SCHEDA TECNICA

Zero Trust Cloud

Proteggi il traffico da workload a Internet e tra workload con la potenza di Zscaler Zero Trust Exchange™.

La trasformazione digitale sta portando alla creazione e all'utilizzo di workload attraverso numerose infrastrutture e ambienti on-premise, cloud privati e cloud pubblici. La tua azienda opera proprio grazie a questi workload; ecco perché prevenire gli attacchi informatici e la perdita dei dati è essenziale.

Le architetture legacy sono inadeguate: forniscono una protezione dei dati inaffidabile contro le minacce, estendono la superficie di attacco, favoriscono il movimento laterale e aumentano i costi operativi e la complessità.

Zscaler Zero Trust Cloud semplifica radicalmente la sicurezza dei workload ibridi. Grazie alla potenza della piattaforma Zero Trust Exchange, protegge il traffico da workload a Internet e tra workload in uscita attraverso cloud pubblici e data center on-premise per tutelare i workload e i server critici.

Zero Trust Cloud fornisce una protezione costante dei dati e contro le minacce, elimina la superficie di attacco, blocca il movimento laterale, riduce la complessità e abbatte i costi operativi.

> “Con Workload Communications di Zscaler, siamo in grado di standardizzare le policy di sicurezza con estrema facilità, sia per gli utenti che per le applicazioni, indipendentemente dalla loro ubicazione.”
>
> **Rui Cabeço,** IT Manager, Global Outbound Connectivity Lead, Siemens

Le sfide relative a workload legacy e sicurezza dei server

Molte aziende si affidano ad architetture legacy per proteggere i propri workload cloud. La maggior parte di esse adotterà una combinazione delle seguenti operazioni:

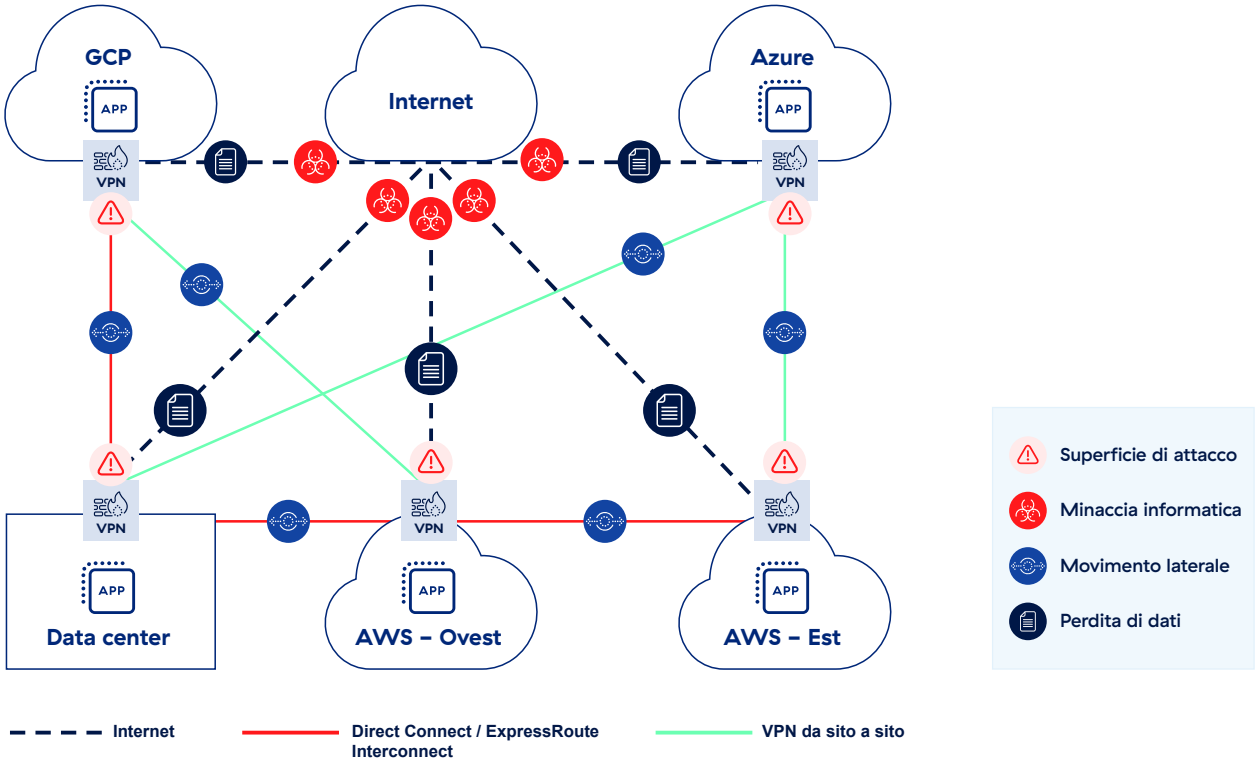
Configurazione di soluzioni di sicurezza native del cloud fornite da provider di servizi cloud pubblici

