Zscaler Internet Access

Protezione basata sull'AI ovunque, per tutti gli utenti, le app e le sedi

SCHEDA TECNICA

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

La sicurezza della rete legacy è inefficiente per un mondo incentrato sul cloud e la mobilità

Le architetture di tipo "Hub and spoke" legacy erano efficaci quando gli utenti si trovavano principalmente nella sede centrale o in una filiale dell'azienda, le applicazioni risiedevano esclusivamente sul data center aziendale e la superficie di attacco era limitata a quanto autorizzato dall'organizzazione. Oggi viviamo in un mondo radicalmente diverso, in cui pericoli come ransomware, minacce cifrate, attacchi alla catena di approvvigionamento e altre minacce avanzate riescono a superare le difese di rete tradizionali. È tempo di trovare una soluzione di sicurezza nativa del cloud in grado di ridurre in modo olistico i rischi e le complessità, offrendo al contempo la flessibilità necessaria per portare 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 di Security Service Edge (SSE) più diffusa al mondo, frutto di una leadership decennale nel campo dei Secure Web Gateway.

ZIA è un servizio distribuito attraverso una piattaforma di sicurezza sul cloud di tipo SaaS, scalabile e resiliente, che consente di eliminare le soluzioni per la sicurezza di rete legacy per bloccare gli attacchi avanzati e prevenire la perdita di dati, con 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.

Un accesso istantaneo, senza infrastrutture fisiche: un'architettura direct-to-cloud garantisce un'esperienza utente rapida e fluida, eliminando il backhauling, migliorando le prestazioni e l'esperienza utente e semplificando l'amministrazione della rete, senza bisogno di alcun tipo di infrastruttura 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'AI, 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: l'utilizzo di una soluzione di sicurezza nativa del cloud basata sull'AI riduce l'hardware da gestire, introduce l'automazione per semplificare i flussi di lavoro e permette di creare policy incentrate sul business, consentendo ai team di avere più tempo a disposizione per lavorare sugli obiettivi strategici.

Servizi integrati di sicurezza e protezione dei dati alimentati da algoritmi di 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 con 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 completa inline e 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.
- **Zscaler Sandbox:** blocca i malware sconosciuti ed elusivi nei protocolli di trasferimento file e web con la quarantena basata sull'AI e offri una protezione uniforme e globale a tutti gli utenti in tempo reale.
- **Zero Trust Browser basato sull'AI:** dimenticati degli attacchi web e previeni la perdita dei dati creando uno spazio virtuale tra utenti, web e SaaS.

VANTAGGI:

- **Previeni le minacce informatiche e la perdita dei dati con l'AI:** proteggi la tua organizzazione dalle minacce avanzate con una suite di servizi AI di tutela dei dati e difesa dalle minacce informatiche insieme ad aggiornamenti in tempo reale provenienti da 500 bilioni di segnalazioni giornaliere di minacce provenienti 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.
- **Riduci costi e complessità:** realizza un ROI del 139% con Zscaler sostituendo il 90% delle tue apparecchiature costose, complesse e lente con una piattaforma zero trust integralmente nativa del cloud.
- **Proteggi la tua forza lavoro ibrida:** consenti a dipendenti, clienti e terze parti di accedere in modo sicuro ad app web e servizi cloud da qualsiasi luogo e su qualsiasi dispositivo, con la certezza che potranno godere di un'esperienza digitale d'eccellenza.
- **Unifica le attività di SecOps e NetOps:** ottieni risultati di sicurezza più rapidi e collaborativi grazie a strumenti condivisi che includono informazioni sul traffico in tempo reale, integrazioni API-first e RBAC granulare.
- **Ottieni la massima sovranità su dati e contenuti:** assicura la conformità implementando un accesso sicuro e localizzato, senza compromessi in termini di prestazioni, utilizzando Egress NAT, contenuti geolocalizzati e logging dei dati a livello nazionale.
- **Proteggi l'uso dell'AI nel tuo ambiente:** consenti un utilizzo sicuro di Microsoft Copilot e di altre applicazioni AI.
- **Proteggi gli ambienti degli sviluppatori su larga scala:** automatizza l'ispezione SSL/TLS di oltre 30 strumenti per sviluppatori mentre esegui il sandboxing del codice e dei file sconosciuti o di grandi dimensioni e ricevi verdetti AI immediati, il tutto senza rallentare l'innovazione.

