

Firewall for AI

Akamai Firewall for AI는 새롭게 등장하는 사이버 위협으로부터 AI 기반 애플리케이션, 대규모 언어 모델(LLM), AI 기반 API를 보호하도록 설계된 전용 보안 솔루션입니다. 이 방화벽은 인바운드 AI 쿼리와 아웃바운드 AI 응답을 보호해, 생성형 AI 기술이 초래할 수 있는 보안 취약점을 차단합니다.

실시간 탐지, 정책 기반 적용, 적응형 보안 조치를 통해 프롬프트 삽입 공격, 민감한 데이터 유출, 공격적 악용, AI 특화 DoS(서비스 거부) 공격 등으로부터 AI 환경을 방어합니다.

Firewall for AI는 엣지, 클라우드, 하이브리드, 온프레미스 환경 전반에 원활하게 통합되어, 보안의 일관성, 안전성, 거버넌스, 컴플라이언스를 보장하고 성능 저하 없이 운영됩니다.

AI 위협 방어

Firewall for AI는 기존 보안 툴로는 해결하지 못하는 AI 고유의 취약점을 식별하고 방어함으로써 AI 기반 애플리케이션에 대한 포괄적인 보안을 제공합니다.

- **프롬프트 삽입 차단** — 공격자가 교묘한 입력을 통해 AI 모델을 조작하지 못하도록 방지합니다.
- **데이터 유출 차단(DLP)** — AI 응답에서 민감한 데이터 유출을 탐지하고 차단하며, 요청을 통해 민감한 데이터를 수신하지 못하도록 보호합니다.
- **유해하고 해로운 콘텐츠 필터링** — 혐오 표현, 가짜 정보, 공격적인 콘텐츠를 사전에 식별하고 차단합니다.
- **적대적 AI 보안** — 원격 코드 실행, 모델 백도어, 데이터 중독 공격으로부터 보호합니다.
- **DoS 방어** — 과도한 쿼리 사용과 모델 과부하를 제어해 AI 기반 DoS 공격을 방어합니다.

기업이 누릴 수 있는 장점

-  **통합된 AI 보안 체계**
엣지, 클라우드, 하이브리드, 온프레미스 전반에 걸친 표준화된 AI 보안 제공
-  **자동화된 AI 위협 탐지**
수동으로 룰을 조정하지 않는 AI 전용 보안 기능 제공
-  **WAAP와의 원활한 통합**
AI 방어를 추가해 웹 애플리케이션 및 API 보안(WAAP) 기능을 확장
-  **AI 오용 및 법적 리스크 방지**
데이터 유출, IP 도용, 규제 위반 차단
-  **AI 보안 간소화**
사내 엔지니어가 보안 정책을 수동으로 적용하지 않아도 됨
-  **멀티클라우드의 유연성**
환경 전반에서 AI 워크로드 보호
-  **엔터프라이즈급 AI 보호**
Akamai의 글로벌 위협 인텔리전스 지원

유연한 배포 옵션

Firewall for AI는 다양한 AI 아키텍처와 클라우드 환경에 맞게 조정된 여러 가지 배포 모델을 제공합니다.

배포 모델	설명
Akamai 엣지 통합	Akamai 엣지에서 저지연 보안 적용을 통해 인라인으로 AI 애플리케이션을 보호합니다.
REST API	API 기반의 리스크 탐지 및 점수 산출을 통해 AI 입력 및 출력을 스캔합니다.
역방향 프록시 배포(로드맵 기능)	심층 검사 및 필터링을 위해 Akamai의 보안 프록시를 통해 AI 트래픽을 라우팅합니다.

이러한 유연성 덕분에 기업은 멀티클라우드, 하이브리드, 온프레미스 환경 등 모든 배포 환경에서 LLM을 보호할 수 있습니다.

작동 방식

AI 트래픽 분석

방화벽은 AI 상호작용을 모니터링하고 분석해, 수신 사용자 프롬프트와 AI가 생성한 출력을 검사함으로써 잠재적인 위협이 모델이나 최종 사용자에게 도달하기 전에 탐지합니다. 방화벽은 AI 쿼리 및 응답 주기를 분석함으로써 보안 리스크를 효과적으로 방지하고 애플리케이션 성능을 유지합니다.

리스크 점수 및 적응형 위협 대응

프롬프트 삽입, 민감한 데이터 노출, 공격적 악용 등 여러 가지 보안 지표를 기반으로 AI 상호작용을 평가합니다.

보안 적용 조치

Firewall for AI는 리스크 점수와 고객의 리스크 수용 정도에 따라 세 가지 중요한 보안 조치를 시행합니다.

- **모니터링:** AI 쿼리 또는 응답을 방해하지 않고 분석을 위해 탐지된 위협을 기록합니다.
- **수정:** 자연스러운 대화 흐름을 유지하면서 AI가 생성한 출력을 조정해 안전하지 않은 콘텐츠를 제거하거나 변경합니다.
- **거부:** 리스크가 높은 입력이 AI 모델에 들어가는 것을 차단하고 안전하지 않은 응답이 사용자에게 반환되는 것을 방지합니다.

컴플라이언스 및 거버넌스 신뢰

Firewall for AI는 보안 및 컴플라이언스 기준을 준수하도록 지원합니다. AI 기반 애플리케이션으로 인해 새로운 규제 문제가 발생하면서 데이터 프라이버시, 모델 무결성, 보안 리스크에 대한 감독을 유지하는 것이 중요합니다.

규제 준수

방화벽은 기업이 프라이버시, 안전, 보안 지침을 준수하는 데 도움이 될 수 있습니다. 기업은 AI 전용 보안 정책을 시행함으로써 데이터 보호 규정, 윤리적 AI 사용, 기업 거버넌스 의무와 관련된 리스크를 방어할 수 있습니다.



보안 애널리틱스 및 로깅

Firewall for AI는 상세한 감사 로그와 실시간 보안 애널리틱스를 제공해 보안팀이 AI 보안 이벤트에 대한 가시성을 확보할 수 있도록 합니다. 기업은 쿼리 패턴, 위협 지표, 대응 행동을 모니터링함으로써 사전에 비정상을 탐지하고, 정책 통제를 강화하고, 컴플라이언스 보고서를 생성할 수 있습니다.

엔터프라이즈급 AI 보호

Akamai의 글로벌 위협 인텔리전스를 기반으로 하는 방화벽은 새롭게 등장하는 AI 보안 위협에 지속적으로 적응합니다. 기업은 AI 보안 리서치와 위협 모델링을 통해 얻은 실시간 데이터 인사이트를 활용함으로써 탄력적인 보안 체계를 유지하면서 AI 애플리케이션이 안전하고 책임감 있게 운영되도록 할 수 있습니다.



전문가에게 문의하고 자세히 알아보세요.