ホワイトペーパー

包括的なセグメンテーションで AWS のワークロードを保護 — よりシンプルで迅速なセキュリティ

はじめに

セキュリティを理由にクラウド導入をためらう必要はありません。AWS のアセットとリソースに対する可視性、ラテラルムーブメントの防止、セキュリティ侵害の検知と応答を、1 つのソリューションで対応できます。

Amazon Web Services（AWS）で Platform as a Service（PaaS）リソースを使用し、重要なワークロードをオフプレミスに移行することの利点は明らかです。インフラのコストやメンテナンスの手間が省け、ほぼ無限のリソースとパワーでスケーラビリティと弾力性を向上でき、機械学習や AI などの最新のイノベーションを活用して、パフォーマンスと分析能力を高めることができます。しかし、多くの企業が、セキュリティ上の懸念から導入を躊躇しています。とりわけ、クラウドリソースがサイバー攻撃の最大の標的になっていることが理由として挙げられます。

AWS におけるセキュリティの課題

まったく新しい環境を検討する場合、セキュリティを最初から再確認する必要があることは意外ではありません。クラウドをこれまで利用していなかった場合や、別のベンダーから移行する、新しいハイブリッドソリューションを選択した場合、既存のエコシステムに AWS を追加する場合が考えられます。いずれにしても、クラウドを導入する場合は、クラウドというインフラがもたらす固有の課題に対応するため、クラウド独自のツールセットが必要となります。すべてのクラウドベンダーに共通する要因もありますが、Microsoft Azure、Google Cloud Platform（GCP）、AWS に固有の要因もあります。AWS テクノロジーを含むクラウドまたはハイブリッドクラウドを使用している企業の主な懸念事項を以下に示します。

責任分担についての理解：ワークロードを AWS に移行する際、または AWS に組み込まれた PaaS リソースを活用する際には、多くの責任を負うことを認識する必要があります。顧客データ、アプリケーション、プラットフォームを保護する必要があります。Gartner は、2025 年にかけてクラウドにおけるセキュリティインシデントの 99% がクラウド利用者側の落ち度が原因で発生すると予測していますが、その根拠としているのが責任分担モデルに対する理解不足です。

可視性の欠如：把握できないものは制御できません。クラウドでは、可視性がはるかに複雑になります。特に、水平方向（East／West）と垂直方向（North／South）に移動するネットワークトラフィックの保護と可視化にあたっては複雑さが顕著です。フローを見るだけでは不十分です。重要な資産が複数の AWS アカウント、コンテナ、またはネットワーク・セキュリティ・グループに分散して存在していることがあります。このような資産がどこに存在しているかを含め、資産に関するあらゆる情報を的確に把握しなければ、フローや相互依存関係を正確に理解できない可能性があります。

ポリシー作成の制御が限定的：オンプレミスでレイヤー 7 のレベルでの知見を獲得できている企業であれば、ワークロードをクラウドに移行したとたんにレイヤー 4 レベルでの可視性しか得られない状態に逆戻りし、今まで手にしていた詳細な知見やきめ細かな制御機能を失うのは望ましくないでしょう。Amazon のセキュリティグループでは、レイヤー 4 までのトラフィックの制御がサポートされています。しかし、基盤となるインフラにかかわらずレイヤー 7 のレベルでの可視性と制御を手にできれば、ポートと IP にのみ頼る場合と比べてはるかに有用な知見を手にし、確実な制御を実施できます。多くの場合ポートと IP のみに頼っていたのではセキュリティ侵害の検知やトラブルシューティングを行うことができません。

コンテナのセキュリティ：AWS では、Amazon セキュリティグループを使用してコンテナのセキュリティポリシーを適用しますが、このポリシーはクラスターのレベルでしか適用できず、個々のポッドのレベルでは適用されません。通信の内容を完全に把握するためには、物理的なインフラ上で実行されているオーバーレイネットワークのコンテキストを認識し、ポッドレベルまで詳細にドリルダウンできるソリューションが必要です。仮想マシン（VM）とコンテナの両方を含むネットワークポリシーを作成する場合は設定や管理がさらに複雑になり、多くの場合、セキュリティ制御の仕組みを 2 種類用意しなければならなくなります。

