SCHEDA TECNICA

Zscaler Private Access™

Potenzia la tua forza lavoro offrendo un accesso veloce, sicuro e affidabile alle app private con l'unica soluzione ZTNA alimentata dall'AI del settore.

Zscaler Private Access (ZPA) è una soluzione nativa del cloud che fornisce un accesso zero trust a tutti gli utenti attraverso una connettività diretta alle applicazioni private, riducendo al minimo la superficie di attacco, eliminando il movimento laterale e proteggendoti da attacchi sofisticati.

Gli approcci legacy alla sicurezza della rete non rispondono efficacemente alle esigenze della forza lavoro ibrida e del business.
I firewall e le VPN tradizionali generano una superficie di attacco enorme rilevabile e sfruttabile dagli aggressori. Inoltre, collocano gli utenti direttamente sulla rete, favorendo la propagazione laterale delle minacce, e se le credenziali di un utente vengono compromesse, gli aggressori riescono con facilità ad accedere ai dati sensibili. L'utilizzo di una VPN per supportare la forza lavoro ibrida e l'accesso di terze parti accresce il rischio informatico, genera esperienze utente scadenti e aumenta il sovraccarico amministrativo. Per fornire un accesso sicuro agli utenti da qualsiasi dispositivo e posizione, serve un approccio più efficace.

Secondo Gartner, entro il 2025, almeno il 70% delle nuove distribuzioni di accesso remoto sarà fornito prevalentemente con lo ZTNA (Zero Trust Network Access) anziché tramite servizi VPN; questa percentuale era inferiore al 10% alla fine del 2021.

Vantaggi:

- **Sostituisci le soluzioni VPN vulnerabili**
  Riduci la superficie di attacco ed elimina il movimento laterale collegando gli utenti direttamente alle applicazioni, non alla rete, e migliora così il profilo di sicurezza.
- **Previeni gli attacchi informatici**
  Riduci al minimo il rischio di subire violazioni sfruttando la protezione delle app private contro minacce web e dirette all'identità, la difesa dalle minacce avanzate con ispezione inline completa e la prevenzione della perdita dei dati.
- **Rafforza la tua forza lavoro ibrida**
  Estendi in modo fluido e rapido l'accesso alle app private a tutti gli utenti, alla sede centrale, alle filiali e alle terze parti.
- **Riduci la complessità operativa**
  Offri un accesso sicuro e ottimizzato, senza ricorrere a prodotti costosi e complessi, grazie a una piattaforma ZTNA unificata e nativa del cloud per utenti, workload e OT/IT

Gli approcci legacy alla sicurezza della rete possono essere aggirati con estrema facilità dagli aggressori, che sfruttano l'attendibilità intrinseca e l'accesso troppo permissivo delle architetture tradizionali di tipo "castle-and-moat", in particolare:

- **L'architettura legacy non è in grado di scalare o offrire un'esperienza utente rapida e fluida:** le VPN richiedono il backhauling, che introduce costi, complessità e una latenza troppo eccessiva per la forza lavoro da remoto di oggi
- **Firewall tradizionali, VPN, VDI e app private creano una superficie di attacco molto estesa:** gli aggressori sono in grado di individuare e sfruttare le risorse vulnerabili ed esposte all'esterno
- **L'accesso all'intera rete consente il movimento laterale senza limitazioni:** le VPN collocano gli utenti sulla rete, e questo offre agli aggressori un facile accesso ai dati sensibili
- **Gli utenti compromessi e le minacce interne riescono a eludere i controlli tradizionali:** gli aggressori avanzati sono in grado di rubare credenziali e sabotare le identità per accedere alle app private con strumenti di accesso remoto legacy

È giunto il momento di offrire agli utenti un modo innovativo, rapido e sicuro per connettersi alle applicazioni di cui hanno bisogno e di ridefinire la sicurezza delle applicazioni private con un approccio ZTNA.

Zscaler Private Access™ (ZPA)

Zscaler Private Access (ZPA), la prima soluzione ZTNA basata sull'AI del settore, è una soluzione nativa del cloud che fornisce un accesso zero trust a tutti gli utenti attraverso una connettività diretta alle applicazioni private. È una soluzione che riduce al minimo la superficie di attacco, nasconde le app dietro Zero Trust Exchange, elimina il movimento laterale, utilizza la segmentazione utente-app basata sull'AI e ti protegge dagli attacchi sofisticati con l'integrazione dell'ispezione del traffico e della protezione di applicazioni e dati. Si tratta di un servizio resiliente, nativo del cloud e basato su un'architettura SSE (Security Service Edge) olistica che può essere distribuito in poche ore per sostituire VPN legacy e strumenti di accesso remoto, in modo da poter:

