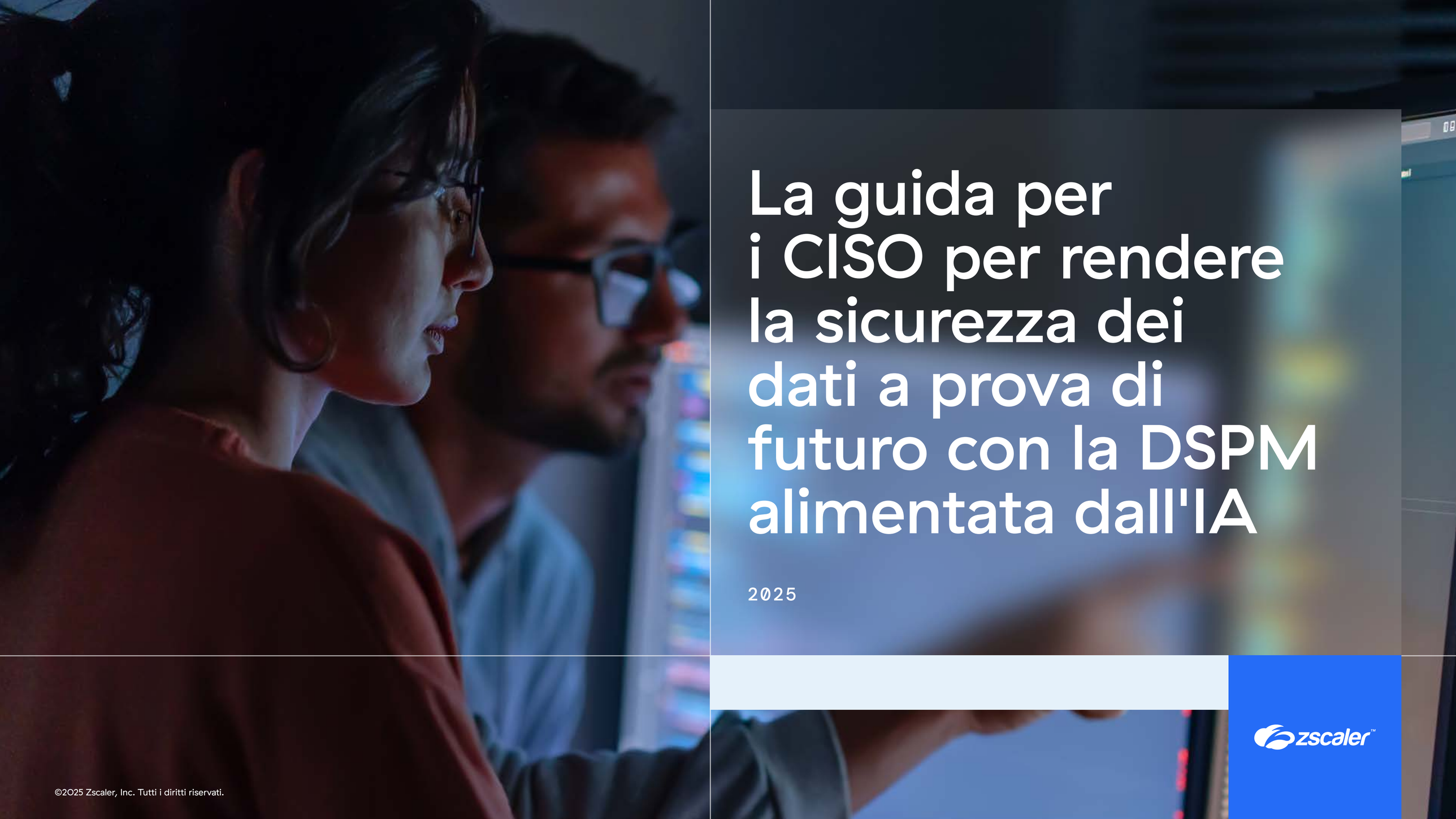


La guida per i CISO per rendere la sicurezza dei dati a prova di futuro con la DSPM alimentata dall'IA

2025

Indice

Come muoversi nel panorama della sicurezza dei dati moderna

La crescita esponenziale del volume dei dati e la relativa dispersione su più piattaforme hanno accresciuto la complessità, i costi e i rischi per molte organizzazioni. I responsabili della sicurezza, oggi, si trovano in grave difficoltà a comprendere a fondo e a tenere sotto controllo i propri dati critici. Questo scenario viene ulteriormente aggravato dalla rapida adozione dell'IA, che disperde ancor di più i dati, rendendo le organizzazioni più vulnerabili ai rischi associati ai dati e alla conformità.

Per mitigare efficacemente i rischi per la sicurezza e garantire una conformità rigorosa, i team addetti alla sicurezza dei dati necessitano di strumenti innovativi che offrano una comprensione approfondita e in tempo reale dell'intero universo di dati. La gestione del profilo di sicurezza dei dati (Data Security Posture Management, DSPM) si è affermata come l'approccio moderno definitivo, che consente ai responsabili della sicurezza dei dati di ottenere tale grado di visibilità continua e comprensione sfruttando l'IA e l'automazione.

Questo utile ebook analizza il potenziale trasformativo della DSPM, offrendo ai responsabili della sicurezza e ai loro team strategie pratiche per salvaguardare in modo proattivo i dati sensibili. Pensato specificamente per i tecnici più esperti che operano negli ambiti della sicurezza e della gestione dei rischi, fornisce informazioni concrete per orientarsi tra le complessità che caratterizzano la sicurezza dei dati moderna. Questa risorsa, in quanto guida completa per potenziare la sicurezza dei dati aziendali, esplora le tendenze critiche, affronta le sfide più urgenti e svela strategie innovative, evidenziando infine il ruolo indispensabile della DSPM nella protezione dei dati nella dinamica era dell'IA.

Un imperativo per i CISO: padroneggiare la sicurezza dei dati nell'era dell'IA

Per i direttori della sicurezza informatica, o CISO (Chief Information Security Officer), la rapida adozione dell'IA e delle tecnologie cloud rappresenta un profondo dilemma. Pur offrendo opportunità senza precedenti in termini di risparmio sui costi, migliori risultati aziendali e notevoli guadagni nella produttività, questa trasformazione digitale introduce al contempo un complesso panorama di sfide per la sicurezza dei dati.

La crescita esplosiva dei dati

Il fulcro di questa sfida risiede nella crescita esplosiva dei dati aziendali. Le informazioni preziose e sensibili non sono più confinate, anzi sono sempre più frammentate e distribuite in ambienti diversi: ecosistemi IA, SaaS, PaaS, distribuzioni multicloud, architetture cloud ibride e infrastrutture tradizionali on-premise. Si tratta di una proliferazione sconcertante e IDC prevede una crescita dei dati a un tasso annuo composto del 21,2%, per raggiungere quota 221.000 exabyte entro il 2026.

Come gestire la complessità e il rischio

Questo contesto rappresenta una sfida enorme per i CISO, che oggi sono chiamati a gestire la sicurezza dei dati in un ecosistema di dati in continua espansione ed effimero. I dati vengono costantemente creati, condivisi e archiviati su centinaia di sistemi e applicazioni diversi in tutta l'azienda, rendendo incredibilmente difficile implementare una protezione integrale.