Implementazione di strumenti di terze parti (firewall, ispezione TLS/SSL, DLP, ecc.) per aggiungere ulteriori livelli di protezione

Backhauling del traffico verso infrastrutture di sicurezza di rete on-premise per l'ispezione e la protezione

L'utilizzo di questi metodi comporta diverse sfide, tra cui:

- **Aumento della superficie di attacco e della possibilità di movimento laterale.** Le soluzioni come i firewall estendono la rete a workload e server, amplificando così il rischio di movimento laterale, e ogni firewall rivolto a Internet aumenta la superficie di attacco, che può estendersi da Internet a cloud diversi e ambienti on-premise. Inoltre, un insieme di dispositivi virtuali, strumenti operativi e policy non standard introduce lacune note e sconosciute nella copertura della sicurezza, intensificando i rischi.
- **Lacune nella visibilità sul TLS.** Quando abilitata, l'ispezione TLS può richiedere un elevato numero di risorse informatiche e porre sfide come il peggioramento delle prestazioni. La gestione dei certificati distribuiti o l'applicazione di esclusioni ai workload bloccati crea sfide operative e spesso comporta un aumento dei costi dell'infrastruttura di sicurezza per supportare la scalabilità.
- **Maggiore complessità e prestazioni scadenti.** Dato che le soluzioni legacy per la rete e sicurezza non sono state create per supportare i workload sul cloud, è necessario implementare prodotti singoli come firewall virtuali, proxy e gateway NAT. Alcune soluzioni possono utilizzare VM separate per ogni funzione di sicurezza, con una conseguente ispezione sequenziale in stile catena di montaggio, che aumenta la latenza. Tutto questo crea notevoli complessità operative negli ambienti multicloud.
- **Costi elevati.** L'uso di dispositivi indipendenti legacy per la sicurezza e la rete (come firewall, IPS e router), il provisioning eccessivo delle infrastrutture di rete per compensare la mancanza di scalabilità e il maggiore utilizzo di servizi nativi del cloud contribuiscono ad aumentare capex e opex.
- **Mancanza di una gestione comune dei log.** Alcuni obblighi legali e normativi possono richiedere alle organizzazioni di archiviare i log per periodi prolungati. Accedere a questi registri da diversi ambienti cloud e archiviarli in un'infrastruttura SIEM centrale può risultare complesso e costoso.



Estendi l'architettura zero trust nei cloud pubblici e nei data center on-premise

Zero Trust Cloud elimina la superficie di attacco della rete collegando i workload e i server a Internet e alle applicazioni private con un'architettura zero trust. Si tratta di un cambiamento che semplifica notevolmente la connettività, riducendo la dipendenza della tua organizzazione da soluzioni legacy come i firewall, consentendo un inoltro flessibile e semplificando la gestione delle policy con il collaudato framework di Zscaler Internet Access™ (ZIA) e Zscaler Private Access™ (ZPA).

Tutto ciò è reso possibile dalla piattaforma Zero Trust Exchange, che opera su larga scala ed è in grado di gestire qualsiasi incremento dei workload o del traffico dei server con una scalabilità orizzontale flessibile. Con Zero Trust Cloud, tutto il traffico in uscita dei workload e dei server viene inoltrato a Zero Trust Exchange, dove si applicano le policy di sicurezza per l'ispezione TLS/SSL completa e il controllo degli accessi.

Il traffico in uscita viene quindi inoltrato direttamente alla relativa destinazione, come Internet, applicazioni SaaS o altri workload e server ospitati in cloud pubblici o data center.

