AWSクラウドとコンテナの保護に関する5つのポイント

コンテナとクラウドの導入が加速する中、企業はコンテナとクラウド環境に関する可視性を確保するのに苦労しています。Gartner社によれば、「クラウドサービスに対する攻撃が成功する原因は、ほぼすべて顧客の設定ミスや操作ミスである」とのことです[1]。

コンテナは基本的にブラックボックスであり、その内部で何が行われているかを見ることは困難です。また、もう1つの問題として、コンテナの寿命が非常に短いことが挙げられます。Sysdig 2022年版クラウドネイティブセキュリティと利用状況レポートによると、コンテナの44%は5分未満の寿命しかありません。従来のセキュリティツールでは、コンテナの内部を見ることができないのはもちろんのこと、動的なKubernetes環境において寿命の短いワークロードを把握することもできません。

アマゾン ウェブ サービス（AWS）環境において、コンテナやクラウドサービスの効率的なセキュリティおよびコンプライアンス管理を自動化するにはどうすればよいでしょうか？Amazon Elastic Kubernetes Service（EKS）、Amazon Elastic Container Service（ECS）、AWS Fargateでワークロードを正常に実行するために必要となる可視性とセキュリティ制御を確保できていますか？クラウドネイティブ環境向けに構築された適切な統合ツール群を使用すれば、AWSアカウント、インフラストラクチャー、ワークロードのすべてについて、クラウドとコンテナのセキュリティリスクを適切に管理できるようになります。

重要なのは、クラウドの設定ミスによるリスクを減らすこと、クラウドとコンテナの脆弱性を継続的にスキャンすること、異常な活動を検知すること、脅威を優先順位付けすること、そしてお使いのアプリケーションがそのライフサイクル全体にわたってセキュアであることを確実にすることです。これら5つの重要なワークフローを通じて、最も重要なセキュリティと可視性の要件をカバーできるようになり、その結果、AWSにおいてコンテナ、Kubernetes、およびクラウドの運用を、自信を持ってセキュアに実行することが可能となります。

[1] Gartner: Innovation Insight for Cloud Security Posture Management

1

AWSクラウドとコンテナの保護に関する5つのポイント

継続的なクラウドセキュリティを実現

設定ミスや不審な振る舞いを即座に特定するためには、継続的なクラウドセキュリティが必要となります。責任共有モデルでは、これらのセーフガードを実装して管理するのはAWSユーザーの仕事となります。自身のクラウドセキュリティポスチャーを判定するには、次のチェックリストが役立ちます。

AWS環境で実行されている資産を自動的に検知できる。これには、システムやアプリケーションをはじめ、Amazon VPC、Amazon RDS、Amazon S3、Amazon ECS、Amazon EKS、AWS Fargateなどのサービスが含まれる。

CIS（Center for Internet Security）のベンチマークに照らしてクラウドの設定を定期的にチェックし、設定ミス（公開ストレージバケット、公開セキュリティグループ、アクセス制御など）を特定し、違反の是正措置を取ることができる。

AWS CloudTrailのログとポリシーを使用して、クラウドのアカウント、ユーザー、サービスにおけるアクティビティを監視することで、サービスの変更、疑わしい振る舞い、潜在的な脅威に対してアラートを発行できる。

Infrastructure-as-codeテンプレートがセキュリティポリシーに準拠しているかどうかをスキャンし、Gitのプルリクエスト（PR）を通じてソースレベルでの自動修復が行える。

クラウドインフラストラクチャーエンタイトルメント管理（CIEM）を通じて、ユーザーとサービスによるクラウドリソースへのアクセスに関する可視性を確保することで、過剰なパーミッションを是正できる。

アプリケーションのライフサイクル全体を通じて一貫性のあるポリシーを適用することで、コンプライアンスとガバナンスを自動化している。

2

AWSクラウドとコンテナの保護に関する5つのポイント

脆弱性の管理：コンテナイメージとホストをスキャンする

コンテナのイメージ、バージョン、ビルドの数が増加すると、どのソフトウェアが使用されているか、必要なソフトウェア更新が適用されているかどうかを制御できなくなる可能性があります。「シフトレフト」型のセキュリティ対策は、お客様のデリバリーパイプラインにセキュリティを組み込むことに重点を置くものです。実際のリスクに基づいて脆弱性を特定し、優先順位付けを行うことで、問題への対処をより早期に行えるようになり、導入のスピードを落とすことがなくなります。脆弱性の管理を実現できているかどうかを判定するには、次のチェックリストが役立ちます。

