Forcepoint

Scheda dati

Forcepoint Data Security Posture Management

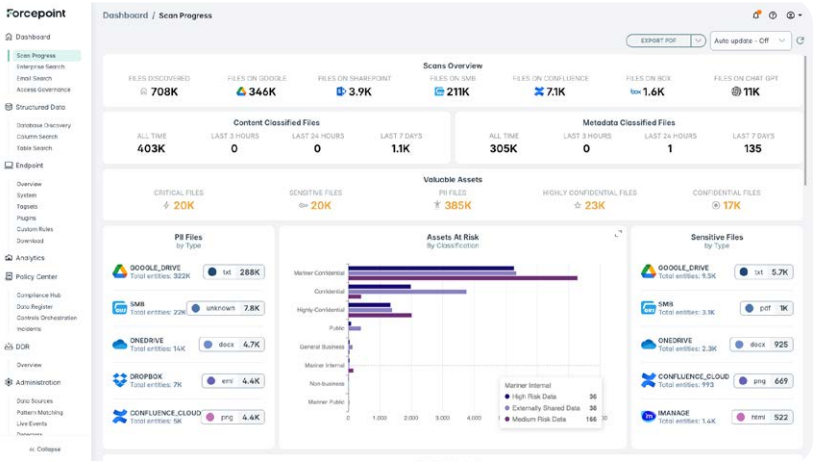
Funzionalità e vantaggi:

- **AI Mesh Classification** – L'ispezione completa dei contenuti garantisce una classificazione altamente precisa ed efficiente utilizzando GenAI, l'apprendimento automatico e i migliori classificatori di dati di Forcepoint.
- **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 in una trasformazione basata sull'IA, guidata dall'integrazione delle tecnologie di IA nei processi aziendali, in particolare le applicazioni GenAI e l'Agentic AI. Le organizzazioni affrontano una difficoltà costante nel tenere traccia di dove si trovano i propri dati sensibili, chi può accedervi e come controllarne l'utilizzo, mentre migrano applicazioni e dati tra sistemi on-premise e cloud, ampliando al contempo l'uso dell'IA. La crescita esponenziale dei "dark data", nascosti in repository basati sul cloud o distribuiti su singoli dispositivi e ora anche nelle applicazioni Gen AI, rappresenta un rischio sostanziale. Si stima che fino all'80% dei dati di un'organizzazione si trovi in questo stato di "dark data" sfuggendo ai controlli tradizionali.

Le conseguenze di questo scenario di dati oscurati possono essere gravi. Senza una visibilità e una gestione chiare, le organizzazioni sono esposte a rischi crescenti di violazioni, con conseguenze potenzialmente devastanti nei settori commerciale, no-profit e governativo. Nell'attuale era della trasformazione basata sull'IA, la necessità di riprendere il controllo delle informazioni sensibili non è mai stata così urgente. L'unico modo per risolvere questo problema, mantenendo il passo con il ritmo sempre più rapido del business, è l'automazione unita a precisione e spiegabilità.

Forcepoint DSPM individua e classifica rapidamente i dati sensibili su larga scala, coprendo sia i dati strutturati sia quelli non strutturati. Il suo esclusivo AI Mesh offre un'ispezione completa dei contenuti, rapida e spiegabile, grazie a uno Small Language Model (SLM) altamente efficiente e a oltre 20 anni di classificatori di dati accuratamente curati da Forcepoint. Questo AI Mesh consente inoltre la personalizzazione senza un ampio riaddestramento del modello, garantendo una classificazione rapida e precisa per una maggiore fiducia e conformità.

