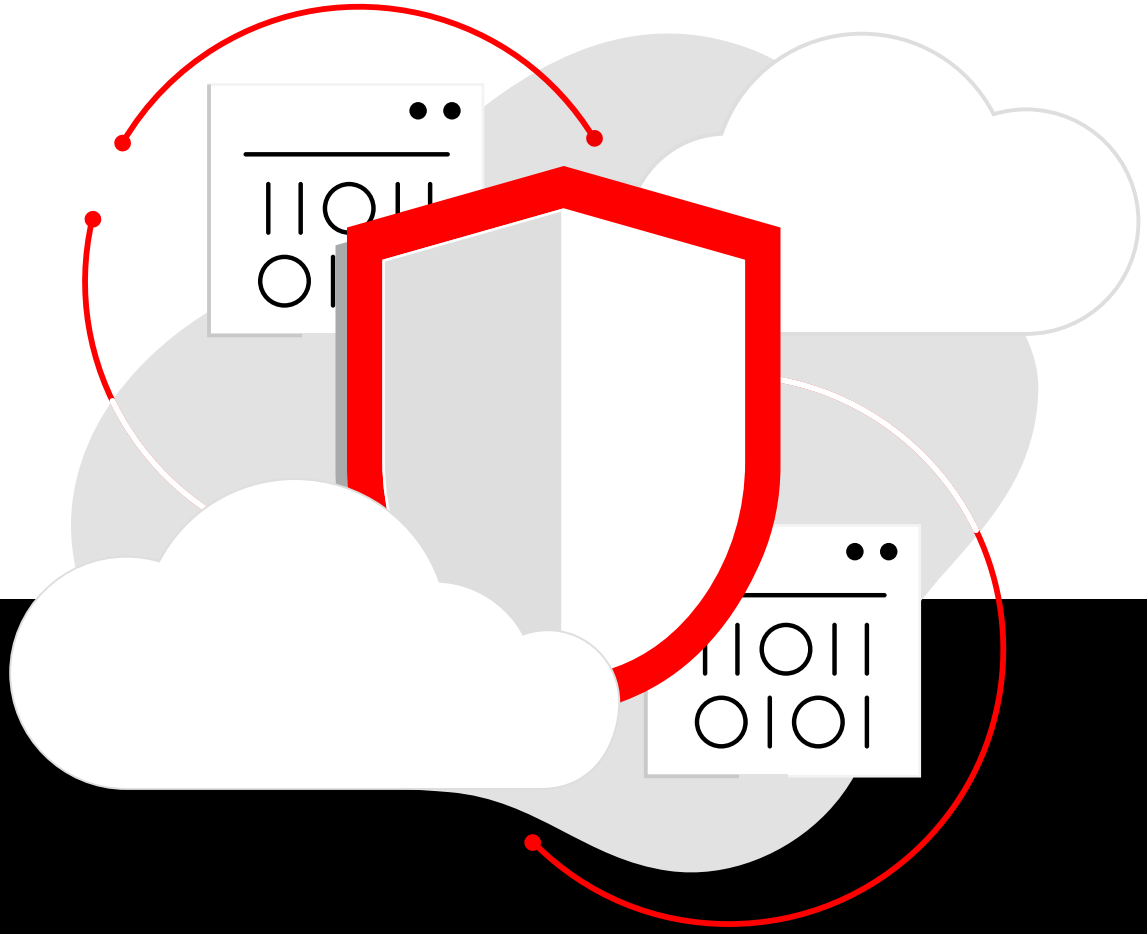
Red Hat



DevSecOps によるアプリケーション・ライフサイクルのモダナイズとセキュリティ保護

目次

はじめに

アプリケーション・セキュリティはデジタル世界で重要

クラウド、コンテナ、マイクロサービス・テクノロジーを導入してデジタル世界での競争力を得ようとする組織が増える中、セキュリティは依然として最大の懸念事項です。実際、エンタープライズのシニア IT リーダーの 50% が、テクノロジーに関する取り組みにおける上位 3 つの優先事項の中にサイバーセキュリティを挙げています。[1]同時に、86% が自社のデジタルトランスフォーメーションのペースは 2021 年に加速すると推定しています。[1]

このような新しいテクノロジーには、セキュリティに対して異なるアプローチを採用する必要があります。従来の境界ベースのアプローチは分散環境には有効ではないからです。さらに、DevOps とクラウドネイティブ手法によって開発のスピードとデプロイメントの柔軟性が増すにつれて、プロセスの早い段階でセキュリティを考慮する重要性がますます高まっています。セキュリティ対策を開発サイクルの最後にのみ適用していると、提供の遅延や保護の低下につながりがちです。

