E-BOOK

Tutelare i dati in un mondo in cui si lavora da qualsiasi luogo

Preserva la sicurezza delle informazioni critiche grazie a Zscaler Data Protection

Contenuti

Le sfide principali

Proteggere i dati non è mai stato così complesso

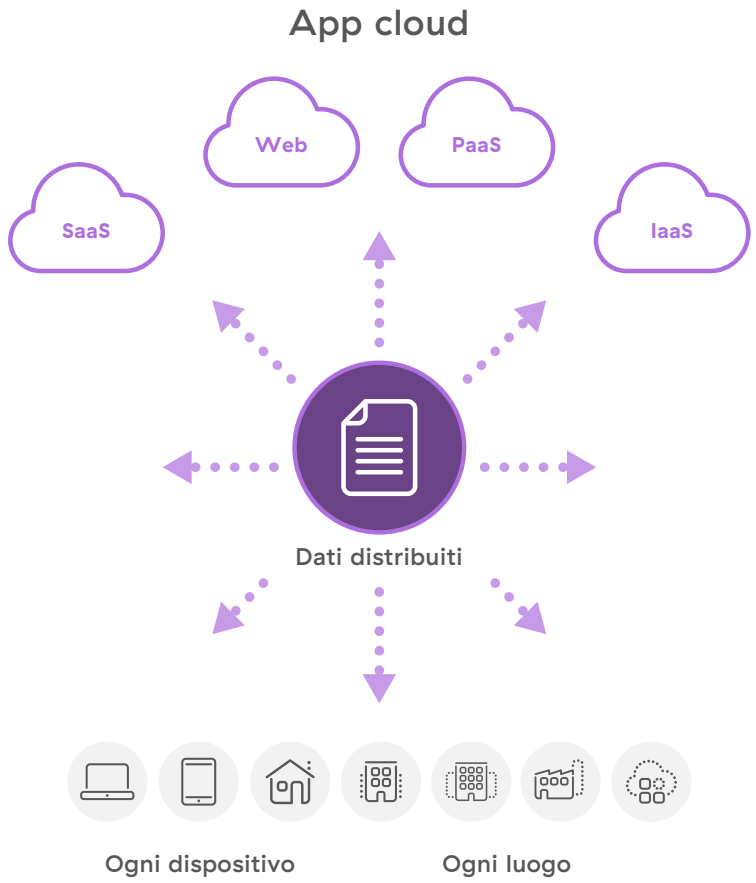
Con le app cloud, ora i dati sono distribuiti su larga scala e i dipendenti si connettono da qualsiasi luogo in cui lavorano, che potrebbe essere ovunque. Gli approcci tradizionali alla protezione dei dati non sono in grado di offrire un controllo adeguato sulle informazioni. Ecco perché:

È impossibile seguire gli utenti
Non è possibile proteggere i dati nel modo corretto, perché le applicazioni cloud sono accessibili tramite Internet, lontano dalla rete e dal controllo sui dati stessi.

Non si conosce lo stato di conformità
Comprendere lo stato di conformità aziendale è diventato difficile, perché le app cloud sono distribuite in più sedi e gruppi.

Ispezione TLS/SSL limitata
La maggior parte del traffico è cifrata, ma poiché gli approcci tradizionali alla protezione dei dati non sono in grado di ispezionare il traffico TLS/SSL su larga scala, non è possibile individuare i potenziali rischi.

Non si conosce il quadro generale
I prodotti singoli e gli approcci basati sull'aggiunta di strumenti creano complessità e impediscono di avere la visione unificata necessaria per comprendere il grado di esposizione.



La soluzione di Zscaler

Grazie a Zscaler è possibile riprendere il controllo sui dati

Zscaler Data Protection può aiutare a ottenere un livello di protezione dei dati senza precedenti grazie a questi principi fondamentali:

Architettura SASE costruita ad hoc

Offri una protezione in tempo reale a tutti gli utenti sfruttando un cloud inline ad alte prestazioni distribuito attraverso 150 data center globali.

Ispezione SSL su larga scala

Ispeziona tutto il traffico SSL per verificare l'esposizione dei dati con una capacità di ispezione illimitata per utente.