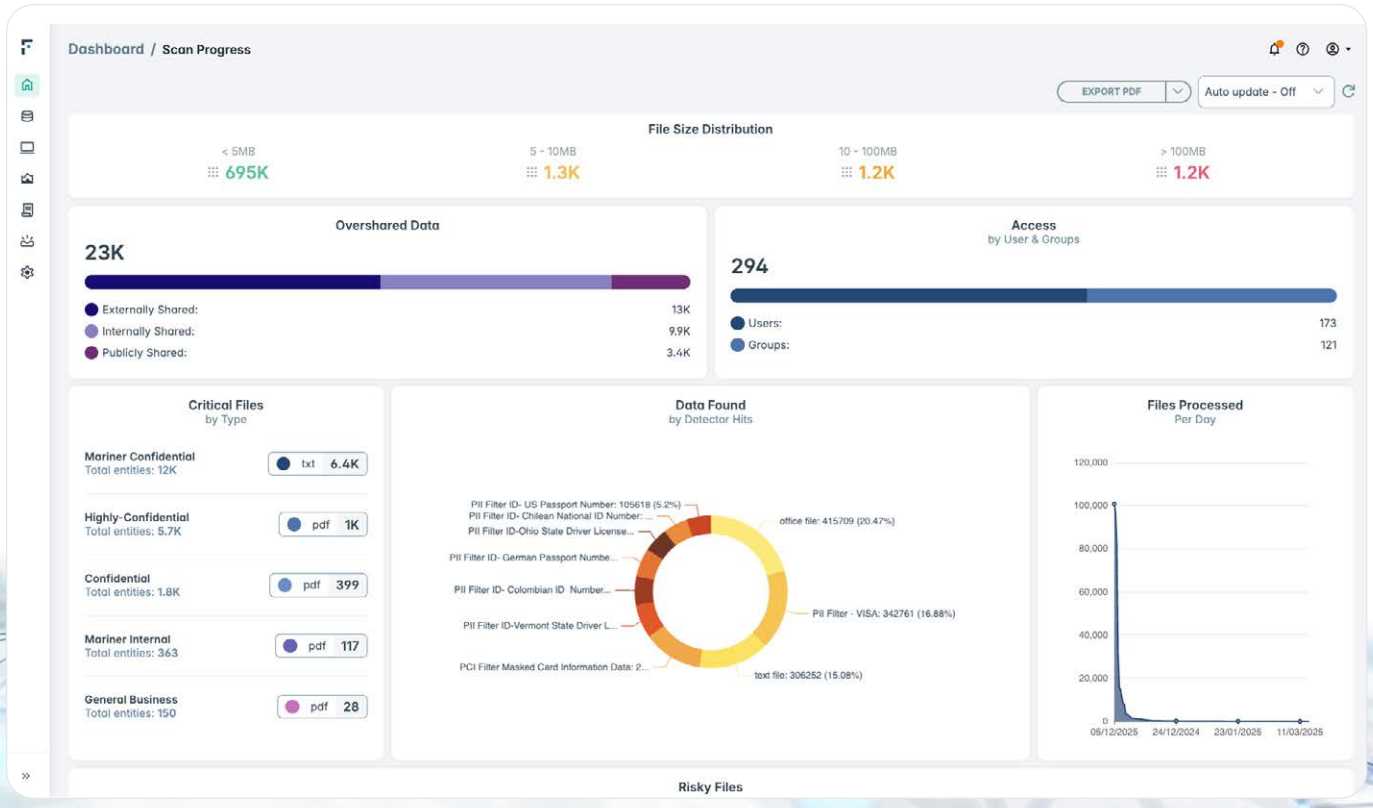


Individuazione rapida e completa

Grazie a una moltitudine di connettori, Forcepoint DSPM individua e classifica in modo efficiente i dati sensibili tramite l'ispezione completa dei contenuti in diversi ambienti di archiviazione, sia in cloud sia on-premise, sia per dati strutturati sia non strutturati, effettuando la scansione delle principali piattaforme come Amazon (AWS S3 e IAM), Microsoft (Azure AD, OneDrive, SharePoint Online) e Google (Google Drive e IAM), oltre ai sistemi locali LDAP e SharePoint.