Amazon ECRなどのレジストリやAWS CodePipelineなどのCI/CDパイプラインにスキャン機能を組み込むことで、リスクのあるイメージが導入されるのを回避している。

自身のセキュリティポリシーに沿うように、Dockerfile命令やイメージ属性（サイズやラベル）のようなビルド構成を検証している。

Kubernetesとクラウドのコンテキストを利用して、問題に対処する適切なチームを特定し、チームにアラートを発行できる。

クラウドアカウント内でイメージをチェックするインラインスキャン機能を採用することで、お使いのイメージに関する完全な制御を維持している。

すでに実稼働中のコンテナに影響を与えるような、新たに報告された脆弱性を特定できる。

CI/CDツールを使って開発者チームに直接通知することで、脆弱性への対処を効率化している。

AWS Fargateのサーバーレスタスクのイメージスキャンを自動化することで、脆弱なコンテナを実行するリスクを低減している。

公開されているイメージと社内で作成したイメージについて、独自のポリシーを設定できる。外部ソースから取得したイメージに対する厳しいチェックを検討している。

Amazon EC2インスタンスをスキャンすることで、OSおよび非OSパッケージにおける既知の脆弱性を特定できる。

3

AWSクラウドとコンテナの保護に関する5つのポイント

ランタイムの脅威を検知し、それに対応する

適切な設定を確実に行い、脆弱性に対処した後でも、ランタイムアクティビティの監視には警戒が必要です。ゼロデイ攻撃や悪意あるアクターが、お使いの本番環境のアプリケーションやデータを脅かす可能性があるからです。ランタイムリスクを低減するためには、クラウドとコンテナ向けに構築された脅威の検知と対応が必要となります。ランタイムの脅威検知・対応を実現できているかどうかを判定するには、次のチェックリストが役立ちます。

AWSのクラウドおよびコンテナサービスにおいて、ワークロードの動作監視、クラウドアクティビティの監視、異常なイベントの特定を行うためのランタイムセキュリティを実装している。

- → Linuxのシステムコールなど、信頼できる真のソースを使って、コンテナの動作を監視している。
- → ワークロードの振る舞いを監視し、クラウドのアクティビティを監視し、異常なイベントを特定するような、ランタイムセキュリティポリシーを作成および維持している。
- → コンテナの役割とKubernetesのコンテキストに基づいたセキュリティポリシーを適用している。
- → AWS CloudTrailのログフィルタリングを自動化することで、予期せぬサービスアクティビティや設定変更を検知できる。

AWS Fargate上のサーバーレスアプリケーション向けに、インストルメンテーションを自動化することで、寿命の短いタスクであっても、脅威に関するリアルタイムの可視性を確保している。

Amazon EKSで利用可能なKubernetesネイティブのコントロールを活用することで、コンテナワークロードのランタイム保護を実現している。

- → Admission Controllerを使用して、クラスター上で実行を許可されるものを定義している。
- → クラスターとコンテナに対して「最小権限」を強制することで、求められるタスクを実行するために必要となる権限のみを提供している。
- → Amazon EKSを通じて、最小特権のKubernetesネットワークポリシーを実装している。

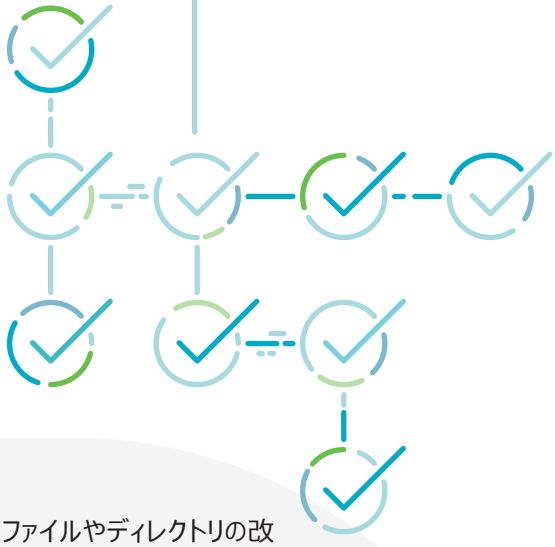
コンテナのドリフトを監視することで、コンテナが本番環境に導入された後に、追加または変更されたパッケージやバイナリファイルの実行をブロックしている。

