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 tradizionali alla sicurezza delle rete non rispondono alle esigenze della tua forza lavoro ibrida e della tua azienda.
I firewall e le VPN tradizionali generano una superficie di attacco molto estesa, che può essere individuata e sfruttata dagli aggressori. Inoltre, collocano gli utenti direttamente sulla rete, favorendo la propagazione laterale delle minacce. Inoltre, se le credenziali degli utenti vengono compromesse, gli aggressori possono accedere con facilità ai dati sensibili. L'utilizzo di una VPN per supportare la forza lavoro ibrida e l'accesso delle terze parti intensifica il rischio informatico, crea esperienze utente scadenti e accresce il sovraccarico amministrativo. Per fornire un accesso sicuro agli utenti, indipendentemente dal dispositivo usato e dal luogo in cui si trovano, è necessario un approccio più efficace.

Secondo il Report del 2025 di Zscaler ThreatLabz sui rischi delle VPN, il 92% degli intervistati teme che le falle delle VPN che non vengono corrette possano causare direttamente incidenti ransomware, evidenziando quanto sia difficile applicare patch alle VPN in modo continuo e tempestivo.

Vantaggi:

- **Sostituire le soluzioni VPN vulnerabili**
  Riduci la superficie di attacco ed elimina il movimento laterale, collegando gli utenti direttamente alle applicazioni, non alla rete, migliorando così il profilo di sicurezza.
- **Prevenire gli attacchi informatici**
  Mitiga il rischio di incorrere in violazioni adottando la protezione delle app private dalle minacce web e dirette alle identità, la protezione dalle minacce avanzate tramite l'ispezione inline completa e la prevenzione della perdita dei dati.
- **Potenziare la forza lavoro ibrida**
  Estendi l'accesso fluido e rapido alle app private, coprendo utenti, sede centrale, filiali e terze parti.
- **Ridurre la complessità operativa**
  Offri un accesso sicuro e ottimizzato, senza ricorrere a prodotti dedicati costosi e complessi, grazie a una piattaforma ZTNA unificata e nativa del cloud per utenti, workload e IoT/OT.

©2025 Zscaler, Inc. Tutti i diritti riservati.

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 di connettersi alle applicazioni di cui hanno bisogno e di ridefinire la sicurezza delle applicazioni private con una soluzione ZTNA (Zero Trust Network Access).

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

Il 92% degli intervistati teme che le falle delle VPN che non vengono corrette possano causare direttamente incidenti ransomware, evidenziando quanto sia difficile applicare patch alle VPN in modo continuo e tempestivo

— Report del 2025 di Zscaler ThreatLabz sui rischi delle VPN

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

©2025 Zscaler, Inc. Tutti i diritti riservati.

Casi d’uso principali

Accesso remoto sicuro (sostituzione della VPN)
Le VPN con base cloud o basate su dispositivi fisici espongono agli attacchi informatici, perché sono afflitte da vulnerabilità e vengono prese continuamente di mira dagli aggressori. Il loro design incentrato sulla rete prevede il backhauling del traffico, espande la superficie di attacco e favorisce il movimento laterale, perché colloca gli utenti direttamente sulla rete, comportando potenziali attacchi ransomware. Le VPN non sono sicure, 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 a Zero Trust Exchange, elimina il movimento laterale tramite la segmentazione utente–app basata sull’IA e 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 le app ospitate da partner commerciali (extranet), senza la necessità di implementare infrastrutture aggiuntive come i connettori delle app.

Accesso sicuro alle app per gli utenti in ufficio e da remoto
La forza lavoro di oggi vede gli utenti lavorare sia da casa che da altre postazioni da remoto, filiali e sedi centrali, mettendo alla prova i paradigmi della sicurezza tradizionale. Le organizzazioni necessitano di un accesso ininterrotto alle applicazioni, senza compromettere la sicurezza zero trust anche quando si verificano eventi dirompenti o disagi nell’accesso all’infrastruttura. Devono inoltre rispettare gli standard di conformità e normativi per garantire la continuità operativa.

