Zscaler Data Security Posture Management (DSPM)

ソリューションの概要

概要：クラウド時代におけるデータ保護

マルチクラウド環境で膨大な量のビジネス データを保護する際の課題として挙げられるのが、データ保護の複雑さと規模の管理、内部脅威やデータ侵害、サード パーティーやベンダーのアクセス、サプライ チェーンのリスクへの対処、そしてデータ規制の順守です。組織の重要なデータ資産をさまざまな脅威から保護しながら、インベントリーの作成、分類、制御、保護を行うことは簡単ではありません。さらに、さまざまな環境に保存された多数のデータと一貫性のない役割や権限によってこの状況はますます複雑になっています。

複雑な環境	データ量	高度な 標的型攻撃	過剰な特権アクセス
クラウドに保存されたデータに関連する侵害は全体の 82%[1]	2025 年までにクラウドに保存されるデータは推定で 175 ZB[2]	2024 年のデータ侵害の世界平均被害額は 488 万ドル [3]	アイデンティティー関連の侵害を受けた組織の割合は 80%[4]

残念ながら、従来のデータ保護ソリューションは動的なマルチクラウド環境に適した設計にはなっていませんでした。同時に、DSPM を単体で提供するベンダーはサイロ化したアプローチを採用しているため、既存のデータ保護プログラムにシームレスに統合できません。クラウド データの保護には、一元的な新しいアプローチが求められているのです。

Zscaler は、マルチクラウド環境におけるこうしたデータ セキュリティの課題を完全に統合されたエージェントレスのデータ セキュリティ ポスチャー管理 (DSPM) ソリューションで解消します。

DSPM とは

「データ セキュリティ ポスチャー管理 (DSPM) は、機密データの保管先やそのデータにアクセスできる人物、使用状況、保存データやアプリケーションのセキュリティ態勢などを可視化します」 —Gartner

DSPM は「データ ファースト」セキュリティとも呼ばれ、他のサイバーセキュリティ技術や慣行に採用されている保護モデルとは逆のアプローチを取ります。データを格納、移動、処理するデバイス、システム、アプリケーションを保護するのではなく、データを直接保護することを重視し、組織のセキュリティ スタックに含まれる他の多くのソリューションを補完します。

DSPM はセキュリティ制御を継続的に監視、評価、最適化して、マルチクラウド プラットフォーム全体にわたって機密データを保護します。また、機密データ、潜在的な脆弱性、設定ミス、コンプライアンス違反を自動的に特定するため、組織は情報漏洩のリスクに予防的に対処できるようになります。DSPM のこうした機能により、データ セキュリティ態勢全体の強化、データ侵害リスクの最小化、各種規制要件の順守が可能になります。

1. https://www.informationweek.com/cyber-resilience/data-breaches-just-keep-piling-up
2. https://www.forbes.com/sites/tomcoughlin/2018/11/27/175-zettabytes-by-2025/
3. https://www.ibm.com/reports/data-breach
4. https://www.darkreading.com/cybersecurity-operations/identity-related-breaches-last-12-months

