Zscaler Data Security Posture Management (DSPM)

Panoramica sulla soluzione

Panoramica: come proteggere i dati in un mondo incentrato sul cloud

Le sfide legate alla protezione di grandi quantità di dati aziendali in ambienti multicloud includono la gestione della complessità e della portata del programma di protezione, la gestione di minacce interne, violazioni dei dati e accesso di terze parti e fornitori, i rischi relativi alla catena di approvvigionamento e la conformità alle normative sui dati. Le organizzazioni hanno difficoltà a inventariare, classificare, controllare e proteggere i dati critici tutelandoli al contempo dalle varie minacce. Questa complessità è ulteriormente aggravata dalla frammentazione delle distribuzioni dei dati, dei ruoli e dei diritti nei diversi ambienti.

Ambienti complessi	Volume dei dati	Attacchi mirati sofisticati	Accesso con privilegi eccessivi
L'82% delle violazioni coinvolge i dati archiviati sul cloud[1]	Seconde le stime, entro il 2025, 175 ZB di dati saranno archiviati sul cloud[2]	Il costo medio globale di una violazione dei dati nel 2024 è di 4,88 milioni di dollari[3]	L'80% delle organizzazioni ha subito violazioni legate alle identità[4]

Le vecchie soluzioni di protezione dei dati non sono state progettate per ambienti multicloud dinamici. Allo stesso tempo, i fornitori di soluzioni di DSPM indipendenti offrono approcci frammentati che non riescono a integrarsi in modo ottimale con i programmi di protezione esistenti.

Le organizzazioni necessitano quindi di un approccio nuovo e unificato per proteggere i propri dati sul cloud.

Zscaler risponde a queste sfide negli ambienti multicloud con una soluzione per la gestione del profilo di sicurezza dei dati (Data Security Posture Management, DSPM) completamente integrata ed agentless.

Che cosa è il DSPM?

"Data Security Posture Management (DSPM) fornisce visibilità su dove si trovano i dati sensibili, chi vi ha accesso, come vengono utilizzati e qual è il profilo di sicurezza di quelli archiviati o delle applicazioni". — Gartner

Talvolta, il DSPM viene definito sicurezza "incentrata sui dati", invertendo il modello di protezione adottato da altre tecnologie e pratiche di sicurezza informatica. Invece di proteggere i dispositivi, i sistemi e le applicazioni che ospitano, spostano o elaborano i dati, il DSPM si concentra sulla protezione diretta dei dati e si integra con molte altre soluzioni nello stack di prodotti di sicurezza di un'organizzazione.

Nello specifico, il DSPM prevede il monitoraggio, la valutazione e l'ottimizzazione costanti dei controlli di sicurezza per proteggere i dati sensibili sulle piattaforme multicloud.

Automatizzando l'identificazione di dati sensibili, potenziali vulnerabilità associate, errori di configurazione e violazioni della conformità, il DSPM assicura alle organizzazioni di riuscire a rispondere in modo proattivo al rischio rappresentato dall'esposizione dei dati. Così facendo, la DSPM li aiuta a rafforzare la sicurezza complessiva dei dati, a ridurre al minimo il rischio di subire violazioni e a soddisfare i requisiti normativi.

1. https://www.informationweek.com/cyber-resilience/data-breaches-just-keep-piling-up
2. https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/
3. https://www.ibm.com/reports/data-breach
4. https://www.darkreading.com/cybersecurity-operations/identity-related-breaches-last-12-months

Perché il DSPM è importante?

