Scheda tecnica

Zscaler Private Access™

Potenzia la tua forza lavoro offrendo un accesso veloce, sicuro e affidabile alle applicazioni private con l'unica soluzione ZTNA di nuova generazione del settore.

Zscaler ridefinisce l'accesso privato alle applicazioni fornendo funzionalità avanzate di connettività, segmentazione e sicurezza, per proteggere l'azienda dalle minacce e offrire al contempo un'esperienza utente ottimale.

Gli approcci tradizionali alla rete e alla sicurezza non soddisfano le esigenze della forza lavoro flessibile di oggi.
Connettere gli utenti alle app private non dovrebbe essere lento, complicato o rischioso. Il lavoro ibrido e la trasformazione del cloud hanno stravolto i modelli di sicurezza della rete basati sul perimetro, con lo spostamento delle applicazioni private sul cloud e l'accesso degli utenti alle applicazioni tramite la rete Internet pubblica, su qualsiasi dispositivo e da qualsiasi luogo. Gli approcci tradizionali, che si basano su VPN e firewall legacy per controllare l'accesso alle applicazioni, sono diventati inefficaci nel mondo cloud–first e mobile.

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

Vantaggi:

- **Aumenta la produttività della forza lavoro ibrida** Ottieni un accesso rapido e semplice alle app private, da casa, in ufficio o altrove
- **Mitiga il rischio di subire violazioni dei dati** Riduci al minimo la superficie di attacco ed elimina il movimento laterale, rendendo le applicazioni invisibili a Internet e applicando il principio dell'accesso a privilegi minimi
- **Blocca gli aggressori più avanzati** Una protezione unica nel suo genere delle app private e l'ispezione completa del traffico inline riducono al minimo il rischio associato agli utenti compromessi e agli aggressori attivi
- **Estendi lo zero trust ad app, workload e dispositivi** La piattaforma ZTNA più completa al mondo, che offre un accesso a privilegi minimi ad app private, workload e dispositivi OT/IIoT
- **Riduci la complessità operativa** La nostra piattaforma nativa del cloud elimina le soluzioni di accesso remoto legacy, come le VPN, che sono difficili da scalare, gestire e configurare

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 che risulta 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 possono aggirare i controlli tradizionali:** sfruttando gli strumenti di accesso remoto legacy e le soluzioni ZTNA di prima generazione, gli aggressori avanzati possono rubare le credenziali e compromettere le identità per accedere alle applicazioni private

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 di nuova generazione.

Zscaler Private Access™ (ZPA)

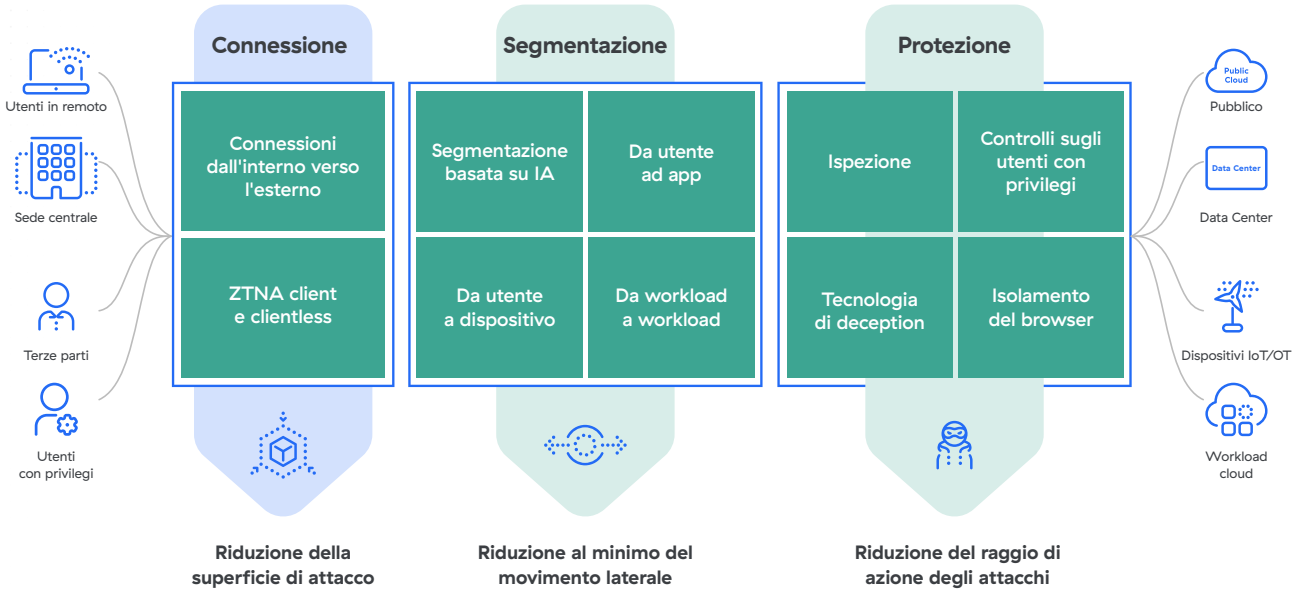
ZPA è la piattaforma ZTNA più distribuita al mondo, che applica il principio dell'accesso a privilegi minimi per offrire agli utenti una connettività sicura e diretta alle applicazioni private on-premise o su cloud pubblico, eliminando al contempo l'accesso non autorizzato e il movimento laterale. Si tratta di un servizio nativo del cloud e basato su un'architettura SSE (Security Service Edge) olistica, che può essere distribuito in poche ore per sostituire le VPN legacy e gli strumenti di accesso remoto, in modo da poter:

