

Proofpoint Data Security Posture Management

Scopri e proteggi i dati sulle piattaforme SaaS, l'infrastruttura cloud e gli ambienti on premise



Vantaggi principali

- **I classificatori basati sull'IA** identificano i dati sensibili e specifici dell'azienda senza regole manuali negli ambienti SaaS, cloud e on premise.
- **La Data Risk Map** assegna le priorità ai rischi in base alla sensibilità, all'accesso, all'impatto aziendale e allo spostamento dei dati.
- **La governance dell'accesso sensibile ai processi aziendali** semplifica le attività di applicazione di misure correttive dirette e delegate, nonché la creazione di policy DLP.
- **La sicurezza dei dati integrata, ottimizzata dall'IA**, identifica i dati sensibili esposti alle applicazioni di IA e alle pipeline di addestramento dell'IA.
- **Le dashboard di conformità** monitorano il livello di sicurezza rispetto a oltre 25 framework con reportistica fruibile.
- **La sicurezza dei dati unificata** condivide le informazioni pertinenti tra le soluzioni DSPM, DLP, Data Security for AI e di governance degli accessi.

L'esplosione dei dati aziendali

L'avvento dell'IA, delle piattaforme DBaaS (Database as a Service) e dell'archiviazione cloud ha accelerato la proliferazione dei dati on premise, nel cloud e nelle applicazioni SaaS. Dal momento che i dati sensibili sono sparsi in sistemi e pipeline, per i team è sempre più complesso stabilire la loro esatta posizione. Ciò crea punti ciechi in termini di sicurezza, aumenta il rischio di esposizione e complica il raggiungimento della conformità.

Le conseguenze di un accesso incontrollato

Tale proliferazione dei dati è amplificata dalla mancanza di controllo su chi e cosa può accedere alle informazioni sensibili. Utenti con privilegi eccessivi, strumenti non autorizzati e condivisioni rischiose creano un rischio di origine umana. I modelli di IA, gli agenti e i flussi di lavoro automatizzati aggiungono nuovi vettori non umani. In assenza di una governance rigorosa, gli errori di configurazione, le autorizzazioni eccessive e una supervisione inadeguata possono causare perdite di dati, usi impropri e violazioni della conformità.

55%

le aziende che affermano che tra il 21% e il 40% dei loro dati sono sensibili.

Fonte: Proofpoint

68%

le aziende che affermano che un uso improprio dell'IA ha esposto dati sensibili.

Fonte: Proofpoint

Scoprire, classificare, governare e proteggere i dati

Proofpoint Data Security Posture Management (DSPM) aiuta i team a riprendere il controllo dei dati frammentati e ridurre gli accessi a rischio da parte di esseri umani e dell'IA. La soluzione identifica e classifica i dati sensibili, indica gli utenti e le entità che possono accedervi e stabilisce le priorità dei rischi. I team possono risolvere più rapidamente le vulnerabilità e rafforzare la sicurezza dei dati.

Funzionalità uniche

Nell'ambito della sicurezza dei dati di Proofpoint, la soluzione DSPM con la governance dell'accesso integrata, condivide il suo framework di classificazione dei dati con Proofpoint Enterprise DLP e Proofpoint Data Security for AI. I classificatori basati sull'IA identificano le categorie di documenti sensibili in base al contesto e al significato, non solo a partire dai modelli. L'identificazione e la classificazione sono così ottimizzati. La soluzione aiuta inoltre i team a governare gli accessi, creare policy DLP e proteggere i dati in ambienti cloud, SaaS, on premise e IA.

Proofpoint DSPM individua autorizzazioni eccessive, accessi a rischio, errori di configurazione, dati obsoleti e percorsi d'attacco. La Data Risk Map mostra dove si trovano i dati sensibili, quanto sono esposti e quali utenti, applicazioni e strumenti di IA possono accedervi. I flussi di lavoro di governance dell'accesso ai dati supportano l'applicazione di misure correttive in blocco e delegata. I risultati DSPM possono essere convertiti in regole DLP in soli pochi clic in modo che i team possano ridurre l'esposizione e far rispettare il principio del minimo privilegio.

