クラウドとコンテナを保護するための5つのセキュリティベストプラクティス

コンテナとクラウドの導入が加速する中、多くの企業がコンテナとクラウド環境に関する可視性の確保に苦労しています。Gartner社によると、「クラウドサービスへの攻撃が成功する要因のほぼすべては、顧客の設定ミスや間違いにある」とのことです。また、同社は、2023年までに、クラウドセキュリティ障害の少なくとも99%は顧客の責任になるだろうと予測しています[1]。

また、コンテナは基本的にブラックボックスです。コンテナでは内部で何が起こっているのかを確認するのが困難であり、しかもコンテナの寿命は非常に短期です。実際、当社の調査によると、現在72%のコンテナの寿命が5分未満です[2]。従来のセキュリティツールでは、コンテナの内部を確認することも、Kubernetesの動的な性質を処理することも、マルチクラウド環境におけるスケーリングも行えません。また、プロプライエタリなセキュリティツールは、オープンソースソフトウェアが持つ標準化と技術革新のスピードについていけません。

効率的で安全なDevOpsワークフローを実現するためには、セキュリティとコンプライアンスの管理をどうやって自動化すればよいのでしょうか？適切な統合ツールセットを使用してセキュリティとコンプライアンスを自動化することにより、クラウドとコンテナのセキュリティリスクを管理できるようになります。

そのためには、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、異常なアクティビティを検知すること、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保証することが必要となります。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ます。その結果、AWS上でのコンテナやKubernetesの実行、そしてクラウド運用を自信を持ってセキュアに実現できるようになります。

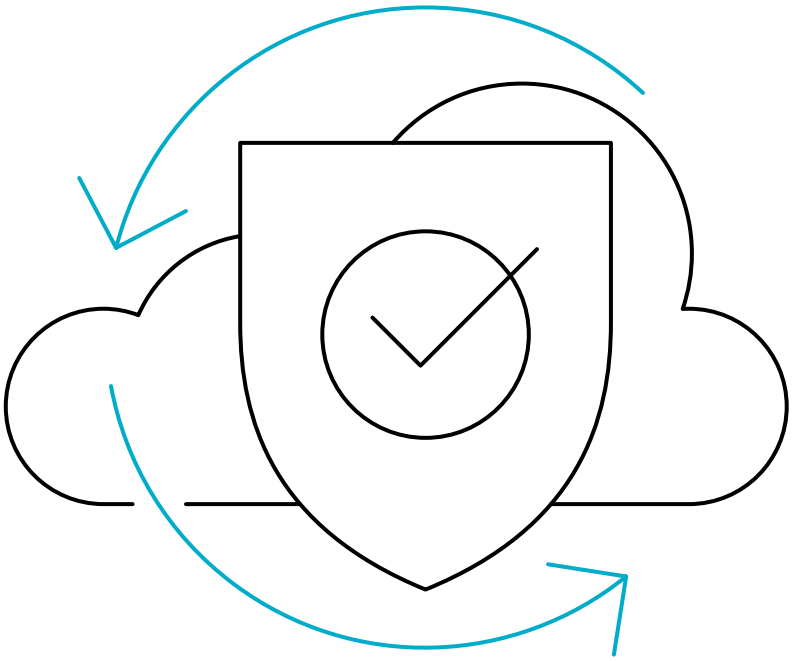
[1] Gartner: Innovation Insight for Cloud Security Posture Management

[2] Sysdig 2023年度版 クラウドネイティブ セキュリティおよび利用状況レポート
https://sysdig.jp/resources/reports/s-2023-cloud-native-security-and-usage-report/

