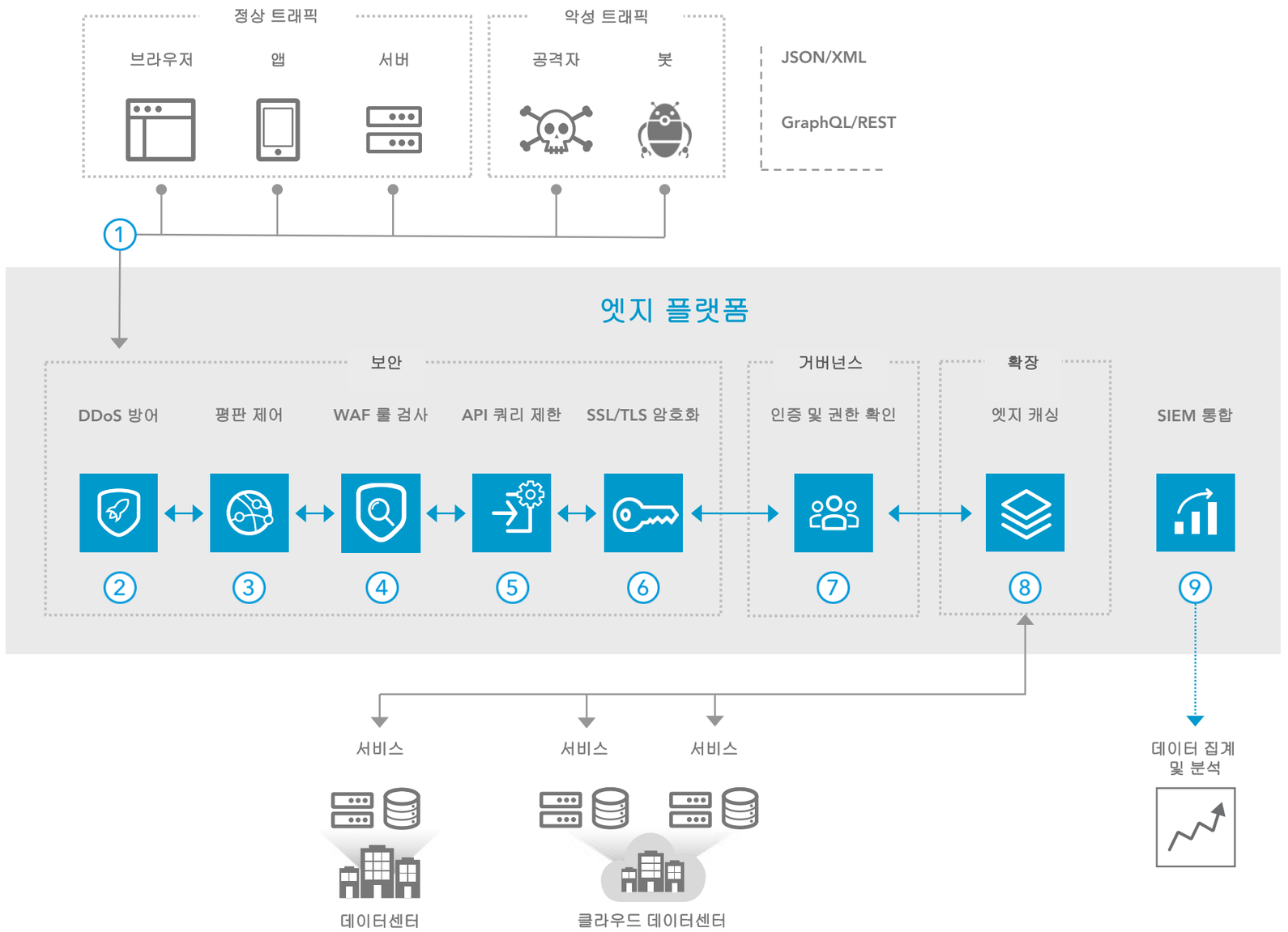
API 보안 개선

레퍼런스 아키텍처



OVERVIEW

API 보안은 관리가 소홀하거나 일관성 없이 적용되는 경우가 있기 때문에 이로 인해 기업이 악성 공격에 취약해지고 데이터 유출, 매출 손실, 브랜드 가치 하락 등이 발생합니다. Akamai 솔루션은 DDoS, 애플리케이션, 크리덴셜 스터핑 공격으로부터 API를 보호합니다. 인프라에서 멀리 떨어진 엣지에서 API 보안 기능이 적용되기 때문에 광범위하고 세분화된 공격면에 걸쳐 보안 체계를 강화할 수 있습니다.

1. 정상 사용자와 악성 공격자는 Akamai Intelligent Edge Platform을 통해 API에 접속합니다.
2. 엣지 서버가 자동으로 네트워크 레이어 DDoS 공격을 방어하고 애플리케이션을 DDoS 및 애플리케이션 공격으로부터 보호합니다.
3. Akamai가 IP 주소의 이전 행동에 대한 가시성을 통해 얻은 평판 점수를 기준으로 악성 공격자의 트래픽을 차단합니다.
4. 악성 콘텐츠에 대한 API 요청을 자동으로 검사하고 디바이스 핑거프린팅을 기반으로 공격 툴을 차단합니다.
5. 데이터 유출 및 삽입을 방지하기 위해 개별 API 사양을 기반으로 한 포지티브 보안 모델입니다. DoS 공격으로부터 백엔드 마이크로서비스와 애플리케이션을 보호합니다.
6. 전송 중 민감한 데이터 노출을 방지하기 위해 SSL/TLS 암호화를 제공합니다.
7. API Gateway는 API 요청을 검증하여 정상 사용자가 API에 접속할 수 있도록 합니다.
8. 캐시에서 API 응답을 제공하여 성능을 개선하고 인프라·대역폭 비용을 절감할 수 있습니다.
9. 보안 정보와 이벤트를 캡처하고 저장하며 SIEM 애플리케이션에 실시간으로 전송합니다.

주요 제품

보안 ▶ Kona Site Defender, Web Application Protector, Bot Manager
거버넌스 ▶ API Gateway
확장 ▶ Ion 또는 Dynamic Site Accelerator
SIEM 통합 ▶ SIEM Connector

2019년 8월 발행