Con Zero Trust Cloud puoi:

Ottenere una protezione coerente e integrale dei dati e contro le minacce

Applica policy di sicurezza comuni a tutti gli ambienti

- Previeni gli attacchi O-day con l'ispezione TLS su scala cloud e la protezione dalle minacce
- Ferma la perdita dei dati con l'ispezione DNS e la protezione dei dati inline
- Limita il numero di destinazioni a cui i workload e i server possono accedere tramite controlli rigorosi

Eliminare la superficie di attacco e il movimento laterale

Connetti le app e non le reti per evitare il rilevamento

- Applica l'accesso a privilegi minimi ai workload dei segmenti utilizzando IP, FQDN, VPC, VNet o tag
- Connetti i workload utilizzando Zero Trust Exchange ed elimina la superficie di attacco della rete
- Supporta il passaggio da cloud a cloud, da cloud a data center, da regione a regione

Ridurre la complessità operativa e i costi

Utilizza un'unica piattaforma fornita sul cloud per proteggere tutti i workload

- Proteggi i workload su tutti i principali provider di servizi cloud, tra cui AWS, Azure e GCP, con un'unica piattaforma
- Automatizza le distribuzioni sicure tramite interfacce programmabili con modelli IaC (Infrastructure as Code)
- Utilizza le integrazioni dei cloud pubblici, come il bilanciatore di carico del gateway, i tag definiti dall'utente e il ridimensionamento automatico di AWS

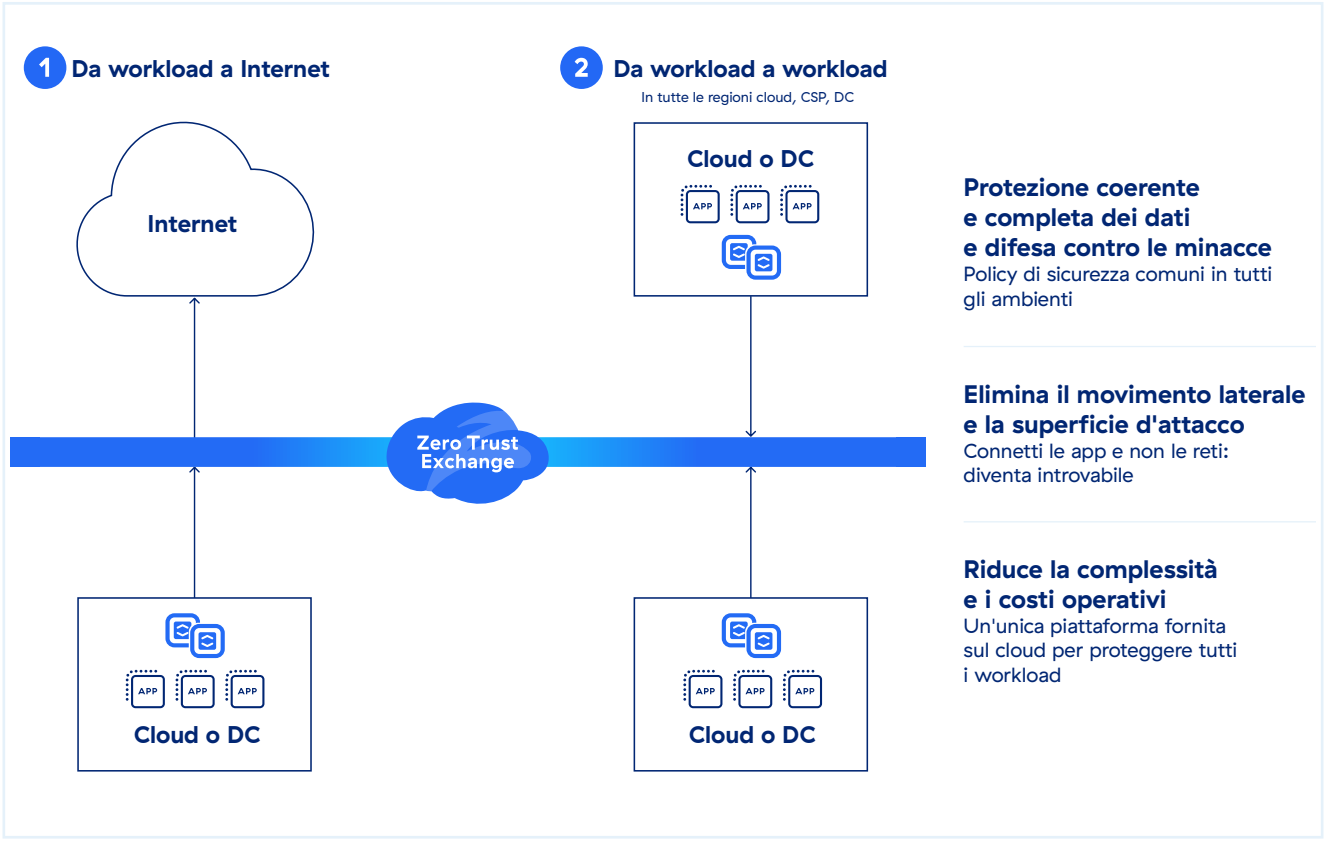


FIGURA Zscaler Zero Trust for Workloads

Le funzionalità di Zero Trust Cloud

Zero Trust Cloud si basa su Zero Trust Exchange, che connette in modo sicuro utenti, dispositivi e app utilizzando policy aziendali su qualsiasi rete e in qualsiasi cloud su larga scala.

