Prisma AIRS® 런타임 보안

새로운 위협으로부터 AI 에코시스템 보호

엔터프라이즈 AI 애플리케이션은 진화하는 위협 환경에 직면해 있습니다. 조직은 고객 서비스 및 직원 생산성 향상과 같은 업무를 지원하기 위해 애플리케이션에 AI를 빠르게 도입하고 있습니다. 그러나 이러한 AI 애플리케이션은 기존 보안 솔루션으로는 보호할 수 없는 AI에 특화된 위협에 직면해 있습니다.

애플리케이션에 AI를 통합하는 것은 단순히 AI 모델을 추가하는 플러그 앤 플레이 프로세스 그 이상입니다. AI 애플리케이션이 가장 정확하고 가치 있는 응답을 제공하려면 "복합 시스템"으로 구축해야 합니다. 이를 위해서는 전체 AI 스택을 구현해야 하며, 여기에는 본질적으로 민감한 내부 데이터에 대한 액세스를 관리하고 보호하는 작업이 포함됩니다. 즉, 다중 AI 모델, 플러그인, 벡터 데이터베이스, 심지어 인터넷 검색 기능까지 원활하게 통합할 수 있습니다. AI 애플리케이션의 각 새로운 요소로 인해 공격자가 런타임 작업 중에 악용할 수 있는 잠재적 취약점이 생깁니다.

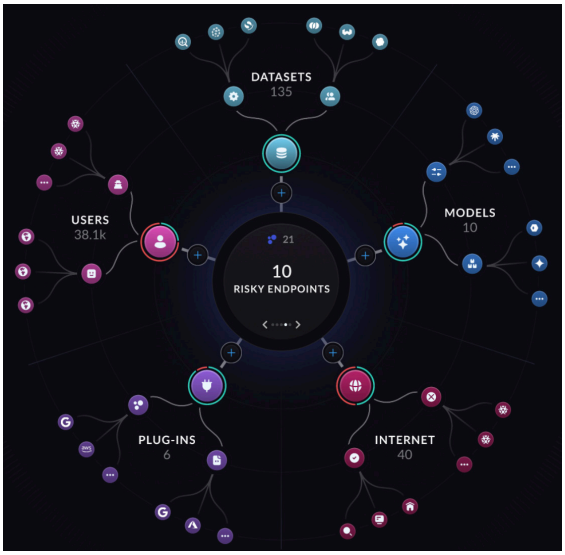
귀사와 같은 조직이 AI 환경을 방어할 준비를 갖추려면 이를 지원하는 엔터프라이즈 AI 보안 솔루션이 필요합니다:

- AI 에코시스템(AI 애플리케이션, 모델, 사용자, 데이터 세트)을 자동으로 **검색합니다.**
- AI에 특화된 근본적인 공격으로부터 모델, 데이터, 앱을 **보호합니다.**
- AI 에코시스템의 런타임 위험 노출을 지속적으로 **모니터링합니다.**

주요 이점	
네트워크 인터셉트	**API 인터셉트**
• 수천 개의 앱과 프로토콜을 위한 애플리케이션 레이어 디코딩 및 세분화입니다. • Google Cloud, AWS, Azure의 40개 이상의 모델을 보호하고 OpenAI API에 직접 호출하는 트래픽을 보호합니다. • 하나의 솔루션으로 네트워크, 기본 및 AI에 특화된 위협을 보호합니다. • 기본 제공되는 이스트-웨스트 트래픽 검사로 컨테이너화되고 가상화된 워크로드를 보호합니다. • 클라우드 제공 보안 서비스(CDSS)로 어디서나 일관된 동급 최고의 보호 기능을 제공합니다. › 25개 이상의 DNS 공격 유형을 포함하여 웹 기반 공격으로부터 40% 더 효과적으로 보호합니다. › AI 기반 제로데이 애플리케이션 명령 및 SQL 인젝션 공격의 90% 이상을 방지합니다. • 동급 최고의 데이터 보호: › 다른 클라우드 기반 데이터 유출 방지 솔루션보다 2배 더 넓은 범위의 데이터를 보호합니다. › 1,000개 이상의 사전정의된 데이터 패턴이 있습니다. › 99%의 멀웨어 탐지 정확도로 기존 샌드박스보다 26% 더 많은 탐지가 가능합니다.	• 완전히 독립적인 배포 - 퍼블릭 또는 프라이빗 모델에 관계없이 보안을 유지합니다. • 암호 해독 오버헤드 없이 AI 앱, 모델 및 데이터를 보호합니다. • 로우코드/노코드 환경에서 AI 에이전트를 보호합니다. • 에이전트 위협 • 모든 AI 애플리케이션에 대한 세분화된 탐지 및 보호가 가능합니다. › 탐지된 위협에 따라 사용자에게 사용자 지정 오류 응답을 반환합니다.