I principali rischi per la sicurezza dei dati nell'era dell'IA:

- **Rischi legati a vulnerabilità e conformità:** la dispersione e frammentazione dei dati intensificano marcatamente il rischio di incorrere in violazioni e di non risultare conformi alle normative. Garantire il rispetto di regolamenti in continua evoluzione in materia di governance dei dati e privacy (come GDPR, CCPA, ecc.) rappresenta ormai un'impresa titanica.
- **La minaccia dei dati ROT:** la proliferazione incontrollata di dati shadow (anche detti dati ombra, ovvero copie di dati sconosciute o non autorizzate) e di dati abbandonati (dati obsoleti o dimenticati) genera vulnerabilità critiche che spesso portano a significative sviste nella sicurezza ed espandono esponenzialmente la superficie di attacco.
- **Sfide per la sicurezza di IA generativa (GenAI) ed LLM:** l'ascesa dell'IA generativa e dei modelli linguistici di grandi dimensioni (Large Language Models, LLM) introduce una nuova ondata di rischi altamente mirati, come la shadow AI (IA ombra), la fuga dei dati (esposizione involontaria di informazioni sensibili), i problemi correlati alle autorizzazioni all'interno dei sistemi di IA, nonché nuove strade che possono tradursi in violazioni delle normative. Una sicurezza vigile dell'IA e la governance dei dati degli LLM sono pertanto fondamentali.

Per affrontare queste sfide multiformi in materia di sicurezza dei dati è necessario un approccio strategico e proattivo da parte dei CISO, incentrato sull'implementazione di una solida governance dei dati, soluzioni avanzate di protezione dati e framework completi per la sicurezza dell'IA, per salvaguardare le informazioni sensibili in quest'era dinamica.

Il rischio di perdere dati preziosi

Data la crescente ondata di attacchi mirati e un contesto normativo altamente dinamico, è diventato fondamentale per i CISO dare la priorità alla sicurezza di questi ambienti. Circa il 44% delle aziende ha subito una violazione dei dati nel proprio ecosistema cloud negli ultimi 12 mesi.[1] Una violazione dei dati può avere gravi conseguenze, tra cui la fuga dei dati, danni alla reputazione e perdite finanziarie. Man mano che gli attacchi legati ad IA e cloud si fanno sempre più insidiosi, il ruolo del CISO diventa ancora più determinante.

4,44 MLN USD

Il costo medio globale di una violazione dei dati nel 2025[2]

1. Infosecurity Magazine, **Cloud Breaches Impact Nearly Half of Organizations**, 25 giugno 2024.
2. **IBM: Cost of a Data Breach Report 2025**

Per gestire questi rischi e garantire il rispetto delle normative, i responsabili della sicurezza devono conoscere approfonditamente i propri ambienti di dati. Tuttavia, il volume, la varietà e la velocità dei dati rendono difficile implementare una protezione adeguata, e spesso i responsabili non sanno rispondere a domande come:

- Dove sono i dati?
- Quali archivi di dati contengono dati preziosi o sensibili?
- Chi, cosa o quali strumenti IA hanno accesso a questi archivi?
- Come vengono consultati/resi accessibili o condivisi i dati con questi strumenti?
- Qual è il valore dei dati?
- Come vengono gestiti i dati e qual è l'impatto sul profilo di conformità?

Oltre i limiti: perché la sicurezza dei dati tradizionale fallisce nell'era dell'IA

La sicurezza dei dati è radicalmente cambiata. Per molti CISO e i loro team, la risposta convenzionale a delle minacce crescenti è stata quella di accumulare una vasta gamma di strumenti di sicurezza eterogenei. Questi strumenti tradizionali per la sicurezza dei dati si stanno rivelando però altamente inadeguati, non riuscendo a fornire le informazioni e le protezioni critiche realmente necessarie negli ambienti dinamici di oggi.

Le sfide irrisolte della sicurezza dell'IA

Un punto debole critico delle soluzioni legacy risiede nella loro incapacità di affrontare specifici comportamenti, le nuove modalità di errore e i requisiti mirati di governance dei dati imposti dalle tecnologie emergenti. In particolare, si rivelano inefficaci nel salvaguardare LLM, agenti di IA generativa e altri modelli di base. Questi nuovi rischi correlati all'IA richiedono quindi un approccio radicalmente diverso.

Perché è importante introdurre un nuovo paradigma di sicurezza

Con l'emergere di ulteriori minacce sono necessarie non solo delle soluzioni nuove, ma anche un approccio olistico e integrato alla governance dei dati e alla sicurezza nell'era dell'IA. Stiamo parlando di un cambio di paradigma in cui la sicurezza dell'IA non è più un optional secondario, ma una componente fondamentale della strategia generale di sicurezza informatica.

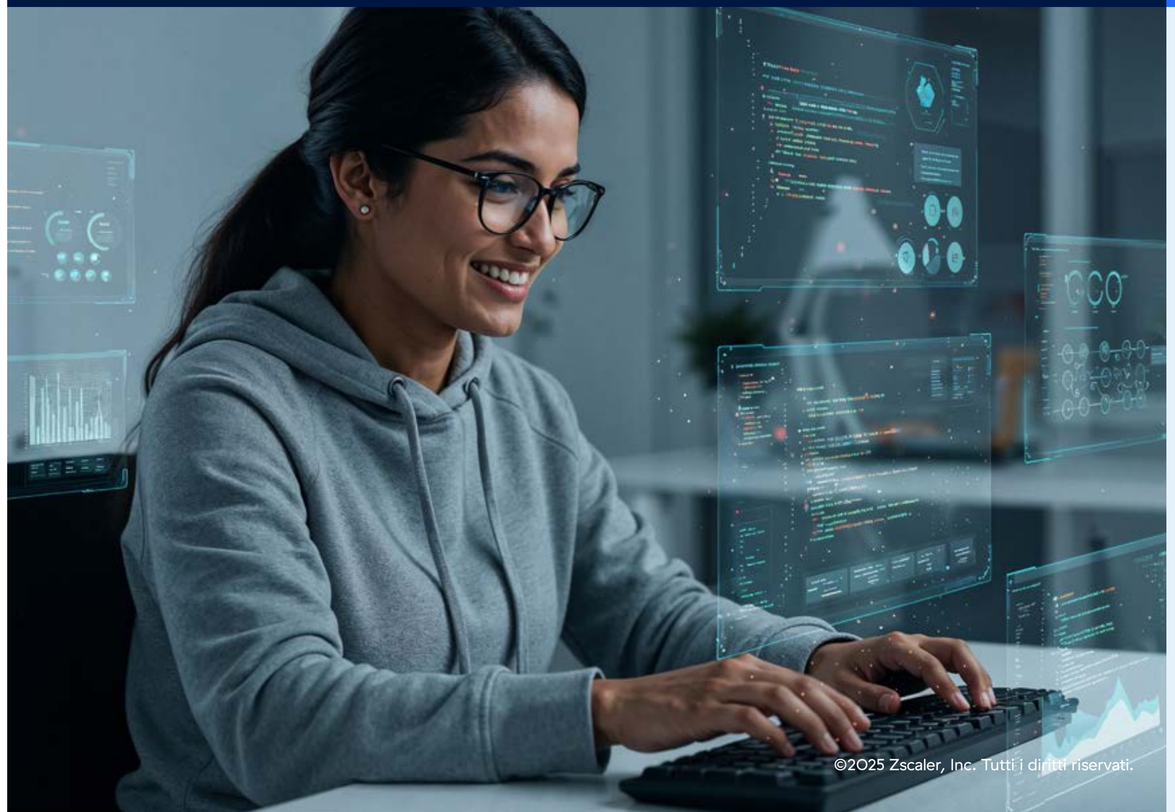
Ottimizzare gli investimenti quando i budget sono limitati