詳細な活動記録を取得することで、インシデント対応を合理化し、コンテナが消失した後でも、コンテナとクラウドに関するセキュリティ脅威に迅速に対応できる。

4

AWSクラウドとコンテナの保護に関する5つのポイント

コンプライアンスを継続的に検証



企業や組織は、SOC2、PCI、NIST、HIPAAなどのコンプライアンスに準拠しなければならない場合があります。動きの速いクラウド環境では、コンプライアンスの監視と測定に独自の課題をもたらします。コンプライアンス関連のベストプラクティスを確実に満たすためには、お使いの環境の定期的なチェックを簡単に行えるようにするソリューションが必要となります。コンプライアンスの継続的な検証を実現できているかどうかを判定するには、次のチェックリストが役立ちます。

- AWS、Docker、KubernetesのCISベンチマークと比較して、お使いのコンテナとプラットフォームの構成をチェックしている。
- コンテナイメージのスキャンポリシーを標準規格（NIST、PCI、SOC2、HIPAAなど）や社内コンプライアンスポリシー（ブラックリスト化されたイメージ、パッケージ、ライセンスなど）にマッピングすることで、構築時にコンプライアンスを検証している。
- 規制標準に合わせてカスタマイズしたポリシーを使用して、実行時にコンプライアンスを管理することで、自社がベストプラクティス（特権付きコンテナの実行やルートでのコンテナ実行の禁止など）に従うことを確実にしている。
- 既知の敵対者の戦術、手法、手順（TTP）を具体的に調べるポリシーを実装している。
- クリティカルなシステムファイルやディレクトリの改竄、不正なデータ変更を検知するために、File Integrity Monitoring（FIM）を実装している。
- ネットワーク、ファイル、コマンド、kube-APIアクティビティを追跡し、必要なコントロールに準拠していることを証明するためのアクティビティ監査を取得している。
- 脆弱性スキャン報告書を通じて、コンテナ適合性の証明を提供している。
- インシデントに関する詳細な活動記録を取得し、それらを必要に応じてフォレンジックや調査のために利用している。
- AWS CloudTrailを使用して、AWSクラウドサービス全体における構成変更やポリシー変更を監視している。

5

AWSクラウドとコンテナの保護に関する5つのポイント

コンテナ、Kubernetes、クラウドの監視とトラブルシューティング

コンテナやクラウドサービスは動的であり、絶えず変化しています。AWSのワークロードとインフラストラクチャーの健全性とパフォーマンスに関する可視性を確保することは、お使いのクラウドアプリケーションの可用性を確実にするために不可欠です。コンテナやクラウドの監視やトラブルシューティングを実現できているかどうかを判定するには、次のチェックリストが役立ちます。

コンテナ、Kubernetes、AWSクラウドサービス向けに構築された監視を実装している。アプリケーションのパフォーマンスを向上させ、問題を迅速に解決するには、Kubernetesとクラウドのコンテキストで強化された深い可視性と、きめ細かなメトリクスが必要となる。

→ 過剰なリソースを消費しているサービスやワークロードを特定できるほか、キャパシティ制限を監視できる。

→ コンテナとクラウドのコンテキストを使用して、問題解決のための所有者を特定できる。

オープンソースのPrometheusやAWS CloudWatchのような、クラウド監視における標準を採用している。これら2つの視点を組み合わせることで、AWS Fargate、Amazon S3、Amazon RDS、AWS Lambdaなどのサービスに対する可観測性を実現できる。

→ 監視情報の集約や文書化、そして監視の統合をサポートすることにより、迅速な生産性向上を実現している。

Kubernetesの状態を監視することで、コンテナオーケストレーションサービスの健全性を把握している。

→ ノード、ネームスペース、ポッドなどの主要なメトリクスを監視することで、エラーを特定し、アプリケーションの実行に十分なリソースを確保している。

→ クラスターとクラウド間のキャパシティを最適化することにより、コストを削減している。

履歴データと詳細なシステムアクティビティを取得することで、問題の迅速な調査、相互関連付け、解決までを確実に実現できるようにしている。

DoS攻撃やクリプトマイニングのような攻撃の指標となるCPUやリソースの使用状況を監視している。また、ネットワーク接続を監視することで、攻撃や拡散ベクターに関するインサイトを取得している。

sysdig

クラウドとコンテナを保護

www.sysdig.jp

無料お試しはこちら

デモを依頼

Sysdigについての詳細は www.sysdig.jp

Sysdig Japan合同会社
〒107-0052 東京都港区赤坂7-9-4 赤坂Vetoro 3階
https://sysdig.jp/company/contact-us/

sysdig