



# Zscaler Cloud Firewall

Una protezione zero trust sicura e adattiva per tutto il traffico Internet

**Zscaler Cloud Firewall protegge il traffico Internet di ogni utente, applicazione e posizione.**

Oggi, il mondo del lavoro è distribuito e mobile. Le applicazioni si spostano dai data center al cloud, mentre i nuovi carichi di lavoro digitali vengono sempre più spesso distribuiti in modo nativo sul cloud. Inoltre, gli utenti che lavorano da varie sedi, tra cui uffici domestici, ambienti di lavoro condivisi, filiali e da remoto, accedono alle applicazioni aziendali direttamente da Internet.

Questo significa che utenti e applicazioni cloud producono grandi volumi di traffico. Le regole di sicurezza tradizionali incentrate sulla rete falliscono nel gestire la larghezza di banda aggiuntiva dovuta al backhauling del traffico Internet e SaaS prodotto dagli utenti, e influiscono negativamente sulla produttività creando colli di bottiglia nella connettività. I firewall virtuali cercano di risolvere questa problematica, ma sono limitati alle sedi fisiche dei provider di servizi cloud e, spesso, richiedono risorse aziendali dedicate per essere amministrati correttamente. Ad aggravare questo scenario si aggiungono gli utenti malintenzionati, che utilizzano la crittografia e le porte non standard per eludere il rilevamento e lanciare attacchi alle reti delle vittime.

## I vantaggi di Zscaler Cloud Firewall:

- **Protezione completa per gli utenti che lavorano da qualsiasi luogo.**  
Le policy di sicurezza dinamiche, basate sul rischio, seguono gli utenti ovunque, senza una complessa matrice di policy e configurazioni di rete.
- **Ispezione completa per rilevare gli attacchi nascosti.**  
L'ispezione del traffico inline illimitata e la decriptazione SSL nativa terminano le connessioni dannose e bloccano le minacce.
- **Rilevamento del traffico web elusivo sulle porte non standard.**  
È possibile identificare e intercettare rapidamente le minacce informatiche elusive e criptate che si nascondono nel traffico delle porte non standard.
- **Punti di accesso a Internet locali forniti sul cloud.**  
Connessioni dirette a Internet rapide e sicure per tutto il traffico ibrido e delle filiali, scalabili in modo elastico e in grado di migliorare l'esperienza degli utenti.
- **Sistema di prevenzione delle intrusioni cloud sempre attivo.**  
Firme IPS comportamentali adattive, gestite da Zscaler ThreatLabz, che funzionano in tempo reale e sono facili da condividere, per arricchire i flussi di lavoro di SecOps.
- **Protezione dei DNS senza compromettere le prestazioni.**  
La risoluzione delle problematiche a livello locale consente di migliorare le prestazioni, mentre gli utenti e gli endpoint rimangono al sicuro dai siti dannosi e dal tunneling DNS.
- **Protezione fornita sul cloud con presenza all'edge a livello globale.**  
Zscaler Cloud Firewall offre sicurezza ed esperienza utente senza pari, è completamente integrato in Zscaler Internet Access™ e fa parte di Zero Trust Exchange™ di Zscaler.

Per ispezionare completamente il traffico criptato con SSL e il traffico che attraversa le porte e i protocolli non standard, i team di rete e sicurezza, spesso, si trovano a dover sacrificare le prestazioni e la velocità.

Ma i firewall fisici raggiungono presto i loro limiti di capacità, e si rivelano incapaci di ispezionare del tutto il traffico criptato con SSL o porte e protocolli non standard senza risorse supplementari che influiscono negativamente sulle prestazioni. I firewall virtuali, invece, sono limitati alle sedi fisiche dei provider di servizi cloud, e richiedono spesso risorse aziendali dedicate affinché possano essere amministrati correttamente.

## Zscaler Cloud Firewall

Per migliorare la connettività e la disponibilità, le organizzazioni devono indirizzare in modo sicuro il traffico degli utenti utilizzando punti di accesso a Internet locali, senza effettuare il backhauling tramite VPN e senza duplicare il set di apparecchi di sicurezza in ogni sede. **Zscaler Cloud Firewall** consente al traffico Internet di uscire localmente e in modo sicuro, per tutte le porte e i protocolli.