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.

Accesso di dispositivi personali e utenti terzi
L’accesso tradizionale degli utenti terzi si basava 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 dei dispositivi non gestiti/BYOD attraverso la verifica di tale browser 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 per OT/IT
I dipendenti e i fornitori terzi devono poter accedere regolarmente alle risorse OT/IT per massimizzare l’uptime della produzione ed evitare interruzioni dovute

©2025 Zscaler, Inc. Tutti i diritti riservati.

a guasti delle apparecchiature e problemi nei processi. ZPA consente un accesso rapido, sicuro e affidabile agli ambienti OT/IT da postazioni sul campo, impianti produttivi o da qualsiasi altro luogo. ZPA for OT/IT fornisce un accesso desktop remoto completamente isolato e clientless ai sistemi RDP, SSH e VNC target interni, senza richiedere agli utenti di installare un client sul proprio dispositivo utilizzando jump host e VPN legacy.

Alternativa alla VDI

I team IT e responsabili della sicurezza non hanno il controllo sui dispositivi non gestiti, il che comporta dei rischi per l'azienda. Per supportare l'accesso alle applicazioni dai dispositivi non gestiti, le organizzazioni solitamente utilizzano la VDI, che collega gli utenti direttamente alla rete, esponendo le applicazioni interne a endpoint non gestiti. Inoltre, la VDI è costosa, complessa da gestire e non è scalabile. Sulla scia della trasformazione digitale, le applicazioni moderne sono in genere basate su web o browser e lo streaming di un intero desktop tramite la VDI non offre un'esperienza ottimale agli utenti finali.

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.

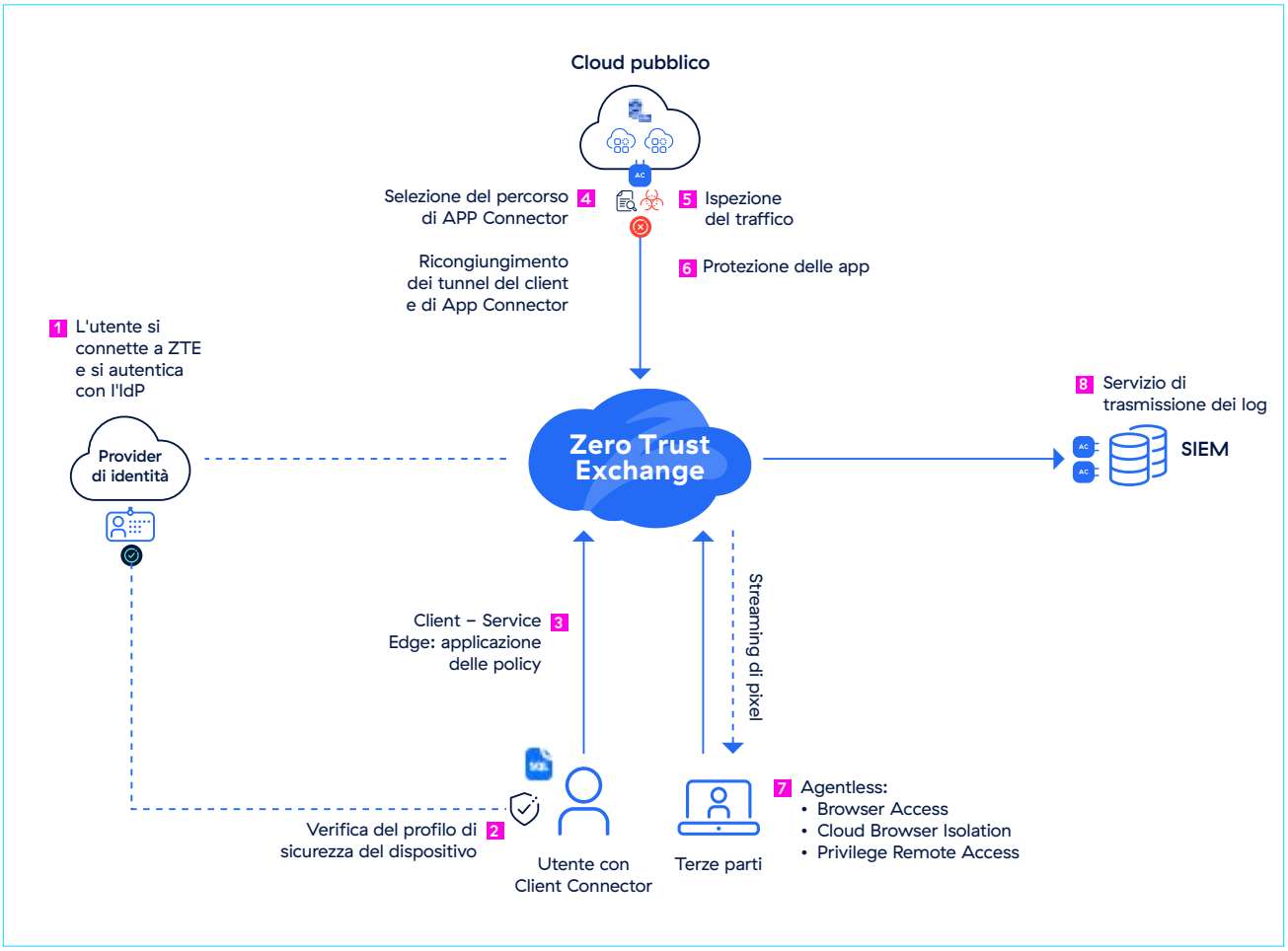
Microsegmentazione (segmentazione utente–app)