A complicare queste sfide ci sono i budget per la sicurezza che sono sempre più limitati, che costringono i responsabili della sicurezza a valutare e ottimizzare criticamente gli investimenti. L'attenzione si sta spostando marcatamente verso la riduzione della complessità operativa e l'abbattimento dei costi, migliorando al contempo le difese di sicurezza informatica e colmando le lacune critiche nella sicurezza. Paradossalmente, questo investimento strategico spesso include l'utilizzo di sofisticate soluzioni di sicurezza basate sull'IA. Questi strumenti avanzati non devono quindi essere visti solo come una parte del problema, ma anche come potenti risorse per potenziare la visibilità, velocizzare il rilevamento dei rischi e accrescere l'efficienza della risposta agli incidenti, rafforzando in definitiva l'intero profilo di sicurezza contro le minacce dell'era dell'IA.

3. IBM: Cost of a Data Breach Report 2025

97%

delle organizzazioni che hanno segnalato una violazione correlata all'IA non disponeva di adeguati controlli dell'accesso all'IA[3]



Adottare la DSPM: l'imperativo moderno per la sicurezza dei dati IA

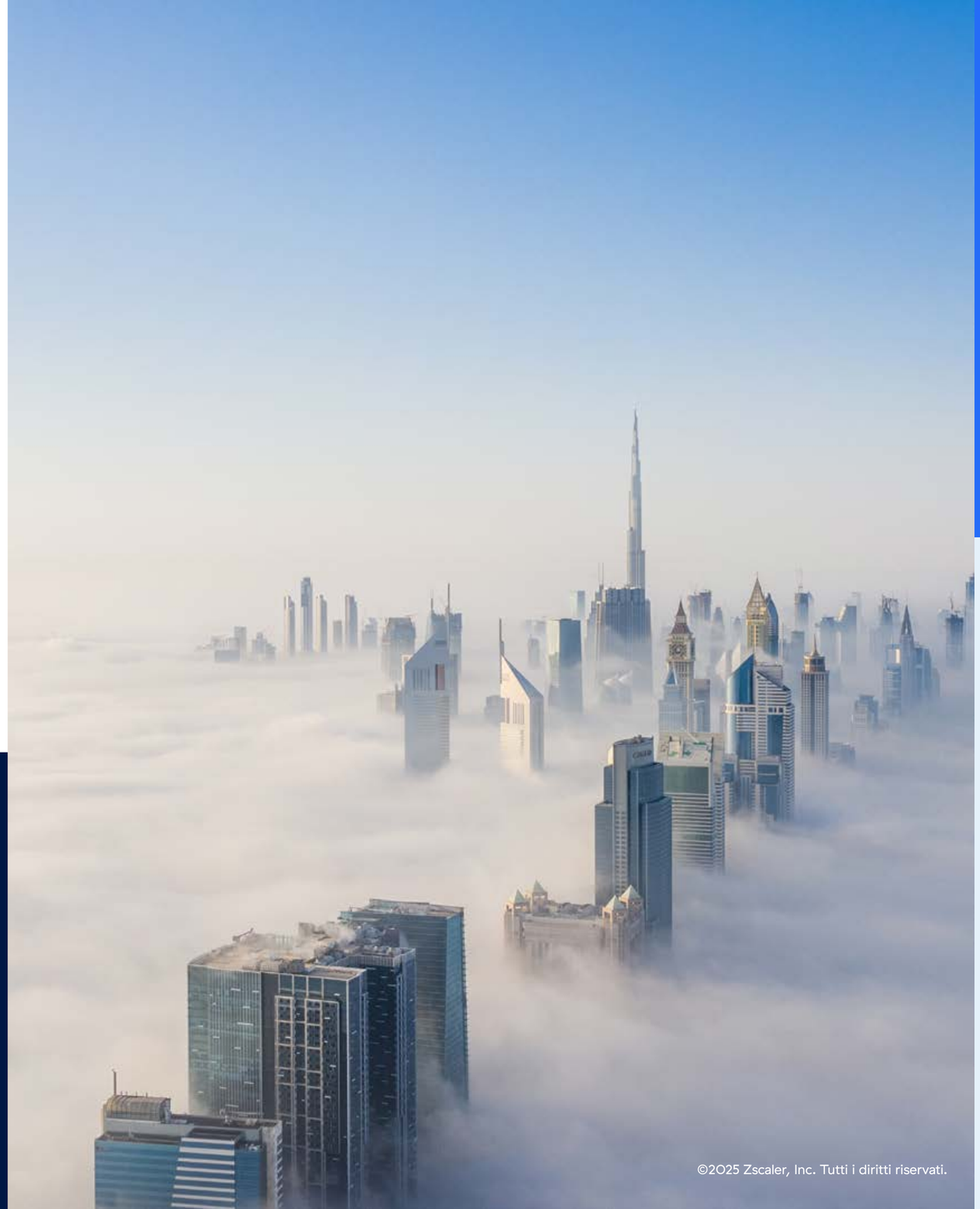
Di fronte ai rischi senza precedenti posti dall'IA e ai limiti noti che caratterizzano gli strumenti tradizionali di sicurezza informatica, un approccio veramente moderno alla sicurezza dei dati non è solo vantaggioso: è essenziale. È qui che la gestione del profilo di sicurezza dei dati (Data Security Posture Management, DSPM) emerge come soluzione chiave e indispensabile.

La DSPM offre il contesto e l'automazione necessari per affrontare con disinvoltura le complessità degli ecosistemi di dati moderni. Adottando una metodologia lungimirante, i CISO possono conoscere in modo più proattivo i propri dati, garantire il rispetto delle normative e ridurre i rischi associati all'utilizzo dell'IA.

4. Ibid.

1,9 MLN USD

Il risparmio medio delle organizzazioni che utilizzano l'IA e l'automazione della sicurezza in modo esteso[4]



In che modo i CISO possono potenziare il profilo di sicurezza dei dati con la DSPM integrata

Ecco alcuni modi in cui i CISO possono utilizzare efficacemente l'IA, l'ML e la correlazione del rischio per potenziare il profilo di sicurezza dei dati:

Come risolvere i problemi relativi a shadow AI, dati shadow e dati abbandonati

Dati shadow I dati shadow e i dati abbandonati presentano rischi critici per la sicurezza, poiché spesso operano al di fuori dell'ambito di applicazione dei protocolli di sicurezza IT e dei framework di governance dei dati. Secondo IBM, il 35% delle violazioni dei dati ha coinvolto i dati shadow e questi incidenti sono stati associati in media un costo superiore del 16%. Inoltre, le violazioni che coinvolgono i dati shadow hanno richiesto il 26,2% di tempo in più per essere identificate e il 20,2% in più per essere contenute[5]. I dati shadow possono essere presenti in file non strutturati, database strutturati, soluzioni di archiviazione sul cloud o in dispositivi personali senza un'adeguata supervisione, mentre i dati abbandonati, privi di un corretto ciclo di vita, possono trasformarsi in una vera e propria passività per le aziende.
Le soluzioni di DSPM impiegano l'IA per individuare costantemente gli archivi dati, migliorando così la visibilità complessiva sull'ecosistema. L'IA può aiutare a catalogare i dati dark e shadow aumentandone la visibilità. I team ricevono inoltre avvisi di sicurezza sui potenziali rischi per ridurre al minimo la possibilità di subire violazioni. Con queste soluzioni, è possibile monitorare le irregolarità nell'accesso ai dati e i pattern, rilevare anomalie e prevedere potenziali violazioni della sicurezza.

