보안 모델 및 책임

Information Security for Workload Factory

NetApp
September 16, 2026

목차

보안 모델 및 책임

NetApp Workload Factory의 보안 모델에 대해 알아보십시오.

NetApp Workload Factory는 AWS 환경의 Amazon FSx for NetApp ONTAP에서 실행되는 워크로드를 관리하고 최적화하는 데 도움이 되는 SaaS 제어 플레인입니다. 보안 결과는 NetApp, AWS 및 조직 간의 공동 책임에 따라 달라집니다.

고수준 보안 모델

- Workload Factory는 IAM assume-role 모델을 사용하여 계정의 AWS API를 호출하기 위한 임시 AWS STS 자격 증명을 얻습니다.
- 일부 워크플로는 AWS API를 통해 노출되지 않는 ONTAP 네이티브 작업을 필요로 합니다. 이러한 작업은 고객이 배포한 실행 구성 요소(예: Lambda 링크)를 사용하여 VPC 내에서 실행할 수 있습니다.
- 관측 가능성 신호(측정 지표, 원격 측정 데이터 및 운영 기록)는 운영 모니터링 및 조사를 지원합니다.

주요 복습 질문

- Workload Factory는 AWS 계정에 대해 어떤 액세스 권한(역할 신뢰 + 권한)을 요구합니까?
- 의도하는 워크플로에 적용되는 실행 경로는 무엇입니까(AWS API 전용 또는 VPC 구성 요소를 통한 ONTAP 네이티브 작업)?
- 어떤 데이터 범주(구성/메타데이터, 운영 로그/이벤트, 텔레메트리)가 처리되며, 이러한 데이터는 어디에 저장됩니까?
- 어떤 모니터링 신호가 존재하며, 그 신호의 보존 특성은 무엇입니까?

다음 단계

- "NetApp Workload Factory의 공동 책임 경계"
- "NetApp Workload Factory의 연결 및 신뢰 경로"
- "NetApp Workload Factory의 최소 권한 권한 계층"

NetApp Workload Factory의 공동 책임 경계

NetApp Workload Factory의 보안 책임은 NetApp(SaaS 운영), AWS(클라우드 인프라 및 관리형 서비스), 그리고 고객(구성)이 공유합니다. 각 주체의 책임 범위를 명확히 이해하면 AWS 환경을 올바르게 구성하고 보안 취약점을 방지할 수 있습니다. 이러한 경계는 NetApp이 운영하는 부분, AWS가 보호하는 부분, 그리고 고객이 직접 구성하고 유지 관리해야 하는 부분을 명확히 합니다.

NetApp 책임 (서비스 측면)

NetApp은 Workload Factory SaaS 플랫폼의 운영 및 보안을 담당합니다. 여기에는 저장된 구성 참조 및 운영 데이터에 대한 서비스 측 처리가 포함됩니다.

AWS 관련 책임 (클라우드 플랫폼)

AWS는 배포 및 워크플로에서 사용하는 클라우드 인프라 및 관리형 서비스(IAM/STS, FSx for ONTAP, CloudWatch, KMS, Secrets Manager, CloudFormation, Lambda 및 네트워킹 기본 요소 등)의 보안을 담당합니다.

고객 책임 사항 (사용자 구성)

귀하는 다음 사항에 대한 책임이 있습니다:

- AWS IAM 역할, 신뢰 정책 및 최소 권한 부여
- VPC 제어(서브넷, 보안 그룹, 라우팅, 엔드포인트 및 송신)
- 자격 증명 거버넌스(워크플로우에 필요한 경우 ONTAP 자격 증명 포함)
- 암호화 및 키 관리 결정 사항(예: FSx for ONTAP의 선택적 고객 관리 KMS 키)
- 모니터링, 경고, 보존 정책 및 사고 대응 프로세스

