

Forcepoint Data Security Posture Management

主な機能と利点:

- ▶ **AI メッシュと ML** - AI メッシュ カタログ作成は、比類のない精度と効率性を提供し、機械学習を通じて継続的に進化し、継続的な機能強化を実現します。
- ▶ **迅速な発見** - データを可視化したいタイミングで何度でもクラウドやオンプレミスのストレージロケーションにて Forcepoint DSPM を実行します。
- ▶ **リアルタイム監視とリスク評価** - アクセス許可やその他のデータリスクをチェックします。
- ▶ **ワークフローオーケストレーション** - ステークホルダーのためにビジネス優先事項を実装しています

デジタルトランスフォーメーションは、AIテクノロジー、特にGenAIアプリケーションをビジネスに統合することでAIトランスフォーメーションへと進化した。社内のアプリケーションとデータをクラウドに移行し、ChatGPT、Co-pilot、Gemini などの GenAI ツールを利用する組織によるデータの拡散と相まって、機密データがどこにあるのか、誰がアクセスできるのか、およびその使用方法を追跡するという継続的な課題に直面しています。クラウドベースのリポジトリ内に隠されたり、個々のデバイスや Gen AI アプリケーションに分散している「ダーク データ」の急激な増加は、大きなリスクをもたらします。組織のデータの80%以上が、この不明瞭な「ダークな」状態にあり、従来の監視を回避していると推定されています。

この曖昧なデータ環境の結果は危機的です。明確な可視性と管理がなければ、組織に侵害のリスクが高まり、ビジネス全体に壊滅的な影響が及ぶ可能性があります。それは非営利団体や政府機関においても同様です。今日のデジタル変革の時代において、機密情報の管理を取り戻すことが急務であることは未だかつてありません。

Forcepoint DSPMに備わるAI Meshが、データ分類において優れた精度を提供します。そのネットワーク化されたAIアーキテクチャ、世代を活用AI Small Language Model (SLM) と高度なデータおよびAIコンポーネントは、非構造化テキストからコンテキストを効率的にキャプチャします。カスタマイズ可能で効率的なこのアーキテクチャは、大規模なトレーニングなしで迅速かつ正確な分類を保証し、信頼性とコンプライアンスを強化します。

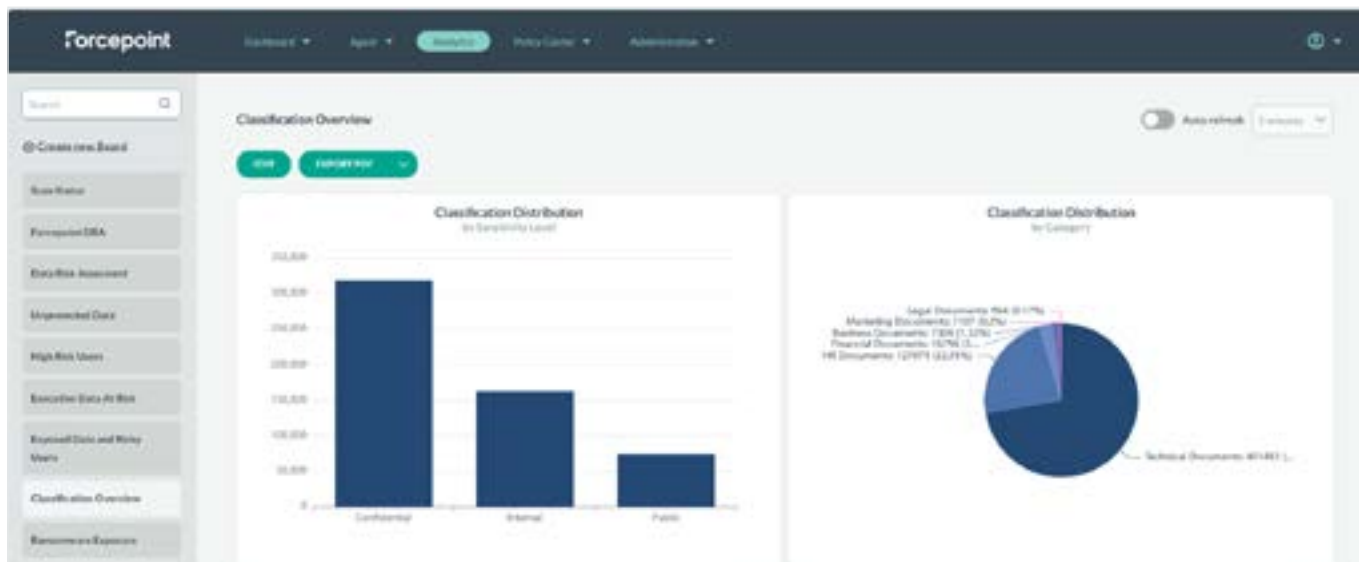


迅速で包括的な発見

Forcepoint DSPMは、多数のコネクタを使用して、クラウドまたはオンプレミスにかかわらず多様なストレージ環境全体で機密データを効率的に配置し、Amazon (AWS S3とIAM)、Microsoft (Azure AD、OneDrive、SharePoint Online)、Google (Google DriveとIAM) などの主要なプラットフォーム、ローカルLDAPとSharePointシステムで1時間あたり約100万ファイルをスキャンすることができます。

