Red Hat OpenShift Virtualization으로 보안을 강화하는 4가지 방법

이 체크리스트를 활용해 보안 운영을 효율화하고, 하이브리드 클라우드 전반의 가상 머신(VM)과 컨테이너에 일관된 제어를 적용하세요. Red Hat® OpenShift® Virtualization 툴을 사용하여 보안 태세를 강화하고 워크로드를 보호할 수 있는 4가지 방법을 소개합니다.

1 플랫폼 보안을 고려한 초기 설계

OpenShift Virtualization의 기반 플랫폼인 Red Hat OpenShift는 보안 강화를 기본으로 적용할 수 있는 기반을 제공하며 컨테이너와 VM을 모두 관리할 수 있습니다. 이를 통해 모든 워크로드 전반에서 일관된 보안 수준을 유지할 수 있습니다.

- **Red Hat Compliance Operator로 Red Hat OpenShift의 컴플라이언스 기준을 강화합니다.** Compliance Operator를 통해 관리자는 클러스터의 필수 컴플라이언스 상태를 설명할 수 있습니다. 그런 다음, Compliance Operator에서 제공된 컴플라이언스 격차와 해결 방안을 확인할 수 있습니다.
- **GPU 및 USB 패스스루를 승인 장치로 제한** 하여 연결된 하드웨어에서 무단 데이터 액세스 또는 코드 실행이 이루어질 리스크를 줄입니다.
- **비필수 기능 게이트를 비활성화하고 TLS(Transport Layer Security)를 사용하여 신뢰할 수 있는 컨테이너 레지스트리를 적용**함으로써 검증되지 않은 이미지 및 구성 오류에 노출되는 일을 제한합니다.

2 모든 계층에서 워크로드 제어

OpenShift Virtualization에서는 VM을 쿠버네티스 오브젝트로 관리하므로 워크로드를 생성, 수정 및 상호작용할 수 있는 사용자를 더욱 정교하게 제어할 수 있습니다. 중요 VM의 변경 사항이 컨테이너화된 애플리케이션과 동일한 거버넌스 모델에 따르도록 역할 기반 액세스 제어(RBAC) 및 감사 정책을 일관되게 적용할 수 있습니다.

- **고위 액세스, VNC(Virtual Network Computing) 콘솔 액세스 및 라이브 마이그레이션 작업은 승인된 관리자로 제한**하여 무단 변경 또는 데이터 노출의 리스크를 줄입니다.
- 필요하지 않을 때는 **게스트 메모리 과다 할당 및 공유 가능 디스크를 비활성화**하여 테넌트 간 리소스 경합을 줄이고 단일 워크로드가 손상된 경우 노출을 제한합니다.
- **일관된 오류 처리 및 검증 정책을 적용** 하여 서로 다른 환경에서 중요 워크로드에 일관되지 않은 동작이 발생하는 것을 방지하고 사전 경고 없이 발생하는 장애의 리스크를 줄입니다.

3 네트워크 트래픽 세분화를 통한 보안 태세 강화

OpenShift Virtualization의 보안은 네트워크 구성까지 확장됩니다. 네트워킹 제어가 컨테이너 및 VM 수준 모두에 적용되므로, 모든 워크로드에 마이크로 세그멘테이션 모델을 유지할 수 있습니다.

이러한 환경 전반에서 네트워크 정책, 관측성 및 로깅을 일관되게 적용하여 의심스러운 트래픽 패턴을 더 빠르게 감지하고 문제 해결을 간소화합니다.

- **VLAN(Virtual Local Area Network)을 사용하여 테넌트 또는 애플리케이션 트래픽을 격리**함으로써 네트워크 세그먼트 간의 내부 이동 리스크를 줄입니다.
- 민감한 워크로드에 **MAC(Media Access Control) 주소 스푸핑 필터링 및 멀티네트워크 정책을 적용**하여 네트워크상의 신원 스푸핑을 방지하고 가치가 높은 애플리케이션의 트래픽을 격리 유지합니다.
- SR-IOV(단일 루트 I/O 가상화) 인터페이스와 같은 **보조 네트워크의 명확한 경계를 정의**하고 이 네트워크를 특정 워크로드 또는 테넌트에 매핑함으로써 가상 스위치를 우회하는 트래픽의 제어 및 감사 가능성을 유지합니다.

4 스토리지의 데이터 무결성 보호

OpenShift Virtualization은 컴퓨팅 및 네트워킹과 동일한 관리 플레인에서 스토리지 보안 정책을 관리합니다.

가상 및 컨테이너화된 워크로드 전반에 동일한 암호화, 액세스 제어 및 복제 정책을 적용할 수 있어, 컴플라이언스 및 복구 계획이 간소해집니다. 이러한 제어를 중앙화하면 스토리지, 보안 및 플랫폼 팀이 일관된 정책하에 협업하고 시간 경과에 따라 감사하기가 더 쉬워집니다.

- **네임스페이스 간 DataVolume(DV) 복제를 제한**하여 민감한 데이터셋을 승인된 경계 내에 유지하고 규제 대상 정보나 고위험 정보가 의도치 않게 전파되는 일을 방지합니다.
- **필요 없는 경우, 공유 가능한 디스크를 비활성화**하여 워크로드 간의 의도치 않은 데이터 공유를 줄이고 동시 쓰기로 인해 손상이 발생할 리스크를 낮춥니다.
- 중요한 데이터에 대한 **errorPolicy 설정 및 스토리지 권한을 검증**하여 실패한 스토리지 작업이 예측 가능하게 처리되고 승인된 워크로드만 민감한 볼륨에서 읽기 또는 쓰기가 가능하도록 합니다.

다음 단계

OpenShift Virtualization 강화 가이드 전문을 읽고 하이브리드 클라우드에서 조직 IT 환경의 보안을 강화하는 방법을 종합적으로 확인하시기 바랍니다.