DevSecOps のアプローチとプラクティスを導入すると、アプリケーション環境とビジネスの保護の改善に役立ちます。

DevSecOps とは

DevSecOps では、DevOps の協調的な文化が拡張され、アプリケーション・ライフサイクル全体にセキュリティが組み込まれます。これには、分散型の環境でセキュリティの普及を促進する人材、プロセス、テクノロジーが含まれます。

DevSecOps により、セキュリティの適用は 1 つのチームが担当し、開発およびデプロイのプロセスの最終時点で行われる一連の作業ではなく、すべてのチームが共有する任務になります。セキュリティ、開発、運用の各チームが連携して、情報、フィードバック、学んだ教訓、知見を共有します。このアプローチにより、アプリケーション開発とインフラストラクチャのデプロイメントの開始時からセキュリティを統合できるため、保護が強化され、リスクが軽減されます。

DevSecOps のメリット

セキュリティの向上とリスクの低減

セキュリティの問題にプロダクションではなく開発の時点で対処して、アプリケーションの保護を強化し、ポリシーチェックに適合しなかったために遅延または停止されるデプロイメントの数を選らします。

セキュリティの問題の迅速な修復

コラボレーションを促進して自動化を取り入れる先進的なセキュリティプラクティスとツールを適用してリリースサイクルを加速し、プロダクションにおけるセキュリティ問題の修復に必要な時間を短縮し、時間とコストを削減します。

コンプライアンスと可視性の向上

手作業のミスのリスクを減らして予測性と反復性を向上させる自動化プロセスとツールを導入して、コンプライアンスを向上させ、監査プロセスを単純化します。

1 Flexera、「2021 Flexera State of Tech Spend Report」、2021 年 1 月。

DevSecOps 実装の課題

DevSecOps アプローチからは多数のメリットがもたらされますが、DevSecOps の実装を困難にする要因もいくつかあります。

- **進化するセキュリティ事情：** セキュリティの脅威と規制 (ビジネス上の要件、技術的要件、地理的要件など) は急速に変化し続けており、最新情報を把握するのは困難になっています。
- **アプリケーション環境の複雑さ：** 複雑で大規模なアプリケーション環境を構成するさまざまなテクノロジー (コンテナ、マイクロサービス、クラウドサービスなど) のすべての接続とセキュリティへの影響を理解することは困難です。
- **不足している既存ツールとプロセス：** 多くのチームが、DevSecOps の取り組みを開始するときに既存のツールとプロセスを適用していますが、このやり方ではその後の目標達成に役立ちません。
- **複数のセキュリティツール：** 組織に適したセキュリティツールの選択、テスト、統合、維持には、時間、調査、継続的な取り組みが必要です。

DevSecOps の成功は文化、プロセス、テクノロジーに掛かっている

DevSecOps でアプリケーション・ライフサイクルをセキュリティ保護するには、文化、プロセス、テクノロジーの 3 つの領域で変化と連携が必要になります。

文化

コラボレーションと共有された目標を、開発、運用、セキュリティの各チーム間に浸透させます。各チームがセキュリティをアプリケーション・ライフサイクルに組み込む理由と手法を理解できるよう支援します。

