna

Gli elementi che caratterizzano un approccio basato sulla rete attendibile, ovvero il presupposto di privilegi di accesso estesi, una segmentazione limitata e la rilevabilità intrinseca delle reti interne, non sono più in linea con la realtà di oggi, che vede minacce sempre più avanzate. In un mondo in cui gli attacchi informatici sempre più sofisticati, le minacce interne e la proliferazione degli strumenti di accesso remoto sono la norma, i modelli di sicurezza basati sul perimetro risultano del tutto inefficienti nel rispondere alle vulnerabilità moderne. Gli aggressori sfruttano le inadeguatezze delle architetture legacy aggirando i controlli di segmentazione scadenti e riuscendo a muoversi lateralmente una volta all'interno della rete, spesso utilizzando delle credenziali legittime per evitare di essere rilevati. Questa realtà richiede un cambio di paradigma nell'approccio alla sicurezza delle organizzazioni, passando da una rete basata sull'"attendibilità per impostazione predefinita" a un modello che opera secondo i principi dello zero trust: verificando e convalidando ogni tentativo di accesso in modo dinamico, per tutti gli utenti, i dispositivi e le applicazioni.

Le organizzazioni hanno bisogno di un approccio che:

- Restringe l'estensione dell'accesso con connessioni granulari specifiche per app
- Introduce l'applicazione dinamica delle policy in base all'identità e al profilo di sicurezza del dispositivo
- Consente una verifica continua con una valutazione costante del singolo accesso

Questa non è un'infrastruttura futuristica, è già disponibile nell'architettura di rete zero trust (ZTNA), creata per supportare il lavoro da remoto.

Un ambiente di lavoro supportato dallo zero trust

Quando i dipendenti hanno iniziato a lavorare da qualsiasi luogo, le applicazioni sono state spostate sul cloud e i presupposti sull'attendibilità su cui si basavano i modelli tradizionali sono crollati. L'approccio zero trust, che sostituisce il principio di "presunzione dell'attendibilità" con quello della "verifica costante", si è rivelato la soluzione più efficace per fornire agli utenti l'accesso di cui avevano bisogno.

Nel contesto del rientro in ufficio, il concetto dello zero trust diventa ancora più essenziale. Negli ultimi anni, la maggior parte delle applicazioni e dei servizi IT si è spostata sul cloud, con il conseguente incremento della produttività e dell'efficienza operativa. Il ritorno a pratiche obsolete, pre-cloud e basate sul perimetro, sarebbe controproducente e incompatibile con gli ambienti di lavoro moderni.

Lo zero trust è più di un semplice aggiornamento della sicurezza: è un'opportunità strategica per reinventare e rendere gli uffici moderni a prova di futuro.
Un approccio zero trust offre alle organizzazioni agilità, scalabilità e risparmi sui costi. Che si tratti di creare una nuova filiale, realizzare hub di collaborazione temporanei o gestire team ibridi, lo zero trust elimina la necessità di ricorrere a costose installazioni di rete, come le soluzioni MPLS o gestite dalle compagnie di telecomunicazione. Riduce inoltre la dipendenza non necessaria da complesse infrastrutture di sicurezza on-premise.

Ma la cosa più importante è che lo zero trust garantisce la piena attualità ed efficacia dell'approccio alla sicurezza. Con la continua evoluzione degli strumenti e dei flussi di lavoro, le organizzazioni basate su un approccio zero trust possono integrare le nuove tecnologie, senza essere ostacolate da configurazioni di rete obsolete. Possono così liberarsi definitivamente dai firewall e dagli altri dispositivi datati e rendere la loro strategia di sicurezza a prova di futuro.

Gli utenti sono rientrati in ufficio, ma le app no

Oggigiorno, la maggior parte del lavoro avviene tramite applicazioni con base cloud, anche per i dipendenti che lavorano dalla sede centrale di un'azienda. L'ufficio non è più il fulcro di tutto ciò che riguarda l'IT. Anzi, chi lavora dagli uffici accede alle risorse in modo molto simile ai dipendenti che lavorano da remoto.

Questo cambiamento radicale ha introdotto diverse criticità:

- **Uffici come colli di bottiglia per la connettività:** gli utenti che rientrano in ufficio spesso comportano il backhauling del traffico dal cloud verso la rete aziendale, generando latenza e incidenti non necessari.