Architettura proxy zero trust: la nostra architettura proxy multitenant si colloca inline e permette di connettere in modo sicuro origini e destinazioni, garantendo al contempo la massima visibilità sul traffico in uscita.

Decifrazione TLS su scala cloud: l'ispezione ad alte prestazioni viene eseguita da un'architettura Single-Scan, Multi-Access (multi-accesso a scansione singola), creata per essere scalabile.

Segmentazione granulare da app ad app: l'accesso a privilegi minimi e zero trust per tutti i workload e i server semplifica l'applicazione e la gestione delle policy aziendali.

Ispezione bidirezionale delle minacce: la protezione dalle minacce supportata dall'AI e basata su 500 bilioni di segnali e 320 miliardi di transazioni ogni giorno offre una protezione da ransomware, minacce 0-day e malware sconosciuti sempre attiva e completa.

Protezione dei dati inline: ispezione DLP scalabile e ad alte prestazioni per tutti i canali e le sedi

Piattaforma consolidata che supporta gli ambienti multicloud: una piattaforma unificata fornisce gestione delle policy, monitoraggio del traffico e tracciamento dei log, con policy standardizzate che vengono applicate su AWS, Azure, GCP e sui data center on-premise.

Le funzioni di Zero Trust Cloud

PIATTAFORMA ZSCALER ZERO TRUST CLOUD	
FUNZIONALITÀ	**DETTAGLI**
Copertura per il cloud pubblico e gli ambienti on-premise	Supporta la protezione dei workload nelle regioni AWS, Microsoft Azure, Google Cloud Platform, Microsoft Azure Cina e AWS GovCloud con supporto aggiuntivo per i server dei data center on-premise. Certificazione FedRamp per AWS GovCloud.
Ispezione TLS/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 conformità.
Streaming dei log	Consolida i log di tutti i workload e server a livello globale in un repository centrale definito dalla tua organizzazione con Zscaler Nanolog Streaming Service. Gli amministratori possono visualizzare ed estrarre i dati sulle transazioni dai workload cloud in tempo reale.
Infrastructure as Code	Zscaler fornisce modelli e provider Terraform che automatizzano il provisioning e la distribuzione di policy di sicurezza e macchine virtuali di connettori cloud.
Supporto alla connettività	Sfrutta IPsec, GRE o Cloud Connector per indirizzare il traffico in uscita dei workload verso Zero Trust Exchange. IPsec e GRE proteggono il traffico tra workload e Internet. I Cloud Connector vengono utilizzati per proteggere sia il traffico Internet che quello dei workload.

ZSCALER INTERNET ACCESS PER I WORKLOAD SU INTERNET	
FUNZIONALITÀ	**DETTAGLI**
Comunicazione da workload a Internet Protezione	Previeni le minacce informatiche e la perdita dei dati nelle comunicazioni tra workload e Internet. Include ispezione SSL, IPS, filtraggio degli URL e protezione dei dati per tutte le comunicazioni.
Filtro URL	Concedi, blocca, limita o isola l'accesso dei workload a categorie o destinazioni web specifiche per fermare le minacce web e garantire la conformità alle policy dell'organizzazione.
Minacce avanzate – Protezione	Impedisci gli attacchi informatici avanzati, come malware, ransomware, attacchi alla catena di approvvigionamento e altro, grazie alla protezione dalle minacce avanzate con tecnologia proprietaria. Imposta policy granulari basate sulla tolleranza al rischio dell'organizzazione.
Analisi dei malware	Rileva, previeni e metti in quarantena le minacce sconosciute che si nascondono nei payload dannosi inline con le tecnologie avanzate di AI/ML per bloccare gli attacchi da paziente zero.
Prevenzione delle intrusioni	Ottieni una protezione completa da minacce come botnet, minacce avanzate e O–day e ricevi informazioni contestuali sui workload. L'IPS cloud e web funziona in modo ottimale con firewall, sandbox e DLP.
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.
Filtro DNS	Controlla e blocca le richieste DNS in base alle destinazioni conosciute e nocive.
Controllo dei file	Blocca o consenti il download/upload di file dalle applicazioni in base all'identità del workload o all'applicazione.
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.
Policy di accesso e sicurezza dinamiche basate sul rischio	Adatta automaticamente le policy di sicurezza e di accesso al rischio associato a workload, server, destinazioni Internet e contenuti.
Informazioni correlate sulle minacce	Accelera le indagini e i tempi di risposta grazie ad avvisi contestualizzati e correlati contenenti informazioni approfondite sul punteggio assegnato alle minacce, le risorse colpite, la gravità e molto altro.
Filtraggio dei contenuti e regole stateful	Filtra le policy tra 6 classi, 101 categorie e 29 supercategorie. Approfitta della classificazione dinamica dei contenuti per URL sconosciuti e ricerca sicura. Applica policy granulari basate su indirizzo IP, gruppi e identità ospitate.