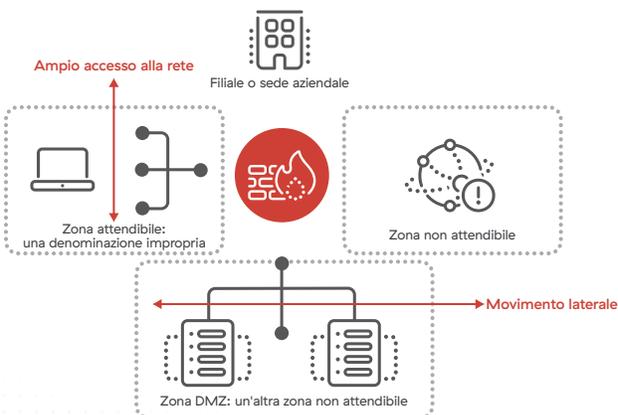
Instradando le connessioni Internet e SaaS verso Zscaler, il firewall cloud-gen ispeziona in modo nativo tutto il traffico degli utenti, compreso quello criptato con SSL, e garantisce elasticità e scalabilità per la gestione di volumi elevati di connessioni a lunga durata.

Dato che non sussiste più la necessità di rinnovare e aggiornare hardware e software, per il firewall basato su cloud la responsabilità di eseguire aggiornamenti e upgrade e di applicare patch, e la responsabilità di garantire la scalabilità, ricadono su Zscaler. Eliminando le complesse matrici di policy e le configurazioni di rete legate alle sedi fisiche, la gestione delle policy dei firewall si semplifica radicalmente. Grazie a policy adattive basate sul rischio, che seguono gli utenti ovunque, all'interno e all'esterno della rete aziendale, Zscaler Cloud Firewall offre una protezione coerente indipendentemente dal dispositivo o dal luogo in cui si effettua la connessione.

Nell'ambito della funzionalità firewall, Zscaler Cloud Firewall registra ogni sessione per fornire visibilità su tutti gli utenti e le posizioni, e ti garantisce l'accesso alle informazioni necessarie proprio quando ne hai bisogno.

## Lo zero trust con il firewall cloud-gen

### Architettura zonale del firewall legacy



### Piattaforma zero trust di Zscaler



Zscaler trasforma la connettività ibrida e delle filiali e fornisce una soluzione alle esigenze di sicurezza, garantendo scalabilità per soddisfare le tue esigenze di trasformazione cloud e il passaggio all'utilizzo di applicazioni sul cloud, come Microsoft 365.

## I vantaggi del firewall cloud-gen

Realizzato appositamente per il mondo digitale di oggi, Zscaler Cloud Firewall garantisce l'accesso sicuro a Internet e la gestione di tutto il traffico web e non web, su tutte le porte e i protocolli, con una scalabilità elastica senza limiti e prestazioni imbattibili. Gli utenti possono usufruire di una protezione coerente, indipendentemente dal dispositivo utilizzato o dalla loro posizione, che sia a casa, nelle sedi centrali, nelle filiali o in viaggio, senza incorrere nei costi, nella complessità e nei limiti prestazionali dei tradizionali apparecchi firewall di nuova generazione.

### Supportato da una piattaforma adattiva zero trust

Basta con le compromissioni che derivano da ispezioni statiche, dalla riduzione delle prestazioni e dai limiti di capacità dagli apparecchi firewall fisici. Basato su una piattaforma completamente integrata e nativa del cloud, Zscaler Cloud Firewall si adatta in modo elastico per gestire il traffico

delle applicazioni cloud che richiedono connessioni di lunga durata mentre intercetta e ispeziona in modo nativo il traffico SSL/TLS, su larga scala, per rilevare i malware nascosti nel traffico criptato.