- **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 di 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 la necessità che i workload accedano a Internet attraverso strumenti legacy incentrati sulla rete, 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 ZIA ai workload, puoi unificare la sicurezza zero trust e applicarla a utenti e workload grazie a un'unica piattaforma integrata.

Associando ZIA a Zscaler Private Access, puoi estendere la protezione alle tue app e ai tuoi workload privati, indipendentemente dal fatto che risiedano sul cloud pubblico o in un data center privato.

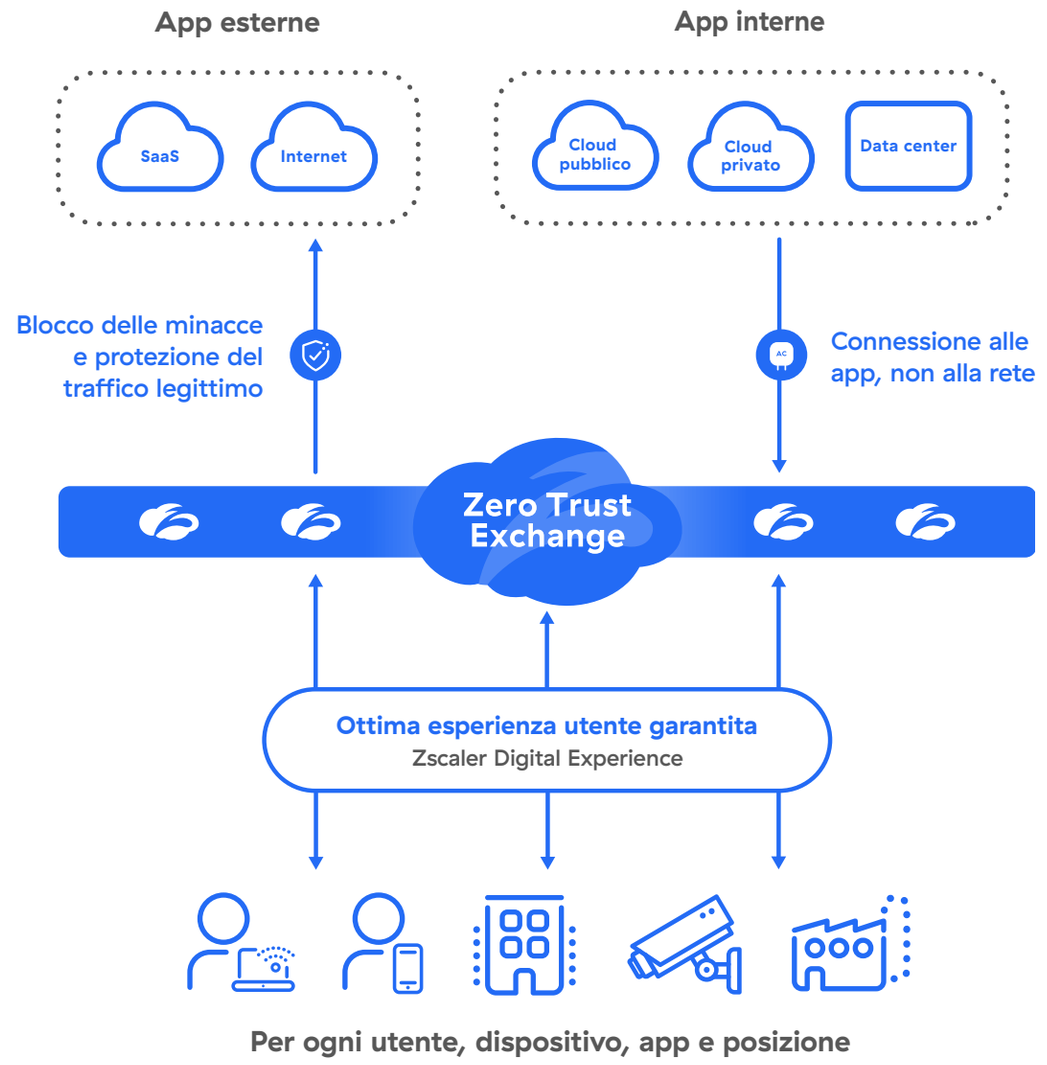

Figura 1: Zero Trust Exchange

*Gartner Magic Quadrant for Security Service Edge, 15 aprile 2024, Charlie Winckless, et al.

