AKAMAI ソリューション概要

Akamai Guardicore Segmentation による Kubernetes の可視化とセキュリティの確保

Kubernetes（K8s）は、クラウドネイティブのデータセンターでアプリケーションの展開と管理を行うために最も広く採用されているテクノロジーの 1 つであり、かつてないスピードと柔軟性を実現します。Gartner 社によると、2026 年までに世界的企業の 90% がコンテナ化されたアプリケーションを運用するようになると予測されています。これは 2021 年の 40% から増加しています。さらに、2026 年までには、すべてのエンタープライズアプリケーションの 20% がコンテナで実行されるようになる見込みです。これは、2020 年の 10% 未満から増加しています。[1] このプラットフォームの人気の高まりは、ユーザーのみならず攻撃者をも引き寄せており、セキュリティチームは当初身構えていなかった課題に直面しています。

新たなテクノロジーとセキュリティ上の課題

K8s クラスターは、DNS サービス、負荷分散、ネットワーキング、自動拡張に加え、アプリケーションの実行に必要なその他の機能を含む完全なエコシステムを提供します。K8s は、エンタープライズ組織が迅速なイノベーションとコスト削減の両方を達成できるようにしているため、当然ながらこうした幅広い導入を視野に入れています。一方で、K8s の魅力となっているそうした特性により、セキュリティの確保が困難になります。

K8s はフラットなネットワークであるため、各ポッドはクラスター内の他のポッドと通信できます。攻撃者は最初のデータ侵害で、ラテラルムーブメント（横方向に移動）し、接続されているすべてのデータセンターにアクセスできるようになります。これは典型的なランサムウェア攻撃プロセスですが、別の攻撃ベクトルでも同じ戦略を簡単に活用できます。

300 超の DevOps、エンジニアリング、セキュリティの専門家を調査対象とした 2022 Red Hat State of Kubernetes Security Report によると、回答者の 93% が、過去 12 か月間に K8s 環境で 1 件以上のセキュリティインシデントを経験しており、中には収益や顧客の損失につながっているケースもあります。

ソリューションとしてのマイクロセグメンテーション

アプリケーション展開自体の K8s の概念は異なっており、異なるセキュリティ方式が必要です。セキュリティチームは、既存のセキュリティソリューションを「リフト & シフト」し、こうした新しいテクノロジー上で動作することを期待するだけでは不十分です。K8s クラスターのセキュリティを保護するためには、K8s ネイティブの方法で実行する必要があります。

そのため Akamai は、K8s クラスターのセキュリティ保護に特化したソフトウェアベースのセグメンテーションソリューションを提供しています。このソリューションは、レガシーシステム、クラウド、オンプレミスワークロード、コンテナなど、環境内の他のワークロードに対しても同様に動作します。そのため、1 つの画面で企業全体のアセットを可視化、セキュリティ保護、管理できます。

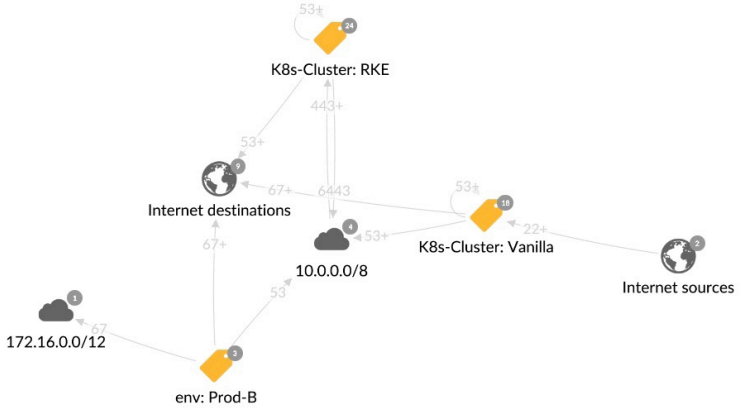
メリット

- 他のアセットと同じ画面とプロセスで、K8s クラスターを可視化、強化、監視
- K8s の脆弱性を悪用する高度な攻撃から簡単に保護
- ポッド、サービス、ホスト、名前空間のすべての接続のリアルタイムおよび履歴ビュー
- すぐに使えるテンプレートで、K8s クラスターを簡単にリングフェンス
- K8s、エンドポイント、オンプレミス、クラウドのワークロードに対する統合コンソールおよびポリシー管理
- クラスターを監視するエージェントの数や Kubernetes オーケストレーションの状態など、デプロイされたクラスター上の運用データを受信

