ORACLE AUDIT VAULT AND DATABASE FIREWALL

スケーラブルなデータベース・アクティビティの監視と監査おもな機能

主な機能

- アクティビティの監視およびブロックと、Oracle、MySQL、Microsoft SQL Server、SAP Sybase、IBM DB2 の監査データの統合
- ネットワークでのホワイト・リスト、ブラック・リスト、および例外リストをベースとしたポリシーの実施
- XML および表をベースとした監査データ用のテンプレートが付属した拡張可能な監査コレクション・フレームワーク
- カスタマイズ可能な多数の組込みコンプライアンス・レポートと、事前アラートおよび通知
- PDF および Excel 形式のインタラクティブ・レポート
- 監査者および管理者に対するソースをベースとしたきめ細かな認可
- 通信量の多いデータベースを多数サポートするためのスケーラビリティの高いアーキテクチャ
- 利便性および信頼性のためにあらかじめ構成されているソフトウェア・アプライアンス
- 高可用性サポート

おもな利点

- 防御の最前線として、認可されていないトラフィックを透過的にブロックし、データベース・アクティビティの全体像を提供して、監査データを統合
- パッケージ化されたカスタマイズ可能なレポートにより、すばやくコンプライアンスを達成
- 単一の配備でセキュリティ要件とコンプライアンス要件の両方に適合
- 高精度の SQL 解析、標準装備されたレポート、事前アラートで総所有コストを削減

Oracle Audit Vault and Database Firewall はデータベースを最前線で防御し、データベースやオペレーティング・システム、ディレクトリから得られた監査データを統合します。これは SQL の文法に基づいた精度の高いエンジンで、不正な SQL トラフィックを監視し、データベースに到達する前にブロックします。ネットワークから得られたデータベースのアクティビティに関するデータは、詳しい監査データと結合され、コンプライアンス・レポートの作成やアラート生成が容易になります。Oracle Audit Vault and Database Firewall を使用すると、エンタープライズ・セキュリティ要件に合わせて監査や監視の制御を簡単にカスタマイズできます。

発見的統制と予防的統制

境界ファイアウォールは、外部からの不正アクセスに対してデータセンターを保護するために重要な役割を果たしていますが、データベースへの攻撃は次第に手の込んだものになってきています。たとえば、境界のセキュリティをバイパスし、信頼された中間層を悪用するだけでなく、特権を持つ内部関係者になりすまします。このため、データベース・アクティビティの監視や、データベース内やその周辺のセキュリティ統制が非常に重要になりました。効果的な監視と監査により、ポリシーに違反しようとする行為に対してアラートが発せられ、ブロックが行われます。同時に、コンプライアンスのために包括的なレポートが作成されます。

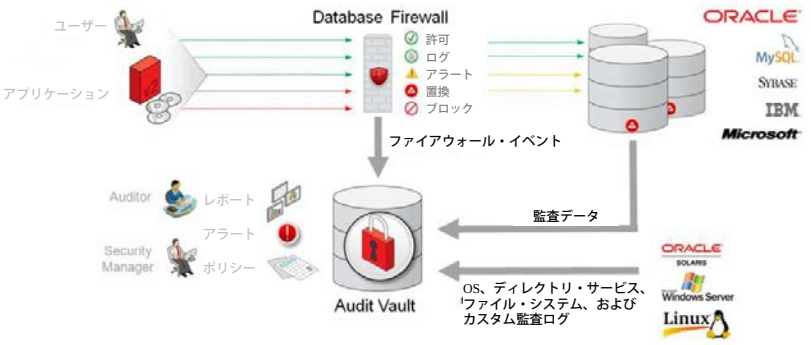

図 1：Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall は、データベース・アクティビティの監視イベントと監査ログを統合します。ポリシーは、アプリケーションに予想どおりの動作を行わせ、SQL インジェクション、アプリケーション・バイパスなどの悪意のあるアクティビティがデータベースに到達することを阻止しながら、データベース内で特権ユーザーやその他のアクティビティを監視し、監査します。また、Oracle Audit Vault and Database Firewall は、Microsoft Active Directory や Microsoft Windows、Oracle Solaris、Oracle Linux、Oracle ASM Cluster File System から得た監査データを統合することもできます。プラグイン・アーキテクチャは、アプリケーション表などのソースから得たカスタム監査データを統合します。