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

Zscaler è stata nominata una leader del Gartner® Magic Quadrant™ per il Security Service Edge.

VEDI DI PIÙ

Casi d’uso

PROTEZIONE DA MINACCE INFORMATICHE E RANSOMWARE

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

Scopri di più

PROTEZIONE DELLA FORZA LAVORO FLESSIBILE

Dipendenti, partner, clienti e fornitori potranno accedere in modo sicuro alle applicazioni web e ai servizi cloud da qualsiasi luogo e su qualsiasi dispositivo, con la certezza di poter godere di un’ottima esperienza digitale.

Scopri di più

PROTEZIONE DEI DATI

Impedisci la perdita dei dati da utenti, app SaaS e infrastruttura del cloud pubblico, che si tratti di un’esposizione accidentale, di un furto di dati o di un ransomware a doppia estorsione.

Scopri di più

MODERNIZZAZIONE DELL’INFRASTRUTTURA

Elimina le reti costose e complesse, e offri un accesso rapido, affidabile, sicuro e diretto al cloud, per rimuovere la necessità di firewall edge e di filiale.

Scopri di più

L’ecosistema di Zero Trust Exchange di Zscaler

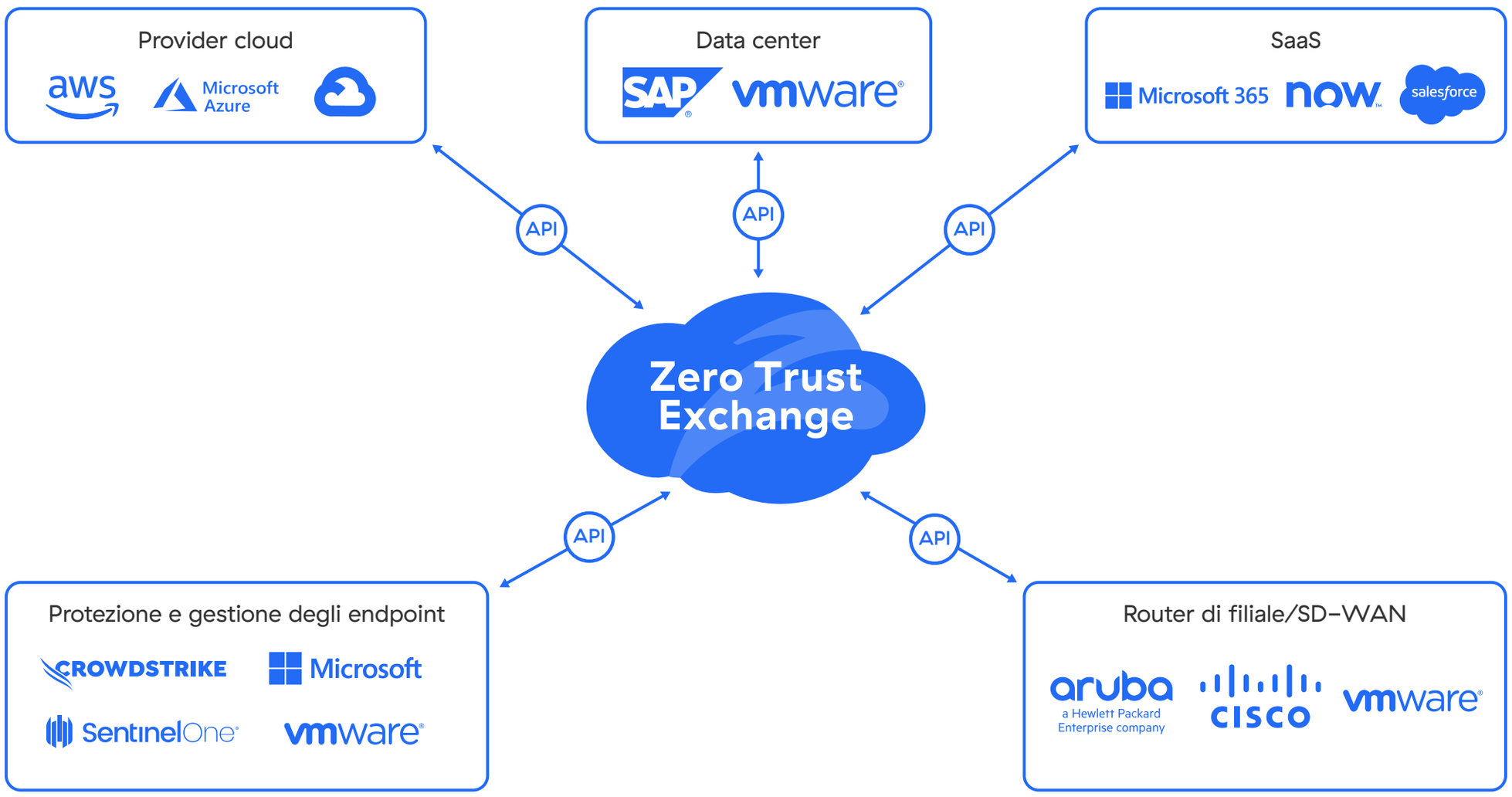

TABELLA 1: CARATTERISTICHE E FUNZIONALITÀ DI ZSCALER INTERNET ACCESS	
FUNZIONALITÀ	**DETTAGLI**
FUNZIONALITÀ	
Filtraggio URL	Concedi, blocca, limita o isola l'accesso degli utenti a categorie o destinazioni web specifiche per fermare le minacce basate sul web e garantire la conformità alle policy aziendali.
Ispezione SSL	Ottieni un'ispezione illimitata del traffico TLS/SSL per identificare le minacce e bloccare la perdita dei dati che si nascondono nel traffico cifrato. Specifica le categorie web o le app da ispezionare in base ai requisiti di privacy o di conformità. Integra l'ispezione con lo strumento per sviluppatori per proteggere i flussi di lavoro di questi ultimi.
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.
IP dedicato	Fornisci l'accesso alle applicazioni sulla base di un elenco di indirizzi IP consentiti che include solo gli IP autorizzati dell'organizzazione. Favorisci inoltre una facile transizione dall'architettura legacy a quella zero trust.
Controllo dei file	Blocca o consenti il download/upload di file dalle applicazioni a seconda dell'app, dell'utente o del gruppo di utenti.
Bring Your Own IP (IP personale)	Mantieni coerenza e controllo sulle identità di rete e assicura alle app di terze parti o alle infrastrutture dipendenti che il traffico provenga esclusivamente dall'organizzazione.
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.
Logging basato sul Paese	Archivia e gestisci i log entro i confini di un Paese specifico, per soddisfare i requisiti di sovranità dei dati che impongono che i dati relativi ai cittadini siano trattati in conformità alle leggi locali.
