SCHEDA TECNICA

Zscaler Internet Access

Protezione basata sull'AI per ogni utente, app e luogo

Zscaler Internet Access™ fornisce un accesso sicuro e veloce a Internet e SaaS con la piattaforma zero trust più completa del settore.

Le soluzioni di sicurezza legacy non sono più efficaci in un mondo cloud e mobile

Le architetture legacy hub-and-spoke erano efficaci quando gli utenti si trovavano prevalentemente presso la sede centrale o in una filiale, le applicazioni risiedevano esclusivamente nel data center aziendale e la superficie di attacco era limitata a ciò che l'organizzazione aveva autorizzato. Oggi viviamo in un mondo totalmente diverso e dobbiamo difenderci da numerosi pericoli, come ransomware, minacce cifrate, attacchi alla catena di approvvigionamento e altre minacce avanzate in grado di violare le difese tradizionali della rete. È il momento di trovare una soluzione di sicurezza nativa del cloud in grado di ridurre in modo olistico rischi e complessità e di offrire al tempo stesso la flessibilità necessaria per far andare avanti le iniziative aziendali.

Zscaler Internet Access

La protezione dell'azienda cloud e mobile di oggi richiede un approccio radicalmente diverso e basato sullo zero trust. Zscaler Internet Access, parte di Zscaler Zero Trust Exchange™, è la piattaforma Security Service Edge (SSE) più diffusa al mondo, frutto di una leadership decennale nel campo dei

Vantaggi:

- **Previeni le minacce informatiche e la perdita dei dati con l'IA:** proteggi la tua organizzazione dalle minacce avanzate sfruttando una suite di servizi di protezione dei dati e dalle minacce informatiche basati sull'IA, arricchiti da aggiornamenti in tempo reale provenienti da 500 bilioni di segnalazioni di minacce giornaliere derivanti dal security cloud più grande del mondo.
- **Esperienza utente impareggiabile:** ottieni l'esperienza Internet e SaaS più veloce del mondo (fino al 40% più rapida rispetto alle tradizionali architetture di sicurezza) e aumenta la produttività e l'agilità aziendale.
- **Architettura di sicurezza più moderna:** ottieni un ROI del 139% grazie a Zscaler e sostituisci il 90% delle appliance costose, complesse e lente con una piattaforma zero trust nativa nel cloud.

Secure Web Gateway. Offerta sotto forma di piattaforma SaaS scalabile e basata sul security cloud più grande del mondo, consente di eliminare le soluzioni legacy per bloccare gli attacchi avanzati e prevenire la perdita dei dati adottando un approccio zero trust completo che include:

Sicurezza uniforme e di alto livello per la forza lavoro flessibile di oggi: quando la sicurezza viene spostata sul cloud, tutti gli utenti, le app, i dispositivi e le posizioni ottengono una protezione dalle minacce sempre attiva basata su identità e contesto; le tue policy di sicurezza seguono gli utenti, ovunque.

Accesso veloce con un'infrastruttura azzerata: l'architettura direct-to-cloud garantisce un'esperienza utente ideale ed elimina il backhauling, migliora le prestazioni e semplifica l'amministrazione della rete senza la necessità di ricorrere ad alcun tipo di infrastrutture fisica.

Protezione basata sull'AI supportata dal security cloud più grande del mondo: l'ispezione inline di tutto il traffico Internet e SaaS, che comprende la decifrazione dell'SSL, con una suite di servizi di sicurezza sul cloud basati sull'IA, consente di bloccare i ransomware, i malware 0-day e gli attacchi avanzati grazie all'intelligence sulle minacce ottenuta attraverso 500 bilioni di segnalazioni giornaliere.

Gestione semplificata: sfruttando una soluzione di sicurezza nativa del cloud con AI integrata, nessun hardware da gestire, flussi di lavoro semplificati e policy create in base alle necessità dell'azienda, il team addetto alla sicurezza può finalmente concentrarsi sugli obiettivi strategici.

