

Forcepoint Data Security Posture Management

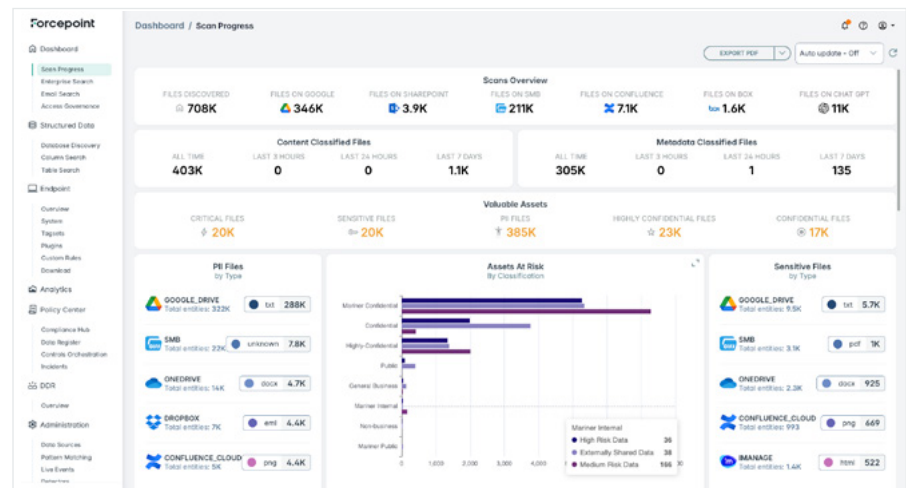
Funzionalità e vantaggi:

- IA Mesh Classification:** Architettura di classificazione altamente precisa ed efficiente che utilizza l'IA generativa, l'IA predittiva e le funzionalità di scienza dei dati.
- Rilevamento rapido:** Esegui Forcepoint DSPM nel cloud e nelle posizioni di archiviazione on-prem, tutte le volte che desideri.
- Valutazione del rischio in tempo reale:** controlla le autorizzazioni di accesso e altri rischi legati ai dati.
- Orchestrazione del flusso di lavoro:** Implementa le priorità aziendali per le parti interessate.

La trasformazione digitale si è evoluta nella trasformazione dell'IA, guidata dall'integrazione delle tecnologie di IA, in particolare delle applicazioni GenAI, nei processi aziendali. Associata all'espansione dei dati da parte delle organizzazioni che migrano applicazioni e dati dall'on-premise al cloud e utilizzano strumenti GenAI come ChatGPT, Copilot e Gemini, si trovano a dover affrontare la continua difficoltà di tenere traccia di dove si trovano i loro dati sensibili, chi può accedervi e come vengono utilizzati. La crescita esponenziale dei "dati oscuri," nascosti all'interno di repository basati su cloud o diffusi su singoli dispositivi e ora sulle applicazioni Gen AI, presenta un rischio sostanziale. Si stima che circa l'80% dei dati di un'organizzazione esista in questo oscuro stato "oscuro", sfuggendo alla sorveglianza tradizionale.

La conseguenza di questo panorama di dati oscuri è critica. Senza una visibilità e una gestione chiare, le organizzazioni sono esposte a maggiori rischi di violazioni, con conseguenze potenzialmente devastanti sia per quanto riguarda i settori commerciali, che per quelli no-profit e governativi. Nell'attuale era della trasformazione digitale, l'imperativo di riprendere il controllo delle informazioni sensibili non è mai stato così urgente.

Forcepoint DSPM scopre e classifica rapidamente i dati sensibili su scala, coprendo i dati strutturati e non strutturati. La sua IA Mesh unica offre velocità e spiegabilità con un'architettura SLM (Small Language Model) altamente efficiente. Questa IA Mesh consente anche la personalizzazione senza un'ampia riformazione del modello e garantisce una classificazione rapida e accurata per una fiducia e una conformità migliorate.