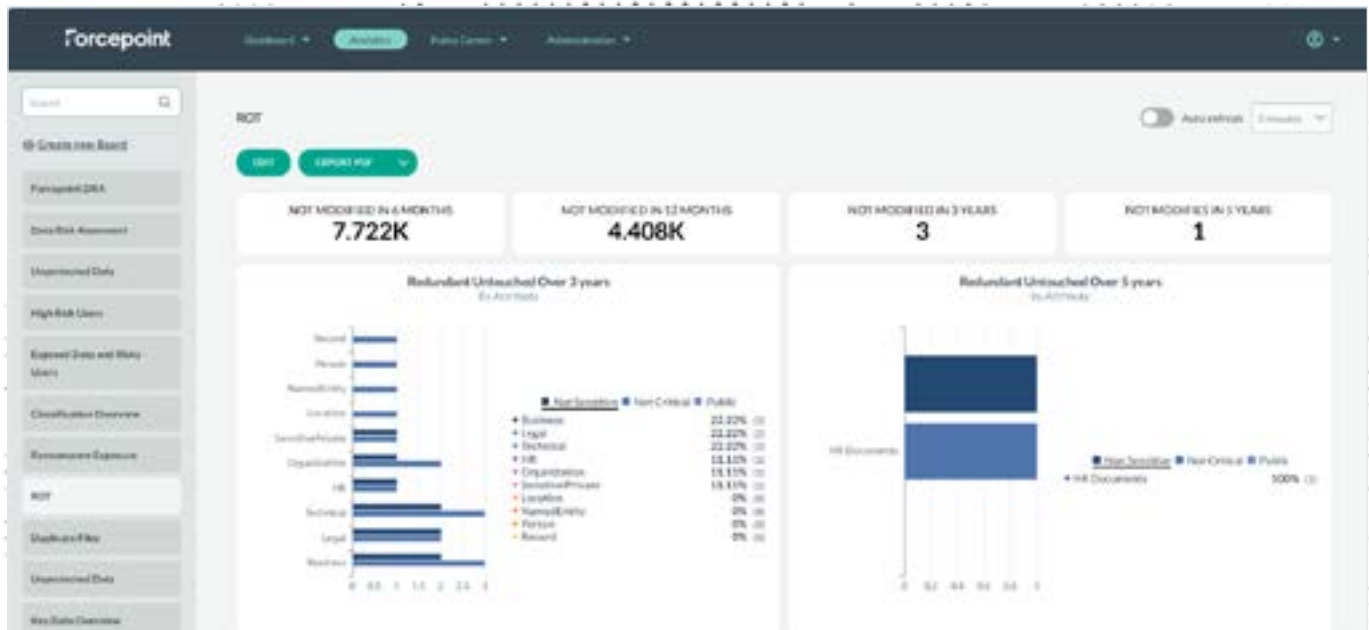
AIメッシュで実現した精度

Forcepoint DSPMのAI Mesh機能は、優れたデータ分類精度で今日の組織を支援することに優れています。他のDSPMソリューションとは異なり、GenAI SLMと高度なデータおよびAIコンポーネントのネットワークを活用したマルチノード接続AIアーキテクチャを提供します。この構造はコンテキストを効率的にキャプチャし、非構造化テキストを正確なドキュメント分類に変換します。AI Meshはカスタマイズ可能で、業界のニーズや規制環境に合わせて調整できます。GPUを必要とせず、標準的な計算リソース上で効率的に実行でき、同時に高性能な分類も提供します。広範なMLトレーニングをすることなく高精度を実現し、メンテナンスコストを削減します。AI Meshの説明可能性により信頼とコンプライアンスを強化し、非常に安全なデータポスチャーとプライバシー規制の遵守を保証します。



リアルタイム監視とデータリスク評価

Forcepoint DSPMはデータをスキャンして検出すると、重要な情報を含む内部的に有されたファイルの数、リスクにさらされているPIIファイルの量、冗長で古い、些細なデータ (ROT) ファイルの数などの詳細な情報を提供します。



ワークフローオーケストレーション

Forcepoint DSPMを使用して、データ・セキュリティ・ガバナンスを簡単に合理化します。直感的なワークフローオーケストレーションにより、データの所有権とアカウントビリティの効率的な追跡が保証されます。縄張り意識を解消し、ステークホルダー間のコラボレーションを促進することで、責任範囲を調整し、運用効率を高め、組織全体の透明性を向上させます。

