Forcepoint

データシート

Forcepoint Data Security Posture Management

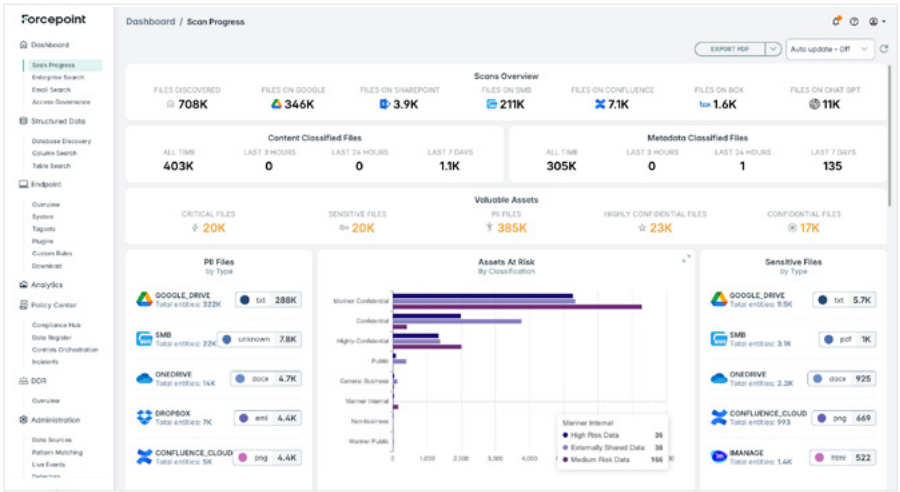
主な機能と利点：

- **AI Mesh分類 –** 生成AI、予測AI、データサイエンスの機能を活用した、高精度で効率的なアーキテクチャ。
- **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。
- **リアルタイムのリスク評価 –** アクセス許可やその他のデータリスクをチェック。
- **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効果的に実現。

デジタルトランスフォーメーションは、AIテクノロジー、特に生成AI（GenAI）アプリケーションのビジネスプロセスへの統合によって、AIトランスフォーメーションへと進化しました。この変化に加え、オンプレミスからクラウドへのアプリケーションやデータの移行、さらにChatGPT、Copilot、GeminiといったGen-AIツールの活用により、組織は「機密データがどこに存在し、誰がアクセスでき、どのように利用されているのか」を継続的に把握し続けなければいけないという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は、構造化データと非構造化データを網羅し、機密データを大規模に迅速に検出し、分類します。独自のAI Meshは、高効率なSmall Language Model（SLM）アーキテクチャにより、スピードと説明可能性を提供します。このAI Meshは、広範なモデル再トレーニングなしでカスタマイズを可能にし、迅速で正確な分類を保証し、信頼とコンプライアンスを強化します。