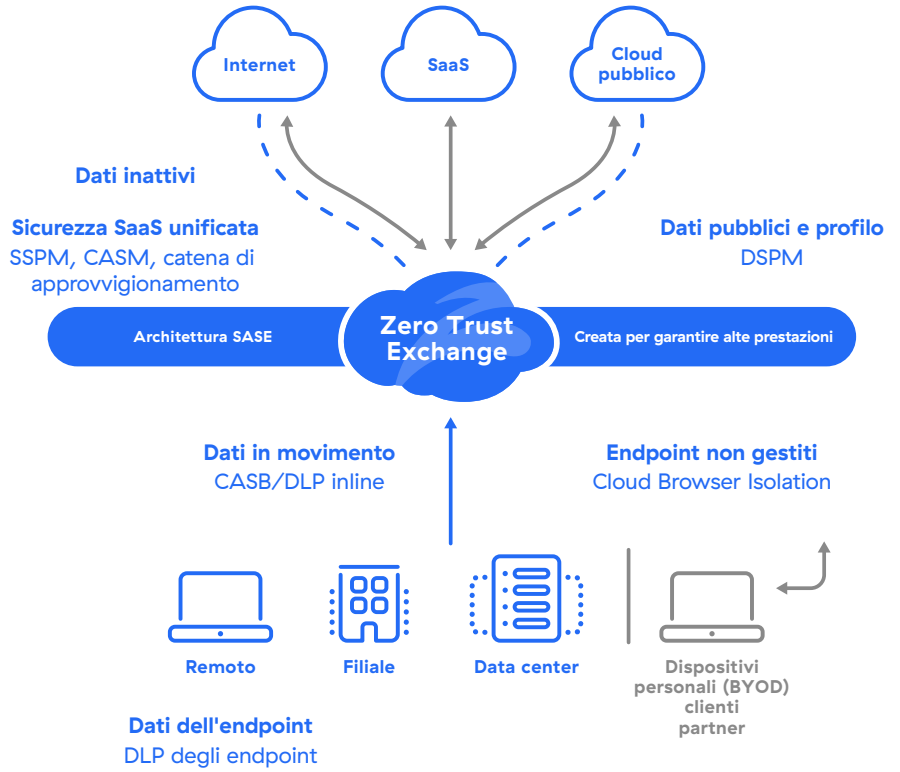
Visibilità sulla conformità

Preserva facilmente la conformità eseguendo la scansione di SaaS, Microsoft 365 e dei cloud pubblici per verificare la presenza di violazioni ed errori di configurazione.

Una piattaforma, una policy, piena visibilità

Proteggi tutti i canali di dati cloud, tra cui quelli in movimento, inattivi e sui vari endpoint e cloud, con un'unica piattaforma semplice e unificata.

Protezione dati di Zscaler: panoramica sulla soluzione



Controlla in modo sicuro le app autorizzate grazie a un CASB fuori banda

Le app cloud possono favorire la collaborazione, soprattutto se ci sono molti dipendenti che lavorano in remoto, ma al contempo possono rappresentare un rischio ed esporre i dati. I dipendenti usano spesso queste app in modo improprio, aprendo la porta alla possibilità che si verifichino attività dannose.

Come proteggere le app e i dati cloud grazie al CASB fuori banda di Zscaler:

- **Proteggi i dati esposti inattivi**
  Identifica i dati critici nelle app cloud, nella posta elettronica e nella condivisione di file. Applica policy di DLP per controllare l'accesso e l'esposizione.

- **Impedisci la condivisione impropria dei dati**
  Applica policy granulari sui dati sensibili inattivi per assicurarti che non vengano condivisi al di fuori dell'organizzazione.

- **Correggi le minacce**
  Scansiona gli archivi di dati nei servizi di hosting dei file, come OneDrive o Box, per trovare e mettere rapidamente in quarantena i contenuti dannosi.

- **Semplifica la protezione dei dati**
  Evita la complessità derivante dall'uso di molteplici prodotti singoli grazie a una piattaforma unificata che fornisce una sola policy per dati e minacce, su tutti i dati in movimento e quelli inattivi.

Visibilità e controllo in tempo reale grazie al CASB inline

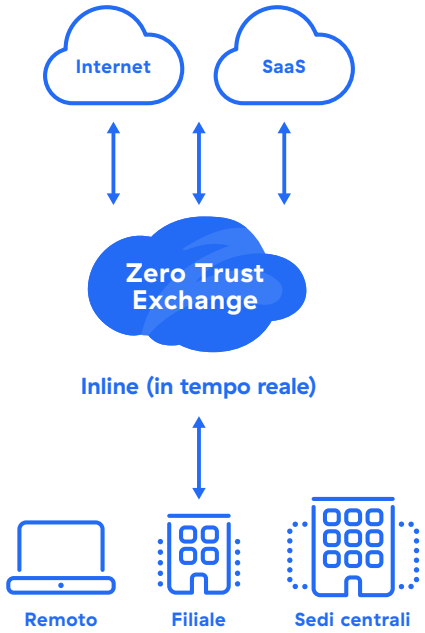
Sebbene la tecnologia CASB fuori banda aiuti a proteggere i dati a riposo, hai comunque bisogno di controllare in tempo reale le app cloud. In che modo il CASB inline consente di passare al cloud in modo sicuro?

