

Forcepoint Data Security Posture Management

Funzionalità e vantaggi:

- › **AI Mesh e ML** - La catalogazione AI Mesh offre precisione ed efficienza senza pari, evolvendosi continuamente attraverso l'apprendimento automatico per miglioramenti continui.
- › **Rilevamento rapido** - Esegui Forcepoint DSPM nel cloud e nelle posizioni di archiviazione on-prem, tutte le volte che desideri.
- › **Monitoraggio in tempo reale e valutazione dei rischi** - Controlla i permessi di accesso e altri rischi relativi ai dati.
- › **Orchestratura 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, Co-pilot 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.

L'AI Mesh di Forcepoint DSPM consente alle organizzazioni di ottenere una precisione di classificazione dei dati di alto livello. La sua architettura di IA in rete, che sfrutta un modello SLM (Small Language Model) GenAI, oltre che dati e componenti di IA avanzati, rileva in modo efficiente il contesto dal testo non strutturato. Personalizzabile ed efficiente, garantisce una classificazione rapida e accurata senza un training approfondito, migliorando il grado di fiducia e conformità.

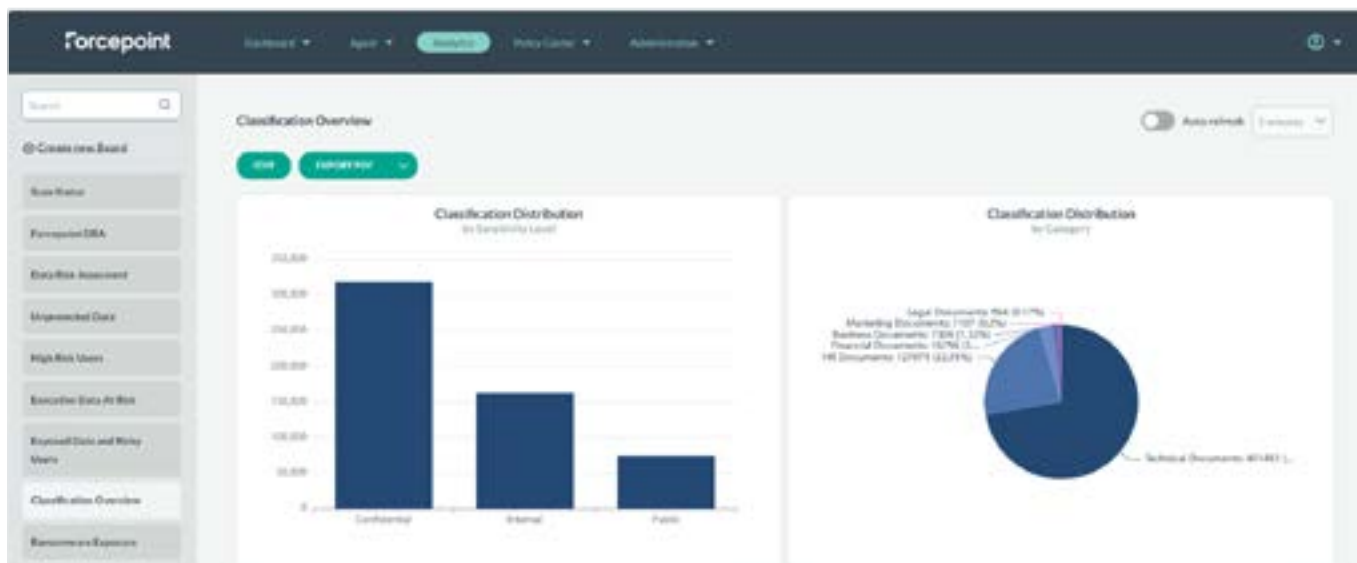


Rilevamento rapido e completo

Con una moltitudine di connettori, Forcepoint DSPM localizza in modo efficiente i dati sensibili in diversi ambienti di archiviazione, sia in cloud che on-premise, scansionando circa un milione di file all'ora sulle principali piattaforme come Amazon (AWS S3 e IAM), Microsoft (Azure AD, OneDrive, SharePoint Online) e Google (Google Drive e IAM), nonché sui sistemi LDAP locali e SharePoint.