- **Ridurre al minimo la superficie di attacco:** le applicazioni vengono rese invisibili a Internet, impedendo a utenti e dispositivi non autorizzati di individuarle. Le connessioni dall'interno verso l'esterno tra utente e app garantiscono che app e IP non vengano mai esposti
- **Implementare l'accesso con privilegi minimi:** l'accesso alle applicazioni viene determinato in base all'identità e al contesto, non attraverso un indirizzo IP. Inoltre, gli utenti non vengono mai collocati sulla rete per l'accesso.
- **Eliminare il movimento laterale:** le applicazioni vengono segmentate in modo che gli utenti possano accedere solo a un'app specifica, e questo contribuisce a limitare il movimento laterale
- **Bloccare gli attacchi informatici attraverso l'ispezione completa:** il traffico delle app private viene ispezionato inline per prevenire le tecniche di attacco web più diffuse
- **Prevenire la perdita dei dati:** la DLP integrata per le app private, la risposta avanzata agli incidenti e la classificazione dei dati consentono di proteggere le app critiche
- **Offrire un'esperienza utente di livello superiore:** connettere gli utenti direttamente alle app private consente di eliminare il backhauling lento e costoso verso le VPN legacy; inoltre, permette di monitorare costantemente e risolvere in modo proattivo i problemi dell'esperienza utente

Entro il 2025, almeno il 70% delle nuove distribuzioni di accesso remoto avverrà prevalentemente tramite servizi ZTNA, e non attraverso servizi VPN, una percentuale che era inferiore al 10% alla fine del 2021.*

— Gartner

*Gartner, Emerging Technologies: Adoption Growth Insights for Zero Trust Network Access, Nat Smith, Mark Wah, Christian Canales. 8 aprile 2022

Casi d'uso principali

Offrire un accesso remoto sicuro (sostituendo la VPN)
le VPN basate sul cloud o su dispositivi fisici espongono agli attacchi informatici, presentano vulnerabilità intrinseche e vengono sfruttate costantemente dagli aggressori. Il loro design incentrato sulla rete esegue il backhauling del traffico, espande la superficie di attacco e consente il movimento laterale, in quanto gli utenti vengono collocati direttamente sulla rete, favorendo così la diffusione degli attacchi ransomware. Le VPN, quindi, non garantiscono la sicurezza e sono lente e complesse da gestire.

ZPA risolve queste sfide offrendo un accesso zero trust a tutti gli utenti attraverso una connettività diretta alle applicazioni private. Inoltre, riduce al minimo la superficie di attacco nascondendo le app dietro Zero Trust Exchange, elimina il movimento laterale tramite la segmentazione utente–app basata sull'AI e ti protegge dagli attacchi sofisticati grazie all'ispezione del traffico e alla protezione di applicazioni e dati. ZPA fornisce un accesso rapido e diretto alle applicazioni tramite oltre 160 punti di presenza (PoP) distribuiti a livello globale, eliminando i rischi per la sicurezza posti dalle VPN. Il design nativo del cloud di ZPA consente ai team IT di eliminare i dispositivi gateway in entrata, come bilanciatori del carico, concentratori VPN e altri dispositivi di sicurezza, riducendo i costi, la complessità e le spese di gestione. ZPA garantisce l'accesso zero trust a tutte le applicazioni, comprese quelle connesse alla rete, come Voice over IP (VoIP), applicazioni server–client e persino app ospitate da partner commerciali (extranet), in cui i clienti non possono implementare gli app connector.

Un accesso sicuro alle app per gli utenti in ufficio e in modalità ibrida
Nella forza lavoro moderna, gli utenti lavorano da casa e da altre sedi in remoto, filiali e sedi centrali; questa distribuzione mette a dura prova i paradigmi di sicurezza legacy. Le organizzazioni hanno bisogno di un accesso senza interruzioni alle applicazioni senza compromettere la sicurezza zero trust durante eventi imprevisti o periodi in cui l'accesso all'infrastruttura è scadente. Inoltre, per assicurare la continuità aziendale, è necessario garantire la conformità alle normative.

ZPA Private Service Edge consente di fornire la potenza del cloud a tutte le sedi aziendali, applicando gli stessi controlli di sicurezza impiegati per gli utenti in remoto e mantenendo delle prestazioni sempre ottimali. Distribuendo Zscaler Private Service Edge con controller cloud privati, ZPA supporta il passaggio completamente automatico alla modalità Business Continuity in caso di rilevamento di un'interruzione. Le policy e l'autenticazione vengono applicate anche quando ZPA Cloud non è raggiungibile.

Dispositivi personali (BYOD) e accesso di utenti terzi
Tradizionalmente, l'accesso di terze parti si è basato su soluzioni costose, complesse e rischiose, come VDI, RDP, SSH o VNC, che collegavano gli utenti direttamente alla rete ed esponevano i sistemi interni a dispositivi non attendibili.

