ORACLE

Oracle Audit Vault and Database Firewall 20

データシート

Oracle Audit Vault and Database Firewall（Oracle AVDF）は、Oracle Databaseのセキュリティ体制を管理するためにデータベース・アクティビティ監視を超えて機能が拡張されています。AVDFのクラス最高のアクティビティ監視機能は、セキュリティ構成、ユーザー・エンタイトルメント、ストアド・プロシージャ、データベース内のデータの量とタイプの可視化によって強化されています。

AVDFは、クラウドとオンプレミスのどちらにあるかとは関係なく、OracleデータベースとOracle以外のデータベース、オペレーティング・システム、ディレクトリからの監査データを収集します。AVDFは、集約された監査データをセキュアなリポジトリ内で保護します。このリポジトリ内でデータは改ざんから保護されます。監査証跡を生成するほぼすべてのものと連携できるAVDFは、スケーラビリティ、セキュリティ、自動化を備えたエンタープライズレベルの監査プラットフォームです。

データベース・ファイアウォールは、ネットワークベースのSQL検査を実現することで、簡単に異常を特定し、SQLインジェクション攻撃を含む不正なSQLをブロックできるようにします。

AVDFのフリートレベルのビューにより、すべてのシステムに関するインサイトが提供され、IT資産全体の問題を検出できるようになります。強力なレポートとアラートを備えたAVDFは、コンプライアンス監査とインシデント調査をサポートし、データベース・アクティビティとセキュリティ体制の全方位を対象とした最新のスケーラブルなプラットフォームを提供します。

おもな機能

データベース・セキュリティ体制管理（オラクル）

- データベース・セキュリティ構成を評価し、実用的な軽減プランを策定する
- ユーザー、権限、ずれを理解する
- ベースラインを基準にセキュリティ構成のずれを追跡する
- 組織の要件に応じて重大度を低下または変更する
- 機密データの種類、場所、量を検出する
- 評価結果をCIS、DISA STIG、EU-GDPRのセキュリティ・ベンチマークにマップする

データベース監査と監査収集

- 誰がデータにアクセスしたか把握する
- ユーザー・アクティビティ（特権ユーザーを含む）を監査する
- ポリシーとストアド・プロシージャの変更を監査する
- アカウントとエンタイトルメントの変更を監査する
- 機密データへのアクセスを監査する
- データベースとOSのアクティビティ（SUDOを含む）を関連付ける
- Oracle Database 23aiのSQLファイアウォール違反イベント
- 機密表から選択された行の数を追跡する

ORACLE

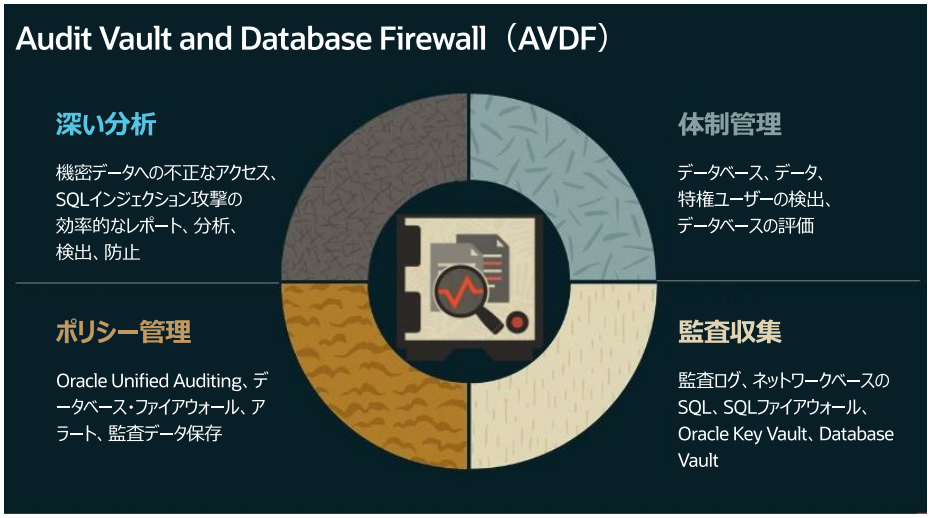

図1：ユーザー・アクティビティの包括的なビュー

評価と検出

Oracle Databaseのセキュリティ体制管理により、機密データが検出され、その保護方法が評価され、誰が機密データにアクセスしたか監視されます。

セキュリティ評価により、すべてのOracleデータベースのセキュリティ構成とセキュリティの調査結果および関連するリスクの簡単なフリート全体のビューが適用されます。詳細な注釈が、リスクをより深く理解し、そのリスクを軽減するための戦略を評価するのに役立ちます。データベース・セキュリティ体制管理を使用すると、セキュリティ構成のずれを検出して追跡し、セキュリティのベースラインを定義し、ベースラインのセキュリティ体制からの逸脱を監視できます。