*Gartner Magic Quadrant for Security Service Edge, 10 aprile 2023, Charlie Winckless, et al.

Servizi integrati di sicurezza e protezione dei dati basati sull'AI

Zscaler Internet Access include una suite completa di servizi di sicurezza e protezione dei dati alimentati da algoritmi di AI per bloccare gli attacchi informatici e la perdita di dati. In quanto soluzione SaaS completamente distribuita sul cloud, è possibile aggiungere nuove funzionalità senza hardware aggiuntivo o lunghi cicli di implementazione. I moduli disponibili con Zscaler Internet Access sono:

- **Cloud Secure Web Gateway (SWG):** offri un'esperienza web sicura e veloce che elimina i ransomware, i malware e gli altri attacchi avanzati sfruttando l'analisi in tempo reale basata sull'AI e il filtraggio degli URL.
- **Cloud Access Security Broker (CASB):** proteggi le applicazioni cloud grazie al CASB integrato per tutelare i dati, bloccare le minacce e garantire la conformità negli ambienti SaaS e IaaS.
- **Cloud Data Loss Prevention (DLP):** proteggi i dati in movimento con un'ispezione inline completa e altre misure avanzate, come EDM (Exact Data Match), riconoscimento ottico dei caratteri (OCR) e machine learning.

- **Zscaler Firewall e IPS cloud:** estendi la protezione più all'avanguardia del settore a tutte le porte e i protocolli e sostituisci i firewall all'edge e quelli delle filiali con una piattaforma nativa del cloud.
- **Cloud Sandbox:** blocca i malware sconosciuti ed elusivi nei protocolli web ed FTP sfruttando la quarantena basata sull'AI e offri una protezione uniforme, globale e in tempo reale a tutti gli utenti.
- **Cloud Browser Isolation basato su AI:** rendi gli attacchi basati sul web un ricordo del passato e previeni la perdita di dati creando uno spazio virtuale tra utenti, web e SaaS.
- **Digital Experience Monitoring:** riduci il carico operativo dell'IT e accelera la risoluzione delle richieste di assistenza grazie a una visione unificata delle metriche di applicazioni, percorsi cloud e prestazioni degli endpoint per l'analisi e la risoluzione dei problemi.
- **Zero Trust Branch Connectivity:** riduci il rischio e la complessità con una connettività non instradabile per filiali e data center, per utenti, server e dispositivi IoT/OT.
- **DNS Security:** ottimizza la sicurezza e le prestazioni del DNS per tutti gli utenti, i dispositivi e le applicazioni, su tutte le porte e i protocolli, ovunque nel mondo.

Zscaler Internet Access per utenti e workload

Grazie a Zscaler Internet Access, è possibile eliminare il rischio che i workload cloud accedano indiscriminatamente a destinazioni Internet o SaaS. Eliminando l'accesso dei workload a Internet attraverso strumenti di rete legacy, come VPN, firewall (compresi i firewall virtuali) o tecnologie WAN, è possibile prevenire le compromissioni e bloccare il movimento laterale senza dover ricorrere a un insieme incoerente di strumenti di sicurezza. Applicando la suite completa di funzionalità di sicurezza e protezione dei dati di Zscaler Internet Access (ZIA) ai workload, puoi unificare la sicurezza zero trust di utenti e workload con un'unica piattaforma integrata.

Abbinando ZIA a Zscaler Private Access, è possibile estendere la protezione ad applicazioni e workload privati, siano essi nel cloud pubblico o in un data center privato.

