Forcepoint DSPM

Forcepoint

パンフレット

forcepoint.com/ja

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。システムとデバイスに焦点を当てる他のタイプのデータセキュリティ手法とは異なり、DSPMは、構造化または非構造化、知的財産から規制対象データまで、クラウドまたはプライベートネットワークの組織のデータ全体に焦点を当て、コンプライアンスを確保し、データ侵害のリスクを軽減します。

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、これは従業員のユーザー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）、フォーブス、2022年2月

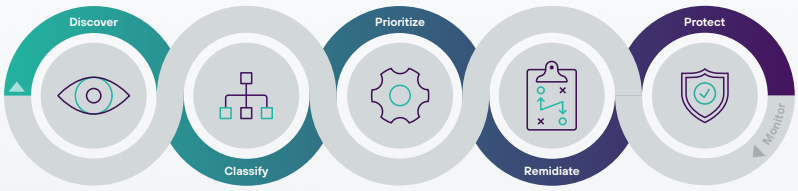
2 ダークデータ：クラウドの知られざるセキュリティとプライバシーのリスク（Dark Data: The Cloud's Unknown Security and Privacy Risk）、フォーブス、2023年6月

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

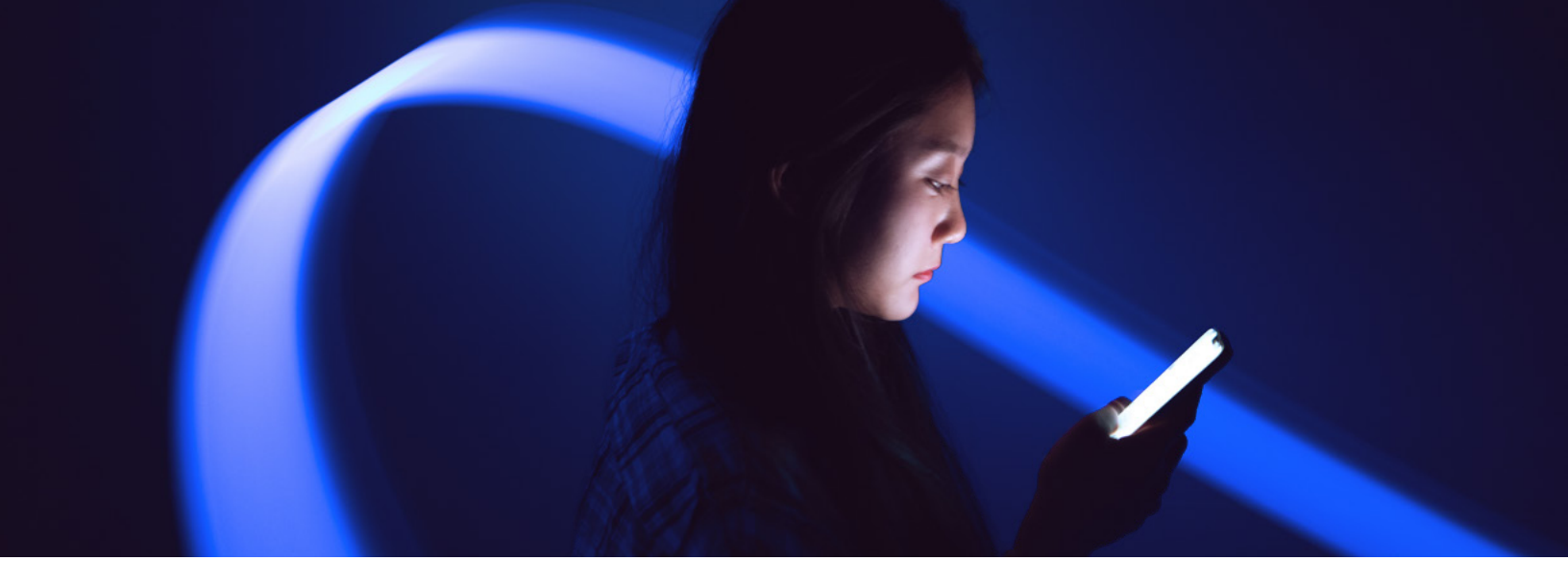
DSPMが対処するものとは?

