Zero Trust Cloud

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

SCHEDA TECNICA

La trasformazione digitale sta portando alla creazione e all'utilizzo dei workload attraverso numerosi ambienti, che includono data center on-premise e cloud privati e pubblici. Il business dipende da questi workload, e prevenire gli attacchi informatici e la perdita dei dati è quindi essenziale.

Le architetture legacy, come firewall e VPN, sono inadeguate, in quanto forniscono una tutela dei dati e una protezione contro le minacce inaffidabili, 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, questa soluzione protegge il traffico tra workload e tra workload e Internet su data center on-premise e cloud privati e pubblici.

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.

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 adotta una combinazione delle seguenti operazioni:

- Configurazione di soluzioni di sicurezza native del cloud fornite da provider di servizi cloud
- Distribuzione di strumenti di terze parti come firewall, ispezione TLS, DLP e altro
- 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:

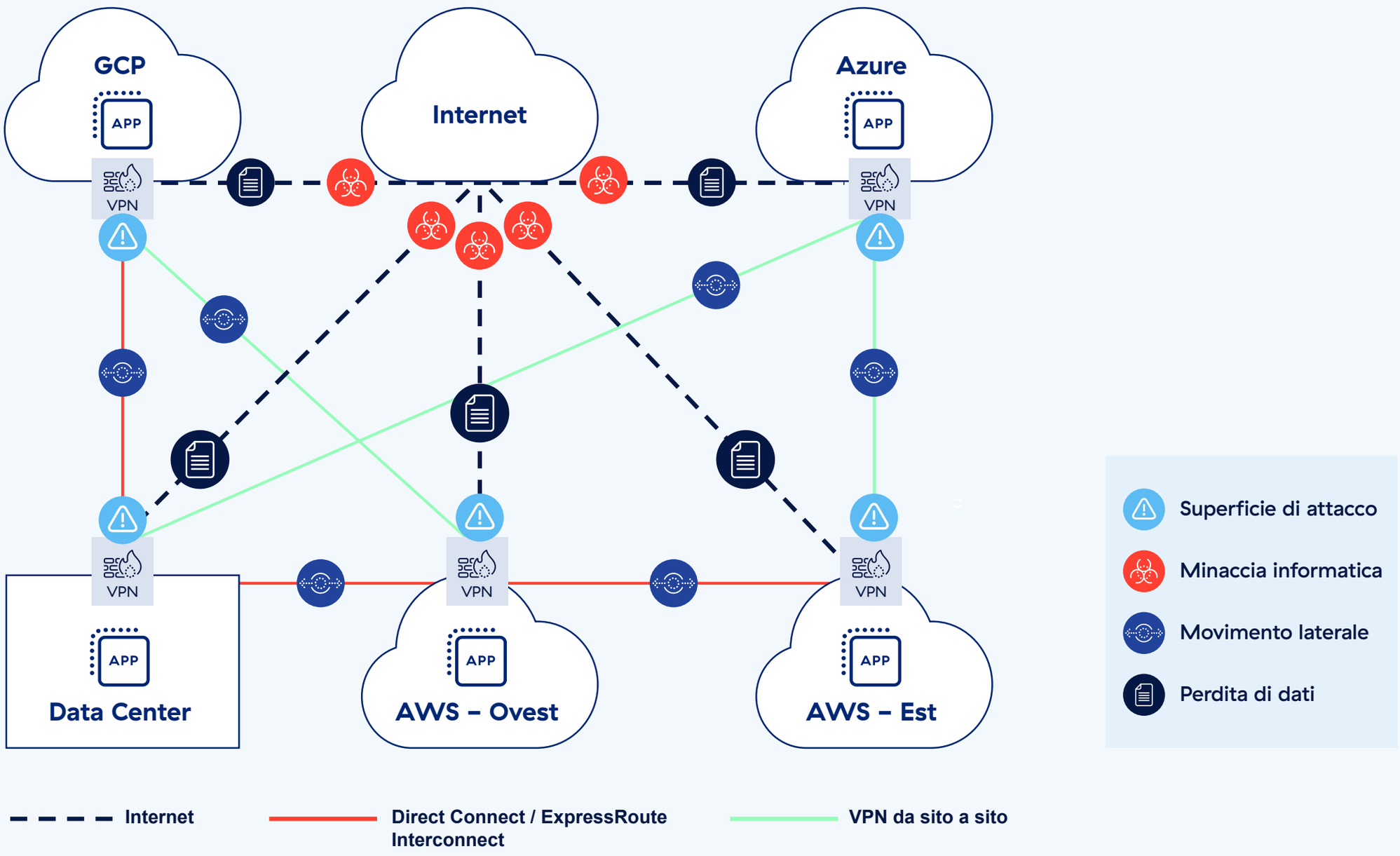
- **Aumento della superficie di attacco e della possibilità di movimento laterale:** soluzioni come i firewall estendono la rete ai workload, amplificando i rischi di subire il movimento laterale. Ogni firewall che si interfaccia con Internet incrementa inoltre la superficie di attacco, che può estendersi da Internet ad ambienti cloud e on-premise differenti. Inoltre, l'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 causare la riduzione delle prestazioni. Inoltre, la gestione di certificati distribuiti o l'applicazione di esclusioni ai workload incrementa la complessità dal punto di vista

