Oracle Data Safe

クラウドのデータを盗難や誤用から守ることは、クラウド・サービスのすべてのコンシューマにとって一番の関心事です。オラクルの目標は、お客様のビジネスに効果的で管理が容易なセキュリティを備えたクラウド・インフラストラクチャ・サービスおよびクラウド・プラットフォーム・サービスを提供し、お客様がミッションクリティカルなワークロードを実行して自信を持ってデータを保存できるようになることです。その信頼の確立に、Oracle **Data Safe** が非常に役に立ちます。Oracle Data Safe は、クラウドに保存しているデータの日々のセキュリティ管理に必要な機能を提供します。

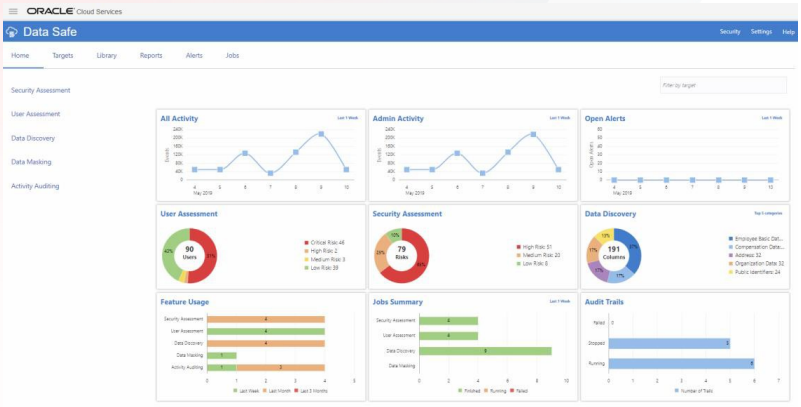
おもな機能

- 機密データの検出と分類
- システム内に含まれる機密データの種類と量の定量化
- 機密データをマスキングすることで、本番以外のデータセットからリスクを排除
- データベース監査情報の収集と安全な保管の自動化
- データベース構成の分析によりセキュリティを改善できる場所を特定
- リスクの高いデータベース・ユーザー・アカウントの特定、およびデータベース内でのそれらのユーザーのアクティビティの簡易検査の実行
- 拡張可能なライブラリを備え、カスタム・データタイプの追加が容易な 125 を超える組込みの機密データ形式
- データベース監査設定の管理の簡略化
- RESTful API による迅速な統合および自動化

はじめに

Oracle Data Safeは、オラクルのDatabase as a Serviceのコンシューマがデータベースのセキュリティをより適切に管理できるよう支援するサービスです。自己保護型のOracle Autonomous Databaseを使用している場合であれ、Exadata Cloud Serviceやより基本的なデータベース・サービスを使用している場合であれ、クラウドのセキュリティは共有責任です。お客様には、クラウドにロードするデータと、ユーザーがそのデータにどのようにアクセスし、そのデータをどのように使用するかに責任があります。Oracle Data Safeを使用すると、単一のセキュリティ・コンソールを用いて、お客様はその責任共有モデルにおいて自身が担う責任を管理できるようになります。そのコンソールからは以下を実行できます。

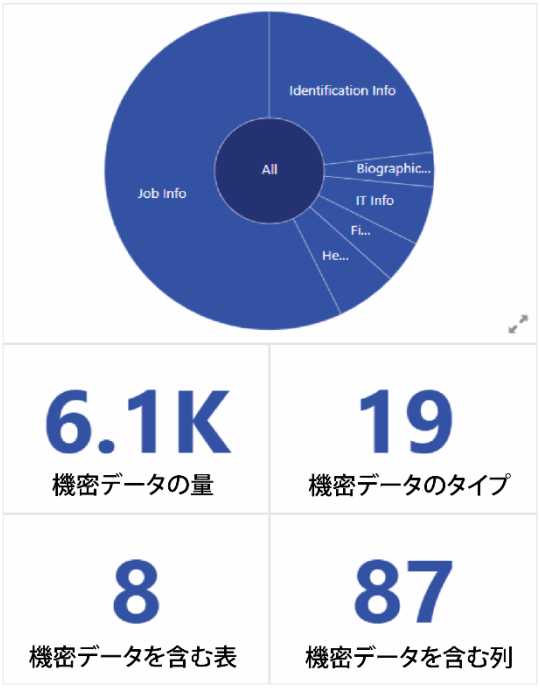
- システム構成を評価してリスク分野を特定
- データベース・ユーザーを調査して、最高レベルのリスクを示すユーザーを特定
- ユーザー・アクティビティを調査して、データへの不適切なアクセスや悪意を含む可能性のあるアクティビティを特定
- データベースをスキャンして、データベース内にある機密データの種類と量を判断
- データ・マスキングを用いて機密データを人為的データまたはスクランブル・データに置き換えることにより、本番以外のデータベースからリスクを排除
- データベース監査情報を収集して分析
- 監査結果に基づいてアラートを生成
- データベース監査の設定を制御