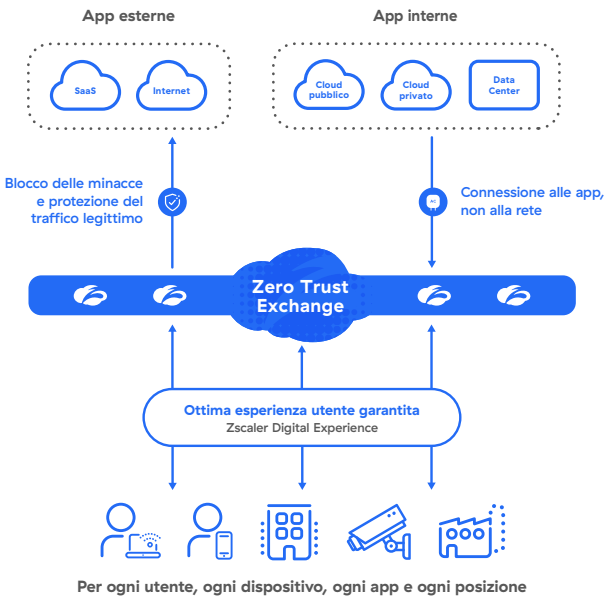

Figura 1: Zero Trust Exchange

Casi d'uso

Protezione da minacce informatiche e ransomware

Passa dalla sicurezza legacy alla rivoluzionaria architettura zero trust di Zscaler e previeni le compromissioni, elimina la superficie di attacco, blocca il movimento laterale e mantieni i dati al sicuro.

Scopri di più →

Protezione della forza lavoro flessibile

Consenti a dipendenti, partner, clienti e fornitori di accedere in modo sicuro alle applicazioni web e ai servizi cloud da qualsiasi luogo e su qualsiasi dispositivo, con la certezza di poter usufruire sempre di un'esperienza digitale ottimale.

Scopri di più →

Protezione dei dati

Blocca la perdita di dati causata da utenti, applicazioni SaaS e infrastruttura del cloud pubblico derivante da esposizioni accidentali, furti di dati o ransomware a doppia estorsione.

Scopri di più →

Modernizzazione dell'infrastruttura

Elimina le reti costose e complesse a favore di un accesso rapido, sicuro e diretto al cloud, che azzera la necessità di firewall all'edge e nelle filiali.