operativo, e a ciò si aggiunge il fatto che l'ispezione TSL su larga scala comporta un incremento dei costi dell'infrastruttura e delle operazioni.

- **Maggiore complessità e prestazioni scadenti:** dato che le soluzioni legacy per la rete e la sicurezza non sono progettate per supportare i workload sul cloud, è necessario implementare altri prodotti come firewall virtuali, proxy e gateway NAT. Alcune soluzioni possono utilizzare VM separate per ogni funzione di sicurezza, generando di conseguenza un'ispezione sequenziale in stile catena di montaggio, che aumenta la latenza. Questo approccio crea notevoli complessità operative, in particolare quando applicato ad ambienti multicloud.

- **Costi elevati:** l'utilizzo di prodotti legacy per la sicurezza della rete, come firewall e VPN, comporta un sovradimensionamento dell'infrastruttura, e l'implementazione di strumenti di sicurezza nativi del cloud su più CSP richiede risorse altamente specializzate.

- **Archiviazione inefficiente dei log.** Alcuni obblighi legali e normativi possono richiedere alle organizzazioni di archiviare i log per periodi prolungati. Accedere a tali registri da diversi ambienti cloud e archiviarli in un'infrastruttura SIEM centralizzata può risultare complesso e oneroso.



Estendere l'architettura zero trust ai data center on-premise e ai cloud privati e pubblici

Zero Trust Cloud elimina la superficie di attacco della rete, collegando i workload e i server a Internet e alle applicazioni private tramite un'architettura zero trust. Si tratta di un cambiamento radicale che semplifica notevolmente la connettività, riducendo la dipendenza dell'organizzazione da soluzioni legacy come i firewall e le VPN, 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 possibile grazie alla visibilità completa offerta dalla piattaforma Zero Trust Exchange. Con Zero Trust Cloud, tutto il traffico dei workload viene inoltrato a Zero Trust Exchange, dove vengono applicate le policy di sicurezza per l'ispezione TLS/SSL completa e il controllo degli accessi. Il traffico in uscita viene quindi inoltrato alla relativa destinazione, come Internet, applicazioni SaaS o altri workload ospitati in data center on-premise o su cloud privati o pubblici.

Con Zero Trust Cloud puoi:

OTTENERE UNA PROTEZIONE COERENTE E INTEGRALE DEI DATI E CONTRO LE MINACCE

Applica policy di sicurezza uniformi per data center on-premise, cloud privati e cloud pubblici

- 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 possono accedere implementando controlli rigorosi

