



Ask Me AI 어시스턴트 Information Security for Workload Factory

NetApp
September 16, 2026

목차

Ask Me AI 어시스턴트	1
NetApp Workload Factory용 Ask Me 보안 아키텍처	1
Ask Me의 RAG 아키텍처	1
다중 계층 프롬프트 보안	1
모델 데이터 격리 및 개인 정보 보호	1
툴 사용 및 에이전트 보안	2
NetApp Workload Factory용 Ask Me 액세스 제어	2
인증	2
자격 증명 보호 및 기밀 처리	2
인프라 보안	2
NetApp Workload Factory의 Ask Me 실행 모드	2
툴 실행 보호 장치	3
출력 제어	3
NetApp Workload Factory용 Ask Me 개인 정보 보호 및 가용성	3
데이터 처리 및 개인정보 보호	3
가용성 및 격리 제어	3

Ask Me AI 어시스턴트

NetApp Workload Factory용 Ask Me 보안 아키텍처

Ask Me는 NetApp Workload Factory 내에 내장된 생성형 AI 기반 어시스턴트입니다. Amazon FSx for NetApp ONTAP 및 Workload Factory 주제에 대한 실시간 대화형 지원을 제공합니다. 답변은 검증된 NetApp 문서를 기반으로 하며, Ask Me는 퍼블릭 인터넷에 액세스하거나 모델을 학습시키는 데 고객 데이터를 사용할 수 없습니다. 다중 보안 레이어는 악성 쿼리를 차단하고, 지원되는 도메인으로 답변을 제한하며, 사용자 입력이 시스템 지침을 재정의하지 못하도록 방지합니다. Ask Me가 톨을 사용할 때 권한 부여 경계, 읽기 전용 쿼리 적용, 임시 샌드박스 및 감사 로깅은 실행을 제한하고 모니터링하는 데 도움이 됩니다.

Workload Factory 관리 설정에서 언제든지 Ask Me를 옵트아웃할 수 있으며, 이렇게 하면 사용자 계정에 대한 어시스턴트가 비활성화됩니다. ["GenAI 기능 관리에 대해 자세히 알아보십시오."](#)

Ask Me의 RAG 아키텍처

Ask Me는 검색 증강 생성(RAG)을 사용합니다.

- 엄선된 지식 기반: 답변은 검증되고 게시된 NetApp 문서 모음을 기반으로 합니다.
- 검색 점수화 및 필터링: 충분히 관련성이 높은 콘텐츠만 모델 컨텍스트에 포함됩니다.
- 인터넷 접속 불가: 모델이 외부 콘텐츠를 가져오거나, 검색하거나, 스크래핑할 수 없습니다.
- 출처 표기: 답변에는 사용된 출처 문서에 대한 참조가 포함됩니다.

다중 계층 프롬프트 보안

- 1단계: 보안 분류기(LLM-as-a-judge)는 악의적인 쿼리(프롬프트 주입, 권한 상승, 데이터 유출, 소셜 엔지니어링, 정책 위반)를 차단합니다.

시스템은 차단된 쿼리를 기록하지만, 생성 모델은 이를 전혀 인식하지 못합니다.

- 2단계: 시스템 프롬프트 강화는 사용자 입력이 시스템 명령을 덮어쓰는 것을 방지합니다.
- 레이어 3: 도메인 범위 지정으로 인해 FSx ONTAP 및 Workload Factory 주제에 대한 응답이 제한됩니다.
- 레이어 4: 톨 사용 거버넌스는 강화된 샌드박스에서 매개변수를 검증하고 쿼리를 실행합니다. 모델은 임의의 작업을 실행할 수 없습니다.

모델 데이터 격리 및 개인 정보 보호

- 고객 데이터를 사용한 모델 학습 없음
- 요청 수준 격리(테넌트 간 데이터 유출 방지)
- 제한된 기록을 가진 세션 범위의 대화 컨텍스트
- 영구적인 모델 메모리 없음
- 관리형 추론 인프라

툴 사용 및 에이전트 보안

- 권한 범위 기반 툴(사용자 권한 경계 적용)
- 엄격한 툴 실행 시간 제한
- 검색된 데이터를 위한 임시 세션 범위 샌드박스
- 허용 목록을 사용한 읽기 전용 쿼리 강제 적용
- 민감한 매개변수 스크리빙을 통한 툴 호출 감사 기능

NetApp Workload Factory용 Ask Me 액세스 제어

NetApp Workload Factory의 Ask Me 액세스 보안은 인증된 세션, 사용자 수준의 책임, 런타임 작업 중 보호된 비밀 키 처리에 중점을 둡니다. 인증 제어는 각 세션을 검증하고 상호 작용을 특정 사용자와 연결합니다. 민감한 자격 증명은 런타임에 관리되는 비밀 키 저장소에서 검색되고 로그에서 삭제됩니다. 또한 이 서비스는 루트 권한이 없는 컨테이너 실행 및 제한된 CORS 허용 목록을 포함한 인프라 제어를 적용합니다.