プロセス

プロセスとワークローを標準化、文書化、自動化して、アプリケーション・ライフサイクル全体を通じて効率とセキュリティを向上させます。

テクノロジー

アプリケーションの開発、デプロイメント、運用に使用しているプラットフォーム、ツール、プロセスを、1 つに統合された構造に組み込みます。

DevSecOps の基本についての詳細

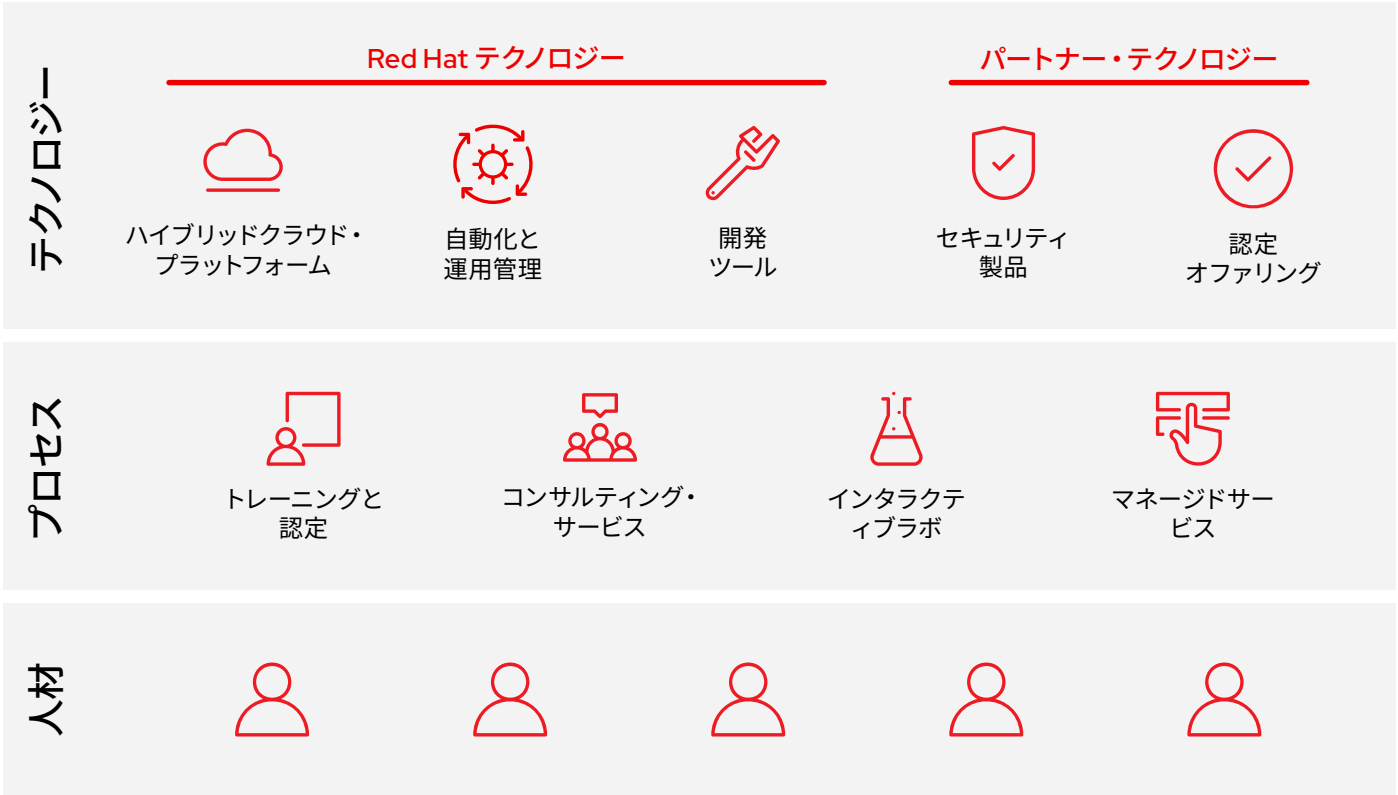
「DevSecOps プラクティスが不十分な理由」についての短いブログ記事を読み、DevSecOps の実装の成功に必要な変化についてご確認ください。**e ブック「ハイブリッドクラウドのセキュリティの強化」**を読み、クラウドネイティブのセキュリティアプローチでビジネスを保護する方法をご覧ください。

Red Hat の DevSecOps 戦略

Red Hat は、ハイブリッドクラウド環境でのアプリケーションのビルド、保護、デプロイに対応する認定パートナーエコシステム、広範な専門知識、革新的なプラットフォームをすべて備えています。この組み合わせにより、包括的な DevSecOps ソリューションを実装して、アプリケーション・セキュリティの向上、リスクの低減、パフォーマンスの向上、投資価値の最大化を実現できます。

Red Hat® プラットフォームは、信頼できるコンテンツ・サプライチェーン、専任のセキュリティチームによるサポート、主要なセキュリティ機能のバックポートを備えており、DevSecOps ソリューションに最適な基盤を提供します。Red Hat のパートナーはこの基盤を、セキュリティと自動化をアプリケーション・ライフサイクル全体に適用するための革新的な統合製品で拡張し、強化します。そのうえ、**トレーニングと認定のコース**、**インタラクティブなラボ**、**コンサルティング業務**、**マネージドサービス**を提供しており、DevSecOps 実装に成功できるよう支援します。

Red Hat は、お客様の DevSecOps 実践の進捗状況にかかわらず、そのニーズに応えます。当社のモジュール式で拡張可能なソリューションと専門家サービスにより、お客様は、現在必要なものをデプロイし、将来の変化に適応し、効率的かつ効果的な DevSecOps の導入に必要な手法とアプローチを習得できます。



Red Hat 製品でオープンな DevSecOps 基盤を構築する

Red Hat OpenShift

Red Hat OpenShift® はエンタープライズ対応でセキュリティ重視のハイブリッドクラウド・プラットフォームで、組み込みの DevOps ツールとセキュリティ機能が搭載され、デフォルトで有効になっています。このプラットフォームはパートナーやサードパーティのセキュリティツールおよびテクノロジーと連携し、セキュリティを強化して強力な DevSecOps を実装します。**Red Hat OpenShift セキュリティガイド**で、テクノロジースタック全体でセキュリティに対処する方法をご覧ください。

無料で試用する

主要なセキュリティ機能

- Security-Enhanced Linux (SELinux)
- セキュリティ・コンテキストによる制約 (SCC)
- ID 管理とアクセス管理
- データ暗号化
- 連邦情報処理標準 (FIPS) モード

