3 requisiti essenziali per una protezione dati impeccabile

Desideri un CASB più efficace e una DLP più forte? Devi iniziare con le basi giuste.

Chiunque lavori nell'IT o sulla sicurezza della rete te lo dirà: "La protezione dati era molto più semplice in passato, quando tutti i dati si trovavano nel data center e i dipendenti lavoravano tutti in ufficio". Ma i tempi sono decisamente cambiati.

Oggi, i tuoi dati hanno lasciato il data center e sono sparsi ovunque, distribuiti in centinaia di app cloud, e i dipendenti stanno adottando il lavoro da remoto, fuori dalla rete aziendale e lontano dai controlli di sicurezza. Come se ciò non fosse già abbastanza problematico la maggior parte del traffico Internet è crittografato e difficile da ispezionare, motivo per cui i malintenzionati nascondono lì le proprie minacce. I dipendenti inoltre utilizzano reti non protette o dispositivi non gestiti, che sottopongono i dati a maggiori possibilità di esposizione.

In questo mondo nuovo e rischioso le organizzazioni necessitano di una piattaforma di protezione dati pensata per il cloud e la mobilità, che includa questi requisiti essenziali.

Ciò che c'è da sapere

L'efficacia della protezione dei dati con CASB e DLP è pari all'architettura su cui risiedono. Questo concetto è essenziale per comprendere la ricetta del successo.

Requisito essenziale n. 1:

Insistere su un'architettura SASE progettata ad hoc

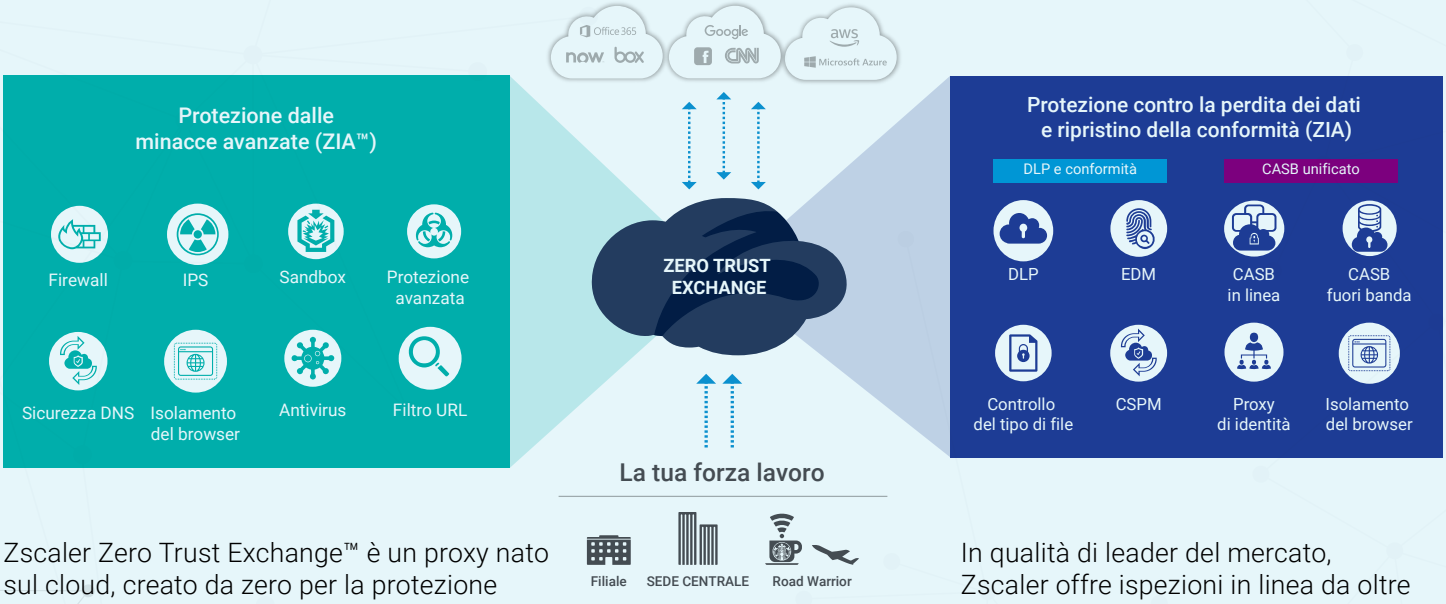
Con il cloud e la mobilità, i dispositivi di sicurezza non possono essere presenti ovunque. Quando gli utenti abbandonano la rete, si perde visibilità, sottoponendo gli utenti e i dati all'esposizione. Inoltre, per fornire funzionalità CASB (Cloud Access Security Broker) ermetiche e protezione contro la perdita dei dati (DLP), è necessario un controllo SSL completo. I dispositivi non sono in grado di fornire tutto questo, per via delle restrizioni in termini di hardware.

Una piattaforma cloud SASE progettata ad hoc è il primo requisito essenziale per fornire connessioni sempre sicure e ad alte prestazioni, indipendentemente dalla posizione dell'utente. Il SASE riunisce tutti i servizi CASB, DLP e di sicurezza in una piattaforma cloud distribuita a livello globale, in modo da poter contare su una riduzione della complessità, una protezione dati più efficace e un'esperienza utente rapida.