- **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
- **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
- **Applicare il principio dell'accesso a privilegi minimi:** l'accesso alle applicazioni viene determinato in base all'identità e al contesto, non a un indirizzo IP, e gli utenti che richiedono l'accesso non vengono mai collocati sulla rete
- **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
- **Rilevare utenti e dispositivi compromessi:** le esche integrate consentono di identificare e rimuovere rapidamente utenti e dispositivi dannosi

Entro il 2025, almeno il 70% delle nuove distribuzioni di accesso remoto sarà fornito con un approccio principalmente ZTNA (Zero Trust Network Access).

— Gartner

Ecco come ZPA affronta i casi d'uso emergenti per lo ZTNA



Casi d'uso principali

Alternative alle VPN Le VPN non sono state progettate pensando alla sicurezza, alla scalabilità o all'esperienza utente. Tradizionalmente, le VPN funzionano trasferendo tutto il traffico degli utenti in remoto verso data center a migliaia di chilometri di distanza, generando latenza, e frustrazione negli utenti. Una volta connesse, le VPN instradano gli utenti sui tunnel attraverso un firewall e li collocano sulla stessa rete delle applicazioni, consentendo il movimento laterale senza ostacoli.

ZPA elimina tutti questi pericoli fornendo un accesso rapido e diretto alle applicazioni tramite oltre 150 punti di presenza (PoP) distribuiti a livello globale, senza i rischi per la sicurezza posti dalle VPN. La connettività dall'interno verso l'esterno garantisce che l'accesso alle app sia separato dall'accesso alla rete, eliminando al contempo la superficie che si interfaccia con Internet. ZPA connette gli utenti alle applicazioni, non alle reti, e gli utenti possono accedere solo ad app specifiche, senza la possibilità di muoversi lateralmente. 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.

Una forza lavoro ibrida più sicura
I lavoratori moderni operano dalle proprie case e da altre sedi in remoto, filiali e sedi centrali, mettendo a dura prova i paradigmi della sicurezza legacy. ZPA consente un accesso semplice e sicuro alle app private da qualsiasi luogo di lavoro e su qualsiasi dispositivo. Inoltre, gli utenti del campus beneficiano di un'esperienza identica grazie a ZPA Private Service Edge.

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 prestazioni sempre ottimali. ZPA è ora in grado di fornire funzionalità Universal ZTNA per un'esperienza utente rapida

e coerente. Inoltre, il monitoraggio dell'esperienza digitale consente di ottenere una visibilità in tempo reale sulla riduzione delle prestazioni e sulle interruzioni, favorendo così la produttività del lavoro ibrido. In quanto parte di Zscaler Zero Trust Exchange™, gli utenti beneficiano di una piattaforma SSE integrata che offre un accesso sicuro, veloce e diretto a Internet, SaaS, workload, dispositivi e app private.