Le funzionalità di accesso clientless di ZPA semplificano l'accesso delle terze parti riducendo i costi e mitigando i rischi. Gli utenti terzi, come collaboratori, fornitori e partner, possono utilizzare qualsiasi browser web dai propri dispositivi per connettersi a siti web intranet, sistemi interni e apparecchiature, senza bisogno di un client. In questo modo, gli utenti terzi e i dispositivi non gestiti sono isolati dalla rete e dalle applicazioni, ed è possibile garantire che i dati sensibili siano protetti dalle azioni non autorizzate, come accessi, copia/incolla, stampa e upload/download. L'integrazione di ZPA e del browser Google Chrome Enterprise migliorerà la sicurezza per i dispositivi non gestiti/BYOD attraverso la verifica del browser appena citato e l'inclusione di ulteriori informazioni sul profilo di sicurezza nei controlli delle policy di ZPA. Grazie all'accesso clientless, l'IT è in grado di offrire agli utenti un'esperienza migliore e più sicura senza i costi di gestione della VDI legacy. Fusioni, acquisizioni e cessioni pongono sfide in termini di integrazione della rete, ma ZPA è in grado di accelerare questo processo, portandolo da mesi a poche settimane. ZPA offre un accesso fluido alle app private eliminando la necessità di far convergere le reti o di aggiungere ulteriori apparecchiature.

Accesso remoto con privilegi a OT/IT
I dipendenti e i fornitori terzi devono poter accedere regolarmente alle risorse OT e IT per massimizzare i periodi di attività della produzione ed evitare interruzioni dovute a guasti nelle apparecchiature e intoppi nei processi. ZPA consente un accesso rapido, sicuro e affidabile agli ambienti OT e IT da siti sul campo, stabilimenti produttivi o qualsiasi altro luogo. ZPA for OT/IT fornisce un accesso con desktop remoto completamente isolato e clientless ai sistemi target interni RDP, SSH e VNC, senza che gli utenti installino un client sul proprio dispositivo o utilizzino jump host e VPN legacy.

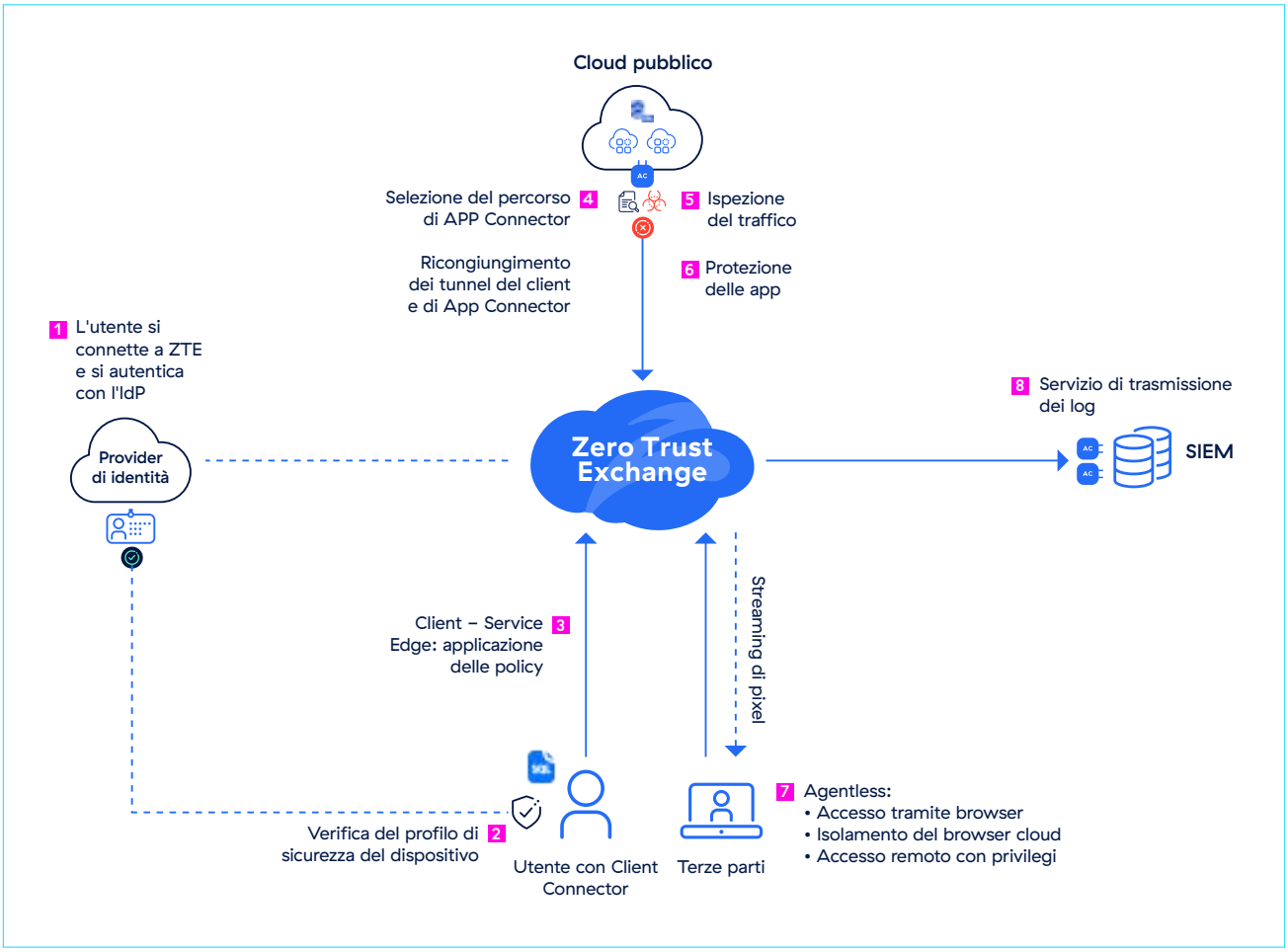
Alternativa alla VDI
I team IT e di sicurezza non hanno controllo sui dispositivi non gestiti, e questo genera rischi per l'azienda. Per supportare l'accesso alle applicazioni sui dispositivi non gestiti, le organizzazioni tradizionalmente utilizzavano la VDI. Le infrastrutture VDI collocano gli utenti direttamente sulla rete, esponendo le applicazioni interne a endpoint non gestiti; sono inoltre costose, difficili da gestire e non scalabili. La trasformazione digitale ha introdotto sempre più app basate su web o browser, e lo streaming di un intero desktop tramite VDI non fornisce un'esperienza ottimale all'utente finale.