1

継続的なクラウドセキュリティの実現

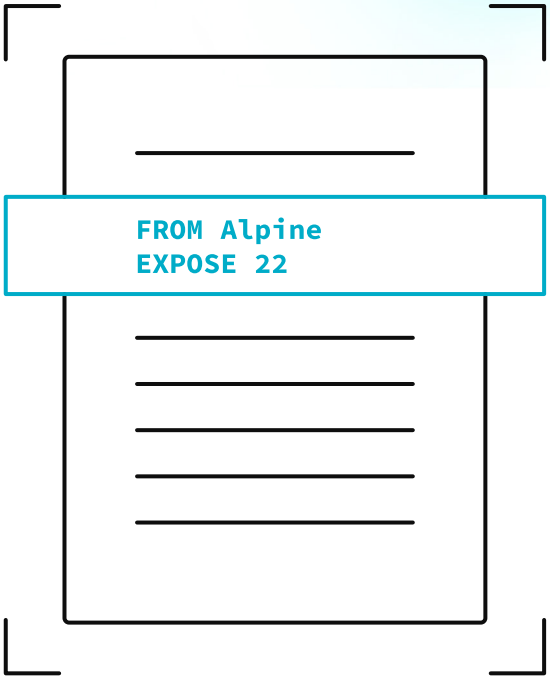
設定ミスや不審な動作を即座に特定するためには、継続的なクラウドセキュリティが必要です。下記に示す事項は、自社のクラウドセキュリティ体制を検証するのに役立ちます。



- マルチクラウド環境全体におけるクラウドリソースのインベントリを通じて、可視性を向上させましょう。
- CISのベンチマークに照らして、お使いのクラウドの設定を定期的にチェックし、設定ミス（パブリックなストレージバケット、公開されているセキュリティグループ、アクセス制御など）を特定した上で、違反を是正するための措置を取りましょう。
- 自動化を進めることで設定ミスの修正にかかる時間を短縮し、修正作業をGitOpsのワークフローへと統合しましょう。
- 環境間のセキュリティ制御を標準化した上で、できれば共有ポリシーモデルで一貫したポリシーを適用しましょう。
- 設定ミス、過剰な権限、脆弱な制御など、多くのセキュリティ上の問題を改善する修正プログラムを優先的に適用することにより、効率性を高めましょう。
- 本番環境での設定ミスをIaC（Infrastructure as Code）マニフェストへとマッピングすることで、ドリフトを減らしましょう。
- クラウドのアクティビティログを解析することで、すべてのクラウドアカウント、ユーザー、サービスにおける予期せぬ変化や疑わしい活動を検検知しましょう。