### Connessioni trasformatrici ibride e per le filiali

Abbandona le infrastrutture costose e incentrate sulla rete e passa a punti di accesso a Internet locali, distribuiti sul cloud. Il traffico Internet viene instradato localmente per fornire connessioni dirette al cloud e per instaurare connessioni sempre veloci, offrendo al contempo controlli di sicurezza e degli accessi per tutte le porte e i protocolli. Senza la necessità di distribuire o gestire appliance, è possibile ridurre i costi di backhauling MPLS ed eliminare la gestione delle patch, il coordinamento delle interruzioni e la gestione delle policy, tutte attività costose e dispendiose in termini di tempo.

### Sicurezza onnipresente per la forza lavoro moderna

Sfruttando aggiornamenti di sicurezza in tempo reale basati su 300 bilioni di segnalazioni giornaliere e condivisi in tutto il cloud ogni giorno, è possibile usufruire della stessa protezione su qualsiasi dispositivo e da qualsiasi posizione: uffici domestici, ambienti di lavoro condivisi, filiali o in viaggio. Portando l'intero set di servizi di sicurezza vicino agli utenti, puoi offrire loro una protezione dalle minacce impareggiabile basata su app e utenti, con policy dinamiche in grado di seguirli dentro e fuori dalla rete aziendale.

# Gartner

Zscaler è stata nominata azienda leader nel MQ di Gartner per il Security Service Edge, posizionandosi al vertice per capacità di esecuzione.

Per saperne di più →

### **Protezione sempre attiva per bloccare gli attacchi dannosi conosciuti**

Sfruttando una protezione dalle intrusioni fondata su un IPS (Intrusion Prevention System) con base cloud e sensibile al contesto, gestita da Zscaler ThreatLabz, è possibile arrivare anche dove le soluzioni tradizionali falliscono. Attraverso un'ispezione illimitata del traffico inline, tra cui IoT/OT e traffico criptato all'interno e all'esterno della rete, le firme IPS comportamentali vengono applicate in tempo reale quando si effettua l'accesso a migliaia di applicazioni web e non web, indipendentemente dal tipo di connessione o dalla posizione.

### **Ottimizzazione dei DNS per prestazioni e sicurezza**

Risolvi più rapidamente le problematiche abbinando le app locali a livello geografico, migliora l'esperienza utente e le prestazioni delle app cloud, e implementa policy di controllo e sicurezza DNS. In questo modo, proteggi gli utenti dai domini dannosi e impedisce il tunneling DNS. Distribuendo il DNS come servizio, Zscaler riduce al minimo la latenza e protegge i punti di accesso a Internet locali, utilizzando proxy completi per tutto il traffico DNS e utilizzando il machine learning per rilevare e bloccare l'attività dei tunnel di esfiltrazione dei dati.

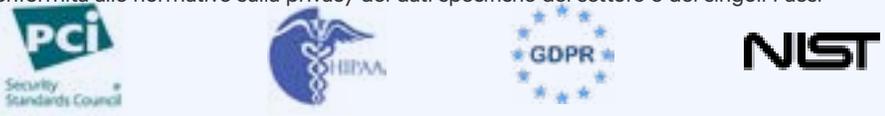
### **Gestione delle policy facile da comprendere**

Definisci, implementa e applica immediatamente policy per tutti gli utenti, in tutte le posizioni e da un'unica console. Al posto di complesse matrici di policy e configurazioni di rete e invece di ricreare policy per ciascuna posizione dei firewall, il firewall cloud-gen semplifica la gestione centralizzando regole granulari in base a utenti, applicazioni, posizione, gruppi e reparti. Inoltre, gli amministratori possono inviare log di analisi completi di dettagli su utenti, richieste, risposte, servizi utilizzati e altro ancora agli strumenti SIEM e XDR, per migliorare le indagini sulla sicurezza e la risposta agli incidenti.

