DNP

クラウドワークロードセキュリティ
パート１：知っておくべきこと

クラウドの活用が急増している中、セキュリティ関係者は、発展するクラウドセキュリティパラダイムに沿ったソリューションをこれまで以上に模索しています。進化する脅威と高度化するサイバー攻撃が毎日報告されていることを考えると、クラウドに展開した重要なワークロードを保護するため、適切な制御を備えた明確な戦略を立てる必要があることは明らかです。

クラウドセキュリティ戦略を開発する際に考慮する制御とカテゴリは、クラウドの展開だけでなくワークロードのセキュリティも左右する可能性があります。これらの制御を理解して特定する一助としてIntezer 社は本ブログシリーズを作成しました。あなたが選択したクラウドプラットフォームにそれらを実装するガイドラインとしてもお役立てください。

このシリーズでは、主要なクラウドプラットフォームである Azure、AWS、GCP が提供するセキュリティツールとサービスやサポートする制御について説明します。また、各プラットフォームのセキュリティ機能の成熟度を調査し、最後に各サービスの完全比較を行います。

このパート１では、次の領域について詳しく説明します。

- クラウドセキュリティ戦略を開発する際に、何に焦点を当てる必要があるか。
- それぞれの関連性とともに、どんなセキュリティ管理策を考慮すべきか。
- 最後に、これらの制御を実装する最良のアプローチは何か。

クラウドのセキュリティ：何に焦点を当てるべきか？

ワークロードをクラウドに展開する際に、クラウドのセキュリティ制御を絞り込むのは通常大変なことだと感じます。可能性のある攻撃に注意しながらセキュリティを最大化することも非常に重要です。そして、攻撃発生時の軽減計画を備えることも重要です。バランスの取れた取り組みが大切で、一方の領域に焦点を合わせ、もう一方の領域を無視すると、クラウドのワークロードが脆弱になり、公開されることになります。

最大領域をカバーする成熟したクラウドセキュリティ戦略を開発するために、考慮すべき主要分野を調べてみましょう。

©2021 Dai Nippon Printing Co., Ltd. All Rights Reserved.

攻撃対象領域を減らす

攻撃対象領域を理解し、そのサイズの縮小させることで、クラウドセキュリティが確保されます。つまり、攻撃の可能性を効果的に減らすことができます。これを実現するのに実装できる制御には、接続されたネットワークのセグメンテーション、パッチ管理、ランタイム脆弱性管理、およびコンテナイメージスキャン等です。また、アプリケーションのライフサイクルの早い段階で必要なセキュリティ対策を組込み、DevSecOps プラクティスに合わせる必要があります。

継続的な保護のためにセキュリティ戦略を調整するには、継続的な監視と最適化が不可欠であることに注意してください。これはセキュリティチームの責任のみならず、環境にアクセスして使用するすべての人、つまり開発者、DevOps エンジニア、監視チームなどに責任があります。継続的な取り組みを行っても、攻撃対象領域を完全に排除することは実際には不可能かもしれません。したがって、より実用的なアプローチとして、違反の検出と対応に焦点を当てることによって、可能な限りそれを最小限に抑えることです。

攻撃/侵入を検出する

侵入の検出に時間がかかるほど、被害は大きくなります。したがって、クラウドセキュリティ戦略を成功させるには、最初の攻撃から検出までの時間を最小限に抑えることです。

また、疑わしく見えない孤立したイベントは、環境内の他のイベントと相関している場合、検出されない攻撃を示している可能性があることにも注意してください。たとえば、コンピューティング環境で実行されている新しいプロセスと相関する場合のサーバ間の通信増加は、攻撃者が侵害された VM /コンテナからネットワーク内のコンポーネントへの横方向のアクセス取得に関連している可能性があります。

包括的な検出を行うには、ネットワークレベルおよびコンピューティングリソースレベルで機能するサービスを利用する必要があります。また、脅威は日々進化しているため、脅威/攻撃のベースラインデータベースを最新の脅威情報に更新してください。

攻撃に対応する

パズルの最後のピースは、効果的な脅威対応戦略を通じて、検出から完全な回復までの時間を最小限に抑えることです。また、実際の脅威と誤警報を調査して区別する必要があります。これには、監視ツールとログによってキャプチャされた攻撃ベクトル情報の詳細な分析を意味します。そして、アラートと統合した webhook や自動化スクリプトなどの自動修復機能が、防御の最前線を作成するのに役立ちます。

©2021 Dai Nippon Printing Co., Ltd. All Rights Reserved.