2

ランタイムインテリジェンスに基づいて脆弱性を優先順位付けする

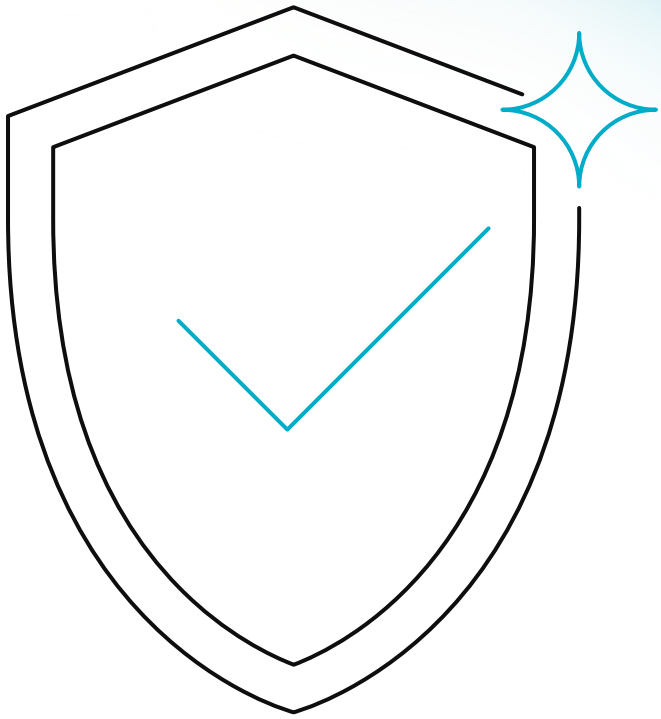


CI/CDパイプラインやコンテナ構築に使用されるオープンソースソフトウェアを通じてアプリケーション開発のスピードが加速する中、コンテナイメージの普及や本番環境で実行されるコンテナ数の増加により、報告される脆弱性の件数が急増しています。脆弱性が効果的に優先順位付けされず、脆弱性管理がアプリケーションのライフサイクル全体に統合されていない場合、セキュリティリスクを制御できなくなり、開発者の時間を浪費してしまう可能性があります。脆弱性によるリスクを制御するために取るべき事項としては、次のことが挙げられます。

- ランタイムに何が使われているかを知ることで、脆弱性の優先順位付けを自動的に行いましょう。
- CI/CDパイプラインやレジストリにスキャンを組み込むことで、リスクのあるイメージが導入されないようにしましょう。
- OSパッケージおよび非OSパッケージの両方における脆弱性をスキャンしましょう。
- 指示、ユーザー権限、秘密の有無、ラベルなどをチェックすることにより、イメージを検証しましょう。
- 本番環境に導入されたコンテナに影響を与えるような新しい脆弱性を特定しましょう。
- ホストスキャン機能（ベアメタル、VM、クラウドインスタンスを含む）を脆弱性管理に取り入れましょう。
- 個々の問題に関して適切なチームにアラートを発行し、CI/CDツールの内部で対応を統合しておきましょう。
- このプロセスにセキュリティ分析とコンプライアンス検証を組み込んでおきましょう。これにより、より早い段階で問題に対処できるようになり、導入のスピードを落とすこともなくなります。これは、「セキュリティのシフトレフト」と呼ばれます。