Scopri di più →

L'ecosistema di Zero Trust Exchange di Zscaler

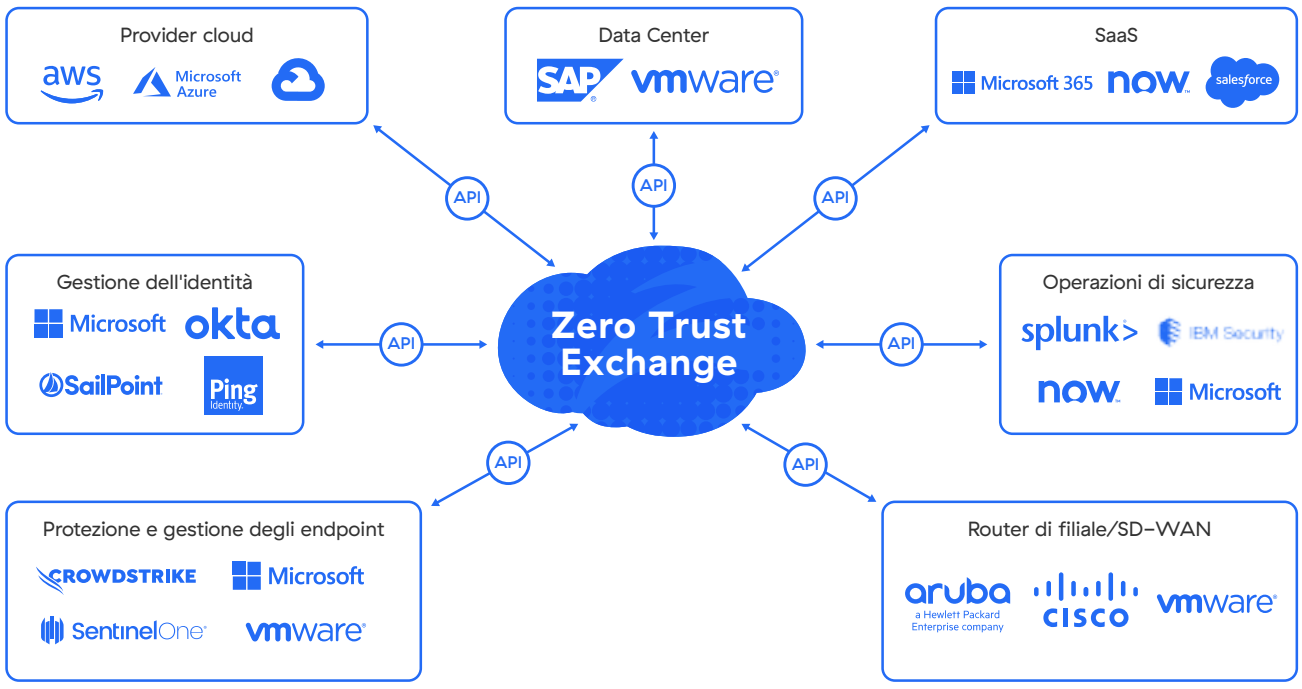

Figura 2: ecosistema dei partner di Zscaler Internet Access

TABELLA 1: CARATTERISTICHE E FUNZIONALITÀ DI ZSCALER INTERNET ACCESS	
FUNZIONALITÀ	**DETTAGLI**
Funzionalità	
Filtraggio URL	Concedi, blocca, limita o isola l'accesso degli utenti a categorie o destinazioni web specifiche per bloccare le minacce web e garantire la conformità alle policy aziendali.
Ispezione SSL	Offri un'ispezione illimitata del traffico TLS/SSL per bloccare la perdita di dati e identificare le minacce che si nascondono nel traffico cifrato. Specifica le categorie web o le app da ispezionare in base ai requisiti di privacy o di conformità alle normative.
Sicurezza DNS	Identifica e instrada le connessioni sospette di comando e controllo verso i motori di rilevamento delle minacce di Zscaler e ottieni un'ispezione completa dei contenuti.
Controllo dei file	Blocca o consenti il download/upload di file dalle applicazioni a seconda dell'app, dell'utente o del gruppo di utenti.
Controllo della larghezza di banda	Applica policy sulla larghezza di banda e assegna priorità alle applicazioni critiche per il business rispetto al traffico non legato al lavoro.
Protezione dalle minacce avanzate	Interrompi gli attacchi informatici avanzati, come malware, ransomware, attacchi alla catena di approvvigionamento, phishing e altro grazie alla protezione dalle minacce avanzate con tecnologia proprietaria. Definisci policy granulari basate sulla tolleranza al rischio dell'organizzazione.
Protezione dati inline (dati in movimento)	Utilizza le funzionalità proxy di inoltro e ispezione SSL per controllare in tempo reale il flusso delle informazioni sensibili verso destinazioni web rischiose e app cloud, e blocca le minacce ai dati, siano esse interne o esterne. La protezione avanzata inline viene fornita indipendentemente dal fatto che un'app sia autorizzata o non gestita, senza la necessità dei log dei dispositivi di rete.
Protezione dei dati fuori banda (dati inattivi)	Utilizza le integrazioni API per scansionare le app SaaS, le piattaforme cloud e i loro contenuti al fine di identificare i dati sensibili inattivi, ed esegui correzioni automaticamente, ad esempio revocando l'autorizzazione per le condivisioni pericolose o dirette verso ambienti esterni.
Prevenzione delle intrusioni	Ottieni una protezione completa da botnet, minacce avanzate e O-day, e ricevi informazioni contestuali su utenti, applicazioni e minacce. L'IPS cloud e web funziona senza problemi con firewall, sandbox, DLP e CASB.
Policy di accesso e sicurezza dinamiche e basate sul rischio	Adatta automaticamente le policy di sicurezza e di accesso al rischio associato a utenti, dispositivi, applicazioni e contenuti.
Acquisizione del traffico	Acquisizione semplice dei pacchetti: acquisisci con facilità il traffico decifrato secondo criteri specifici all'interno dei motori di policy di Zscaler, ed esegui un'efficiente analisi forense della sicurezza senza la necessità di ricorrere a dispositivi aggiuntivi.
Analisi dei malware	Rileva, previeni e metti in quarantena le minacce sconosciute che si nascondono nei payload dannosi inline sfruttando tecnologie avanzate di IA/ML per bloccare gli attacchi da paziente zero.
Filtraggio DNS	Controlla e blocca le richieste DNS in base alle destinazioni conosciute e nocive.
Isolamento web	Rendi le minacce web un ricordo del passato e offri contenuti attivi attraverso un flusso benigno di pixel trasmesso al browser dell'utente finale.
Correlazione delle informazioni sulle minacce	Accelera le indagini e i tempi di risposta grazie ad avvisi contestualizzati e correlati, con informazioni approfondite sul punteggio assegnato alle minacce, le risorse colpite, la gravità e molto altro.
Isolamento delle applicazioni	Consenti ai dispositivi non gestiti di accedere in sicurezza e senza agente ad applicazioni SaaS, cloud e private, e ottieni un controllo granulare delle azioni degli utenti, come copia/incolla, upload, download e stampa, bloccando così la perdita dei dati sensibili.
Monitoraggio dell'esperienza digitale	Ottieni una visione unificata delle metriche delle prestazioni relative ad applicazioni, percorsi cloud ed endpoint per l'analisi e la risoluzione dei problemi.
Zero Trust Branch Connectivity	Modernizza la connettività delle filiali attraverso Zero Trust Exchange eliminando la superficie di attacco e prevenendo il movimento laterale.
Protezione delle comunicazioni da workload a Internet	Impedisci le compromissioni e interrompi il movimento laterale nelle comunicazioni da workload a Internet. Include ispezione SSL, IPS, filtraggio URL e protezione dei dati per tutte le comunicazioni.
Visibilità sui dispositivi IoT	Ottieni una visione completa sui dispositivi IoT, i server e i dispositivi utente non gestiti in tutta l'azienda, sfruttando il rilevamento automatico, il monitoraggio continuo e la classificazione basata su IA ed ML con funzionalità avanzate di marcatura automatica

