COHESITY

バイヤーズガイド

データとAIリスクを適切なDSPMソリューションで管理する

エグゼクティブサマリー

機密データは現在、クラウドプラットフォーム、SaaS、データベース、バックアップ、ハイブリッド環境、NASなど、さまざまな場所に分散しています。すでに、容易に管理しきれない量のデータを抱えている可能性があります。しかし、最も機密性の高いデータがどこに存在するのか、どの程度公開されているのか、誰がアクセスできるのか、そしてそのアクセスが適切かどうかを把握するのは困難です。

これにより、経営層レベルでのビジネスリスクが一層高まる状況が生じています。そして、この課題は拡大し続けています。人々がデータにアクセスし、変更し、移動させ続ける一方で、AIエージェントが新たなリスクを次々と生み出しています。

こうしたセキュリティおよび保護のギャップこそが、データセキュリティポスチャ管理（DSPM）が現代の企業リーダーにとって戦略的優先事項となっている理由です。

89% セキュリティリーダーの89%が、自社のデータセキュリティの現状に課題があると認識しています。

39% セキュリティリーダーの39%が、従来のテクノロジーでは現在の要件を満たせないと回答しています。

60% 企業の60%は、自社のデータ資産の少なくとも半分について可視性を欠いています。[1]

[1]Omdiaホワイトペーパー：実行可能なデータインテリジェンスによるサイバーレジリエンスの実現

現代のDSPMソリューションは、単なるデータの棚卸し以上の役割を果たすべきです。リスクを能動的に低減し、サイバーレジリエンスを強化し、インシデント対応やセキュリティ訓練、監査時に重要な問いへ答えられるよう支援する必要があります。

- 当社の機密データはどこにあり、どのようなものか？
- 誰または何がそれにアクセスできるのか？
- 最初に対処すべきことは何か？
- ビジネスの革新と成長を阻害せずに、どのようにリスクを低減するか？
- データは適切に保護され、迅速かつ安全に、コンプライアンスを満たして復旧できるか？

セキュリティリーダーにとってこれは、攻撃の前後を通じて「可視化」から「実行可能なリスク低減」へと移行することを意味します。

本ガイドは、DSPMソリューションを評価するチームが、自社のニーズに最適な選択を行うためのものです。

インベントリだけでは不十分です。

重要なのは、ソリューションが単にデータの所在を示せるかどうかではありません。そのデータがなぜ高リスクなのかを特定し、今すぐ実行可能なリスク低減策を提示できるかどうかです。

DSPMが解決すること

DSPMを評価する際に多くの組織が犯す典型的な誤りの一つは、単なるデータ発見ツールとして捉えてしまうことです。DSPMソリューションは、可視化にとどまるものではありません。適切なソリューションは、データリスクポスチャに関する課題解決を支援するものであるべきです。