Red Hat Ansible Automation Platform

Red Hat Ansible® Automation Platform は、セキュリティ・ソリューションを自動化および統合でき、セキュリティツール間に共通言語を提供する、柔軟で強力なプラットフォームです。**自動化のユースケース**をご確認ください。

Red Hat Enterprise Linux CoreOS

Red Hat Enterprise Linux® CoreOS は軽量でコンテナに最適化されたイミュータブルなオペレーティングシステムで、Red Hat Enterprise Linux のセキュリティ重視の基盤をベースとし、Red Hat OpenShift 内で使用されます。

Red Hat Quay

Red Hat Quay は高可用性の分散型コンテナ・イメージ・レジストリで、コンテナを構築、分散、デプロイできます。

Red Hat CodeReady Workspaces

Red Hat CodeReady Workspaces は、Red Hat OpenShift 上で実行されるコンテナで開発者がコード作成、構築、テストできるようにするツールです。

Red Hat Advanced Cluster Security for Kubernetes

Red Hat Advanced Cluster Security for Kubernetes は、コンテナセキュリティ向けにクラウドネイティブのアーキテクチャを提供し、アプリケーションの構築からランタイムまでを保護します。

Red Hat Advanced Cluster Management for Kubernetes

Red Hat Advanced Cluster Management for Kubernetes は、セキュリティポリシーを組み込んだ単一のコンソールで、クラスタとアプリケーションを制御します。

認定セキュリティ・パートナー・エコシステムで柔軟性と信頼性を得る

効果的な DevSecOps を完全に実装するために必要なすべての機能を 1 社で提供するベンダーはありません。さらに、どの組織も同じではないので、それぞれのニーズを満たすには、製品とテクノロジーの独自の組み合わせが必要になります。

Red Hat は**業界をリードする革新的なセキュリティパートナー**とのコラボレーションにより、認定された統合、コンテナイメージ、**Red Hat OpenShift Operator** に基づく完全なソリューションを提供しています。連携に信頼性と一貫性があることがわかっているので、パートナー、製品、テクノロジーの中からニーズに最適なものをいつでも自信を持って選択できます。これらのソリューションには、エキスパートのサービス、サポート、トレーニングによる補助もあり、DevSecOps の文化、プロセス、ツールの実装の成功を支援します。

Red Hat のセキュリティ・パートナー・エコシステムのメリット

選択の自由

組織のニーズに最適な製品とベンダーをいつでも選択できます。

認定資格

すべてのコンポーネントが確実に連携することが認定済みであるとわかっているので、自信を持ってソリューションを構築できます。

専門知識

Red Hat とパートナーが持つ DevSecOps の知識と経験を組み合わせて活用します。

Services

DevSecOps の文化、プロセス、ツールを組織内に適切に実装するためのサポートを受けられます。

トレーニング

ベストプラクティスを学習し、DevSecOps アプローチを導入するために必要なスキルを獲得します。

Red Hat Vulnerability Scanner Certification

Red Hat Vulnerability Scanner Certification は、脆弱性スキャナーの結果の不一致を最小化します。Red Hat は認定セキュリティパートナーと協力して、Red Hat が公開したイメージやパッケージについて、より正確で信頼性の高いコンテナ脆弱性のスキャン結果を提供します。

