IBM Cloud

クラウド・プラットフォームをセキュアにするためのガイド

目次

3 クラウドベース・アプリケーションのセキュリティーの再考
4 クラウド・プラットフォーム上のアイデンティティーの検証およびアクセス管理
6 ネットワークの分離と保護の再定義
7 暗号化とキー管理よるデータの保護
9 DevOps 対応セキュリティーの自動化
11 インテリジェント・モニタリングを使用したセキュリティーの影響を受けないシステム構築
12 ビジネスの成功を促進するセキュリティー

IBM

重要事項

1 クラウド・プロバイダーは会社のアイデンティティー管理システムをプラットフォームに統合し、どんな場合でも信頼できるアイデンティティー管理システムを必要に応じて提供できる能力を持つ、というのがあるべき姿です。

2 信頼を得るための措置として、十分に統合されたファイアウォール、セキュリティー・グループ、ワークロードと信頼できるコンピュート・ホストに基づくマイクロ・セグメンテーションに対応するオプションをクラウド・プラットフォームで提供していることを検証します。

3 クラウド・プロバイダーには、すべてのデータ・ストレージとサービスにアクセスする鍵を組織が独占的に管理できる BYOK ソリューションの提供を期待します。

4 コンテナーのベスト・セキュリティー・プラクティスは、デプロイメント前と稼働中の両方で脆弱性に関してスキャンすることです。

5 クラウド・プラットフォームのセキュリティーでは、効果的な制御アクセス、ワークロード・レベルでの運用、詳細なアクティビティーの追跡、およびオンプレミス・システムへの統合が必要です。

クラウドベース・アプリケーションのセキュリティーの再考

多くの組織がアプリの開発やワークロードの管理のためにクラウドネイティブ・モデルに移動するため、クラウド・コンピューティング・プラットフォームでは、従来の境界ベースのセキュリティ・モデルの有効性が 急速に制限されています。境界のセキュリティーは依然として必要ですが、それ自体では不十分です。クラウドにあるデータとアプリケーションは古い企業境界の外にあるため、新しい方法で保護する必要があります。

クラウドネイティブ・モデルに移行する、あるいはハイブリッド・クラウド・アプリ・デプロイメントを計画している組織は、従来の境界ベースのネットワーク・セキュリティーをクラウドベースのワークロードを保護するテクノロジーで補完する必要があります。企業は、クラウド・サービス・プロバイダーがインフラストラクチャーからスタックの安全を確保する状況について信頼する必要があります。プラットフォーム・セキュリティーの信頼を築くことは、プロバイダーの選択において基本となります。

クラウド・セキュリティー・ドライバー

データ保護と法令遵守はクラウド・セキュリティーの主な原動力であり、クラウドの採用を抑制する力でもあります。これらの懸念への取り組みは、開発と運用のすべての局面に広がります。クラウドネイティブ・アプリケーションを使用すると、データがオブジェクト・ストア、データ・サービス、クラウドの至る所に広がり、攻撃を受ける可能性がある前線を複数作成してしまう可能性があります。攻撃を受けるのは巧妙なサイバー犯罪者や外部ソースからだけとは限りません。最近の調査によると、回答者の 53% は過去 12 か月に内部から攻撃を受けたことを確認しています。[1]

クラウド・セキュリティーの 5 つの基本

組織はクラウド・プラットフォームの使用について特殊なセキュリティーのニーズを扱うため、プロバイダーが信頼できるテクノロジー・パートナーになることを必要とし、期待します。実際、セキュリティーの 5 つの側面は組織固有の要件に関連するため、組織はそれらに基づいてクラウド・プロバイダーを評価する必要があります。

1. **アイデンティティーおよびアクセス管理:** 認証、アイデンティティーおよびアクセスの制御
2. **ネットワーク・セキュリティー:** 保護、分離、セグメンテーション
3. **データ保護:** データの暗号化とキー管理
4. **アプリケーション・セキュリティーと DevSecOps:** セキュリティー・テストとコンテナー・セキュリティーを含む
5. **可視性とインテリジェンス:** パターンのログ、フロー、イベントのモニターと分析