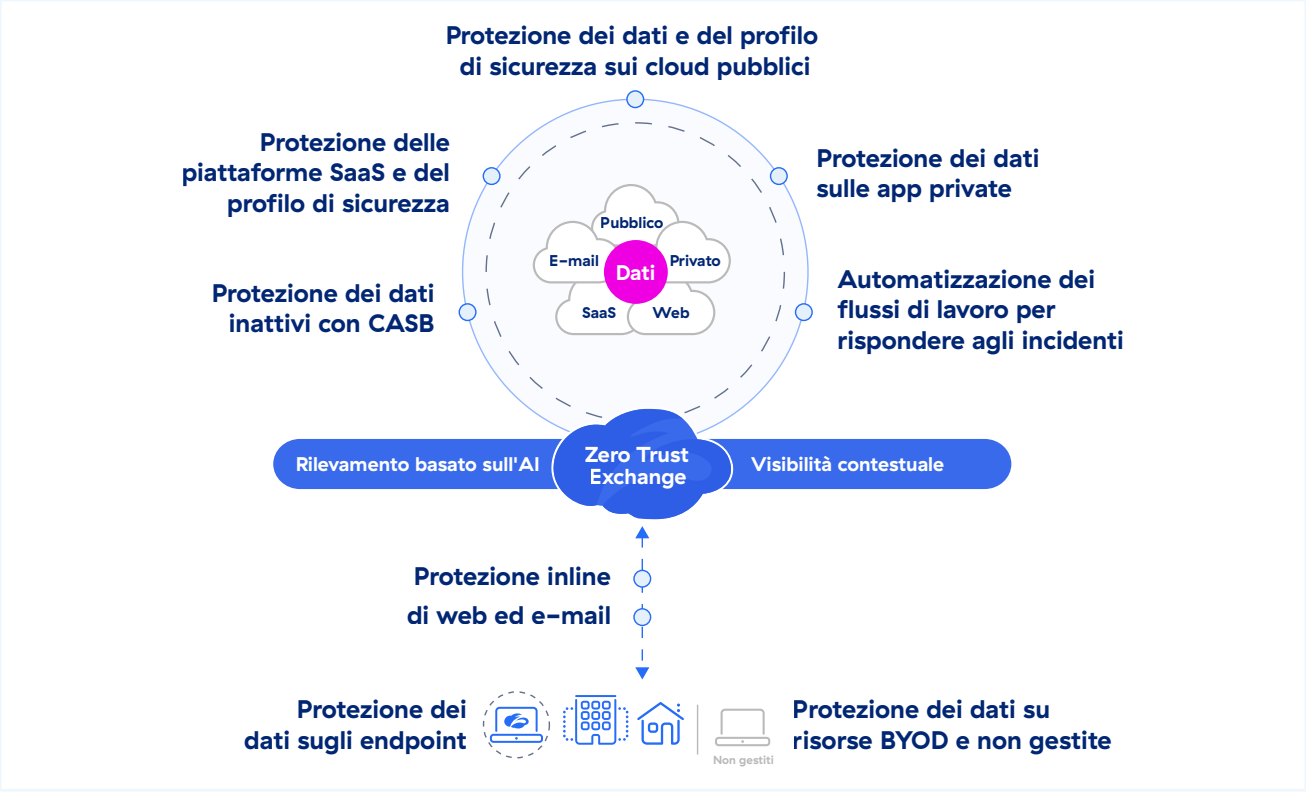
L'obiettivo principale degli strumenti di DSPM consiste nel valutare e gestire il profilo di sicurezza dell'ecosistema dei dati di un'organizzazione, individuando i punti deboli, monitorando le impostazioni di sicurezza e identificando le potenziali minacce ai dati sensibili. Il DSPM non si limita a considerare le policy, ma analizza i dati stessi.

Grazie alla scansione e alla classificazione dei dati che offre, le organizzazioni possono comprendere appieno dove si trovano i dati sensibili e come vengono utilizzati. Inoltre, consente di assegnare la giusta priorità ai problemi identificati ed evita la proliferazione delle allerte, che spesso porta a ignorare alcuni problemi.