Oracle Data Safeメイン・コンソール

機密データの検出

Oracle Data Safe を使用すると、クラウドのどのデータベースに機密データが含まれているか、その中にどのようなタイプのデータがあるか、そして含まれる機密データの量はどのくらいかを特定できます。また、Data Safe では、125 を超える異なる機密データタイプの事前構築済みライブラリを利用することにより、デフォルトのデータ・モデルを柔軟に拡張してお客様のビジネスに関連した機密データの定義を含めることができます。マウスを数回クリックするだけで、侵害された場合にどのデータベースがもっとも高いリスクの原因となるかを判断し、本番以外のデータベース・コピーでマスキングするべきデータを見つけ、より高いレベルの監査と保護が必要なデータを特定することができます。



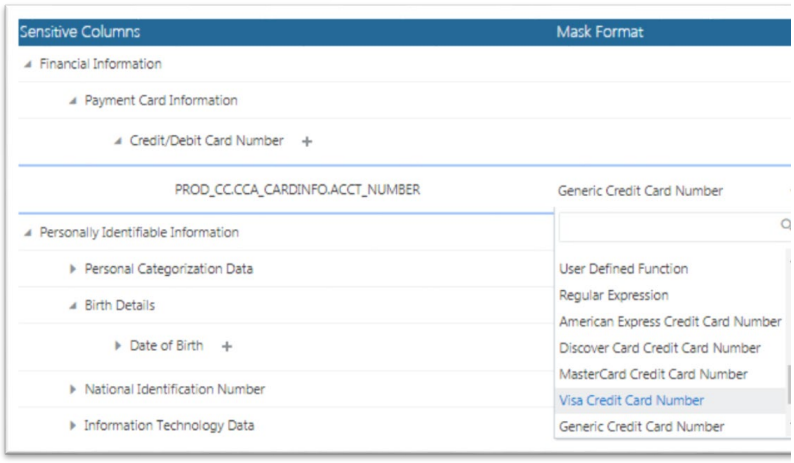
機密データの種類と量の特定

ビジネス上のおもなメリット

- 確実にデータベースをクラウドに移動、可視性の向上、セキュリティの強化
- リスクの高い構成の特定
- システム構成の検証による不要なリスクの排除
- セキュアで一元化されたリポジトリでデータベース監査データを管理して保存
- データベース・アクティビティに関する包括的なレポート
- 個人データを含む機密データの最小化
- リスクの高いデータベース・ユーザーの簡単な検知および監査

機密データのマスキング

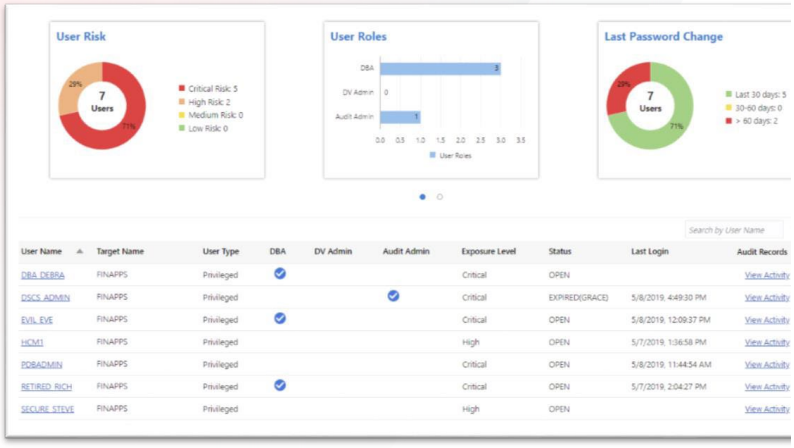
開発やテストの目的で現実的な非本番環境を作成するために、開発者が本番のOracle Databaseをコピーすることがよくあります。ここでの問題は、元の本番環境に内在するセキュリティ・リスクがすべておのおののコピーに含まれるということです。機密データをマスキングすることで、機密データをテストに適した本物に見えるデータと置き換えて、実際の本番データについて関連するセキュリティ・リスクを伴わずにセキュリティ・リスクを排除できます。Oracle Data Safeのデータ・マスキング機能は、機密データを検知すると自然に開始されます。125 を超える機密データ形式のそれぞれに、事前定義されたデフォルトのマスキング形式があります。これは、デフォルトのマスキング・オプションをカスタマイズする必要がない場合は、マウスを数回クリックするだけでデータベースの非本番コピーを完全にマスキングできることを意味します。機密データ形式と同様に、50 以上のデータ・マスキング形式は拡張可能であるため、お客様のデータ・マスキング形式を Data Safe ライブラリに簡単に追加できます。