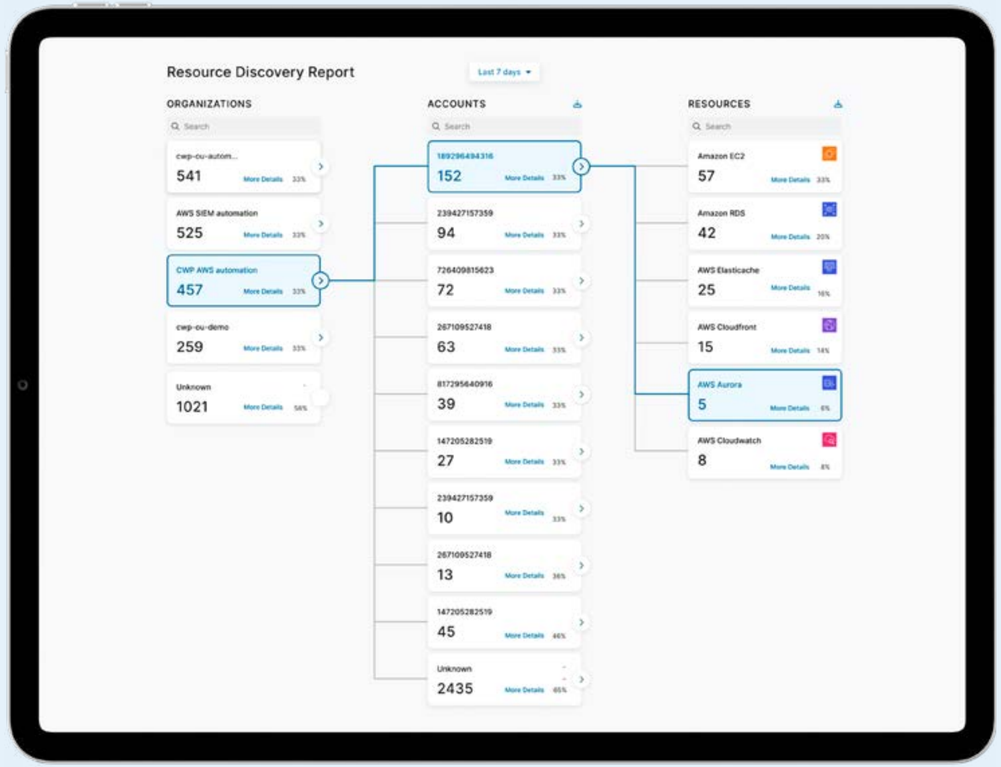
Shadow AI La shadow AI, come lo shadow IT, si riferisce principalmente all'uso di strumenti IA non autorizzati per interagire con dati aziendali sensibili, con conseguenze di vasta portata per la sicurezza e la conformità dei dati. Via via che questi strumenti IA diventano più accessibili e performanti, i dipendenti finiscono per adottarli senza la supervisione dell'IT. Sebbene possa sembrare un comportamento innocuo, in realtà può comportare rischi a cascata che i framework di sicurezza tradizionali non sono in grado di affrontare, in quanto agiscono semplicemente bandendo gli strumenti IA, il che non è sufficiente.

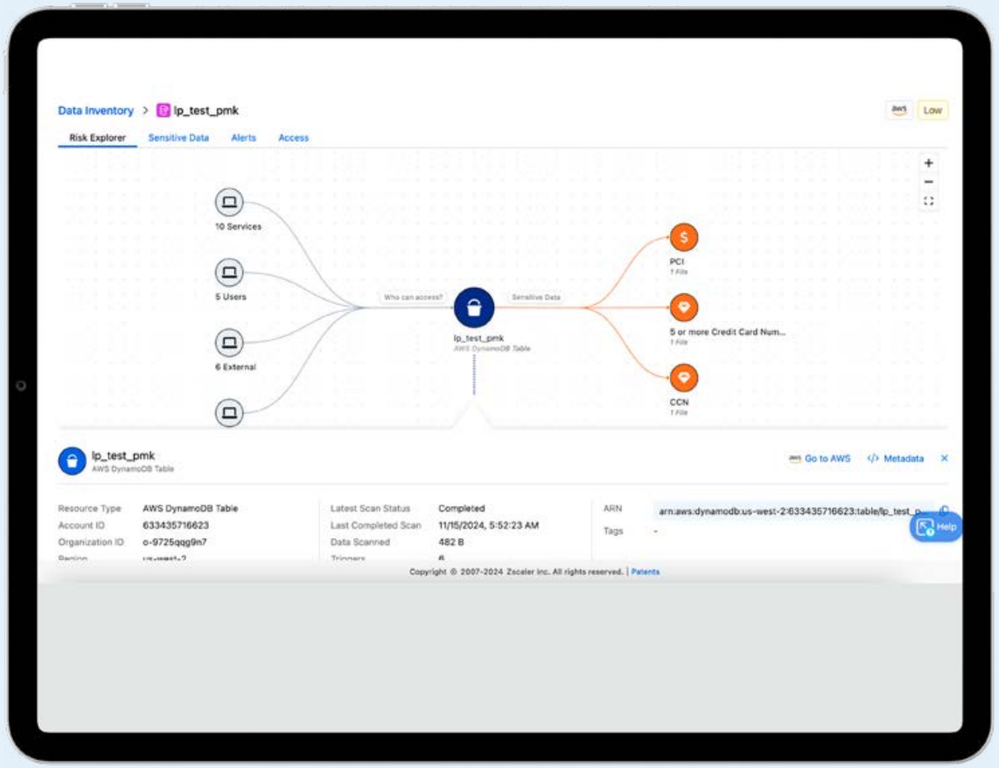
Grazie alla DSPM le organizzazioni possono sfruttare i vantaggi dell'IA. Invece di bloccare o vietare gli strumenti IA, le organizzazioni possono gestire i rischi della shadow AI con la DSPM, riuscendo così a continuare a usufruire appieno dei vantaggi dell'IA. La funzionalità di sicurezza dell'IA integrata nella DSPM aiuta i team a ottenere visibilità e controllo end-to-end sui dati e sui modelli IA, per proteggersi in modo proattivo dai rischi dell'IA. Aiuta a:

- Ottieni una visione completa dei tuoi modelli, agenti e servizi AI
- Identifica e proteggi i dati di training dell'AI da data poisoning, configurazioni errate ed esposizione
- Assicura l'allineamento con i framework di conformità per l'AI nuovi ed emergenti

Con la DSPM i responsabili della sicurezza possono trasformare il caos che aleggia sulla sicurezza in un'innovazione controllata, fornendo un rilevamento unificato dei dati, una valutazione contestuale dei rischi e una governance automatizzata in ogni interazione con l'IA.