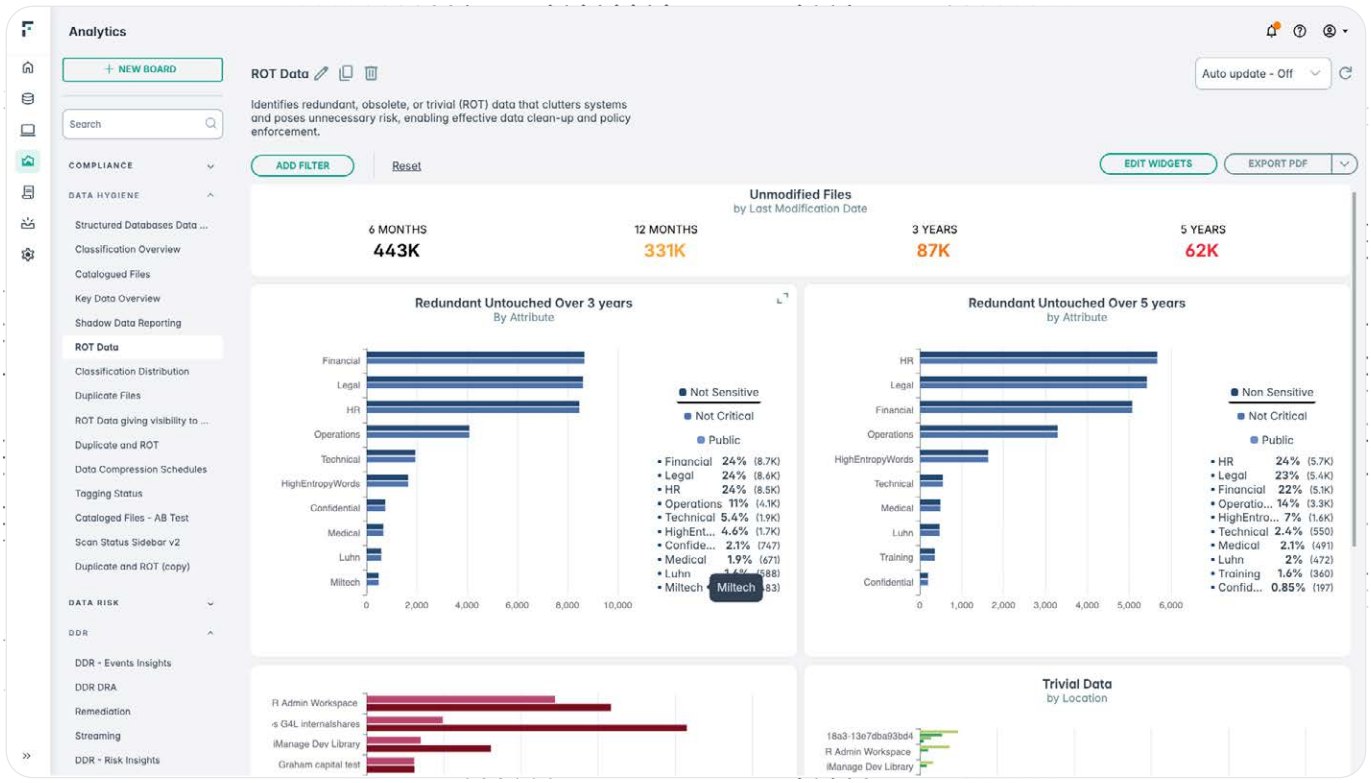
Accuratezza dei dati di AI Mesh

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 addestramento approfondito dei modelli ML, 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	Identifica 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.
Capacità di associare i tag alle etichette di Microsoft Purview Information Protection (MIP)	Fornisce un ulteriore livello di granularità della classificazione, a integrazione dei tag MIP. Consente di correggere i tag MIP.
Tagging dei dati	Applica etichette a 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)	La dashboard integrata di valutazione del rischio sui dati analizza l'attuale postura di sicurezza dei dati di un'organizzazione su 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 controlli avanzati sui dati e avvisi relativi ad anomalie o potenziali violazioni rilevate durante le scansioni
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.
Generatore di report 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.
Gestione degli incidenti relativi al controllo dei dati	Fornisce una visione chiara di eventuali violazioni del controllo dei dati e uno stato di risoluzione degli incidenti.

Correzione

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.
Sposta i file	Utilizza DSPM per spostare i file da posizioni a rischio o eccessivamente esposte verso repository più sicuri, con la possibilità di creare automaticamente uno stub del file.
File stubbing	Creare automaticamente stub di file per mantenere i processi aziendali documentando le modifiche alla posizione dei file quando vengono spostati tramite DSPM.

Forcepoint

Forcepoint.com/contact

© 2026, Forcepoint. Forcepoint e il logo FORCEPOINT sono marchi di Forcepoint. Tutti gli altri marchi utilizzati nel presente documento sono di proprietà dei rispettivi proprietari. [FP-DSPM Datasheet-IT] 19Aug2026