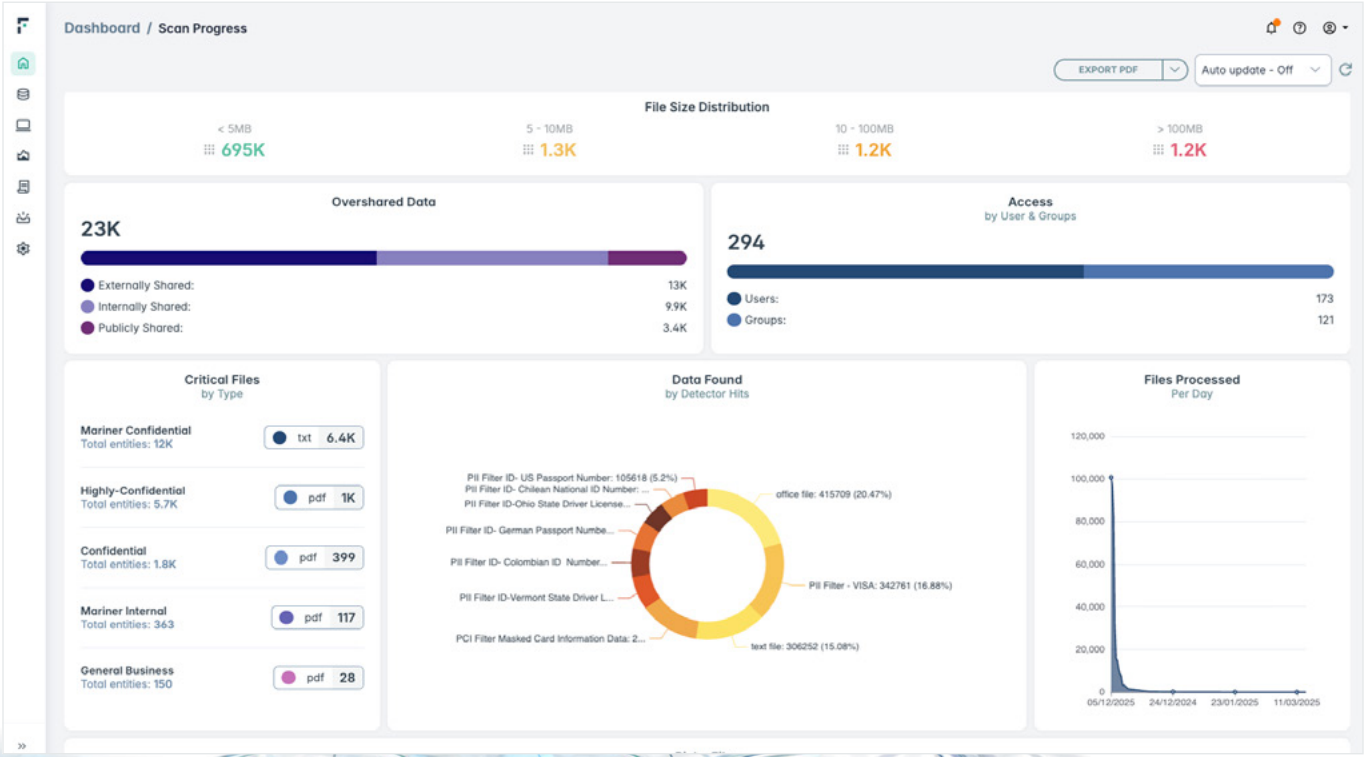


迅速で包括的な発見

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、構造化データと非構造化データを含む多様なストレージ環境全体で、多数のコネクタを活用して、Amazon（AWS S3とIAM）、Microsoft（Azure AD、OneDrive、SharePoint Online）やGoogle（Google DriveとIAM）などの主要なプラットフォームをスキャンし、ローカルLDAPとSharePointシステムを活用した、多数のコネクタを活用したデータが検出されます。