クラウド・プラットフォーム上のアイデンティティーの検証およびアクセス管理

クラウド・プラットフォームを使用したインタラクションは、アイデンティティーを検証し、誰 (管理者やユーザー) が、あるいは何 (サービスの場合があります) がインタラクションをしているかを証明して始まります。API エコノミーでは、サービスは独自のアイデンティティーを持ちます。そのため、このアイデンティティーに基づいたサービスに対して API を正確かつ安全に呼び出す能力がクラウドネイティブ・アプリを正常に実行するために欠かせません。

API アクセスとサービスを呼び出すためのアイデンティティーを認証するために、整合性のある方法を提供するプロバイダーを探します。クラウドにホストされているアプリケーションにアクセスするエンド・ユーザーを識別および認証する方法も必要です。たとえば、IBM® クラウド ではアプリ ID を開発者が認証をモバイルや Web のアプリに組み込む方法として使用します。

強力な認証は、無許可のユーザーがクラウド・システムにアクセスできないようにします。プラットフォームのアイデンティティーおよびアクセス管理 (IAM) は非常に基本的なものであるため、既存のシステムを持つ組織は、クラウド・プロバイダーが会社のアイデンティティー管理システムを統合することを期待します。これは複数のシステムにわたって個人の ID と属性をリンクするアイデンティティー・フェデレーション・テクノロジーによってサポートされることがよくあります。

認証サービスを呼び出す理由

マイクロサービスベースのアーキテクチャーでは、API を使用したアプリケーションによるデータの通信と共有が可能です。アプリケーションの実行時に、さまざまな操作を完了させるために必要に応じてサービスを呼び出すのに API を使用します。たとえば、アプリケーションがデータに対応するオブジェクト・ストア・サービスを呼び出す場合があります。要求を満たす一環として、オブジェクト・ストア・サービス自体が鍵管理サービスを呼び出し、データの復号に必要な暗号鍵を取得する場合があります。そして、ユーザー・エクスペリエンスの実現の一環として、アプリが API を使用してユーザー・アイデンティティー情報にアクセスしたり、アプリ間でコンテンツを投稿したり(アプリから Twitter へのコンテンツの投稿など)、位置固有情報を役立てるためにユーザーの位置を判定したりします。**これらのすべてをまとめると、セキュリティー上の課題が明らかになります。**

クラウド・プロバイダーは整合性がある方法で、API またはサービスへのアクセスを必要とするユーザーやサービスのアイデンティティーを認証する必要があります。もちろん、認証の一部としてすべてのアクセス要求のセッションとトランザクションのログが監査目的のために記録されている必要があります。**API とサービスは貴重な知的財産を保持する可能性が高く、誰にでも使用させるのは望ましくありません。**

見込みのあるクラウド・プロバイダーには、その IAM インフラストラクチャーとシステムがすべての基盤をカバーしている証明を求めます。たとえば、IBM クラウドではアイデンティティーおよびアクセス管理は複数の重要な機能に基づきます (図 1)。

アイデンティティー

- 各ユーザーは一意の識別子を持つ
- サービスとアプリケーションはサービス ID によって識別される
- リソースは、クラウド・リソース名 (CRN) によって識別および処理される
- ユーザーとサービスはアイデンティティーを使用して認証され、トークンが発行される

アクセス管理

- ユーザーとサービスがリソースへのアクセスを試みると、IAM システムがアクセスとアクションの許可または拒否を決定します。
- サービスは、アクション、リソース、役割を定義します。
- 管理者は、ユーザーの役割と権限をさまざまなリソースに割り当てるポリシーを定義します。
- 保護は、API、クラウド機能、クラウドにホストされているバックエンド・リソースまで拡張されます。

クラウド・プロバイダーのセキュリティーを評価する際には、ユーザーを特定のリソースにだけでなく、リソースの特定操作にまで制限できる、共通リソース名を使用するアクセス制御リストを求めます。この機能は、社内外両方の無許可ユーザーのアクセスから確実にデータを保護するのに役立ちます。

独自のエンタープライズ・アイデンティティー・プロバイダー (エンタープライズ IdP) をクラウドに拡張するのは、エンタープライズ IdP を使用する既存のエンタープライズ・アプリケーション上にクラウドベース・アプリを構築する際に特に有用です。ユーザーは、複数のシステムや ID を使用せずに、クラウドネイティブ・アプリケーションと基本アプリケーションの両方にスムーズにログインできます。複雑さの軽減は、常に意義のある目標です。