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. Imposta policy granulari basate sulla tolleranza al rischio dell'organizzazione.
Protezione dei 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, bloccando le minacce interne ed esterne ai dati. 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 minacce come 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. Distribuisci firme delle minacce personalizzate utilizzando Cloud Custom IPS per rilevare e fermare gli attacchi mirati.
Policy di accesso e sicurezza dinamiche 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 AI/ML per bloccare gli attacchi da paziente zero.
Filtraggio DNS	Controlla e blocca le richieste DNS in base alle destinazioni conosciute e nocive.
Zero Trust Browser (isolamento web)	Rendi obsolete le minacce basate sul web e offri contenuti attivi sotto forma di un flusso benigno di pixel al browser dell'utente finale.
Correlazione delle informazioni sulle minacce	Accelera le indagini e i tempi di risposta grazie ad avvisi contestualizzati e correlati contenenti informazioni approfondite sul punteggio assegnato alle minacce, sulle risorse colpite, sulla gravità e altro.
Isolamento delle applicazioni	Consenti ai dispositivi non gestiti di accedere in sicurezza e senza agente ad applicazioni SaaS, cloud e private, ottieni un controllo granulare delle azioni degli utenti, come copia/incolla, upload/download e stampa, e blocca così la perdita dei dati sensibili.
Monitoraggio dell'esperienza digitale (ZDX)	Ottieni una visione unificata delle metriche delle prestazioni relative ad applicazioni, percorsi cloud ed endpoint per l'analisi e la risoluzione dei problemi.
Connettività zero trust per le filiali	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 blocca il movimento laterale nelle comunicazioni tra workload e Internet. La soluzione include ispezione SSL, IPS, filtraggio URL e protezione dei dati per tutte le comunicazioni.
Visibilità sui dispositivi IoT	Ottieni una visibilità completa sui dispositivi IoT, i server e i dispositivi utente non gestiti in tutta l'azienda grazie al rilevamento automatico, il monitoraggio continuo e la classificazione basata su AI ed ML con funzionalità avanzate di labeling automatico.
Controllo dell'accesso basato sui ruoli (RBAC)	Autorizzazioni ottimizzate per controllare ciò che gli amministratori possono modificare e visualizzare, i report sulle policy e le analisi all'interno della piattaforma Zscaler, per prevenire i conflitti e migliorare la governance.