- **Riduce il rischio associato allo shadow IT**
  Individua rapidamente le app cloud sicure e non sicure che vengono utilizzate nell'organizzazione.

Esempio: l'attività delle app rischiose che accedono ai dati viene bloccata, come ad esempio quella dei convertitori di PDF online o dei siti per la condivisione dei file.

- **Esegue le app autorizzate ufficialmente**
  Limita l'attività degli utenti alle app cloud approvate dall'IT e dall'organizzazione.

Esempio: migliora la condivisione e la produttività di Microsoft 365 permettendo solo l'utilizzo di OneDrive e bloccando Box.



- **Impedisce la perdita dei dati mediante controlli del tipo di file**
  Limita il trasferimento dei dati per tipo di file mediante blocco condizionale e segnalazione.

Esempio: previeni l'upload o il download di file Word, Excel o PowerPoint da parte di particolari utenti o gruppi.

- **Adotta restrizioni delle tenancy**
  Controlla i flussi di dati consentendo solo specifiche istanze di app cloud.

Esempio: impedisci la perdita di dati in istanze personali di Microsoft 365 consentendo l'accesso solo a Microsoft 365 Business.

Semplifica il modo in cui controlli i dati dei dispositivi con Endpoint DLP

Una protezione ottimale dei dati richiede una strategia per gli endpoint. Con Endpoint DLP ottieni una protezione totale dei dispositivi, senza la complessità degli approcci tradizionali.

- **Policy e visibilità unificate**
  Con un motore di DLP centralizzato, ottieni allerte coerenti sugli endpoint, inline e sul cloud.
- **Agente singolo e leggero**
  Grazie all'integrazione con l'agente di Zscaler, ottieni un'esperienza utente migliore riducendo il numero di agenti richiesti sul tuo endpoint.
- **Distribuzione rapida**
  Sfrutta le policy DLP esistenti di Zscaler per un'implementazione immediata.
- **Gestione più rapida degli incidenti**
  Rispondi agli incidenti più velocemente con l'automazione dei flussi di lavoro, pannelli di controllo avanzati e analisi di grado forense.

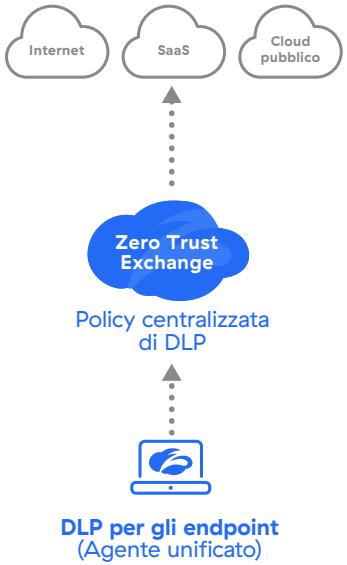
I principali casi d'uso di Endpoint DLP

Migliora la copertura dei dati
Assicurati che i dati di valore siano adeguatamente tracciati e protetti ovunque, senza lacune

Tutela i dati durante le dimissioni dei dipendenti
Assicurati che i dipendenti che lasciano l'azienda non copino i dati dei dispositivi e non li portino nel loro nuovo posto di lavoro

Elimina la DLP degli endpoint legacy
Elimina i complicati prodotti non integrati e sfrutta una piattaforma unificata

Migliora la conformità
Preserva la conformità alle normative per tutti i file e i dispositivi



Canali protetti

Supporti rimovibili	Sincronizzazione dell'archiviazione su cloud personale
Condivisioni di rete	Stampa

Riduci la complessità con l'approccio unificato e in tempo reale offerto da Email DLP

Uno dei principali rischi per i dati è rappresentato dalla posta elettronica. Con Email DLP di Zscaler, le organizzazioni possono adottare un approccio efficace per aggiungere un controllo DLP completo sui dati delle email

Gli approcci legacy alla protezione dei dati delle email possono risultare farraginosi e complessi. Quando adottano l'SSE, i team IT ricercano approcci unificati per proteggere i dati attraverso i canali di posta elettronica, in modo da ridurre la complessità di queste operazioni.

Con Email DLP di Zscaler, che utilizza Smarthost, la protezione dei dati può essere facilmente estesa anche alla posta elettronica in tempo reale. Grazie all'uso dell'SMTP Relay, Zscaler consente un'integrazione semplice nei sistemi di posta elettronica esistenti, offrendo il controllo completo sui dati e sugli allegati delle email.