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 da remoto e, per loro natura, richiedono traffico in entrata, creando una superficie di attacco pubblica. Senza un'adeguata segmentazione della rete, una violazione di un segmento potrebbe compromettere l'intera rete aziendale. Detto questo, l'implementazione della segmentazione richiede complesse regole per i firewall, che risultano difficili da gestire e che spesso interrompono le applicazioni e possono ostacolare l'accesso alla VPN da parte degli utenti. Nelle grandi organizzazioni, ciò richiede spesso un'elevata disponibilità, routing complesso e costosi collegamenti privati.

La soluzione Zscaler Autonomous user–to–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. Automatizza l'intero ciclo della segmentazione, esaminando ogni applicazione attraverso il rilevamento, segmentando più velocemente con raccomandazioni basate sull'IA e rafforzando il profilo di sicurezza con informazioni strategiche in tempo reale.

©2025 Zscaler, Inc. Tutti i diritti riservati.

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.

©2025 Zscaler, Inc. Tutti i diritti riservati.

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

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 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 autonoma utente-app	Automatizza l'intero ciclo della segmentazione, esaminando ogni applicazione attraverso il rilevamento, segmentando più velocemente con raccomandazioni basate sull'IA e rafforzando il profilo di sicurezza con informazioni strategiche in tempo reale. Grazie ai modelli ML, che vengono addestrati continuamente sfruttando milioni di segnali dei clienti e i tuoi specifici modelli interni di accesso alle applicazioni, la segmentazione autonoma utente-app può aiutarti a eliminare il movimento laterale delle minacce, accelerare il tuo percorso verso lo ZTNA e semplificare e scalare le operazioni zero trust.
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.
Protezione dalle minacce e protezione dei dati	Riduci il rischio associato alle minacce con l'ispezione completa dei contenuti. Individua e controlla i dati sensibili nelle connessioni tra utenti e app.
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.
Accesso sicuro alle app S2C legacy	Offri un accesso sicuro alle applicazioni di rete legacy connesse, come VoIP, stampanti follow me e app server-to-client.
Accesso alle applicazioni B2B	Abilita l'accesso sicuro bidirezionale alle applicazioni e ai workload ospitati nella rete del tuo partner commerciale (Extranet)

©2025 Zscaler, Inc. Tutti i diritti riservati.