FUNZIONALITÀ	DETTAGLI
FUNZIONALITÀ DELLA PIATTAFORMA	
Opzioni flessibili per la 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: utilizza tunnel GRE e/o IPsec per inviare il traffico a Zero Trust Exchange per i dispositivi senza ZCC. • Isolamento del browser: connetti senza problemi qualsiasi dispositivo personale o non gestito con l'isolamento integrato tramite Zero Trust Browser. • Concatenamento dei proxy: Zscaler supporta l'inoltro del traffico da un server proxy a un altro, ma questa opzione non è consigliata negli ambienti di produzione. • File PAC: invia traffico a Zero Trust Exchange tramite i file PAC per i dispositivi senza ZCC.
Distribuzione sul cloud	Una piattaforma al 100% nativa del cloud e fornita sotto forma di servizio SaaS. Per la pianificazione della continuità aziendale e altri casi d'uso specifici, sono disponibili service edge privati e virtuali.
Privacy e conservazione dei dati	Quando si registrano i dati, il contenuto non viene mai scritto sul disco, ed esistono controlli granulari per determinare la posizione in cui 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 separati per reparto o funzione, in ottemperanza alle principali normative di conformità. I dati vengono conservati per un periodo variabile di sei mesi o inferiore, a seconda del prodotto. È possibile acquistare ulteriore spazio di archiviazione per estendere il periodo di conservazione dei dati a tutto il tempo desiderato.
Certificazioni di conformità principali	Le certificazioni includono: • FedRAMP • ISO 27001 • SOC 2 tipo II • SOC 3 • NIST 800-63C Consulta l'elenco completo delle nostre certificazioni di conformità qui.
Supporto granulare delle API	Gestiamo integrazioni delle 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 o on-premise (come Splunk). Scopri di più
Peering diretto	Il peering diretto con i principali provider di servizi Internet, app SaaS e cloud pubblici garantisce il percorso più rapido per il traffico.

FUNZIONALITÀ	DETTAGLI
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 o successivi • Android 8 o successivi • Windows 8 o successivi • Mac OS X 10.14 o successivi • CentOS 9 • Ubuntu 20.04 Scopri di più
Branch Connector	Supporto per: • VMware vCenter o vSphere Hypervisor • CentOS • Redhat