I vantaggi di Email DLP di Zscaler:

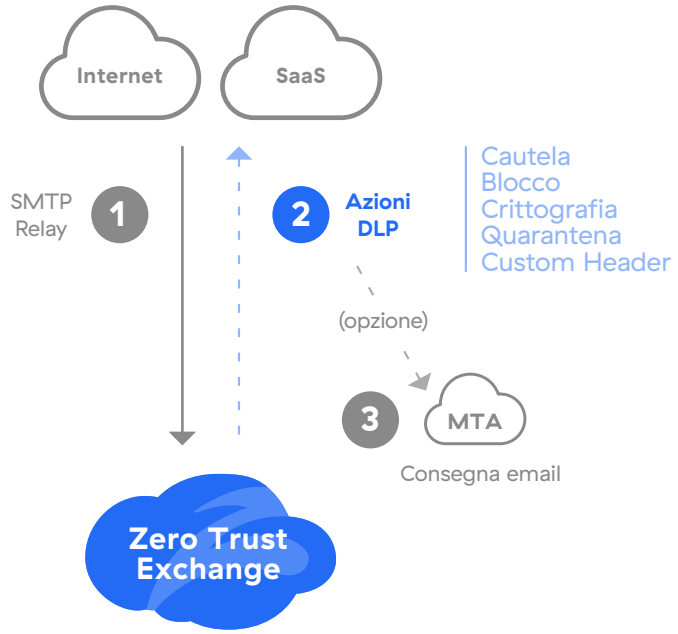
Indipendenza dai protocolli
Funziona sui dispositivi gestiti, non gestiti e persino sui dispositivi mobili