FUNZIONALITÀ	DETTAGLI
Funzionalità della piattaforma	
Opzioni flessibili di connettività	• **Zscaler Client Connector (ZCC):** inoltra il traffico a Zero Trust Exchange tramite un agente leggero che supporta Windows, macOS, iOS, iPadOS, Android e Linux. • **Tunnel GRE o IPsec:** impiega tunnel GRE e/o IPsec per inviare il traffico a Zero Trust Exchange per i dispositivi senza ZCC. • **Isolamento del browser:** connetti in modo fluido qualsiasi dispositivo personale o non gestito sfruttando la funzionalità integrata Cloud Browser Isolation. • **Concatenamento di proxy:** Zscaler supporta l'inoltro del traffico da un server proxy a un altro (sconsigliato negli ambienti di produzione). • **File PAC:** invia il traffico a Zero Trust Exchange con file PAC per i dispositivi senza ZCC.
Distribuzione sul cloud	Una piattaforma al 100% nativa del cloud e fornita come servizio SaaS. Per i casi d'uso più particolari, sono disponibili service edge privati e virtuali.
Privacy e conservazione dei dati	Quando i dati vengono registrati nei log, il loro contenuto non viene mai scritto su disco, e vi sono controlli granulari per determinare dove avviene esattamente la registrazione. Utilizzando il controllo degli accessi basato su ruoli (RBAC), è possibile garantire l'accesso in sola lettura e l'anonimizzazione/offuscamento dei nomi utente e dei diritti di accesso in base al reparto o alla funzione, nel rispetto delle principali normative di conformità. I dati vengono conservati per un periodo variabile di sei o meno mesi, a seconda del prodotto. È possibile acquistare ulteriore spazio di archiviazione per estendere il periodo di conservazione dei dati per tutto il tempo desiderato.
Principali certificazioni di conformità	Le certificazioni includono: • FedRAMP • ISO 27001 • SOC 2 tipo II • SOC 3 • NIST 800-63C Visualizza l'elenco completo delle nostre certificazioni di conformità qui.
Supporto granulare delle API	Disponiamo di integrazioni API REST con numerosi provider di servizi di identità, reti e sicurezza. Ad esempio, puoi condividere i log tra Zscaler e il tuo SIEM cloud oppure on-premise (come Splunk). Scopri di più
Peering diretto	Il peering diretto con i principali provider di servizi Internet e SaaS e le principali destinazioni su cloud pubblico garantisce il percorso più rapido per il traffico.
Accordi sul livello del servizio (SLA)	
Disponibilità	99,999%, misurata in base alle transazioni perse
Latenza del proxy	< 100 ms, anche quando è attiva la scansione DLP e delle minacce
Cattura dei virus	100% dei virus e dei malware noti
Piattaforme e sistemi supportati	
Client Connector	Supporto per: • iOS 9 e versioni successive • Android 5 e versioni successive • Windows 7 e versioni successive • Mac OS X 10.10 e versioni successive • CentOS 8 • Ubuntu 20.04 Scopri di più
Branch Connector	Supporto per: • VMware vCenter o vSphere Hypervisor • Centos • Redhat

