ORACLE

データのセキュリティと保護を最優先に

自動化された、常時オンの、アーキテクチャに組み込まれたセキュリティ

クラウド・セキュリティの現状

データは現代のビジネスにおいてもっとも価値があります。2019年のデータ侵害によって79億件のレコードが流出したことが示すように、サイバー犯罪の最大の目的はデータです。そのため、一部の組織が、データの責任をパブリック・クラウド・プロバイダに委ねることに依然として疑念を抱いていることは驚くに当たりません。

ただし、オンプレミスのデータセンターを自社で運用している組織に固有のリスクがないというわけではありません。権限の乱用、構成ミス、ポリシーに関する知識の欠如は、IT部門における一般的な課題です。これらの課題はすべて、セキュリティ優先を掲げるパブリック・クラウド・プロバイダを利用することで低減できます。実際のところ、考え方は急速に変化しています。『Oracle and KPMG Cloud Threat Report 2020』によれば、現在75 %の組織がパブリック・クラウドはオンプレミス・システムよりもセキュアであると考えており、この割合は前年よりも増加しています。

オラクルは、すべての組織が、内部データや顧客データが侵害されることなく、クラウドの俊敏性、柔軟性、スケーラビリティを活用することを望んでいます。当社が、すべてのクラウド・ソリューションにアーキテクチャ・レベルでセキュリティを焼き付けて、フル・スタックの保護と、設計によって保護されるプラットフォームを実現しているのはそのためです。

75 %

現在、パブリック・クラウドがオンプレミス・システムよりもセキュアであると考える組織の割合

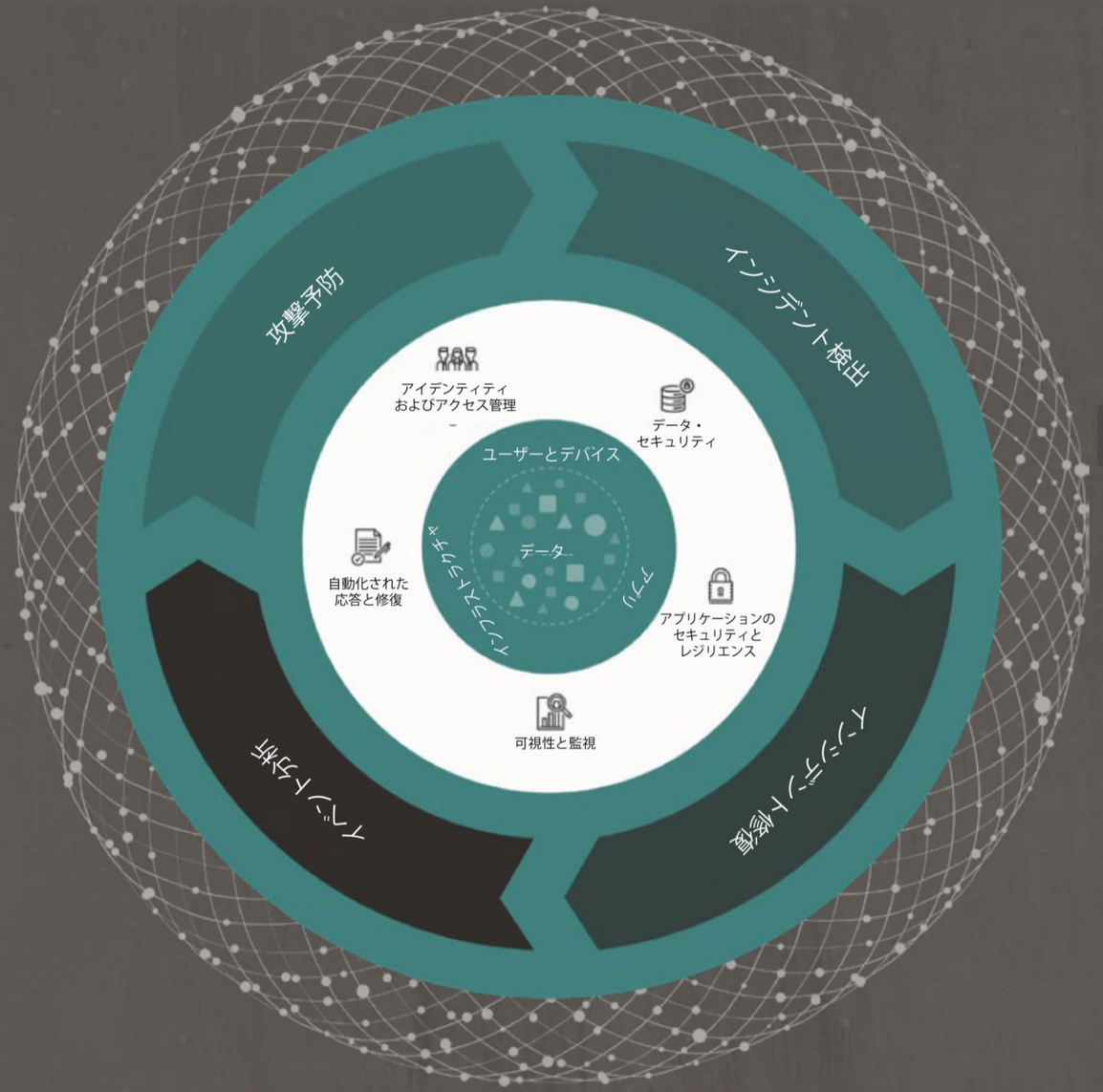
オラクルは、サイバー犯罪に特効薬がないことを認識しています。そのため、オラクルのセキュリティは、次のような主要な脆弱性ポイントを回避します。