アクティビティの監視とブロックのための Database Firewall

Oracle Database Firewall は、洗練された次世代 SQL 文法解析エンジンを提供します。このエンジンはデータベースに入ってくる SQL 文を検査し、この SQL への対応（許可、ログ、アラート、置換、またはブロック）を高い精度で決定します。Oracle Database Firewall はホワイト・リスト、ブラック・リスト、例外リストに基づくポリシーをサポートしています。ホワイト・リストは、データベース・ファイアウォールを通過すると想定されている、承認済みの SQL 文を単純にまとめただけのものです。このリストは、時間をかけて学習させることも、テスト環境で開発することもできます。ブラック・リストには、そのデータベースには許可されない具体的なユーザーや IP アドレス、特定のタイプの SQL 文がまとめられています。例外リストに基づくポリシーは、ホワイト・リストやブラック・リストのポリシーより優先されるため、これを使用するとさらに柔軟な配備が可能になります。ポリシーは、SQL のカテゴリ、時間帯、アプリケーション、ユーザー、IP アドレスなどの属性に基づいて適用できます。この柔軟性と高精度の SQL 文法解析のおかげで、組織は誤認アラートを最小限に抑えて、重要なデータだけを集められるようになります。また、Database Firewall イベントは Audit Vault Server のログに記録されるので、監査データとともに、ネットワークで観察された情報までレポートに記載されるようになります。

企業の監査データ統合とライフ・サイクル管理

ネイティブの監査データからは、データベース・アクティビティの全体像だけでなく、SQL 文が直接実行されたか、動的 SQL を通じて行われたか、ストアド・プロシージャ経由で実行されたかに関係なく、すべての実行コンテキストが提供されます。データベース、オペレーティング・システム、ディレクトリから得られた監査データの統合に加え、Audit Collection プラグインを使用して、アプリケーション表や XML ファイルから監査データを収集し、Audit Vault Server に送信することもできます。データベースから取得された監査データは、Audit Vault Server への移動後、自動的に消去されます。Audit Vault Server は、内部または外部コンプライアンス要件に適合できるようにするために、ソースごとに日、週、または年単位でのデータ保存方針をサポートしています。

カスタマイズ可能できめ細かなレポートやアラート

標準で搭載されている多数のレポートを利用して、SOX、PCI DSS、HIPAA などの規制に適合したレポートを簡単にカスタマイズできます。このレポートは、ネットワーク・イベントと、監視対象のシステムから得られた監査データの両方をまとめたものです。レポートのデータをフィルタして、特定のシステムやイベントをすばやく簡単に分析することができます。Security Manager は、不正アクセスやシステム権限の乱用が試みられたことを示す可能性のあるアクティビティに対して、しきい値に基づいたアラート条件を定義できます。きめ細かな認証を行うことにより、監査者などのユーザーによる特定のソースからの情報へのアクセスを Security Manager が制限できるようになるため、複数の組織で構成される企業全体に単一のリポジトリを配備することができるようになります。

配備の柔軟性とスケーラビリティ

セキュリティ統制は、一部のデータベースではインライン監視とブロックを使用して、一部のデータベースでは監視のみを使用してカスタマイズすることができます。そのときに有効なネットワーク構成で動作させるために、Database Firewall をインライン、帯域外、またはプロキシ・モードで配備することができます。また、リモート・サーバーを監視するために、データベース・サーバーの Audit Vault Agent は、ネットワーク・トラフィックを Database Firewall に転送できます。さらに、ソフト・アプライアンスとして配信された Audit Vault Server は、無数のデータベースから得た監査ログとファイアウォール・イベントを統合することができます。フォルト・トレランスのため、Audit Vault Server と Database Firewall は両方とも、HA モードで構成可能です。

お問い合わせ先

詳しい情報については oracle.com を参照するか、+1.800.ORACLE1 でオラクルの担当者にお問い合わせください。

Oracle is committed to developing practices and products that help protect the environment

Hardware and Software, Engineered to Work Together