クラウド・セキュリティ -基本と基礎

ORACLE

今日、あらゆるものがデジタル化され、クラウドやモバイル、ソーシャル、IoTによってビジネスの手法は変化を続けています。組織によるクラウドへの急速な移行は転換点を過ぎ、その利点は、柔軟性、敏捷性、コスト削減、将来性など明らかです。デジタル・トランスフォーメーションにより、プライベート・クラウド、パブリック・クラウドおよびハイブリッド・クラウド、Software-as-a-Serviceアプリケーションなど、企業における異種クラウドの採用が導入され促進されています。

この避けることができないトレンドは、しかしながら、組織に多くの課題をもたらしました。それは、クラウド・アプリケーションに、一貫した可視性、セキュリティ、コンプライスおよびコントロールが欠けていたことが要因です。個別に述べると、一部のクラウド・プロバイダは、顧客に特定のクラウド・アプリケーション内のセキュリティの定義と実施を許可する制限付きのコントロールを提供しています。しかし、クラウド・ベンダーが提供するセキュリティ手法は、多くの場合それぞれで異なります。加えて、すべてのクラウド・プロバイダのセキュリティ・ポリシー施行は、深刻な欠陥に悩まされています。企業は、インタフェースやワークフローが異なる複数のプラットフォームで個別にセキュリティ・ポリシーを管理し、セキュリティ・コントロールを適用することを求められています。その結果、セキュリティのサイロ化、一貫性のないクラウド・セキュリティ施行および管理費の増大が発生しています。この状況に対応するには、オンプレミスと複数のクラウド環境にわたり拡大する攻撃ポイントのリスクを軽減できる、クラウド横断型のセキュリティ・アプローチが求められます。

ビジネス上の課題

パブリック・クラウドベースのSoftware as a Service (SaaS)は、企業で使用するオフィス用アプリケーション、販売やマーケティングのソフトウェアなど、ビジネス・アプリケーションの一般的なデリバリ・モデルとなっています。結果として、企業グループと従業員、外部のパートナや顧客は、多様なクラウドベースのSaaSアプリケーションのサポートをIT組織に求めます。さらに、大規模に使用されるInfrastructure as a Service (IaaS)やPlatform as a Service (PaaS)ソリューションが存在します。クラウドベースのアプリケーション、プラットフォームおよびインフラストラクチャの需要は、次のビジネス要件から生じています。

- 迅速な導入: 新しいアプリケーションの迅速な導入およびアプリケーション・プロバイダの速やかな変更を求めているビジネス・ユニット。
- 費用便益: 短期間でのコスト効果の高いライセンス供与
- 効果的なコラボレーション: パートナと顧客、サプライヤ、子会社および買収先とのコラボレーションを求めている企業グループ

図1.上の図中の説明に従いSEOデータを盛り込みましょう。

主なセキュリティおよびプライバシの問題

パブリック・クラウド・コンピューティングの出現は比較的最近のパラダイム・シフトですが、セキュリティに関する重要なインサイトは、現在の導入者の経験、および利用可能なパブリック・クラウド・サービスと関連技術で実験を行っているセキュリティの研究者から学ぶことができます。主なセキュリティおよびプライバシ関連の問題の一部を次で説明します。

図2: クラウドの主なセキュリティおよびプライバシの問題

アプリケーションおよびデータのセキュリティ

組織がクラウドを導入する場合、理解する必要がある重要なコンセプトの1つは、クラウドにおけるセキュリティが共同責任であるということです。クラウド・サービス・プロバイダは、サービスが本質的に構成されていることを保証する必要があり、組織(つまりクラウド・コンシューマ)は、組織側においてもアプリケーションおよびデータのセキュリティが必要であることを理解する必要があります。アプリケーション・セキュリティは、一般的に2つの領域を対象とします。

- 導入されている各クラウド・サービスの***構成設定***。これには、クラウド・サービスが安全なデフォルト設定とコンプライアンス準拠のための組織固有の設定の両方を備えていることが含まれます。
- 次のいずれかによる***クラウドの使用***
    - ユーザーによる使用
    - 他のクラウド・アプリケーションとの統合の一部としての使用