事前定義された50を超えるデータ・マスキング形式

リスクの高いユーザーの特定と監視

権限が昇格されたユーザーのうち、しばらくの間パスワードを変更していないユーザーや、パスワード・ポリシーが比較的脆弱なユーザーは、データベース侵害の一般的な経路です。Oracle Data Safe では、データベース・ユーザーを調査してどのユーザーが高リスクであるかを特定し、高リスクのユーザーに付与された権限を調査し、それらのユーザーに対して取得された監査データを確認できます。



ユーザー・リスク管理

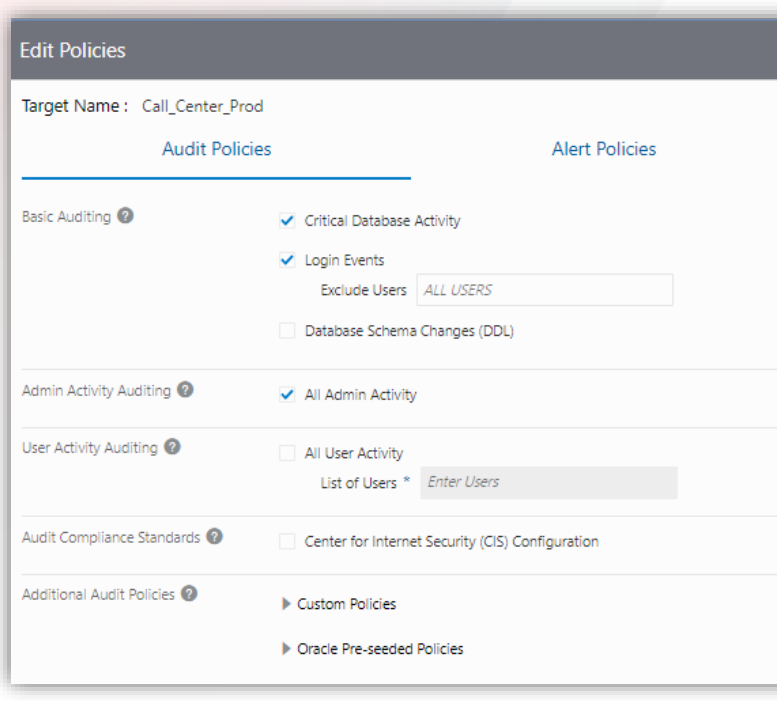
監査設定とデータの一元管理

Oracle Data Safe を使用すると、マウスを数回クリックするだけで適用できるシンプルで理解しやすい監査設定のグループ化によって、データベースの監査設定を簡単に制御できます。Oracle Database Unified Audit のすべての機能と複雑性はまだ使用可能ですが、Data Safe は、大半のサービス・コンシューマが使用できる監査ポリシーによって複雑性を排除します。

また、Data Safe は、ターゲット・データベースから監査データを収集して安全に保管し、事前作成されたレポートを提供することで取得したデータの分析を簡単にします。前に述べたように、監査収集はユーザー評価と統合されているため、個々のユーザーごとのアクティビティを迅速に特定できます。

Oracle Data Safe は、Oracle Database Security スイートの重要な制御手段です。Database Cloud Service にも含まれる Oracle Database Security の関連製品には次のものがあります。

- Oracle Advanced Security
- Oracle Database Vault
- Oracle Label Security
- Oracle Key Vault



Data Safeにより監査ポリシーの管理およびプロビジョニングを簡略化

まとめ

Oracle Data Safe は、共有セキュリティ・モデルでお客様が担当される部分を管理するためのワンストップ・サービスです。Oracle Autonomous Database または Oracle Database Cloud Service に含まれており、Data Safe の機能を利用してクラウド・データベース環境のリスクを特定、定量化、および管理できます。詳しくは、以下を参照してください。
https://www.oracle.com/jp/database/security

CONNECT WITH US

+1.800.ORACLE1 までご連絡いただくか、oracle.com をご覧ください。
北米以外の地域では、oracle.com/contact で最寄りの営業所をご確認いただけます。

Integrated Cloud Applications & Platform Services

ORACLE