重要事項

理想的には、クラウド・プロバイダーは会社のアイデンティティー管理システムをプラットフォームに統合し、どんな場合でも信頼できるアイデンティティー管理システムを必要に応じて定義できる能力を持つべきです。

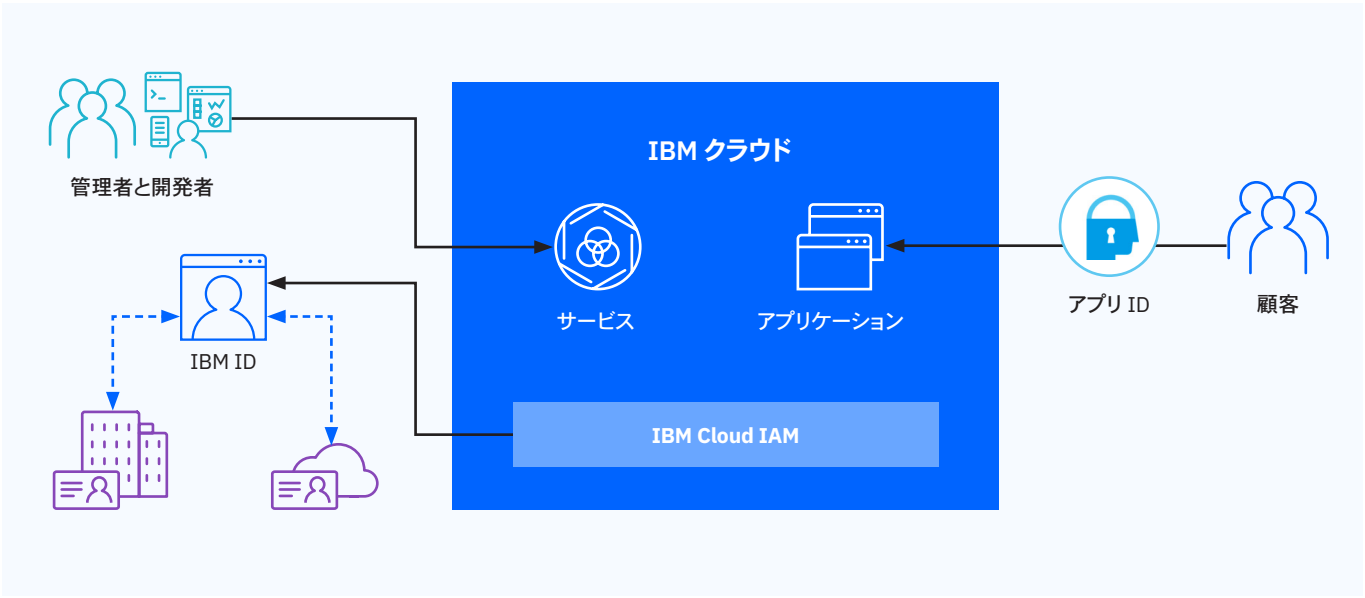

図 1.プロバイダーのマネージド・クラスター要素とお客様のマネージド・クラスター要素の分離。

ネットワークの分離と保護の再定義

多くのクラウド・プロバイダーは、同じネットワーク内のデバイスとサーバーへのアクセスを制限するためにネットワーク・セグメンテーションを使用します。さらに、プロバイダーは物理インフラストラクチャー上に仮想分離ネットワークを作成し、特定の分離ネットワークへのユーザーやサービスを自動的に制限します。これらやその他の基本的なネットワーク・セキュリティー・テクノロジーは、クラウド・プラットフォームで信用を構築するための最低条件です。

クラウド・プロバイダーは、Web アプリケーション・ファイアウォールから仮想プライベート・ネットワークやサービス不能の軽減まで、ソフトウェア定義のネットワーク・セキュリティーと使用に応じた料金に対応するサービスとしての保護テクノロジーを提供することがよくあります。クラウド・コンピューティング時代に重要なネットワーク・セキュリティーとして、以下のテクノロジーを検討します。

