



Zscaler Internet Access vi fornisce uno stack di sicurezza globale dal cloud. Rispetto ai tradizionali sistemi di web security semplifica la vostra architettura e vi permette di ridurre i costi.

Zscaler Internet Access

**Con Zscaler Internet Access i vostri collaboratori sono protetti in modo affidabile dai rischi legati a internet, indipendentemente dal luogo e dal dispositivo.**

#### Cos'è Zscaler Web Security?

Zscaler è un servizio web gateway per i vostri collaboratori. Oltre ad anti-malware, antivirus e protezione da advanced persistent threat, Zscaler consente di attuare le direttive aziendali attraverso filtri URL e regole di utilizzo dell'accesso a internet e applicazioni web 2.0. Data leakage protection (DLP) impedisce il deflusso di dati confidenziali dalla vostra organizzazione. Il servizio è gestito nei centri di calcolo sicuri di Swisscom in Svizzera; si possono inoltre utilizzare ulteriori gateway nel cloud globale.

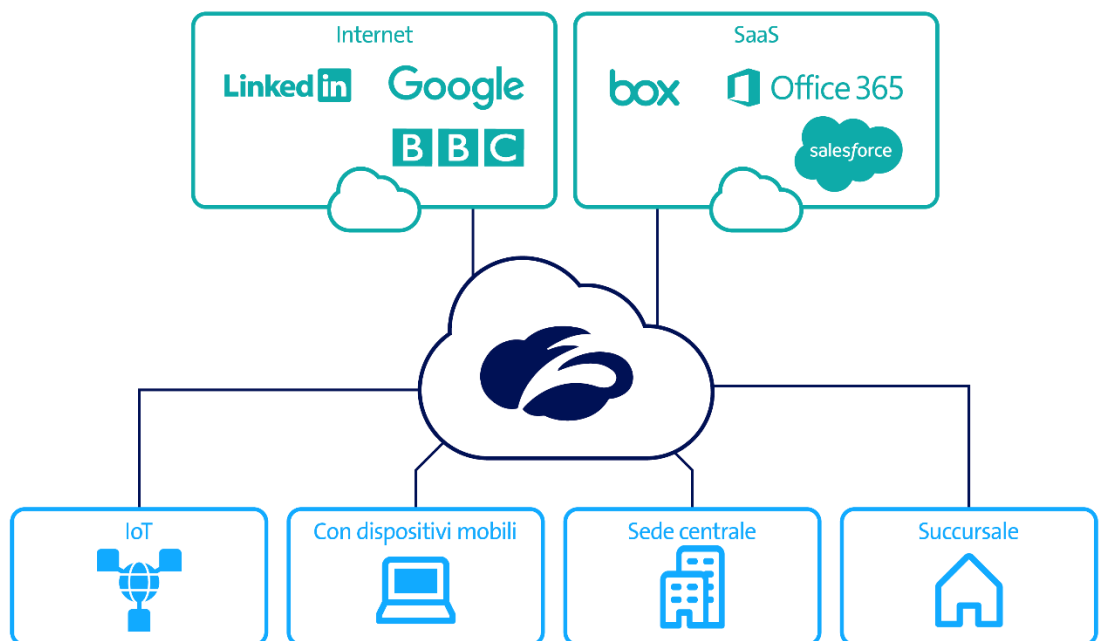
#### I vantaggi con Zscaler Web Security

- Proteggete i vostri utenti ovunque e su qualsiasi dispositivo
- Riducete la complessità e l'infrastruttura di rete
- Ottimizzato per Office 365 e altre applicazioni cloud
- Ottenete una sicurezza internet ininterrotta attraverso tutti i protocolli e porte
- Approfittate in qualsiasi sede nel mondo della migliore performance e in Svizzera del collegamento al backbone Swisscom

#### La soluzione cloud semplice ed efficace

Zscaler Web Security può essere implementato nella vostra organizzazione con un onere ridotto e senza necessità di un'infrastruttura aggiuntiva. Richiedete un'offerta non vincolante o un'installazione di prova.

[swisscom.ch/zscaler](http://swisscom.ch/zscaler)



Tutti i dispositivi, ovunque, on-net o off-net

swisscom



Le informazioni del presente documento non costituiscono un'offerta vincolante. Con riserva di modifiche in qualsiasi momento.

