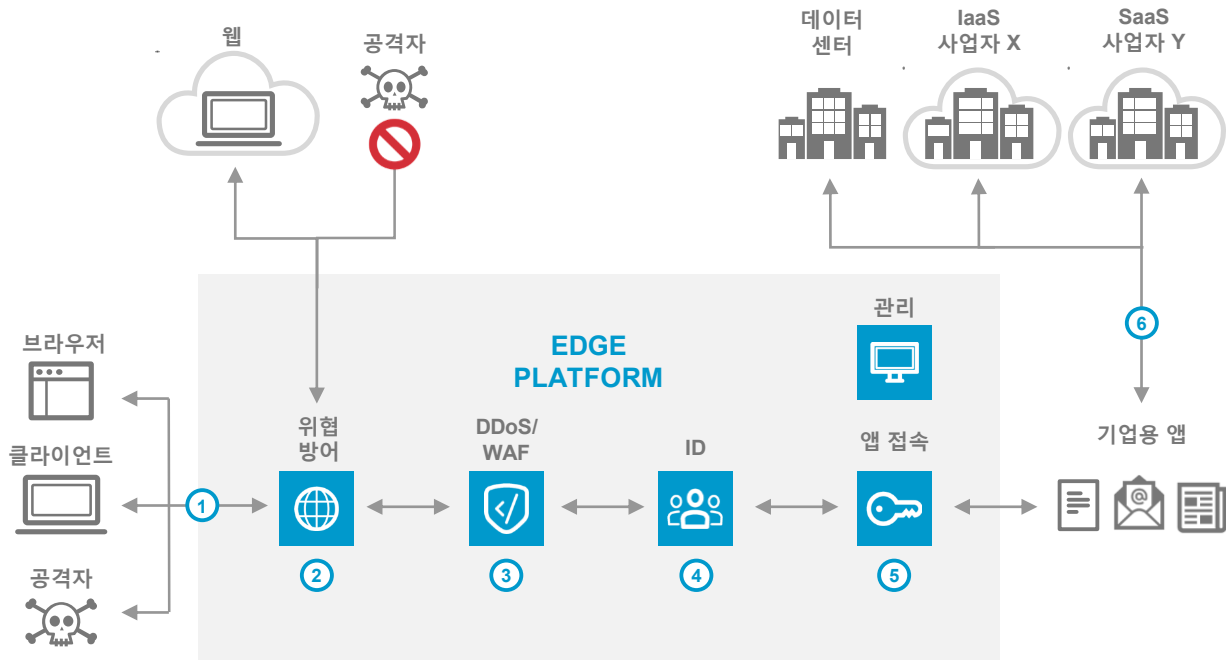


제로 트러스트 보안

레퍼런스 아키텍처



개요

제로 트러스트 보안 아키텍처는 경계를 뚫고 측면 이동하여 데이터를 탈취하는 악의적 공격자로 인해 발생할 수 있는 리스크를 최소화합니다. 최소 권한과 기본 거부를 기반으로 하는 제로 트러스트는 비즈니스 요구사항에 따라 유한한 리스크를 확장하는 경우에도 단일 보안 및 접속 제어를 통해 사용자를 보호하고 안전한 접속을 제공합니다.

- 1 사용자가 Akamai Intelligent Edge Platform을 통해 기업용 애플리케이션과 웹에 접속합니다.
- 2 위협 방어를 통해 멀웨어, 피싱, 악성 웹 콘텐츠로부터 사용자를 보호하는 동시에 기업 전반의 위험 요소에 대한 가시성을 제공합니다.
- 3 기업용 애플리케이션의 경우 엣지 서버가 자동으로 네트워크 레이어 DDoS 공격을 방어하고 SQL 인젝션, XSS, RFI 등 악성 위협을 차단하기 위해 웹 요청을 검사합니다.
- 4 사용자 ID가 온프레미스, 클라우드 기반 또는 Akamai ID 스토어를 기반으로 확인됩니다.
- 5 사용자 ID 및 기타 보안 신호를 기반으로 기업의 전체 네트워크가 아닌 필요한 애플리케이션에 대한 접속만 제공됩니다.
- 6 Akamai Intelligent Edge Platform이 인증과 권한이 확인된 사용자만 기업용 애플리케이션으로 라우팅합니다.

주요 제품

- 위협 방어 ▶ Enterprise Threat Protector
- DDoS/WAF ▶ Kona Site Defender 또는 Web Application Protector
- ID 및 애플리케이션 접속 ▶ Enterprise Application Access