Zscaler Internet Access: diverse opzioni per iniziare

	PIATTAFORMA ESSENTIALS Inizia il tuo percorso zero trust con un accesso a Internet sicuro e affidabile e l'accesso privato limitato, insieme ad altre innovazioni di Zscaler.	PIATTAFORMA ZSCALER Ottieni la soluzione SASE/SSE completa che comprende tutti i servizi per l'accesso a Internet, l'accesso privato e la protezione dei dati.
SERVIZI DELLA PIATTAFORMA		
Inoltro del traffico – Client Connector, GRE, PAC, Proxy Chaining, IPsec	✓	✓
Più provider di identità (IdP), Accesso API, Profilo del dispositivo	✓	✓
Autenticazione – SAML, Secure LDAP, Kerberos	✓	✓
Ambiente di test ZS	–	–
Accesso ai DC pubblici di Zscaler	✓	✓
Accesso ai DC pubblici di Zscaler ad alto costo (Australia, Nuova Zelanda, Dubai [non regolamentato], Sud America, Africa, Corea del Sud, Taiwan e Cina continentale)	–	✓
Accesso ai DC Premium per la Cina e regolamentati in Medio Oriente	–	–
ACCESSO A INTERNET		
Filtraggio dei contenuti	✓	✓
Controllo del tipo di file	✓	✓
Ispezione TLS/SSL	✓	✓
Certificato privato SSL	✓	✓
Controllo della larghezza di banda	✓	✓
Trasmissione al SIEM on-premise (Nanolog Streaming Service con gestione diretta)	✓	✓
Cloud NSS (per >500 Utenti)	✓	✓
Ancoraggio agli IP di origine	–	✓
ZIA Private Service Edge – Dispositivo virtuale	–	✓
Hardware: ZIA Private Service Edge – 3 istanze, 5 istanze	–	–

PROTEZIONE DALLE MINACCE INFORMATICHE		
Protezione dalle minacce informatiche standard: Advanced Threat Protection, Sandbox Standard, Zero Trust Firewall Standard, Zero Trust Browser Standard	✓	✓
Antivirus e antispyware inline	✓	✓
Sandbox Advanced	–	–
Zero Trust Firewall Advanced	–	–
Zero Trust Browser Advanced (1,5 GB di traffico a utente al mese, misurato per tutti gli utenti di Zero Trust Browser)	–	–
Zero Trust Browser Unlimited (nessun limite di utilizzo del traffico)	–	–
PRIVATE ACCESS (ZPA)		
Accesso sicuro alle app private (su cloud, data center): streaming dei log, ancoraggio dell'IP di origine, IdP multiplo, monitoraggio dell'integrità)	1 utente ogni 20 abbonati (min. 500 utenti abbonati)	✓
App Connector	Quanti ne servono (fino al massimo del sistema)	Quanti ne servono (fino al massimo del sistema)
PROTEZIONE DEI DATI		
Protezione dei dati standard: Cloud App Control, report sullo Shadow IT, restrizioni della tenancy, inline web (modalità di monitoraggio), API SaaS (1 app), sicurezza della GenAI	✓	✓
Web inline e DLP per la GenAI, tutte le app (Internet e Private Access)	–	✓
GESTIONE DEL RISCHIO		
Gestione del rischio standard: deception standard	–	✓
ZERO TRUST PER I WORKLOAD		
Zero trust per i workload standard: filtraggio stateful, DNS, ispezione TLS	1 GB di traffico di workload al mese per utente abbonato	2 GB di traffico di workload al mese per utente abbonato
ESPERIENZA DIGITALE (ZDX)		
ZDX Standard: preconfigurato	✓	–
ZDX standard	–	✓
SUPPORTO		
Supporto standard	✓	✓
Supporto Plus	–	–

MODELLO DI LICENZA

Tutte le edizioni di Zscaler Internet Access hanno un prezzo per utente. Per alcuni prodotti all'interno dell'edizione della tua piattaforma, il prezzo potrebbe variare indipendentemente dal numero di utenti. Per maggiori informazioni sui prezzi, rivolgiti al team dedicato 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. Questa soluzione è 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.

La cosa fantastica di Zscaler è che fornisce tutto ciò che ricerchiamo da una piattaforma zero trust: ispezione scalabile del traffico SSL, altre funzionalità di prevenzione delle minacce e protezione dei dati.

NITIN NEGI
Senior Manager, Cybersecurity Engineering and Operations, Micron Technology

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. La piattaforma Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 160 data center a livello globale, Zero Trust Exchange™, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Per saperne di più, visita **www.zscaler.com/it** oppure seguici su x (precedentemente Twitter) **@zscaler**.

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

zscaler™

Zero Trust Everywhere