ユーザー・エンタイトルメントにより、ユーザー、そのロール、権限、アクティビティ、およびこれらのエンタイトルメントが時間の経過とともにどれくらいずれた可能性があるかに関するインサイトを入手できます。

データ検出は、Oracleデータベース内に保存されている機密データの量と種類を理解するのに役立ちます。また、AVDFは、そのデータにアクセスしたユーザーを特定します。

AVDFは、そのデータに対してセキュリティ体制が適切であるかどうかを検証し、ギャップを埋めるための軽減プランを策定するのに役立ちます。たとえば、データへのアクセスを監査するためのポリシーを作成したり、広く知れ渡っているパスや信頼できるパスへのアクセスを制限するデータベース・ファイアウォール・ポリシーを作成したりできます。

Nmapスキャンを実行して、新しいデータベースを検出し、スキャン結果をAVDFにアップロードすることで、AVDFを使用して監視したいデータベースを迅速に特定して登録できます。また、定期的なスキャンを行うと、AVDFが現在監視していないフリート内の新しいデータベースを検出することもできます。この機能を使用すると、データベースが監視対象外にならないよう徹底できます。

- 変更前の値と変更後の値を追跡する（Oracle Database、Microsoft SQL Server、MySQL）
- 監査ポリシーを一元的に管理する（Oracle Database）

SQLトラフィックの監視

- データベース・ファイアウォールを使用して受信SQLを監視して分析する
- AVDFの特許取得済みSQL文法エンジンを使用して脅威を正確に検出する
- SQLインジェクションの試みまたは異常なアクセスを検出してブロックする
- SELECT（Oracle Database）を使用して窃取の試みに対するアラートを生成する
- 複数のDBFWポリシーとアラート・ポリシー全体で使用するグローバル・セット
- すべてのアクティビティ・レポートとGDPRレポート全体で使用するグローバル・セット

強力なレポートとアラート

- セキュリティとコンプライアンスに役立つ設定不要のレポート
- 上位のユーザー・アクティビティに関する監査インサイト
- 調査に役立つカスタマイズ可能なレポートとフィルタリング
- PDF/XLSレポート
- サード・パーティ製レポート・ツール用のオープン・スキーマ
- 強力なアラート・ビルダー
- AVDFシステムの自己監査レポート

サポートされているターゲット・タイプ

- データベース：Oracle、Microsoft SQL Server、MySQL、IBM Db2、PostgreSQL、SAP Sybase、MongoDB（以下のカスタム・コレクタを参照）
- オペレーティング・システム：Linux、Windows、Solaris、AIX
- アプリケーション監査表、XML/JSONデータ、MongoDB、CSV、RESTからデータを収集するためのカスタム・コレクタ
- MariaDB、EnterpriseDB（Postgres）、CSVに監査データを作成するその他のシステムなどのデータベース用のQuckCSVコレクタ

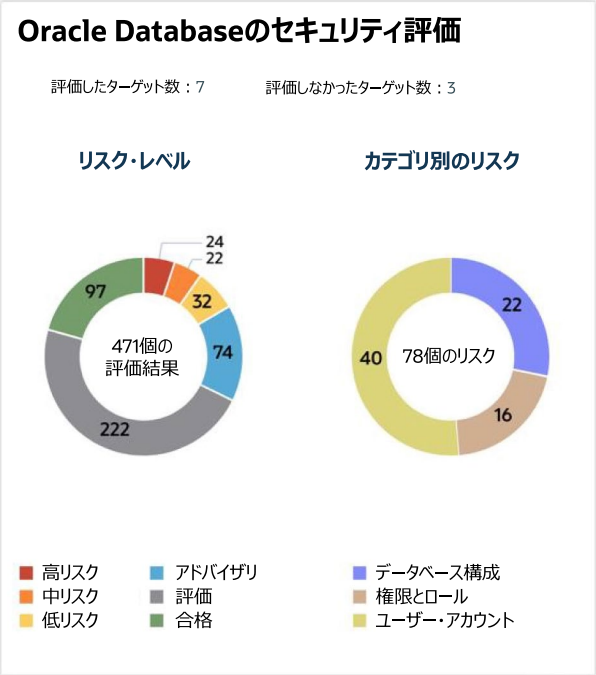

図2：データベース・セキュリティ体制管理

監査と監視

AVDFは、監査データの収集と集約およびもっとも普及しているリレーショナル・データベースのSQL文のネットワークベースの監視によってデータベース・アクティビティを可視化します。AVDFは、データを分析、アラート生成、レポートに使用できるセキュアなリポジトリであるAudit Vaultに監査/アクティビティ・データを集約します。Audit Vaultは、データベース・ユーザーとアプリケーション（特権ユーザーを含む）、重要な変更、ユーザー・アカウント変更、認可変更、ログイン/ログアウト・イベントからアクティビティを取得します。また、AVDFは、SQLのSELECT文から返された行数を監視して潜在的なデータ窃取の試みを特定します。