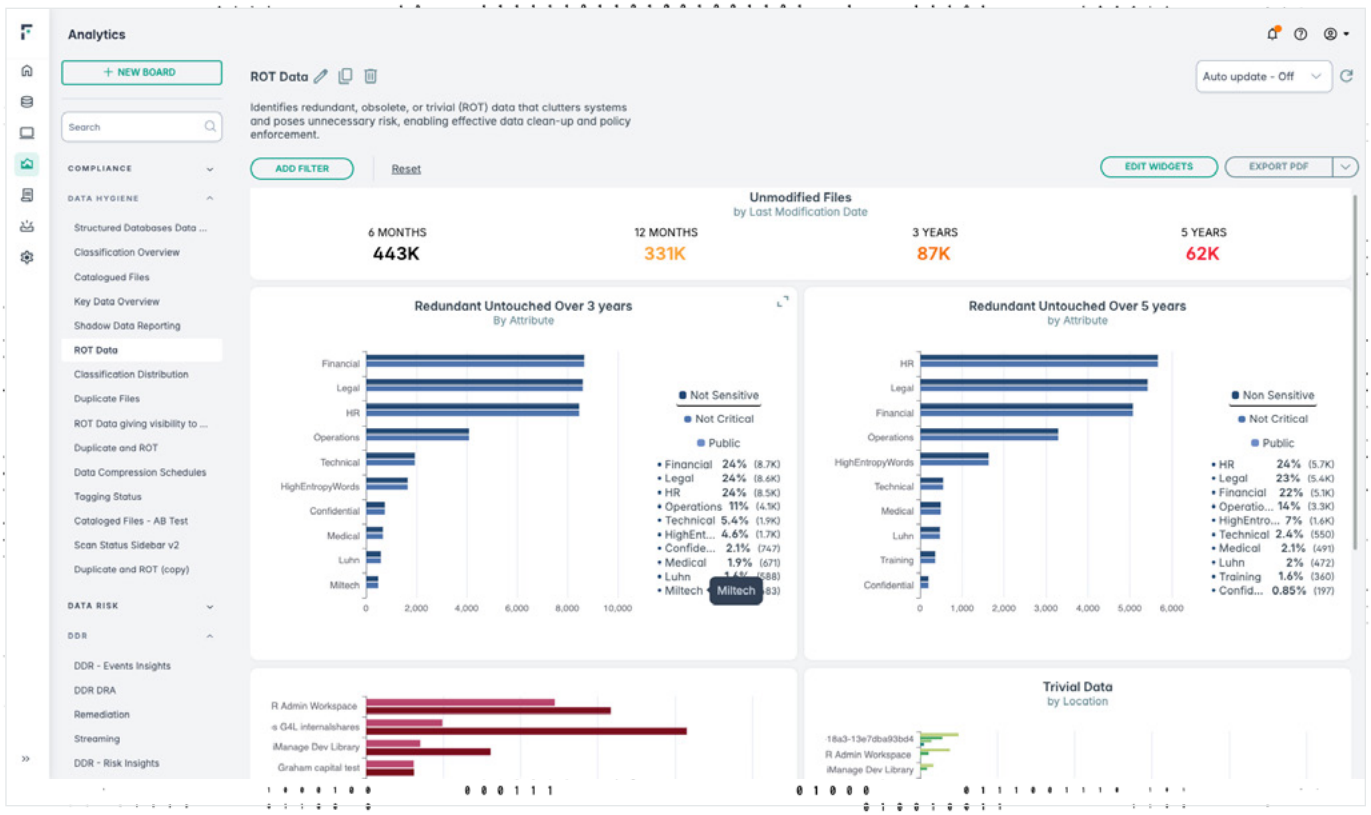
AIメッシュで実現した精度

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、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。



高性能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タ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ソリューションの導入は、データセキュリティ態勢を強化し、クラウドおよびオンプレミスのデータストレージ環境全体で機密情報を保護しようとする組織にとって不可欠です。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し、AI導入を支援し、コラボレーションを促進することで生産性を向上させることができます。同時に、機密データの不適切な使用をプロアクティブに特定して対処することでリスクを軽減し、データ漏洩を防止することができます。最終的に、組織はすべての環境にわたる機密データへの真の可視性と制御を実現することで、コンプライアンスへの取り組みを効率化できます 。

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、秒/時あたりより多くのファイルをスキャンし、非構造化データ資産と構造化データ資産に関する詳細を合成し、簡単に消化できるフォーマットに整理します。
重要なデータソースに接続	さまざまなデータソースコネクタを提供することで、非構造化データと構造化データの堅牢な可視化を実現します。
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。
アクセス許可を表示し修復	各ファイルのアクセスを表示し、最小特権（POLP）の Zero Trust セキュリティを確立するために修正します。
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
非構造化データと構造化データのAI Mesh分類	非構造化データと構造化データ向けの高精度なAI分類を実現します 。
カスタム・モデル・トレーニング	組織は、AI Meshモデルを独自のデータニーズ（IP、営業秘密など）に合わせてカスタマイズし、高精度なデータ分類を実現し、DSPMとDLPの誤陽性/否定的を減らすことができます。
タグをMicrosoft Purview IPタグにマッピング	分類粒度の追加レイヤーを提供し、MIPタグを補完し、修正することができます。MIPタグを修正することができます。
データタグ	スキャンおよび分類されたすべてのファイルに、標準タグ付け（分類、高度機密、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、POなどのサブタグ付き）でDLPで読み取れる永続的なラベルを付けてください。
Forcepoint DLPと統合	Forcepoint DLPと統合し、DSPMのAI Meshタグ付け を活用し、強力なポリシーを構築することができます。

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で、組織の現在のデータセキュリティ体制を複数のカテゴリーにわたって分析することができます。
詳細なインタラクティブダッシュボード	ファイルとデータベースの総合的な詳細を1つのソリューションで表示します。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の生成を簡素化して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に対する洞察を簡単に得られる高度な分析スイートを体験できます。さまざまな定義済みのダッシュボードから選択、または独自に作成し、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。事前定義されたダッシュボードには、過剰露出とランサムウェア分析、重要なデータの重複、危険なユーザーの検知、データ保持、誤った配置データ、データリスク評価、主権、データ管理違反のインシデント追跡に加え、さらに多くが含まれます。
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る可能性のあ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	コーディングスキルを必要とせずにカスタム・ユース・ケースと分析レポートを簡単に作成します。
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。

権限の修復

特徴	利点
権限の修復	データセキュリティガバナンスのインシデントやコンプライアンス上の問題に関する通知を受け取り、既存のITSMおよび生産性ツールを使用した追跡・管理を効率化します。過剰に公開されたデータに対するアラートも含まれます。
データ重複排除の修復	DSPMの重複排除機能は冗長なデータを特定・排除し、ストレージ需要とコストを削減してリソース配分を最適化します。カスタマイズ可能なデータコントロールに従って自動的に削除されます。
ファイルスタビング	DSPMを使用してファイルを移動する際に、ファイルの場所の変更を記録することでビジネスプロセスを維持するため、ファイルスタブを自動的に作成します。

© 2025 Forcepoint. ForcepointおよびFORCEPOINTのロゴはForcepointの商標です。この文書で使用される他のすべての商標はそれぞれの所有者の財産です。[FP-Data Security Posture Management Datasheet-JA] 23Dec2025