Red Hat OpenShift Virtualization でセキュリティ重視を強化する 4 つの方法

これは、セキュリティの取り組みに焦点を当て、ハイブリッドクラウド内の仮想マシン (VM) とコンテナ全体に一貫した制御を適用するためのチェックリストです。Red Hat® OpenShift® Virtualization ツールを使用してセキュリティポスチャを強化し、ワークロードを保護する 4 つの方法をご紹介します。

1 プラットフォームを根本から強化する

Red Hat OpenShift 上で実行される OpenShift Virtualization は、強化に対応した基盤を提供し、コンテナと VM の両方を管理できます。これにより、すべてのワークロードにわたり一貫してセキュリティを適用できます。

- **Red Hat の Compliance Operator を使用して、Red Hat OpenShift にコンプライアンスのベースラインを適用する：** Compliance Operator にクラスタの望ましいコンプライアンス状態の説明を入力すると、ギャップとその修復方法の概要を取得できます。
- **GPU と USB のパススルーを承認済みデバイスのみに制限する：**接続されたハードウェアからの不正なデータアクセスやコード実行のリスクを軽減します。
- **必須ではないフィーチャーゲートを無効にし、信頼できるコンテナレジストリだけを使用する：**トランスポート・レイヤー・セキュリティ (TLS) を使用して、検証されていないイメージや構成ミスが導入される可能性を制限します。

2 すべてのレイヤーでワークロードを制御する

OpenShift Virtualization では、VM を Kubernetes オブジェクトとして管理することにより、ワークロードを作成、変更、操作できるユーザーを詳細に制御できます。ロールベースのアクセス制御 (RBAC) と監査ポリシーを一貫して適用し、重要な VM にはコンテナ化アプリケーションと同じガバナンスモデルに従った変更のみが適用されるようにします。

- **エグゼクティブアクセス、仮想ネットワーク・コンピューティング (VNC) コンソールへのアクセス、ライブマイグレーション操作を、承認された管理者のみに制限する：**不正な変更が実行されたり、データが漏洩したりするリスクを軽減します。
- **必須でない限りゲストメモリーのオーバーコミットと共有可能ディスクを無効化する：**テナント間のリソースの競合を減らし、1 つのワークロードが侵害された場合でも露出を制限できます。
- **重要なワークロードに一貫したエラー処理ポリシーと検証ポリシーを適用する：**環境間で動作が異なることがないようにし、サイレント障害やデータ破損のリスクを軽減します。

3 ネットワークトラフィックをセグメント化してセキュリティポスチャを強化する

OpenShift Virtualization のセキュリティはネットワーク構成もカバーします。ネットワーク制御がコンテナレベルと VM レベルの両方に適用されるため、すべてのワークロードで同じマイクロセグメンテーション・モデルを維持できます。

この環境全体に一貫したネットワークポリシー、可観測性、ロギングを適用すれば、疑わしいトラフィックパターンをより迅速に検出し、トラブルシューティングを単純化できます。

- **仮想ローカル・エリア・ネットワーク (VLAN) を使用してテナントトラフィックやアプリケーション・トラフィックを分離する：**ネットワークセグメント間のラテラルムーブメントのリスクを軽減します。
- **機密性の高いワークロードにメディアアクセス制御 (MAC) アドレス・スプーフィング・フィルタリングとマルチネットワーク・ポリシーを適用する：**ネットワーク上での ID スプーフィングを防止し、価値の高いアプリケーションのトラフィックを分離します。
- **セカンダリー・ネットワークの明確な境界を定義する：**シングルルート I/O 仮想化 (SR-IOV) インタフェースなどを定義し、それらを特定のワークロードまたはテナントにマッピングすることで、仮想スイッチをバイパスするトラフィックに対する制御と可監査性を維持します。

4 ストレージ内のデータの整合性を保護する

OpenShift Virtualization は、ストレージのセキュリティポリシーをコンピューティングやネットワーキングと同じ管理プレーンで管理できるようにします。

仮想化およびコンテナ化されたワークロード全体に同じ暗号化、アクセス制御、レプリケーションポリシーを適用して、コンプライアンスとリカバリープランニングを効率化できます。これらの制御を一元化することで、ストレージ、セキュリティ、プラットフォームの各チームが協力して一貫したポリシーを作成することが容易になり、監査も長期にわたって容易になります。

- **複数の namespace 間での DataVolume (DV) クローニングを制限する：**機密データセットが承認された境界内から出ないようにし、規制された情報やリスクの高い情報が意図せず伝播されることを防ぎます。
- **不要な共有可能ディスクを無効にする：**ワークロード間でデータが意図せず共有されてしまうことを防ぎ、平行書き込みによる破損のリスクを軽減します。
- **重要なデータの errorPolicy 設定とストレージ権限を検証する：**失敗したストレージ操作が一貫した方法で処理され、承認されたワークロードのみが機密ボリュームの読み取りまたは書き込みを行えるようにします。

次のステップ

OpenShift Virtualization 強化ガイドで、ハイブリッドクラウド全体で組織の IT 環境を強化する方法を包括的にご確認ください。