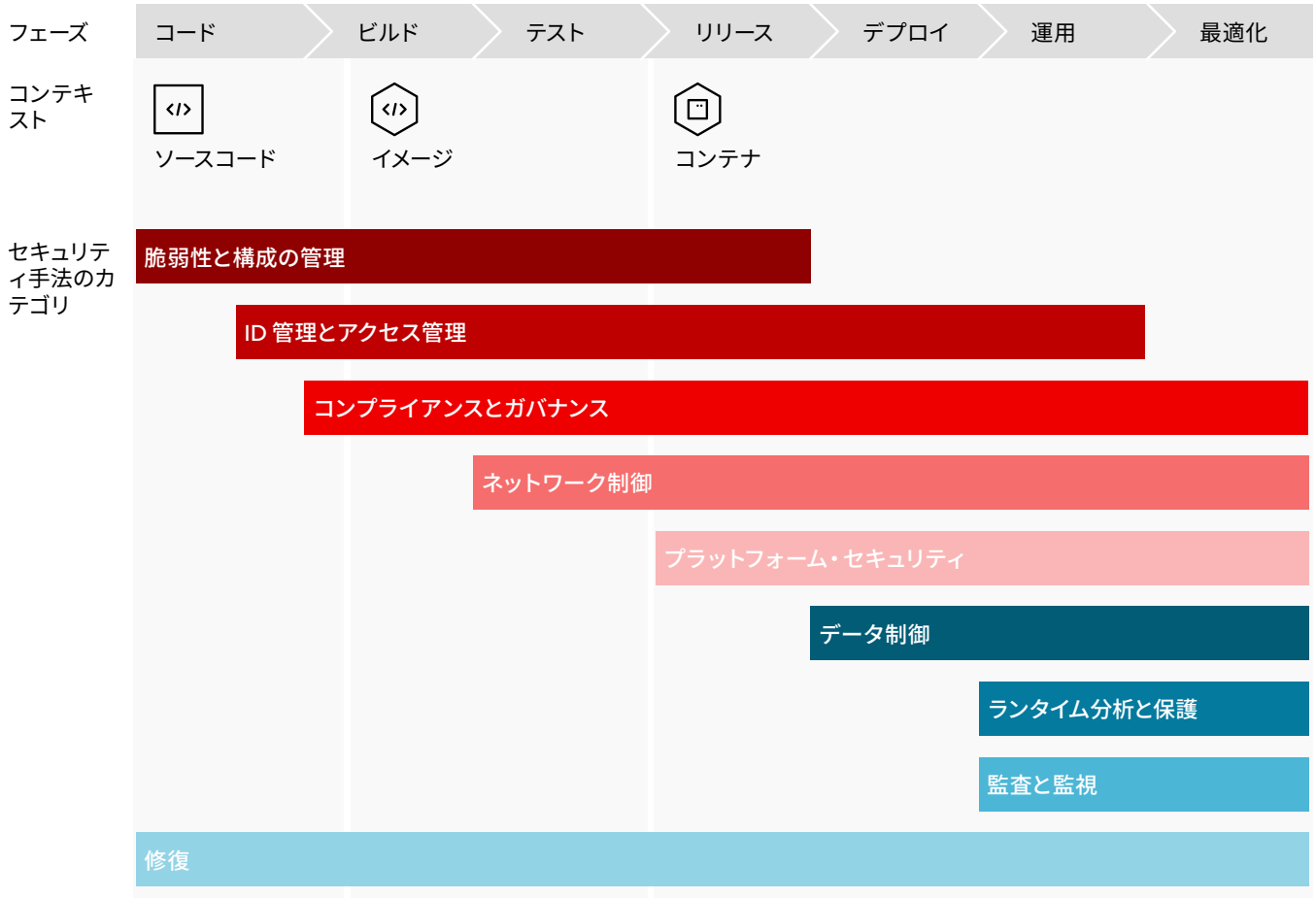
- 偽陽性やその他の不一致を最小化
- 戦略的プロジェクトと取り組みの時間と予算を解放
- 高いレベルの保証を達成
- Red Hat が公開したイメージの一元化されたデータで精度を向上
- 脆弱性の管理の単純化

認定済み製品を探す

完全な DevSecOps ソリューションを作成する

Red Hat では、アプリケーション・ライフサイクル全体を通じてセキュリティ要件に対処する、極めてスケーラブルで包括的な DevSecOps ソリューションを構築するためのフレームワークを提供しています。当社のセキュリティパートナーと協力して作成されたこのフレームワークは、お客様の現在のニーズおよび予測されるニーズに応じて DevSecOps を組織に実装するために役立ちます。

Red Hat DevSecOps フレームワークは、機能ごとに分類されたセキュリティツールと手法の包括的なセットを、アプリケーション開発ライフサイクルに対応付けます。



概要を読む

ニーズに適したセキュリティ手法と製品を選ぶ

Red Hat DevSecOps フレームワークでは、34 個の主なセキュリティ手法を 9 つのカテゴリに整理しています。Red Hat および認定パートナーのテクノロジーはこれらの 1 つまたは複数の手法と連携し、組織のニーズに対処し、将来の変化に適応する、完全な DevSecOps ソリューションの構築を支援します。

脆弱性と構成の管理

- 静的アプリケーション・セキュリティ・テスト (SAST)
- 静的コード解析 (SCA)
- インタラクティブ・アプリケーション・セキュリティ・テスト (IAST)
- 動的アプリケーション・セキュリティ・テスト (DAST)
- 構成管理
- イメージリスク

ID 管理とアクセス管理

- 認証
- 認可
- シークレットボールト
- ハードウェア・セキュリティ・モジュール (HSM)
- Provenance

コンプライアンスとガバナンス

- 法令順守の監査
- コンプライアンス統制と修正

ネットワーク制御

- コンテナ・ネットワーク・インタフェース (CNI) プラグイン
- ネットワークポリシー
- トラフィック制御
- サービスメッシュ
- 可視化
- パッケージ分析
- アプリケーション・プログラミング・インタフェース (API) 管理