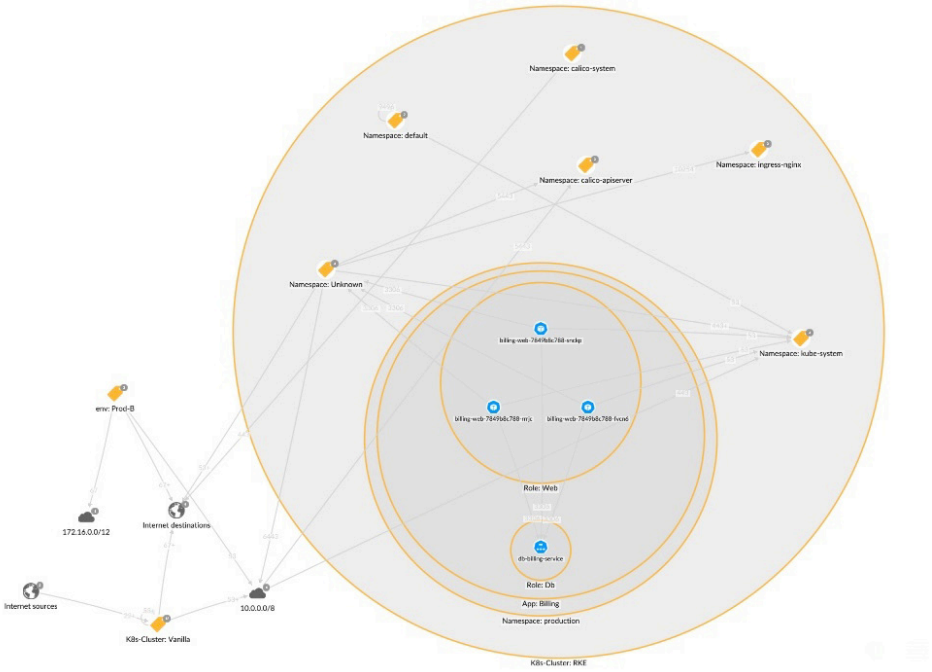
Kubernetes クラスターをセグメンテーションするための主な機能

可視性。Akamai Guardicore Segmentation は、K8s 環境で何が実行されているかを認識し、トラフィックが目的の場所のみに送信されていることを確認する機能を提供します。これは、ポリシーを作成するために不可欠の機能です。

- **相互依存性マップ**：Akamai は、VM、K8s、Docker コンテナなどのあらゆるタイプのテクノロジーについて、社内およびデータセンター間の通信を視覚化するためのマップを提供します。このマップを使用すると、ポッド、サービス、ホスト、名前空間の間の疑わしい接続を可視化して検知できます。
- **ラベル**：複数のラベルレイヤーを使用して、アプリケーションをクラスターに展開する方法を正確に反映したマップです。この可視化では、アプリケーションのマネージャーが計画したように K8s 階層が示されます。こうしたきめ細かなレベルにより、Akamai のユーザーは、クラスターに何が展開されているかや、展開されたアプリケーションとその他のインフラの間のネットワーキングの関係を把握できます。



Reveal（表示）マップに表示されたクラスター。クラスターをダブルクリックすると、名前空間とクラスター内の相互接続が表示されます。



Reveal（表示）マップに、ポッド情報が表示されます

回答者の 93% が、過去 12 か月間に K8s 環境で 1 件以上のセキュリティインシデントを経験しており、中には収益や顧客の損失につながっているケースもあります。

実施：K8s クラスターのアタックサーフェスを最小化するためには、厳密なセグメンテーションポリシーが必要です。セグメンテーション実施ソリューションは、主に次の 2 つの基準に対応する必要があります。拡張性やパフォーマンスを制限することのない、非侵入型である必要があります。また、名前空間、コントローラー、K8s ラベルなど、K8s オブジェクトのすべてのレベルを柔軟にリングフェンスできる必要があります。

Akamai は、ネイティブの Kubernetes Container Network Interface（CNI）を活用しています。CNI は、K8s でネットワークのセグメンテーションを実施するために設計されたネットワーク・セキュリティ・ポリシー・プラグインで構成されています。これは、拡張制限のない非侵入的な方法です。専用テンプレートを使用すると、名前空間、アプリケーション、その他のオブジェクトなど、Kubernetes のビジネス上重要なアプリケーションをリングフェンスできます。

Ring Fence a K8s Application by whitelisting inbound and outbound flows for an application on K8s cluster K8s-Cluster within Namespace

Kubernetes **アプリケーション・リングフェンシング・テンプレート**

高度なモニタリング。高度なロギングと監視システムを使用して、専用のネットワークログを K8s ネットワークに合わせて調整し、イベントごとに宛先サービス、ノード IP、送信元ポートおよび宛先ポート、プロセスを表示します。そのため、ネットワーク内の異常なアクティビティを簡単に調査し、SIEM などのサードパーティー製アプリケーションにデータをエクスポートできます。

サマリー

Kubernetes は、多くのビジネス環境にとって不可欠な要素となっています。Kubernetes は、従来とは異なるアプローチであり、リソース使用効率の向上、開発プロセスの合理化、ポータビリティとスケーラビリティの向上を実現します。ただし、アプリケーション開発のアプローチが異なっていれば、セキュリティに対しても異なったアプローチが必要です。

Akamai Guardicore Segmentation は、1 つのマップでさまざまなタイプの展開（ベアメタル、VM、K8s など）にわたる通信フローを確認できる包括的な単一ソリューションを提供します。このソリューションは、可視性、監視、実施について、非侵入型でスケーラブルな K8s ネイティブのアプローチを提供します。そのため、セキュリティチームと開発チームの負担が軽減され、セキュリティを犠牲にすることなく迅速にイノベーションを進めることができます。

『2022 Red Hat State of Kubernetes Security Report』によると、K8s の導入に関する最大の懸念事項の 1 つはセキュリティであり、アプリケーションの本番環境への展開に遅れが生じ続けています。

詳細については、**akamai.com** または **Akamai** の営業担当チームにお問い合わせください。

1. Gartner 社『The Innovation Leader's Guide to Navigating the Cloud-Native Container Ecosystem』
Arun Chandrasekaran、Wataru Katsurashima、2021 年 8 月 18 日