S Swisscom (Svizzera) SA Enterprise Customers, casella postale, CH-3050 Berna, telefono 0800 800 900, [www.swisscom.ch/enterprise](http://www.swisscom.ch/enterprise)

**swisscom**

## Facts & Figures

Zscaler Internet Access (ZIA)	Essentials Edition	Business Edition	Transformation Edition
<b>Centri dati</b> Accesso globale, elevata disponibilità, con SLA latenza.	●	●	●
<b>Traffic forwarding</b> Tunnel GRE, IPsec, proxy chaining, file PAC o Zscaler app (anche per dispositivi mobili).	●	●	●
<b>Autenticazione</b> SAML, Secure LDAP (AD Sync), Kerberos, base utenti nel cloud.	●	●	●
<b>Aggiornamenti cloud security in tempo reale</b> Ottenete la condivisione totale delle informazioni sulle minacce, quotidianamente oltre 120000 aggiornamenti di security e la massima sicurezza attraverso 60 diversi security feed	●	●	●
<b>Report e log in tempo reale</b> Report di tutte le transazioni web in pochi secondi. Log conservazione dati per sei mesi, in Svizzera	●	●	●
<b>Ispezione SSL</b> Ispezione minacce inline dell'intero traffico SSL. Policy granulari ed eccezioni attraverso la whitelist specifica del cliente.	●	●	●
<b>Nanolog streaming service</b> Trasmettete in tempo reale i log di tutte le transazioni utenti e le sedi alla vostra SIEM on premise	●	●	●

● = standard (compreso nel prezzo)    ○ = dietro sovrapprezzo    — = non disponibile



Le informazioni del presente documento non costituiscono un'offerta vincolante. Con riserva di modifiche in qualsiasi momento.

S Swisscom (Svizzera) SA Enterprise Customers, casella postale, CH-3050 Berna, telefono 0800 800 900, www.swisscom.ch/enterprise

**swisscom**

## Facts & Figures

Servizi Cloud Security	Essentials Edition	Business Edition	Transformation Edition
<b>URL e content filtering</b> Regole granulari per utenti, gruppi, sedi, orari e quote	●	●	●
<b>File type control</b> Controllo del tipo di file true con policy in base a utente, sede e destinazione	●	●	●
<b>Antivirus e antispyware inline</b> Anti-malware basato su firma e ispezione totale file inbound e outbound	●	●	●
<b>Protezione dalle minacce basata sulla reputazione</b> Individua e impedisce, se noti, botnet, comunicazione command e control e phishing	●	●	●
<b>Standard cloud firewall</b> Regole outbound granulari in base a indirizzo IP, porta e protocollo (regola delle cinque tuple)	●	●	●
<b>Advanced cloud firewall</b> Cloud firewall outbound next-gen globale con regole per applicazioni e utenti e controllo sede; logging e reporting completi	○	○	●
<b>Bandwidth control</b> Garantisce la priorità delle applicazioni business, quali Office 365, rispetto al restante traffico	○	●	●
<b>Standard cloud sandbox</b> Protezione zero-day da file .exe e .dll di siti web sconosciuti e sospetti	●	●	●
<b>Advanced cloud sandbox</b> Protezione zero-day da tutti i tipi di file di tutti i siti web; ritenzione fino all'esecuzione del Sandbox clean check; advanced reporting	○	○	●
<b>Advanced threat protection</b> PageRisk™ e content analyse di malware, callback, cross-site scripting, cookie stealing e servizi anonimi	●	●	●
<b>Cloud application visibility and control</b> Monitoraggio e controllo delle applicazioni web	○	●	●
<b>Mobile application reporting and control</b> Controllo policy granulare e protezione dalle minacce per dispositivi mobili	—	○	●
<b>Web access control</b> Verifica della compliance di browser e plugin obsoleti	●	●	●
<b>Data loss prevention (DLP)</b> Impedisce il deflusso di dati confidenziali dell'organizzazione cliente	○	○	○

● = standard (compreso nel prezzo)    ○ = dietro sovrapprezzo    — = non disponibile