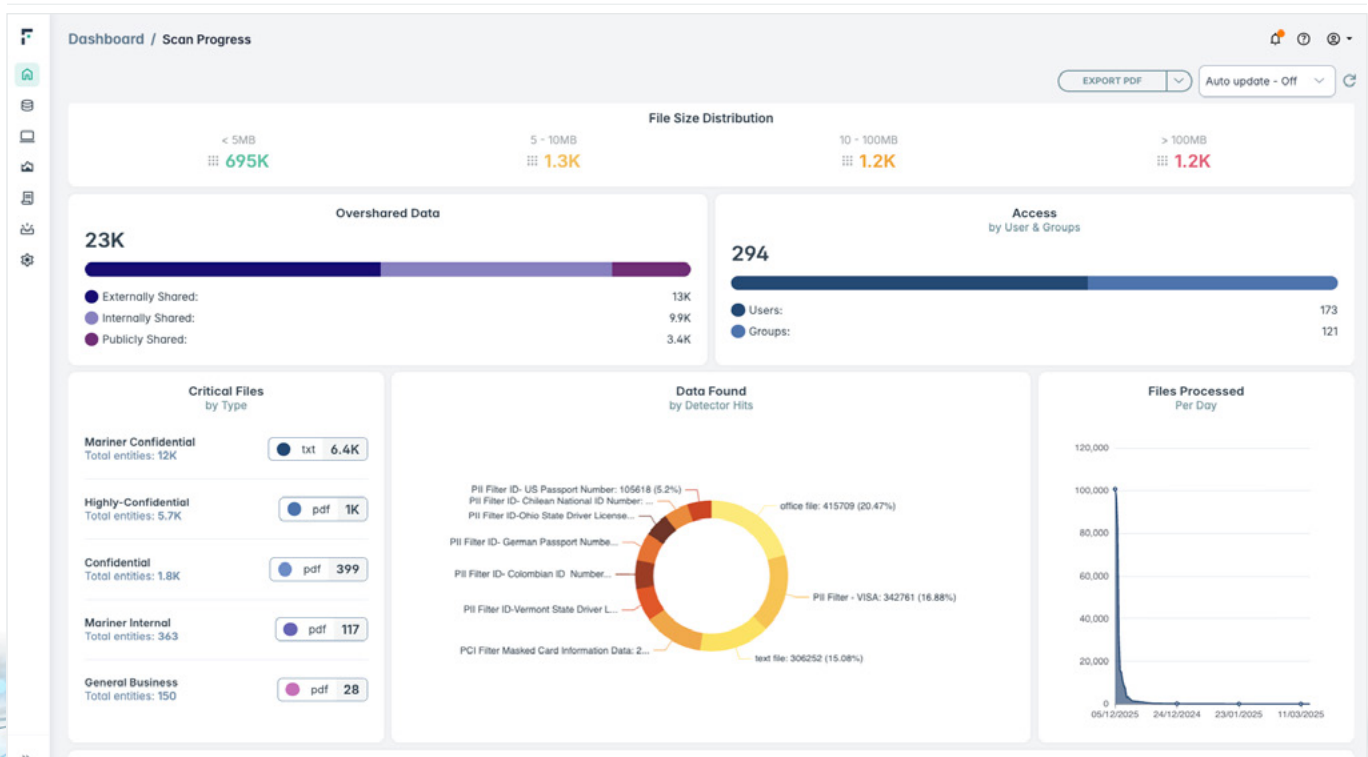


Rilevamento rapido e completo

Con una moltitudine di connettori, Forcepoint DSPM localizza in modo efficiente i dati sensibili attraverso i diversi ambienti di archiviazione, che si trovino nel cloud o on-premise, che si tratti di dati strutturati o non strutturati, scansionando attraverso le principali piattaforme come Amazon (AWS S3 e IAM), Microsoft (Azure AD, OneDrive, SharePoint Online) e Google (Google Drive e IAM), nonché i sistemi LDAP e SharePoint locali.

