ORACLE DATA SHEET

Oracle Database Vault

Oracle Database 18c

18c ORACLE Database

Oracle Database Vault は強力なセキュリティ制御機能を提供することで、アプリケーション・データを不正アクセスから保護し、データベース管理者とデータ所有者間の職務を分離してプライバシ要件や規制要件に対応します。制御機能によって特権アカウントによるアプリケーション・データへのアクセスをブロックするとともに、認可された信頼パスでデータベース内部での機密情報の操作を制御できます。また、使用される権限とロールの自動分析により、既存のアプリケーションのセキュリティを強化できます。さらに、Oracle Database Vault によって既存のデータベース環境を透過的に保護することで、コストと時間のかかるアプリケーション変更が不要になります。

おもな機能と利点

- 特権ユーザーと DBA によるデータベース内の機密データへのアクセスをブロックするための予防的制御を実装しています。
- データベース内部での操作を制御することで、潜在的な脅威による構成の不正な変更を防止して、監査不適合を回避できます。
- メンテナンス中やサイバー攻撃の発生時に機密性の高いアプリケーション・オブジェクトを不正アクセスから保護します。
- 権限分析により、使用される権限と未使用の権限または使用されるロールと未使用のロールを識別して、攻撃の対象となる範囲を狭めます。
- シミュレーション・モードを使ってカスタム・アプリケーションとパッケージ・アプリケーションをテストすることで、セキュリティ制御を迅速に検証します。
- エンタープライズ・アプリケーション（Oracle Fusion Applications、Oracle E-Business Suite、Oracle PeopleSoft、Oracle Siebel、SAP など）に関するアプリケーションごとの保護ポリシーにより、時間を節約し環境を保護します。

特権アカウントの制御

特権データベース・アカウントは、機密データにアクセスするためにもっとも一般に使用されるルートの 1 つです。この広範な無制限のアクセスは、データベースのメンテナンスを容易にしますが、大量のデータにアクセスするための攻撃の糸口にもなります。アプリケーション・スキーマ、テーブル、およびストアド・プロシージャについて定義された Oracle Database Vault のレルムの制御機能により、悪意のあるユーザーが特権アカウントを利用して機密データにアクセスするのを防止できます。さまざまな標準ファクタ（IP アドレス、認証方式、プログラム名など）を使用して、盗まれたパスワードによる攻撃を防止する信頼パス認可を簡単に実装できます。

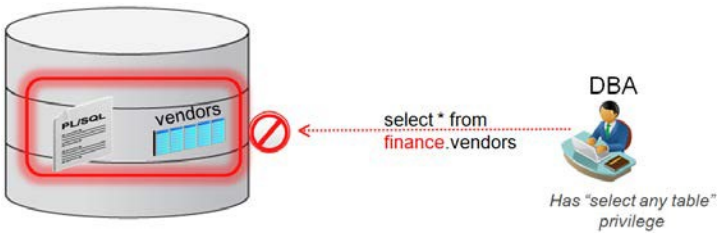

図1：Oracle Database Vaultのレルムによる特権アカウントでのアクセスの防止

データベース構成の制御

監査で指摘されることがもっとも多いものとして、データベース権限の不正変更（DBA ロールや新しいアカウントおよびデータベース・オブジェクトの付与など）が挙げられます。本番環境の不正な変更により、セキュリティが弱まり、ハッカーの侵入経路が開かれ、プライバシおよびコンプライアンス規制に違反する可能性があるため、そのような変更を防止することはセキュリティだけでなくコンプライアンスの点からも重要です。Oracle Database Vault のコマンド・ルールにより、データベース内部での操作（表作成、表切り捨て、ユーザー作成などのコマンドを含む）を制御できます。これらの制御機能により、誤った構成変更を防止するとともに、ハッカーや悪意のあるインサイダーによるアプリケーションの改ざんや変更も防止できます。

ORACLE

関連製品

- Oracle Database 18c の多層防御セキュリティ・ソリューション：
- Oracle Advanced Security
- Oracle Key Vault
- Oracle Data Masking and Subsetting
- Oracle Label Security
- Oracle Audit Vault and Database Firewall

職務の分離

Oracle Database Vault は、セキュリティ管理、アカウント管理、および日常的なデータベース管理アクティビティの 3 つの職務を明確に分離する制御機能を標準で提供します。Oracle Database Vault が提供する職務分離の制御機能はカスタマイズが可能で、リソースが限られている企業では、Oracle Database Vault によって分離される複数の職務を同じ管理者に割り当てることもできます。

ユーザーとアプリケーションの実行時権限分析

権限分析では実行時に実際に使用される権限とロールを認定することでアプリケーションの安全性を向上させています。その後、管理者は、それ以外の未使用ロールと権限を監査して無効化することにより、攻撃の対象となる範囲を狭めるとともに、共有アプリケーション・アカウントとデータベース・ユーザーに対して最小権限モデルを実装することができます。また、管理者に権限分析を適用することで、これらの管理者が職務を果たすために付与されるロールや権限を制限することもできます。

エンタープライズ・アプリケーション保護ポリシー

主要なエンタープライズ・アプリケーション（Oracle Fusion Applications、Oracle E-Business Suite、Oracle PeopleSoft、Oracle Siebel、Oracle Financial Services（i-Flex）、Oracle Primavera、SAP、Finacle from Infosys など）に関しては、Oracle Database Vault のアプリケーション別の保護ポリシーを使用できます。

Database Vault のセキュリティ制御とシミュレーション・モードを使用して、顧客のアプリケーションを迅速に検証することができます。シミュレーション・モードではセキュリティ違反を適用するのではなくキャプチャするので、リグレッション・テストにより、必要なセキュリティの変更をキャプチャできます。シミュレーション・モードでは、既存のセキュリティを低下させることなく、新しい制御を本番環境に素早く導入できます。

管理性

Oracle Database Vault は Oracle Database 18c に組み込まれており、容易に有効にすることができます。Oracle Database Vault の管理は Oracle Enterprise Manager Cloud Control と完全に統合されるため、セキュリティ管理者は、一元化された効率的なインタフェースによって Oracle Database Vault を管理できます。セキュリティの責務をドメイン・セキュリティのエキスパートに任せることができます。

統合環境およびクラウド環境の制御

統合環境やクラウド環境はコストの削減につながるものの、大量の機密アプリケーション・データへの不正アクセスに関するリスクが増大します。ある国に存在するデータがまったく別の国で提供される場合がありますが、それらのデータへのアクセスは、データが帰属する国の規制に基づいて制限される必要があります。Oracle Database Vault の制御機能は、データベース管理者のアプリケーション・データへのアクセスを防止することにより、こうした環境のセキュリティを強化します。さらに、これらの制御機能を使用すると、アプリケーション・バイパスを防止し、アプリケーション層からアプリケーション・データへの信頼できるパスを実装できます。

お問い合わせ

Oracle Database Vault の詳細については、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。