データ・セキュリティ・リスクは、次の2つの状態にあるデータの流出です。

- ***保存データ(Data at Rest)***とは、外部のクラウド・プロバイダに格納されているデータを指します。組織は、クラウド・プロバイダの利用に関するリスクを十分に理解し、クラウド・プロバイダが真のデータ管理者として職責を果たしていることを確認する必要があります。データの所有者である組織は、クラウド・プロバイダによってデータが確実に保証されるように積極的に働きかけ、組織のデータのセキュリティを自らも管理できるように適切なセキュリティ・コントロールを利用できるようにする必要があります。
- ***移動中のデータ(Data in Motion)***とは、格納されている状態から別の場所へ移動されるデータを指します。データがクラウド内に格納されるとき、またはデータが個人のコンピュータまたはモバイル・デバイスにダウンロードされるとき、いずれもデータは転送中(*data in transit*)と見なされます。暗号化は、移動中のデータの保護形態の1つです。

アイデンティティおよびアクセス管理

クラウド・アクター間でユーザー認証および認可を理解し定義することは、クラウド・セキュリティの重要な側面です。クラウドベースの情報システムに誰がログインし、どのデータに誰がアクセスしているかを把握することなしに、クラウド・エコシステムは保護できません。

- ***ユーザー認証***は、ユーザーのアイデンティティに対する信頼を確立するプロセスであり、通常、有効なユーザー名と有効なトークン(パスワード、鍵、生体認証)の入力によって、情報システムまたはリソースへのアクセス権を付与することを目的に行われます。認証の保証レベルは、アクセスされるアプリケーションや情報資産の機微性、および関連するリスクに対し適切である必要があります。
- ***認可またはアクセス制御***は、ユーザーにアクセスが許可されているリソースやサービスの決定などのポリシーを施行するプロセスです。通常、認可は認証のコンテキストで発生します。認可ポリシーの施行は、クラウド・システムで非常に重要です。
- ***アイデンティティ・フェデレーション***は、組織とクラウド・プロバイダによる、双方のドメイン間でのデジタル・アイデンティティの信頼と共有を可能にし、クラウド・サービス間でのシングル・サインオンの手段を提供します。クラウド・プロバイダがクラウド・コンシューマのデジタル・アイデンティティから明確に分離されていることを保証し、コンシューマのリソースをクラウド・プロバイダの認証済エンティティから保護する必要があります。

コンプライアンス、ガバナンスおよび信頼

コンプライアンスとは、組織が、制定されている法律、規制、標準および仕様に従って事業を行う義務を指し、企業はこれを順守する必要があります。この要件は、社外または社内のいずれの場合もあり、事業目標、顧客との契約、法律や業界の規制、社内方針およびその他の要因によって推進されます。

パブリック・クラウドへの安全な移行

オラクルは、クラウド・サービスの需要や企業による導入が拡大していることを認識しています。次に示す複数のステップから成るアプローチおよび特性化は、NISTおよび国際標準化機構(ISO)の研究から派生し適応させたものであり、組織のクラウド・セキュリティの課題への対応に使用できます。