セキュリティー・グループとファイアウォール

クラウド・カスタマーは、しばしば境界保護のためにネットワーク・ファイアウォールを挿入し (仮想プライベート・クラウド/サブネットレベル・ネットワーク・アクセス)、インスタンスレベル・アクセスに応じたネットワーク・セキュリティー・グループを作成します。セキュリティー・グループは、アクセスをクラウド・リソースに割り当てるために適切な第 1 防衛線です。このグループを使用して、パブリック・ネットワークとプライベート・ネットワークの両方で入出力のトラフィックを管理するためにインスタンスレベル・ネットワーク・セキュリティーを簡単に追加できます。

多くの顧客は、境界ネットワークとサブネットを安全に保護する境界管理を必要とし、仮想ファイアウォールはこのニーズを満たすために容易にデプロイできる方法です。ファイアウォールは、望ましくないトラフィックがサーバーに達するのを防ぎ、攻撃対象領域を狭くするために設計されます。クラウド・プロバイダーには、ネットワーク全体またはサブネットに対して権限ベースのルールを構成できる仮想およびハードウェア両方のファイアウォールの提供を期待します。

もちろん、VPN でクラウド・バックからオンプレミス・リソースまでのセキュアな接続を提供します。これらは、ハイブリッド・クラウド環境を稼働するのに欠かせません。

マイクロセグメンテーション

小さなサービスのセットとしてのクラウドネイティブ・アプリケーションを開発すると、ネットワーク・セグメントを使用して分離可能になり、セキュリティー上のメリットをもたらします。ネットワーク構成とネットワーク・プロビジョニングの自動化を使用してマイクロ・セグメンテーションを導入するクラウド・プラットフォームを探します。**マイクロサービス・モデルで構築され、コンテナー化されたアプリケーションが、最初にワークロード分離のスケーリングをサポートする基準になります。**

重要事項

信頼を築く一環として、十分に統合されたファイアウォール、セキュリティー・グループ、ワークロードと信頼できるコンピュート・ホストに基づくマイクロ・セグメントーションに対応するオプションをクラウド・プラットフォームで提供していることを検証します。

暗号化とキー管理によるデータの保護

データの確実な保護は、すべての、特に金融サービスやヘルスケアなどの高度に規制された産業のデジタル・ビジネスにとってセキュリティーの基本です。

クラウドネイティブ・アプリケーションに関連付けられたデータは、オブジェクト・ストア、データ・サービス、およびクラウドの至る所に広がる可能性があります。従来のアプリケーションは独自のデータベースと独自の VM を持ち、機密データはファイルにある場合がありました。このケースでは、保存中および転送中の両方で機密データの暗号化が重要になります。

ビジネスで、知識なしにデータにアクセスするクラウド・オペレーターやその他の無許可のユーザーを心配し、データ・アクセスに完全な可視性を期待するのは当然です。**暗号化を使用したデータへのアクセス管理と、暗号鍵へのアクセス管理もまた、当然の安全措置になります。**結果として、現在では Bring-Your-Own-Keys (BYOK) モデルはクラウド・セキュリティー要件です。暗号鍵を一元管理でき、ルート鍵が鍵管理システムの境界に決して残らないことを保証し、すべての鍵管理ライフサイクル・アクティビティーを監査できます(図 2)。