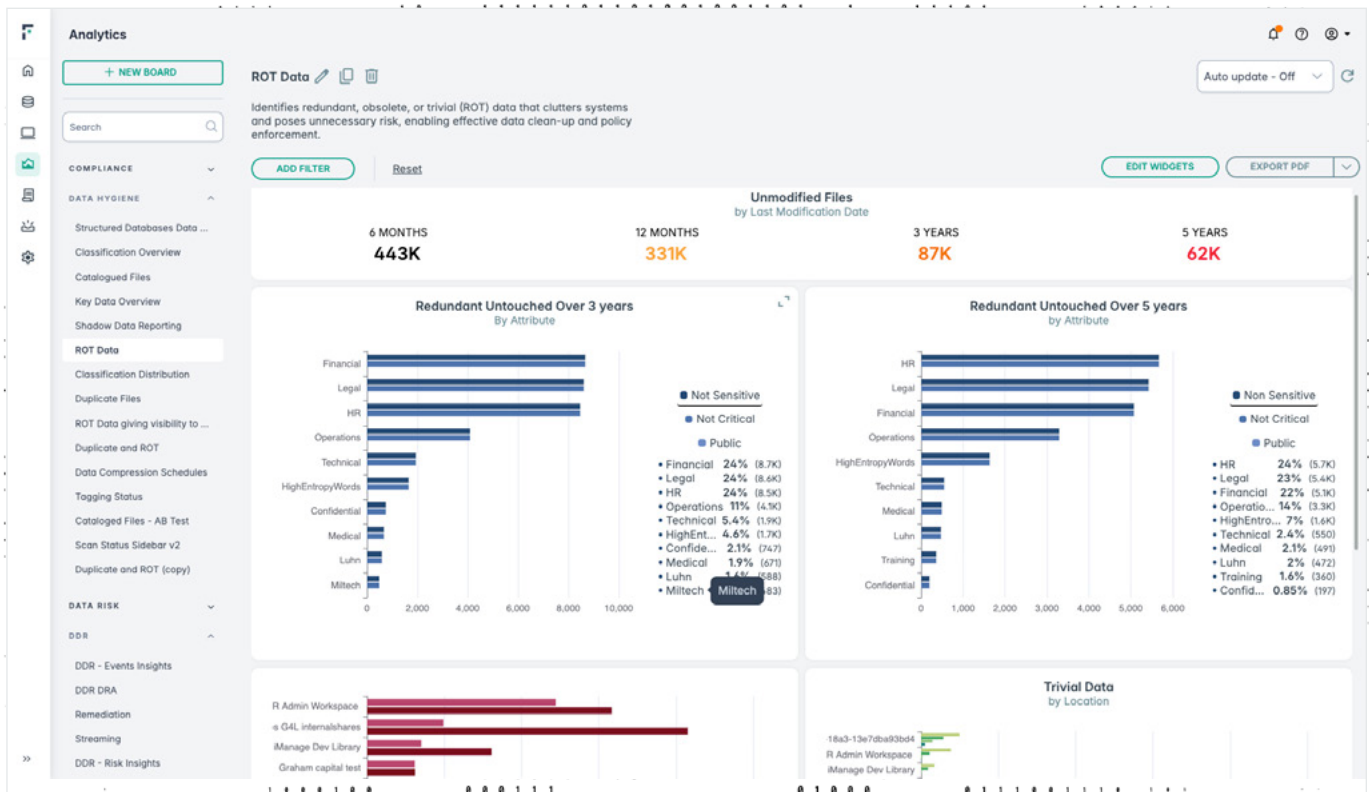
Accuratezza dei dati di AI Mesh

La funzionalità IA Mesh di Forcepoint DSPM eccelle nel fornire alle organizzazioni una precisione superiore nella classificazione dei dati. A differenza di altre soluzioni DSPM, offre un'architettura IA connessa e multi-nodo, che sfrutta uno SLM GenAI e una rete di dati e componenti di IA avanzati. Questa struttura cattura in modo efficiente il contesto e trasforma il testo in classificazioni precise dei documenti. L'IA Mesh è personalizzabile e può essere adattata in base alle esigenze del settore e agli ambienti normativi. Funziona in modo efficiente su risorse di calcolo standard senza richiedere GPU e fornisce al contempo una classificazione ad alte prestazioni. L'elevata precisione viene raggiunta senza il bisogno di un training ML estensivo, riducendo così i costi di manutenzione. L'explainability dell'IA Mesh migliora la fiducia e la conformità, garantendo una postura dei dati altamente sicura e il rispetto delle normative sulla privacy.



Monitoraggio delle prestazioni elevate e valutazione del rischio dei dati

Eseguendo la scansione e scoprendo i dati, Forcepoint DSPM fornisce informazioni dettagliate come il numero di file condivisi a livello interno contenenti informazioni critiche, la quantità di file PII a rischio e il conteggio di file di dati ridondanti, obsoleti e banali (ROT).



Organizzazione dei flussi di lavoro

Ottimizza facilmente la governance della protezione dei dati con Forcepoint DSPM. La sua orchestrazione intuitiva dei flussi di lavoro garantisce un tracking efficiente della proprietà e della responsabilità dei dati. Eliminando i sistemi isolati e facilitando la collaborazione tra le parti interessate, allinea le responsabilità, migliorando l'efficienza operativa e favorendo la chiarezza in tutta l'organizzazione.