ZPA è un'alternativa efficace alla VDI che offre un accesso sicuro, agentless e basato su browser dai dispositivi non gestiti. Gli utenti ottengono così un accesso rapido e fluido alle app private mediato dal service edge più vicino. L'architettura di ZPA fornisce un accesso diretto alle applicazioni senza dover collocare l'utente sulla rete, rendendo così l'accesso alle app private molto più sicuro. ZPA Browser Access consente agli utenti di sfruttare un browser web per l'autenticazione utente e l'accesso alle applicazioni senza dover installare Zscaler Client Connector sui propri dispositivi. ZPA integra l'isolamento del browser, che consente di trasmettere al dispositivo dell'utente finale solo i pixel anziché il contenuto effettivo, mentre i dati all'interno delle app restano al sicuro. ZPA consente agli amministratori di creare policy di isolamento per definire il modo in cui un utente può interagire all'interno dell'ambiente isolato.

Microsegmentazione
Le soluzioni di accesso remoto, come le VPN, concedono l'accesso completo alla rete ed espongono IP e applicazioni a Internet. Le VPN estendono la rete interna ai dispositivi in remoto e, per come sono state progettate, richiedono traffico in entrata, generando così una superficie di attacco esposta al pubblico, in cui, senza un'adeguata segmentazione della rete, una violazione in un segmento potrebbe compromettere l'intera rete dell'organizzazione. Inoltre, l'implementazione della segmentazione richiede regole complesse per i firewall che sono difficili da gestire, spesso bloccano l'operatività delle applicazioni e possono complicare l'accesso per gli utenti delle VPN. Nelle grandi organizzazioni, ciò richiede spesso un'elevata disponibilità, un routing complesso e costosi collegamenti privati.

La soluzione alimentata dall'AI, Zscaler App Segmentation, offre una segmentazione accurata da utente ad app e una soluzione solida per implementare facilmente policy coerenti su larga scala ed eliminare il movimento laterale delle minacce. Questa soluzione aiuta a rilevare tutte le applicazioni all'interno dell'organizzazione e fornisce informazioni visive su quali utenti hanno accesso a quali applicazioni; inoltre, genera in automatico raccomandazioni per i segmenti di app e policy basate su modelli di machine learning per un'implementazione più semplice.

Come funziona ZPA



Come funziona

Quando un utente (dipendente, fornitore, partner o collaboratore) tenta di accedere a un'applicazione interna, ZPA fornisce una connettività sicura e diretta attraverso questi passaggi:

1 L'utente si connette a Zero Trust Exchange tramite Client Connector e si autentica con il provider dell'identità (IdP). Dopo che l'autenticazione va a buon fine, si riconnette al Public Service Edge, stabilendo un'unica connessione TLS permanente.

2 Dopo l'autenticazione dell'utente e la creazione del tunnel verso il Service Edge, il Client Connector scarica la propria configurazione, che include il controllo del profilo di sicurezza del dispositivo.

3 L'app di Zscaler inoltra il traffico dell'utente al Service Edge di ZPA più vicino, che agisce da broker, e le policy di sicurezza e di accesso dell'utente vengono verificate.

4 In seguito, due tunnel in uscita, uno dal Client Connector sul dispositivo e l'altro dall'App Connector, vengono ricongiunti dal Service Edge.

5 Una volta instaurata la connessione tra il dispositivo dell'utente e l'applicazione, l'App Connector ispeziona automaticamente il traffico inline per rilevare e bloccare le potenziali minacce provenienti da utenti o dispositivi che potrebbero essere stati compromessi.