5. Ibid.





Classificazione dei dati basata sull'IA

Una classificazione efficace dei dati è un aspetto fondamentale per una sicurezza ottimale dei dati. La mappatura proattiva dei dati sensibili rispetto ai rischi associati è essenziale per evitare le potenziali esposizioni causate da errori di configurazione o pratiche non sicure. Gli approcci convenzionali, spesso basati su procedure manuali o sul riconoscimento di pattern semplicistici, sono soggetti a un elevato numero di falsi positivi e a un'allocazione non ottimale delle risorse di sicurezza. Spesso, le organizzazioni fanno largo uso di soluzioni basate sulle espressioni regolari: un approccio rigido e gravato da falsi positivi, che si è rivelato fragile e inefficiente. Anche gli attuali approcci basati sui prodotti dedicati non sono in grado di integrare la classificazione all'interno di una piattaforma centralizzata e unificata, il che comporta avvisi incoerenti e una visibilità isolata, soprattutto quando i dati si spostano all'interno dell'ecosistema di un'organizzazione.

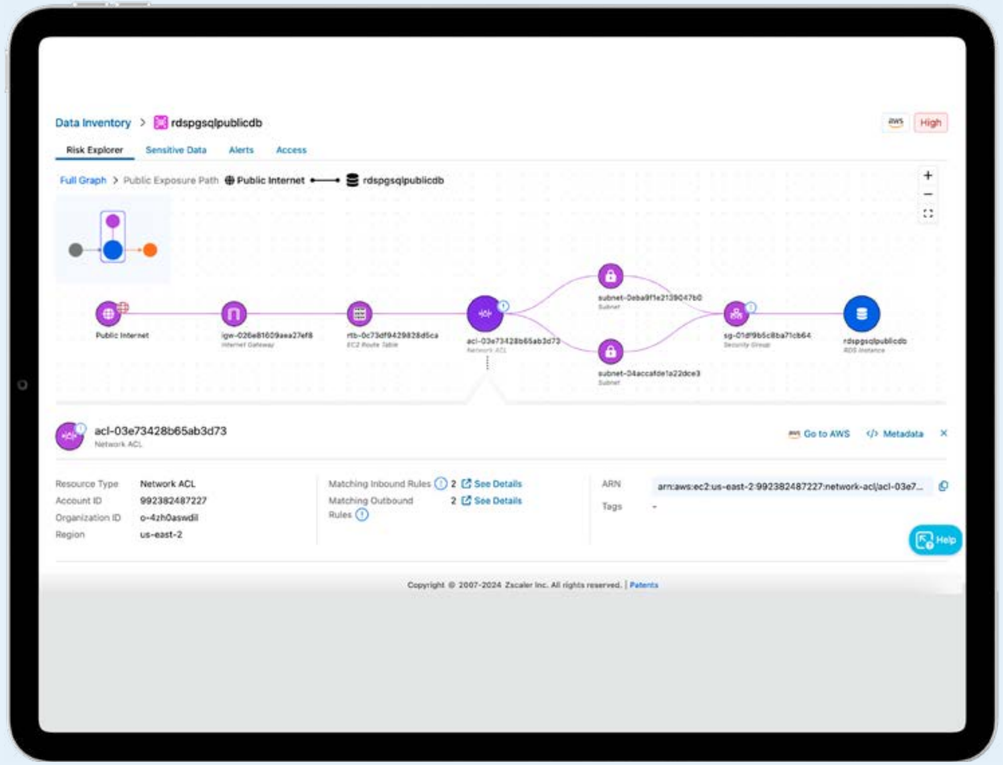
I responsabili della sicurezza possono sfruttare la DSPM che offre la classificazione LLM basata sull'IA, che potenzia le operazioni correlate ai flussi di lavoro regex tradizionali, fornendo visibilità e flessibilità incredibilmente superiori, che consentono di proteggere i dati sensibili noti e sconosciuti come mai prima d'ora. A differenza delle tecniche basate sulle parole chiave, la classificazione LLM permentte di ottenere un'identificazione più approfondita dei contenuti. Utilizza un'elaborazione avanzata del linguaggio per la classificazione dei dati, al fine di comprendere l'intento e il contesto associato ai contenuti, senza bisogno di pattern o parole chiave predefiniti. Ciò consente alle organizzazioni di migliorare le proprie pratiche esistenti, nonché di riuscire a individuare e proteggere nuovi tipi di dati sensibili che in precedenza venivano trascurati o non erano rilevabili.

La gestione proattiva del rischio

Per tenere efficacemente sotto controllo i rischi per la sicurezza e garantire la conformità, i responsabili della sicurezza dei dati devono adottare un approccio proattivo per gestire il proprio profilo. Una delle applicazioni più interessanti dell'IA nell'ambito della sicurezza dei dati è l'approccio proattivo alla sicurezza, oltre all'analisi predittiva. Analizzando e correlando i dati, gli algoritmi IA sono in grado di prevedere i potenziali rischi per la sicurezza. Questo approccio proattivo consente alle organizzazioni di prevenire le minacce e i rischi critici.

La DSPM sfrutta l'IA e tecniche di correlazione avanzate che aiutano a identificare pattern e tendenze nei dati che potrebbero indicare incidenti di sicurezza imminenti. Inoltre, è in grado di assegnare la priorità agli archivi dati in base al relativo valore (gravità del rischio), per fare in modo che gli interventi di sicurezza siano indirizzati alle risorse più critiche. Inoltre, grazie all'automatizzazione di numerose procedure, riduce il carico di lavoro dei professionisti della sicurezza, consente un approccio proattivo alla sicurezza e migliora l'efficienza complessiva delle operazioni.

Ad esempio, la correlazione avanzata di Zscaler DSPM è in grado di collegare proattivamente i punti e rilevare i rischi nascosti, consentendo di dare la priorità alle operazioni più critiche per la sicurezza dei dati.



49%

delle organizzazioni investono nella sicurezza dopo aver subito una violazione[6]

6. IBM: Cost of a Data Breach Report 2025

Come semplificare la conformità attraverso la governance in tempo reale

Preservare la conformità a normative in evoluzione e ai protocolli di sicurezza interni è un pilastro della sicurezza dell'IA e dei dati, sancito da diversi regolamenti come il GDPR o le disposizioni della SEC. Oggi, le organizzazioni devono destreggiarsi non solo tra regolamenti ormai consolidati, come GDPR e HIPAA, ma anche tra quadri normativi emergenti specificamente mirati all'IA, tra cui la legge sull'IA dell'UE, il NIST AI 600 e altri ancora. La sicurezza e il rischio associato alla mancanza di conformità condividono un legame indissolubile, si influenzano profondamente a vicenda e plasmano la traiettoria di un'organizzazione. Le violazioni possono comportare sanzioni dovute alla mancanza di conformità, con gravi ripercussioni, severe sanzioni e danni alla reputazione di un'organizzazione. Al contrario, conformarsi alle normative può fungere da scudo, rafforzando la protezione di IA e dati contro le vulnerabilità e le minacce alla sicurezza.

Molte normative si concentrano sul riconoscimento dell'IA e dei dati sensibili, a limitare chi può accedervi e a monitorare costantemente il rischio. Anche se tutto ciò può sembrare semplice, la complessità degli ecosistemi dei dati può rendere tutto molto impegnativo. Inoltre, le norme sono in continua evoluzione per via delle nuove tecnologie, delle mutevoli preoccupazioni in materia di privacy e della crescente interconnessione dell'economia globale. Questo scenario normativo in costante mutamento richiede una vigilanza e un adattamento continui da parte delle organizzazioni che vogliono mantenere la conformità. Gli approcci tradizionali alla conformità, caratterizzati da viste frammentate, valutazioni manuali e risposte reattive, faticano a garantire trasparenza ed efficienza.

