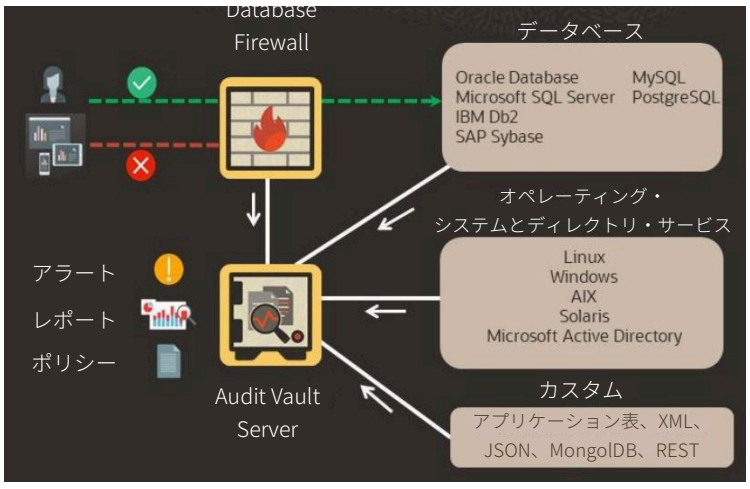
ORACLE

# Oracle Audit Vault and Database Firewall 20

Oracle Audit Vault and Database Firewall（Oracle AVDF）は、Oracleデータベース、Oracle以外のデータベース、オペレーティング・システム、ディレクトリのアクティビティ監査データを統合し、セキュリティとコンプライアンスに関するレポートを作成します。Database FirewallはSQL文法に基づく精度の高いエンジンを通して、SQLトラフィックを監視し、不正なSQLをブロックします。多機能な最新UIが搭載された、拡張可能な監査プラットフォームであるOracle Audit Vault and Database Firewall 20は、エンタープライズレベルのスケーリング、セキュリティ、自動化を備えた、最初の防衛ラインとして機能します。




## データベース・アクティビティの監査と監査データの収集

Audit Vaultは、データベースのユーザーとアプリケーション（高度な管理権限が付与されているものを含む）から、監査データやアクティビティ・データを収集します。データベース全体を対象として、重要度の高い変更、ユーザー・アカウントの変更、認可の変更、ログイン/ログアウトのイベントについて、監査データを収集します。

設定不要でサポートされるソースに加えて、アプリケーション表やファイルからも監査データを収集し、標準の形式にマッピングし、すべてのソースからのデータを1つのレポートにまとめます。

### ビジネス上のおもな利点

- 企業のデータベース全体でデータベースのアクティビティを監査し、監視することで、セキュリティのリスクを低減させる
- 不正なSQLトラフィックがデータベースに到達しないようにブロックする
- 設定不要で監査レポートやアクティビティ・レポートが作成されるため、コンプライアンスやセキュリティの調査に役立つ
- エンタープライズレベルのスケーリング、セキュリティ、自動化、拡張性を備えている

### おもな機能

**データベース監査と監査収集**

- 特権ユーザーのアクティビティの監査
- 構成変更の監査
- ユーザー・アカウント管理の監査
- セキュリティ変更の監査
- ログオン/ログオフ・イベントの監査
- 機密データへのアクセスの監査
- 前後の値も含めた、ストアド・プロシージャおよびエンタイトルメントの変更の監査（Oracleが対象）
- シード済みポリシーの作成（Oracleが対象）
- OSのアクティビティとの関連付け

**SQLトラフィックの監視**

- 複数の段階があるデータベース・ファイアウォールで、受信SQLを分析する
- SQL文法エンジンを使用して、脅威を正確に検出し、記録する
- データベース・トラフィックを監視する
- SQLインジェクション攻撃を防ぐ

Oracleデータベースの場合は、前後の値と、ユーザー・エンタイトルメントおよびストアド・プロシージャへの変更も取得します。シード済みの監査ポリシーがサポートされているため、監査のベスト・プラクティスを実践しやすくなっています。