Accesso basato su 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 fornisce ai collaboratori terzi e agli utenti BYOD un accesso agevole alle app da qualsiasi dispositivo e browser web.
ZTNA in ufficio	Applica lo ZTNA agli utenti in ufficio utilizzando i private service edge di ZPA, garantendo un accesso rapido e senza interruzioni alle applicazioni. 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 ospitata dal cliente o completamente gestita.

Vantaggi

Ridurre al minimo la superficie di attacco
Eliminare le VPN vulnerabili e rendere le app invisibili a Internet rende impossibile per gli utenti non autorizzati individuarle e attaccarle. ZPA crea un segmento univoco tra un utente autorizzato e una specifica app privata, rimuovendo tutta la connettività in ingresso e consentendo solo connessioni inside-out, ovvero dall'interno verso l'esterno, tramite microtunnel cifrati ai dispositivi degli utenti. Gli amministratori possono individuare e segmentare automaticamente applicazioni, servizi e workload non autorizzati utilizzando la funzionalità per il rilevamento delle app, che contribuisce a ridurre ulteriormente la superficie di attacco.

Eliminare il movimento laterale
La connettività basata sull'accesso con privilegi minimi garantisce che l'accesso alle applicazioni sia concesso su base uno a uno, da un utente autorizzato ad applicazioni specifiche, anziché consentire un accesso completo alla rete. Pertanto, 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 impostare e gestire complesse segmentazioni di rete, liste di controllo degli accessi (ACL), policy dei firewall o traduzioni degli indirizzi di rete.

Prevenire utenti compromessi, minacce interne e aggressori avanzati
Le funzionalità integrate di ispezione inline e DLP riducono al minimo il rischio correlato a utenti compromessi e aggressori attivi. ZPA blocca automaticamente gli attacchi web attraverso una copertura completa delle tecniche più diffuse, tra cui le minacce OWASP Top 10, e un supporto integrale 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 BYOD, fornendo un accesso completamente isolato alle applicazioni, che mantiene i dati sensibili lontani dai dispositivi non gestiti utilizzando l'isolamento integrato del browser cloud.

Offrire un'esperienza utente ottimale
Una connettività costantemente 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 senza ostacoli da qualsiasi dispositivo e browser web, senza la necessità di installare un client. Gli utenti si registrano con le proprie credenziali SSO esistenti (Azure AD, Okta, Ping, ecc.), in più gli amministratori possono mantenere la produttività degli utenti rilevando e risolvendo in modo proattivo i problemi prestazionali degli utenti finali causati dalla difficoltà ad accedere alle app private, dalle interruzioni nel percorso di rete o dalla congestione della rete.

Una piattaforma unificata per l'accesso sicuro per 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 scollegati, unificando le policy di sicurezza e di accesso per bloccare le violazioni e ridurre la complessità operativa.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Zscaler Private Access (ZPA): diverse opzioni per iniziare