인증

- 대상, 발급자 및 RS256 등 알고리즘 검사를 포함한 암호화 검증을 통한 서명된 JWT 인증
- 서비스 경계에서 미들웨어를 이용한 인증
- 사용자 ID 범위를 지정하여 상호 작용이 특정 사용자에게 귀속되도록 합니다.

자격 증명 보호 및 기밀 처리

- 안전한 저장소: 서비스에서 사용하는 민감한 자격 증명은 관리형 비밀 저장소에 저장되며 런타임에 검색됩니다. 비밀 정보는 애플리케이션 코드, 구성 파일 또는 컨테이너 이미지에 저장되지 않습니다.
- 로그 정제: 민감한 값(자격 증명, 토큰, 암호, 액세스 키, 인증서)은 로그에 기록되기 전에 삭제됩니다.

인프라 보안

- 루트 권한이 없는 컨테이너 실행
- CORS는 신뢰할 수 있는 NetApp 도메인의 명시적인 허용 목록으로 제한됩니다.

NetApp Workload Factory의 Ask Me 실행 모드

NetApp Workload Factory는 Ask Me에 대해 서로 다른 보안 및 개인 정보 보호 특성을 가진 여러 실행 모드를 제공합니다. Ask Me가 툴 통합을 사용하는 경우(예: 고객의 Workload Factory 리소스를 쿼리하는 경우), 툴 실행은 계층화된 보안 조치를 통해 제어됩니다. 툴을 사용한 실행은 인증된 사용자의 권한 범위 내에서 작동하며 각 작업의 지속 시간과 범위에 제한이 적용됩니다. 검색된 데이터는 외부 액세스가 차단되는 임시 세션 샌드박스에 저장되며 세션이 종료되면 삭제됩니다. 독립적인 프롬프트 및 코드 제어를 통해 읽기 전용 쿼리가 적용되며, 감사 기록은 민감한 값이 삭제된 상태로 툴 활동을 기록합니다.

툴 실행 보호 장치

- 권한 범위 툴은 인증된 사용자의 권한 내에서 작동합니다.
- 툴 실행 시간 초과는 장시간 실행되는 작업을 제한합니다.
- 임시 데이터 샌드박스는 툴로 검색된 데이터를 세션 범위 내에 저장하고, 외부 액세스, 파일 I/O, 네트워크 호출 및 엔진 수준에서의 확장 프로그램 로딩을 차단하며, 세션이 종료되면 소멸됩니다.
- 읽기 전용 쿼리 강제 적용은 엄격한 허용 목록을 통해 생성된 쿼리의 유효성을 검사합니다.
- 프롬프트 적용 보안과 코드 적용 보안은 독립적으로 적용됩니다.
- 툴 호출 감사 기능은 툴 이름, 매개변수, 타임스탬프 및 결과 상태를 로깅하며, 민감한 값은 스크리빙됩니다.

출력 제어

- 토큰 제한 시행
- 분류/보안 중요 작업에 대한 결정론적 출력(온도 0)
- 조기 종료 및 정리 기능을 갖춘 스트리밍

NetApp Workload Factory용 Ask Me 개인 정보 보호 및 가용성

NetApp Workload Factory의 Ask Me 개인정보 보호 제어는 데이터 노출을 제한하고, 세션 처리를 격리하며, 사용자 상호 작용에 대한 개인정보 보호 경계를 유지합니다. 사용자의 입력은 관리형 AI 서비스에서 처리되며, 이 서비스는 해당 입력을 기본 모델 학습이나 개선에 사용하지 않습니다. 검색된 운영 데이터는 세션 기간 동안 임시 메모리 저장소에 보관되며 영구 저장되거나 공유되지 않습니다. 여러 클라우드 지역에 걸쳐 있는 멀티 모델 풀백 체인은 기본 모델의 성능 저하 또는 사용 불가 시에도 가용성을 보장하며, 풀백 모델에도 동일한 보안 제어가 적용됩니다.