アダプティブチューニングを通じてセキュリティ戦略を強化するには、攻撃とその後の軽減策から学んだことをフィードバックする必要があることを忘れないでください。

クラウドセキュリティの制御とカテゴリ

ID およびアクセス管理、データ保護、アプリケーションセキュリティなど、前のセクションで説明した 3 つの戦略に組み込まれている他の要素があります。しかしながら、これらの制御はかなり標準的であるか、アプリケーション固有であるため、このブログではフォーカスしません。

代わりに、これまでに説明したクラウドセキュリティ戦略の実用的な実装方法に移りましょう。

このプロセスは、さまざまなセキュリティ制御とカテゴリにマッピングできます。最も顕著なものには、ワークロードのネットワーク境界、ベストプラクティスに従った構成の管理、ランタイム保護メカニズム、適切な CWPP ソリューションの選択、信頼性の高い SIEM ソリューションの統合などがあります。

これらのカテゴリとコントロールについては、以下で詳しく説明します。

ネットワーク

ネットワークのセグメンテーション

従来のオンプレミスネットワークと比較して、クラウドネットワークは SDN に基づいており、マイクロセグメンテーションを実施するための優れたレベルの柔軟性を提供します。さまざまな仮想ネットワークを使用した基本的な分離、コンテナワークロードのポリシーベースのセグメンテーション、ワークロード層のセグメンテーションなどの手順は、東西トラフィックを制限するのに役立ち、焦点を絞ったセキュリティポリシーを適用するための明確な境界も作成します。

たとえば、ネットワーク層の境界とポリシーは、未知の IP や公開されている既知のポートを標的とする攻撃からの保護に役立ちます。ただし、アプリケーション層で発生するより複雑な攻撃では、これらの境界を対象としたアプリケーションコンポーネントとポリシーのセグメンテーションが必要です。

Web アプリケーションファイアウォール

クラウドでホストされているアプリケーションは攻撃を受けやすいため、高度な保護レイヤーを構成する必要があります。クラウドサービスプロバイダーが提供する Web アプリケーションファイアウォール（WAF）は、既知の脆弱性やエクスプロイトに対してアプリケーション層で包括的な保護を提供するため、ここで検討できます。OWASP の攻撃検出ルールに基づく WAF は 、インジェクション（SQL、NoSQL、OS、LDAP）、機密データの公開、セキュリティの設定ミス、XSS の欠陥、認証とアクセス制御の破損など、一般的なアプリケーションのセキュリティリスクを検出して保護するのに役立ちます。

©2021 Dai Nippon Printing Co., Ltd. All Rights Reserved.

DDoS 保護

組織化された DDoS 攻撃は、クラウドアプリケーションを数秒でダウンさせることが出来ます。これらの攻撃は、クラウドプラットフォームやプラットフォームにホストされている特定のワークロードを標的にすることがあります。従って、マルチレイヤーDDoS 保護アプローチは避けられず、プラットフォームから開始して、アプリケーションレイヤーまで保護を提供すべきです。すべての主要なクラウドサービスプロバイダーには、プラットフォーム攻撃から保護し、必要な軽減策を講じるためのネイティブ機能が組み込まれています。

これに加えて、特定の IaaS / PaaS サービスに焦点を合わせた構成可能な DDoS 保護サービスも検討する必要があります。サービスの望ましい特性には、構成可能な軽減ポリシーと自動化された軽減サービス、および攻撃への洞察を提供する豊富な分析サービスが含まれます。

クラウドセキュリティ ポスチャマネジメント（CSPM）

多くの場合、サービスの構成ミス、手動エラー、または管理ミスが、クラウドワークロードへの攻撃成功の根本原因です。CSPM ソリューションは、構成の誤りがないかクラウド展開を継続的に監視し、逸脱があれば報告して、必要な是正措置を実装できるようにします。このコントロールプレーンビューは、多くの場合、クラウド環境のセキュリティスコアを使用して定量化され、クラウド環境のセキュリティ体制の概要を提供します。

主要なコンプライアンス標準に準拠したデフォルトのセキュリティポリシーに加えて、効果的な CSPM ソリューションにより、業界動向やビジネス要件に特有なカスタムセキュリティポリシーを定義することもできます。CSPM ソリューションは、組織のセキュリティポリシーからの逸脱を報告するだけでなく、修復手順を推奨したり、それらを実装したりすることもできます。CSPM ソリューションの範囲は、VM、ネットワーク、ストレージ、PaaS サービス等のクラウドサービスランドスケープ全体をカバーし、コンテナ環境やサーバーレス環境にも拡張する必要があります。