DSPM が必要な理由

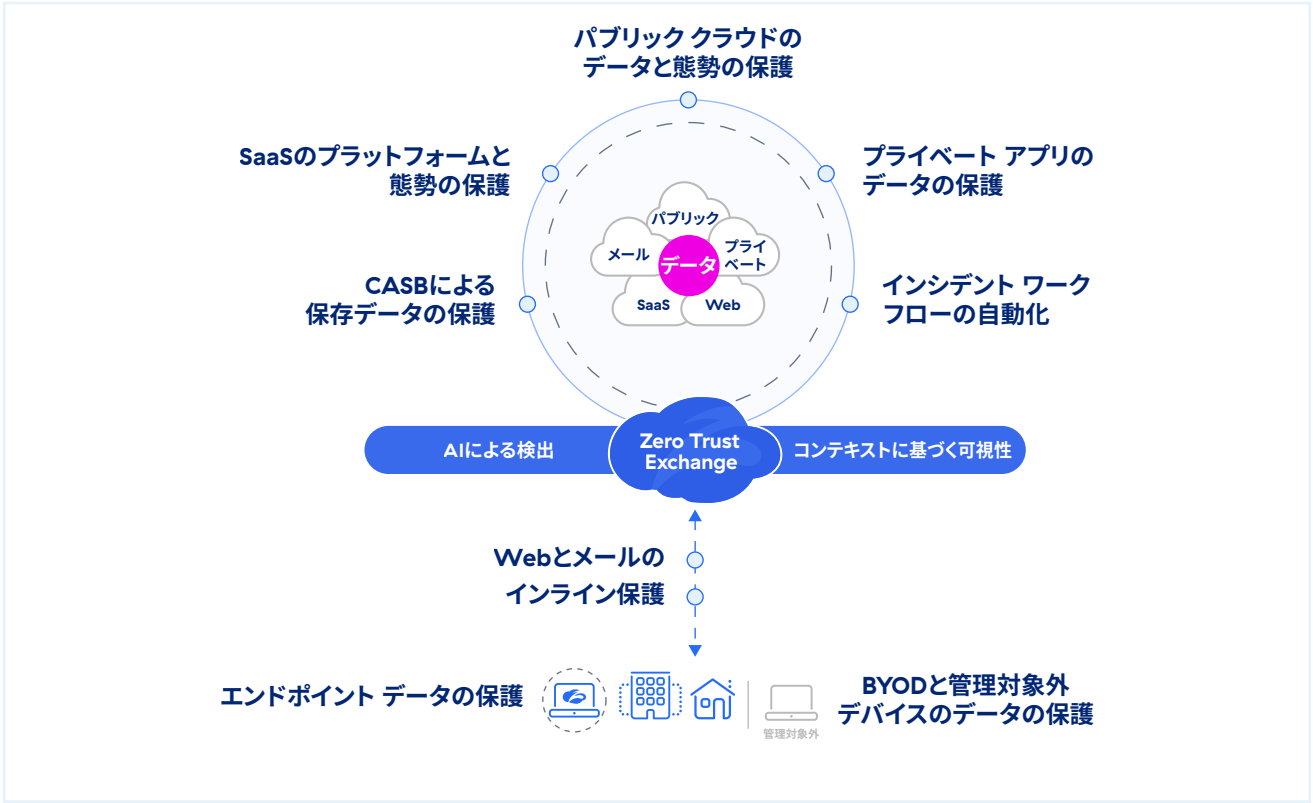
DSPM ツールは主に、脆弱な部分を見つけ、セキュリティ設定を監視し、機密データに対する潜在的な脅威を特定することで、組織のデータ環境のセキュリティ状態を評価し、対処することを目的としています。その機能はポリシー管理だけにとどまらず、実際のデータ自体も監視します。

DSPM はデータをスキャンして分類することで、組織が機密データの場所と使用状況を完全に把握できるようにします。同時に、特定された問題に優先順位を付け、そのような問題を見落とす原因にもなりえる大量のアラートも防ぎます。