제품 기능

AI 에코시스템 알아보기 및 이해하기



Prisma AIRS 플랫폼의 이 핵심 구성 요소를 사용하면 AWS, Microsoft Azure, GCP의 클라우드 환경이 AI 애플리케이션을 어떻게 사용하고 있는지 이해할 수 있습니다. 직관적인 온보딩 프로세스를 통해 사용자는 Terraform 템플릿을 빠르게 생성하여 데이터 흐름을 분석하고 자산 인벤토리를 시각화하고 서로 소통하는 방식을 이해할 수 있습니다. 이를 통해 AI 애플리케이션을 관련 모델, 사용자, 외부 사이트, 플러그인, 데이터 소스에 상세하게 매핑하여 복잡하고 때로는 알려지지 않은 상호 연결을 파악할 수 있습니다.

이러한 관계를 시각화하고 이해함으로써 사용자는 AI 인프라에 대한 심층적인 인사이트를 확보하여 정보에 입각한 결정을 내리고 Prisma AIRS Runtime Security 인스턴스를 배치하고 선제적으로 관리하여 클라우드 기반 AI 구현의 효율성, 보안 및 규정 준수를 강화할 수 있습니다.

AI에 특화된 위협으로부터 보호

애플리케이션 보호

고급 URL Filtering 기능을 핵심으로 하는 최첨단 CDSS를 활용하여 악성 URL에 대한 강력한 방어를 보장함으로써 AI 애플리케이션을 보호합니다. AI 애플리케이션과 모델 간에 이동하는 URL을 스캔하고 탐지하여 애플리케이션이 악성 URL을 표시하거나 가져오는 것을 차단(또는 플래그 지정)할 수 있도록 합니다. 이렇게 하면 애플리케이션이나 최종 사용자가 오염된 검색 증강 생성(RAG) 또는 학습 데이터 세트로 인해 모델 출력에 나타날 수 있는 악성 URL을 수신하지 못하게 됩니다.

또한, AI 앱의 URL 보안은 앱이나 최종 사용자가 가져오려고 시도할 수 있는, URL 매개 변수에 민감한 데이터가 임베딩되는 공격자 소유 도메인이 포함된 URL을 컴파일하도록 AI 모델을 속여 데이터를 공격자의 서버로 전송하는 데이터 유출 공격을 방지합니다. 또한 모델 입력 또는 출력에 나타나는 특정 URL 도메인을 허용, 경고 또는 차단하는 정책을 구성하여 세분화된 RAG 웹 액세스 제어를 시행할 수 있습니다.

또한 Prisma AIRS Runtime Security를 사용하면 환경 내의 모든 애플리케이션 구성 요소를 세부적으로 세분화하여 포트 간 트래픽부터 네임스페이스 간 트래픽까지 모든 통신 경로를 보호함으로써 알려진 공격과 제로데이 애플리케이션 계층 공격을 효과적으로 방지할 수 있습니다.