- 権限のエスカレーション
- 構成ミス
- 脆弱なクラウド・セキュリティ体制
- パッチが適用されていないシステム
- 暗号化されていないデータ
- 人為的エラー
- 脆弱なWebアプリケーション
- 悪意のある内部関係者による不正行為

フル・スタックの保護

オラクルは階層化されたアプローチを使用して、さまざまなリスクや脅威に対する強力なデータ保護を実現します。中心に据えられているのはお客様のデータです。お客様のデータは、ゼロトラスト・アーキテクチャの設計によって保護されます。このアーキテクチャは、インフラストラクチャ、ユーザー、デバイス、アプリケーションがデータとやり取りする方法をお客様が決定するのに役立ちます。

オラクルは、リスクと信頼性を継続的に評価することで、包括的なセキュリティを提供します。また、当社のセキュリティ・ソリューションによって、フル・スタックの保護がお客様のインフラストラクチャに適用されるため、次に何が起きようとも、お客様はオラクルのセキュリティ・ソリューションが脅威を検出し、エラーや異常を修正し、常にデータを攻撃から保護してくれるという確信の下でビジネスを成長させることができます。



3倍

IT専門家は、自宅の安全よりも企業のセキュリティを心配しています。

『Oracle and KPMG Cloud Threat Report 2020』

オラクルのセキュリティにおける3つの基本原則

すべての組織が自信を持って前進できるよう支援するために、当社は、次に示す3つのセキュリティに関する戦略的な柱で、それぞれのコア・ソリューション領域を支えています。

自動化、常時オン、アーキテクチャへの組込み

Oracle Cloud Infrastructureのセキュリティ

Oracle Cloud Infrastructureは、最新の開発管理機能を提供しながら、ミッション・クリティカルなアプリケーションのニーズを満たすことができるよう、ゼロから構築されています。

Oracle Cloud Infrastructureは、業界初の唯一の自己稼働型のデータベースであるOracle Autonomous Databaseを実行するために構築された唯一のクラウド・プラットフォームです。では、オラクルはどのようにお客様と、お客様のデータ、クラウドベースのワークロード、およびイノベーションの安全性を確保するのでしょうか。