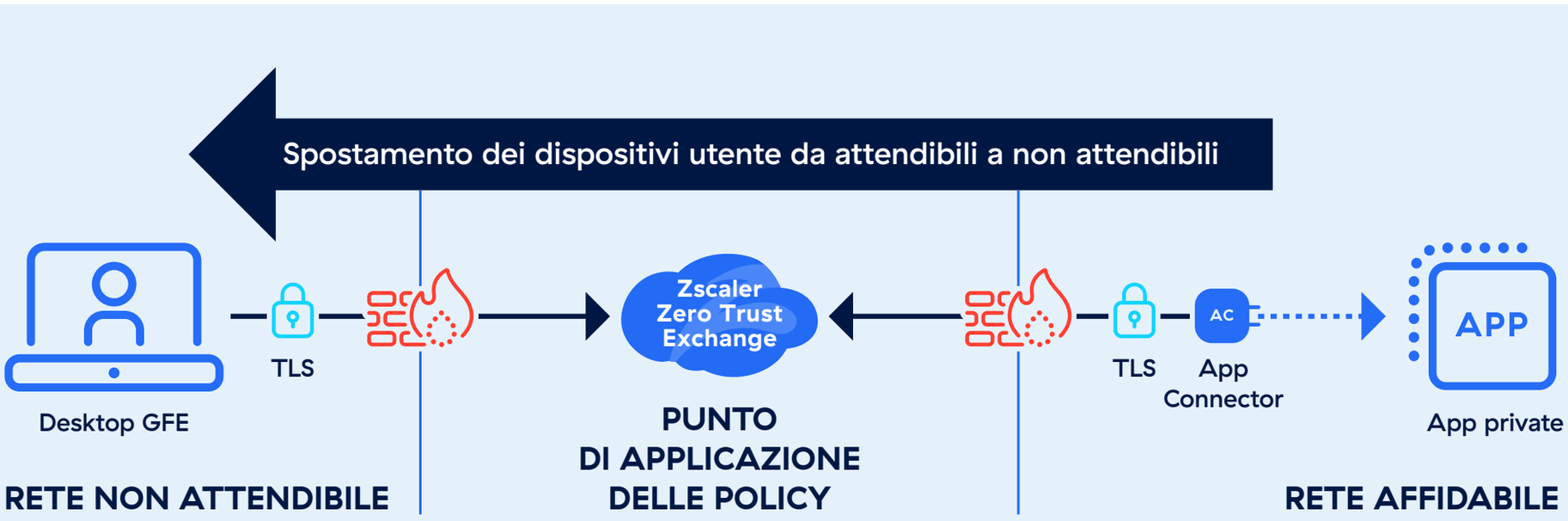
- **Esperienza utente compromessa:** quando lavorano in ufficio, i dipendenti potrebbero notare un peggioramento delle prestazioni delle applicazioni rispetto alle loro configurazioni da remoto. Il problema non è sempre la rete, potrebbe infatti dipendere da qualsiasi cosa: da una risoluzione DNS lenta a una connessione Wi-Fi scarsamente ottimizzata, ma senza il giusto grado di visibilità, individuare la causa alla radice risulta molto arduo per l'IT.

- **Strumenti di monitoraggio non integrati tra loro:** i sistemi di monitoraggio legacy spesso si concentrano sulla disponibilità della rete, anziché sui parametri effettivi dell'esperienza utente, come le prestazioni delle applicazioni, la latenza o l'integrità degli endpoint.

Come ripensare le reti degli uffici

Immaginiamo per un attimo un modello di connessione a Internet simile a quello che potremmo trovare in un "bar", in cui i dipendenti si collegano a Internet proprio come farebbero a casa loro. Sebbene questa prospettiva possa rappresentare un cambiamento radicale, l'infrastruttura per realizzarlo esiste già nell'architettura di rete zero trust.

In questo scenario, non vi è alcuna presunzione dell'attendibilità tramite la connessione alla rete. Di conseguenza, le postazioni di lavoro degli utenti non sono più considerate attendibili, ma vengono invece protette esattamente come quelle degli utenti che lavorano da casa, utilizzando le stesse policy di accesso.



In definitiva, recarsi in un ufficio e connettersi alla rete non dovrebbe fornire agli utenti un accesso alle applicazioni o alle risorse più esteso di quello di cui disporrebbero se lavorassero tramite il loro ISP di casa. La rete dovrebbe essere puramente il mezzo trasporto, senza che venga attribuito alcun privilegio presunto.