6 Zscaler AppProtection protegge le app private basate sul web e sull'identità tramite un'ispezione completa di Livello 7, migliorando così il profilo di sicurezza complessivo.

7 Gli utenti terzi possono connettersi alle applicazioni private con l'accesso integrato basato su browser o tramite Zscaler Browser Isolation per l'accesso clientless dai dispositivi non gestiti.

8 Il servizio di streaming dei log (Log Streaming Service, LSS) trasmette al sistema SIEM vari log, tra cui quelli relativi all'attività dell'utente

Un Service Edge di ZPA può essere ospitato da Zscaler sul cloud (ZPA Public Service Edge) o essere eseguito in locale all'interno dell'infrastruttura (ZPA Private Service Edge), offrendo un percorso più breve verso le app locali e supportando la pianificazione della continuità aziendale.

Funzionalità principali

Motore di policy basato sul rischio	Un potente motore di policy nativo consente di convalidare continuamente le policy di accesso in base al profilo di rischio di utenti, dispositivi, contenuti e applicazioni, per garantire che solo gli utenti autenticati possano accedere alle applicazioni private.
Accesso unificato con client e clientless	Scegli il metodo di protezione che meglio si adatta al tuo ambiente ibrido. L'accesso basato su client garantisce la protezione degli utenti gestiti, anche quando sono fuori dalla rete aziendale, grazie al leggero agente Zscaler Client Connector. L'accesso clientless offre agli utenti non gestiti un accesso rapido alle app da qualsiasi dispositivo e browser web.
Accesso tramite browser	Consenti agli utenti che usano dispositivi personali (BYOD) e alle terze parti di utilizzare liberamente i propri dispositivi per accedere alle applicazioni interne in modo rapido e sicuro sfruttando qualsiasi browser web, senza bisogno di client.
ZTNA in sede	Prova lo ZTNA per gli utenti in sede collegando in modo sicuro gli utenti alle applicazioni negli uffici aziendali. Lo Universal ZTNA garantisce agli utenti di beneficiare di accesso e policy uniformi, indipendentemente dalla loro posizione e dalle applicazioni utilizzate.
Continuità operativa e disaster recovery	Offri un accesso senza interruzioni alle applicazioni fondamentali per il business, anche durante un evento imprevisto, con una soluzione per la continuità aziendale controllata dal cliente o completamente gestita in grado di creare un percorso di accesso alle applicazioni private critiche attraverso ZPA Private Service Edge.
Rilevamento delle app	Le applicazioni vengono rilevate e catalogate automaticamente, utilizzando nomi di dominio specifici e sottoreti IP, per ottenere informazioni dettagliate sul portfolio di applicazioni private dell'azienda e sulla potenziale superficie di attacco.
Segmentazione delle app basata su AI	Applica la segmentazione basata sul machine learning, suggerita e fornita in automatico su ZPA, semplificando e accelerando l'identificazione dei segmenti di app corretti e la creazione di policy di accesso adeguate. Sfruttando modelli di machine learning in continuo aggiornamento, basati su milioni di segnali dei clienti e sui pattern di accesso specifici dell'azienda, la segmentazione basata sull'ML può aiutare a ridurre al minimo la superficie di attacco interna.
Segmentazione da utente ad app	Assicurati che tutti gli accessi alle applicazioni siano concessi in base alla necessità di utilizzo e a privilegi minimi, con una segmentazione utente–app. Fornisci agli utenti autorizzati un accesso sicuro ad applicazioni specifiche, senza collocarli mai sulla rete. Evita di ricorrere a complicate segmentazioni della rete con i firewall interni.
Protezione delle app	Proteggi le applicazioni e le infrastrutture private dagli attacchi più diffusi grazie all'ispezione di sicurezza inline e ad alte prestazioni di tutti i payload delle applicazioni per rilevare le minacce. Inoltre, identifica e blocca i rischi di sicurezza web noti, come l'OWASP Top 10 e le vulnerabilità 0–day emergenti che sono in grado di aggirare i controlli di sicurezza della rete tradizionali.

Accesso remoto con privilegi	Consenti agli amministratori e agli operatori con privilegi di connettersi in modo sicuro ai siti web sulla intranet, ai sistemi interni e alle apparecchiature senza dover ricorrere a VPN, VDI o client Desktop remoti, come RDP, SSH e VNC.
Protezione dalle minacce e protezione dei dati	Riduci il rischio di subire minacce con l'ispezione completa dei contenuti e individua e controlla i dati sensibili nelle connessioni tra utenti e app.
Identità e Single Sign-On (SSO)	Questa soluzione si integra facilmente con l'infrastruttura esistente per la verifica dell'identità e l'autenticazione, e impiega l'SSO per ridurre ulteriormente la complessità.
Accesso sicuro alle app di rete	Offri un accesso sicuro alle applicazioni di rete legacy connesse, come VoIP e app server-to-client.
Connettività IPsec	Abilita l'accesso zero trust alle applicazioni dei partner commerciali e dei fornitori (applicazioni sull'extranet) ospitate nelle loro reti