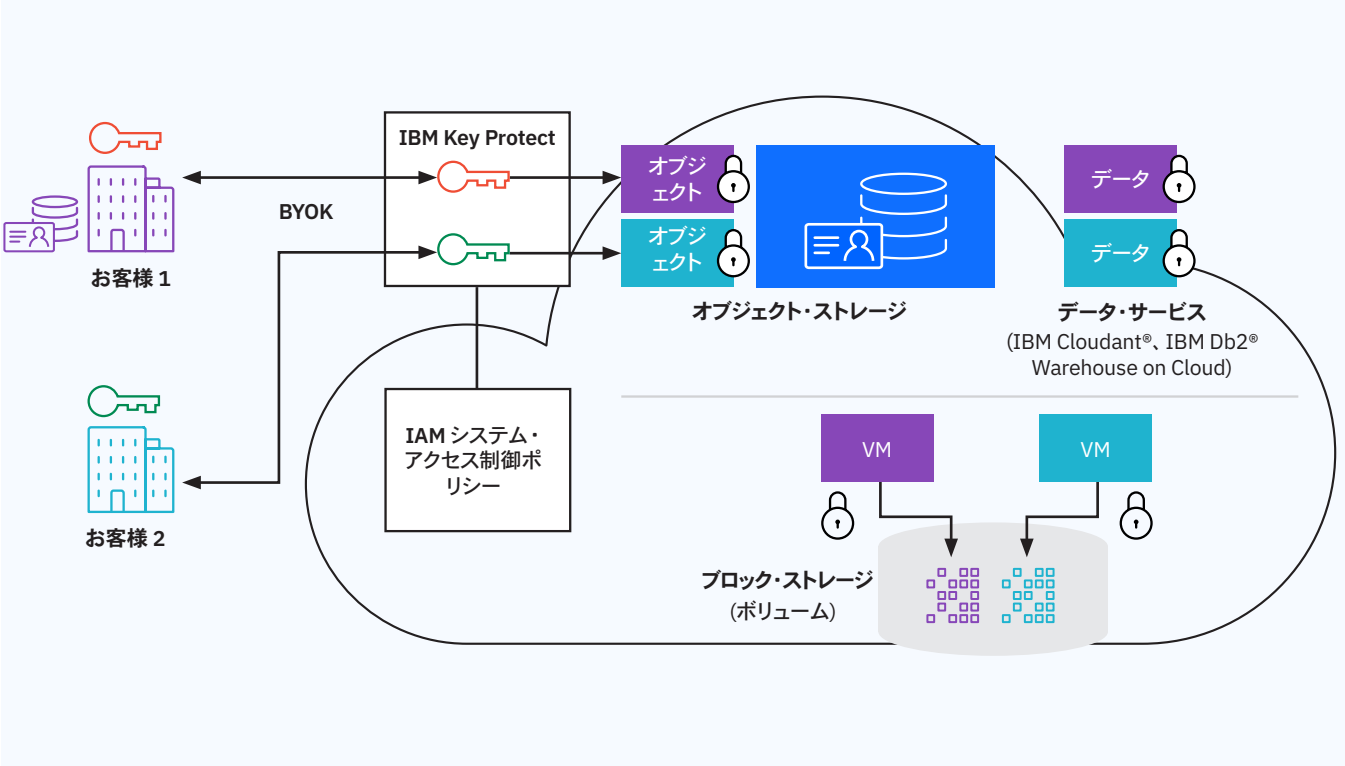

図 2.BYOK ソリューションのアーキテクチャー

信頼できるコンピュート・ホスト

これはハードウェアに行き着きます。貴重なデータとアプリケーションを信頼されていないホストにデプロイすることは、誰も望みません。測定、検証、開始の手続きを踏んでハードウェアを提供するクラウド・プラットフォーム・プロバイダーは、コンテナー・オーケストレーション・システム内にデプロイされるアプリケーションに高度にセキュアなホストを提供します。

Intel トラステッド・エグゼキューション・テクノロジー(Intel TXT) とトラステッド・プラットフォーム・モジュール (TPM) は、クラウド・プラットフォームへの信頼を可能とするホストレベル・テクノロジーの例です。Intel TXT は、システムまたは BIOS コードを破損させるか、プラットフォームの構成を修正して機密情報を盗むことを目的としたソフトウェアベースの攻撃を防ぎます。Intel TPM は、システム制御をオペレーティング・システムに渡す前に改ざんされていないことを保証して、システムの起動プロセスの保護を支援するハードウェアベースのセキュリティ・デバイスです。

保存中と転送中のデータ保護

BYOK に暗号化を組み込むと、オンプレミスベースでも、クラウドベースでも、データの制御を維持できます。これは、クラウドネイティブ・アプリケーション・デプロイメントでデータのアクセスを制御する優れた方法です。このアプローチでは、顧客の鍵管理システムでオンプレミスの鍵を生成し、プロバイダーの鍵管理サービスに渡します。
このアプローチでは、ブロック、オブジェクト、データ・サービスなどの複数のストレージ・タイプの至る所で保存中のデータの暗号化が含まれます。