La DSPM può contribuire a semplificare i processi legati alla conformità con funzionalità in tempo reale per la conformità e la governance dei dati. Una soluzione di DSPM fornisce alle organizzazioni una visione più ampia dello stato di conformità dei dati, analisi complete, benchmarking, correzione e reportistica per intervenire rapidamente sulle lacune legate alla conformità. Ciò si rivela particolarmente importante nei settori fortemente regolamentati, in cui è essenziale una chiara comprensione dello stato dei dati e della mitigazione del rischio. Dai passaggi di correzione guidati ai flussi di lavoro automatizzati, la dashboard sulla conformità consente ai team responsabili della sicurezza di agire in modo rapido ed efficace. L'applicazione dell'IA nella governance dei dati garantisce che le organizzazioni possano soddisfare i requisiti normativi, mantenendo al contempo solide misure di sicurezza.

63%

delle organizzazioni non dispongono di policy per la governance dell'IA[7]

7. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

Come implementare l'accesso a privilegi minimi

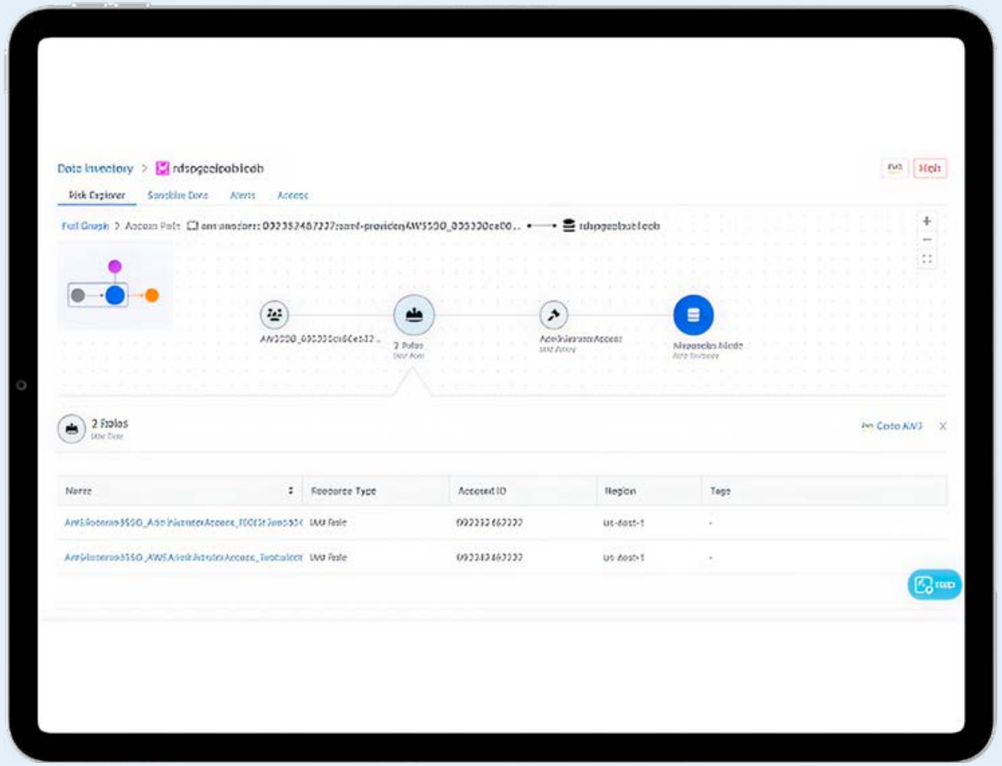
Considerato l'enorme volume di utenti, applicazioni e risorse, gli ecosistemi di dati celano rischi significativi legati a controlli dell'accesso inadeguati, alla proliferazione incontrollata delle identità e a repository orfani. Circa il 90% delle organizzazioni ha subito violazioni legate alle identità, che si sono tradotte in costosi incidenti di sicurezza.

Questo contesto è aggravato dai modelli IA e dagli strumenti basati sugli LLM, che introducono ulteriori rischi legati all'accesso non autorizzato ai dati, I principali rischi includono la divulgazione involontaria o non autorizzata dei dati sensibili, l'esfiltrazione dei dati (in cui i dati sensibili vengono rubati tramite gli output dell'IA), oltre alla possibilità di incorrere in attacchi sofisticati, dove le identità compromesse sfruttano i sistemi IA per ottenere un accesso non autorizzato.

Ecco perché garantire l'accesso a privilegi minimi agli archivi dati è un principio imprescindibile per garantire la sicurezza dei dati. La governance dell'accesso ai dati è resa più difficoltosa dalla proliferazione di dati e autorizzazioni e dalle complesse architetture dei sistemi IA e multicloud. Ciononostante, resta una componente essenziale della sicurezza dei dati, poiché l'esposizione non autorizzata dei dati sensibili è in genere il primo passo di un attacco sofisticato.

La DSPM offre un approccio unificato alla governance dell'accesso ai dati con un monitoraggio continuo della sicurezza dei dati e del comportamento degli utenti. Esamina attentamente i ruoli di gestione dell'accesso ai dati e l'identità, le autorizzazioni e gli attributi correlati per identificare rapidamente i percorsi di accesso agli archivi dati più a rischio. Inoltre, la DSPM supporta sia i dati strutturati che non strutturati, in ambienti on-premise, multicloud e SaaS, consentendo alle organizzazioni di identificare e affrontare in modo coerente i rischi correlati all'accesso e di applicare policy di accesso in diversi ambienti di dati ed ecosistemi IA. Grazie alle informazioni dettagliate che ricevono sui pattern di accesso e sulle potenziali vulnerabilità, i team responsabili della sicurezza dei dati riescono a implementare in modo più efficace l'accesso a privilegi minimi. Questo approccio riduce il rischio di accessi non autorizzati e migliora la sicurezza complessiva dell'ecosistema dei dati.

8. Studio di Security Today: "**Nell'ultimo anno, il 90% delle organizzazioni ha subito un incidente correlato alle identità**", 5 giugno 2024.



90%

delle organizzazioni ha subito un incidente correlato alle identità[8]

Come ottimizzare i costi di archiviazione e utilizzo

I team responsabili dei dati devono ottimizzare i costi di archiviazione e di utilizzo identificando i repository di dati duplicati o non più utilizzati che possono essere eliminati o trasferiti a soluzioni di archiviazione più convenienti. I metodi convenzionali spesso non sono in grado di identificare e gestire questi dati, con conseguenti spese di archiviazione superflue.

Le soluzioni di DSPM rispondono a questo problema fornendo informazioni sugli archivi dati duplicati o abbandonati, consentendo alle organizzazioni di adottare le dovute misure. Per fare un esempio, Zscaler DSPM fornisce una visione completa degli archivi dati duplicati o abbandonati, permettendo ai team di identificare i dati che possono essere eliminati o spostati in modo sicuro.

Grazie alle informazioni basate sull'AI, le organizzazioni possono abbattere le spese superflue per l'archiviazione e garantire la corretta gestione e protezione delle informazioni sensibili.