プラットフォーム・セキュリティ

- セキュアなホスト
- コンテナ・プラットフォーム
- 名前空間
- 分離
- Kubernetes とコンテナ強化

データ制御

- データ保護と暗号化

ランタイム分析と保護

- アドミッション・コントローラー
- アプリケーション動作分析
- 脅威防御

監査と監視

- クラスタ監視
- セキュリティ情報およびイベント管理 (SIEM)
- フォレンジック

修復

- セキュリティ・オーケストレーション、自動化、応答 (SOAR) プラットフォーム
- 自動解決

認定パートナーを探す

パートナーのハイライト

Sysdig

Sysdig は、セキュリティ重視の DevOps テクノロジーにより、組織がクラウド内のワークロードを確実に実行できるよう支援しています。Sysdig のアプリケーション、ワークロード、コンテナの監視およびセキュリティ保護の製品は、数百の企業において、クラウドネイティブ・アプリケーションの迅速な納品に役立っています。

Red Hat と Sysdig は連携して、企業へのクラウドネイティブ・アプローチの迅速な導入をサポートします。 **Sysdig Secure DevOps Platform**、**Sysdig Secure**、**Sysdig Monitor** は Red Hat OpenShift および **Red Hat Advanced Cluster Management for Kubernetes** と連携して、プライベート、ハイブリッド、マルチクラウドの各環境に、統合されたセキュリティ、コンプライアンス、監視を提供します。これらのソリューションにより、構築パイプラインを保護し、脅威を検出して対応し、クラウド体制とコンプライアンスを継続的に検証し、パフォーマンスをモニタリングします。オープンソーススタック上に構築される Sysdig のクラウドネイティブの監視、セキュリティ、フォレンジック機能からは、低リスクでクラウドに移行するために必要な知見と制御が得られます。

Red Hat と Sysdig のソリューションは以下の実現に役立ちます。

- 継続的インテグレーション/継続的デプロイメント (CI/CD) パイプライン内でイメージを直接スキャンする
- クラウドの規模でパフォーマンスと可用性を監視する
- 継続的なコンプライアンスとランタイムのセキュリティを実装する
- Red Hat OpenShift インフラストラクチャ構成を検証する
- 問題へのトラブルシューティングと対応をより容易にする

2020
Red Hat Rising Star Partner of the Year (公共部門)[2]

セキュリティリスクの管理

パイプライン全体を通じて脆弱性を特定し、修復します。自動化されたポリシーと制御で、ランタイム時に脅威を検出してブロックします。コンテナが廃棄された後も、インシデントに対応して調査します。

パフォーマンスと可用性の向上

数百万単位のメトリクスを調査し、保持します。環境上で正常性とパフォーマンスを監視して、問題を事前に見つけて修正します。クラスタ、Pod、コンテナ内部の問題のトラブルシューティングを、より容易にします。

クラウドのコンプライアンスの検証

Red Hat OpenShift 環境が共通の標準に準拠していることを検証します。クラスタ、ノード、コンテナを詳細なアクティビティレポートで監査します。コンテナのライフサイクル全体でファイル整合性の監視を実施します。

統合にアクセス

2 Red Hat ブログ、「**Red Hat オープンソース・イノベーションへの貢献について北米のパートナーを表彰**」、2020 年 4 月 23 日。

パートナーのハイライト

Synopsys

Synopsys は、セキュアなソフトウェアを迅速に構築するための、静的なソフトウェア・コンポジションと動的な分析ソリューションを影響しています。業界をリードするツール、サービス、専門知識を兼ね備えた Synopsys は、DevSecOps を適用して、ソフトウェア開発ライフサイクル全体を通じてセキュリティと品質を最適化できるように支援します。

Red Hat と Synopsys は、セキュリティ重視の高品質なコードの作成をサポートし、リスクを最小化しながら速度と生産性を最大化します。 **Synopsys Black Duck ソフトウェア・コンポジション分析 (SCA)** は Red Hat OpenShift と統合されて、お客様のコンテナ内のオープンソース・コードにおけるセキュリティの脆弱性およびポリシー違反に対する可視性と制御を向上します。**Black Duck for OpenShift** は、Red Hat OpenShift クラスタ内にあるすべてのコンテナイメージを自動的に検出、スキャン、監視、検査して、コンテナ構築のあらゆる段階でオープンソースのセキュリティおよびコンプライアンスのリスクを特定します。このソフトウェアは、脆弱なコンテナがプロダクションにプッシュされないようにし、実行中のコンテナに影響を与える新しい脆弱性に迅速に対応できるようにします。

Black Duck for OpenShift ソリューションには、以下の機能があります。

- 各コンテナイメージにおいてすべてのサードパーティのオープンソースコードを網羅したリストを提供し、脆弱性およびポリシーメタデータで Pod に注釈を付ける
- コンテナに影響を与える新しい脆弱性を即座に通知し、どのイメージおよびコンテナが影響されるかを特定する
- オープンソースのフォークとバックポートを理解し、該当する場合に脆弱性をパッチ適用済みとマークし、調査が必要な脆弱性の数を削減する
- Red Hat Advanced Cluster Management for Kubernetes と**統合**して、すべてのクラスタ上で一貫性のあるデプロイメントを確保する