DSPMソリューションが解決すべき5つの課題は次のとおりです。

課題	DSPMによる解決策
自社の機密データがどこにあるのかわからない。	多くの組織は、クラウド、SaaS、ハイブリッド環境全体において、重要度の高いデータや規制対象データがどこに存在するかを自信を持って把握できていません。なぜこのような状況が生じているのでしょうか？ 従来のデータセキュリティツールは、特定のデータ種別、導入形態、またはユースケースごとに分断されています。 一定のインベントリが存在していても、不完全であったり、最新でなかったり、リスクの文脈と結び付いていない場合が多くあります。データ量の増大と分散に対応するには、最新のクラウドネイティブアーキテクチャが不可欠です。
誰または何が自社のデータにアクセスしているのか（あるいはアクセス可能なのか）がわからない。	一般的な従業員は、200以上のコラボレーションツールを通じて、1日に約36のクラウドサービスとやり取りしています。機密情報はさまざまなプラットフォームに拡散し、しばしば既存のガバナンス統制の外で共有されます。機密データは、過剰な公開、過剰な権限付与、過度な共有、不適切な場所での保存、あるいは想定以上のアイデンティティ（非人間を含む）からアクセス可能になることで、さらにリスクが高まります。 DSPMソリューションは、単に分類ポリシーに一致するデータではなく、実際にリスクにさらされているデータを把握できるようにする必要があります。
どのデータリスクから優先的に対処すべきかがわからない。	ほとんどのエンタープライズ環境には大量の機密データが存在します。しかし、すべてのデータリスクが同じ緊急度を持つわけではありません。チームは、ノイズ（不要なアラート）と実質的なリスク露出を見極める手段を必要としています。適切なソリューションは、機密性、アクセス状況、露出範囲、環境、そしてビジネスコンテキストに基づき、ビジネスへの影響が最も大きい課題に注力できるよう支援する必要があります。
データリスクを迅速かつ自動的に是正できない。	データコンテキストは、セキュリティツールチェーン全体との深い統合と組み合わせることで、高リスクデータの是正におけるMTTR（平均対応時間）を短縮する上で不可欠です。従来のデータセキュリティ手法は、パターンやタグに大きく依存しており、信頼性に欠けるノイズの多いアラートを大量に発生させがちです。 DSPMソリューションは、実際のアクションにつながるものであるべきです。検出結果は、理解しやすく、担当者に割り当て可能で、追跡可能でなければなりません。セキュリティチームおよびITチームは、それらに対して確信を持って対応できる必要があります。
データ復旧が必要な際、対応は遅く、リスクが高く、コストもかかる。	インシデント対応および復旧においては、セカンダリデータ（バックアップなど）が極めて重要です。また、このデータ自体がリスクや潜在的なコンプライアンス違反を引き起こす可能性もあり、対処が必要です。 最新のDSPMソリューションは、サイバーレジリエンスの向上に寄与し、適切な保護レベルが適用されるようデータインテリジェンスを提供する必要があります。機密データは、インシデント対応時に優先順位付けされ、コンプライアンスに準拠して復旧されるべきです。

「望ましい状態」とは何か

ベンダー評価に入る前に、「望ましい状態」の定義を明確にする必要があります。最新のDSPMソリューションが優れているべき5つの領域は次のとおりです。

迅速に導入し、制約なくシームレスにスケールできること

優れたディスカバリー機能は、長期かつ重い導入プロセスを経ることなく、迅速に露出状況の全体像を把握できるよう支援するものであるべきです。

組織は、パフォーマンスを損なうことなく、数百ペタバイト規模のデータを継続的にスキャンできることを期待すべきです。適切なベンダーは、クラウドデータストア、SaaSアプリケーション、ファイルシステム、必要に応じてオンプレミスデータベースなど、主要な環境全体にわたる幅広い対応を提供します。

正確なディスカバリーと分類により死角を排除する

強力なディスカバリーは、質の低い結果が後続のすべてのプロセスに悪影響を及ぼすことを防ぎます。DSPMツールが重要なデータの所在を見逃したり、機密情報を誤分類したり、過度な手動チューニングを必要としたりすると、得られる結果の有用性は低下し、場合によっては無意味になります。

適切なDSPMソリューションは、環境に適応しつつデータを自動分類（知的財産や自社特有の重要データを含む）することで、死角を明らかにします。

ノイズではなく、本当のリスクを優先する

時間は限られており、どのチームもすべてを同時に是正することはできません。優れたDSPMソリューションは、露出状況とコンテキストを組み合わせ、最も重大なリスクに焦点を当てます。特に、広範に露出している高機密データに関するリスクを優先的に扱うべきです。

これには、データの機密性、ビジネス目的、アイデンティティ、アクセスアクティビティ、露出状況を相関分析し、実際のビジネスリスクを可視化する高度な機能が求められます。

大規模な是正を自動化する

現代のDSPMは、単に露出を可視化するだけでなく、それを低減する支援を行う必要があります。組織は、すぐに利用可能な是正機能を備えたDSPMを選定すべきです。たとえば先進的なソリューションでは、アクセス権の剥奪、データマスキング、事前定義ワークフローの実行、データ所有者への自動割り当てなどをワンクリックで実行でき、迅速な解決に必要なコンテキストも同時に提供されます。

