クラウド・セキュリティ – CASBの要件

ORACLE

クラウド・テクノロジがデジタル・ビジネスの運営に占める割合がより大きく重要になっている状況において、クラウド・コンピューティング・プラットフォームにより、従来のセキュリティ・モデルの有効性が急速に限定的なものになっています。クラウドによって、組織はセキュリティの再検討が必要になりました。クラウド内のデータおよびアプリケーションは、企業の旧来の境界線の外に存在しているため、これからはこれらを新しい方法で保護する必要があります。

パブリック・クラウド・アプリケーションに直接接続するユーザーはますます増え続け、ワークロードは、プロバイダによって提供されるInfrastructure-as-a-ServiceやPlatform-as-a-Serviceの利用へとシフトし続けているため、Cloud Access Security Broker (CASB)と呼ばれる製品カテゴリが新たに出現して注目を集め、クラウド・セキュリティの課題に対応する主力のソリューションとなっています。何年にもわたり、CASBは、急激なクラウド導入のトレンドに後れを取ることなく進化を続けています。この資料では、組織がCASBソリューションに求める主要な機能の一部の定義を試みます。

CASBの概要

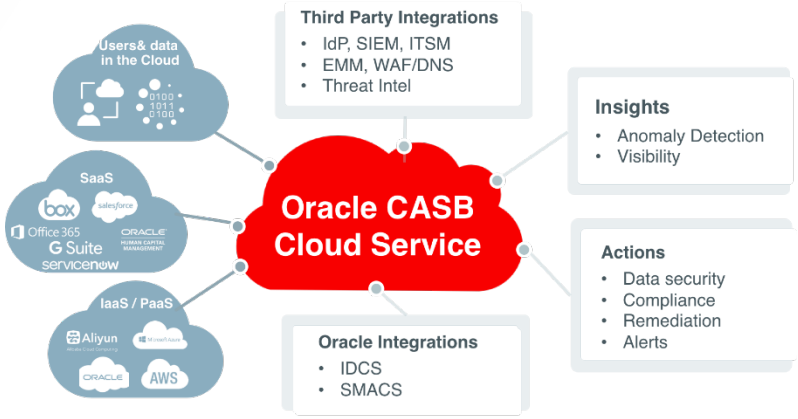

図1: 代表的なCASBソリューション

Gartnerは次のように説明しています。「**Cloud Access Security Broker (CASB)**は、オンプレミスまたはクラウドベースのセキュリティ・ポリシー施行ポイントであり、クラウド・サービス・コンシューマとクラウド・サービス・プロバイダの間に配置され、クラウドベースのリソースがアクセスされる際、企業のセキュリティ・ポリシーを結び付け、適切な対応を取ります。CASBは、複数のタイプのセキュリティ・ポリシー施行を統合します。」

スタック全体(インフラストラクチャ、プラットフォームおよびソフトウェア)にわたるクラウド・サービスの導入が急速に進み、CASBの役割の重要性は一層増しています。CASBの初期の使用事例は、主に組織内のユーザーによって使用されているクラウド・リソースへの可視性を得ることでしたが、最新の使用事例は、それに加えてクラウド・サービスの状態の保護、ユーザー・アクティビティの監視、クラウド・サービス内のデータのロック・ダウンへと拡大しています。

CASBの主要機能

すべてのクラウド・アプリケーションとリソースにわたる検知、可視化およびセキュリティ

CASBソリューションは、ユーザーがどこにいるかに関係なく、クラウド・アクセスに対する完全なビューを提供する必要があります。このソリューションにより、次のようなクラウド・エコシステム全体のセキュリティ・アセスメントが合理化されます。

- 使用しているSaaSアプリケーション
- ビジネスで利用しているIaaSおよびPaaSプロバイダ

事前に作成済およびカスタマイズ可能なコンプライアンス・レポートをサポートし、コンプライアンスへのセキュリティ・ファーストのアプローチを実現する必要があります。また、リスクが発生した場合、それを修正する手段の提供も必要です。クラウド・スタック全体の積極的な監視は考慮すべき重要事項です。

今日のほとんどの組織がクラウドを導入しており、その大部分がマルチクラウド戦略を採用しています。このような組織のBYODポリシーは、生産性を高めコストを低減する一方、Infrastructure-as-a-Service (IaaS)サービスおよびSoftware-as-a-Service (SaaS)アプリケーションに、脅威防御、機微データの保護および法規制の遵守への対応のためのクラウド・アプリケーション・セキュリティが必要になります。Cloud Access Security Broker (CASB)ソリューションは、安全で生産的な利用を実現するために、認可済および未認可のクラウド・サービスに対する可視性とコントロールをクラウド・セキュリティに提供する必要があります。さらに、CASBは、クラウド・サービスの初期または検知された状態が組織のすべての要件を満たし、許容できる最低限のセキュリティ・ポスチャおよび基準を達成していることを保証できる必要があります。