그림 1. 현재 보호 상태 및 경고된 위협을 보여주는 대시보드

모델 보호

직접 및 간접 프롬프트 인젝션과 같은 위협으로부터 AI 애플리케이션을 방어합니다. 이러한 시스템의 무결성을 유지하려면 단순한 사칭을 넘어 다양한 유형의 프롬프트 인젝션 공격을 방어하는 것이 중요합니다. Prisma AIRS AI Runtime Security는 목표 하이재킹 및 DAN(do-anything-now) 공격과 같은 프롬프트 인젝션을 차단할 수 있습니다.

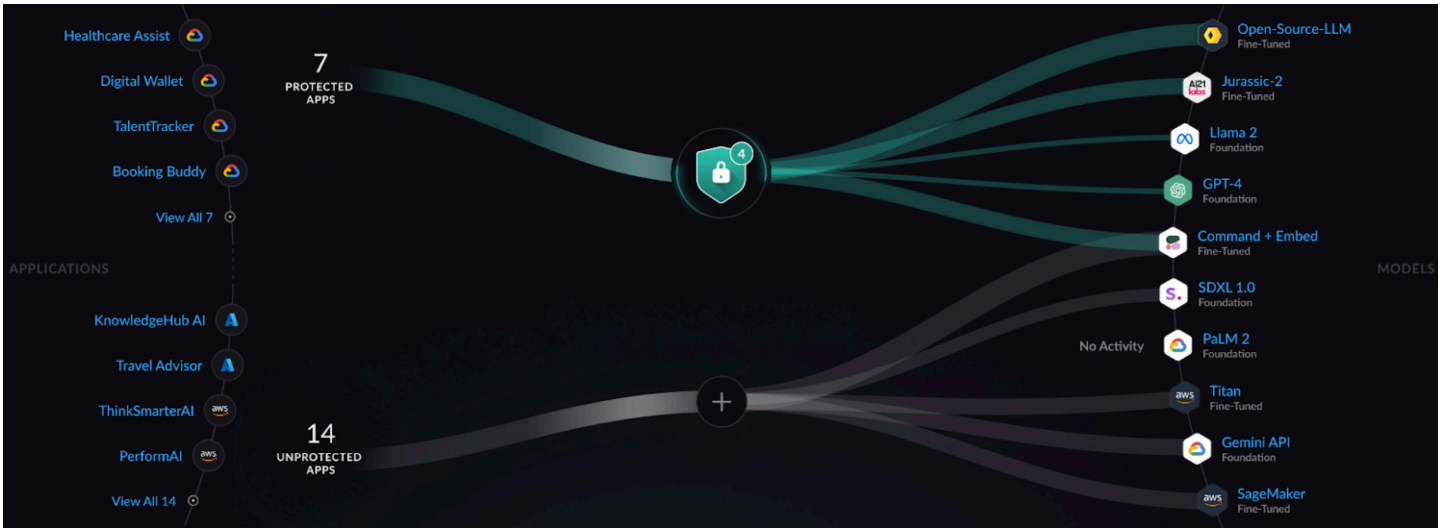


그림 2. Prisma AIRS Runtime Security 인스턴스의 배치와 애플리케이션과 모델 간의 연결을 보여주는 모델 보기

데이터 보호

기본 제공되는 엔터프라이즈 데이터 손실 방지(DLP) CDSS로 AI 애플리케이션에서 데이터 유출을 차단합니다. 사용자 환경에 정교하게 조정된 모델을 배포하고 훈련할 때, 애플리케이션 출력에서 훈련 데이터가 유출되지 않도록 해야 합니다. Prisma AIRS Runtime Security에 내장된 데이터 보호 기능은 1,000개 이상의 사전정의된 데이터 패턴(정규식 및 ML 기반)을 감지하고 프롬프트 및 응답에서 사용자 지정 데이터 패턴을 지원할 수 있으며 다른 클라우드 기반 데이터 유출 방지 솔루션에 비해 두 배의 커버리지가 있습니다.