移動中のデータに関しては、Transport Layer Security/Secure Sockets Layer (TLS/SSL) でセキュアな通信と転送が行われます。TLS/SSL 暗号化は、暗号システムまたはインフラストラクチャーの管理を必要とせずに、コンプライアンス、セキュリティー、およびガバナンスを証明することもできます。SSL 証明書の管理能力は、クラウド・プラットフォームでの信頼要件です。

監査とコンプライアンスのニーズを満たす

サービス・プロバイダーのアクセスなしで、独自の暗号鍵を提供し、クラウドで保管すると、CISO のコンプライアンス監査に必要な情報の可視性と管理が可能になります。

重要事項

クラウド・プロバイダーには、すべてのデータ・ストレージとサービスにアクセスする鍵を会社が管理できる BYOK ソリューションの提供を期待します。

DevOps 対応セキュリティーの自動化

DevOps チームはクラウドネイティブ・サービスを構築し、コンテナー・テクノロジーを使用して作業するため、ますます増大する自動化パイプライン内でセキュリティー・チェックを統合する方法が必要です。Docker Hub などのサイトがオープン・エクスチェンジを促進しているので、開発者は必要物をダウンロードするだけでイメージの準備時間を簡単に節約できます。しかし、柔軟性とともに、レジストリーに配置されたすべてのコンテナー・イメージをデプロイする前に定期的に調べる必要性が発生します。

自動化されたスキャニング・システムは、イメージの実行を開始する前に考えられる脆弱性を調べて信頼性を確保するのに役立ちます。プラットフォーム・ベンダーに、組織が DevOps パイプライン・セキュリティーの一部としてポリシー(「脆弱性のあるイメージはデプロイしない」、「イメージを稼働環境にデプロイする前に警告を出す」など) を作成できるか問い合わせます。

たとえば IBM Cloud コンテナー・サービスでは、静的およびライブ両方のコンテナー・スキャニングを行う Vulnerability Advisor (VA) システムを提供します。VA は、クラウド・カスタマーのプライベート・レジストリーにあるすべてのイメージのすべてのレイヤーを調べ、イメージをデプロイする前に脆弱性とマルウェアを検出します。レジストリー・イメージをスキャニングするだけでは、静的イメージからデプロイされたコンテナーまでのドリフトなどの問題を見逃す可能性があるため、VA は稼働中のコンテナーも異常がないかスキャンします。また、段階的な警告の形式で推奨事項も提供します。

重要事項

コンテナーのベスト・セキュリティー・プラクティスは、デプロイメント前と稼働中の両方で脆弱性に関してスキャンすることです。

その他に VA には、次のように DevOps パイプラインでセキュリティーの自動化に役立つ機能があります。

- **ポリシー違反設定:** VA を使用すると、管理者は、イメージがエラーになる 3 種類の状況 (インストールされたパッケージに既知の脆弱性がある、リモート・ログインが有効化される、リモート・ログインが容易に推測されるパスワードを持つユーザーをで有効化される) に基づいて、イメージ・デプロイメント・ポリシーを設定できます。
- **ベスト・プラクティス:** VA は現在、パスワードの最小年齢や最低限の長さなどの設定を含め、ISO 27000 に基づく 26 ルールを確認します。
- **セキュリティーの不適切な構成の検出:** VA は、不適切な構成の各問題についてフラグを立て、その説明を表示し、修正するための行動方針を推奨します。
- **IBM X-Force® との統合:** VA は 5 つのサードパーティー・ソースからセキュリティー・インテリジェンスを取り入れ、各脆弱性を評価するのに、攻撃ベンダーや既知の解決策の複雑さと可用性などの基準を使用します。この評価システム (重大、高、中ぐらい、または低)は、管理者が脆弱性の重大性を素早く理解し、修正の優先度を決めるのに役立ちます。

修正する際は、VA はパッチをあてるためのイメージの実行を邪魔しません。その代わり、IBM はレジストリーにある「高品質の」イメージを修正し、新しいイメージをコンテナーにデプロイします。このアプローチは、イメージの今後のすべてのインスタンス化に、所定の同じ解決策が必ず含まれるようにするのに役立ちます。VM は、VM にパッチをあて、Linux のセキュリティー脆弱性を修正するためにエンドポイント・セキュリティー・サービスを使用して、従来と同様に運用される場合があります。