	Piattaforma Zscaler Essentials (ZS-ESS-PLATFORM)	Piattaforma clientless ZPA (ZPA-CLIENTLESS-PLATFORM)	Piattaforma Zscaler Private Access (ZS-ZPA-PLATFORM)	Piattaforma Zscaler (ZS-PLATFORM)
Servizi della piattaforma Private Access				
Controllo granulare dell'accesso per utente, gruppi di utenti e porte	✓ 1 utente ogni 20 abbonati (min. 500 utenti abbonati)	✓	✓	✓
Servizio di trasmissione dei log				
Monitoraggio continuo dell'integrità di tutte le app				
Ancoraggio IP sorgente: inoltra selettivamente il traffico dell'app ai server di destinazione appropriati				
App Connector: VM leggera che consente connessioni inside-out a Zscaler ZTE	Quanti ne servono, fino al massimo del sistema	Quanti ne servono, fino al massimo del sistema	Quanti ne servono, fino al massimo del sistema	Quanti ne servono, fino al massimo del sistema
ZPA Private Service Edge: ZTNA per utenti in remoto e in ufficio	–	–		
ZPA per app legacy (VOIP, S2C, ecc.)	–	–	Service Edge VPN aggiuntivi (minimo: 50 utenti)	Service Edge VPN aggiuntivi (minimo: 50 utenti)
ZPA Business Continuity Cloud	–	–	Componente aggiuntivo (minimo: 500 utenti)	Componente aggiuntivo (minimo: 500 utenti)
Segmentazione da utente ad app	10 segmenti di app	20 segmenti di app	20 segmenti di app	20 segmenti di app
Segmentazione autonoma utente-app e dati utili	–	–	**Elemento aggiuntivo**	**Elemento aggiuntivo**
Accesso di terze parti			Componente aggiuntivo (minimo: 500 utenti)	Componente aggiuntivo (minimo: 500 utenti)
Accesso basato su browser per dispositivi non gestiti	–	✓	✓ È possibile acquistare licenze aggiuntive per gli utenti guest con ZPA-CLIENTLESS-PLATFORM	✓ È possibile acquistare licenze aggiuntive per gli utenti guest con ZPA-CLIENTLESS-PLATFORM
Portale utente: portale web unico per consentire agli utenti di accedere alle app autorizzate e alle console con privilegi				
Privileged Remote Access Standard: PRA clientless per i sistemi OT (fino a 10) (RDP/SSH/VNC)				
Browser Isolation per le applicazioni private/SaaS		**Elemento aggiuntivo**	**Elemento aggiuntivo**	**Elemento aggiuntivo**
Monitoraggio dell'esperienza digitale	–	–	✓	✓
ZDX Standard: visibilità sulla telemetria di utenti, connettività e applicazioni				
Protezione di app private e dati	**Elemento aggiuntivo**			
Protezione dei dati per app private, risposta agli incidenti e classificazione dei dati		–	**Elemento aggiuntivo**	✓
Zscaler Deception: esche integrate per rilevare gli utenti compromessi		–	✓ (Minimo 500 utenti)	✓ (Minimo 500 utenti)
AppProtection per proteggere le app private da OWASP Top 10 e ispezionare il traffico web		**Elemento aggiuntivo**	**Elemento aggiuntivo**	**Elemento aggiuntivo**

©2025 Zscaler, Inc. Tutti i diritti riservati.

Differenze principali

ZPA è la prima soluzione ZTNA basata sull'IA 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 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
- **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 sicuro da browser:** sfrutta l'accesso basato su browser per terze parti con la DLP integrata
- **Eliminazione del movimento laterale con la segmentazione autonoma utente–app:** fornisce una segmentazione precisa utente–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 stata nominata tra i leader del Gartner® Magic Quadrant™ 2025 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, che, inoltrando automaticamente il traffico utente al Zscaler Service Edge più vicino, garantisce l'applicazione delle policy di sicurezza e accesso in 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 basato su browser integrato (web, RDP, SSH, VNC) o Zscaler Browser Isolation per l'accesso clientless su dispositivi non gestiti.

ZPA App Connector
Gli App Connector sono macchine virtuali leggere che si collocano davanti alle applicazioni private distribuite nel data center o nel cloud pubblico, per negoziare la connettività sicura tra un utente autorizzato e un'app specifica, con una connessione inside-out che non espone le app a Internet.

ZPA Network Connector
I Network Connector sono macchine virtuali leggere che vengono distribuite davanti ai server applicativi nel data center e si connettono ai VPN Service Edge sul cloud Zscaler tramite un tunnel inside-out.