これは、多くのチームが関与する大規模環境において特に重要です。セキュリティチームが問題を特定しても、是正はストレージ管理者、データ所有者、アイデンティティ管理チーム、ビジネス部門など複数の関係者に依存する場合が多いためです。こうした引き継ぎを明確に支援できるソリューションほど、セキュリティ体制の向上につながる実効的な成果を生み出しやすくなります。

インシデント前後のセキュリティを強化する

侵害発生前のプロアクティブなリスク低減については既に述べました。適切なDSPMソリューションはさらに、復旧対応を強化するためのデータインテリジェンスとコンテキストを提供し、機密データの所在、重要資産、そして組織の最重要資産に適切な保護が適用されているかを、セキュリティおよびデータ保護チームが確実に把握できるようにします。

機密性が高くビジネス上重要なデータに関する明確な洞察により、DSPMはサイバーレジリエンスを支えるデータ保護戦略の高度化に貢献します。これにより、復旧時に最重要データを優先できるほか、適切なコンテキストによってインシデント対応を迅速化し、不要・重複・低価値データの特定と削減によってコストと複雑性を低減できます。

その結果、可視化、保護、対応、復旧の間に継続的なフィードバックループが形成されます。適切なDSPMソリューションを導入することで、これらの機能を連携させ、分断されたセキュリティ対策から、エンドツーエンドの包括的なデータセキュリティおよびサイバーレジリエンス戦略へと移行することが可能になります。

ベンダー評価キット

ベンダーに確認すべき重要な質問

以下の質問は、DSPM製品の候補評価に役立ちます。

ディスカバリーとカバレッジについて：

- 現在、どのクラウド、SaaS、AI、データベース、ハイブリッド環境に対応していますか？
- 異なるデータタイプにまたがる機密データをどのように検出・分類しますか？ 通常どの程度の時間がかかりますか？
- 構造化データおよび非構造化データにはどのように対応していますか？ どちらかに強みや制約はありますか？
- 有効な結果を得るまでに、どの程度のチューニングが必要ですか？
- 顧客が早期にカバレッジと信頼性を検証できるよう、どのように支援しますか？

露出とアクセス制御について：

- 機密データの過剰な露出をどのように判断しますか？ 機密データにアクセス可能なアイデンティティ、グループ、ユーザーを可視化できますか？
- 広範・過剰・リスクの高いアクセスをどのように特定しますか？
- アクセスコンテキストとデータの機密性をどのように関連付けますか？
- 機密データがAIモデルやシステムに入力されたり、そこから流出したりすることを防止できますか？
- 最もリスクの高い問題をどのように可視化・強調しますか？

リスクの優先順位付けと是正について：

- 検出結果をどのようにランク付け・優先順位付けしますか？ 重大度やリスクスコアに影響を与える要因は何ですか？
- 多数の検出結果から、実行可能なアクションプランへどのように落とし込みますか？
- 是正対応をどのように導きますか？
- 検出結果を適切なチームや担当者に割り当てることはできますか？
- 得られたインサイトをデータ保護プラットフォームとシームレスに連携し、セキュリティおよび復旧の成果向上に活用できますか？

価値創出までの時間と導入について：

- 初期導入にあたり、自社チームには何が求められますか？
- 有用な検出結果はどの程度の期間で得られますか？
- 最初の30日、60日、90日での成功はどのように定義されますか？

注意すべきレッドフラグ

アクセスリスクに関する可視性が不十分

機密データへのアクセスは最大のリスク要因です。ベンダーが、誰（または何）がデータにアクセス可能か、どのようなリスクが存在するかを明確に示せない場合、それは重大な制約となります。

検出結果が個別のビジネスリスクやコンテキストと結び付いていない

ビジネスごとに前提は異なります。機密データや露出した知的財産がもたらすリスクは、その組織にとっての重要性によって大きく変わります。検出結果は、学習されたコンテキストおよび分類ロジックに基づき、正確なリスク是正の提言を導き出すものであるべきです。