IaaS、SaaSおよびPaaSの継続的なセキュリティ・アセスメント

Infrastructure-as-a-Service (IaaS)の拡大と急速な導入により、同様の領域をカバーするクラウド・セキュリティ・ソリューションの必要性が生まれました。Cloud Access Security Brokerソリューションは、SaaS、IaaS、PaaSのいずれでも、クラウドのすべての利用に対し保護とセキュリティを提供できる必要があります。つまり、CASBは、これらの環境のセキュリティ構成を継続的に監視することで、サービスが適切に構成されていること、またクラウド・サービスの状態変更の原因である構成の変更が検知され適切なユーザーに警告が表示されることを保証することが求められます。また、CASBは、機微データの検知、保護およびクラウド・データ損失防止機能も提供する場合があります。加えて、クラウド・サービスの数が増加すると、サービス・プロバイダが行う進行中の構成変更を識別し管理することが非常に困難になります。このような複雑な状況を管理する特定の人材を確保することも簡単ではありません。優れたCASBソリューションは、組織がサービスの専門家に頼ることなく、保証されたセキュリティ・ポスチャを即座に入手できるように、すぐに利用可能な豊富なポリシー・セットを提供する必要があります。たとえば、企業がIaaSサービスを導入した場合、その企業の専門家にIaaSプロバイダのコンピュート、ネットワーク、ストレージおよびセキュリティ機能を理解させるだけではなく、その基礎となるインフラストラクチャのコンポーネントと構成も理解させる必要があります。これを怠ると、インフラストラクチャの脆弱性が偶発的に高まる可能性があります。理想として、CASBソリューションは、クラウド・サービス全体にただちにデプロイできるセキュリティ・ポリシー備えている必要があり、そのポリシーにより、導入の障壁が軽減され、価値実現までの時間が短縮され、全体的なセキュリティ・ポスチャが強化されます。

機械学習と脅威防御によるユーザーとエンティティの行動分析(UEBA)

本質的に、クラウド・サービス、特にクラウド・サービスのコントロール・プレーンにはインターネット経由でアクセスできます。クラウド・サービスを誰が使用しているかを把握することが必要なだけではなく、結果として生じる膨大な脅威となり得る点を絶えず監視することも必要です。これが、まさにUEBAが機械学習に基づくプロファイリングと異常検知をセキュリティにもたらす領域です。UEBAは、原則的に、企業内で発生する正規のプロセスがどのような特性を持つかをマップし、脅威をどのように識別し阻止するかを学習します。

CASBソリューションは、UEBAを組み込み、実践可能なインテリジェンスを供給し、内部および外部の脅威に対する保護を提供する必要があります。CASBソリューションは、クラウド環境への内部または外部の脅威の可能性のある異常なユーザー・アクティビティやデータ移動および資格情報の漏洩を検知できる必要があります。

アイデンティティおよびアクセス管理との統合

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レベルとなります。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。CASBソリューションは、オープン・プラットフォームとして、既存のアイデンティティおよびアクセス管理ソリューションやIdentity-as-a-Serviceソリューションとのシームレスで標準ベースの統合を提供する必要があります。

データ・セキュリティ

通常、アプリケーション・セキュリティは、SaaSアプリケーションとの統合面をカバーします。データ・セキュリティに対するリスクは、保存されているデータおよび移動中のデータの流出です。CASBソリューションは、クラウドのデータ・セキュリティに対応できる必要があります。さらに、CASBは、クラウド・サービス固有のインサイトを提供できる必要があり、これには、アプリケーションのリスク・ポスチャ、使用パターンおよびアプリケーション内の危険な行動が含まれます。マルチモーダルCASBは、プロキシの使用をサポートしますが、このようなインフラストラクチャ・コンポーネントの導入は、デプロイメントを複雑にし、導入の時間を長引かせます。

クラウドによる提供 - 即応性と高信頼性

企業にとって、攻撃が巧妙化しているということは、従来のセキュリティ手法では、もはや適切な保護を提供できないということを意味します。多くの組織が、オンプレミスのハードウェアまたはソフトウェア・セキュリティ製品よりクラウドのSecurity-as-a-Service製品の方が優れたセキュリティを提供できることに賛同し始めています。CASBソリューションは、高速で即応性があり高い信頼性を備えている必要があります。

負担のないフリクションレスなユーザー・エクスペリエンス

CASBソリューションは、生産性に影響しない、万全なセキュリティを提供する必要があります。速度の低下や、デバイスのパフォーマンスへの影響を発生させることなく、必要な保護を提供する必要があります。加えて、CASBソリューションは、他のセキュリティ・ソリューションと統合して改善を促進するために、十分なAPIを備えていることも必要です。理想として、CASBソリューションはエージェントレスであるべきであり、そうであれば、ユーザーによる採用への摩擦が削減されます。

結論

CASBマーケット全般で機能が進化を続けていますが、これまでに述べた各要素で、大部分の組織を対象としたCASB機能の概要を示せているはずです。ほとんどの組織がマルチクラウド戦略を採用していることを考えると、CASBは、IaaS、PaaSおよびSaaSにわたる複数のクラウド・サービスに対する包括的なサポートを、価値実現までの期間を短縮しつつ、提供することが非常に重要です。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。つまり、Oracle CASB Cloud Serviceは、クラウド・セキュリティ・ポスチャの迅速な改善を支援する、市場において最も包括的なCASBであると言えます。

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