데이터 처리 및 개인정보 보호

- 프롬프트에 포함된 사용자 데이터: 사용자의 입력을 기본 모델 학습 또는 개선에 사용하지 않는 관리형 AI 서비스에서 처리됩니다.
- 기술 자료 콘텐츠: 엄선되어 게시된 NetApp 문서만 포함되며, 사용자 데이터는 포함되지 않습니다.
- 운영 데이터: 사용자가 자신의 리소스를 조회할 때만 검색되며, 세션 기간 동안 임시 메모리 저장소에 보관되고 영구 저장되거나 공유되지 않습니다.
- 감사 로깅: 쿼리 메타데이터(익명 처리된 사용자 ID, 타임스탬프, 지속 시간)가 기록되며, 민감한 필드는 삭제됩니다.
- 피드백 데이터: 별도로 저장되며 쿼리 ID에 연결되고, 익명화된 사용자 ID 외의 개인 식별 정보와는 연결되지 않습니다.

가용성 및 격리 제어

Ask Me는 여러 클라우드 지역에 걸쳐 다중 모델 대체 체인을 사용합니다.

기본 모델이 조절되거나 사용할 수 없는 경우, 시스템은 대체 모델로 페일오버할 수 있습니다.

모든 모델은 동일한 보안 제어, 시스템 프롬프트 강화 및 격리 보장이 적용됩니다.

저작권 정보

Copyright © 2026 NetApp, Inc. All Rights Reserved. 미국에서 인쇄된 본 문서의 어떠한 부분도 저작권 소유자의 사전 서면 승인 없이는 어떠한 형식이나 수단(복사, 녹음, 녹화 또는 전자 검색 시스템에 저장하는 것을 비롯한 그래픽, 전자적 또는 기계적 방법)으로도 복제될 수 없습니다.

NetApp이 저작권을 가진 자료에 있는 소프트웨어에는 아래의 라이선스와 고지사항이 적용됩니다.

본 소프트웨어는 NetApp에 의해 '있는 그대로' 제공되며 상품성 및 특정 목적에의 적합성에 대한 명시적 또는 묵시적 보증을 포함하여(이에 제한되지 않음) 어떠한 보증도 하지 않습니다. NetApp은 대체품 또는 대체 서비스의 조달, 사용 불능, 데이터 손실, 이익 손실, 영업 중단을 포함하여(이에 국한되지 않음), 이 소프트웨어의 사용으로 인해 발생하는 모든 직접 및 간접 손해, 우발적 손해, 특별 손해, 징벌적 손해, 결과적 손해의 발생에 대하여 그 발생 이유, 책임론, 계약 여부, 엄격한 책임, 불법 행위(과실 또는 그렇지 않은 경우)와 관계없이 어떠한 책임도 지지 않으며, 이와 같은 손실의 발생 가능성이 통지되었다 하더라도 마찬가지입니다.

NetApp은 본 문서에 설명된 제품을 언제든지 예고 없이 변경할 권리를 보유합니다. NetApp은 NetApp의 명시적인 서면 동의를 받은 경우를 제외하고 본 문서에 설명된 제품을 사용하여 발생하는 어떠한 문제에도 책임을 지지 않습니다. 본 제품의 사용 또는 구매의 경우 NetApp에서는 어떠한 특허권, 상표권 또는 기타 지적 재산권이 적용되는 라이선스도 제공하지 않습니다.

본 설명서에 설명된 제품은 하나 이상의 미국 특허, 해외 특허 또는 출원 중인 특허로 보호됩니다.

제한적 권리 표시: 정부에 의한 사용, 복제 또는 공개에는 DFARS 252.227-7013(2014년 2월) 및 FAR 52.227-19(2007년 12월)의 기술 데이터-비상업적 품목에 대한 권리(Rights in Technical Data -Noncommercial Items) 조항의 하위 조항 (b)(3)에 설명된 제한사항이 적용됩니다.

여기에 포함된 데이터는 상업용 제품 및/또는 상업용 서비스(FAR 2.101에 정의)에 해당하며 NetApp, Inc.의 독점 자산입니다. 본 계약에 따라 제공되는 모든 NetApp 기술 데이터 및 컴퓨터 소프트웨어는 본질적으로 상업용이며 개인 비용만으로 개발되었습니다. 미국 정부는 데이터가 제공된 미국 계약과 관련하여 해당 계약을 지원하는 데에만 데이터에 대한 전 세계적으로 비독점적이고 양도할 수 없으며 재사용이 불가능하며 취소 불가능한 라이선스를 제한적으로 가집니다. 여기에 제공된 경우를 제외하고 NetApp, Inc.의 사전 서면 승인 없이는 이 데이터를 사용, 공개, 재생산, 수정, 수행 또는 표시할 수 없습니다. 미국 국방부에 대한 정부 라이선스는 DFARS 조항 252.227-7015(b)(2014년 2월)에 명시된 권한으로 제한됩니다.

상표 정보

NETAPP, NETAPP 로고 및 <http://www.netapp.com/TM>에 나열된 마크는 NetApp, Inc.의 상표입니다. 기타 회사 및 제품 이름은 해당 소유자의 상표일 수 있습니다.