Proofpoint DSPM consente un'adozione più sicura dell'IA. Il sistema rileva i dati sensibili esposti ai copiloti, ai modelli linguistici di grandi dimensioni (LLM) e alle applicazioni di IA.

Insieme alla governance dell'accesso ai dati, Enterprise DLP e Data Security for AI, DSPM offre ai team un modo unico per identificare, governare e proteggere i dati sensibili durante tutto il loro ciclo di vita.

Classificazione autonoma di documenti strategici

Proofpoint DSPM offre una classificazione dei dati di prim'ordine. Utilizza espressioni regolari, elaborazione del linguaggio naturale e LLM per migliorare le prestazioni e ridurre il consumo di risorse.

Proofpoint Autonomous Custom Classification (ACC) identifica i documenti specifici dell'azienda senza bisogno di regole manuali o formazione. I team possono identificare i dati proprietari, eliminare i punti ciechi in termini di visibilità e migliorare il rilevamento dei rischi e l'applicazione delle policy.

La soluzione DSPM può anche applicare etichette di sensibilità Microsoft Information Protection (MIP) basate su classificatori basati sull'IA. Questo aiuta i team a far rispettare le policy di governance, supportare la conformità e proteggere i dati Microsoft da accessi non autorizzati o usi impropri.

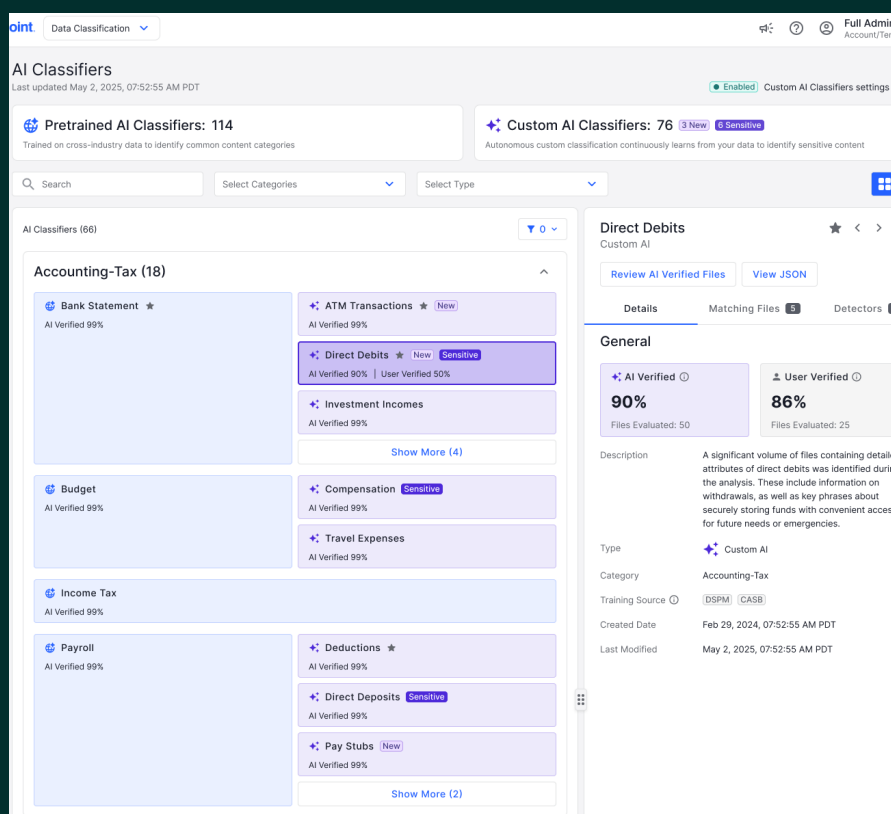


Figura 1. I classificatori basati sull'IA, pre-addestrati e autonomi di DSPM identificano documenti standard e specifici dell'azienda, inclusi contratti, documenti finanziari, codice sorgente e dati dei collaboratori.