## **Caratteristiche principali del firewall cloud-gen**

<b>Gestione centralizzata delle policy</b>	Definisci e applica immediatamente le policy in tutte le sedi, senza doverle ricreare per ogni sede
<b>Servizi di sicurezza completamente integrati</b>	Le informazioni contestuali vengono condivise su DLP, APT, sandbox e altri servizi per fornire una migliore protezione e una maggiore visibilità
<b>Controllo granulare, logging e visibilità in tempo reale</b>	Creazione di log ricchi di informazioni, unificati a livello globale e illimitati per sei mesi, per fornire una visibilità dettagliata e consentire l'analisi e la correlazione, per scoprire tendenze, analisi della produttività e facilitare la risoluzione dei problemi
<b>Protezione dalle minacce in base all'utente</b>	Gli utenti vengono definiti per gruppi, reparti o sedi, indicando anche se lavorano da casa o da remoto, e i dati estrapolati vengono integrati con i provider di identità e i database degli utenti locali, per applicare policy uniformi indipendentemente dalla posizione fisica.

## Caratteristiche principali del firewall cloud-gen (cont.)

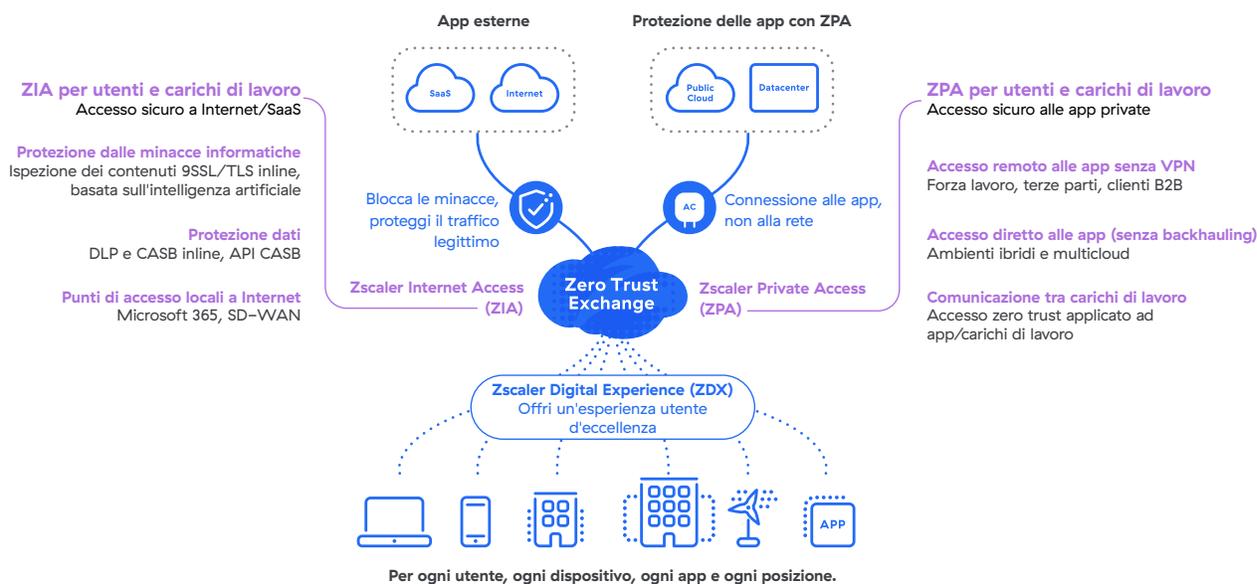
<p><b>Protezione dalle minacce in base alle app</b></p>	<p>Identificazione e classificazione delle app al primo pacchetto, per abilitare policy di firewall di filtraggio e inoltra e intraprendere azioni immediate e con priorità più alta, con policy adattative e basate sul contesto</p> <p>Supporto dei diversi tipi di applicazioni su tutti i servizi di rete: porte e protocolli, applicazioni di rete, SNI (hostname), DPI, UCaaS basato sull'identificazione del primo pacchetto, IP, gruppi FQDN e altri rilevamenti basati sull'euristica</p>
<p><b>Sicurezza e controllo IPS adattivi</b></p>	<p>Sfruttando le firme IPS personalizzate e migliaia di firme IPS adattive e comportamentali su qualsiasi porta e protocollo, è possibile offrire una protezione dalle minacce sempre attiva e fornita sul cloud, indipendentemente dal tipo di connessione o dalla posizione, ispezionando tutto il traffico Internet degli utenti. <b>Visualizza l'elenco di tutte le firme IPS gestite da ThreatLabZ.</b></p>
<p><b>Ispezione di sicurezza avanzata</b></p>	<p>L'ispezione avanzata dei pacchetti viene applicata sui protocolli non web, tra cui FTP, DNS, RDP, Telnet e altri, per identificare e prevenire il traffico elusivo sulle porte non standard.</p>