Vantaggi

Riduzione della superficie di attacco
Eliminando le VPN vulnerabili e rendendo le app invisibili a Internet, per gli utenti non autorizzati diventa impossibile individuarle e attaccarle. ZPA crea un segmento univoco tra un utente autorizzato e un'app privata specifica, rimuovendo tutta la connettività in entrata e consentendo solo connessioni dall'interno verso l'esterno tramite microtunnel cifrati che raggiungono i dispositivi degli utenti. Gli amministratori sono in grado quindi di individuare e segmentare automaticamente le applicazioni, i servizi e i workload non autorizzati utilizzando il rilevamento delle app; questo contribuisce a ridurre ulteriormente la superficie di attacco.

Eliminazione del movimento laterale
La connettività basata sull'accesso a privilegi minimi garantisce che l'accesso alle applicazioni sia concesso su base univoca (one-to-one) da un utente autorizzato a un'app specifica, anziché alla rete. In questo modo, il movimento laterale tra app o attraverso la rete risulta impossibile. Dato che ZPA non si basa sugli indirizzi IP, viene eliminata la necessità di configurare e gestire segmentazioni di rete complesse, elenchi di controllo degli accessi (ACL), policy dei firewall o traduzioni degli indirizzi di rete.

Prevenzione della compromissione degli utenti e difesa da minacce interne e aggressori avanzati
L'ispezione inline integrata e le funzionalità di DLP riducono al minimo il rischio associato alla compromissione degli utenti e alla presenza di aggressori attivi. ZPA blocca in automatico gli attacchi web offrendo una copertura completa contro le tecniche più diffuse, incluse quelle riportate nello standard OWASP Top 10, e offre un supporto completo delle firme personalizzate per l'applicazione immediata di patch virtuali contro le vulnerabilità 0-day. ZPA riduce al minimo i rischi associati a terze parti e ai dispositivi BYOD fornendo un accesso completamente isolato alle applicazioni che tiene i dati sensibili lontani dai dispositivi non gestiti grazie all'isolamento integrato nel browser sul cloud.

Esperienza ottimale per l'utente
Una connettività sempre veloce, che non richiede l'accesso e la disconnessione dai client VPN, offre agli utenti in remoto un'esperienza di accesso più sicura ed efficiente. Collaboratori, fornitori e partner terzi beneficiano di un accesso semplice da qualsiasi dispositivo e browser web, senza la necessità di installare un client. Gli utenti si registrano con le credenziali SSO esistenti (Azure AD, Okta, Ping, ecc.), mentre gli amministratori riescono a preservare la produttività rilevando e risolvendo in modo proattivo i problemi prestazionali degli utenti finali causati dalla difficoltà di accedere alle app private, dalle interruzioni nel percorso di rete o dalla congestione della rete.

Una piattaforma unificata per l'accesso sicuro ad app, workload e dispositivi
Estendi lo zero trust alle app private e ai dispositivi OT/IT per semplificare e integrare più strumenti di accesso remoto separati e unifica le policy di sicurezza e di accesso per bloccare le violazioni e ridurre la complessità operativa.

Pacchetti con Zscaler Private Access

	Piattaforma Zscaler Essentials (ZS-ESS-PLATFORM)	Piattaforma Zscaler Private Access (PIATTAFORMA ZS-ZPA)	Piattaforma Zscaler (ZS-PLATFORM)
Servizi della piattaforma Private Access	incluso 1 utente ogni 20 utenti abbonati (Min: 500 utenti abbonati)	incluso	incluso
Controllo granulare dell'accesso per utente, gruppo e porte			
Servizio di trasmissione dei log			
Monitoraggio continuo dell'integrità di tutte le app			
Ancoraggio agli IP di origine			
App Connector	$	Quanti ne servono, fino al massimo del sistema	Quanti ne servono, fino al massimo del sistema
ZPA Private Service Edge			
Accesso di terze parti	$	incluso PRA per oltre 500 utenti	incluso PRA per oltre 500 utenti
Accesso basato su browser			
Portale utenti			
Privileged Remote Access (PRA) Standard			
Monitoraggio dell'esperienza digitale	$	incluso	incluso
Standard ZDX			
Sicurezza per le app private	$	$	incluso Deception per oltre 500 utenti
Protezione dei dati per le app private			
Gestione del rischio: Deception			
Segmentazione	20 segmenti di app (10 rec/90 giorni, retrospettiva limitata)	20 segmenti di app (10 rec/90 giorni, retrospettiva limitata)	20 segmenti di app (10 rec/90 giorni, retrospettiva limitata)
Anteprima dei segmenti e della segmentazione delle app			
Componente aggiuntivo: Segmentation	incluso 100 rec/14 giorni Report settimanali su richiesta, download e analisi dei dati raccolti fino a 30 giorni Importazione delle app dal sistema interno o da fonti di terze parti (Qualys, Tenable, ServiceNow)	incluso 100 rec/14 giorni Report settimanali su richiesta, download e analisi dei dati raccolti fino a 30 giorni Importazione delle app dal sistema interno o da fonti di terze parti (Qualys, Tenable, ServiceNow)	incluso 100 rec/14 giorni Report settimanali su richiesta, download e analisi dei dati raccolti fino a 30 giorni Importazione delle app dal sistema interno o da fonti di terze parti (Qualys, Tenable, ServiceNow)
Segmenti di app illimitati			
Segmentazione basata su AI			
Informazioni utili per la segmentazione			
Importazione dei segmenti delle app (da file di dati strutturati)			
Componente aggiuntivo: AppProtection	Elemento aggiuntivo	Elemento aggiuntivo	Elemento aggiuntivo
Visibilità sugli attacchi alle applicazioni			
Difesa OWASP Top 10: iniezione SQL, cross-site scripting, scanner ambientali e delle porte			
Protezione dalle minacce 0-day			
Monitoraggio degli utenti ad alto rischio			