自動化
パッチの適用

Oracle Cloud Infrastructureでは、Oracle Autonomous LinuxとOCI OS Managementによって、OSのセキュリティ・パッチが自動的に適用されます。そのため、コストを削減し、セキュリティと可用性を向上させながら、複雑性と人為的エラーを低減させることができます。

人的介入が不要なため、ITスタッフの生産性、セキュリティ、可用性の向上に役立ちます。また、プロビジョニング、スケーリング、監視が自動化され、他のオンプレミス・プラットフォームやクラウド・プラットフォームと比較して、5年間でTCOが30～50 %削減されます。

常時オン
暗号化

Oracle Cloud Infrastructureは、広く普及している暗号化プログラムを使用して、あらゆる場所のあらゆるデータを常時暗号化します。
お客様のテナント・データについては、保存中のデータと転送中のデータの両方が暗号化されます。

実際、OCI Block VolumesとOCI Object Storageの各サービスでは、256ビット暗号化によるAdvanced Encryption Standard（AES）アルゴリズムを使用した保存データの暗号化がデフォルトで有効化されています。転送データは、Transport Layer Security（TLS）1.2以降を使用して保護されます。

お客様は、オラクルのデータセンター内の物理的なハードウェア・レイヤーからWebレイヤーにまで広がる多層防御戦略と極めてセキュアな運用からも恩恵を受けます。Oracle Cloudで提供される保護と制御の多くは、サード・パーティのクラウドやオンプレミス・ソリューションとも連携されるため、ホストされる場所にかかわらず、最新のエンタープライズ・ワークロードとデータを保護できます。

アーキテクチャへの組込み
お客様の独立性

Oracle Cloud Infrastructureは、オラクルのセキュリティ優先の原則を中心に構築されています。このアーキテクチャは、高度な脅威がもたらすリスクの軽減を促進し、テナント・データを分離して、データのプライバシーとセキュリティを確保します。

つまり、お客様は以下のような利点を享受できます。

- 分離されたネットワーク仮想化により、ハイパーバイザベースの攻撃のリスクが軽減されます
- お客様のテナンシーの分離により、脅威が拡散するリスクが限定されます
- ハードウェアベースの信頼の起点により、各サーバーがクリーンなファームウェアでプロビジョニングされることが保証されます
- ネットワークのセグメント化により、サービスが分離され、厳格なポリシーによってアクセスが制御、監視、実行されることが保証されます

金融サービスにおける Oracle Cloud Infrastructure

セキュリティ優先を掲げるOracle Cloud Infrastructureは、従来型のインフラストラクチャの管理と更新に疲弊している金融サービス企業にとって理想的です。

レガシー・プラットフォームの更新には時間がかかる可能性があり、アップグレード・コストは徐々に増加しています。そのため、新たなイノベーションの提供や、チャレンジャー・バンクや、フィンテック・スタートアップ企業のようなデジタルに精通した競合他社との競争に、貴重なリソースを有効利用できなくなる可能性があります。

インフラストラクチャをパブリック・クラウドに移行することで、企業はインフラストラクチャの複雑性を軽減し、セキュリティを向上できます。同時に、ITスタッフは、確認されたセキュリティ・リスクへの対応やお客様の環境の革新など、より価値の高いタスクに能力を再び集中させることができるようになります。

Oracle Cloud Infrastructureでは、セキュリティに影響されやすいワークロードを、自動化されたセキュリティ監視機能とともに実行できるため、企業は業界の厳格な規制を順守しながら、データの可視性とアプリケーションのセキュリティを向上させ、デジタルに精通した競合他社の先を行くことができます。

Oracle Autonomous Databaseのセキュリティ

Oracle Autonomous Databaseは、パッチ適用、更新、保護、および管理を自動的に行うことで、組織がIT部門のデータベース運用を変革できるよう支援します。Oracle Autonomous Databaseを使用すれば、人為的エラーや予期せぬ停止時間が低減され、より少ないリソースでイノベーションの速度を上げることができます。