Mappatura dei rischi di accesso ai dati

La Data Risk Map mostra dove si trovano i dati sensibili nei sistemi SaaS e on premise. Illustra il perimetro di condivisione dei dati nonché gli utenti, le applicazioni e gli strumenti di IA che possono accedervi. Combina la classificazione basata sull'IA con informazioni sull'accesso e sull'utilizzo.

I team della sicurezza possono identificare i dati esposti in modo eccessivo, assegnare le priorità ai rischi, convalidare le correzioni e verificare la pertinenza degli accessi man mano che l'uso dell'IA si diffonde. I risultati dell'analisi dei rischi tengono conto della sensibilità dei dati, delle modalità di accesso e dell'esposizione. Queste informazioni aiutano i team a concentrarsi sui dati di alto valore e ad alto rischio, riducendo al contempo i costi e la superficie di rischio dell'azienda.

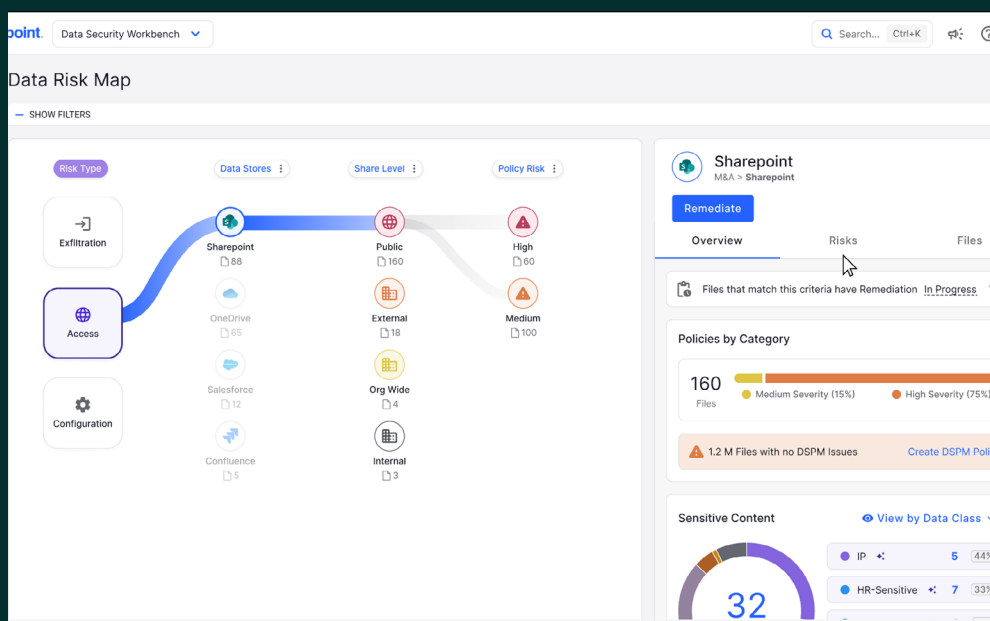


Figura 2. La Data Risk Map mostra quali archivi contengono dati sensibili, l'ambito della condivisione dei dati e l'accesso da parte di utenti, applicazioni e strumenti di IA.

Assegnare le priorità ai rischi in base al valore monetario dei dati

I team della sicurezza dei dati devono proteggere numerosi archivi di dati. Ma non tutti gli archivi hanno lo stesso valore o livello di rischio. DSPM utilizza una tecnologia di valutazione dei dati per stimare il costo di una violazione per ogni archivio dati. I team possono così concentrarsi sulle risorse più importanti. DSPM include inoltre oltre 200 risultati di analisi predefiniti sull'accesso e l'esposizione, con rilevamento di combinazioni tossiche. Questa matrice dei rischi mette in evidenza gli archivi di dati a rischio elevato e a forte impatto finanziario.

Ridurre i dati obsoleti

Nei sistemi SaaS e on premise, DSPM individua e rimuove i file che non sono stati consultati di recente. I classificatori basati sull'IA aiutano i team a conservare i dati strategici necessari. Negli ambienti IaaS (Infrastructure as a Service), DSPM identifica gli archivi di dati non necessari. Si tratta, per esempio, di dati shadow, duplicati e abbandonati, come backup e snapshot obsoleti.