## データベース・ファイアウォールによるSQLトラフィックの監視

データベース・ファイアウォールは複数の段階があるファイアウォールで、データベースに入ってくるSQLトラフィックを検査し、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。SQLトラフィックは、IPアドレス、データベース/OSのユーザー、プログラム名、SQL文のカテゴリ（DDL、DML）、およびアクセスされているデータベース表のチェックなどの、複数の段階を通過します。データベース・ファイアウォールは、拒否リストにあるSQLと許可リストにないSQLの両方について、ブロックしたりアラートを出したりすることで、SQLインジェクション攻撃を防止します。SQL文法エンジンによって、SQL文に定義されたファイアウォール・ポリシーが、該当のSQL文にとって適切なものとなり、強力な効果を持つポリシーを作成しやすくなります。

Database Firewallのイベントは、Audit Vault Serverに保存され、監査データと統合されて、ユーザーはすべてのアクティビティを統一された画面で見ることができます。

## 強力なレポート機能とアラート機能

Audit Vaultによって、データベース構成、セキュリティ、ユーザー・エンタイトルメントに加えられた変更について、設定不要で複数のレポートを作成できます。また、ログイン/ログアウト、機密データへのアクセスと変更、ストアド・プロシージャへの変更などに関するレポートも作成できます。レポート・データは、調査のために簡単にフィルタリングしたり検索したりできます。

GDPR、PCI、GLBA、HIPAA、IRS 1075、SOX、UK DPA向けのコンプライアンス・レポートによって、ユーザーは監査者向けに必要なレポートを簡単に準備できます。サード・パーティのレポート作成ツールをAudit Vaultスキーマに接続して、さらに分析することができます。

Audit Vaultは、ユーザーが指定したイベントが発生すると、アラートを発します。たとえば、複数回のログイン失敗、無許可のユーザーからの機密データを含む表へのアクセス、データのエクスポート操作などです。

## エンタープライズでのデプロイメント

設定済みのソフトウェア・アプライアンスとして提供されるAudit Vault and Database Firewallは、任意のx86ハードウェアにインストール可能で、ユーザーが必要とするスケーリングを提供します。Oracle AVDFの定期的なリリース更新には、組込みのオペレーティング・システム、Oracleデータベース、AVDFアプリケーション自体への更新が含まれ、メンテナンスが簡便化されています。さらに、Audit Vaultは自動的に、監査データの収集に使われているエージェントを更新し、管理者の介入を必要としません。ユーザーは機能豊富なコマンドライン・インタフェースを使用して、運用を自動化できます。

Audit Vault Serverは、多数のデータベースおよびオペレーティング・システムからの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。アクティブ・モードとスタンバイ・モードでデプロイできるため、可用性が確保されます。ユーザーはデータ・アーカイブのポリシーを構成して、履歴データを低コストのストレージに自動でアーカイブして、必要に応じて取り出せます。

構成の強化に加えて、Oracle AVDFは透過的データ暗号化を使用して、収集したデータを暗号化し、ネットワーク・トラフィックを暗号化し、Database Vaultを使用してデータへのアクセスを制限し、管理者と監査者の責任を分離します。

Oracle Audit Vault and Database Firewall 20は、クラウドとオンプレミスの両方のデータベースを、1つのダッシュボードでサポートするため、ユーザーはデータベースのアクティビティに関する独自の分析情報を得ることができ、それはクラウド・ベンダーに管理されているデータベースにも当てはまります。

### 強力なレポート機能とアラート機能

- 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
- カスタマイズ可能なレポート
- 分かりやすい図
- 調査に役立つ簡単なフィルタリング
- オープン・スキーマによるサード・パーティのレポート作成ツールとの統合
- 強力なカスタム・アラートの作成機能

### エンタープライズでのデプロイメント

- 非常にスケーラブルなアーキテクチャ
- x86ハードウェアにデプロイできるフルスタックのソフトウェア・アプライアンス
- 自動更新可能なエージェント
- 監査データのアーカイブ/リストア
- 職務分離（SoD）
- Active Directory認証
- SIEM/Syslogの統合
- オンプレミスとクラウドに対応

### サポートされるターゲットの種類

- データベース：Oracle、Microsoft SQL Server、MySQL、IBM Db2、PostgreSQL、SAP Sybase
- 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、RESTからのデータを収集するためのカスタム・コレクタ
- Microsoft Active Directory
- Oracle ASM Cluster File System（Oracle ACFS）

### 関連製品

- Oracle Advanced Security
- Oracle Key Vault
- Oracle Database Vault
- Oracle Label Security
- Oracle Data Masking and Subsetting
- Oracle Database Security Assessment Tool

## オラクルの情報を発信しています

+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