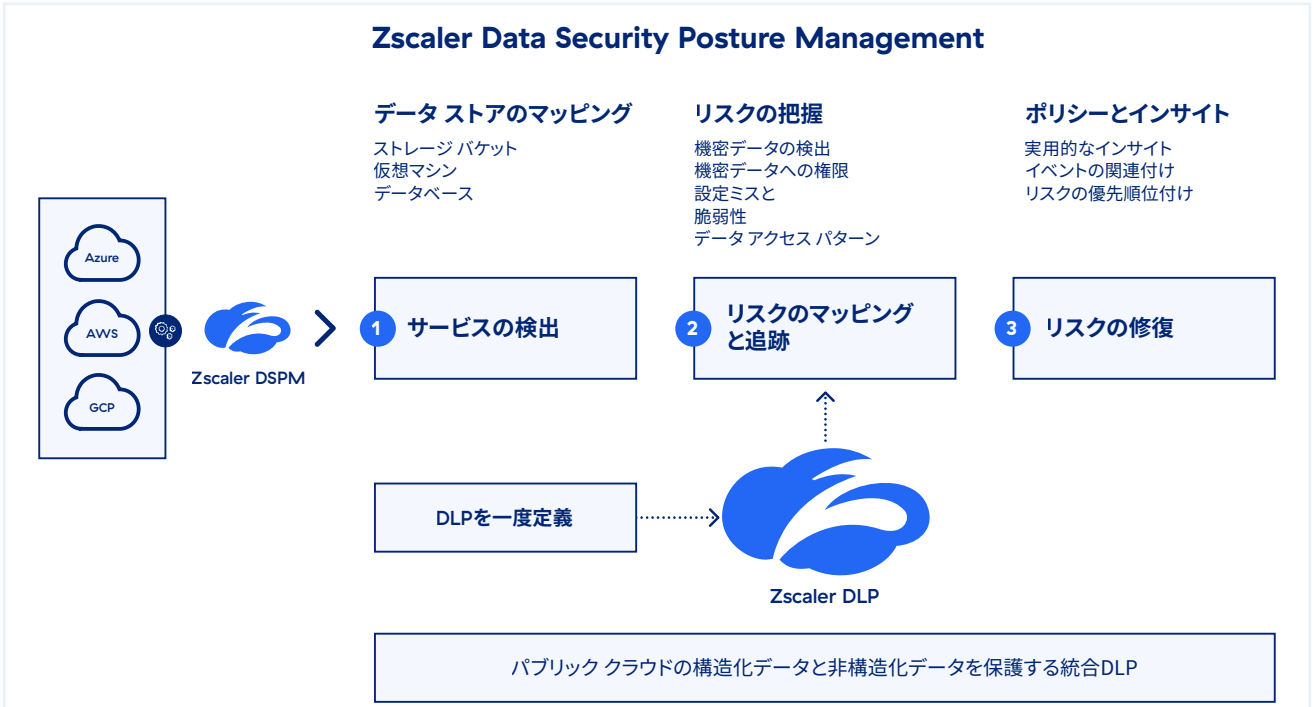
DSPM の実際のユース ケースには、クラウド環境におけるセキュリティの脆弱性 (暗号化など) の検出、アクセス ポリシーの施行、インシデント管理用のアラートと調査機能の提供などがあります。

Zscaler DSPM の仕組み

最も包括的な完全統合型データ保護プラットフォームである Zscaler AI Data Protection は、Web、SaaS ベースのサービス、パブリック クラウド (AWS、Azure、GCP)、プライベート アプリケーション、メール、エンドポイントなど、あらゆる環境の構造化データおよび非構造化データを保護します。



Zscaler DSPM はこのプラットフォームの一部として、クラス最高の堅牢なデータ セキュリティをパブリック クラウドに拡張します。そして、クラウド データを詳細に可視化するとともに、データとアクセスを特定して分類し、データの公開状況とセキュリティ態勢をコンテキスト化します。セキュリティ部門はこれらの情報を活用することで、大規模なクラウド データ侵害を阻止し、修復できるようになります。



また、統合された単一の DLP エンジンにより、すべてのチャネルで一貫したデータ保護が実現します。あらゆる場所のあらゆるユーザーを追跡し、使用中のデータと保存データを管理することで、機密データをシームレスに保護しながら、コンプライアンスを確保します。

Zscaler DSPM の主な機能

データの検出、分類、インベントリー
従来のスキャン方法はコストがかかり、実用的な結果を得るには多大な労力が必要です。Zscaler DSPM は、クラウド環境 (AWS、Azure、GCP) のリソースへのアクセスを最小限に抑えながら、データ ストアをスキャンし、機密データの検出と正確な分類を行います。この機能により、以下を実現できます。

- **包括的なデータ検出：**クラウド環境を常に監視し、変化し続けるデータ環境でインスタンス化された新しいデータ ストアを自動的に検出することで、時間を節約し、データの死角をなくします。
- **綿密なデータ分類：**定義済みの DLP エンジンと辞書を使用してデータを分類します。クラウド リソースに保存されている機密データの種類、地域、機密データを含むファイル、機密データに関連するリスクの重大度などを可視化します。さらに、使用可能な既存のポリシーを作成または複製する柔軟性も提供します。
- **正確なデータ インベントリー：**データ資産を正確にマッピングし、インベントリーを作成します。そのため、セキュリティ部門は機密データの場所を特定し、そのデータにアクセスした人物や使用状況を把握できます。

Zscaler DSPM を使用することで、クラウド インフラ内のデータの可視性が高まるため、SaaS や PaaS、IaaS、データベースの複雑なレイヤーが含まれるマルチクラウド環境のデータ セキュリティ態勢の管理と改善がはるかに容易になります。