Oracle Autonomous Databaseは以下を実現します。

自動化
パッチの適用

Oracle Autonomous Databaseを使用すると、これまで手動で行われていたセキュリティ・タスクが自動化されるため、セキュリティ管理に伴うコストを最大で55 %削減できます。

パッチ適用の自動化などのプロアクティブなセキュリティ自動化によって、一般的な脆弱性やリスクに関するアラートが発行された後にデータ侵害が発生するリスクも軽減できます。

パッチは停止時間なしでデプロイされるため、組織は安全性と生産性を維持しながら、人為的エラーが発生するリスクや管理業務が遂行されないリスクを排除できます。

常時オン
暗号化

Oracle Cloud Infrastructureのデータと同じく、Oracle Autonomous Databaseのデータも、保存中であれ、送信中であれ、常に暗号化されます。

Oracle Autonomous Databaseの各サービスは、業界標準のTransport Layer Security 1.2を使用して送信中のデータを暗号化するように自動的に構成されます。一方、保存中のデータはOracle Transparent Data Encryptionを使用して暗号化されます。

Oracle Transparent Data Encryptionは、GDPR、CCPA、PCIなどのデータ・プライバシー規制の順守を簡素化するのに役立つだけでなく、OSユーザーが権限を乱用して機密データにアクセスできないようにします。
また、データの盗難、データの損失、ストレージやバックアップの不適切な廃棄を防止するのにも役立ちます。

アーキテクチャへの組込み
職務の分離

Oracle Autonomous Databaseにより、データベース・ノードやローカル・ファイル・システムへの直接アクセスが排除されます。一方、サービス管理者とサービス利用者の独立性は、Oracle Database Vaultによって確保されます。

この職務の分離により、管理者が不正行為を行うリスクが軽減され、Oracle Autonomous Databaseに保存されているエンタープライズ・データをOracleサービスの管理者が表示または変更できなくなります。Oracle Database Vault内のセキュリティ制御は、GDPRなどのデータ・プライバシーに関する法律や基準の順守を継続し、ユーザー権限の乱用を防止するのにも役立ちます。

また、職務の分離のおかげで、サイバー犯罪者がセキュリティ制御を無効にしたり、偽のユーザーを作成したり、機密データにアクセスしたりすることがより困難になります。

通信分野での Oracle Autonomous Database

ある一般的な通信事業者は、多くのグローバル顧客に対して、委託されたデータを開示しないという法的拘束力のある義務を負っています。

残念ながら、ある日データ侵害が発生しました。そして、通信事業者のデータベースが最新のセキュリティ要件で更新されていれば、侵害を防止できた可能性があることがすぐに明らかになりました。
何が原因だったのでしょうか。1台のシステムにパッチを適用しなかった人為的エラーです。この人為的エラーによって、サイバー犯罪者は短期的な脆弱性を悪用して、機密性の高い顧客データにアクセスできました。

暗号化とパッチ適用を自動化する自己保護型のデータベースに移行することで、この通信事業者は将来的に人為的エラーが起きる可能性をなくすことができるだけでなく、セキュリティ衛生を向上させ、顧客ベースとの信頼を再構築できます。

Oracle Software as a Serviceのセキュリティ

すべてのOracle SaaSソリューションでは、最新のクラウド・スイートの利点が提供されます。高額で物理的なオンプレミス・ソリューションの更新や管理に伴う注意事項はなく、完全で俊敏性のある、セキュアかつオープンなソリューションが組織全体に提供されます。

また、オラクルのセキュリティ優先のアプローチを組み込んだこれらのソリューションは、全面的な安心感ももたらします。

自動化
対応と修復

Oracle Identity Cloud Service（Oracle IDCS）により、フル・スタック全体で動作の監視が自動化され、多要素認証（MFA）などのセカンダリ認証が提供されます。