継続的なリスクとコンプライアンスの評価とレポートの機能は、攻撃対象領域を減らす上で重要な役割を果たし、CSPM をクラウドセキュリティ戦略の不可欠な部分にします。

脆弱性管理

リアルタイムの脆弱性スキャンおよび修復メカニズムは、オンプレミスと同様にクラウドでも重要です。クラウドでのマイクロサービスの成長を考慮すると、脆弱性検出および管理ツールは、コンテナランタイムスキャン、CI / CD パイプラインとの統合などのオプションを通じて、コンテナ化された環境を保護

©2021 Dai Nippon Printing Co., Ltd. All Rights Reserved.

しなければなりません。理想的には、脆弱性についてワークロードを継続的に分析し、レポートを生成し、ダッシュボードに結果を表示し、可能な場合はいつでも脆弱性を自動修正すべきです。

Windows マシンと Linux マシンの両方への体系的なパッチ管理プロセスは、オペレーティングシステムの攻撃対象領域を減らすのに役立ちます。クラウドプラットフォームまたはサードパーティの統合で利用可能な組み込みのパッチ管理ソリューションを活用して、これを実現することもできます。報告された脆弱性と完了した軽減手順、および実行されたパッチサイクルをカバーする包括的なレポートは、ほとんどの監査のコンプライアンス基準を満たすために必要なセキュリティコンプライアンスの履歴ビューを維持するのに役立ちます。

クラウドワークロード保護プラットフォーム（CWPP）

脅威アクターがクラウドに移行し、複雑な攻撃方法を採用するにつれ、セキュリティの焦点は、オンプレミスシステムで使用される厳格なパラメーターから、より進化したワークロード中心のアプローチに移行しなければなりません。違反を検出して報告するアプローチは全体論的である必要があり、クラウドワークロード保護プラットフォーム（CWPP）がワークロード中心のセキュリティアプローチを支援する場所です。CWPP ソリューションは、セキュリティ体制に関する包括的な洞察を提供するエージェントの助けを借りて、デプロイしたリソース（VM、コンテナ、機能など）を監視するように設計されています。

アプリケーションはハイブリッド環境またはマルチクラウド環境にまたがることができ、CWPP ソリューションはそれらに単一ペインの可視性と保護を提供します。CWPP 機能には、違反/脅威の検出、システムの整合性の保証、サービスの強化、アプリケーション制御、およびメモリ内保護が含まれますが、これらに限定されません。シグネチャ・ベースのマルウェア対策スキャンプログラムは、クラウドワークロード、特に Linux でホストされているワークロードにとっては時代遅れなアプローチの可能性があります。したがって、CWPP は、高度な脅威検出方法と組み込みのアプリケーション制御機能を追加で提供する必要があります。CWPP 脅威検出戦略は、従来のアプローチを一歩超えて、コンピューティングリソースで実行されているすべてのコードが信頼できるソースからのものであることを保証します。不正または悪意のあるコードの実行は、ツールの脅威検出機能によって識別されます。

従来、Linux は「デフォルトで安全な」OS と見なされていました。ただし、Linux やクラウド環境を標的とする Doki や IPStorm のような脅威は、検出されないセキュリティの抜け穴（脆弱なプラグインやパッチが適用されていないソフトウェアを含む）とともに、Linux システムをクラウドでも同様に脆弱にします。従来のセキュリティソリューションは主に Windows での脅威の検出に重点を置いていますが、CWPP ソリューションは、Linux のセキュリティ管理と脅威検出に特化して、決定的な付加価値をもた

©2021 Dai Nippon Printing Co., Ltd. All Rights Reserved.

らす必要があります。

コンテナセキュリティ

コンテナのセキュリティには、コンテナの保護だけでなくオーケストレーションが含まれ、クラウドで最も人気のあるものは Kubernetes（K8s）です。ほとんどのクラウドサービスプロバイダーはマネージド K8s サービスを提供していますが、コントロールプレーンにアクセスする必要がある場合は、独自の K8s クラスターをデプロイすることも選択します。

業界標準のセキュリティベースラインは、K8s クラスターとコンテナに対して定義し、それらの標準に対して継続的に監視し、逸脱を報告しなければなりません。コンテナ特権アクセス、疑わしいソースからの API アクセス、Web シェル検出など、コンテナまたはホストレベルでの悪意のあるアクティビティは、リアルタイムで報告し、根本的なセキュリティ上の欠陥を分析する必要があります。この機能は、多くの場合、CWPP ソリューションの一部として含まれています。