PaaS の導入：クラウド中心の組織が抱えるニーズの拡大に伴い、重要なワークロードをクラウドに移行するだけでなく、PaaS リソースを採用するという傾向が顕著になっています。しかし、これらの PaaS リソースはエージェントをサポートできません。そのため、ほとんどのエージェントベースのセキュリティソリューションは限定的すぎ、PaaS リソースに完全な保護を拡張することはできません。これによって、クラウド・セキュリティ・ポリシーが断片化され、チームのオーバーヘッドが増加し、攻撃者に悪用されるセキュリティギャップが残ってしまう可能性があります。

オールインワンのセキュリティプラットフォームでこれらの問題に対処

Amazon には、Amazon セキュリティグループなどの組み込みのツールが用意されており、これらを使用することでインフラをクラウドに移行する際に生じるいくつかの課題に対処できます。AWS を利用する組織には、グループを使用して権限を割り当て、認証情報を定期的にローテーションし、アイデンティティアクセス管理（IAM）グループを利用して簡略化を図るなど、AWS IAM を最大限に活用することをお勧めしています。しかし、パブリッククラウドがさまざまな形で利用されるようになっている現在、特にレガシーインフラからコンテナテクノロジー、そして様々なパブリッククラウド環境で利用されている PaaS リソースなど、全てをカバーするハイブリッド環境を検討している場合にあっては、このようなツールだけでは単なる足掛かりにしかなりません。

ハイブリッド環境においても、盲点を取り除き、他のセキュリティスタックとシームレスに連携できるテクノロジーで AWS の機能を補完できる、高度なセキュリティソリューションが必要です。Akamai が提供するサービスをご紹介します。

AWS インスタンスの完全な可視性

IT インフラの複雑性が高まるにつれて、自動的に深いレベルの可視性を実現できる仕組みがますます重要となります。手動による移動、追加、変更、削除は、信頼性が低くギャップやエラーが発生しやすいだけでなく、速度が低下するため、クラウド導入の妨げとなります。一方、自動化により優れた可視性を手にすることができれば、あらゆるアプリケーションやフローを検出して、個々のプロセスのレベルに至るまでインスタンスの可視化を実現できます。

Akamai Guardicore Platform for Zero Trust の 中核である Akamai Guardicore Segmentation には、オーケストレーションデータを取得する強力な AWS API と、アセット、フロー、タグ情報を収集する専用コンポーネントを備えているため、ラベリングやアプリケーションマッピングに使用できる貴重なコンテキストが得られます。インフラのベースライン測定を通して、アプリケーション相互でどのように通信が行われ、どこに依存関係が存在し、スムーズでアジャイルな運用のためにはどのようにポリシーを作成すればよいかをしっかりと把握するのに必要な詳細情報を手にすることができます。ユーザーは、クラウドベンダーや環境ごとに個別のセキュリティソリューションを用意するのではなく、ネイティブクラウド情報と AWS 固有のデータをすべて同じダッシュボードに表示できます。Akamai のソリューションはあらゆるプラットフォーム、インフラ、クラウドをカバーできるため、環境全体をくまなく可視化できます。

セグメンテーションと適用 - ワークロードに沿って機能する単一のポリシー

すべての環境をカバーするこの「単一画面」ビューを手にしたら、セキュリティポリシーの設計と展開の作業に取り掛かることができます。アプリケーション認識型ポリシーを使用すると、Amazon セキュリティグループで実現できるレイヤー 4 のレベルにとどまらず、レイヤー 7 でのきめ細かなセキュリティを実現できます。ラテラルムーブメントを制限するためにオンプレミスで次世代ファイアウォールの使用を試みる組織もありますが、このようなファイアウォールでは水平方向（East／West）のトラフィックのおおまかなセグメンテーションしかサポートされません。この方法では、ファイアウォールを通じてトラフィックを再ルーティングするためにインフラおよびネットワークの大規模な変更が必要となるため、セグメンテーションによるきめ細かな制御のソリューションとして使用するのは非常に困難です。オンプレミスでは実現できたとしても、このレベルの制御をクラウドでも行うのは至難の業と言えます。