Distribuzione semplice
Non sono necessarie modifiche ai record MX

Policy flessibili
Definizioni adattabili e valutazioni granulari delle policy

Motori di DLP e UI singoli, centralizzati e unificati
per tutti i canali

DLP email in tempo reale

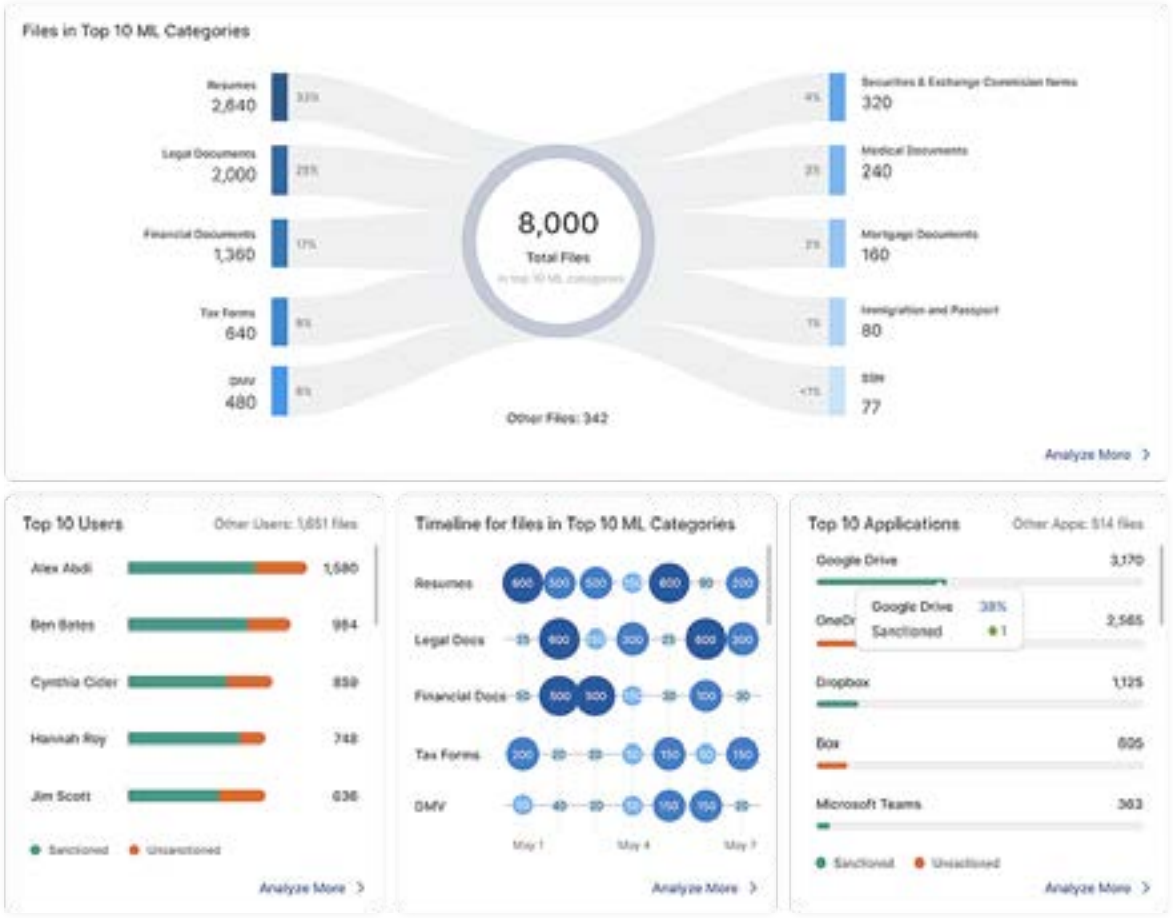


Individua e proteggi i dati istantaneamente con il rilevamento dei dati basato sull'AI

L'implementazione e la messa in funzione di un programma di protezione dei dati possono richiedere anche mesi. Con l'innovativo sistema di rilevamento dei dati di Zscaler, puoi comprendere rapidamente i rischi e i comportamenti associati ai tuoi dati.

Rilevamento dei dati basato sull'AI:

- Rileva i dati inline, sugli endpoint e sui cloud pubblici
- Valuta rapidamente il rischio di subire perdite associato a utenti e app
- Crea policy in pochi semplici clic



Classifica dati, immagini e moduli personalizzati e previenine la perdita

La classificazione dei dati è al centro di un buon programma di DLP. Con la classificazione avanzata dei dati, puoi proteggere tipi speciali di dati sensibili dalla perdita.

Exact Data Match (EDM)

Crea impronte digitali e proteggi i dati aziendali personalizzati. Esempio: attivazione sui numeri di carta di credito dei clienti e non su tutti i numeri di carta di credito (come nel caso di un acquisto su Amazon).

IDM (Indexed Document Matching)

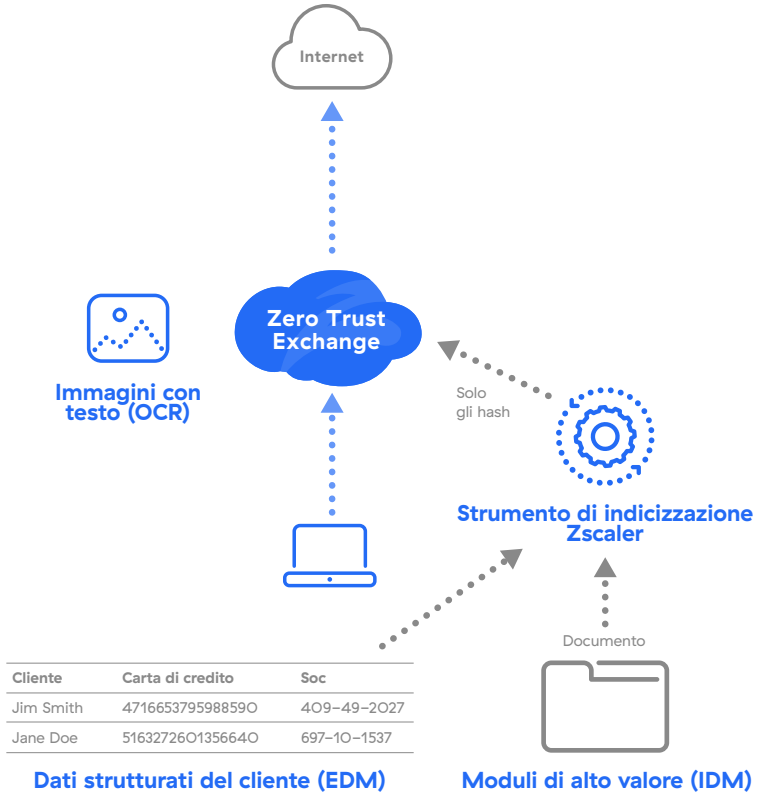
Crea impronte digitali e proteggi i documenti e i moduli personalizzati. Esempio: impronte digitali su un modulo fiscale o ipotecario vuoto e blocco di tutte le altre copie compilate.

Riconoscimento ottico dei caratteri (OCR)

Individua e previeni la perdita dei dati identificando il testo all'interno delle immagini. Esempio: monitora gli screenshot che potrebbero contenere informazioni sensibili.

Strumento di indicizzazione di Zscaler

Strumento per le impronte digitali per EDM e IDM. Crea hash di dati EDM e IDM e li carica su Zscaler Cloud per la creazione delle policy.