캡처할 증거

- IAM 역할 신뢰 관계(외부 ID 조건 포함)
- IAM 권한 계층 선택 및 정책 아티팩트
- 네트워크 경계 결정 (AWS API 전용 vs. Lambda 링크 등 VPC 실행 구성 요소)
- 관찰 가능성 결정 및 유지 기대치
- AI 활성화 결정 (AI 진단은 명시적으로 비활성화하지 않는 한 기본적으로 활성화됩니다)

NetApp Workload Factory 온보딩 보안 워크플로

NetApp Workload Factory 온보딩은 제품 사용을 시작하기 전에 AWS 환경에 대한 안전한 액세스를 설정하는 과정입니다. 이 프로세스에는 AWS 신뢰 구성, 권한 범위 설정, 연결 설정, 관찰 가능성 검증 및 선택적 AI 진단 활성화가 포함됩니다.

1단계: 온보딩 방식 결정

- AWS 계정 및 환경 경계(예: 프로덕션과 비프로덕션 분리)를 식별합니다.
- 필요한 워크플로(읽기 전용 검색, 프로비저닝, ONTAP 네이티브 작업)를 식별합니다.
- 워크플로 요구 사항에 따라 VPC 실행 구성 요소(예: Lambda 링크)를 배포할지 여부를 결정합니다.
- AI 진단 활성화 여부를 결정합니다(기본적으로 활성화됨).

관련 정보

- "자격 증명 유형"
- "Lambda 링크 개요"
- "AI 제어 개요"

2단계: AWS 신뢰 및 액세스 설정

1. AWS 계정에 IAM 역할을 배포합니다.
2. 신뢰 정책에서 외부 ID를 사용하여 게이트 역할 가정을 설정합니다.
3. Workload Factory에 역할 ARN과 외부 ID를 등록합니다.

관련 정보

"AWS 계정 연동"

3단계: 최소 권한 권한 적용

1. 원하는 워크플로를 지원하는 최소 권한 등급을 선택하십시오.
2. 요청별 세션 정책이 수행 중인 작업으로만 작업을 제한하는지 확인합니다.

관련 정보

"NetApp Workload Factory의 최소 권한 권한 계층".

4단계: 연결 및 VPC 경계 구성(필요한 경우)

1. AWS 엔드포인트에 필요한 네트워크 경로를 검증합니다.
2. ONTAP 네이티브 작업이 필요한 경우 VPC에 적절한 실행 옵션을 배포하고 유효성을 검사하십시오.

관련 정보

- "NetApp Workload Factory의 연결 및 신뢰 경로"
- "NetApp Workload Factory용 ONTAP 실행 옵션"

5단계: 관찰 가능성 검증

1. 측정 지표와 원격 측정 데이터가 예상대로 수집 및 보존되는지 확인하십시오.
2. 문제 해결 및 조사에 필요한 운영 기록에 접근할 수 있는지 확인하십시오.

관련 정보

- "NetApp Workload Factory의 관찰 가능성 개요"
- "NetApp Workload Factory의 메트릭 및 원격 측정"

6단계: AI 진단 활성화(선택 사항)

AI 진단은 기본적으로 활성화되어 있습니다. 이 기능을 활성화하는 경우 필수 조건을 충족하는지 확인하고 범위 권한을 필요한 최소한으로 설정하십시오.

관련 정보

- "Bedrock에서 NetApp Workload Factory AI 진단 옵트인"
- "NetApp Workload Factory용 AI 툴 경계"

NetApp Workload Factory의 규정 준수 및 보안 태세

NetApp Workload Factory는 규정 준수 및 보안을 핵심 우선순위로 삼아 구축되었습니다. Workload Factory의 모든 워크로드는 Amazon FSx for NetApp ONTAP에서 실행됩니다. 또한 "AWS 보안 기능", NetApp Workload Factory에는 "SOC2 Type 1, SOC2 Type 2 및 HIPAA 규정 준수"가 있습니다.

Amazon FSx for NetApp ONTAP for NetApp Workload Factory는 "기업용 애플리케이션 배포를 위한 AWS 솔루션 "이며, AWS Well-Architected 모범 사례를 따릅니다.

저작권 정보

상표 정보