クラウド・セキュリティーに関する 5 つの重要な質問

クラウドベースのデータとアプリは、従来の企業の境界外にあり、新しい保護方法を必要とします。必要なものすべてがプロバイダーにあることを 確認しましょう。

ID とアクセスの管理

1. 貴社のクラウド・プラットフォームは当社の ID 管理システムを統合するか、信頼できる別の方法を提供できますか?

クラウド・プラットフォームとのやり取りでは、誰または何(管理者、ユーザー、またはサービス)がやり取りを行っているのかが最初に検証されます。次のことを常に同じ方法で実施するプロバイダーを見つけてください。

- クラウド・プラットフォームにアクセスするユーザーを識別および認証する
- クラウドでホストされているアプリのエンドユーザーを識別および認証する
- API アクセスとサービス呼び出しの ID を認証する
- 既存の ID アクセス管理 (IAM) システムをクラウド・プラットフォームに統合する

IBM Cloud™ の開発者は **アプリ ID** を使って、モバイル・アプリと Web アプリに自動認証を組み込むことができます。

セキュアなインフラストラクチャー

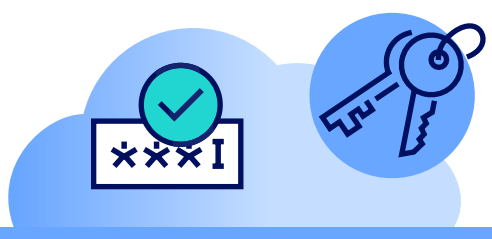
2. 貴社のクラウド・プラットフォームはワークロードに基づいて適切に統合されたファイアウォール、信頼できるコンピュート・ホスト、マイクロセグメンテーションのオプションを提供していますか?

- **セキュリティー・グループとファイアウォール**—ネットワーク・ファイアウォールは境界の保護、インスタンスレベル・アクセス用のネットワーク・セキュリティー・グループの作成に必要不可欠です。
- **マイクロセグメンテーション**—一連の小さいサービスとしてアプリケーションをクラウドネイティブに開発することは、セキュリティー上の利点になります。ネットワーク・セグメントを使ってこれらのアプリケーションを隔離できるからです。
- **信頼できるコンピュート・ホスト**—measure-verify-launch (評価-検証-開始)プロトコルによるハードウェアベースのホスト・セキュリティーは、ワークロードの実行に対して優れた保護を提供します。

IBM Cloud Secure Virtualization および IBM Cloud 信頼コンテナーを使用するコンテナー・アプリを備えた信頼できるプラットフォームに仮想化ワークロードを展開しましょう。

データの暗号化とキー管理

3. 貴社のプラットフォームでは、Bring Your Own Keys がサポートされていますか?



Bring Your Own Keys (BYOK) モデルにより、暗号化キーを中央で管理でき、キー管理システムの境界からルート・キーが絶対に流出しないようにし、キー管理ライフサイクルを監査できます。

IBM Cloud は **IBM Cloud Key Protect** サービスにより、データ暗号化への BYOK サポートを実現します。

アプリケーション・セキュリティー

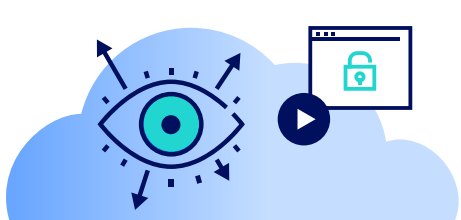
4. 脆弱性を見つけるために、コンテナー化アプリをどのくらいの頻度と範囲でスキャンしますか?

DevOps チームはセキュリティー・チェックの自動化が必要です。レジストリー画像と実行中のコンテナーの潜在的な脆弱性を検出するために、継続的なスキャンを実行する統合ツールを利用することが求められます。

IBM Cloud Container Service の **Vulnerability Advisor**は、静的およびライブ双方のコンテナー画像スキャンを実行できます。

可視性とインテリジェンス

5. 貴社のセキュリティー・ログとレポートは、複数の可視性ポイントを反映し、顧客の SIEM と統合していますか?



組み込みのクラウド・アクティビティ・トラッカーは API、Web、モバイル・アクセスなど、プラットフォームとサービスへの全アクセスを自動的に記録し、追跡できます。企業はこれらのログを自社のセキュリティー・インテリジェンスおよびイベント監視 (SIEM) システムに統合して、環境を 360 度把握することができなければなりません。

IBM® QRadar® は包括的な SIEM 製品です。企業のニーズに合わせて拡張可能な、一連の AI 搭載セキュリティー・インテリジェンス・ ソリューションを提供します。

クラウド・セキュリティーの質問について他の回答をお探しですか?
それなら、**ibm.com**/cloud/security をご覧ください。

39013839-JPJA-00