Ottieni il massimo della visibilità e del controllo sulle app di AI generativa

Controllare e prevenire la perdita dei dati sensibili nelle app di AI generativa è fondamentale per far sì che queste app shadow possano essere produttive. Il nuovo approccio innovativo di Zscaler riunisce tutta la protezione e la visibilità in un unico luogo

Le app di AI generativa hanno il potenziale di migliorare la produttività delle organizzazioni, ma c'è bisogno della massima visibilità e del controllo integrale su queste app per ottimizzare le decisioni di blocco.

L'innovativa soluzione di GenAI Security di Zscaler consente ai team IT di individuare tutte le app di AI generativa all'interno dell'organizzazione e offre una visibilità senza precedenti, anche sui comandi immessi, in modo da poter ottimizzare le decisioni di blocco.

Vantaggi

- Visualizza i comandi di input inviati all'app di AI dagli utenti e ottieni una visibilità contestuale completa
- Controlli flessibili delle policy attraverso l'ispezione DLP e Cloud App Control
- Applica l'accesso isolato e proteggi i dati nel Cloud Browser di Zscaler.

Visibilità su AI generativa

Rilevamento della Shadow AI
Catalogo completo di tutte le applicazioni AI più diffuse

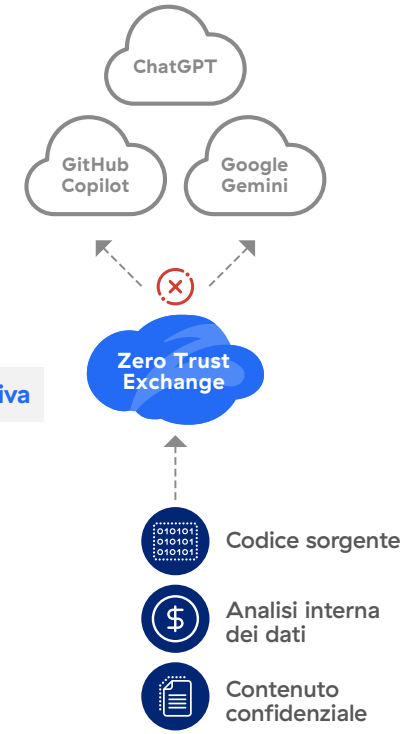
Visibilità sui comandi immessi
Visualizza i comandi immessi dagli utenti verso le app AI

Controllo delle app di AI generativa

Ispezione DLP
Blocca dati e contenuti sensibili diretti alle app AI

Controlla le app cloud
Controlla l'accesso all'applicazione AI di utenti, dipartimenti e sedi

Isolamento del browser
Limita l'utilizzo di dati e app a un browser cloud sicuro



Difendi la tua piattaforma SaaS con un approccio completamente integrato

La protezione dei cloud e dei dati SaaS richiede troppi strumenti. Unendo l'SSPM ad altri approcci alla sicurezza SaaS è possibile semplificare notevolmente il modo in cui i team IT proteggono i dati e il profilo di sicurezza SaaS.

Molte violazioni del cloud sono causate da errori di configurazione o app di terze parti a rischio connesse alle piattaforme SaaS. Saper valutare e amministrare il proprio profilo di sicurezza SaaS è un passo importante per proteggere le grandi quantità di dati sensibili presenti in questi cloud.

Con SaaS Security Posture Management (SSPM) di Zscaler, puoi ottenere un approccio unificato per scansionare e proteggere le piattaforme SaaS come Office 365 o Google. Ottieni una visibilità approfondita sugli errori di configurazione e le integrazioni delle app a rischio con la correzione automatica, le linee guida e il controllo sulla revoca delle app connesse pericolose.

Data Security Posture Management (DSPM)

Proteggi i cloud pubblici e i dati con un approccio alla protezione dei dati completamente integrato

I team responsabili della protezione dei dati necessitano di un approccio unificato per proteggere i dati sul cloud pubblico. DSPM di Zscaler si integra perfettamente nei programmi di protezione dati esistenti.

I dati sensibili archiviati nei cloud pubblici come AWS e Azure possono essere altamente dinamici. Da privilegi in eccesso e vulnerabilità ai dati shadow, i team IT hanno bisogno di un modo più efficiente per individuare, classificare e proteggere i dati sul cloud pubblico.