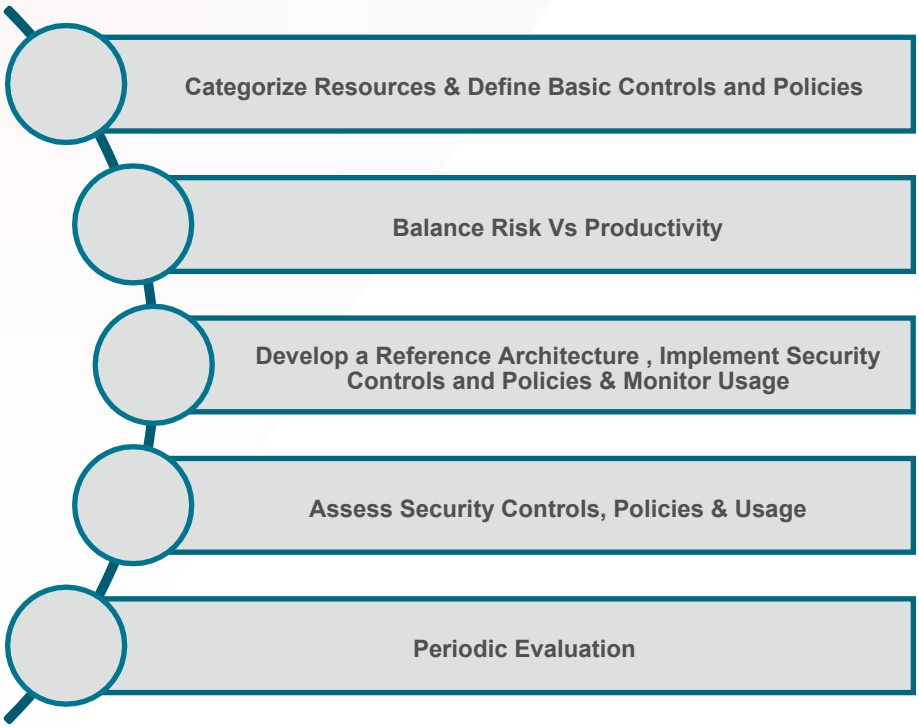

図3.クラウドへの安全な移行ステップ

リソースの分類および基本的なセキュリティ・コントロールとポリシーの定義

このステップの目的は、クラウド・リソースの重要性および機微性を規定し、それらをリスク・レベルと関連付けることです。リスク・レベルは、アクセスの種別、データおよびアプリケーションにアクセスしているユーザーに基づき算出できます。また、アプリケーションのリスク・スコアを、クラウド・アプリケーションの評判などの外的要因に基づき算出することもできます。

セキュリティ・コントロールの選択: セキュリティ・コントロールは、セキュリティ・リスクを阻止、抑制、あるいは逆に対処するための対策措置または予防手段です。これは、最小限必要なセキュリティが実施されるようにクラウド・サービスごとに設定されます。セキュリティ・コントロールは、各クラウド・リソースの分類に基づいて、関連付けられたリスク・レベルにマップされるように選択する必要があります。このセキュリティ・コントロールにより、クラウド・サービスの状態がどの時点においても保護されます。たとえば、AWSインスタンスのセキュリティ・コントロールでは、すべてのS3バケットが暗号化されるようにする必要があります。暗号化がオフの場合、組織のセキュリティは本質的に低下します。

アプリケーションおよびデータのセキュリティ・コントロール

アプリケーション・レベルのセキュリティ・コントロールは、各アプリケーションが組織のセキュリティのニーズや任務に合致しているようにするために必要不可欠です。

たとえば、組織が共同作業のためにOffice 365、IaaSとしてAmazon Web Services (AWS)とOracle Cloud Infrastructure (OCI)、人事管理のためにOracle HCM Cloudを導入している場合、各アプリケーションを適切に構成する必要があります。それぞれが複数のサービスを提供しており、たとえば、IaaSはコンピュート、ネットワーク、ストレージおよびセキュリティ・サービスを、Office 365はExchange、OneDriveなどを提供しています。各分野の専門家に指示し確実かつ適正に構成を実施させることは、難度の高い課題です。加えて、これらすべてはクラウド・アプリケーションであるため、ネットワーク効果の特有の利点があります。つまり、他の組織のベスト・プラクティス・デプロイメントから学べるということです。

クラウドにおいて、暗号化は、保存されているデータおよびストレージと処理フェーズの間にあるデータを保護するための主要手段です。組織は、暗号化で使用される鍵が安全に格納され、適切に管理されるようにする必要があります。

アイデンティティおよびアクセス管理(IAM)コントロール

アイデンティティおよびアクセス管理は、運用中のクラウドの主要なセキュリティ要素であり、通常、組織の多層防御戦略の第1レベルのコントロールとなります。このコントロールは、アイデンティティ情報の機密性、完全性および可用性を保護する必要があり、クラウド利用者の認証のニーズをサポートします。アイデンティティ管理システムは、ユーザーのアイデンティティの可搬性を実現し、内部アクセスおよびテナントやユーザー・アクセスに単一のメカニズムを提供します。フェデレーテッド・アイデンティティ管理システムは、顧客とサードパーティ・アイデンティティ・プロバイダとの相互運用を可能な限り実現します。

個別のIAMコントロールを整備する必要があります。パスワード・ポリシーなどの基本的なコントロール、機微データへのアクセス、および高度な特権操作に対する強力なマルチファクタ認証(MFA)、ユーザーやアプリケーション、使用しているデータのリスク計算が必要になります。

クラウド管理のための認可メカニズムには制限が必要であり、クラウド全体のアクセスは許可されません。このような認可メカニズムは、通常、ユーザーがクラウド・アプリケーションで実行する可能性のあるアクティビティにまでおよび、ポリシーによって管理されます。

ベスト・プラクティスの活用をサポートし、クラウド・サービスごとに数多くのコントロールをすぐに利用できる状態で提供し、発生するあらゆる変更への可視性を提供するソリューションであれば、組織は、安全なクラウド・ポスチャを迅速に実現できます。

リスクと生産性のバランス

組織にとって重要なことは、包括的なクラウド・セキュリティ戦略を持つことです。セキュリティ対策のROIは、ビジネス・ユニットが導入しようとしている新しいクラウド・サービスの価値と同じように簡単に説明できる必要があります。