L'implementazione di una solida soluzione DSPM è fondamentale per le organizzazioni che mirano a proteggere la propria postura dei dati e salvaguardare le informazioni sensibili nelle posizioni di archiviazione cloud e on-premise. Utilizzando Forcepoint DSPM, le organizzazioni possono aumentare la produttività migliorando l'affidabilità dell'accesso ai dati e della condivisione, promuovendo l'innovazione, facilitando l'adozione dell'IA e incoraggiando la collaborazione. Allo stesso tempo, possono mitigare i rischi identificando e affrontando proattivamente l'uso improprio dei dati sensibili, prevenendo così le violazioni dei dati. In definitiva, le organizzazioni possono semplificare gli sforzi di conformità ottenendo una visibilità e un controllo reali sui dati sensibili in tutti gli ambienti.

Solida scoperta

FUNZIONE	VANTAGGIO
Rilevamento e catalogazione rapidi	Si esegue su più fonti per scansionare maggiori volumi di file al secondo/all'ora e riassume i dettagli sulle risorse di dati non strutturati, organizzandoli in un formato facile da elaborare.
Si connette a fonti di dati importanti	Visibilità solida sui dati non strutturati e strutturati offrendo una gamma di connettori per le fonti di dati.
Analisi dei dati sovraesposti	Identificare i dati sovraesposti che sono condivisi pubblicamente, condivisi esternamente con terze parti e condivisi in maniera eccessiva internamente.
Visualizza e corregge le autorizzazioni	Consulta gli accessi per ciascun file e correggili di conseguenza per stabilire la sicurezza Zero Trust secondo il principio del minimo privilegio (POLP).
Elimina il rischio ai dati (ridondanti, obsoleti, banali) ROT	Identifica ed elimina i file che sono ridondanti, obsoleti o banali (ROT).
Visibilità sugli accessi e sulle autorizzazioni	Le integrazioni con Active Directory e altre soluzioni IRM migliorano la sicurezza degli accessi all'interno delle organizzazioni.