情報漏洩のマッピングと追跡

クラウドのサービスや構成は頻繁に変更されるため、情報漏洩につながる可能性があります。こうしたセキュリティ ギャップは、悪意のある人物に悪用される前に修正する必要があります。Zscaler DSPM は、公開されているリソースだけでなく、データ リソースに関連付けられているさまざまなコンポーネント (ネットワーク セキュリティ グループ、ロード バランサー、仮想ネットワークなど) の脆弱性や設定ミスも検出します。この機能により、以下を実現できます。

- **エクスポージャー分析：**データ ストアとサービスの公開状況、設定ミス、脆弱性を特定します。
- **リスク評価：**影響と可能性を組み合わせて、全体的なリスク レベルを集計します。リスクは、高、中、低のレベルに分類されます。
- **リスクの優先順位付け：**セキュリティ部門はノイズを排除し、リスクと重大度に基づいてインシデントに優先順位を付けられます。
- **高度な脅威相関：**脅威やリスク要因、隠れた攻撃経路を関連付けて、リスクを最小限に抑えます。
- **適応型アクセス インテリジェンス：**ミッションクリティカルなデータと構成へのすべてのアクセス経路をリスクとユーザーに基づいてきめ細かく表示します。

リスクの修復

Zscaler DSPM では、コンテキストベースの修復ガイダンスによってリスク管理が合理化されるため、セキュリティ部門は問題や違反を発生元で簡単に修正して、中断を未然に防ぐことができます。DSPM の主な機能は以下のとおりです。

- **効果的な調査と対応**により、セキュリティ部門はデータ セキュリティ イベントを調査する際に潜在的な根本原因を迅速に把握できます。
- **詳細な修復ガイダンス**：自動化されたワークフローと、完全なコンテキストを含むステップごとの修復プロセスで、機能横断的な部門がデータ セキュリティ リスクに対処し、効果的に修復できるようにします。
- **セキュリティ対応時間の短縮**：データとその環境の急速な変化に対応するリアルタイムのカスタム アラートを設定し、調査と対応を迅速化できます。
- **シームレスな統合**：既存の ITSM、SIEM、ChatOps のツールやプラットフォームと簡単に統合し、アラート、修復、ガイダンス、ワークフローの管理を行えます。

Zscaler DSPM のさらなる詳細

デモを依頼
ガイド付きのデモで Zscaler DSPM を体験してください。

デモを依頼

DSPM の購入ガイドをダウンロード
組織に最適な DSPM を選択するために考慮すべき 5 つの要件を解説します。

今すぐダウンロード

詳細は、zscaler.com/jp/dspm をご覧ください。

参考

用語

- データ セキュリティ ポスチャー管理(DSPM)
- クラウド ネイティブ アプリケーション保護プラットフォーム(CNAPP)
- クラウド セキュリティ ポスチャー管理(CSPM)
- クラウド インフラストラクチャー エンタイトルメント管理(CIEM)

その他のリソース
QRコードをスキャンして
DSPMリソースにアクセス

オンデマンド セッション

- 基調講演：Zenith Live '24 のセッション「Zscaler DSPM: Secure Cloud Data with a Fully Integrated Platform (英語)」
  —Inter&Co の DSPM の取り組み
- ウェビナー：「Why Does DSPM Belong In Your Data Protection Strategy? (英語)」

zscaler™ | Experience your world, secured.™

Zscaler について
Zscaler (**NASDAQ: ZS**) は、より効率的で、俊敏性や回復性に優れたセキュアなデジタル トランスフォーメーションを加速しています。**Zscaler Zero Trust Exchange** は、ユーザー、デバイス、アプリケーションをどこからでも安全に接続させることで、数多くのお客様をサイバー攻撃や情報漏洩から保護しています。世界 **150** 拠点以上のデータ センターに分散された **SSE** ベースの **Zero Trust Exchange** は、世界最大のインライン型クラウド セキュリティ プラットフォームです。詳細は、**zscaler.com/jp** をご覧いただくか、**Twitter** で **@zscaler** をフォローしてください。

+1 408.533.0288 Zscaler, Inc. (HQ) • 120 Holger Way • San Jose, CA 95134 zscaler.com/jp