データリスクをサイバーレジリエンスの成果に結び付けられない

データおよびAIのリスクポスチャの最適化は、サイバーレジリエンスにおいて極めて重要です。データインテリジェンスは、プロアクティブなデータセキュリティの指針として活用され、より良い復旧成果につながるべきです。特に是正対応は部門横断で行われることが多いため、検出結果がサイロ化されてはなりません。

過度な手作業に依存して価値が決まる

過剰なチューニングや解釈、あるいは顧客側でのプロセス設計を必要とする製品は、継続的な運用コストと複雑性を増大させる可能性があります。

ベンダー比較表

本表を用いて、有効なDSPM戦略に必要な主要機能についてベンダーを横並びで比較できます。各項目を確認する際は、機能の有無だけでなく、実運用における提供品質にも着目してください*。

ベンダー比較の一貫性と客観性を高めるため、各機能はシンプルな0〜5のスコアリングモデルで評価できます。このアプローチにより、単なるチェックリスト比較を超えて、各機能の相対的な強度、成熟度、実用性を評価できます。スコアが高いほど、その機能が単に存在するだけでなく、エンタープライズ用途に適し、運用効率に優れ、大規模環境で価値を発揮することが実証されていることを意味します。

スコア	定義
5	完全に提供され、高度に自動化され、スケーラブルで統合性にも優れたベストインクラスの機能
4	十分に確立された機能を備え、軽微なギャップのみが残る強力な機能
3	コア要件は満たすものの、深さ・スケール・使いやすさのいずれかに制約がある標準的な機能
2	明確なギャップや手動作業を伴う、または適用範囲が限定的な基本的／部分的な対応
1	最小限の機能、初期段階の実装、または大きな制約のある対応
0	未対応、または有効な根拠が示されていない

カテゴリー	ベンダー1	ベンダー2	ベンダー3	注記
迅速かつエージェントレスな導入を実現するクラウドネイティブアーキテクチャ				
大規模かつ高速な継続的データディスカバリー				
AIを活用したデータ分類				
データコンテキストの把握				
規制要件に紐付いたリスク管理				
柔軟なアクセス制御と適用				
リアルタイムのデータ検知と対応				
コンテキストに基づくアラート				
統合された是正ワークフロー				
データ保護プラットフォームとのシームレスな連携				
合計				

*スコアはロードマップではなく、現時点で一般提供されている機能に基づいて評価してください。各スコアは、製品デモ、顧客リファレンス、ドキュメント、導入要件、統合レベルの検証を通じて裏付ける必要があります。

結論

DSPMソリューションの選定は、単なるツール選びではありません。その重要性は非常に高いものです。データは急速に増加・分散しており、手動対応やレガシー技術ではもはや追随できません。適切なDSPMソリューションは、状況の可視化を促進し、チームの優先順位を明確にし、リスクを低減するとともに、データセキュリティとサイバーレジリエンスの双方を強化します。このソリューションは、AIモデル、システム、エージェントを支えるデータの保護に寄与し、長期的に大きな価値をもたらします。

当社のDSPMソリューションの詳細と、データおよびAIのリスクポスチャ最適化についてご確認ください。または今すぐお問い合わせください。

© 2026 Cohesity, Inc. All rights reserved.

Cohesity、Cohesityロゴ、およびその他の Cohesityマークは、米国および/または国際的におけるCohesity, Inc.またはその関連会社の商標です。その他の会社名、製品名は各社の登録商標または商標です。本資料は、(a) Cohesityと弊社の事業および製品に関する情報を提供することを目的としています。(b) 本資料が作成された時点では、真実かつ正確であると考えられていますが、予告なく変更されることがあります。(c) 本資料は、"現状有姿"で提供されます。Cohesityは、いかなる種類の明示的または黙示的な条件、表明、保証も放棄します。

COHESITY

cohesity.com
1-855-926-4374
2625 Augustine Drive, Santa Clara, CA 95054

4500066-001-EN 5-2026