Ciò che c'è da sapere

Creare un'architettura di protezione dati in linea di livello enterprise/business, che sia anche scalabile sull'SSL, non è semplice. Puoi affidare il tuo traffico a un fornitore con la massima esperienza, con risultati comprovati e SLA di livello business.

Il modello Zscaler™



Zscaler Zero Trust Exchange™ è un proxy nato sul cloud, creato da zero per la protezione dati e l'ispezione SSL su larga scala su 150 data center. Ogni utente può godere di una connessione veloce e sicura. Inoltre, la nostra capacità SSL illimitata ti consente di proteggere tutti i tuoi dati su qualsiasi tipo di connessione utente, dentro o fuori dalla rete.

In qualità di leader del mercato, Zscaler offre ispezioni in linea da oltre un decennio. La cosa più interessante è che, dato che DLP, CASB e tutti gli altri servizi di sicurezza sono integrati, potrai godere di una policy semplificata e un approccio unificato alla protezione dei dati e dalle minacce.

Requisito essenziale n. 2:

Una migliore protezione dei dati richiede il miglior contesto

Per classificare correttamente i dati in tuo possesso, hai bisogno del contesto, ma è la qualità del contesto che ti aiuta a prendere decisioni migliori e più consapevoli.

In passato era tutto più semplice, perché gli utenti accedevano alla posta elettronica da un server Exchange o si disponeva solo di pochi server di file. Tutto ciò di cui si aveva bisogno, per prendere decisioni consapevoli, era a disposizione ed era facile accedervi.

Oggi, i tuoi dati si spostano attraverso centinaia di canali, dalle app cloud verso i cloud pubblici e piattaforme di condivisione file, e tutto il contesto di cui hai bisogno in quei canali si nasconde all'interno della crittografia SSL.

Ciò che c'è da sapere

Il contesto è la linfa vitale di CASB e DLP. Assicurati la piattaforma con il motore di classificazione più potente, che individui il maggior numero di attributi in ogni singola transazione cloud, dentro e fuori dalla rete, nonché all'interno dell'SSL.

Il modo di Zscaler

Quando si tratta di contesto, Zscaler non ha eguali.

Zero Trust Exchange e la nostra app Client Connector ti aiutano a fornire una protezione dati sempre attiva su ogni connessione in rete o fuori dalla rete. Offrono inoltre visibilità su TUTTO il traffico SSL, guidando le imprese alla scoperta del tesoro che tanto inseguivano, il contesto.

Sfruttando inoltre i dizionari personalizzati e settoriali di Zscaler e utilizzando le tecniche piu' avanzate, come Exact Data Match (EDM), potrai classificare rapidamente i dati nei formati di settore più comuni (PCI, HIPAA) e usufruire di definizioni personalizzate.

Contesto da un firewall o proxy	**172.16.1.12** IP sorgente **64.81.2.24** IP di destinazione **TCP/443** porta di destinazione **Protocollo** SSL **Protocollo** HTTPS	Gli approcci tradizionali in linea non forniscono abbastanza visibilità sul contesto.
Contesto aggiunto ottenuto grazie alla decrittazione completa dell'SSL	**John Doe** utente **Gruppo** gest. prodotto **Posizione** sede centrale **Caricamento** della funzione dell'app **Applicazione** jumpshare **Tipo di file** PowerPoint **Condivisione file** categoria URL **Contenuto** confidenziale	Se è possibile decrittare tutto l'SSL senza limitazioni, sara' possibile ottenere il contesto necessario per prendere le migliori decisioni in termini di protezione.

Requisito essenziale n. 3:

Richiedere una piattaforma unificata che protegga tutti i canali

Proteggere i dati da perdite ed esfiltrazioni richiede che la sicurezza sia presente ovunque risiedano tali informazioni. Se non si è in grado di controllare tutti i canali, i dati diventano vulnerabili ed esposti a potenziali minacce.

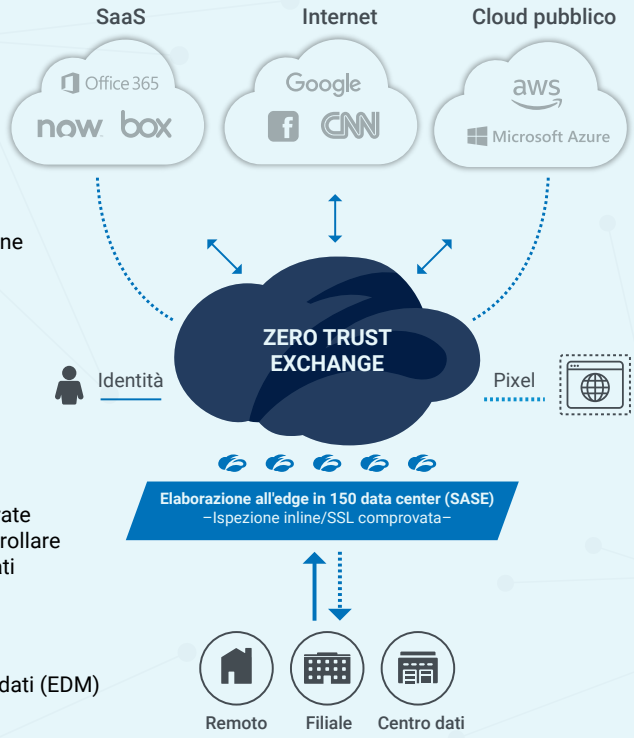
Inoltre, se non si è in grado di unificare tutte le protezioni CASB e DLP in un'unica piattaforma, la situazione si fa ancora più complessa. Senza la visione offerta da una piattaforma unificata, si finirà per incappare in policy sconcatenate, lacune nella sicurezza e una maggiore propensione a commettere costosi errori di configurazione.