コンテナイメージを自動的にスキャンする

オープンソースコードを継続的に監視する

セキュリティ脆弱性を特定する

「Synopsys と Red Hat はセキュアなアプリケーションとデプロイの今後について類似するビジョンを共有しており、組織がコンテナ化アプリケーションに信頼を寄せられるようになることを期待しています」

Vatsal Sonecha 氏
Synopsys ビジネス開発担当バイスプレジデント

統合にアクセス

パートナーのハイライト

Palo Alto Networks

Palo Alto Networks はイノベーションを届けることで、変化の速度が増してもセキュアなデジタル・トランスフォーメーションをサポートしています。同社は、世界中の 60,000 を超える顧客がビジネスの保護に役立てているセキュリティ・ソリューションのポートフォリオを有しています。

Red Hat と Palo Alto Networks は、クラウドネイティブ・セキュリティとコンプライアンス遵守によって、開発ライフサイクル全体を通じて環境の保護を支援します。 Palo Alto Networks の Prisma Cloud は Red Hat OpenShift と連携して、包括的なクラウドセキュリティ体制管理 (CSPM) およびクラウドワークロード保護 (CWP) をお客様のデプロイメントに提供します。このソリューションは、ホスト、コンテナ、サーバーレスの完全なライフサイクルセキュリティと、セキュリティ体制に対する可視性とガバナンスを提供します。

Red Hat とのパートナー開始

2017 年

特長とメリット

脆弱性の管理

アプリケーション・ライフサイクスの各段階で、脆弱性検出、把握、防御を行う、開発からプロダクションまで組み込まれたセキュリティ

コンプライアンス

Center for Internet Security (CIS) ベンチマーク、外部コンプライアンス体制、カスタム要件へのコンプライアンスを容易に実装して維持する

CI/CD セキュリティ

継続的インテグレーション (CI) プロセスにセキュリティを直接組み込み、問題がプロダクションにデプロイされるまに検出して修復する

ランタイム防御

最も特権が低く許可リストに基づくランタイムモデルをすべてのアプリケーション・バージョンに自動的に作成する機械学習で、セキュリエィを広範囲に適用する

Web アプリケーションとインタフェースのセキュリティ

パブリッククラウドおよびプライベートクラウド環境へのレイヤー 7 および Open Web Application Security Project (OWASP) Top 10 の脅威に対して保護する

アクセス制御

既存の ID 管理、アクセス管理、シークレット管理のツールを統合して、ワークロードおよびアプリケーションへのアクセス制御を確立および監視する

統合にアクセス

パートナーのハイライト

CyberArk

CyberArk は、独自のセキュリティファーストのアプローチを ID ベースの特権アクセス制御に適用します。同社は、エンタープライズ、クラウド、DevOps の環境でユーザー、アプリケーション、スクリプト、マシンが使用する、シークレットと認証情報を保護する完全なソリューションを提供しています。

Red Hat と CyberArk は共同で、コンテナ環境と自動化スクリプトのセキュリティ向上に役立ちます。 全社的な特権アクセス・セキュリティ・ポリシーにより、可視性、監査、適用、シークレット管理を実施し、ビジネスリスクを軽減します。CyberArk DevSecOps 製品は、Conjur Secrets Manager および Credential Provider を含めて、Red Hat OpenShift および Red Hat Ansible Automation Platform と統合し、人、アプリケーション、スクリプト、人間以外のその他のアイデンティティに対する特権認証情報を、一元化されたプラットフォームを使用して保護、ローテーション、監視、管理します。組織全体での一元化された制御として、セキュリティ管理の統合、セキュリティ脆弱性の削減、攻撃対象領域の最小化、運用の効率化を実現できます。

モジュール式アーキテクチャなので各コンポーネントを独立してデプロイでき、ハイブリッドクラウド、マルチクラウド、コンテナ化、DevOps の環境への保護をカスタマイズできます。強力なランタイム認証とロールベースのアクセス制御により、承認された Pod とコンテナのみがシークレットを受け取れるようにします。Red Hat Ansible Automation Platform との統合によって Playbook でマネージドシークレットにアクセスでき、手作業でのシークレットの入力やローテーションの必要性を排除します。この統合により、検出されたセキュリティインシデントに対応する修復作業を自動化することもできます。