ZPA Service Edge
I Service Edge applicano le policy di sicurezza e accesso instaurando una connessione inside-out tra un utente autorizzato (tramite Client Connector e Browser Access) a una specifica applicazione privata (tramite App Connector). La maggior parte dei clienti utilizza i nostri Public Service Edge, ospitati in oltre 160 punti di presenza (PoP) in tutto il mondo, che gestiscono milioni di utenti contemporaneamente per le più grandi organizzazioni a livello globale. I Private Service Edge gestiti da Zscaler sono disponibili anche per l'hosting on-site per fornire agli utenti on-premise il percorso più breve verso le applicazioni interne, senza uscire dalla rete locale. Garantiscono inoltre la continuità aziendale con un accesso ininterrotto alle applicazioni fondamentali per il business, anche in caso di eventi dirompenti imprevisti.

ZPA Private Cloud Controller
I Private Cloud Controller sono controller per singolo tenant per utenti, ZPA Private Service Edge e App Connector che possono essere sfruttati quando il cloud Zscaler non è disponibile o non risulta raggiungibile.

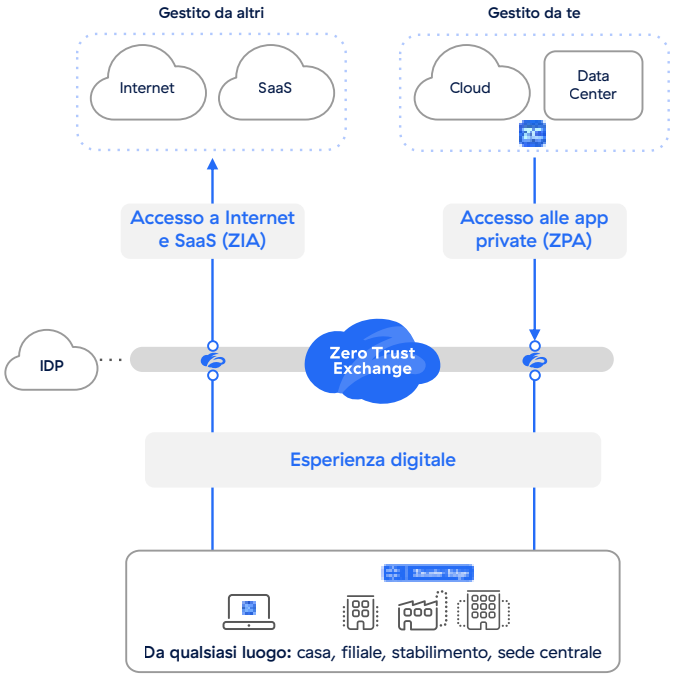
ZPA fa parte della soluzione olistica Zero Trust Exchange

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.

©2025 Zscaler, Inc. Tutti i diritti riservati.

Zscaler protegge la forza lavoro: un accesso sicuro, veloce e affidabile alle app.

Implementabile in pochi giorni per migliorare la protezione informatica e l'esperienza utente.



Protezione dei dati e difesa dalle minacce di livello superiore, esperienza utente eccellente, riduzione dei costi e della complessità

Specifiche tecniche

Componente di Zscaler	Piattaforme e sistemi supportati	
Client Connector	iOS 17 o successivi Android 9 o successivi Windows 8 o successivi	ChromeOS versione 137 o successive Linux MacOS 14 o successivi
Accesso clientless	Browser web moderni: (compatibili con HTML 5), Chrome, Edge, FireFox, Safari	
App Connector	AWS, GCP, Microsoft Azure, Nutanix, VMware, OpenShift, Docker, Red Hat	
Service Edge privato	AWS, GCP, Microsoft Azure, Nutanix, VMware, Docker, Red Hat	
Private Cloud Controller	AWS, Microsoft Azure, VMware, Red Hat	

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 a livello globale, Zero Trust Exchange, basata sull'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) **@zscaler**.

© 2025 Zscaler, Inc. Tutti i diritti riservati. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™ e ZPA™ e gli altri marchi comme ciali indicati su **zscaler.it/legal/trademarks** 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 titolari.

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