Ciò che c'è da sapere

Per tutti i principali canali di dati, in movimento, a riposo, endpoint e provider di servizi cloud, una piattaforma unificata migliorerà notevolmente la forza delle policy e semplificherà i flussi di lavoro.

Il modo di Zscaler

Poiché tutti i servizi cloud di Zscaler sono integrati in un'architettura cloud in linea, progettata ad hoc, tutti i servizi cooperano in armonia per unificare le policies e semplificare la protezione dei canali-dati sul cloud.



Dati a riposo
Controllo degli utenti e dell'esposizione a minacce su Microsoft 365 e SaaS
- DLP
- Prevenzione dalle minacce
- Scansioni dei dati storici
- Condivisione dell'esposizione

Provider
Rimediare agli errori di configurazione su cloud pubblico e SaaS (CSPM)

Dati in movimento
Controllare le app non registrate e shadow, classificare e controllare i dati settoriali e personalizzati
- Controllo del tipo di file
- Controllo delle app cloud
- DLP cloud
- Corrispondenza esatta dei dati (EDM)
- Ispezione di Microsoft 365

Endpoint
Limitare l'accesso non gestito/BYOD e controllare la perdita dei dati
- Proxy di identità
- Isolamento del browser

Ecco come funziona:

Dati in movimento: l'ispezione in linea di livello business è essenziale per garantire una protezione dati in tempo reale. Grazie al cloud in linea progettato ad hoc da Zscaler, è possibile seguire tutti gli utenti fuori dalla rete e all'interno dell'SSL, classificare e bloccare rapidamente i dati critici - indipendentemente dove siano diretti - e bloccare le app cloud non autorizzate.

Dati a riposo: man mano che gli utenti adottano le app cloud è necessario verificare che si stiano prendendo le giuste decisioni. Con il CASB fuori banda di Zscaler, è possibile controllare facilmente la condivisione impropria dei file nelle app di Microsoft 365, come SharePoint e OneDrive, analizzando al contempo gli archivi dei file alla ricerca di DLP e problemi di malware.

Endpoint: questo canale serve a garantire che solo le persone giuste abbiano accesso ai tuoi dati. Con il controllo degli accessi BYOD, è possibile eseguire una rapida ricerca SAML/SSO e bloccare l'accesso non autorizzato alle risorse di Microsoft 365. Zscaler Cloud Browser Isolation aiuta inoltre a prevenire perdite su dispositivi non gestiti (BYOD) eseguendo il rendering dei dati sugli endpoint solo sotto forma di pixel. Ciò significa che una terza parte può visualizzare e interagire con i dati, ma non sarà in grado di salvare, scaricare o copiare e incollare i dati. Questo ti dà la sicurezza che nulla si allontanerà su dispositivi terzi dopo la sessione.

Provider: gli errori di configurazione accidentali delle applicazioni cloud sono una delle cause più comuni di esposizione dei dati, con costi per le aziende in termini di tempo e denaro. Zscaler Cloud Security Posture Management (CSPM) identifica e corregge automaticamente tali errori delle applicazioni in SaaS, IaaS e PaaS, in modo da ridurre il rischio di perdita dei dati e garantire la conformità.

Sommario

Il cloud e la mobilità hanno cambiato il modo in cui le aziende fanno business e il modo in cui lavorano i dipendenti. Al giorno d'oggi i dati sono gestiti in modo differente, e proprio per questo devono essere protetti in modo differente. Nel mondo di oggi i dispositivi di sicurezza non sono più in grado di fornire una protezione adeguata dei dati. C'è bisogno di una piattaforma di sicurezza basata sul cloud, con una base SASE che protegga i dati ovunque si trovino. C'è bisogno di Zscaler.

Guarda il nostro CASB/DLP in linea in azione
youtube.com/watch?v=R88TlNEMgGE

Guarda il nostro CASB/DLP fuori banda in azione
youtube.com/watch?v=1KtoW-IXgMs

Contattaci o prenota una demo personalizzata
zscaler.com/company/contact

Informazioni su Zscaler
Zscaler accelera la trasformazione digitale grazie a Zero Trust Exchange, una piattaforma basata sul SASE che fornisce connessioni rapide e sicure tra utenti, dispositivi e applicazioni, su qualsiasi rete.

Zscaler, Inc.
120 Holger Way
San Jose, CA 95134
+1 408.533.0288
www.zscaler.com