
Forcepoint DSPM

Powered by GetVisibility



Forcepoint

パンフレット

デジタル変革の次の進化となる「AI変革」

この新たな時代、あなたのデータは安全ですか？

デジタル変革を経験した組織のほとんどが今、次の進化となるAI変革に向けて準備を進めています。この新しいAI時代を推進しているのは、ChatGPT、Copilot、GeminiなどのGenAIアプリケーションから得られる多くのメリットです。デジタル変革を経験してきた中で、組織はデータセキュリティが最優先事項でなければならないことを学びました。しかし、多くの組織にとって、今日のデータは巨大な氷山のようなもので、その大部分は表面の下に隠されています。しばしば「ダークデータ」や「シャドウデータ」とも呼ばれるこれらのデータは、目に見えない未知のものでありながらも、組織が直接的な責任を負う重要な機密情報が大量に含まれています。今、組織は、ユーザーがGenAIアプリケーションを安全に活用して、生産性と効率性を高められるようにしながら、同時にユーザーの機密データを確実に保護するために取り組んでいます。



DSPM (Data Security Posture Management、データセキュリティ体制管理) は、不正アクセスや開示、改ざん、またはデータ破壊から情報を保護する包括的なアプローチを提供します。システムやデバイスに焦点を当てる他のデータセキュリティ方式とは異なり、DSPMは組織全体のデータそのものに焦点を当ててコンプライアンスを確保し、データ漏洩のリスクを軽減させます。



IDCによると、データの80%は世界的に構造化されておらず、データの90%は分析されていません。そのデータは「ダークデータ」とも呼ばれています。¹



94%の企業は、データを複数のクラウド環境に保管しています。²



Equifaxは14億ドルの訴訟を解決しましたが、これは従業員の名とパスワードを含む複数ファイルのコピーを保管する共有ドライブが、ハッカーにアクセスされて深刻化したデータ漏洩³に関するものです。同社には、冗長で古いファイルを検出して識別するためのツールが欠けていたのです。

1 目に見えないデータの難問 (The Unseen Data Conundrum)、フォオプス、2022年2月

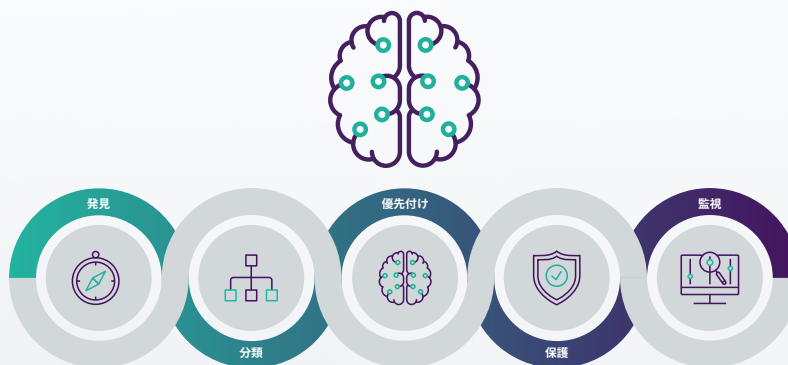
2 ダークデータ：クラウドの知られざるセキュリティとプライバシーのリスク (Dark Data: The Cloud's Unknown Security and Privacy Risk)、フォオプス、2023年6月