Kubernetes が使えます

DevOps チームが有名な Kubernetes コンテナー・オーケストレーション・ソフトウェアを使用して作業する場合は、チームが希望するツールを使用して作業を続行できることを確認します。また、プラットフォームで新しいプロビジョニングと既存の Kubernetes クラスターの管理がどの程度容易か評価します。

クラウド・プラットフォーム・プロバイダーに、Kubernetes システムとともに Calico と Istio をサポートするかを問い合わせます。Calico と Istio は、アプリケーションとワークロードのセキュリティーに役立つ Kubernetes の重要な 2 つのコンポーネントです。 Calico は、コンピュート・ノードのワークロードに割り当てられた IP アドレスの管理を簡素化し、各コンピュート・ノードのアクセス制御リストをプログラムし、セキュリティー・ポリシーを実行します。ポリシー定義を使用して設定し、構成ラベルを使用して実行されます。Istio は、Kubernetes ポッドまたはクラスター内のマイクロサービス間の通信を証明書ベースで管理します。

インテリジェント・モニタリングを使用したセキュリティーの影響を受けないシステム作成

クラウドに移動する際に、CISO（最高セキュリティ責任者）は低い可視性と制御の喪失について懸念を持つことがしばしばあります。特定の鍵が削除されるか、不注意な構成変更でオンプレミス・リソースやエンタープライズ・セキュリティー・オペレーション・センター (SOC) への接続が切断されると、組織のクラウド全体がダウンする可能性があるのに、オペレーション・エンジニアは、クラウドベース・ワークロード、API、マイクロサービスのすべての完全な可視性を期待してはいけないのでしょうか？

アクセス追跡と監査ログ

すべてのユーザーと管理アクセスは、クラウド・プロバイダーによるものでも、自分の組織によるものでも、自動的にログが記録される必要があります。組み込まれたクラウド・アクティビティー・トラッカーは、API、Web、モバイルのアクセスを含む、プラットフォームとサービスへのすべてのアクセスを追跡できます。組織は、ログを使用して、エンタープライズ SOC に統合する能力が必要です。

エンタープライズ・セキュリティー・インテリジェンス

すべてのログとイベントをオンプレミスのセキュリティー情報イベント管理 (SIEM) システムに組み込むオプションがあることを確認します (図 3)。一部のクラウド・サービス・プロバイダーは、インシデント管理とレポートによるセキュリティー・モニタリング、セキュリティー警告のリアルタイム分析、ハイブリッド・デプロイメントを横断する統合ビューも提供します。

たとえば IBM Qradar® は、組織のニーズに合わせて拡大可能なセキュリティー・インテリジェンス・ソリューションのセットを提供する包括的な SIEM ソリューションです。機械学習機能は予測セキュリティー免疫システムを構築する方法で、脅威パターンを学びます。

専門知識を使用するマネージド・セキュリティー

組織に十分なセキュリティーの専門知識がない場合は、自社のためにセキュリティーを管理できるプロバイダーを調査します。一部のプロバイダーは、セキュリティー・インシデントをモニターし、さまざまな業界の脅威インテリジェンスを応用して、行動を起こすための情報を証明できます。プロバイダーに、社内とマネージド・セキュリティーのサービスを統合する、単一ペインのグラスも提供できるか問い合わせます。

重要事項

クラウド・プラットフォームのセキュリティーでは、効果的な制御アクセス、ワークロード・レベルでの運用、詳細なアクティビティーの追跡、およびオンプレミス・システムへの統合が必要です。