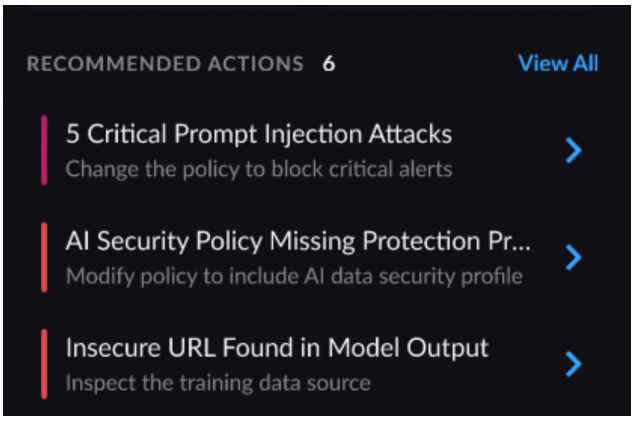
AI 모델을 사용하여 데이터베이스 쿼리를 생성하는 AI 애플리케이션의 경우, 모델에서 반환할 수 있는 쿼리 스크립트 유형(생서, 읽기, 업데이트, 삭제)을 규제하여 데이터베이스의 무단 변경을 방지합니다(현재 SQL 지원).

에이전트 위협 보호

기업이 AI 에이전트(노코드/로우코드 플랫폼에서 구축된 에이전트 포함)를 점점 더 많이 사용하면서 이러한 에이전트 자체의 보안이 무엇보다 중요해졌습니다. Prisma AIRS는 신원 사칭, 메모리 조작 등 새로운 에이전트 위협으로부터 방어하기 위한 AI 에이전트 보안을 제공합니다. 또한, AI 에이전트에 연결된 도구와 API가 남용되지 않도록 하여 도구 오용을 방지합니다.

런타임 위험 모니터링

Prisma AIRS Runtime Security는 AI 런타임 위험 태세를 지속적으로 분석하여 운영 중인 AI 시스템 내의 취약성에 대한 명확한 인사이트를 제공함으로써 AI 환경을 보호하도록 설계되었습니다. 조직 전체에서 보호되지 않은 AI 애플리케이션을 지속적으로 평가하여 필수 보안 조치가 부족한 애플리케이션을 식별합니다. 종합적인 보호를 보장하기 위해 이 소프트웨어는 AI 애플리케이션에서 발생하는 위험한 통신 경로를 정확히 찾아내어 악성 활동의 잠재적 진입 지점을 식별합니다. 이러한 사전 예방적 접근 방식을 통해 조직은 AI 애플리케이션을 보호하고 위험 노출을 줄이며 진화하는 사이버 보안 환경에서 강력한 방어 체계를 유지할 수 있습니다.



유연한 배포 옵션

Prisma AIRS Runtime Security를 배포하여 AI 애플리케이션과 관련 모델, 사용자, 외부 사이트, 플러그인, 에이전트 및 데이터 소스 간의 데이터 및 트래픽 흐름을 보호합니다. Palo Alto Networks는 인프라 및 애플리케이션 요구사항에 맞는 AI 보안을 지원합니다. 중앙 집중식 네트워크 인터셉트(AWS, Azure, GCP 환경의 경우)를 통해 애플리케이션을 보호하거나 API 인터셉트(모든 앱, 환경, 모델의 경우)를 통해 세분화된 보호 기능을 제공합니다. 조직은 옵션 두 가지 중 하나 또는 두 가지 모두를 선택할 수 있지만 정책을 한 번만 정의하고 필요할 때 필요한 곳에 적용하면 됩니다.