ELIMINARE LA SUPERFICIE DI ATTACCO E IL MOVIMENTO LATERALE

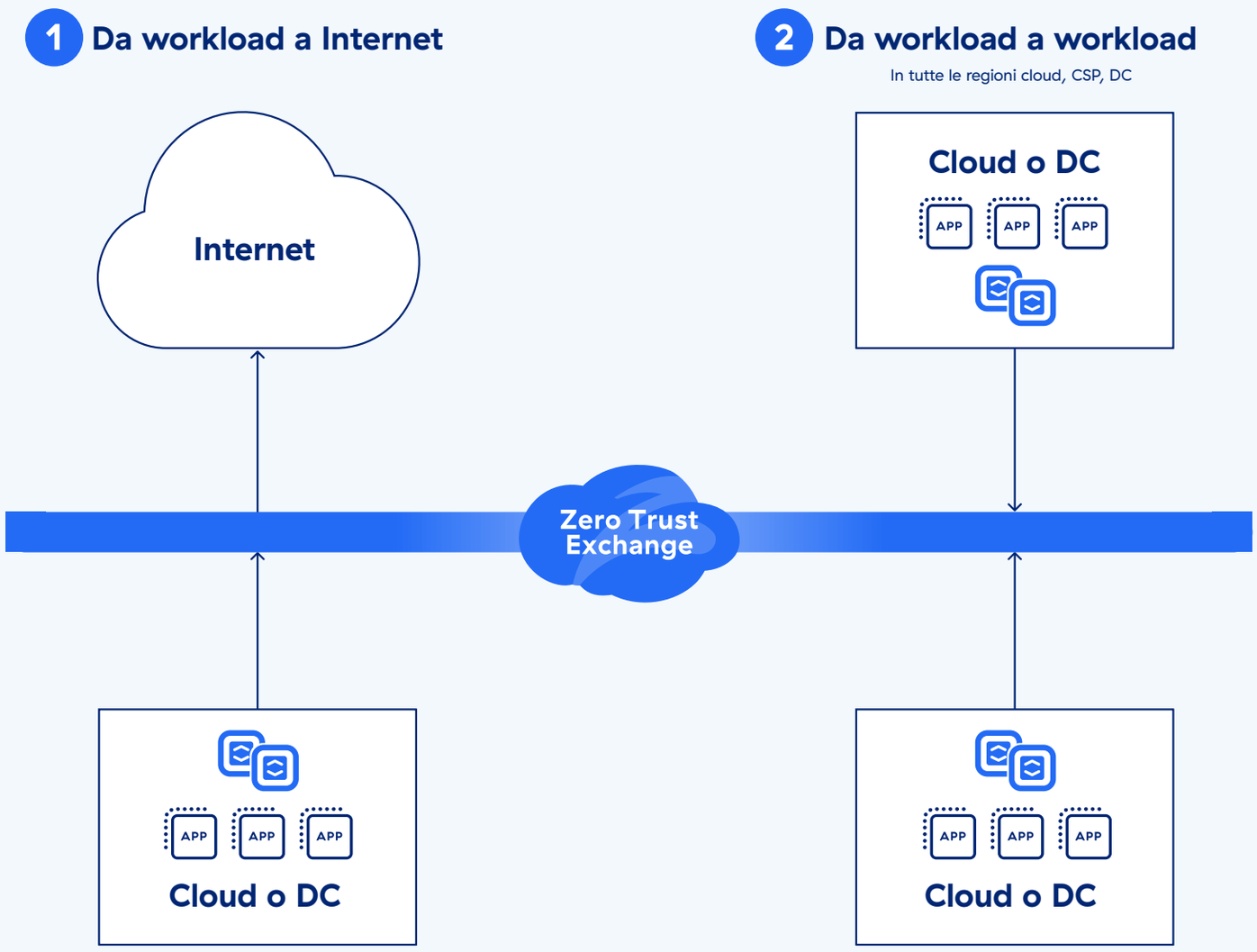
Connetti le app (e non le reti) per evitare il rilevamento

- Applica l'accesso a privilegi minimi ai workload dei segmenti utilizzando IP, FQDN, VPC, VNet o tag definiti dagli utenti
- Connetti i workload utilizzando Zero Trust Exchange ed elimina la superficie di attacco della rete
- Usufruisci del supporto da cloud a cloud, da cloud a data center, da regione a regione, da VPC/VNet a VPC/VNet e da sottorete a sottorete

RIDURRE LA COMPLESSITÀ OPERATIVA E I COSTI

Utilizza un'unica piattaforma di sicurezza per proteggere tutti i workload sui vari cloud

- Proteggi i workload su tutti i principali provider di servizi cloud, tra cui AWS, Azure e GCP, con un'unica piattaforma
- Automatizza le distribuzioni di sicurezza tramite interfacce programmabili, tra cui API Zscaler, Hashicorp Terraform e AWS CloudFormation
- Usa le integrazioni predefinite con i CSP per scalare l'infrastruttura, ottimizzare i percorsi cloud e semplificare le definizioni delle regole con i metadati cloud



Tutela dei dati e protezione contro le minacce uniformi
Policy di sicurezza comuni in tutti gli ambienti

Elimina il movimento laterale e la superficie d'attacco.
Connetti le app e non le reti: diventa introvabile.