Come applicare policy unificate in tutti gli ecosistemi di dati

Con i metodi tradizionali, è molto complicato preservare la coerenza delle policy per la sicurezza dei dati in ambienti diversi. Le soluzioni di DSPM rispondono a questo problema offrendo un approccio unificato alla sicurezza dei dati negli ambienti multicloud, consentendo alle organizzazioni di applicare policy uniformi in tutti gli ecosistemi di dati.

Zscaler DSPM offre una strategia unificata per la sicurezza dei dati. Consentendo alle organizzazioni di definire policy uniformi per tutti gli ambienti di dati, garantisce una sorveglianza totale sui dati cloud e semplifica il processo di identificazione e risoluzione dei rischi. Utilizzando informazioni basate su IA ed ML, le organizzazioni possono ridurre il rischio di subire violazioni dei dati e riuscire a conformarsi alle normative sulla protezione dati.

Risposta rapida agli incidenti

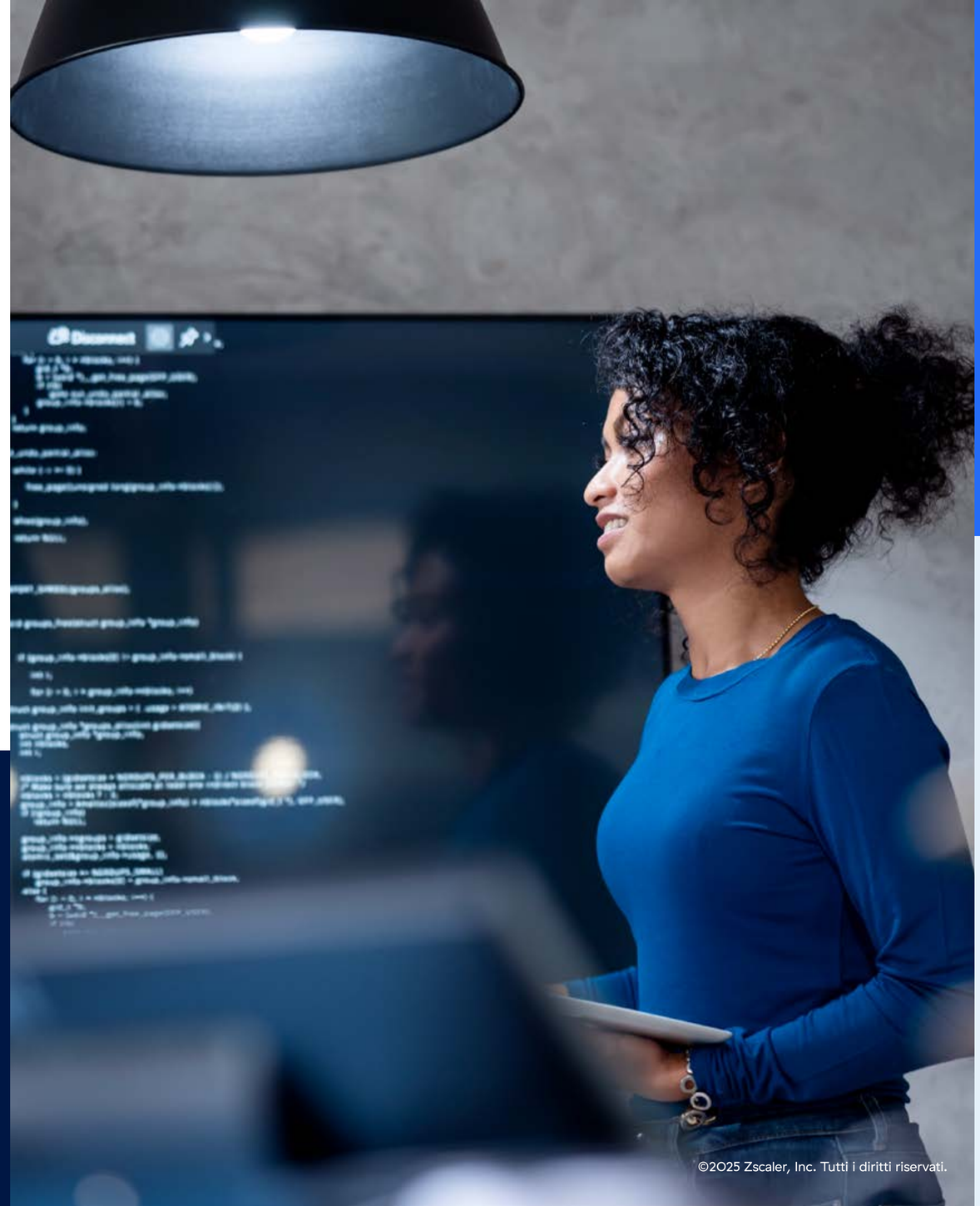
L'identificazione e la mitigazione dei rischi sono compiti fondamentali per i professionisti della sicurezza dei dati. La velocità con cui le minacce si evolvono richiede la capacità di reagire in tempo reale. Le metodologie convenzionali però potrebbero vacillare di fronte a un contesto di minacce guidate dall'IA e altamente dinamiche. L'automazione della sicurezza basata sull'IA è la risposta a questa sfida.

La DSPM è in grado di monitorare costantemente i dati, rilevare le anomalie e contribuire a rispondere alle minacce. Le soluzioni di DSPM rafforzano la mitigazione del rischio, offrendo una correlazione sofisticata dei rischi e un'intelligence sull'accesso adattivo. Alcune soluzioni di DSPM, come Zscaler DSPM, integrano inoltre l'intelligence sulle minacce di Zscaler ThreatLabz, un'attenta procedura di correzione guidata e un'implementazione rapida della sicurezza. Grazie alla correlazione sofisticata delle minacce basata sull'IA, le organizzazioni riescono a far luce sui rischi latenti e i vettori di attacco più critici, riuscendo così a concentrare gli sforzi sulle criticità più urgenti.

9. Statista: "**Tempo medio per identificare e contenere le violazioni dei dati a livello globale, dal 2017 al 2024**", consultato il 9 dicembre 2024.

194 giorni

Il tempo medio per identificare una violazione dei dati[9]



Come potenziare la sicurezza dell'IA

Le organizzazioni stanno adottando applicazioni IA a un ritmo vertiginoso. Sfortunatamente però, le applicazioni IA, come l'IA generativa (GenAI) e i modelli linguistici di grandi dimensioni (LLM), hanno intensificato il rischio di subire violazioni dei dati e di non risultare conformi alle normative. Un recente report ha rivelato che il 13% delle organizzazioni ha segnalato violazioni di modelli o applicazioni IA[10], evidenziando che l'IA si sta trasformando in un obiettivo di alto valore.

Le organizzazioni che integrano la GenAI nelle proprie operazioni devono adottare le dovute misure per impedire l'uso involontario dei dati sensibili all'interno di questi modelli. I team responsabili della sicurezza devono dare la priorità alla segnalazione, all'etichettatura e alla classificazione dei dati per garantire che i vari team impieghino la GenAI in modo responsabile.

La DSPM è in grado di migliorare il controllo e la protezione dei dati negli ambienti di GenAI, grazie alle funzionalità integrate di AI-SPM, ovvero per la gestione del profilo di sicurezza dell'IA. Identificando e categorizzando meticolosamente i dati, la DSPM può impedire che le informazioni sensibili vengano fornite agli LLM, riducendo il rischio associato sia alle violazioni dei dati che alla mancanza di conformità. La DSPM adotta un approccio orientato ai dati, concentrandosi sulla protezione delle informazioni che alimentano l'IA, anziché solamente sull'infrastruttura. Rilevando, classificando e monitorando costantemente i dati durante tutto il loro ciclo di vita, la DSPM contribuisce a mitigare i rischi specifici per la sicurezza dell'IA, come l'avvelenamento dei dati (o data poisoning), l'esposizione dei dati sensibili e il furto dei modelli.