セキュリティの統合

インフラストラクチャ全体でシークレットおよび特権アクセス認証情報を、お客様のポリシーに従って一元管理し、セキュリティ保護します。

運用の単純化

お客様のポリシーに従って開発者と自動化エンジニアが、使用するシークレットおよび認証情報をセキュリティ保護、管理、ローテーションできるようにします。

一貫性の向上

管理コンソールにアクセスするアプリケーション、スクリプト、ユーザーが使用するシークレットと認証情報を、一貫性をもって保護します。

Web セミナーを見る

パートナーのハイライト

Tigera

Tigera は、Kubernetes ネットワークおよびマイクロサービスの通信をセキュリティ保護、観察、トラブルシューティングする方法を変革します。

Red Hat と Tigera は、ネットワークトラフィックを監視、分析、管理して、組織がセキュリティを Kubernetes 環境に組み込む支援をします。Red Hat OpenShift で認定されている Tigera Calico Enterprise は、クラウド環境上での重要なコンテナ化アプリケーションの運用、最適化、保護を支援します。Kubernetes ネイティブのアーキテクチャでは、ソリューションをアプリケーション開発に埋め込み、詳細なセキュリティ制御を向上させ、ネットワークとマイクロサービスのレイヤー間の可視性を向上します。このソリューションでは、既存のセキュリティツール、環境、セキュリティ運用センター (SOC) とも統合し、先進的なワークロードへの制御と機能を補強します。ゼロトラスト・ネットワーク、Egress アクセス制御、トラフィック可視性、脅威への保護と防御、自動化されたコンプライアンス監査レポートにより、開発、テスト、プロダクション環境でのアプリケーション・セキュリティを向上させます。

セキュリティ機能の拡張

既存のファイアウォール、最小権限のセキュリティ、Pod 間トラフィックの暗号化で、アプリケーションを保護します。

ネットワークの可視性の取得

ネットワークフローにアクセスして、接続性のデバッグ、脅威ハンティング、コンプライアンスレポートの自動化を行います。

コンプライアンスの確保

アプリケーションのコンプライアンスを監視し、非準拠のワークロードについてリアルタイムでアラートを通知します。

Operator にアクセス

パートナーのハイライト

Aqua Security

Aqua Security は、顧客が最小限の手間でビジネスを変革して運営できるよう支援します。同社は、アプリケーション・ライフサイクル全体を通じて脅威の防止、検出、対応の自動化を提供し、環境のあらゆる面についてセキュリティを向上させます。

Red Hat と Aqua Security は、クラウドネイティブ・ワークロードの管理とスケーリングを、オンサイト、ハイブリッド、クラウドのインフラストラクチャでより安全に行えるように支援します。Aqua Cloud Native Security Platform は Red Hat OpenShift と統合して、リスクベースの脆弱性管理、詳細なランタイム保護、包括的なインフラストラクチャ保証とコンプライアンスを提供します。開発チーム、セキュリティチーム、運用チームはこのソリューションの機能を活用して、セキュリティを高めたアプリケーションを提供し、脅威からランタイム時に保護し、インフラストラクチャの構成を評価して修復できます。

特長とメリット

DevSecOps アプローチをサポートする

- Red Hat OpenShift レジストリのコード、構成、権限を広範囲にわたって分析する
- 脆弱性の優先度をリスクによって決定する
- CI/CD パイプラインとの統合によって構築プロセスを自動化する

ランタイム時にアプリケーションを保護する

- アプリケーションを中断させずに、不正なコンテナアクティビティを検出して自動的に軽減する
- 標準イメージからの不正な変更を特定および防止して、コンテナの不変性を維持する

ソフトウェアのサプライチェーンにおけるセキュリティを向上させる

- 保護されたプリプロダクションのテスト環境でイメージを実行して検証する
- 静的なスキャナーではデプロイ前に検出できない場合がある高度なマルウェアを特定する

インフラストラクチャのコンプライアンスを維持する

- ベストプラクティスおよび Center for Internet Security (CIS) ベンチマークに準拠しているか、数百もの構成および制御ポリシーをスキャンし、検証する
- Open Policy Agent (OPA) ベースの宣言的保証ポリシーで、ロールベースのアクセス制御 (RBAC) を施行する

統合にアクセス

DevSecOps の導入を今すぐ始めましょう

アプリケーション・セキュリティは、デジタルビジネスにとって必要条件です。DevSecOps のアプローチを導入すると、アプリケーション環境とビジネスの保護の改善に役立ちます。

Red Hat は革新的なテクノロジー基盤と包括的な DevSecOps エコシステムおよび広範な専門知識を兼ね備え、お客様の組織全体で DevSecOps の実装を成功に導くお手伝いをします。

- 業界をリードする多様な認定済みツールおよびテクノロジーを用意し、現在および将来のニーズに合わせて選択できます。
- ベストプラクティスを学習し、エキスパート・トレーニング・リソースから DevSec Ops のスキルを習得します。
- 専門サービスとコンサルティング対応で迅速にデプロイします。

Red Hat で DevSecOps を実装する方法の詳細はこちら：
redhat.com/ja/partners/devsecops

F29623_0721_KVM

Red Hat