Riduce la complessità e i costi operativi
Un'unica piattaforma fornita sul cloud per proteggere tutti i workload

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 (multiaccesso 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: con una protezione dalle minacce basata sull'AI che usa 500 bilioni di segnali giornalieri e 320 miliardi di transazioni elaborate ogni giorno, per garantire una protezione sempre attiva e solida dai ransomware, la prevenzione delle minacce O-day e la difesa contro i malware sconosciuti.

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**
Ambienti on-premise e cloud privati e pubblici	Supporta la protezione dei workload su AWS, Microsoft Azure, Google Cloud Platform e nei data center on-premise. Supporta regioni specializzate tra cui Microsoft Azure China e AWS China. Supporta inoltre AWS GovCloud e Microsoft Azure GovCloud, con certificazioni FedRAMP di livello “moderate” e “high” per entrambi.
Ispezione TLS/SSL	Offre un’ispezione illimitata del traffico TLS/SSL che consente di bloccare la perdita dei dati e identificare le minacce che si nascondono nel traffico cifrato. Permette inoltre di specificare le categorie web o le app da ispezionare in base ai requisiti di privacy o di conformità.
Segmentazione intra-regionale	Protegge i workload tramite la segmentazione tra VPC o tra sottoreti all’interno di una specifica regione cloud. Supporta inoltre i tag di origine e destinazione nelle policy di inoltro del traffico est-ovest.
Streaming dei log	Consolida i log dei workload e dei server, a livello globale, in un repository centralizzato determinato dall’organizzazione. Gli amministratori hanno la possibilità di visualizzare ed estrarre i dati sulle transazioni dai workload cloud.
Infrastructure as Code	Automatizza le distribuzioni delle soluzioni di sicurezza tramite interfacce programmabili, tra cui le API di Zscaler, Hashicorp Terraform e AWS CloudFormation.
Supporto alla connettività	Utilizza connettori appositamente creati o pacchetti di servizi gestiti da Zscaler per indirizzare il traffico. In più, offre la possibilità di usare i tunnel IPsec o GRE esistenti.

ZSCALER INTERNET ACCESS PER I WORKLOAD DIRETTI A INTERNET	
FUNZIONALITÀ	**DETTAGLI**
Protezione delle comunicazioni da workload a Internet	Previene le minacce informatiche e la perdita dei dati nelle comunicazioni tra workload e Internet. Include l’ispezione SSL, IPS, il filtraggio degli URL e la protezione dei dati per tutte le comunicazioni.
Filtro URL	Concede, 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 aziendali.
Protezione dalle minacce avanzate	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 e sulle 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 dinamiche di accesso e sicurezza basate sul rischio	Adatta automaticamente le policy di sicurezza e di accesso al rischio associato a workload, server, destinazioni Internet e contenuti.
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, 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 che ti viene suggerita in automatico su ZPA dal machine learning 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 l'OWASP Top 10 e le vulnerabilità O-day emergenti che sono in grado di aggirare i controlli di sicurezza della rete tradizionali.

PROTEZIONE DEI DATI	
FUNZIONALITÀ	**DETTAGLI**
Protezione dei 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. Le funzionalità e capacità specifiche potrebbero essere disponibili solo con alcune edizioni di Zscaler).

EDIZIONI ZSCALER ZERO TRUST CLOUD	
LIVELLO DELL'EDIZIONE	**FUNZIONALITÀ**
Zero Trust for Workloads Standard	• Abbonamento annuale per GB (gigabyte) di traffico mensile per Zero Trust for Workloads Standard: • Include il filtraggio dei contenuti
Zero Trust for Workloads Advanced	• Tutto ciò che è disponibile nell'edizione Workloads Standard • Internet Access per 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 • Segmentazione est–ovest
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

Zero Trust Cloud è disponibile in due opzioni di distribuzione. Con l'opzione Macchina Virtuale (VM), i clienti ottengono il controllo completo della propria infrastruttura cloud distribuendo i componenti sotto forma di macchine virtuali. Con Zero Trust Gateway, i clienti possono usufruire delle funzionalità sotto forma di servizio nativo del cloud completamente gestito da Zscaler. Entrambe le modalità di distribuzione offrono le medesime funzionalità. Zero Trust Gateway è disponibile nelle edizioni Zero Trust for Workloads Advanced e Zero Trust for Workloads Advanced Plus.

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