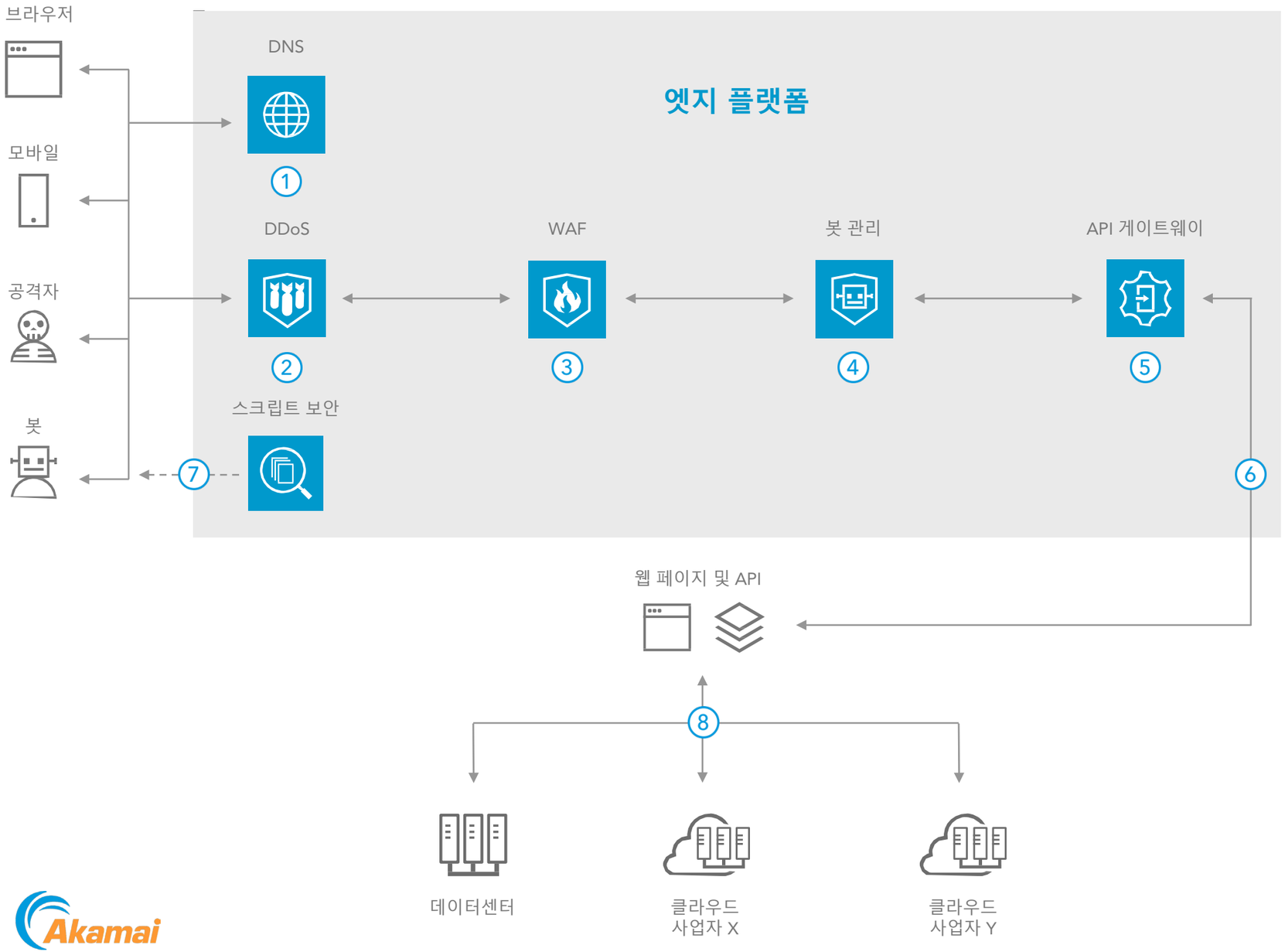
멀티 클라우드 보안

레퍼런스 아키텍처



OVERVIEW

클라우드로의 마이그레이션은 클라우드 여정의 첫 번째 단계입니다. 그 다음 단계는 여러 클라우드 사업자의 기능을 비즈니스, 애플리케이션, 개발자팀에 맞게 탄력적으로 활용하는 것입니다.

멀티 클라우드 환경에 배포된 애플리케이션의 보안을 담당하는 보안팀은 보안 체계의 일관성을 유지하기 위해 한 곳에서 보안을 관리할 수 있어야 하고 비즈니스 요구사항에 맞춰 직원과 리소스를 확장해야 합니다.

1. 권한 DNS는 클라이언트의 룩업 요청을 리졸브하고 대규모 DDoS 공격을 방어합니다.
2. 엣지 서버가 자동으로 네트워크 레이어 DDoS 공격을 방어하고 수 초 안에 애플리케이션 레이어 DDoS 공격에 대응합니다.
3. 웹 애플리케이션 방화벽(WAF)이 웹 요청을 검사하고 SQL 인젝션, XSS, RFI 등 악성 위협을 차단합니다.
4. 봇 관리 기능이 여러 교묘한 봇 트래픽을 탐지하고 관리합니다.
5. API Gateway가 모바일 앱 같은 API 사용자의 요청에 대한 인증, 권한 부여, 제어를 통해 API 트래픽을 관리합니다.
6. Akamai Intelligent Edge Platform이 정상적인 브라우저 및 모바일(특정 봇) 트래픽을 웹 애플리케이션으로 라우팅합니다.
7. 스크립트 보안 기능이 써드파티 스크립트의 행동을 모니터링하고 웹 스키밍과 Magecart 공격을 식별 및 완화합니다.
8. 웹 애플리케이션은 온프레미스 또는 클라우드 데이터 센터를 조합해 구축할 수 있고 단일 또는 다수의 제공업체를 사용할 수 있습니다.

주요 제품

DNS ▶ Edge DNS
DDoS ▶ Kona Site Defender 또는 Web Application Protector
WAF ▶ Kona Site Defender 또는 Web Application Protector
API 보안 ▶ Kona Site Defender 또는 Web Application Protector
봇 관리 ▶ Bot Manager
API 게이트웨이 ▶ API Gateway
스크립트 보안 ▶ Page Integrity Manager

2020년 8월 발행