ZSCALER PRIVATE ACCESS DA WORKLOAD A WORKLOAD	
FUNZIONALITÀ	**DETTAGLI**
Segmentazione da workload a workload	Proteggi la connettività e le comunicazioni tra workload in ambienti ibridi e multicloud.
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 app private dell'azienda e sulla superficie di attacco potenziale.
Segmentazione delle app basata sull'AI	Applica la segmentazione consigliata in base al machine learning che ti viene suggerita in automatico su ZPA per semplificare e accelerare l'identificazione dei corretti segmenti di app e la creazione di policy di accesso adeguate. La segmentazione basata sull'ML può aiutarti a ridurre al minimo la superficie di attacco interna grazie a modelli di ML in continuo aggiornamento e basati su milioni di segnali dei clienti e sui pattern di accesso specifici alle applicazioni.
Protezione delle app	Proteggi le applicazioni e le infrastrutture private dagli attacchi più diffusi grazie all'ispezione di sicurezza inline ad alte prestazioni di tutti i payload delle applicazioni per rilevare le minacce. Inoltre, identifica e blocca i rischi di sicurezza web noti, come quelli della OWASP Top 10 e le vulnerabilità 0-day emergenti che sono in grado di aggirare i tradizionali controlli di sicurezza della rete.

PROTEZIONE DEI DATI	
FUNZIONALITÀ	**DETTAGLI**
Protezione dati inline (dati in movimento)	Per le comunicazioni da workload a Internet e tra workload diversi, utilizza le funzionalità proxy di inoltro e ispezione SSL per controllare in tempo reale il flusso delle informazioni sensibili verso destinazioni web rischiose e applicazioni cloud, e blocca le minacce interne ed esterne. La protezione avanzata inline viene fornita indipendentemente dal fatto che un'applicazione sia autorizzata o non gestita, senza la necessità dei log dei dispositivi di rete.
Exact Data Match (EDM)	Impronte digitali e dati aziendali personalizzati e sicuri.
IDM (Index Document Matching)	Usa il fingerprinting per documenti e moduli sicuri e personalizzati.
Riconoscimento ottico dei caratteri (OCR)	Individua e previeni la perdita di dati che può verificarsi con immagini e screenshot.

(Le capacità elencate non sono esaustive. Alcune funzionalità e capacità specifiche potrebbero essere disponibili solo con determinate edizioni di Zscaler).

EDIZIONI ZSCALER ZERO TRUST CLOUD	
NOME DELL'EDIZIONE	**FUNZIONALITÀ**
Zero Trust for Workloads Standard	• Abbonamento annuale a 1 GB di traffico mensile per Zero Trust for Workloads Standard: • Include filtraggio stateful e Cloud Connector
Zero Trust for Workloads Advanced	• Tutto ciò che è disponibile nell'edizione Workloads Standard • Internet Access for Workloads: ispezione SSL/TLS, protezione dalle minacce avanzate, Cloud NSS, ancoraggio IP sorgente • Private Access for Workloads: segmenti di app, posizioni secondarie, logging LSS standard e reportistica • Data Protection for Workloads: web inline (solo in modalità monitoraggio) • Cyber Protection for Workloads: firewall standard, controllo DNS
Zero Trust for Workloads Advanced Plus	• Tutto ciò che è disponibile nell'edizione Workloads Advanced • Data Protection for Workloads: protezione dei dati inline e classificazione avanzata • Cyber Protection for Workloads: Firewall Advanced for Workloads, Sandbox Advanced for Workloads

zscaler™ | Experience your world, secured.™

Informazioni su Zscaler
Zscaler (NASDAQ: ZS) accelera la trasformazione digitale, in modo che i clienti possano essere più agili, efficienti, resilienti e sicuri. Zscaler Zero Trust Exchange protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati grazie alla connessione sicura di utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in più di 150 data center nel mondo, Zero Trust Exchange, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.com/it** o seguici su X (precedentemente Twitter) **sull'account @zscaler**.

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