Oracle Cloud Access Security Broker Service（Oracle CASB）も動作を分析でき、ユーザーまたはアプリケーションに割り当てられたリスク・レベルに従って機能することができます。疑わしい動作が特定された場合、Oracle CASBは、リスクの高いサービスへのユーザー・アクセスをブロックし、承認されたユーザーに自動的にアラートを送信します。さらに、疑わしいトランザクションについて監査者に通知を自動送信するなど、事前定義されたポリシーに基づいて対応策を講じることができます。

常時オン
監視

オラクルは、次の3つの戦略的テクノロジーを通じて、アプリケーション所有者、監査者、セキュリティ運用チームに対して、完全なSaaSセキュリティ制御を提供します。

- Oracle Identity Cloud Service（Oracle IDCS）
- Oracle Cloud Access Security Broker（Oracle CASB）
- Oracle Risk Management Cloud（Oracle RMC）

これらのテクノロジーを一緒に使用すれば、エンタープライズ・ユーザーは、ユーザーの資格証明とエンタイトルメントがどのように使用されているかを分析できるため、疑わしい動作をより的確に特定し、迅速に対応できるようになります。たとえば、ユーザーの行動を調べ、履歴データを相互参照させて、高度で自動化された監視と対応モデルを作成するといったことも可能です。

アーキテクチャへの組込み
統合されたクラウド・セキュリティ・サービス

すべてのOracle Fusion SaaSアプリケーションには、Oracle Identity Cloud Serviceがデフォルトで内蔵されています。つまり、一貫性のあるIDベースのセキュリティが、エンタープライズ・セキュリティ・ファブリックのあらゆる部分に確実に組み込まれています。

Oracle Cloud Access Security Brokerは、すべてのOracle SaaSアプリケーションのセキュリティ基盤を構成する要素でもあります。Oracle CASBにより、クラウド・スタック全体の可視性を向上できると同時に、自動化された脅威検出、予測分析、セキュリティ構成管理に必要なツールがIT部門に提供されます。

Oracle SaaSユーザーは、Oracle Risk Management Cloudを使って、リスク軽減の制御を向上し、アプリケーションのコンプライアンス基準を有効にできます。

小売業におけるOracle SaaS

あるグローバルなeコマース小売業者は、コア・ビジネスの一環として、顧客向けのアプリを開発し、世界中のユーザーに提供しています。グローバル規模でアプリやサービスの提供を開始する複雑さに対処しなければならない一方で、不正な購入に対処するためのシステムを導入する必要もあります。

Oracle Identity Cloud Service（Oracle IDCS）は、疑わしいトランザクションを自動的に特定することで、このような困難を緩和します。Oracle IDCSは、ジオロケーション・データを使用して、トランザクションが予期しない場所から送信された場合（ユーザーのIPアドレスがアカウントを登録したときの場所と一致しない場合など）にフラグを立てることができます。その後、SMSを使用して2つの要素による認証を行い、トランザクションが有効かどうかを判断します。

小売業者は、疑わしい取引に自動的にフラグを立て、追加のユーザー検証を実行することで、多大なITリソースを投じることなく、収益とブランド・イメージを保護できます。

オラクルのセキュリティが選ばれる理由

Oracle製品は、セキュリティが最初から組み込まれているため、フル・スタックの保護を提供し、
脅威への対応を自動化し、シームレスで常時オンの保護を実現します。

そのためお客様は、データと操作が保護されているという安心感を享受できます。
また、セキュリティが自動化されているため、組織はもっとも重要なこと、
すなわちビジネスの成長へと立ち返ることができます。

Oracle Autonomous Database
は業界初の
自己保護型のデータベースです

詳細を見る

Oracle Cloud Infrastructureは、
アーキテクチャでセキュリティ優先の
アプローチを利用します

詳細を表示する

オラクルは、クラウドの
ミッション・クリティカルなSaaS
アプリケーションを保護します

詳細を見る

ORACLE