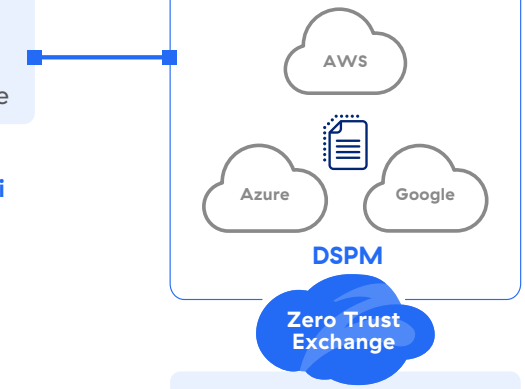
Zscaler DSPM è in grado di rilevare rapidamente i dati sensibili, valutare i rischi e controllare l'accesso e il profilo di sicurezza. Inoltre, sfrutta lo stesso motore di DLP di tutti gli altri canali (endpoint, rete, SaaS), quindi gli avvisi risultano coerenti, indipendentemente da dove si spostino i dati.

Vantaggi

- Individua rapidamente i dati sensibili con il rilevamento automatico basato sull'AI
- Correla errori di configurazione, esposizioni e vulnerabilità per comprendere al meglio il rischio associato ai dati sul cloud
- Estendi i dizionari di DLP esistenti ai dati sul cloud pubblico per ottimizzare la visibilità e il contesto
- Elimina rapidamente i rischi con utili linee guida per la risoluzione

Sicurezza dei dati e del profilo cloud
Trova, proteggi i dati e comprendi i rischi di esposizione

1. **Mappatura degli archivi di dati**
   Mappa bucket, VM e DB con il rilevamento automatico dei dati
2. **Priorità del rischio**
   Comprendi gli errori di configurazione e il rischio di esposizione dei dati
3. **Correzione dei rischi**
   Trova una soluzione con guide alla risoluzione dei problemi e policy



DLP centralizzata:
Definisci una volta, distribuisci ovunque

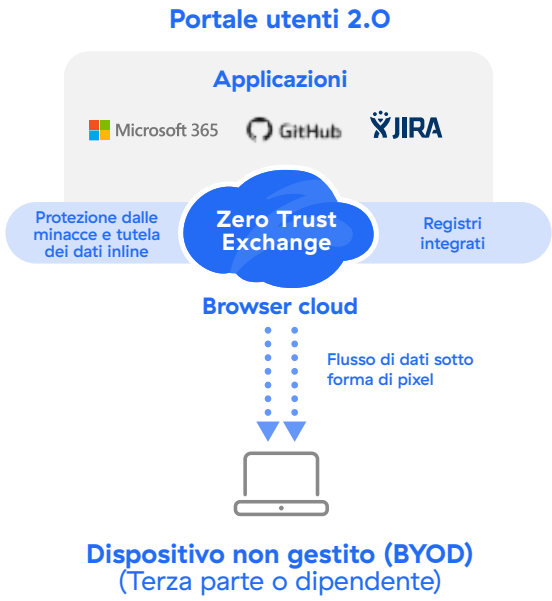
Proteggi i dati delle app web e l'accesso dei dispositivi personali (BYOD)

Partner, collaboratori e dipendenti a volte devono poter accedere ai dati aziendali mentre utilizzano i propri dispositivi personali. Quindi, come puoi preservare il controllo su questi dati quando vengono usati dispositivi non gestiti?

Con Zscaler User Portal 2.0 e Cloud Browser, le organizzazioni possono supportare in sicurezza i dispositivi non gestiti. Ecco come:

In che modo User Portal 2.0 protegge gli accessi e i dati:

- Gli utenti, senza che vi siano requisiti per l'agente di endpoint, si autenticano nel portale e visualizzano un pannello di controllo con le app web autorizzate (SaaS o private).
- Gli utenti accedono all'app all'interno di un browser isolato/confinato. I dati vengono quindi trasmessi in modo sicuro all'endpoint sotto forma di pixel.
- L'app è completamente interattiva, ma le operazioni per tagliare, incollare, scaricare e stampare sono bloccate, e gli screenshot sono persino dotati di filirana.



I vantaggi per i dispositivi BYOD:

Protezione dalle minacce e tutela dei dati

Ispeziona tutto il traffico inline, garantendo lo stesso livello di sicurezza dei dispositivi gestiti.

Isolamento di dati e file

Documenti e file vengono visualizzati o condivisi (tra app) con le funzionalità di download o gli appunti che risultano però disabilitati sull'endpoint.

Policy di DLP integrate

Vengono usare le policy aziendali per garantire protezione e allerte uniformi per i dati sensibili.

Ottimizza la gestione degli incidenti che comportano la perdita di dati con Workflow Automation

Per portare il tuo programma di protezione dati a un livello superiore, hai bisogno di uno strumento potente per la gestione degli incidenti che semplifichi le operazioni e consenta di istruire gli utenti.