3

脅威を検知し、対応する

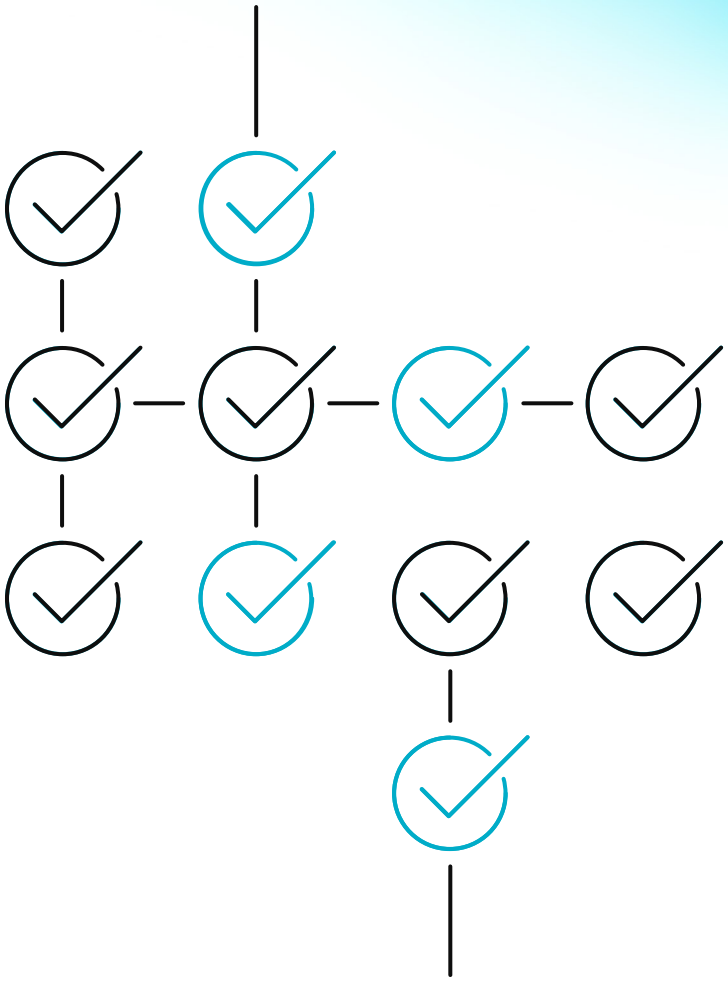


サイバー犯罪は、クラウドネイティブなワークロード、クラウドサービス、ユーザー権限などにより複雑さが増し、アタックサーフェスが拡大する中で、ますます猛威を振るっています。ルールベースのポリシーと機械学習（ML）を組み合わせた多層的な脅威検知は、進化する脅威の状況に対応するための最も効果的な方法です。これにより、コンテキストリッチなイベント、自動アクション、高精度のインシデントデータの探索を通じて、コンテナが消失した後でも確実に調査が行えるようになります。

- ワークロード、クラウドサービス、ユーザーアクティビティに関する統一的な脅威検知を実装しましょう。
- 厳選されたポリシーを利用することで、導入初日から強力な保護を開始できるほか、新たな脅威から継続して身を守ることが可能となります。
- MLベースの検知を使用することで、検知を回避するために設計された、高度に変異したポリモーフィックなマルウェア（クリプトマイナーなど）から身を守ることができます。
- コンテナドリフトを防止すること。これにより、攻撃をブロックし、不変性の原則を実施できるようになります。
- CPU、メモリ、ディスク、ネットワークなどのリソースの使用状況を監視するようにしましょう。一部の攻撃は、セキュリティ違反ではなく、監視アラートとして最初に検知される可能性があるからです。
- ゼロトラストと最小権限の原則を適用してKubernetesネットワークセキュリティを実装しましょう。これにより、影響が及ぶ範囲を縮小し、ラテラルムーブメントのリスクを低減できます。
- インシデント対応を合理化し、コンテキストリッチなイベントを通じて脅威に素早く対応しましょう。
- Kubernetesとクラウドコンテキストでリッチ化されたsyscallデータに基づくキャプチャファイルを使用して、コンテナセキュリティインシデントに関する「いつ」「何を」「誰が」「どこで」「なぜ」という質問に素早く答えれるようにしておきましょう。このような詳細な記録を利用することで、コンテナが消失した後でも、事後分析を行い、根本原因を特定できるようになります。

4

コンプライアンスの継続的な検証

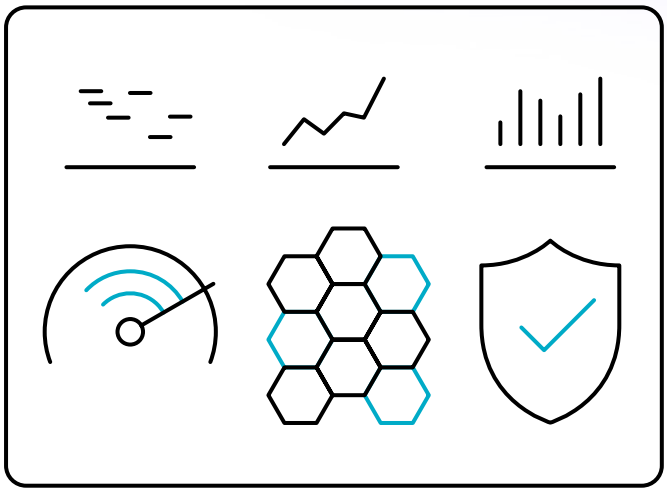


コンテナ、Kubernetes、クラウド環境全体におけるコンプライアンス基準（CIS、SOC2、PCI、NIST 800-53など）を満たすためのコンプライアンスチェックを実施しましょう。また、クラウドサービスを継続的に監視することで、コンプライアンスに影響を与える可能性のある「構成ドリフト」が発生していないかどうかを調べます。さらに、定期的な評価と詳細なレポートを通じて、コンプライアンスの進捗状況を測定します。