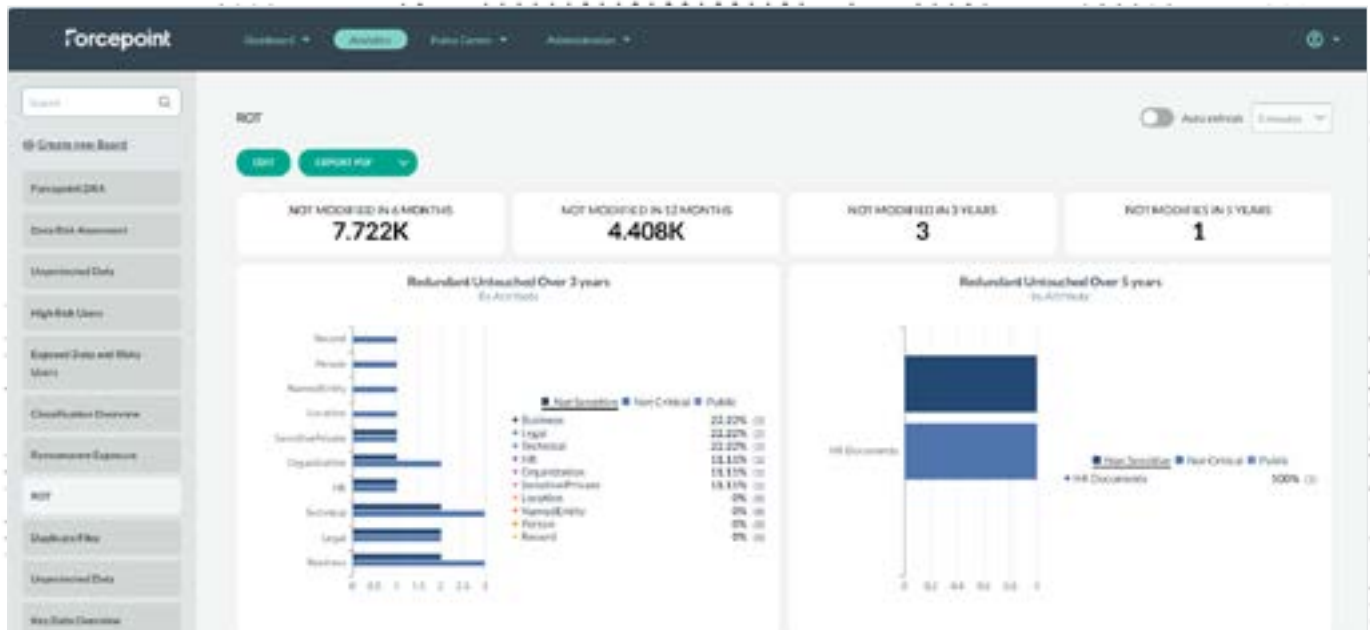
Accuratezza dei dati di AI Mesh

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 rileva in modo efficiente il contesto e trasforma il testo non strutturato 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 in tempo reale e valutazione del livello di rischio dei dati

Eseguito 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 razionalizzare il proprio patrimonio di dati e a salvaguardare i dati sensibili attraverso le posizioni di archiviazione dei dati cloud e on-premise. Utilizzando Forcepoint DSPM, le organizzazioni possono incrementare la produttività aumentando l'affidabilità dell'accesso e della condivisione dei dati, favorendo l'innovazione e incoraggiando la collaborazione. Contemporaneamente, possono ridurre il rischio identificando e affrontando in modo proattivo l'uso improprio di dati sensibili, prevenendo così le violazioni dei dati. In ultima analisi, le organizzazioni possono snellire gli sforzi di conformità ottenendo una visibilità e un controllo effettivi sui dati sensibili in ogni contesto.

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.
Connettori estesi per fonti di dati	Solida visibilità in dati maggiormente non strutturati per offrire un'ampia gamma di connettori per 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 le autorizzazioni per ogni file di dati non strutturato	Visualizza l'accesso di ogni singolo utente per ogni file e vedi gli utenti con accesso al maggior numero di file.
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 e ML dei dati non strutturati esistenti	Suggerimenti di classificazione di alta precisione consigliati per i dati esistenti non strutturati sottoposti a scansione.
Training su modelli personalizzati	Le organizzazioni possono adattare il modello AI Mesh alle esigenze di dati unici (ad esempio, proprietà intellettuale, segreti commerciali, ecc.) e, attraverso l'apprendimento automatico, è possibile migliorare nel tempo per ottenere una maggiore accuratezza.
Abilità di mappare i tag al tagging IP di Microsoft Purview.	Fornisce un ulteriore livello di granularità di classificazione, a complemento dei tag MPIP. Abilità nel correggere il tagging MPIP.
Tagging dei dati	Ottimizzando l'implementazione del DLP migliora l'efficienza del DLP effettuando il tagging di tutti i file scansionati e classificati con etichette leggibili dal DLP con tag tipici (classificati, altamente classificati, pubblici) nonché catalogazione/tagging aziendale (RSI, marketing, finanza, devops - con sottotitoli come curriculum, PO, ecc.).
Si integra con Forcepoint DLP	Può essere integrato per utilizzare il tagging DSPM AI Mesh dei file (classificazione) per realizzare policy efficaci.

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

FUNZIONE	VANTAGGIO
Data Risk Assessment (DRA)	Le valutazioni gratuite del livello di rischio dei dati sono disponibili per analizzare l'attuale posizione di rischio dei dati di un'organizzazione in più categorie.
Dashboard interattiva dettagliata	Visualizza i dettagli completi del file in un'unica schermata. 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 una DSAR per ottemperare rapidamente alle richieste delle normative in materia di privacy.
Suite di analisi	Scopri una suite di analisi avanzata per accedere facilmente alle informazioni sulla sicurezza e sulla classificazione in un 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 di 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.
Analisi dell'esposizione al ransomware	Identifica i dati critici 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 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.

Orchestratura dei flussi di lavoro

FUNZIONE	VANTAGGIO
Proprietà dei dati	Definisce facilmente le responsabilità e raggiunge l'allineamento delle parti interessate.
Task manager	Assegna compiti a chi custodisce e possiede i dati, consentendo il monitoraggio delle statistiche DSPM (come ticket aperti, risolti e chiusi, tempo di risoluzione).