サポートされている設定不要のソースに加えて、AVDFは、アプリケーション表や監査ファイルからの監査データを収集し、標準の形式にマッピングし、すべてのソース全体でこれらのデータを1つのレポートにまとめます。ソースが何であれ、監査証跡が生成される場合、AVDFがそれを処理できる可能性が高いです。Oracleデータベースの場合、ユーザーは、AVDFから監査ポリシーを一元的に管理して公開できます。

レポートとアラート

AVDFには、ログイン/ログアウト、機密データのアクセスと変更、ストアド・プロシージャの変更、その他多くの設定不要の数十のアクティビティ・レポートを備えた強力な対話型レポート・エンジンが用意されています。これらのレポートをスケジュール、ダウンロード、保存できます。レポート・データをさまざまな条件を使用して簡単にフィルタできるため、インシデント後の調査を促進できます。

監査インサイト・ダッシュボードには、俯瞰図が表示され、1つ以上のデータベース全体にわたる上位のユーザー・アクティビティに関するインサイトが即時提供されます。監査イベント、ネットワーク収集監視イベント、すべての収集イベントの包括的ビューが表示される組合せの3つの異なるインサイト・ビューがあります。

- Microsoft Active Directory
- Oracle Cluster File System（Oracle ACFS）
- オンプレミスとクラウド・ターゲット

エンタープライズ・デプロイメント

- 高スケーラビリティ・アーキテクチャ
- 高可用性とディザスタ・リカバリ
- 自動監査データ・アーカイブ
- Security Technical Implementation Guidelines（STIG）に準拠した監査ポリシー（Oracle Database）
- 職務の分離（SoD）（読取り専用監査者のサポートを含む）
- Active Directory認証
- SAML 2.0統合
- SIEM/Syslog統合
- FIPS 140-2モードのサポート
- コマンドライン・インタフェースを介した自動化
- 自動更新可能エージェント
- OracleデータベースとMicrosoft SQL Serverデータベース用のエージェントレスおよび/またはリモート監査収集
- 定期的更新付きのx86サーバー上のフルスタック・ソフトウェア・アプライアンス
- Oracle Cloudテナンシーに数分でデプロイ可能

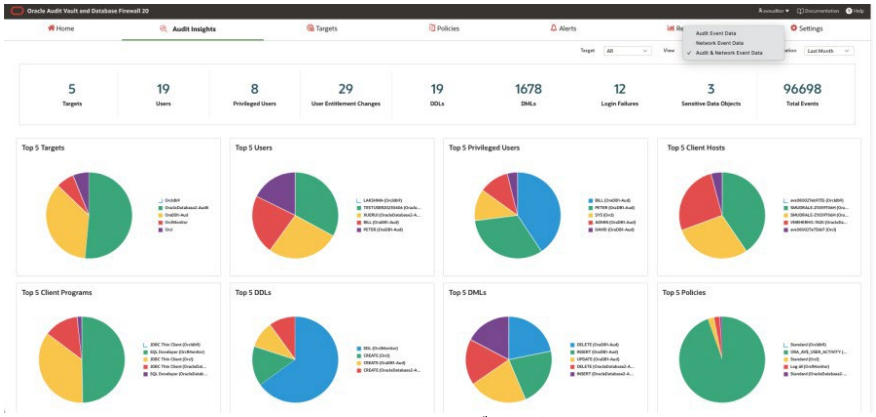

図3：監査インサイト・ダッシュボード

セルフサービス・コンプライアンス・ダッシュボードでは、監査者がGDPR、PCI、GLBA、HIPAA、IRS 1075、SOX、UK DPA向けの事前定義済みのレポートに簡単にアクセスできるため、組織が継続的な監査を効率的に管理しやすくなります。サード・パーティ製レポート・ツールを使用して、Audit Vaultに接続し、さらに分析を行うことができます。

ポリシーベースのアラートにより、疑わしいアクティビティに関する通知が発行されます。アラート・ポリシー・エンジンは柔軟で直観的であるため、誤判定を削減できるターゲットを絞ったポリシーを実現できます。

カスタマイズ可能なしきい値により、機密データが含まれる表が監視され、ポリシーで許可されている数より多い行がSQLクエリーによって返されたときにアラートが生成されます。

AVDFシステムの監査レポートでは、アプリケーション、データベース、オペレーティング・システムの監査からの情報がインフラストラクチャ全体のアクティビティの統合ビューに組み合わされています。これらのレポートは、管理者と監査者のアクティビティを表示して分析するのに役立ち、自己監査に関する規制当局の多くの要件を満たしています。