L'adozione di una soluzione di DSPM con funzionalità di AI-SPM integrate consente e alle organizzazioni di utilizzare le proprie applicazioni IA in totale sicurezza. In questo modo, non solo proteggono i loro dati più importanti, ma rendono anche le applicazioni IA più affidabili e sicure.

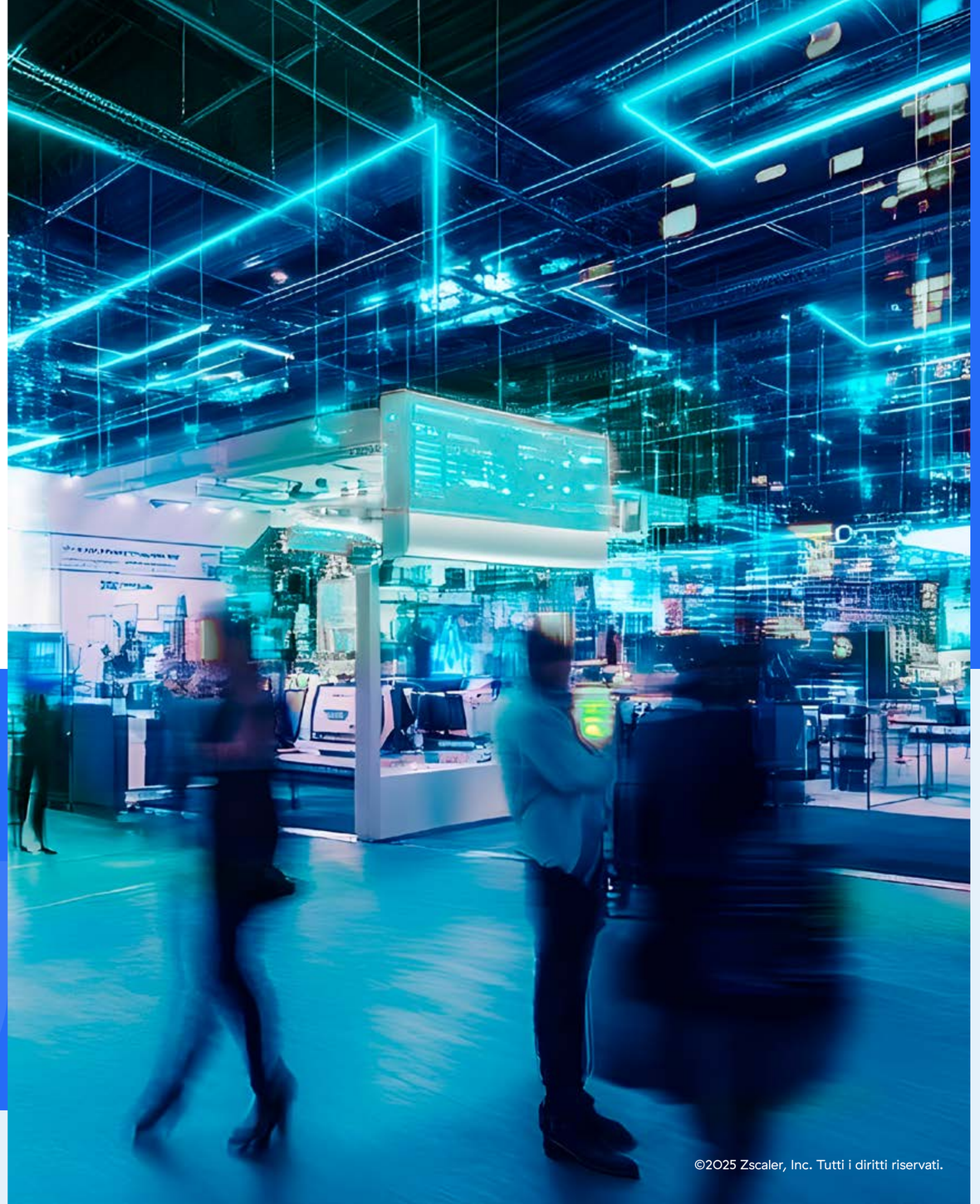
10. https://newsroom.ibm.com/2025-07-30-ibm-report-13-of-organizations-reported-breaches-of-ai-models-or-applications,-97-of-which-reported-lacking-proper-ai-access-controls

Come sfruttare la DSPM per proteggere un ecosistema di dati diversificato

L'uso strategico della DSPM è fondamentale per ottenere una sicurezza dei dati più solida. Queste tecnologie offrono il contesto e l'automazione necessari per gestire in modo efficace le complessità degli ecosistemi di dati moderni. Grazie a un approccio proattivo, i responsabili della sicurezza possono tutelare in modo più efficace i dati sensibili, garantire la conformità e mitigare i rischi associati a tecnologie all'avanguardia come la GenAI.

"Entro il 2026, oltre il 20% delle organizzazioni implementerà una tecnologia di DSPM per rispondere agli urgenti requisiti relativi all'identificazione e alla localizzazione degli archivi dati precedentemente sconosciuti e alla mitigazione dei rischi associati a sicurezza e privacy".

Gartner, Innovation Insight: Data Security Posture Management,
Brian Lowans, Joerg Fritsch, Andrew Bales,
28 marzo 2023



Zscaler DSPM

Zscaler DSPM è la piattaforma integrata di protezione dati più completa al mondo, in grado di proteggere i dati strutturati e non strutturati coprendo SaaS, ambienti cloud pubblici (AWS, Azure, GCP) e on-premise ed endpoint.

Zscaler DSPM fornisce 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 alle organizzazioni e ai team di sicurezza di prevenire e risolvere le violazioni dei dati sul cloud su larga scala.

Zscaler DSPM adotta un approccio unificato basato sull'IA per garantire una solida igiene dei dati in tutti gli archivi dati, inclusi IaaS, SaaS, ambienti on-premise, endpoint e altro ancora. Grazie all'integrazione nativa con la piattaforma Zscaler Data Security, i dati possono essere analizzati e tenuti sotto controllo tutti da un'unica piattaforma.

La piattaforma Zscaler Data Security utilizza un motore di DLP singolo e unificato per offrire una protezione dati coerente e di altissimo livello 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.

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

Fai un tour interattivo del prodotto di DSPM

Perché una soluzione di DSPM dovrebbe far parte della tua strategia di protezione dati?

Guarda il webinar on-demand ⟶

Scansiona il codice QR per accedere alle risorse utili sulla DSPM:

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. La piattaforma Zscaler Zero Trust Exchange™ protegge migliaia di clienti dagli attacchi informatici e dalla perdita dei dati, collegando in modo sicuro utenti, dispositivi e applicazioni in qualsiasi luogo. Distribuita in oltre 150 data center a livello globale, Zero Trust Exchange™, basata sul framework SSE, è la più grande piattaforma di cloud security inline del mondo. Per saperne di più, visita **www.zscaler.com/it** oppure seguici su X (precedentemente Twitter) **@zscaler**.

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