- → **AI変革のプロセス:** Forcepoint DSPMでAIの可能性を解き放ち、高度なAI Mesh技術であらゆる場所でデータを保護します。Forcepoint DSPMの可視化と修復の一元化、Forcepoint DLPのリアルタイムブロック制御により、ChatGPT、Copilot、GeminiなどのGenAIアプリケーションを含む主要なチャネル全体で機密情報を保護し、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可能にします。
- → **機密データの特定:** DSPMは、構造化データと非構造化データ両方を含む、複数のクラウド環境とサービスだけでなく、オンプレミスロケーション全体にわたって組織が機密データを特定するのを支援します。これには、機密データがどこに存在し、どのようにアクセスされるか、誰がデータとやり取りする権限を持っている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。
- → **継続的なリスク監視:** Forcepoint DSPMは、Forcepoint Data Detection and Response(DDR)のアドオンにより、新しいデータリスクの発生時に検出し、修復できます。次回のDSPMスキャンを完了するまで待つ必要はありません。データセキュリティ体制に対するリスクを動的に特定し、修復します。

Forcepoint DSPMは、機密データの強力な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。さまざまなクラウド環境やサーバー全体で可視性を提供することで、データ侵害を防止し、プライバシー規制違反のリスクを軽減します。Forcepointは、データライフサイクル全体にわたって完全な可視化と制御を実現します。Data Security Everywhereは、**各ユーザーのアクションに継続的に適応** (Risk-Adaptive Protection) しながら、**データリスクのプロアクティブな検出** (DSPM)と**データの使用方法に対するアクティブな制御** (DLP) を組み合わせます。継続的な監視 (Forcepoint DDR) により、データリスクを動的に検出し、データ侵害を防止し、データセキュリティの状態を保護します。



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

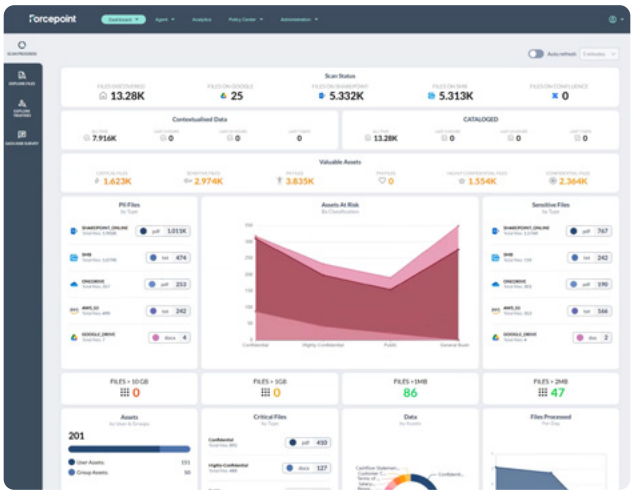
組織データの管理と安全性の確保は、かつてないほど複雑になりました。Forcepoint DSPM は、場所を問わずデータを包括的に可視化し制御できる強力なソリューションを提供します。業界をリードする検出速度と高度な AI Mesh データ分類機能により、Forcepoint DSPM は、データセキュリティ体制について十分な情報に基づいた意思決定を行い、潜在的なリスクに積極的に取り組むことを支援します。

Forcepoint DSPMを使用する主なメリットは次のとおりです。

迅速で包括的な検出：Forcepoint DSPMは、複数のクラウドとオンプレミス全体で、ファイルとデータベースを迅速にスキャンします。組織が責任を持って管理すべきデータの量が数テラバイト、または数ペタバイトにものぼることは珍しくなく、中にはエクサバイト単位のデータを保持している大規模組織もあります。Forcepointは高性能検出機能の実装により、ChatGPT Enterpriseを含む大規模なデータ環境全体にあるデータを企業がすばやく確認することを可能にします。他のDSPMプロバイダーとは異なり、Forcepointは検出スキャンに対して料金を請求しません。お客様は追加料金なしで必要なだけ検出スキャンを実行できます。

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。

データ全体の可視化：Forcepoint DSPMを使用すると、すべてのファイルとユーザーのアクセス許可を検査できます。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、ダークデータの概要を提供するダッシュボードと、データリスク評価の概要を提供し、データリスクが最も高い領域を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/Governance、Risk and Compliance（GRC）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。

Forcepoint DDR：Forcepoint DSPMの強力なアドオンであり、データ侵害に対応するための重要なソリューションです。継続的な脅威検出とデータリスクの視認性を実現し、データ侵害につながる可能性のあるデータへの変更を組織が効果的に確認できるようにします。Forcepoint DDRは、AI駆動の対応を活用することで、脅威を正確に無力化し、組織が堅牢なセキュリティ対策を維持するのに役立ちます。クラウドとエンドポイント全体にわたる広範な視認性と、データ系統の追跡により、機密情報を保護し、財務損失を軽減し、お客様の信頼を維持するために不可欠なツールとなっています。

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。