クラウド・サービスのセキュリティにおけるユーザー行動分析の重要性

ORACLE CLOUD

最新のセキュリティ脅威に対抗するために、多くの企業はユーザー行動分析(UBA)を活用したセキュリティ・ソリューションに目を向け始めています。このソリューションは、ユーザー行動を分析し、標準のベースライン定義を形成することで、逸脱が発生したときにIT管理者に通知することができます。

データ保護の新しい手段の必要性

プロトコル分析やウィルス・シグネチャに基づく従来のセキュリティ対策は、あらゆる企業の防御システムの一部であり続けています。しかし、これらのソリューションは、特定の企業をターゲットにする最新の脅威よりも、以前からある脅威により適したものです。従来のソリューション単独では、ますます高度化する今日の攻撃やハッカーに対応できません。従来のソリューションでは、生産性や便利さのために、既存のセキュリティ対策や会社の方針を度々省略しようとする抜け目のないユーザーに対処することもできません。また、従来のセキュリティ対策では、多くの企業にとって懸念が高まっている内部脅威を検出することはほとんどできません。

クラウド・サービスと従来のITの両方を向上させるために、多くの企業は、ユーザー行動を分析するセキュリティ・ソリューションを実装し始めています。単に、ウィルスやマルウェアなどの攻撃オブジェクトを素早く識別したり、オペレーティング・システムやブラウザ内の脆弱性を早期に検出してハッカーの先手を打つのではなく、UBAソリューションは、特定のユーザーが実行するアクションの分析に重点を置き、通常の行動のベースラインを形成し、許容される規範からの逸脱を継続的に監視します。

ユーザーベースのセキュリティ・ソリューションを実装する理由

- 最新の攻撃は、検出が困難である内部の特権アカウントから行われる場合があります。
- 最新の脅威の標的は、少数の経営幹部ではなく、多数の目立たないユーザーである場合があります。
- 物理的にも仮想的にもアクセスの分離が欠如していると、クラウド環境の保護は困難になります。

最新のセキュリティにおけるユーザー行動分析の重要性

UBAを活用するセキュリティ・ソリューションは、以前から存在しています。しかし、UBAがすべての企業セキュリティ・ソリューションの重要な要素になりつつあるのには大きな理由があります。特に、企業がインフラストラクチャやアプリケーションをクラウドに移行する際に重要になります。

最新の脅威行動

多くの場合、従来のウィルスおよびマルウェアは、固有のシグネチャによって識別されます。一部の攻撃は、コマンド&コントロール・マルウェアで使用される通信シグネチャなどによって識別できます。

ORACLE

しかし、最新の攻撃は、まず、バックアップ特権アカウントを作成する、またはすでに漏洩しているアカウントの追加権限を取得するなどして、従来のセキュリティ対策をくぐり抜けることができます。ハッカーは、追加権限を用いて警報を発生させることなく、様々な操作を実行できます。また、セキュリティ対策をオフに切り替えるだけで、セキュリティ対策を打ち破ります。

このような脅威行動は、会社に最終的にそのドアを閉めさせるために大々的に報じられました。ハッカーは、企業のAmazon Web Services (AWS)環境へのアクセス権を取得すると、まず、バックアップ特権アカウントを作成しました。身代金の要求の後、企業がハッカーの締め出しを図ると、バックアップ・アカウントが使用され、企業のクラウド環境全体のデータが消去されました。UBAを使用するセキュリティ・ソリューションであれば、アカウント権限の変更または認可されていない特権アカウントの作成などの異常行動をIT管理者に警告したでしょう。

最新の脅威の標的

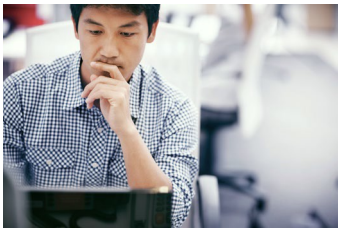
従来のセキュリティ対策は、目立つ立場にあるユーザーの保護に重点を置いていました。経営幹部、財務担当者、販売チームは、極めて重要なデータに容易にアクセスできるグループのごく一部です。一般的に、会社や顧客のデータを盗むために彼らが従来の攻撃の標的になることに驚きはありません。しかし、最新の攻撃は、まず他の目立たないユーザーを通じてアクセス権を手に入れ、間接的にこのグループを標的にすることが多くなっています。ハッカーが企業のネットワークやリソースへのアクセス権を手に入れると、簡単にネットワーク内を移動し、他のアカウントを流出させ、最終的に機微データへのアクセス権を入手できてしまいます。