L’accesso e l’autorizzazione si basano sull’identità, sul dispositivo e sull’applicazione (non sull’indirizzo IP) a cui si accede. Un punto di applicazione delle policy, non le ACL del firewall di rete, arbitra ogni singola decisione relativa all’accesso, che viene presa sulla base della necessità d’uso, secondo quanto stabilito nelle policy di accesso, che indicano a quali applicazioni gli utenti devono accedere e da quali dispositivi.

Questo cambiamento nell’architettura richiede un cambiamento di mentalità.

1. **Estensione delle policy di accesso agli utenti locali:** le policy di accesso seguono l’utente, non la rete a cui è connesso.

2. **Passaggio dall’accesso alla rete all’accesso alle risorse:** con il modello zero trust, gli utenti accedono direttamente alle applicazioni tramite connessioni basate su policy e identità. In questo modo, non è più necessario concedere un accesso esteso alla rete stessa.

3. **La rete aziendale viene trattata come la rete Internet:** il Wi-Fi degli uffici diventa una “rete internet in stile bar” che connette gli utenti a Zero Trust Exchange, dove il controllo viene esercitato applicando le policy di sicurezza. Si eliminano così sia il traffico in entrata, che l’attendibilità implicita.

4. **Convalida continua dell’attendibilità:** lo zero trust valuta ogni richiesta di accesso in modo dinamico, monitorando il profilo di sicurezza del dispositivo, il contesto e i segnali di rischio.

Il valore aggiunto dello zero trust è la sua capacità di garantire la coerenza. I dipendenti non devono preoccuparsi se lavorano “in sede” o “da remoto”: accederanno infatti alle applicazioni nello stesso modo, indipendentemente da dove lavorano. Questa esperienza unificata non solo supporta la produttività degli utenti, ma semplifica anche l’amministrazione IT.

Visibilità migliorata

Un solido framework zero trust garantisce una produttività ottimale, eliminando al contempo i rischi posti dall’attendibilità implicita e dalle infrastrutture obsolete. La visibilità emerge come una capacità critica, al pari dell’identità, del profilo di sicurezza del dispositivo e del controllo delle applicazioni, per ottimizzare le prestazioni e risolvere rapidamente i problemi. La visibilità consente ai team IT di ottimizzare la distribuzione delle applicazioni direttamente agli utenti, nonché di ridurre i tempi di fermo e di risolvere i problemi più rapidamente, limitando le cause alla radice degli eventuali contrattempi. La visibilità integrale sul percorso dall’endpoint fino alla destinazione garantisce una risposta rapida, in quanto gli amministratori possono vedere se il problema è locale per l’utente oppure correlato al trasporto o alla destinazione cloud stessa.

Quando i dipendenti tornano a operare da uffici condivisi è bene considerare questi possibili scenari:

- **Il dilemma del Wi-Fi in ufficio:** un dipendente rientra in ufficio e connette il proprio portatile al Wi-Fi aziendale. Improvvisamente, riscontra un’elevata latenza quando utilizza Microsoft Teams, un’applicazione che funzionava perfettamente quando lavorava da casa con una semplice connessione a banda larga. È un problema di copertura del Wi-Fi? Un ritardo del DNS? Un problema con il server di Teams stesso?

- **Latenza delle soluzioni SaaS data dal backhauling aziendale:** un utente tenta di accedere a un CRM SaaS, come Salesforce, dalla propria scrivania. Il traffico cloud viene forzato attraverso la rete aziendale, introducendo latenza a causa del percorso di backhauling.

- **Lacune nella visibilità sulle forze lavoro ibride:** un'organizzazione globale ha bisogno di una visibilità costante sullo stato dei dispositivi e sulle prestazioni di SaaS e ISP, sia per i dipendenti da remoto, che per quelli in sede, il che comporta frequenti ticket di assistenza che consumano preziosi cicli dell'IT.

Un elemento chiave per implementare lo zero trust in ufficio è garantire il monitoraggio dell'esperienza digitale come parte dell'architettura zero trust complessiva.

Perché scegliere Zscaler per lo zero trust in ufficio?