堅牢なDSPMソリューションを導入することは、クラウドや社内のデータストレージサイト全体でデータ資産を合理化し、機密情報を保護することを目指す組織にとって重要です。Forcepoint DSPMを活用することで、組織は、データアクセスと共有の信頼性を高め、イノベーションを促進することで、生産性を向上させ、コラボレーションを進めることが出来ます。同時に、機密データの不適切な使用を前に特定して対処することでリスクを軽減し、データ侵害を防止できます。最終的に、組織はすべての環境で機密データを真の可視性と制御することにより、コンプライアンスの取り組みを合理化できます。

堅牢な発見

特徴	利点
迅速な発見とカタログ化	複数のソースで実行され、毎秒・毎時大量のファイルをスキャンし、非構造化データ資産の詳細を合成し、それらを簡単に消化できるフォーマットに整理します。
広範なデータ・ソース・コネクタ	幅広いデータ・ソース・コネクタを提供することにより、さらに非構造化したデータへと向かう堅牢な可視性。
公開され過ぎたデータを分析	公開され外部でサードパーティと共有されたり、内部で過剰に共有されたりしている、公開され過ぎたデータを特定します。
すべての非構造化データファイルのアクセス許可を表示	各ファイルに対する個々のユーザーアクセスを表示し、最も多くのファイルにアクセスできるユーザーを表示します。
ROT (冗長、古い、些細な) データによるリスクを排除	冗長、古い、または些細な (ROT) ファイルを識別して排除します。
アクセスとアクセス許可を可視化	Active Directoryやその他のIRMソリューションとの統合により、組織内のアクセスセキュリティが強化されます。

AI メッシュデータ分類

特徴	利点
AIメッシュと、既存の構造化されていないデータのML分類	スキャンされる既存の非構造化データに推奨される高精度な分類提案。
カスタム・モデル・トレーニング	組織は、独自のデータニーズ (IP、取引上の秘密など) に合わせてAIモデルを調整することができ、機械学習を通じて、時間の経過とともに精度を向上させることができます。
タグをMicrosoft Purview IPタグにマッピングすることができます。	分類粒度の追加レイヤーを提供し、MPIPタグを補完し、修正することができます
データタグ	DLPの展開を合理化すれば、スキャンされ分類されたファイルに、典型的なタグ (分類、高度に分類、公開) と、ビジネスカタログ/タグ付け (HR、マーケティング、財務、DevOps、履歴書、注文書などのサブタグ) を使用して、DLPで読み取り可能なラベルをタグ付けすることで、DLPの効率が向上します。
Forcepoint DLPと統合	DSPM AIメッシュタグ付けファイル (分類) を利用して、強力なポリシーを構築するために統合できます。

リアルタイム監視とリスク評価

特徴	利点
データリスク評価 (DRA)	無料のデータリスク評価は、複数のカテゴリにわたる組織の現在のデータリスク状況を分析するために利用できます。
詳細なインタラクティブダッシュボード	包括的なファイルの詳細を1つの画面に表示します。リスクレベル、アクセス許可、ロケーション (IPアドレス、パス) などの重要なファイルデータをドリルダウンします。
レポート機能	一般的なコンプライアンスの準備と特定のプライバシー規制の両方を示すレポートを生成します。
高度なアラートシステム	何かの異常や潜在的な侵害に向けたスキャン中に利用できる高度なデータ制御とアラートを提供します。
データ主体アクセス要求 (DSAR) 検索	DSARの生成を簡素化し、プライバシー規制要求にすぐに応じます。
分析スイート	一目でセキュリティと分類の洞察を簡単に利用するための高度な分析スイートを体験します。さまざまな定義済みのダッシュボードから選択するか、独自に作成して、ワンクリックでPDFスナップショットを簡単にエクスポートします。定義済みのダッシュボードには、公開過剰とランサムウェア分析、重要なデータの重複、危険なユーザー検出、データ保持、誤った配置データ、データリスク評価、主権、データ制御違反に対するインシデント追跡が含まれます。
ランサムウェアによる露出分析	ランサムウェア攻撃にさらされている重要なデータを特定します。
ノーコードでのレポート作成と分析ビルダー	コーディング不要でカスタム・ユース・ケースと分析レポートを簡単に作成できます。
危険なユーザー識別	重要な情報にかなりの回数アクセスできるリスクプロファイルが高いユーザーを特定します。
データ制御インシデント	データ制御違反とインシデント解決のステータスを明確に表示します。

ワークフローオーケストレーション

特徴	利点
データ所有	説明責任を簡単に定義し、ステークホルダーとの整合を達成します。
タスクマネージャー	データ管理者と所有者にタスクを割り当て、DSPM統計 (オープン、解決、クローズチケット、解決時間など) を追跡できます。