ORACLE DATA SHEET

Oracle Audit Vault and Database Firewall

ORACLE
AUDIT VAULT
AND
DATABASE FIREWALL

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・レベルで収集し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。

おもなビジネス上の利点

- アプリケーション・データベースのデータを侵害しようとする試みを検出、ブロックすることで、データのリスクを管理
- ガバナンスと規制政策への準拠にかかる運用費を軽減
- ハイブリッド・データセンターのオンプレミス・システムとクラウド・システムでのシステム使用状況を表示し、これらのシステムのアクティビティを追跡
- 事前に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、コンプライアンスの取組みを素早く実施
- セキュアなアプライアンスのフォーム・ファクタで所有コストを軽減

発見的コントロールと予防的コントロール

境界ファイアウォールが、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る一方で、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。そのため、データベース・アクティビティの監視、データベース内やその周辺のセキュリティ制御が緊急課題になりました。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。

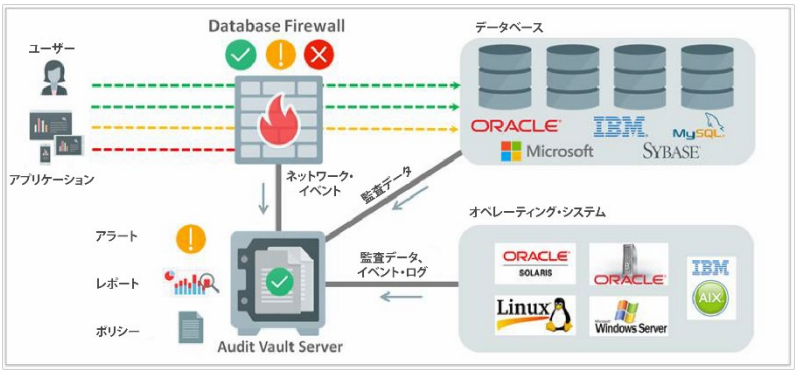

図1：Oracle Audit Vault and Database Firewall

Oracle Audit Vault and Database Firewall はアプリケーション動作を常時監視することで、予期しない動作や不正な動作を認識し、SQL インジェクション、アプリケーション・バイパス、および悪意のあるその他のアクティビティによるデータベースへの侵入を防止します。このソリューションは、データベース内の特権ユーザーとアプリケーション・ユーザーのアクティビティも監視および監査します。また、Oracle Audit Vault and Database Firewall は、Microsoft Active Directory や Microsoft Windows、Oracle Solaris、Oracle Linux、Oracle ASM Cluster File System、IBM AIX から得た監査

おもな機能

- ネットワーク上のアクティビティの監視とブロックを実行し、Oracle、MySQL、Microsoft SQL Server、SAP Sybase、IBM DB2 データベースの監査データを統合
- 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を実施
- オンプレミスおよびクラウドにデプロイされたシステムの監査データを収集
- 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・フレームワークで構築
- カスタマイズ可能な多数の組込みコンプライアンス・レポートを含み、事前アラートおよび通知を配信
- PDF と Excel 形式のインタラクティブ・レポートをサポート
- きめ細かい監査データ・アクセス認可モデルを採用
- 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、事前構成されたセキュアなソフトウェア・アプライアンスとして提供
- 高可用性導入オプションをサポート

データを統合することもできます。プラグイン・アーキテクチャにより、カスタム・エージェントを導入して、アプリケーション表などのソースから得た監査データを統合できます。

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、高度な次世代 SQL 文法解析エンジンを組み込んで、データベースに送られる SQL 文を検査し、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・ベースの各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特定のユーザー、IP アドレス、特定のタイプの文からなる SQL 文が記載されています。例外リストに基づくポリシーは、ホワイト・リストまたはブラック・リストのポリシーをオーバーライドすることで、デプロイメントの柔軟性をさらに高めます。ポリシーは、SQL のカテゴリ、プログラム名、ユーザー、IP アドレスなど、いくつかの問合せの属性に基づいて実施できます。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、監査データに加えて、ネットワークで観察された情報までレポートに記載できます。

企業の監査データ統合とライフ・サイクル管理

Oracle Audit Vault はネイティブの監査データを収集、管理することで、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 を通じて実行されたか、ストアド・プロシージャを介して実行されたかに関係なく、すべての実行コンテキストを提供します。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 にセキュア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、自動的に消去されるので、システム上の領域が解放されます。Audit Vault Server のリポジトリは Oracle Database Vault によって暗号化され、保護されるため、監査データのセキュリティと整合性が守られる一方で、Audit Vault の管理の職務が分離されます。Audit Vault 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、ソースごとに月または年単位でのデータ保管ポリシー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。傾向、特定のシステム、またはイベントを詳しく分析する場合、統合したデータを組み合わせてフィルタリングし、対話形式で表示したりPDF や Excel 形式で表示したり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、監査担当者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導入することができるようになります。

導入の柔軟性とスケーラビリティ

柔軟な導入アーキテクチャにより、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、その他のデータベースでは監視のみを使用してセキュリティ管理をカスタマイズすることができます。さまざま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・モードでデプロイすることができます。または、データベース・サーバーにインストールされたホスト・モニターにより、ネットワーク・トラフィックをリモート・データベース・ファイアウォールに転送できます。さらに、事前構成済みのソフトウェア・アプライアンスとして配信された単一の 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 は両方とも高可用性モードで構成可能です。

お問い合わせ

Oracle Audit Vault and Database Firewall について、詳しくは 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。

CONNECT WITH US

blogs.oracle.com/oracle

facebook.com/oracle

twitter.com/oracle

oracle.com

Integrated Cloud Applications & Platform Services