proofpoint.

ソリューション概要

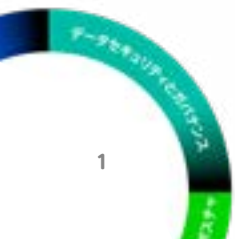
Proofpoint DSPM (Data Security Posture Management) とSnowflakeの連携

成長するData Platform as a Service 環境を保護

主なメリット

- データを広範囲に可視化
- 最低限の権限を適用
- 攻撃対象領域の縮小
- 継続的なコンプライアンス

このソリューションは、人に起因する4つの主要リスクを低減する、プルーフポイントのHuman-Centric Security統合型プラットフォームの一機能です。



Snowflakeは、組織がビッグデータのワークロードを管理する仕組みを変革しました。これにより、大量のデータをよりコスト効率の高い方法で収集、保存、分析できるようになりました。しかし、セキュリティチームやデータチームにとって、データの移動、分類、アクセスを管理しなければならないといった課題も生まれています。これらの課題により、侵害のリスクやガバナンスの問題が高まっています。

Proofpoint DSPM (Data Security Posture Management) は、Snowflakeへの投資の価値を最大化します。Proofpoint DSPMは、セキュリティチームやデータチームが、組織のユーザーに必要なデータを提供する仕組みを簡素化します。急速なデータ成長、データ分類の複雑さ、過度なアクセス権限といった問題を解決します。不十分なリスク管理ツールでは不可能な、継続的なコンプライアンスとガバナンスも確保します。

Proofpoint DSPMは、主要機能に加え、Snowflake AI Data Cloudとシームレスに統合するため、Snowflake Horizonのセキュリティやコンプライアンス機能が利用できます。プルーフポイントを使用すれば、Snowflake環境のコントロールを向上させることができます。Snowflakeテクノロジーやaiといった高度な機能を迅速に導入できます。

広範囲での継続的なアクセスガバナンスとデータ分類の必要性

Snowflakeは柔軟性と拡張性に優れています。しかし、これらのメリットにより、データ移動の増加、複雑なアクセス構造、広範なデータ共有も生じます。結果として、セキュリティチームやデータチームは以下のようなさまざまな課題に直面する可能性があります。

アクセス付与とリスク回避の間で生じるコンフリクト — データチームは、知見を得るために、組織ユーザーが大量のデータセットにアクセスできるようにすることを目指す一方で、セキュリティチームは、ユーザーが、表示と使用が許可されたデータのみへのアクセスに制限する必要があります。

データ分類が不可能 — 構造化されていないデータの急増により、継続的な分類が困難であるといった課題が生じます。セキュリティチームにとって、アクセス制御を適用し、貴重なデータや機密データへのアクセスを試みようとするユーザーを監視するのは簡単なことではありません。

隠れた貴重なデータまたは機密データ — JSON形式のBLOB（Binary Large Object）やAI生成の結果といった、構造化されていないデータにより、貴重なデータや機密データの場所がわかりにくくなっています。そのため、データのアクセスや制御は複雑になります。

Proofpoint DSPM特有の機能

Snowflake環境では、データの移動、分類、アクセスを管理するのが難しいことから、データ侵害のリスクやガバナンス問題も高まります。Proofpoint DSPMは、特別な機能によりこうした課題に対処します。

継続的な検知と高精度の分類 — 重要データを常に完全に可視化します。Proofpoint DSPMのシングルパス スキャナは、継続的にデータを迅速に検知し、高精度で分類します。設定または手動の調整は不要です。

アクセスガバナンスに対応

- 可視化とコントロール

特別な機能

- データコンテキスト
- データアクセスガバナンス
- データ コンプライアンス

アクセスガバナンス — 動的かつ詳細なグラフを用いて、従業員やリソースがどのようにデータにアクセスしているかを確認できます。特定のデータストアにアクセスした人を特定し、権限が付与されているかを判断します。アクティブでない、構成ミスがある、または権限が過度に付与されているユーザーを特定します。ユーザーが必要なデータにのみアクセスできるようにします。

認証情報管理 — 貴重なデータや機密データにアクセスできるが、マルチファクタ認証といった必要なセキュリティ対策が十分でないユーザーを特定します。こうしたユーザーに厳格な認証ポリシーを適用します。

リスク管理 — 侵害または情報漏えいを招きうる攻撃パスを表示します。データの価値と攻撃の成功確率に基づいてリスクの順位付けを行うグラフをリアルタイムで表示します。セキュリティ チームやデータチームが、潜在的な情報漏えいの相対的な影響を評価する上で役立つランキングと共に、データの金銭的価値を示します。攻撃対象領域を縮小し、使用されていないデータを特定することで、ストレージコストを節約します。データダウンロードの想定外の増加や通常とは異なる場所からのアクセスなど、異常なアクティビティを継続的に監視します。これらの知見を用いてリスクの高い問題により迅速に対処します。

データコンプライアンス — ISO 27001、SOC 2、PCI-DSS、NIST CSF 2.0、Snowflake CIS Benchmarkなど、厳格なコンプライアンス プロトコルをサポートする高度なツールで、規制上の課題の一歩先を行き、リスクを低減します。

実装済みスキャン アーキテクチャ — 常に安心できるデータセキュリティ。Snowflakeネイティブアプリとして使用できるProofpoint DSPMは、組織の環境内でスキャナを使用します。これにより、データは組織のセキュアな境界から外れることはありません。

Snowflakeへの投資価値を最大化

Proofpoint DSPMにより、データチームやセキュリティチームのワークフローを最適化することで、Snowflakeへの投資の価値を最大化することができます。

Snowflakeテクノロジーを活用 — DSPMにより、組織内のさまざまなユーザーにとってデータの使用はよりセキュアになります。これにより、Snowflakeの顧客は、AI機能を含め、Snowflakeテクノロジー スタックをさらに活用できます。

不明なポイントを減らす — DSPMは、ユーザーに適切なレベルのアクセス権を付与するプロセスを効率化することで、データチームとセキュリティチームにおける摩擦を排除します。これによりデータはアクセスしやすく、セキュアに維持されます。

ゼロトラストとコンプライアンス要件に対応したコンテキストを提供 — DSPMは、貴重なデータや機密データを高精度で分類し、ユーザーアクセスを効果的に分類することで、ゼロトラストやその他のセキュリティフレームワークの適用をサポートします。

proofpoint.

Proofpoint, Inc.は、サイバーセキュリティのグローバル リーディング カンパニーです。組織の最大の資産でもあり、同時に最大のリスクともなりえる「人」を守ることに焦点をあてています。プルーフポイントは、クラウドベースの統合ソリューションによって、世界中の企業が標的型攻撃などのサイバー攻撃からデータを守り、そしてそれぞれのユーザーがサイバー攻撃に対してさらに強力な対処能力を持てるよう支援しています。また、Fortune 100の 85% の企業などさまざまな規模の企業が、プルーフポイントのソリューションを利用しており、メールやクラウド、ソーシャルメディア、Web関連のセキュリティのリスクおよびコンプライアンスのリスクを低減するよう支援しています。詳細は www.proofpoint.com/jp にてご確認ください。

プルーフポイントとつながる：LinkedIn

プルーフポイント プラットフォームの詳細はこちら