Differenze principali

ZPA è la prima soluzione ZTNA basata sull'AI del settore e offre una sicurezza di livello superiore con un'esperienza utente ineguagliabile:

- **Concepita per applicare l'accesso a privilegi minimi:** consente agli utenti autorizzati di connettersi solo alle risorse approvate, e non alla rete; un'operazione impossibile con le VPN legacy
- **Le app diventano invisibili e inaccessibili agli aggressori:** blocca la compromissione delle app, il furto dei dati e il movimento laterale, rendendo le app, i workload e i dispositivi privati invisibili alla rete Internet pubblica
- **Ispezione inline completa:** proteggi le applicazioni identificando e bloccando lo sfruttamento delle app private, prevenendo in automatico gli attacchi web più diffusi e proteggendo al tempo stesso i tuoi dati con una DLP avanzata
- **Assicura la continuità aziendale globale senza compromettere la sicurezza:** riduci al minimo l'impatto delle interruzioni e applica l'accesso zero trust per mantenere la conformità a rigorosi requisiti di conformità, anche quando il cloud Zscaler non è raggiungibile
- **Accesso clientless:** sfrutta l'accesso basato su browser per gli utenti terzi con DLP integrata
- **Elimina il movimento laterale con la segmentazione basata sull'AI:** fornisci una segmentazione accurata da utente ad app, visualizza l'accesso e ottimizza le policy utilizzando il machine learning per ridurre al minimo le superfici di attacco e prevenire le minacce laterali
- **Edge diffusi a livello globale:** grazie a oltre 160 edge cloud distribuiti in tutto il mondo, puoi ottenere un livello di sicurezza e un'esperienza utente senza eguali. Inoltre, un service edge locale facoltativo estende lo zero trust anche alla tua sede centrale
- **Fondamenta native del cloud:** sfrutta la scalabilità di una piattaforma fornita sul cloud che si adatta alla crescita della tua azienda, senza la necessità di costosi dispositivi on-premise o infrastrutture complesse
- **Piattaforma ZTNA unificata per utenti, workload e dispositivi:** consenti connessioni sicure ad app private, servizi e dispositivi OT grazie alla piattaforma ZTNA più completa del settore
- **Parte di una piattaforma zero trust espandibile:** proteggi e potenzia la tua azienda con Zero Trust Exchange, una soluzione basata su un framework SSE completo

Gartner

Zscaler è una leader del Gartner® Magic Quadrant™ per il Security Service Edge**

Scopri di più

**Gartner, Magic Quadrant for Security Service Edge, Charlie Winckless, Thomas Lintemuth, Dale Koeppen, 15 aprile 2024

Gartner non sponsorizza alcun fornitore, prodotto o servizio descritto nelle sue pubblicazioni di ricerca e non consiglia agli utenti di tecnologia di scegliere solo i fornitori con la valutazione più alta o con altra designazione. Le pubblicazioni di ricerca di Gartner sono frutto delle opinioni dell'organizzazione di ricerca di Gartner e non devono essere considerate come dichiarazioni di fatto. Gartner declina tutte le garanzie, espresse o implicite, relative alla presente ricerca, inclusa qualsiasi garanzia di commerciabilità o idoneità per uno scopo particolare.

GARTNER è un marchio commerciale e un marchio di servizio registrato di Gartner, Inc. e/o delle sue affiliate negli Stati Uniti e a livello internazionale. MAGIC QUADRANT è un marchio commerciale registrato di Gartner, Inc. e/o delle sue affiliate. Entrambi vengono utilizzati in questa sede con relativa autorizzazione. Tutti i diritti riservati.

Componenti fondamentali

Zscaler Client Connector
Client Connector è un'applicazione leggera che viene eseguita sui laptop e sui dispositivi mobili degli utenti. Inoltrando automaticamente il traffico degli utenti allo Zscaler Service Edge più vicino, si può essere certi che le policy di sicurezza e di accesso saranno applicate a tutti i dispositivi, le sedi e le applicazioni.