Molti programmi di protezione sono inefficienti per via di incidenti e strumenti non integrati. Inoltre, gli utenti non riescono mai a capire quali sono i comportamenti rischiosi che hanno adottato quando hanno gestito i dati in modo errato.

Zscaler Workflow Automation offre uno strumento pensato per gli amministratori della DLP affinché possano ottimizzare la gestione degli incidenti.

Grazie alla disponibilità di tutte le analisi di grado forense in un unico luogo, gli amministratori riescono a comprendere rapidamente i comportamenti rischiosi, assegnare gli incidenti ai relativi utenti per consentirne un'eventuale giustificazione e implementare azioni per l'esecuzione delle policy e la risoluzione degli incidenti.

In che modo Workflow Automation supporta il tuo programma di protezione dei dati

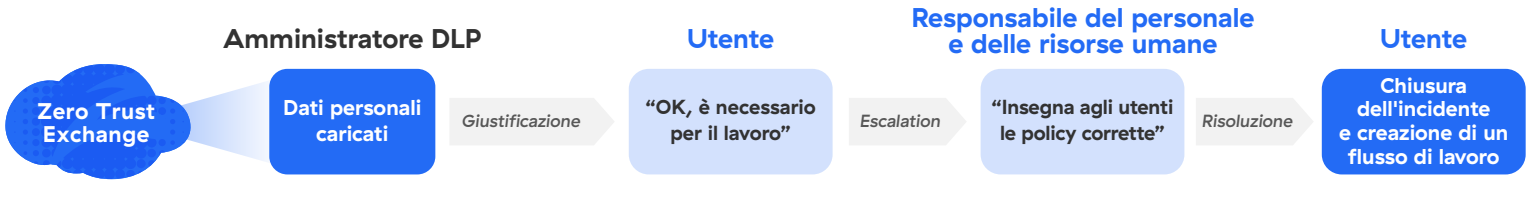
Gestione degli incidenti più rapida
Risparmia tempo con una piattaforma appositamente creata per la gestione degli incidenti che comportano la perdita dei dati

Coaching degli utenti
Consenti agli utenti di giustificare gli incidenti tramite Slack, Teams o via email, istruendoli al tempo stesso sulle best practice per la protezione dei dati

Procedure di routine automatizzate
Semplifica le operazioni di tutti i giorni con i flussi di lavoro per automatizzare le attività ripetitive e le escalation

Integrazione completa
Evita i classici errori dei programmi di protezione fornendo un sistema completo per la gestione degli incidenti

Flussi di lavoro affidabili
Gestione di incidenti, educazione degli utenti e automatizzazione dei flussi di lavoro



Riepilogo

Massima protezione con il minimo sforzo

La protezione dei dati di Zscaler segue gli utenti e le applicazioni a cui accedono per proteggere le informazioni nel mondo cloud e mobile. Zscaler Zero Trust Exchange™ è una piattaforma creata appositamente per offrire la protezione e la visibilità di cui hai bisogno, per semplificare la conformità e la protezione dei dati.

Zero Trust Exchange:

- **Offre la stessa protezione** in modo da poter fornire una policy di protezione dati coerente a tutti gli utenti, indipendentemente dalla loro connessione o posizione.
- **Ispeziona tutto il traffico SSL** per eliminare i punti ciechi ed è supportata dai migliori accordi sul servizio del settore.
- **Semplifica la conformità** in modo da poter trovare e controllare facilmente i dati PCI, PII e PHI e migliorare al contempo la capacità di mantenere i requisiti di conformità.
- **Elimina la complessità** con una piattaforma unificata che ti consente di proteggere tutti i canali dei dati cloud, con dati in movimento e dati inattivi, su endpoint e cloud.

La protezione dei dati creata per un mondo mobile e cloud-first

I tuoi dati non risiedono più nel data center. Sono invece distribuiti ovunque e accessibili ai dipendenti che lavorano fuori sede e praticamente da qualsiasi luogo. Gli approcci alla sicurezza esistenti non sono in grado di proteggere i dati in un mondo mobile e incentrato sul cloud. Con Zscaler Data Protection, puoi fornire una protezione identica ai tuoi dati critici, indipendentemente da dove si connettono gli utenti o da dove sono ospitate le applicazioni. **Scopri con noi come.**

Scopri le storie di successo dei clienti con Zscaler Data Protection >

Scarica l'e-book

Scopri di più sulla piattaforma Zscaler Data Protection >

Visita il sito

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 a livello globale, Zero Trust Exchange, basata sull'SSE, è la più grande piattaforma di cloud security inline del mondo. Scopri di più su **zscaler.com/it** o seguici su Twitter **@zscaler**.

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