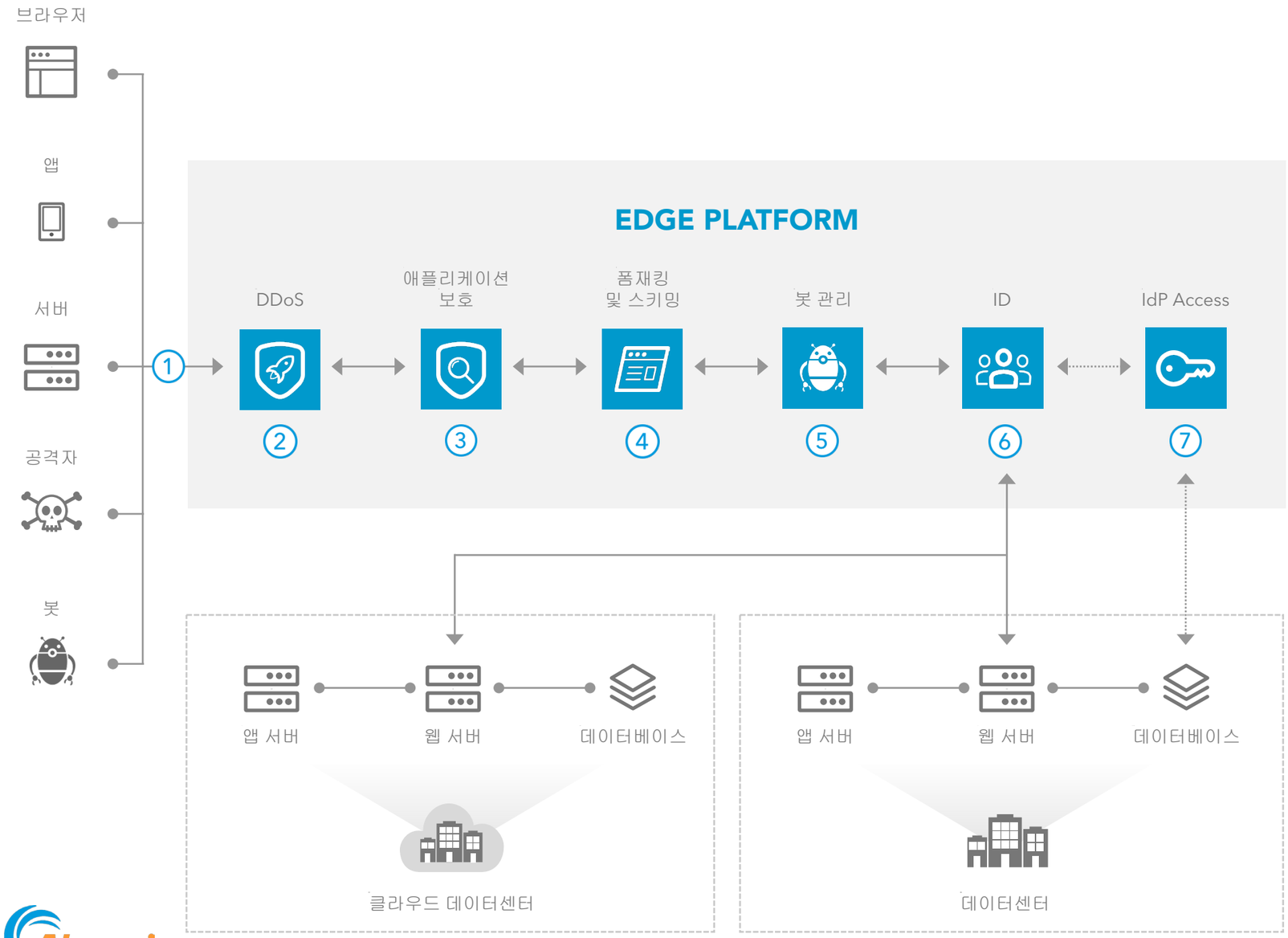
온라인 사기와 사이버 범죄 예방

레퍼런스 아키텍처



OVERVIEW

금융기관들은 매력적인 표적입니다. 탐지를 피해 공격 기법을 끊임없이 변경하는 정교한 범죄자들의 공격 대상이 되기 쉽습니다. 공격이 성공할 경우 규제 부담이 가중되며 더 중요한 문제점은 소비자의 신뢰가 무너진다는 것입니다.

Akamai 솔루션이 끊임없이 변화하는 위협을 선제적으로 방어하고 소비자의 개인 자산을 보호하는 동시에 새로운 등록 프로세스를 더욱 쉽게 만드는 보안 체계를 구축하는 방법은 다음과 같습니다.

1. Akamai Intelligent Edge Platform은 상호 TLS 및 기타 네트워크 제어를 통한 애플리케이션 접속은 물론 대표적인 API 인증과 권한 확인 방식을 지원합니다.
2. DDoS는 상당한 위협이 될 뿐만 아니라 공격자의 실제 목표물로부터 타겟의 주의를 돌릴 수도 있습니다. 엣지 서버가 자동으로 네트워크 레이어 DDoS Flood 공격을 방어하고 애플리케이션 레이어 공격으로부터 보호합니다.
3. API 설정 파일에 정의된 특정 파라미터를 사용하는 웹 요청 검사 및 포지티브 보안 모델을 통해 애플리케이션 데이터를 보호합니다.
4. 손상된 스크립트를 발견하고 데이터를 보호하기 위해 페이지를 심층 검사 및 분석합니다.
5. 최신 봇과 가장 정교한 봇을 식별하는 기능을 사용하여 인증정보 도용 시도와 ATO(계정 탈취)를 방지합니다.
6. 엣지의 고객 ID 및 접속 관리(CIAM)은 중요한 정보를 안전하게 보호하여 복잡한 규제 환경에 대한 성능, 개인 설정, 데이터 보호와 지원을 보장합니다.
7. 인증정보를 온프레미스 디렉토리 또는 퍼스트파티 애플리케이션에 저장하는 옵션입니다.

주요 제품

DDoS, 애플리케이션, 폼재킹 보호 ▶ Kona Site Defender

봇 관리 ▶ Bot Manager

ID 및 애플리케이션 접속 ▶ Identity Cloud, Enterprise Application Access

2020년 05월 발행