3 Equifaxが13億8000万ドルのデータ漏洩訴訟の和解に同意 (Equifax agrees \$1.38bn data breach lawsuit settlement)、Finextra、2020年1月

DSPMが対処するものとは？

- **AI変革の旅:** Forcepoint DSPMでAIの可能性を解き放ち、高度なAI Meshテクノロジーであらゆる場所のデータを保護します。Forcepoint DSPMでは一元的な可視性、Forcepoint ONEデータセキュリティからは管理性を提供することで、ChatGPT、Copilot、GeminiなどのGenAIアプリを含む主要なチャンネル全体にまたがる機密情報を保護することで、生産性を高め、リスクを軽減しながら大胆なイノベーションを推進できるようサポートします。
- **機密データの識別:** DSPMは、組織が複数のクラウド環境やクラウドサービス、およびオンプレミスロケーション全体に保管した機密データを識別する支援をします。これには、機密データの所在場所やアクセス方法、そして操作権限を持つユーザーが誰なのかを理解することが含まれます。
- **脆弱性とリスクの評価:** DSPMは、セキュリティ脅威に対する機密データの脆弱性とコンプライアンス違反のリスクを評価します。データのセキュリティ体制を分析することで、組織は潜在的なリスクに積極的に取り組むことができます。
- **ソースのデータを重視:** 主にデバイス、システム、アプリケーションを保護する他のデータセキュリティツールとは異なり、DSPMは組織全体のデータを直接保護することに焦点を当てています。データ漏洩を防ぎ、そのコアにあるデータを保護することによるコンプライアンス確保を目指しています。
- **ダークデータとROTデータに対処:** DSPMは、ダークデータ（現時点で見られないデータや通常のビジネスプロセスでは使用されないデータ）に直接対処します。同様に、DSPMは、企業が大量のデータをさまざまな理由（今後コンプライアンスの維持に役立つだろうと考えるなど）で保持し続けるために、組織全体で急増しがちであるROT（冗長、古い、低重要度）データに対処することができます。実際には、データを保持し続ける行為はデータリスクをさらに深刻化させますが、DSPMはこのリスクを管理するのに役立ちます。
- **過剰に許可/公開されたデータへの対処:** データは、新しいバージョンをコピーして編集することで増殖するため、データへのアクセス権がユーザー、グループ、さらには組織全体に広がることも多々あります。DSPMは、データ漏洩を防ぐ方法として、過剰に許可されたデータを劇的に削減する「最小権限の原則」、ゼロトラストの概念を強制するのに役立ちます。
- **マルチクラウドおよびハイブリッドクラウド環境:** 組織がマルチクラウドやハイブリッドのクラウド環境を導入することで、データ漏洩のリスクが劇的に増加します。DSPMは、オンプレミスロケーションに加えて、これらの多様なコンピューティング環境全体の機密データに対する可視性と制御を提供します。

Forcepoint DSPMは、ビジネスデータに対する優れた可視性と制御を必要とする現代の組織向けに設計されています。あらゆるクラウド環境やサーバーへの可視性を実現し、データ漏洩を防ぎ、プライバシー規制に対する違反のリスクを軽減します。Forcepointは、データのライフサイクル全体に対する完全な可視性と制御を実現し、**データリスクの積極的な発見** (DSPM) と **データの使用方法に対するアクティブ制御** (DLPとSSE) を組み合わせると同時に、**各ユーザーの行動に継続的に適応** (リスク適応型保護) することで、Data Security Everywhereを提供します。



AIを活用した検出、分類、オーケストレーション



Forcepoint DSPMでデータ環境の全体像に対する可視化と制御を統一

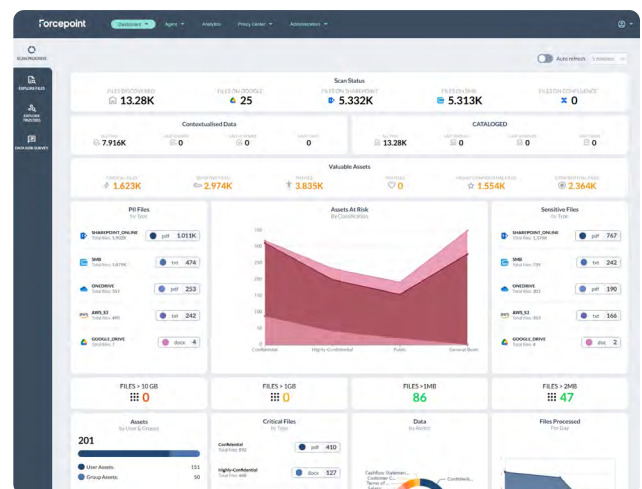
組織データの管理と安全性の確保は、かつてないほど複雑になりました。Forcepoint DSPM は、場所を問わずデータを包括的に可視化し制御できる強力なソリューションを提供します。業界をリードする検出速度と高度な AI Mesh データ分類機能により、Forcepoint DSPM は、データセキュリティ体制について十分な情報に基づいた意思決定を行い、潜在的なリスクに積極的に取り組むことを支援します。