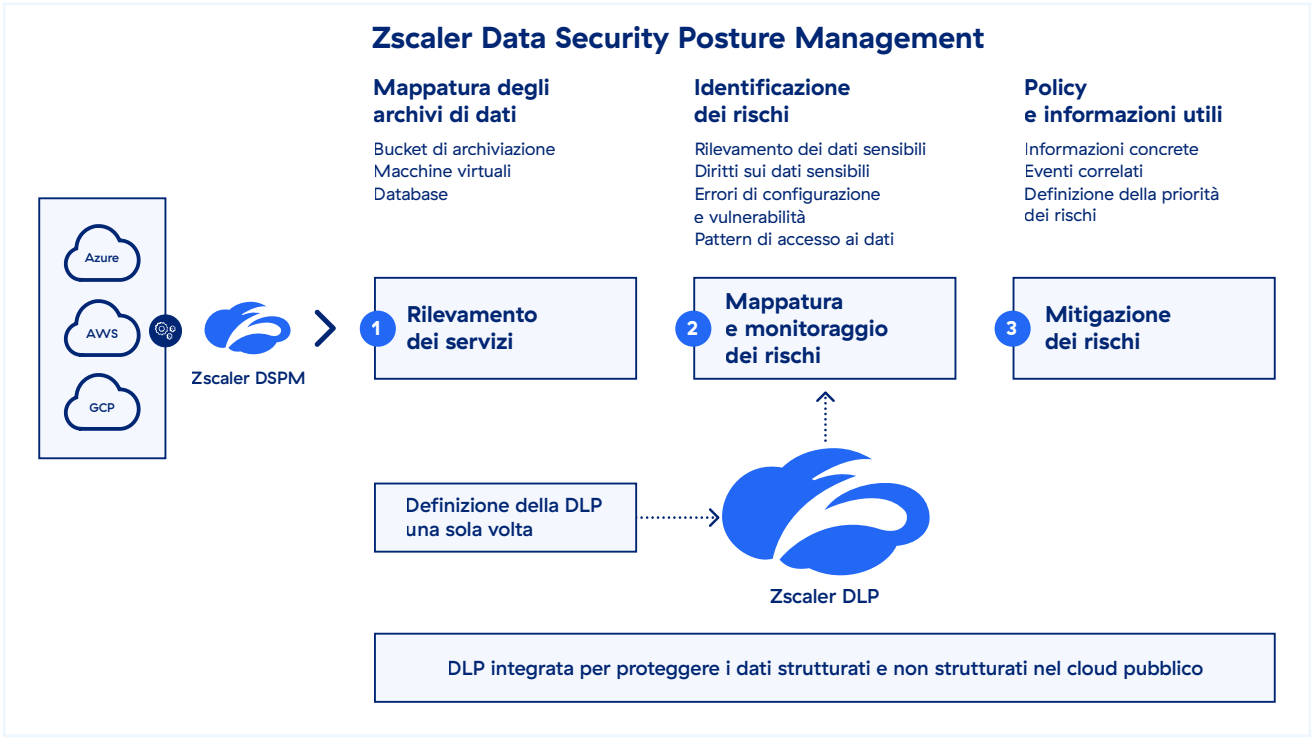
I casi d'uso pratici del DSPM includono il rilevamento delle vulnerabilità nella sicurezza (come la crittografia) negli ambienti cloud, l'applicazione di policy di accesso, la generazione di allerte e l'implementazione di funzionalità di indagine per la gestione degli incidenti.

Scopri di più su Zscaler DSPM

Zscaler AI Data Protection è la piattaforma di protezione dei dati più completa e integrata al mondo. Questa soluzione protegge sia i dati strutturati che non strutturati su web, servizi basati su SaaS, ambienti cloud pubblici (AWS, Azure, GCP), applicazioni private, e-mail ed endpoint.



Parte integrante della piattaforma Zscaler, Zscaler DSPM consente di estendere una sicurezza dei dati di alto livello al cloud pubblico. Fornisce inoltre una visibilità granulare sui dati sul cloud, classifica e identifica i dati e gli accessi e ne contestualizza l'esposizione e il profilo di sicurezza, consentendo ai team responsabili di prevenire e risolvere le violazioni sul cloud su larga scala.



Utilizzando un singolo motore di DLP unificato, Zscaler DSPM garantisce una protezione dei dati coerente su tutti i canali. Seguendo tutti gli utenti in tutte le sedi e amministrando i dati in uso e quelli inattivi, garantisce che i dati sensibili siano sempre protetti e che si raggiunga la conformità.

Principali funzionalità di Zscaler DSPM

Rilevamento, classificazione e inventario dei dati
I metodi di scansione tradizionali sono costosi e richiedono un impegno considerevole per produrre risultati utili. Zscaler DSPM, con un accesso minimo alle risorse negli ambienti cloud (AWS, Azure e GCP), esegue la scansione degli archivi di dati, rileva i dati sensibili e li classifica accuratamente, aiutando con:

- **Rilevamento completo dei dati:** Zscaler DSPM monitora costantemente gli ambienti cloud per rilevare automaticamente i nuovi archivi di dati man mano che vengono create nuove istanze in ambienti in continua evoluzione, per risparmiare tempo ed eliminare i punti ciechi.
- **Classificazione accurata dei dati:** Zscaler DSPM utilizza motori di DLP e dizionari predefiniti per la classificazione dei dati, offre visibilità sul tipo di dati sensibili archiviati nelle risorse cloud, la regione, i file che li contengono, la gravità del rischio associato a questi dati e altro, e fornisce la massima flessibilità per creare o replicare le policy esistenti disponibili.
- **Inventario dettagliato dei dati:** Zscaler DSPM crea inoltre una mappatura e un inventario dei dati altamente dettagliati che aiutano i team di sicurezza a individuare quelli sensibili e a capire chi vi ha accesso e come vengono utilizzati.