Tale approccio riduce i costi di archiviazione, diminuisce la superficie d'attacco e semplifica la gestione dei dati. I team conservano solo i dati rilevanti e attivi.

Garantire il principio del minimo privilegio

Proofpoint DSPM supporta l'accesso secondo il principio del minimo privilegio identificando gli utenti con autorizzazioni eccessive, gli accessi inutilizzati e gli account a rischio nei diversi archivi di dati. Ciò rafforza la governance dell'accesso ai dati e la strategia Zero Trust dell'azienda.

La soluzione analizza i ruoli di gestione delle identità e degli accessi (IAM), le autorizzazioni, i diritti di accesso al database e altri controlli di accesso per le identità umane e delle macchine. Indica chi può accedere ai dati sensibili in tempo quasi reale. I team possono rimuovere le autorizzazioni non necessarie e ridurre l'esposizione al rischio.

Proofpoint DSPM segnala inoltre gli account con protezione insufficiente negli ambienti SaaS e PaaS (Platform as a Service). Per esempio, gli utenti con accesso a dati sensibili senza autenticazione a più fattori (MFA), gli account inattivi e le applicazioni con privilegi amministrativi eccessivi.

Rilevare i percorsi di attacco negli ambienti cloud

Proofpoint DSPM raccoglie informazioni sulle risorse di calcolo e di rete, nonché sui servizi PaaS e SaaS, presso i diversi fornitori di servizi cloud. Rileva gli errori di configurazione e le vulnerabilità in tali risorse. Un grafico mostra i percorsi che un malintenzionato potrebbe utilizzare per accedere a dati sensibili. Il monitoraggio in tempo quasi reale aiuta i team a individuare i cambiamenti che incrementano l'esposizione.

Le informazioni sulla sensibilità dei dati, sui modelli di accesso e sui rischi supportano anche gli strumenti DLP e DDR (Data Detection and Response).

Governare gli accessi direttamente o tramite delega

Nei sistemi SaaS e on premise, i flussi di lavoro DSPM trasformano le informazioni sulle esposizioni di dati in azioni concrete. Poiché strumenti di IA come Microsoft Copilot aumentano l'impatto della condivisione eccessiva, ridurre gli accessi troppo estesi diventa fondamentale. Gli amministratori possono revocare i link pubblici, le condivisioni esterne e l'accesso a livello di dominio su Google Workspace e Microsoft 365. Tale azione permette interventi di applicazione di misure correttive su scala aziendale.

I team della sicurezza non sono in grado, da soli, di valutare il livello di accesso appropriato per ogni singolo file. I flussi di lavoro di governance dell'accesso ai dati consentono loro di assegnare valutazioni di accesso ai proprietari dei contenuti. Campagne automatizzate, promemoria e monitoraggio rendono la governance più facile da sostenere.

L'integrazione con Enterprise DLP estende la protezione oltre i dati a riposo. I dati sensibili classificati e i rischi ordinati per priorità da DSPM possono essere associati alle policy DLP. Ciò favorisce una protezione coerente e una correzione automatizzata per email, endpoint, cloud e canali di collaborazione.

Negli ambienti IaaS e PaaS, informazioni e raccomandazioni concrete aiutano i team a ridurre rapidamente le esposizioni. Le integrazioni con piattaforme di gestione dei ticket, notifica e automazione aiutano gli operatori della sicurezza a collaborare con i team DevOps e di ingegneria della piattaforma attraverso i flussi di lavoro esistenti.

Allineamento ai framework di conformità

Proofpoint DSPM può identificare le lacune di conformità in materia di privacy e sicurezza per oltre 25 framework normativi, tra cui la legge europea sull'IA, GDPR, HIPAA, NIST, CMMC, SOC 2, ecc.

Le violazioni vengono contrassegnate sia per framework che per controllo, in modo che gli analisti possano valutarne l'impatto sulla conformità.