コンテナイメージスキャン機能は、イメージがコンテナレジストリにプッシュされる前に、イメージの脆弱性を識別してフラグを立てることにより、攻撃対象領域を減らすのにも役立ちます。これを実現するために、お客様はクラウドサービスプロバイダーが提供するネイティブコンテナツールを活用して、セキュリティベースラインの監視と画像スキャンを行うことができます。ネイティブツールが利用できない場合は、サードパーティのツールを利用して同じことを行うことができます。

セキュリティ情報イベント管理（SIEM）

クラウドネイティブの SIEM は、クラウドとオンプレミスの両方で、複数のソースからクラウドスケールで関連するログと信号を収集するのに役立ちます。その後、迅速に脅威を分析、検出します。SIEM ツールは、デプロイされている場所に関係なく、アーキテクチャの異なるコンポーネントからのデータを相互に関連付けるのに役立ちます。これは、脅威の検出と対応の強化に役立ちます。

理想的にはこれらのツールは、複数のデータソースとのネイティブ統合を提供し、修復アクティビティの API ベースの自動化を提供すべきです。ほとんどの SIEM ツールは、悪意のあるイベント、データの異常、ネットワークへの侵入などの頻度を簡単に報告および可視化するのに役立つ豊富な視覚化機能も提供します。

追加の脅威検出機能

CWPP ソリューションによって提供されるセキュリティ範囲に加えて、組織は、高度な脅威の検出および保護機能を提供するクラウドサービスプロバイダーからのサービスも検討する必要があります。ここ

©2021 Dai Nippon Printing Co., Ltd. All Rights Reserved.

でのサービスの範囲は、アプリケーション、コンピューティングリソース、データリソースのさまざまなレイヤーと、クラウドコントロールプレーン、ネットワークトラフィック、キー管理ソリューションなどのサポートサービスレイヤーをカバーする必要があります。対象となるシナリオの例としては、疑わしいログインとアクティビティの特定、管理者のアクティビティログの監視、不正なユーザーを検出するための使用パターンの確認などがあります。

利用可能なセキュリティログと監視

すべての主要なクラウドプロバイダーは、関連するサービスシグナルの包括的なログオプションを提供しています。コントロールプレーンとデータプレーンの両方のログを分析、監視して、エンドツーエンドのセキュリティを確保する必要があります。これらのログには、サービスアクティビティログ、ネットワークフロー、IAM ログ、データの入力/出力ログなどが含まれ、調査を行う際の重要な要素になります。

まとめ

クラウドセキュリティの保証は目的地ではなく、ワークロードが成熟するにつれて継続的な最適化を必要とするものです。このブログで説明されているコントロールは、初期のクラウドセキュリティ戦略を定義し、クラウドワークロードを保護するプロセスを加速するために必要なベースラインを提供します。追加の参考資料と推奨読み物を以下にリストします。

参考資料

クラウドセキュリティの姿勢管理：なぜ今それが必要なのか
https://cloudsecurityalliance.org/blog/2019/10/01/cloud-security-posture-management-why-you-need-it-now/

ポスチャー管理：違反をきっかけにクラウドセキュリティツールが台頭
https://www.cio.com/article/3529426/posture-management-cloud-security-tools-rise-in-wake-of-breaches.html

クラウドは安全ですか？
https://www.gartner.com/smarterwithgartner/is-the-cloud-secure/

AWS、Azure、および GCP は、市場をリードするクラウドプラットフォームであり、セキュリティ制御の実装に役立つ多数のネイティブソリューションとサービスを提供します。高度な SIEM 機能またはインメモリ検出やランタイムスキャンなどの脅威検出機能では、ネイティブ機能と一緒にサードパーテ

 ©2021 Dai Nippon Printing Co., Ltd. All Rights Reserved.

ィのソリューションを使用する場合があります。このシリーズの今後の投稿で、このようなツールについて詳しく説明し、これらのクラウドサービスプロバイダーについて説明し、それらの機能を包括的に比較します。

＜原文＞

Intezer Brog

Cloud Workload Security: What You Need to Know - Part 1 (14 October 2020)

https://www.intezer.com/blog/cloud-workload-security-what-you-need-to-know-part-1/

本稿は，Intezer 社ブログを翻訳して作成した。翻訳を許諾いただいた Intezer 社に感謝します。

日本語版作成：2021 年 3 月

©2021 Dai Nippon Printing Co., Ltd. All Rights Reserved.