Alternative per l'accesso di terzi/VDI
In passato, l'accesso di terzi si basava su un'infrastruttura desktop virtuale (VDI) complessa e costosa o su altri client Desktop remoti, come RDP, SSH o VNC, che collegavano gli utenti direttamente alla rete ed esponevano i sistemi interni a dispositivi non affidabili. La funzionalità Clientless Access di ZPA rende l'accesso di terzi semplice quanto l'accesso al web, riducendo al tempo stesso i costi e mitigando i rischi. I fornitori, i collaboratori e i partner possono utilizzare liberamente qualsiasi browser web dai propri dispositivi per connettersi a siti web sulla intranet, sistemi interni e apparecchiature, senza il bisogno di client. Gli utenti terzi e i dispositivi non gestiti rimangono isolati dalla rete e dalle applicazioni; questo garantisce che i dati sensibili siano sempre sotto controllo e protetti da attività non autorizzate di copia e incolla, stampa e upload/download. Con Clientless Access, l'IT è in grado di offrire agli utenti un'esperienza migliore e più sicura, senza i costi di gestione della VDI legacy.

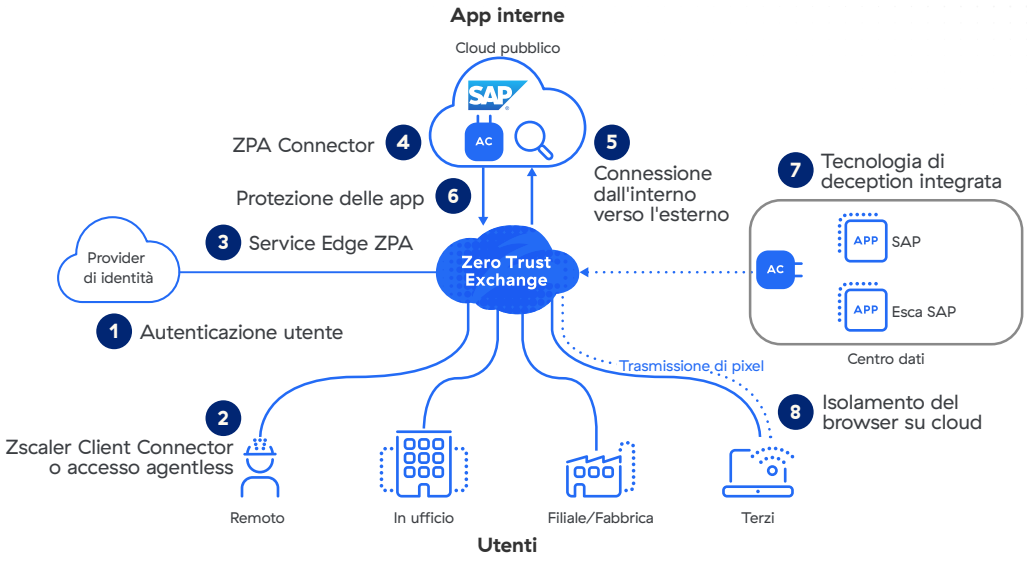
Fusioni, acquisizioni e cessioni
Le attività di fusione, cessione e acquisizione spesso richiedono la congiunzione di reti diverse, che può risultare complicata a causa della sovrapposizione dello spazio IP e della creazione di firewall tra le due entità. ZPA accelera notevolmente l'integrazione e il Time to Value e dopo le operazioni di fusione, acquisizione e cessione riducendo la durata del processo da mesi a poche settimane. Fornisce inoltre un accesso continuo alle app private senza la necessità di una VPN ed elimina la necessità di far convergere più reti o acquistare apparecchiature di rete aggiuntive, consentendo quindi alle risorse di concentrarsi su attività di più alto impatto.

Accesso sicuro degli operatori a OT e IIoT
I dipendenti e i fornitori terzi devono poter accedere regolarmente alle risorse OT e IIoT per massimizzare i periodi di attività della produzione ed evitare interruzioni dovute a guasti nelle apparecchiature e interruzione dei processi. ZPA consente un accesso rapido, sicuro e affidabile agli ambienti OT e IIoT da posizioni sul campo, stabilimenti produttivi o altri luoghi. ZPA for IoT & OT fornisce un accesso da Desktop remoto completamente isolato e senza client ai sistemi target interni RDP, SSH e VNC, senza richiedere agli utenti di installare un client sul proprio dispositivo e di utilizzare jump host e VPN legacy.

Connettività sicura tra workload
Le organizzazioni moderne richiedono una connettività tra workload veloce e sicura, in ambienti privati, ibridi e multicloud. ZPA for Workloads riduce la complessità operativa e i costi, implementando allo stesso tempo una connettività zero trust in tutti questi ambienti. Dato che i workload sono nascosti dietro a ZPA, risultano invisibili su Internet e quindi impossibili da attaccare.