予防と保護

最後に、データベース上の不正なアクティビティを予防および保護するために、AVDFデータベース・ファイアウォールは、SQLトラフィックがデータベースに到達する前にトラフィックを検査します。データベース・ファイアウォール・ポリシーは、SQLをデータベースに転送できるか、またはSQLをブロックする必要があるかどうかを決定します。データベース・ファイアウォールは、アクティビティを記録し、分析、レポート、アラートのためにイベントをAudit Vaultに転送します。

その他のデータベース・アクティビティ・モニターとは異なり、AVDFは、疑わしいアクティビティを検出するために正規表現を利用することはありません。代わりに、AVDFは、特許取得済みの文法ベースのエンジンを使用してSQL文を解析および評価します。AVDFは、SQLのコンテキストをデータベースが理解するのとほぼ同じ方法で理解できるので、選択、挿入、削除などのデータベース・アクションを特定できます。また、AVDFは、表やビューなどのデータベース・オブジェクトも認識できます。アクティビティ監視に対するこのアプローチにより、誤判定をほぼゼロまで削減し、チームに実践可能なアラートを提供します。

AVDFはSQLを認識できるため、ファイアウォール・ポリシーを使用して通常のアプリケーション動作をプロファイリングできます。アプリケーションが（たとえば、SQLインジェクションの攻撃が原因で）異常なSQLの実行を突然開始した場合、データベース・ファイアウォールはこのアクティビティについてアラートを生成し、これをブロックできます。

ファイアウォール・ポリシーは単なるSQLの検査にとどまりません。このポリシーでは、セッションのコンテキストも考慮されます。接続元はどこか。どのようなプログラムが使用されているか。データベースとオペレーティング・システムのユーザーは誰か。この情報を使用すると、信頼できるデータへのパスを作成するファイアウォール・ポリシーを策定し、攻撃者がアプリケーションの接続情報を知っている場合でも、このパスの外部からのデータへのアクセスの試みをブロックできます。

エンタープライズ・デプロイメント

AVDFのAudit Vault Serverは、何千ものデータベース、オペレーティング・システム、アプリケーションから得た監査データとファイアウォール・イベントを統合できます。AVDFは、アクティブ/スタンバイ・モードでデプロイできるため、可用性が確保されます。Oracle Audit Vault and Database Firewallでは、単一のダッシュボードでクラウド・データベースとオンプレミス・データベースを監視できます。AVDFでは、クラウド・ベンダーまたはその他のサード・パーティ・ベンダーがデータベースを管理している場合でも、これらのデータベース上のアクティビティに対する独立したインサイトが提供されます。

管理者は、AVDFの豊富なコマンドライン・インタフェースを使用して、操作を自動化して、エラーのリスクを軽減し、反復操作や大規模な操作を簡素化できます。

監査データ・ライフサイクル管理は自動化されています。さまざまなソースに対して各種多様なポリシーがサポートされているため、組織要件を満たす保存ポリシーを構成できます。履歴データは自動的にアーカイブされるため、ストレージ・コストを削減しやすくなります。必要に応じて、アーカイブ・データを取得できます。

AVDFは、SAML 2.0統合を介してIDプロバイダ（IDP）（Microsoft Entra ID（MS-EI）、Active Directory Federation Services（ADFS）、Oracle Access Manager（OAM）など）と統合できます。この機能を使用すると、シングル・サインオン（SSO）や多要素認証（MFA）などのメカニズムを使用してIDPによってAVDFコンソール・ユーザーを認証できます。

事前構成済みのソフトウェア・アプライアンスとして提供されるAVDFは、選択したx86 64ビットのハードウェアにインストールできるため、必要なスケールを実現できます。Oracle Cloud Infrastructure（OCI）を使用している場合、Oracle Cloud Marketplaceからのイメージを使用してAVDFを数分でデプロイできます。OCI上のAVDFでは、オンプレミスに加えてOracle Cloudにデプロイされたターゲットを監視できます（Oracle Autonomous Databaseサービスを含む）。

保存されているAVDFリポジトリは、Oracle Transparent Data Encryptionを使用して暗号化されます。移動中の収集データも、収集エージェントからリポジトリまで移動しているため、暗号化されます。AVDFは、Oracle Database Vaultを使用してデータへのアクセスを制限し、AVDFの管理者と監査者の責任を分離します。

AVDFの定期的リリース更新には、組込みオペレーティング・システム、Oracleデータベース、AVDFアプリケーションに対する更新が含まれるため、メンテナンスが簡素化されます。Audit Vaultによって更新エージェントが自動的に更新されるため、貴重な時間が節約され、管理者の関与が解消されます。エージェントレス監査収集により、AVDFの実装が促進され、OracleとMicrosoft SQL Serverのデータベースのフリートの保護を始めやすくなります。

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。

blogs.oracle.com　facebook.com/oracle　twitter.com/oracle