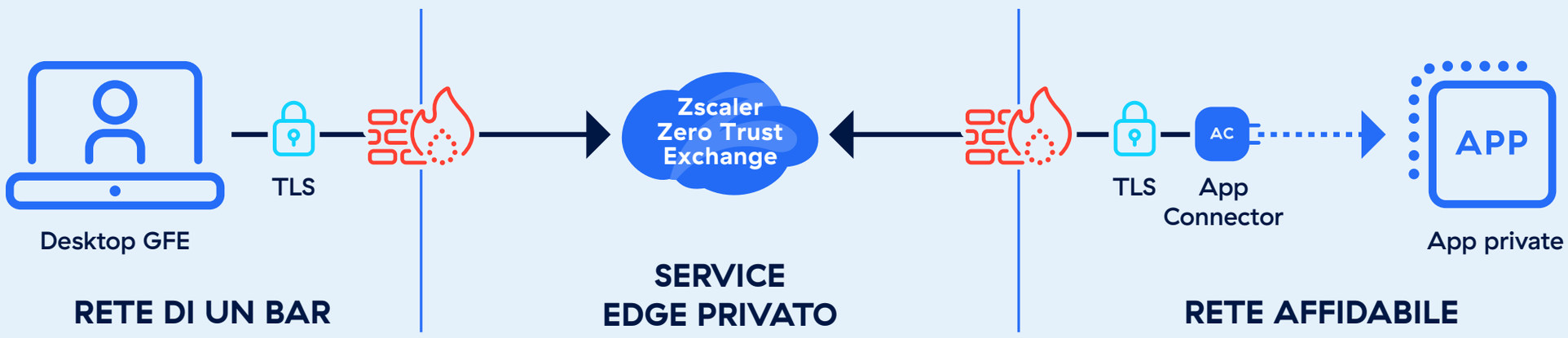
Zscaler è già da tempo partner di fiducia delle organizzazioni governative impegnate nelle iniziative di modernizzazione. In qualità di fornitore leader nel settore dei servizi di sicurezza sul cloud, Zscaler è già la scelta di 14 delle 15 agenzie governative statunitensi, tra cui DHS, DOJ e GSA, per proteggere le reti, semplificare le operazioni e garantire risparmi sui costi. Stiamo proteggendo milioni di utenti in centinaia di enti dei vari gradi della pubblica amministrazione.

Zscaler for Users comprende tre aree di funzionalità per ridurre i rischi, migliorare la produttività e ridurre i costi e la complessità.

- **Accesso sicuro a Internet e SaaS (ZIA):** il punto di accesso degli utenti a Internet e a tutte le applicazioni, che protegge dalle minacce avanzate e dalla fuga dei dati

- **Accesso sicuro alle app private (ZPA):** garantisce che gli utenti vengano connessi tramite il Private Service Edge locale, mediando la connessione dati a un'applicazione privata attraverso la rete dell'ente, senza che il traffico debba uscire su Internet per poi tornare indietro.

- **Esperienza utente digitale (ZDX):** fornisce una visibilità critica sulle esperienze digitali degli utenti, offrendo metriche dall'endpoint fino all'applicazione SaaS, garantendo l'eccellenza operativa sia dentro che fuori dagli uffici.



Modernizzare gli ambienti di lavoro con lo zero trust

Con l'evoluzione del mondo del lavoro, il concetto di "ufficio" è diventato sempre meno rilevante. Che gli utenti lavorino dagli uffici tradizionali, da casa o mentre sono in viaggio, la loro esperienza deve rimanere fluida e sicura.

Con il rientro dei dipendenti in ufficio, le aziende hanno un'opportunità unica per modernizzare l'infrastruttura del proprio ambiente di lavoro. Basandosi su un'infrastruttura zero trust, possono riuscire a potenziare non solo la sicurezza, ma anche la scalabilità, l'agilità e la resilienza a lungo termine. Questa è la visione alla base di un modello Zero Trust Office nella sua forma più evoluta e concretizzata: un ambiente in cui la produttività prospera.

Il modello Zero Trust Office è già qualcosa di realizzabile. Applicando gli stessi principi utilizzati per il telelavoro alle operazioni in ufficio, le organizzazioni possono ridurre significativamente i rischi, migliorare l'esperienza utente e creare un'architettura di sicurezza a prova di futuro.

Informazioni su Zscaler

Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange™, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Per saperne di più, visita **www.zscaler.com/it** oppure seguici su X (precedentemente Twitter) **@zscaler**.

+1 408.533.0288 **Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134** **zscaler.com/it**

zscaler™

Zero Trust Everywhere