Zero Trust Branch Connectivity
Zero Trust Branch Connectivity collega in modo sicuro filiali, stabilimenti produttivi e data center senza la complessità delle VPN, garantendo un accesso zero trust tra utenti, dispositivi IoT/OT e applicazioni in base alle policy aziendali. Elimina inoltre la superficie di attacco e impedisce il movimento laterale delle minacce, collegando utenti e dispositivi IoT/OT alle applicazioni tramite Zero Trust Exchange. Zero Trust Branch Connectivity semplifica notevolmente le comunicazioni tra le filiali eliminando routing complessi, VPN e firewall, consentendo al tempo stesso un inoltro flessibile e una gestione semplice delle policy grazie al solido framework di policy di ZIA e ZPA.

ZPA estende l'accesso a privilegi minimi a tutta l'azienda



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 autentica con l'IdP utilizzando le credenziali SAML SSO esistenti.
2. Il profilo di sicurezza del dispositivo dell'utente è verificato con Zscaler Client Connector, un agente di inoltro leggero che viene installato sul laptop o sul dispositivo mobile dell'utente. ZPA è inoltre in grado di acquisire il profilo di sicurezza del dispositivo tramite l'integrazione con tutti i principali fornitori di EPP/EDR/XDR (ad es. CrowdStrike, Microsoft Defender e SentinelOne).
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. Il Service Edge di ZPA determina quindi qual è l'applicazione più vicina all'utente e instaura una connessione sicura a un App Connector di ZPA, una macchina virtuale leggera installata nell'ambiente che ospita il server e le applicazioni.
5. In seguito, due tunnel in uscita, uno dal Client Connector sul dispositivo e l'altro dall'App Connector, vengono riuniti dal Service Edge di ZPA.
6. Una volta instaurata la connessione tra il dispositivo dell'utente e l'applicazione, App Connector ispeziona automaticamente il traffico inline, per rilevare e bloccare le potenziali minacce provenienti da utenti o dispositivi che potrebbero essere stati compromessi.
7. La soluzione integrata Zscaler Deception rileva gli utenti compromessi che accedono alle app esca ed è in grado di interrompere l'accesso alle risorse interne su Zscaler Zero Trust Exchange.
8. Inoltre, gli utenti terzi possono connettersi alle applicazioni private con l'accesso integrato basato su browser o tramite Cloud Browser Isolation per l'accesso clientless dai dispositivi non gestiti.

Un Service Edge ZPA può essere ospitato da Zscaler nel cloud (ZPA Public Service Edge) o può essere eseguito on-premise sull'infrastruttura del cliente (ZPA Private Service Edge). In entrambi i casi, i service edge sono gestiti da Zscaler senza la necessità di altri dispositivi.

Funzionalità principali

Motore di policy basato sul rischio	Un potente motore delle 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.
Disaster Recovery	Offri un accesso senza interruzioni alle applicazioni fondamentali per il business, anche durante un evento imprevisto, con una soluzione per la continuità operativa controllata dal cliente e 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 IA	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.
Segmentazione da utente a dispositivo	Assicurati che tutti gli accessi alle apparecchiature e ai sistemi OT/IIoT siano concessi con privilegi minimi, sfruttando una segmentazione da utente a dispositivo, e consenti a fornitori terzi e utenti in remoto di connettersi alle apparecchiature da qualsiasi luogo grazie a ZPA for IoT & OT.
Segmentazione da workload a workload	Proteggi la connettività e le comunicazioni tra workload in ambienti ibridi e multicloud con ZPA for Workloads.
Protezione delle app	Proteggi le applicazioni e le infrastrutture private dagli attacchi più diffusi grazie all'ispezione di sicurezza inline e avanzata di tutti i payload delle applicazioni al fine di 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.
Tecnologia di deception integrata	Gli aggressori più sofisticati e le minacce interne vengono bloccati con la tecnologia nativa di deception, che prevede il contenimento automatico degli utenti compromessi in Zero Trust Exchange.
Cloud Browser Isolation integrato	Fornisci un accesso sicuro e clientless alle applicazioni web critiche ai collaboratori e ai dipendenti che utilizzano dispositivi personali (BYOD). Assicurati che gli endpoint non gestiti che presentano vulnerabilità o infezioni da malware non compromettano la tua rete o le tue applicazioni. Applica controlli sull'esfiltrazione dei dati (copia/incolla, stampa, upload/download) per prevenire la perdita dei dati sensibili.
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.
SD–WAN zero trust	Connetti in modo sicuro le filiali, gli stabilimenti produttivi e i data center senza la complessità delle VPN, e garantisci un accesso zero trust a utenti, dispositivi IoT/OT e applicazioni basato sulle policy aziendali.