- CISベンチマークや業界のベストプラクティスに照らして、お使いのクラウド制御プレーン、コンテナ化アプリケーション、プラットフォームの構成をチェックしましょう。
- ビルド時にコンプライアンスを検証しましょう。これは、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（ブラックリストに載ったイメージ、パッケージ、ライセンスなど）にマッピングすることで可能となります。
- セキュリティ標準に対応した豊富なFalcoルールのセットを通じて、実行時にコンプライアンスを管理しましょう。
- 重要なシステムファイルやディレクトリの改竄、および不正な変更を検知するためにFile integrity Monitoring (FIM) を実装しましょう。
- 自動化により、手動プロセスを排除し、自動修復によりコンプライアンスを実現しましょう。これは、本番環境での設定ミスをIaC （Infrastructure as Code) マニフェストへとマッピングすることで可能となります。
- クラウド監査ログとコンテナのフォレンジックデータを使用して、クラウドおよびコンテナのコンプライアンスに関する証明を提示しましょう。

5

コンテナ、K8s、クラウドのモニタリングとトラブルシューティング



コンテナは短命かつ動的であり、絶えず変化しています。コンテナが消失すると、その中のものはすべて消えてしまいます。ユーザーは、Secure Shell（SSH）も利用できず、ログを見ることもできません。モノリシックなアプリケーションに使われる従来のツールのほとんどは、何か問題が発生した際には役に立ちません。

- コンテナベースのアプリケーションの動的な性質をモニタリングすることは、クラウドサービスの高可用性とパフォーマンスにとって不可欠です。マイクロサービスベースのアプリケーションは複数のインスタンスに分散できるほか、コンテナはマルチクラウドインフラストラクチャー全体を移動できます。Kubernetesオーケストレーションの状態をモニタリングすることは、Kubernetesがすべてのサービスインスタンスを稼働させ続けているかどうかを理解する上で極めて重要です。
  - インフラストラクチャー、サービス、アプリケーションに関するディープな可視性を通じて、健全性とパフォーマンスを監視しましょう。Kubernetesオーケストレーションのモニタリングにより、クラスターの運用状況を把握できます。
  - コンテナやクラウドのコンテキストを利用して、オーナーを即座に特定でき、問題解決に結びつけます。
  - 過剰なリソースを消費しているPodを特定し、キャパシティ制限を監視しましょう。オートスケーリングの挙動をモニタリングすることで、予期せぬ課金、アプリケーションのロールアウト、デプロイメントのロールバックを制御します。
  - クラスターとクラウド全体におけるキャパシティを最適化することで、コストを削減します。
- コンテナに関するディープな可視性と、Kubernetesとクラウドのコンテキストでリッチ化されたきめ細かなメトリクスにより、アプリケーションのパフォーマンスを改善し、問題を迅速に解決しましょう。これにより、所定のセキュリティインシデントがサービスの可用性に与える影響をモニタリングできるようになります。
- Promcat.ioを使用すると、迅速に生産性を向上できます。Promcat.ioとは、Prometheus統合におけるリソースカタログであり、Kubernetesプラットフォームやクラウドネイティブサービスにおけるモニタリングの統合に関するキュレーション、文書化、サポートを提供します。

Sysdigは、クラウドとコンテナのセキュリティに関する標準を推進しています。当社は、クラウドネイティブなランタイムの脅威検知および対応のパイオニアであり、FalcoとSysdig Open Sourceをオープンソースの標準として、またSysdigプラットフォームの主要な構成要素として作成しています。このプラットフォームを利用することで、チームは、ソフトウェアの脆弱性の発見と優先順位付け、脅威の検知と対応、クラウド設定・権限・コンプライアンスの管理が行えるようになります。また、コンテナやKubernetesからクラウドサービスに至るまで、チームは、シングルビューを通じてソースから実行までのリスクを把握できるようになります。これにより、死角や当て推量を一掃できるほか、時間を無駄にすることもなくなります。

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/

CL-001-JA Rev. G 2/23