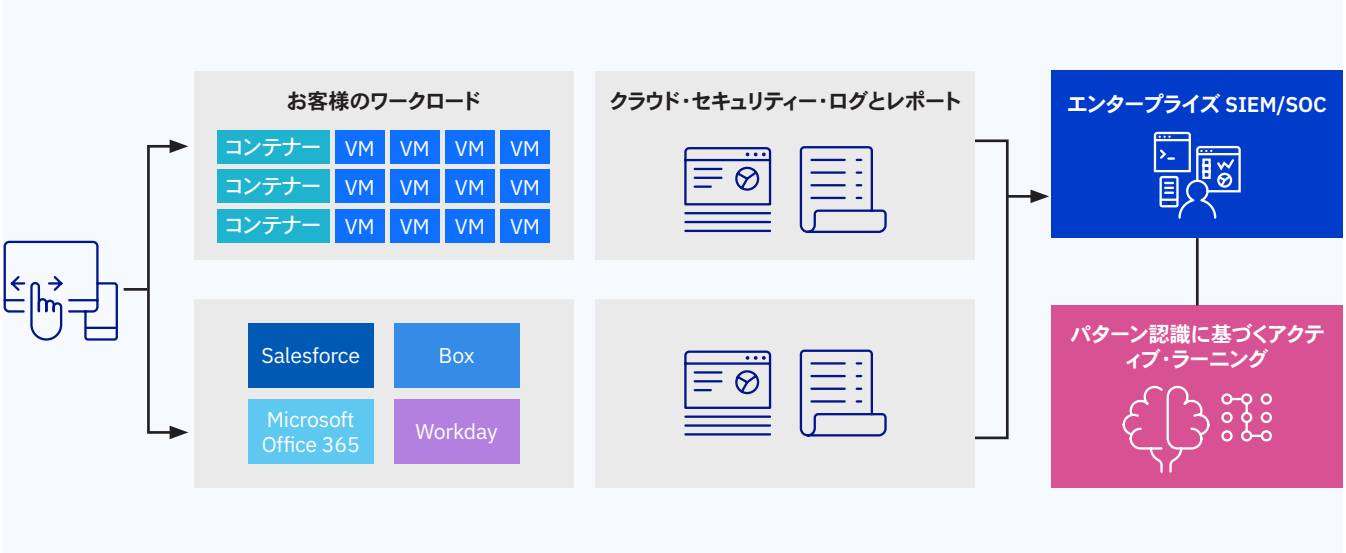

図 3. クラウドの可視性をエンタープライズ SIEM/SOC に統合。

ビジネスの成功を促進するセキュリティー

クラウド・テクノロジーはデジタル・ビジネスを運営するのにますます大きく重要な要素になりつつあるため、データ、アプリケーション、顧客が直面するアプリケーションが依存するクラウド・インフラストラクチャーを保護する能力と管理の適切なセットを提供するクラウド・プロバイダーを探すのは、本当に価値があります。プラットフォーム・セキュリティー・ソリューションが 5 つの重要なクラウド・セキュリティーの重点分野 (アイデンティティーおよびアクセス、ネットワーク・セキュリティー、データ保護、アプリケーション・セキュリティー、可視性とインテリジェンス) をカバーすることを期待します。目標はテクノロジーについての懸念を減らし、コア・ビジネスにさらに重点をあてることです。

十分にセキュアなクラウドは、重大なビジネスと IT のメリットを次のようにもたらします。

- **価値を生み出すまでの時間を短縮:** セキュリティーのインストールおよび構成が済んでいるため、チームによるリソースのプロビジョニング、ユーザー・エクスペリエンスの迅速なプロトタイピング、結果の評価、必要に応じた繰り返しが容易になります。
- **設備投資の削減:** クラウドのセキュリティー・サービスを使用すると、サーバー、ソフトウェアのライセンス、アプライアンスを含む多くの初期費用を除外できます。
- **管理上の負担の緩和:** クラウド・プラットフォームで信頼を無事に確立および維持することで、適切なセキュリティーを提供するプロバイダーは、レポートとリソースのメンテナンスのコストを削減し、管理上の負担が最善であると見なします。

詳細情報

クラウド・セキュリティーの 5 つの重要分野と、関連する IBM のテクノロジーとサービスについては、次のサイトをご覧ください。
ibm.com/cloud/security

最新情報をお伝えします

IBM クラウド ブログ

フォローする

@IBMcloud
Facebook

連絡先

LinkedIn
YouTube

IBM Corporation
1 New Orchard Road
Armonk, NY 10504-1722

Produced in the United States of America, January 2018

[1]『Insider Threat 2018 report』2017 年 11 月発行
http://crowdresearchpartners.com/portfolio/insider-threat-report