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.

Riduzione al minimo del movimento laterale
Anziché offrire un accesso integrale alla rete, la connettività basata sull'accesso a privilegi minimi garantisce che l'accesso alle applicazioni venga concesso su base individuale, da un utente autorizzato a un'applicazione specifica. In questo modo, il movimento laterale tra le app o attraverso la rete è impossibile. Dato che ZPA non si basa sugli indirizzi IP, non vi è più la necessità di impostare e gestire complesse segmentazioni della rete, liste di controllo degli accessi (ACL), policy dei firewall o traduzioni di indirizzi di rete. Le funzionalità di deception integrate di ZPA consentono ai team di sicurezza di rilevare e isolare immediatamente un utente malintenzionato o un dispositivo compromesso che tenta di muoversi lateralmente all'interno dell'organizzazione.

Prevenzione contro utenti compromessi, minacce interne e aggressori avanzati
Una protezione unica nel suo genere delle app private, con funzionalità integrate di ispezione inline, deception e prevenzione della perdita di dati, riduce al minimo il rischio associato agli utenti compromessi e agli aggressori attivi. ZPA blocca in automatico gli attacchi web con una copertura completa delle tecniche più diffuse, come l'OWASP Top 10, e fornisce un supporto integrale delle firme personalizzate per l'applicazione istantanea di patch virtuali contro le vulnerabilità 0-day. ZPA riduce al minimo i rischi associati agli utenti terzi e ai dispositivi personali (BYOD), fornendo un accesso completamente isolato alle applicazioni, che mantiene i dati sensibili lontani dai dispositivi non gestiti attraverso l'isolamento integrato del browser cloud. La tecnologia di deception integrata, che sfrutta le app esca, consente ai team di sicurezza di contenere le minacce attive presenti sulla rete, impedendo agli utenti compromessi di accedere alle risorse.

Offri un'esperienza utente eccezionale
Una connettività veloce e costante 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.); inoltre, 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 a tutte le app, i workload e i dispositivi OT
Lo zero trust viene esteso alle app private, ai workload e ai dispositivi OT/IIoT. In questo modo, è possibile bloccare le violazioni e ridurre la complessità operativa attraverso la semplificazione e l'integrazione di più strumenti di accesso remoto separati e l'unificazione delle policy di accesso e sicurezza.

Versioni di Zscaler Private Access

	ZPA Essentials Edition	ZPA Business Edition	ZPA Transformation Edition	ZPA Unlimited Edition
Servizi della piattaforma	Ancoraggio dell'IP di origine, IdP multiplo, LSS	(+) Accesso esteso al DC	(+) Ambiente di prova, PKI del cliente	(+) Ambiente di prova, PKI del cliente
Segmentazione da utente ad app	10 segmenti di app	500 segmenti di app	Segmenti di app illimitati	Segmenti di app illimitati
App Connector	20 coppie	50 coppie	Coppie illimitate	Coppie illimitate
ZTNA in sede[1]	1 coppia (virtuale)	1 coppia di Private Service Edge per 5000 utenti	1 coppia di Private Service Edge per 2000 utenti	1ª coppia di Private Service Edge inclusa, coppia aggiuntiva ogni 1000 utenti
Accesso clientless[2]	—	✓	✓	✓
Monitoraggio integrato dell'esperienza digitale	—	Standard	Standard	Standard
Tecnologia di deception integrata	—	Standard	Avanzata	Advanced Plus
Protezione delle app	—	—	✓	✓
Isolamento integrato	—	—	Standard	Advanced Plus
Protezione dei dati (app private)	—	—	—	✓
Supporto premium	—	—	—	✓

Differenze principali

Zscaler Private Access è l'unica piattaforma ZTNA di nuova generazione del settore che offre una sicurezza di livello superiore e un'esperienza utente senza eguali:

- **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 di 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
- **Tecnologia di deception integrata:** blocca i tentativi di spostamento laterale e la diffusione dei ransomware con l'unica soluzione ZTNA con funzionalità di deception native
- **Accesso clientless:** sfrutta l'accesso basato su browser per gli utenti terzi con DLP integrata
- **Produttività migliorata:** mantieni una visibilità completa sull'accesso alle app private e rileva i problemi degli utenti che influiscono sull'esperienza utente
- **Edge diffusi a livello globale:** grazie a oltre 150 edge cloud distribuiti in tutto il mondo, puoi ottenere un livello di sicurezza e un'esperienza utente senza pari. Inoltre, un service edge locale opzionale estende lo zero trust anche alla tua sede centrale

[1]ZPA Business Edition supporta fino a 5 coppie di Private Service Edge; è necessario acquistare coppie aggiuntive dopo 50.000 utenti. ZPA Transformation Edition supporta fino a 10 coppie di Private Service Edge; è necessario acquistare coppie aggiuntive dopo 50.000 utenti. ZPA Unlimited Edition supporta fino a 50 coppie di Private Service Edge; è necessario acquistare coppie aggiuntive dopo 50.000 utenti.

[2]L'accesso clientless comprende l'accesso via browser e l'accesso remoto con privilegi (per un massimo di 10 sistemi).

- **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 di infrastrutture complesse
- **Piattaforma ZTNA unificata per utenti, workload e dispositivi:** connessione sicura 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

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 Branch Connector Branch Connector, disponibile sotto forma di apparecchiatura fisica e virtuale, migliora le prestazioni delle applicazioni eliminando il backhauling e inoltrando tutto il traffico delle filiali e dei data center direttamente all'edge di Zscaler più vicino, riducendo così la latenza al minimo. Questo strumento consente la comunicazione bidirezionale tra utenti, server e dispositivi IoT/OT (quando non è possibile installare Client Connector) e applicazioni su qualsiasi rete tramite Zero Trust Exchange.

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.

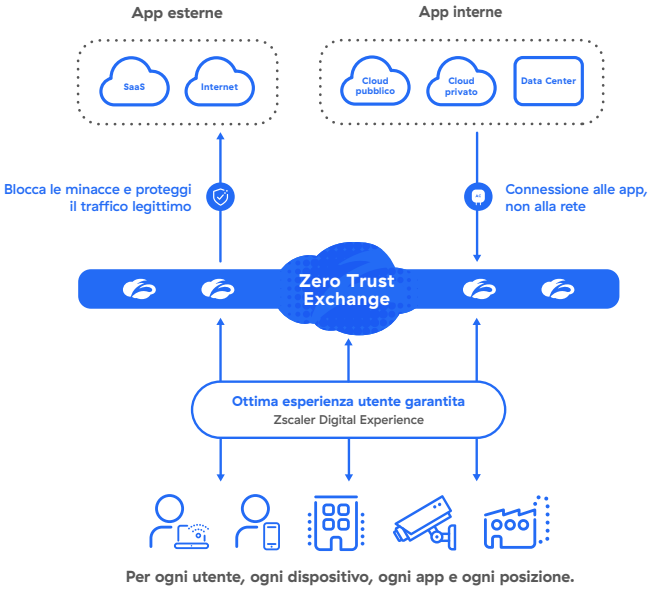
ZPA Service Edge
I Service Edge applicano policy di sicurezza e di accesso mentre congiungono la connessione dall'interno verso l'esterno tra un utente autorizzato (tramite Client Connector e Browser Access) e un'applicazione privata specifica (tramite App Connector). La maggior parte dei clienti utilizza i nostri Public Service Edge, che sono ospitati in più di 150 exchange 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 che si trovano in sede, senza lasciare la rete locale.

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.

Ecco come Zscaler fornisce una sicurezza zero trust a utenti, workload e IIoT/OT

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



Per ogni utente, ogni dispositivo, ogni app e ogni posizione.

Specifiche tecniche

Componente di Zscaler	Piattaforme e sistemi supportati	
Client Connector	iOS 9 e versioni successive Android 5 e versioni successive Windows 7 o successivi	macOSX 10.10 o successivi CentOS 8 Ubuntu 20.04
Branch Connector	CentOs, Red Hat	VMware vCenter o vSphere Hypervisor
Accesso clientless	Browser web moderni: (compatibile con HTML 5)	Chrome Edge FireFox
App Connector	AWS CentOs, Oracle e Red Hat Microsoft Azure	Microsoft Hyper-V VMware vCenter o vSphere Hypervisor 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 su SSE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.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.it