広く報道された全国的な小売業者への攻撃は、目立たないユーザーを突破口として始まりました。ハッカーは、一度ネットワークに入ると、設定されている多くのセキュリティ対策をすり抜けて数百万のクレジット・カードやその他の機微情報を盗みました。UBAを活用するセキュリティ・ソリューションであれば、ネットワーク内からであったとしても、機密情報へのアクセス権を取得しようとするユーザーを検出していたでしょう。実際、堅牢なUBAソリューションは、アカウントが漏洩する前に、危険性のあるユーザー、つまり攻撃の主たる候補者をIT管理者に警告し、予測セキュリティにより企業を武装できます。

アクセス分離の欠如

オンプレミス・セキュリティの管理に慣れているIT管理者は、セキュリティ・アプライアンスの構成へのアクセスを制限することが多くあります。管理アクセスは、直接アプライアンス接続やVPNの使用などの独自の要件により、他のネットワークから多くの場合分離されています。もちろん、アプライアンスは、施錠された配線ボックスの背後での物理的な改ざんから保護されています。
残念ながら、多くのIT管理者は、クラウド・サービスの導入に伴うセキュリティの予防措置を見落としています。つまり、すでに広く知られていたネットワーク分離、物理的な分離、独自のログイン手順は存在しないのです。

ITチームが習慣にしていた、コントロールされた管理アクセスが失われるということが、セキュリティ・ポスチャの甚大な欠如となる場合があります。UBAソリューションは、単純な資格証明以上の別のセキュリティ層として機能することで、この欠如を埋めます。ユーザーの通常の行動を継続的に評価することで、ユーザー権限のアップグレード、機微なセキュリティ設定へのアクセスおよびセキュリティ設定の変更など通常の行動からの逸脱が発生したときに、IT管理者に警告することが可能です。



最新の攻撃は、まず他の目立たないユーザーを通じてアクセス権を手に入れ、目立つ経営幹部を間接的に標的にすることが多くなっています。ハッカーが企業のネットワークやリソースへのアクセス権を手に入れると、簡単にネットワーク内を移動し、他のアカウントを流出させ、最終的に機微データへのアクセス権を入手できてしまいます。

Oracle CASB Cloud Serviceにおけるユーザー行動分析

Oracle CASB Cloud Serviceは、AWS、Salesforce、MS Office 365およびGoogle Appsなどのクラウド・サービス環境において企業が直面する可視性およびセキュリティ面の課題に対応します。すべてのOracle CASB Cloud Serviceソリューションに含まれるUBA機能は、個人のアクティビティ、ビジネスクリティカルなクラウド・アプリケーションの他、複数のアプリケーションに及ぶアクティビティも分析します。このUBA機能により、企業のクラウド環境全体のユーザー行動およびアクティビティの包括的なビューを単一のユーザー・インタフェースから得ることができます。

UBAは、Oracle CASB Cloud Serviceで提供されている多くの機能の1つにすぎません。クラウド・セキュリティの自動化を提供するこのプラットフォームは、ビジネスクリティカルなクラウド・サービス全体にわたる脅威の総合的なビューを提供します。このようなアプローチは、クラウドを横断する脅威を検出し、コンプライアンスを順守して、最も効率的な方法でインシデントに対応する企業にとって非常に重要です。

主な機能

Oracle CASB Cloud Serviceは、クラウド環境全体の包括的な可視性およびセキュリティを提供します。主要なセキュリティ機能は次のとおりです。

- すべてのクラウド・アプリケーション全体で危険性のあるユーザーをグラフィカルに表示するダッシュボード
- 詳細なリスク分析によるフォレンジック、ドリルダウン機能
- ユーザー行動の継続的なアセスメントに基づく、動的なユーザーリスク・スコアリング
- アクセス・パターン、管理アクションおよびデバイスの特性に基づく、不審な、または危険性のある行動の検出
- シングル・サインオン・ソリューションからのユーザー・アイデンティティのインポートによる、ユーザーの関連付けおよび脅威検出の拡張
- シングル・サインオン・ソリューションの統合によるすべてのアプリケーションの全ユーザーのプロファイリング
- 危険性のあるユーザーの監視を含む、統合されたワークフロー
- 統合されたシングル・サインオン・ソリューションによるユーザー・リスク・スコアに基づく、アプリケーション・アクセスの自動修正および拒否

CONNECT WITH US

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

FOR MORE INORMATION
Contact: 1.800.ORACLE1

ORACLE

Integrated Cloud Applications & Platform Services