Edizioni di Zscaler Internet Access

	Funzionalità	Essentials	Business	Transformation	Illimitato
Servizi della piattaforma		Filtraggio dei contenuti, AV inline, ispezione SSL, Nanolog streaming	(+) Certificato privato SSL	(+) Cloud NSS, ripristino log NSS, accesso DC esteso, tunnel IPSec, avvisi contestuali, ZIA Virtual Private Service Edge (8)	(+) Ancoraggio IP di origine, ambiente di test, categorizzazione delle priorità, ZIA Virtual Private Service Edge (32), protezione di server e IoT (1 GB/10 utenti)
Protezione dalle minacce	**Protezione dalle minacce avanzate (con rilevamento basato sull'IA di phishing e C2)** Protezione contro minacce note e sconosciute (URL, AV, Botnet/C2, Phishing)	incluso	incluso	incluso	incluso
	Cloud Sandbox Prevenzione degli attacchi O-day analizzando i file sospetti con la quarantena basata sull'AI	Elemento aggiuntivo	Elemento aggiuntivo	incluso	incluso
	Isolamento: protezione dalle minacce informatiche Protezione contro gli attacchi O-day da contenuti web sospetti. Isolamento basato sul rischio con l'intelligenza artificiale	Elemento aggiuntivo	Elemento aggiuntivo	Isolamento per la protezione informatica: standard (100 MB/utente/mese)	Isolamento per la protezione informatica: standard (1,5 GB/utente/mese)
	Correlazione delle informazioni sulle minacce Indagini e tempi di risposta più rapidi con l'intelligence contestuale sulle minacce	–	incluso	incluso	incluso
	Policy dinamiche basate sul rischio Adattamento e suggerimento automatico delle policy di sicurezza in base a vari fattori di rischio	–	–	incluso	incluso
	Tecnologia di deception integrata Migliora il profilo di sicurezza zero trust attirando, rilevando e intercettando in modo proattivo gli aggressori	–	–	Standard[1]	Standard[1]
Trasformazione della rete	**Risoluzione e filtraggio DNS** DNS resolver affidabile per una risoluzione geocentrica e ottimale	fino a 64 regole	fino a 64 regole	incluso	incluso
	Rilevamento del DNS tunneling Rilevamento e prevenzione degli attacchi basati su DNS e dell'esfiltrazione di dati attraverso i tunnel DNS	–	–	incluso	incluso
	Controllo della larghezza di banda Controllo del traffico e priorità della larghezza di banda, limitazione della velocità per il traffico web		incluso	incluso	incluso
	Firewall cloud Protezione del lavoro da qualsiasi luogo per tutti gli utenti e il traffico (sia web che non web) con ispezione SSL infinita	Rete, servizi di applicazioni, posizioni, FQDN fino a 10 regole	Rete, servizi di applicazioni, posizioni, FQDN fino a 10 regole	(+) utenti da remoto + posizioni, ispezione approfondita di applicazioni e pacchetti	(+) utenti da remoto + posizioni, ispezione approfondita di applicazioni e pacchetti
	Protezione per il traffico non autenticato Protezione delle reti con una sicurezza di livello carrier completamente automatizzata con limitazioni	0,5 GB per utente al mese	1 GB per utente al mese	1,5 GB per utente al mese	2 GB per utente al mese