Con Zscaler DSPM, i team responsabili della sicurezza ottengono una maggiore visibilità sui dati all'interno dell'infrastruttura cloud. Questo rende molto più semplice la gestione e il potenziamento della sicurezza dei dati negli ambienti multicloud che comprendono livelli complessi di soluzioni SaaS, PaaS, IaaS e database.

Mappa e monitora l'esposizione dei dati

I servizi e le configurazioni del cloud cambiano molto frequentemente, e questo può comportare l'esposizione dei dati. È fondamentale colmare queste lacune nella sicurezza prima che gli utenti malintenzionati possano sfruttarle a proprio vantaggio. Zscaler DSPM rileva le risorse esposte pubblicamente, le vulnerabilità e gli errori di configurazione nei diversi componenti (gruppi di soluzioni per la sicurezza della rete, bilanciatori del carico, reti virtuali, ecc.) associati ai dati, aiutandoti con:

- **L'analisi dell'esposizione:** attraverso il rilevamento dell'esposizione pubblica, gli errori di configurazione e le vulnerabilità relative ad archivi di dati e servizi.
- **La valutazione del rischio:** con l'aggregazione del livello di rischio complessivo e la combinazione di impatto e probabilità, consentendo la categorizzazione dei rischi su tre livelli, ovvero alto, medio o basso.
- **La definizione delle priorità dei rischi:** per aiutare i team di sicurezza a filtrare il rumore e a stabilire le priorità degli incidenti in base al rischio e alla gravità.
- **La correlazione avanzata delle minacce:** correlazione di minacce, fattori di rischio e percorsi di attacco nascosti al fine di ridurre al minimo i rischi.
- **L'intelligence adattiva sugli accessi:** per ottenere una visione dettagliata, basata sul rischio e incentrata sull'utente di tutti i percorsi di accesso ai dati e alle configurazioni fondamentali per il business.

Risoluzione dei rischi

Zscaler DSPM semplifica la gestione del rischio con soluzioni guidate e basate sul contesto, permettendo così ai team responsabili della sicurezza di risolvere facilmente problemi e violazioni a monte per prevenire le interruzioni future. Le sue funzionalità includono:

- **Indagini e risposte efficaci**, per aiutare i team di sicurezza a comprendere rapidamente le potenziali cause durante le indagini sugli eventi relativi alla sicurezza dei dati.
- **Risoluzione guidata approfondita**, per aiutare i team interfunzionali con flussi di lavoro automatizzati e istruzioni dettagliate e contestualizzate ad affrontare i rischi per la sicurezza dei dati e mitigarli in modo efficace.
- **Tempi di messa in sicurezza più rapidi**, che consentono ai team di configurare allerte personalizzate in tempo reale per reagire ai rapidi cambiamenti dei dati e del loro ecosistema, accelerando le indagini e la risposta.
- **Integrazione facile**, per l'integrazione semplice con gli strumenti e le piattaforme di ITSM, SIEM o ChatOps esistenti e favorire la generazione di allerte, le procedure di risoluzione e i flussi di lavoro.

Prova Zscaler DSPM

Richiedi una dimostrazione
Guarda Zscaler DSPM in azione con una dimostrazione guidata.

Richiedi una dimostrazione

Scarica la Guida all'acquisto di una soluzione di DSPM
Scopri i 5 requisiti principali da considerare quando scegli la soluzione di DSPM più adatta alla tua organizzazione.

Scarica ora

Per maggiori informazioni, visita: zscaler/it/dp/dspm.

Appendice

Glossario dei termini

- Data Security Posture Management (DSPM)
- CNAPP (Cloud Native Application Protection Platform)
- Cloud Security Posture Management (CSPM)
- Gestione delle autorizzazioni dell'infrastruttura cloud (CIEM)

Letture consigliate

Scansiona il codice QR per accedere alle risorse sul DSPM

Sessioni on-demand

- Evento di presentazione: sessione di Zenith Live '24, Zscaler DSPM: proteggi i dati sul cloud con una piattaforma completamente integrata — Scopri il percorso di implementazione del DSPM di Inter&Co.
- Webinar: "Perché una soluzione di DSPM dovrebbe far parte della tua strategia di protezione dati?"

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