Classificazione dei dati AI Mesh

FUNZIONE	VANTAGGIO
Classificazione AI Mesh dei dati non strutturati e strutturati i dati	Classificazione dell'IA altamente accurata per i dati non strutturati e strutturati.
Training su modelli personalizzati	Le organizzazioni possono personalizzare il modello AI Mesh in base alle esigenze specifiche in materia di dati (ad es. IP, segreti commerciali, ecc.), per una classificazione dei dati altamente accurata, riducendo i falsi positivi/negativi DSPM e DLP.
Abilità di mappare i tag al tagging IP di Microsoft Purview.	Fornisce un ulteriore livello di granularità della classificazione, a integrazione dei tag MIP. Consente di correggere i tag MIP.
Tagging dei dati	Tagga tutti i file scansionati e classificati con etichette persistenti leggibili da DLP con tag standard (classificati, altamente classificati, pubblici) e catalogazione/tagging aziendale (risorse umane, marketing, finanza, devops, con tag secondari come curriculum, ordini di vendita, ecc.).
Si integra con Forcepoint DLP	Può essere integrata con Forcepoint DLP per utilizzare il tagging DSPM AI Mesh dei file per creare politiche efficaci.

Monitoraggio in tempo reale e valutazione del livello di rischio dei dati

FUNZIONE	VANTAGGIO
Data Risk Assessment (DRA)	Offre valutazioni gratuite del rischio dei dati per analizzare la posizione attuale di protezione dei dati delle organizzazioni, in più categorie.
Dashboard interattiva dettagliata	Visualizza i dettagli completi dei file e del database in un'unica soluzione. Scopri i dati cruciali dei file come il livello di rischio, le autorizzazioni e le posizioni (indirizzo IP, percorso).
Funzione di reporting	Genera report che mostrano sia lo stato generale di conformità che le normative specifiche sulla privacy.
Sistema di allerta avanzato	Fornisce sofisticati controlli dei dati e allerte trovate durante le scansioni per eventuali anomalie o potenziali violazioni.
Ricerca DSAR (Data Subject Access Request)	Semplifica la generazione di DSAR per raggiungere rapidamente la conformità per le richieste di regolamentazione sulla privacy.
Suite di analisi	Scopri la suite di analisi avanzata per accedere facilmente alle informazioni sulla sicurezza e sulla classificazione dei dati, a colpo d'occhio. Seleziona da varie dashboard predefinite o crea la tua dashboard ed esporta facilmente istantanee in formato PDF, con un solo clic. Le dashboard predefinite includono l'analisi della sovraesposizione e del ransomware, la duplicazione di dati critici, il rilevamento degli utenti a rischio, la conservazione dei dati, i dati smarriti, la valutazione del rischio dei dati, la sovranità e il monitoraggio degli incidenti per le violazioni del controllo dei dati e molto altro ancora.
Analisi dell'esposizione al ransomware	Identifica i dati critici che potrebbero essere esposti a un attacco ransomware.
Creatore di reporting e analisi senza codice	Crea facilmente casi d'uso personalizzati e report di analisi, senza bisogno di competenze di codifica.
Identificazione dell'utente a rischio	Identifica gli utenti con profili di rischio elevati che hanno accesso a quantità significative di dati fondamentali.
Incidente di controllo dei dati	Fornisce una visione chiara di eventuali violazioni del controllo dei dati e uno stato di risoluzione degli incidenti.

Rimedio

FUNZIONE	VANTAGGIO
Correzione delle autorizzazioni	Ricevete notifiche su incidenti di governance della sicurezza dei dati o problemi di conformità, semplificate il monitoraggio e la gestione con gli strumenti ITSM e di produttività esistenti – inclusi avvisi per i dati eccessivamente esposti.
Correzione tramite deduplicazione dei dati	La funzione di deduplicazione di DSPM identifica ed elimina i dati ridondanti, riducendo le esigenze di archiviazione e i costi, ottimizzando l'allocazione delle risorse. L'eliminazione avviene automaticamente in base a controlli dei dati personalizzabili.
File Stubbing	Creare automaticamente stub di file per mantenere i processi aziendali documentando le modifiche alla posizione dei file quando vengono spostati tramite DSPM.