Zscaler Clientless Access
Gli utenti possono connettersi in modo sicuro ad app, workload e dispositivi OT tramite l'accesso integrato basato su browser (web, RDP, SSH, VNC) o Zscaler Browser Isolation per l'accesso clientless da dispositivi non gestiti.

App Connector di ZPA
Gli App Connector sono dispositivi virtuali leggeri che si collocano di fronte alle app private distribuite nel data center o nel cloud pubblico e agiscono da broker per garantire la connettività sicura tra un utente autorizzato e un'app specifica, instaurando una connessione dall'interno verso l'esterno che non espone le app a Internet.

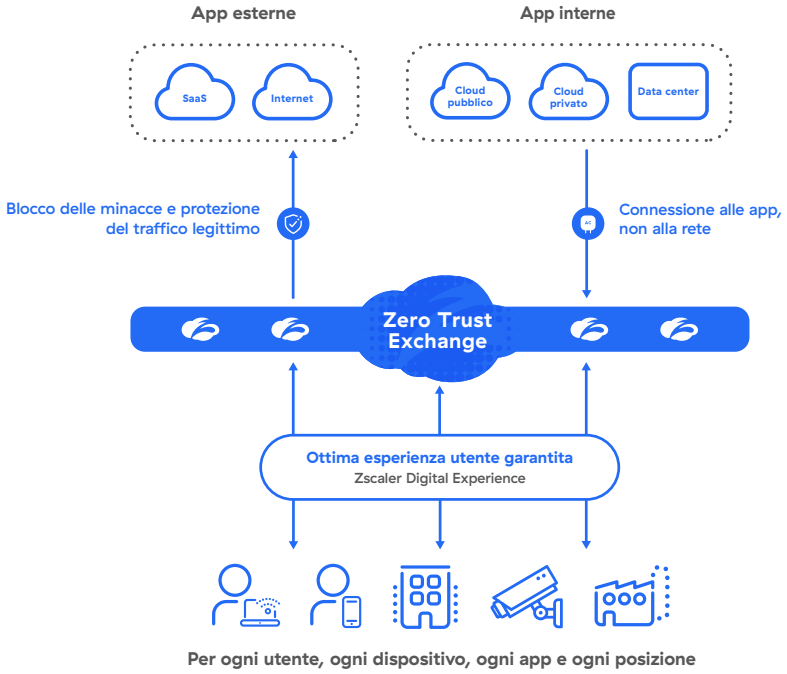
ZPA Service Edge
I Service Edge applicano le policy di sicurezza e di accesso ricongiungendo la connessione inside-out, dall'interno verso l'esterno, tra un utente autorizzato (tramite Client Connector e Browser Access) e un'applicazione privata specifica (tramite App Connector). La maggior parte dei clienti utilizza i nostri Public Service Edge, che sono ospitati in più di 160 PoP (Point of Presence, o punti di presenza) in tutto il mondo e gestiscono milioni di utenti contemporaneamente per le più grandi organizzazioni del mondo. I Private Service Edge, gestiti da Zscaler, possono anche essere ospitati on-premise, per fornire agli utenti in sede il percorso più breve verso le applicazioni on-premise senza lasciare la rete locale. Questo consente di supportare la continuità aziendale offrendo un accesso senza interruzioni alle app fondamentali per il business anche quando si verificano eventi imprevisti.

ZPA fa parte della soluzione olistica Zero Trust Exchange

Zscaler Zero Trust Exchange è una piattaforma nativa del cloud che alimenta un'architettura SSE (Security Service Edge) completa, per connettere utenti, workload e dispositivi senza collocarli sulla rete aziendale. È in grado di ridurre la complessità e i rischi associati alle soluzioni di sicurezza basate sul perimetro, che estendono la rete, ampliano la superficie di attacco, incrementano il rischio associato al movimento laterale delle minacce e non sono in grado di prevenire la perdita dei dati.

Come Zscaler fornisce lo zero trust a utenti, workload e OT/IoT

Distribuzione in poche settimane per migliorare la protezione informatica e l'esperienza utente



Specifiche tecniche

Componente di Zscaler	Piattaforme e sistemi supportati	
Client Connector	iOS 9 o successivi	macOSX 10.10 o successivi
	Android 5 o successivi	CentOS 8
	Windows 7 o successivi	Ubuntu 20.04
Accesso clientless	Browser web moderni:	Chrome
	(compatibile con HTML 5)	Edge
		Firefox
App Connector	AWS	Microsoft Hyper-V
	CentOs, Oracle e Red Hat	VMware vCenter o vSphere Hypervisor
	Microsoft Azure	Host Docker

zscaler™ | Experience your world, secured.™

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 dei dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.com/it** o seguici su X (precedentemente Twitter) sull'account **@zscaler**.

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