자동 또는 수동 네트워크 배포

Strata™ Cloud Manager는 대상 클라우드 환경에 권장되는 모범 사례 아키텍처 스크립트가 포함된 Terraform 템플릿을 제공하여 Google Cloud, AWS 및 Azure 환경으로 자동화된 네트워크 기반 배포를 오케스트레이션합니다. 수동 배포의 경우, 이미지 및 부트스트랩 변수를 선택하고 Prisma AIRS Runtime Security 인스턴스를 퍼블릭 클라우드에 수동으로 배포합니다. 이는 가상화 및 컨테이너 환경에 대한 원활한 보안을 제공하여 Kubernetes 클러스터 내의 이스트-웨스트, 아웃바운드 및 인바운드 보호와 앱 간, 앱과 모델 간, 앱과 데이터베이스 간 상호 작용을 포함한 포괄적인 트래픽 보호를 보장합니다. Prisma AIRS Runtime Security 인스턴스는 노스-사우스 공격으로부터 보호할 뿐만 아니라 컨테이너화된 애플리케이션과 컨테이너화되지 않은 애플리케이션의 무결성을 유지하는 데 중요한 포트 간 격리 기능도 제공합니다.

자세한 내용은 AWS, Microsoft Azure 및 Google Cloud용 배포 가이드를 참조하십시오.

개발자 및 AI 에이전트를 위한 API 기반 배포

개발자는 소프트웨어 개발 사례를 사용하여 AI 애플리케이션 및 AI 에이전트에서 AI 보안의 관리 및 배포를 자동화할 수 있습니다. AI에 특화된 공격으로부터 보호하는 코드를 사용하여 애플리케이션에 AI 보안을 빠르고 간단하게 임베드할 수 있습니다. 이 API 기반 기능을 통해 개발자는 알려진 위협과 알려지지 않은 위협으로부터 AI 애플리케이션과 에이전트를 실시간으로 보호하는 동시에 사용자 지정 오류 동작 및 사용자별 정책을 포함한 세분화된 보호 기능을 사용할 수 있습니다. 또는 개발자(및 탐지 엔지니어)가 분석을 위해 비동기식으로 데이터를 수집합니다. 또한 개발자는 API를 통해 RAG 데이터 소스에서 오염 또는 PII를 스캔할 수 있습니다.

Palo Alto Networks는 모든 환경의 모든 AI 앱, 에이전트, 워크로드, 모델을 보호할 수 있도록 지원합니다. 애플리케이션 및 인프라의 요구 사항에 맞게 네트워크 기반(이미 실행된) 및/또는 코드 기반(신규) 인터셉트를 사용하여 배포합니다.

유연한 소비 모델

고객은 기존 Flexible Software NGFW(FW-Flex) 크레딧을 획득하거나 사용하여 Strata Cloud Manager에서 Prisma AIRS Runtime Security 인스턴스를 배포하고 조달 장애를 최소화하면서 신속하게 보안을 재구성할 수 있습니다. API 기반 인스턴스의 경우 개발자는 FW-Flex 크레딧을 통해 지원 포털에서 배포 프로파일을 생성할 수 있으며, 이를 통해 Strata Cloud Manager에서 API 키를 생성할 수 있습니다. 그런 다음 이 키를 사용하여 애플리케이션 코드에서 API 호출을 수행할 수 있습니다.

제품 사양

네트워크 기반 인터셉트에 대한 클라우드별 AI 모델 지원은 지원 표를 참조하십시오.

용량 및 처리량 정보는 VM-Series 데이터시트를 참조하십시오.

리소스

- Prisma AIRS 제품 페이지
- 소프트웨어 NGFW 크레딧 추정기
- 소프트웨어 방화벽 선택기
- VM-Series 데이터시트

이 데이터시트 정보

본 백서와 함께 제공되는 기술 또는 전문 주제에 관한 정보는 일반적인 이해를 돕기 위한 것이며, 변경될 수 있으며, 법률적 또는 전문적인 조언이나 특정 목적에의 적합성 또는 관련 법률 준수에 대한 보증을 구성하지 않습니다.

3000 Tannery Way
Santa Clara, CA 95054

대표 전화: +1.408.753.4000
판매 문의: +1.866.320.4788
지원 문의: +1.866.898.9087

www.paloaltonetworks.com

prisma_ds_제목_날짜