<p><b>Sicurezza e controllo dei DNS</b></p>	<p>Inoltrando tutto il traffico DNS tramite Zscaler, le prestazioni delle applicazioni cloud vengono ottimizzate e si riduce al minimo la latenza, garantendo una sicurezza senza compromessi. Abilitando le policy in base all'utente, all'app, alla posizione e all'IP del Paese, è possibile bloccare automaticamente gli utenti di domini dannosi e rilevare e prevenire il tunneling DNS.</p> <p><b>Risoluzione:</b> il DNS come servizio offre una risoluzione ottimale, con localizzazione, tenancy e latenza più bassa</p> <p><b>Filtraggio DNS:</b> vengono create regole personalizzate di filtraggio DNS, per bloccare, consentire o reindirizzare le diverse tipologie di richieste DNS correlate a destinazioni conosciute e dannose</p> <p><b>Sicurezza ed esfiltrazione dei dati:</b> utilizzando il machine learning è possibile rilevare malware, phishing, tunnelling DNS ed esfiltrazione dei dati</p> <p><b>DNS over HTTPS (DoH):</b> per impedire i punti ciechi DoH e l'elusione dei controlli dell'organizzazione durante la crittografia delle connessioni DNS nel traffico HTTP comune</p>
<p><b>Nome di dominio completo Policy (FQDN)</b></p>	<p>Configurazione e gestione semplificate delle policy di accesso per le applicazioni ospitate su più IP</p>
<p><b>Controllo del protocollo di trasferimento file (FTP) e supporto della traduzione degli indirizzi di rete (NAT)</b></p>	<p>Supporto per il controllo degli accessi di FTP e FTP over HTTP e supporto per proxy di destinazione NAT e inoltra NAT</p>
<p><b>Certificazioni sulla privacy e sulla conformità</b></p>	<p>Ottemperanza a rigorosi standard globali commerciali e governativi relativi al rischio, alla privacy e alla conformità</p> 
<p><b>Normative di settore e sulla privacy dei dati</b></p>	<p>Conformità alle normative sulla privacy dei dati specifiche del settore e dei singoli Paesi</p> 
<p><b>Protezione condivisa a livello globale</b></p>	<p>Sfruttando l'effetto cloud, ogni volta che una nuova minaccia viene identificata in una qualsiasi delle decine di miliardi di richieste elaborate quotidianamente dal cloud Zscaler, la minaccia viene bloccata per tutti gli utenti Zscaler, ovunque</p>

## Zscaler Cloud Firewall è completamente integrato in Zscaler Internet Access™ e fa parte della soluzione olistica Zero Trust Exchange

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

### Ecco come Zscaler fornisce un approccio zero trust a utenti, carichi di lavoro e IloT/OT

Distribuzione in poche settimane, per migliorare la protezione informatica e l'esperienza utente



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 su SASE, è la più grande piattaforma di cloud security in linea del mondo. Scopri di più su [zscaler.it](https://www.zscaler.it) o seguici su Twitter su [@zscaler](https://twitter.com/zscaler).

© 2022 Zscaler, Inc. Tutti i diritti riservati. Zscaler™, Zero Trust Exchange™, Zscaler Internet Access™, ZIA™, Zscaler Private Access™, ZPA™ e altri marchi commerciali elencati all'indirizzo [zscaler.it/legal/trademarks](https://www.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. Qualsiasi altro marchio commerciale è di proprietà dei rispettivi titolari.