I report mostrano lo stato di conformità dell'intera infrastruttura, con visualizzazioni per account, risorsa e framework. Questo aiuta i team a correggere le vulnerabilità, prepararsi per gli audit e mantenere la conformità.

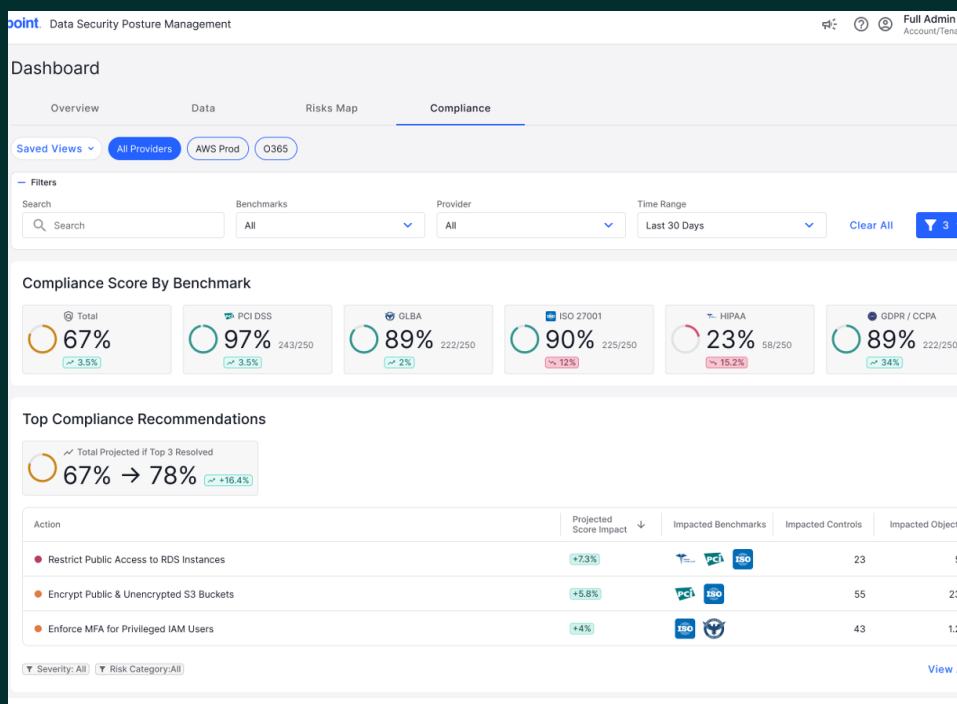


Figura 3. Dashboard che evidenzia il livello di conformità.

Ridurre i rischi di esposizione dei dati all'IA

DSPM aiuta le aziende a gestire la presenza dell'IA identificando i dati sensibili esposti alle applicazioni e ai flussi di lavoro dell'IA.

La soluzione alimenta la dashboard Proofpoint Data Security for AI con informazioni sull'esposizione. La dashboard offre una visione centralizzata dei rischi legati ai dati nelle applicazioni di IA approvate e non approvate. DSPM monitora anche gli errori di configurazione delle applicazioni di IA e aiuta i team a correggerle, riducendo il rischio di perdita di dati, rafforzando la governance dei dati dell'IA e favorendo un'adozione sicura.

Proofpoint DSPM protegge gli LLM personalizzati e le applicazioni di IA su piattaforme come AWS Bedrock e Azure ML. Rileva i dati sensibili inseriti nei modelli di base, nei modelli personalizzati e nei flussi di lavoro di generazione aumentata tramite recupero (RAG).

DSPM fornisce anche API specializzate per la sicurezza degli LLM. Oltre a analizzare in tempo reale i dati sensibili in entrata e in uscita dagli LLM, queste API assicurano la governance e la visibilità sull'utilizzo dei dati e si integrano nei flussi di lavoro dei clienti.

Piattaforme e tecnologie supportate

Proofpoint DSPM identifica e classifica i dati su numerose piattaforme e servizi. Supporta un'ampia gamma di archivi di dati, dai database relazionali ai database agli archivi NoSQL e key-value. I team dispongono di visibilità sui dati strutturati, non strutturati e semi-strutturati.