そこで登場するのが、基盤となるネットワークインフラの変更を一切必要としない、動的なワークロードのためのポリシーを備えたレイヤー 7 のマイクロセグメンテーションです。ポリシーはワークロード自体に沿って機能するため、手作業でインフラなどを変更する必要がありません。そのため組織のアジリティを高め、変化の速い DevOps プロセスへも問題なく対応することができます。1 つのマイクロセグメンテーションポリシーで、一貫性のある単一のポリシー表現を使用して、リージョン、VPC、コンテナ、VM、オンプレミスなどにルールを適用することで、ハイブリッド環境をシンプル化することができます。提供される高い可視性をもとに、セグメンテーションポリシーをわずか数分で定義して適用できます。ポリシー作成プロセスは、パブリッククラウド上でクラス最高のセキュリティプロトコルを提供する自動ポリシー推奨によっても強化されます。

AWS クラウドでのセキュリティ侵害の検知とインシデント対応

Akamai を活用することで、セグメンテーションや可視性だけでなく AWS セキュリティをさらに強化できます。ポリシー違反の検知は、セキュリティ侵害検知の重要な部分であり、アプリケーションレベルの詳細情報を使用して、潜在的なサイバー脅威にリアルタイムで対応できます。ハイブリッドクラウド環境で悪性の活動を即座に警告できるように、以下のような複数のセキュリティ侵害検知方法が提供されています。

- **レピュテーション分析：**ドメイン名や IP アドレスからファイルハッシュやコマンドラインまで、フロー内の疑わしい情報を自動的に検知
- **動的ディセプション：**攻撃者に気づかれないようにして、高インタラクションのハニーポット環境に攻撃者を誘導し、攻撃者のふるまいを安全に観察
- **インシデント対応を迅速化するツール：**AWS との統合により、ポリシー違反やセキュリティインシデントを AWS Security Hub にリアルタイムで送信
- **カスタム脅威ハンティング：**Akamai Hunt サービスを活用することで、Akamai のインフラと膨大なグローバル脅威インテリジェンスを活用し、ハイブリッドクラウド環境での非常に発見しにくい脅威をも阻止

すべてを統合することで、 AWS とその先のセキュリティを強化

パブリッククラウドの利点を享受するからといって、必ずしもオンプレミスよりも低いセキュリティ、可視性、制御で妥協する必要はありません。Akamai を活用することで、AWS アセットとリソース、さらにインフラ全体を完全に可視化できます。この基礎となるマップを使用することで、ポリシーの作成がシームレスになり、既存のセキュリティ対策が強化され、手動サポートを必要とせずにきめ細かな制御が可能になります。侵害検知とインシデント対応も加わって、AWS クラウド上とそれ以外を含めた全ての領域をカバーする、単一のエンドツーエンドのセキュリティソリューションが実現します。

その他の詳細については、akamai.com/guardicore をご覧ください。

Akamai のセキュリティについて

Akamai のセキュリティは、パフォーマンスや顧客体験を損なうことなく、ビジネスを推進するアプリケーションをあらゆる場面で保護します。当社のグローバルプラットフォームの規模と脅威に対する可視性を活用して、お客様と Akamai が提携し、脅威を防止、検知、緩和することで、ブランドの信頼を構築し、ビジョンを実現できます。Akamai のクラウドコンピューティング、セキュリティ、コンテンツデリバリーの各ソリューションの詳細については、akamai.com および akamai.com/blog をご覧いただくか、X（旧 Twitter）と LinkedIn で Akamai Technologies をフォローしてください。公開日：2024 年 11 月。