コントロールが十分で適切であるかどうか、およびコントロールが予測される脅威に対して適切な保護をリスク緩和プランとともに提供しているかを判断してください。簡単に使用、実装および管理できるセキュリティ対策の確立に重点を置けば、セキュリティと生産性のバランスを取ることは可能です。目標は、ユーザーの生産性を強化し、さらにユーザーにリスクについて理解させることです。シンプルさを求めて努力すれば、セキュリティの負担は軽減され、ユーザーはより生産的になることができます。

リスク・シナリオは、専門家と情報セキュリティ・スペシャリストの共同の取組みとして開発される必要があります。セキュリティ・コントロールは、静的な構成として見るのではなく、スケーラブルなデザインとして捉えるべきです。つまり、呼び出されるサービスのインスタンスがどれも同じリスク・ポスチャを示し、脆弱性が検出されたときに、そのデザインを修正するために適切な措置を取ることができるなどです。

リファレンス・アーキテクチャの開発、セキュリティ・コントロールとポリシーの実装および使用状況の監視

この段階では、通常、より広範なアプリケーションおよびセキュリティ・チームが関わり、適切なアプリケーションおよびインタフェースが使用されていることを確認する必要があります。また、サービスが、前のステップで定義されたセキュリティ・コントロールに基づいて構成されていることも確認します。また、組織のニーズに合わせて追加のポリシーを実装することもできます。

この段階でもう1つ重要なステップは、これらのクラウド・サービスの使用状況がポリシーおよびセキュリティのニーズと合致しているかを確認することです。これは、通常、2つのフェーズで提供されます。

- **ユーザー行動分析** - 機械学習(ML)の技術を活用することで、ユーザーのリスクの特定が可能になります。ユーザー行動分析では、複数の要素、つまり一般的な要素(ユーザーが使用しているデバイス、ユーザーの位置など)とクラウド・サービス固有の要素(ユーザーが定期的に消費しているIaaSサービスのインスタンス数など)が考慮されます。
- **不審な行動** - これは、通常、ユーザーの使用パターンに基づきます。たとえば、ログイン失敗の数が多すぎる場合、または1人のユーザーの2回の連続したログインの距離が離れている場合などは不審な行動と判断できます。

当然のことながら、この段階は、適正なリスク・イベントがアプリケーションごとに警告されること、および緩和パスが存在することを確認するために使用するべきです。

セキュリティ・コントロール、ポリシーおよび使用状況のアセスメント

このステップでは、実装されたコントロールの有効性を測り、コントロールが意図したとおりに実装され運用されていることを確認します。一般的に、すべてのコントロールおよびポリシーによって、リスク・イベントが生じます。これらのリスク・イベントは、それらが確実に適切で有益、かつ実践可能であるように監視する必要があります。多くの場合、実装の初期フェーズでは、リスク・イベントがうるさく感じられる可能性があります。使用中のクラウド・セキュリティ・ソリューションでは、結果として発生するリスク・イベントは適切であるように調整されている必要があります。多くの組織は、インシデント管理ソリューションと統合し、リスク・イベントを修正するワークフローを用意しています。

定期的な評価

クラウドの世界のテクノロジは高速に変化しており、ビジネスの世界もおそらく同様でしょう。クラウド・セキュリティも同じペースで進化する必要があります。絶えず変化し進化するクラウド・エコシステムでは、セキュリティ対策を定期的にレビューし、更新する必要があります。クラウド・サービス・プロバイダは、複数の新サービスを提供し、既存のサービスを微調整しています。組織は、この変化を続ける状況に素早く対応できているか、また管理しているセキュリティ・コントロール、ポリシーおよび構成がクラウド・セキュリティ・ポスチャを損なっていないかを確認する必要があります。

結論

Oracle CASB Cloud Serviceは、クラウドへの安全な移行を支援するすべての要素を提供します。Oracle CASB Cloud Serviceは、防御の最前線として機能し、あらゆるクラウドが適切な構成およびコントロールを保有するようにセキュリティ・コントロールとポリシーを提供します。業界最高のユーザーとエンティティの行動分析(UEBA)機能を活用して、クラウドの使用に対するインサイトを提供し、適切な緩和アクションを実行します。

お問い合わせ

+1.800.ORACLE1にお電話いただくか、oracle.comにアクセスしてください。
北米以外のお客様は、oracle.com/contactでお近くの営業窓口を参照いただけます。

blogs.oracle.com/oracle facebook.com/oracle twitter.com/oracle

Integrated Cloud Applications & Platform Services

ORACLE

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