	Funzionalità	Essentials	Business	Transformation	Illimitato
Proteggi i dati e previeni la perdita di dati	**Controllo delle app cloud + Restrizioni della tenancy** Individuazione e controllo dell'utilizzo di app rischiose o non autorizzate (Shadow IT)	incluso	incluso	incluso	incluso
	Isolamento – Protezione dei dati (SaaS) Prevenzione della perdita di dati dalle app SaaS sui dispositivi personali o gli endpoint non gestiti (clientless)	Elemento aggiuntivo	Elemento aggiuntivo	Elemento aggiuntivo	Isolamento per la protezione dati (SaaS): standard (100 MB per utente al mese)
	DLP, CASB, Inline Web Essentials, API SaaS (1 app) Prevenzione della perdita di dati sensibili su Internet. Scansione di 1 app SaaS per impedire la condivisione rischiosa di dati sensibili o malware	–	Protezione dei dati standard (DLP e CASB Essentials)	(+) Retroscansione API SaaS	incluso
	API SaaS, sicurezza della catena di approvvigionamento SaaS, dispositivi non gestiti, classificazione, gestione degli incidenti Protezione standard più: controllo dei rischi dei dispositivi BYOD con streaming di dati sotto forma di pixel, scansione di app SaaS per condivisioni/malware pericolosi, personalizzazione DLP con EDM, IDM, OCR più gestione incidenti e automazione dei flussi di lavoro	Elemento aggiuntivo	Elemento aggiuntivo	Elemento aggiuntivo	incluso
Monitoraggio dell'esperienza digitale	Monitoraggio delle esperienze digitali dal punto di vista dell'utente finale, per ottimizzare le prestazioni e risolvere rapidamente i problemi di applicazioni, rete e dispositivi.	–	Standard	Standard	Standard
Premium Support Plus		Elemento aggiuntivo	Elemento aggiuntivo	Elemento aggiuntivo	incluso

Modello di licenza

Tutte le edizioni di Zscaler Internet Access prevedono una tariffazione per utente. Per alcuni prodotti all'interno della tua edizione, il prezzo può variare in base a fattori diversi dal numero di utenti. Per ulteriori informazioni sui prezzi, rivolgiti al team responsabile del tuo account Zscaler.

Parte della soluzione olistica Zero Trust Exchange

Zero Trust Exchange consente di stabilire connessioni veloci e sicure e permette ai dipendenti di lavorare da qualsiasi luogo utilizzando Internet come rete aziendale. È una soluzione basata sul principio dello zero trust, che si fonda sull'accesso a privilegi minimi e offre una sicurezza completa utilizzando l'identità basata sul contesto e l'applicazione delle policy.

> Quando si verificano attacchi ransomware ad altre aziende, sono migliaia i sistemi nel loro ambiente a essere colpiti, oltre al grave impatto derivante dal dover pagare un riscatto. Quando questi eventi fanno notizia, inizio a ricevere chiamate dai dirigenti in apprensione, e sono felice di poterli rassicurare dicendo loro che noi siamo al sicuro".
>
> **Ken Athanasiou,** VIP e CISO, AutoNation

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