La soluzione supporta le principali piattaforme cloud e SaaS, tra cui AWS, Azure, Google Cloud Platform (GCP), Snowflake, Salesforce, ServiceNow, Workday, LLM e copiloti.

Il framework comune di identificazione e classificazione consente a Proofpoint di aggiungere rapidamente il supporto per nuovi archivi di dati.

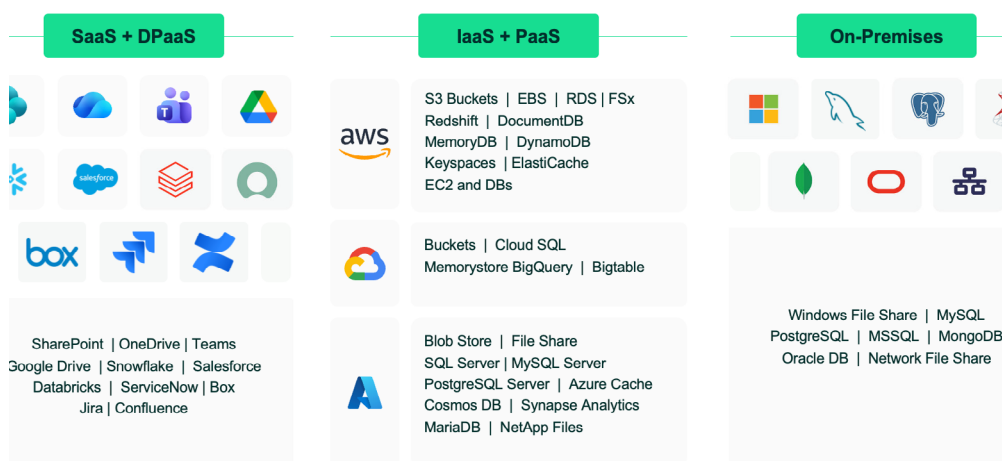


Figura 4. DSPM identifica e classifica i dati su un'ampia gamma di piattaforme e servizi.

Conclusione

Man mano che le aziende adottano l'IA e gestiscono una maggiore quantità di dati, le aziende devono sapere dove si trovano i dati sensibili, chi può accedervi e come vengono utilizzati. Proofpoint DSPM riduce l'esposizione classificando dati sensibili e rischi, identificando gli accessi eccessivi e applicando il principio del minimo privilegio in ambienti cloud, SaaS, on premise e IA.

Nell'ambito delle soluzioni Proofpoint di sicurezza dei dati, Proofpoint DSPM collabora con Proofpoint Enterprise DLP. Insieme, aiutano i team a scoprire, classificare, gestire e proteggere i dati sensibili. Le aziende possono rafforzare la conformità, garantire l'adozione dell'IA, ridurre i rischi e proteggere le proprie informazioni più preziose.

Informazioni su Proofpoint. Inc. Proofpoint, Inc. è un'azienda leader globale nella cybersecurity incentrata sulle persone e sugli agenti, che protegge il modo in cui persone, dati e agenti IA si connettono tramite email, cloud e strumenti di collaborazione. Proofpoint è un partner di fiducia per oltre 80 aziende della classifica Fortune 100, oltre 10.000 grandi imprese e milioni di aziende più piccole, per contrastare le minacce, prevenire la perdita di dati e rafforzare la resilienza di persone e processi di IA. La piattaforma di collaborazione e sicurezza dei dati di Proofpoint aiuta aziende di tutte le dimensioni a proteggere e responsabilizzare i propri collaboratori in modo che possano adottare l'IA in modo sicuro e con fiducia. Per saperne di più, visita www.proofpoint.com/it.

Seguici: [LinkedIn](#)

Proofpoint è un marchio registrato o nome commerciale di Proofpoint, Inc. negli Stati Uniti e/o in altri Paesi. Tutti gli altri marchi qui menzionati appartengono ai rispettivi proprietari.