Forcepoint DSPMを使用する主なメリットは次のとおりです。

高速で包括的な検出:複数のクラウドと オンプレミスで、Forcepoint DSPMは、毎時間100万個のファイルを迅速にスキャンすることができます。組織が責任を持って管理すべきデータが何テラバイト、あるいは何ペタバイトにもものぼることは珍しくありません。Forcepointは高性能な検出機能により、組織がChatGPT Enterprise を含む 膨大なデータ環境全体のデータを 素早く把握できるようにします。DSPMを提供する他のプロバイダーとは異なり、他の DSPM プロバイダーとは異なり、Forcepoint は検出の実行に料金を請求しません。お客様は追加料金なしで、好きなだけ検出を実行できます。

AI Meshで得られる精度:Forcepoint DSPMは、クラウドおよびネットワークソース全体からデータを検出し、高度なAI分類エンジンを活用して、これらのデータを自動的に分類します。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。AI Meshのネットワーク化されたAIアーキテクチャは、GenAI小規模言語モデル (SLM) と高度なデータとAIコンポーネントを活用することで、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のが特徴で、広範なトレーニングをしなくても迅速で正確な分類を確保できるため、信頼性とコンプライアンスが強化されます。最終的に、この高い精度によって、他の一般的な分類方法では満足のいく結果を得られていなかった組織でも、誤検知の問題を大幅に低減させ、知的財産を保護し、時間とリソースの面で大幅にコストを節約することができます。

データ環境全体に対するデータの可視化:Forcepoint DSPMを使用して、すべてのファイルとユーザーのアクセス許可を検査することができます。データ管理者は、組織全体でファイルあるいはファイル共有にアクセスできる個人を確認できます。スキャンされたすべてのファイルに対するアクセス許可をワンクリックで閲覧することが可能です。Forcepoint DSPMは、詳細を示すダッシュボードでリアルタイムでレポートを提供するため、ダークデータ全体を俯瞰的に見る事が可能です。同時に、データリスクアセスメントの概要を提供することで、データのリスクが最も高い領域をユーザーが理解するのに役立ちます。



ワークフロー オーケストレーション: さまざまなデータセットの所有権と説明責任を簡単に定義して、関係者の調整プロセスを効率化します。これにより、各データソースと資産に実行されるアクションに関するより効果的なワークフローを実現します。効果的な修復には、セキュリティ組織を超越して CDO/DataOps グループへの幅広い賛同とコラボレーションが不可欠であり、マーケティング、財務、DevOps、その他数多くの機能も必要です。Forcepoint DSPM は、データ体制の安全性を単にセキュリティ上の問題としてではなく、ビジネスの優先事項として考えます。



データリスクによるビジネスの機能不全を防ぎましょう。Forcepointをご活用ください！

今日のデジタル時代では、データは組織にとって最も価値のある資産です。しかし、データが適切に管理されていないと、組織が重大な責任を負うことになる可能性もあります。Forcepoint DSPMは、機密データを保護し、データ漏洩のリスクを低減し、規制コンプライアンスを確保するための積極的なアプローチを提供します。Forcepoint DSPMを実装することで、データのランドスケープを包括的に可視化し、脆弱性を特定して対処し、データ漏洩や規制違反によって引き起こされる財務的な被害や風評被害を未然に防ぐことで組織を保護しながら、同時にGenAIアプリケーション内のデータも保護することができます。今すぐデータセキュリティ体制を制御しましょう。DSPMが貴重な情報をどのように保護するのかについて、詳しくご覧ください。www.forcepoint.com/ja/dspm にアクセスしてデモをリクエストするか、無料のデータリスク評価にお申し込みください。このリスク評価では、セキュリティエンジニアがお客様固有のデータに対してサンプルランを実行し、現在直面しているデータリスクの種類を確認させていただきます。

Forcepoint

forcepoint.com/contact

Forcepointについて

Forcepointは、グローバルなビジネスと政府機関向けのセキュリティを簡素化します。Forcepointが提供するオールインワン、完全クラウドネイティブ型のプラットフォームにより、ゼロトラストの採用が容易になります。またユーザーがどこで働いていても、機密データや知的財産の盗難や紛失の防止は簡単です。テキサス州オースティンに拠点を置くForcepointは、150か国以上の顧客組織とその従業員に対して、安全で信頼できる環境を作り出しています。 www.forcepoint.com, Twitter で LinkedIn. Forcepointとつながりましょう。