

## 웹 애플리케이션 및 API 보안 기능 체크리스트

정보 보안 전략을 계획, 실행, 최적화하면서 웹 애플리케이션 및 API 보안 솔루션을 배포하면 기업의 리스크를 파악하고, 보안 취약점을 확인하며, 위협을 탐지할 수 있습니다. 포괄적인 인사이트를 통해 지속적인 가시성을 제공하는 웹 애플리케이션 및 API 보안(WAAP) 솔루션과 가장 정교한 공격을 식별하고 차단하는 기능이 필요합니다.

이 체크리스트는 벤더의 역량을 평가하는 데 사용하거나 효과적인 WAAP 솔루션을 구축하는 데 필요한 요구사항 목록으로서 활용할 수 있습니다.

### 카테고리 1: 플랫폼 요구사항

기업의 형태와 규모는 다양하고 요구사항도 상이합니다. 웹 애플리케이션 보안 솔루션은 유연하고 확장 가능하며 관리하기 쉬워야 합니다.

- 트래픽 수요를 충족시키고 성능 저하 없이 지속적인 보안을 제공하는 확장성
- 지리적으로 분산된 애플리케이션의 문제를 해결할 수 있는 아키텍처
- 적절한 사용을 보장하는 감사 로그 기능
- 온프레미스, 프라이빗, 퍼블릭 클라우드(멀티클라우드 또는 하이브리드 클라우드 포함) 사이트 오리진 보호
- 0초 서비스 수준 협약(SLA)을 통한 네트워크 레이어 L3/4 DDoS(Distributed Denial-of-Service) 방어
- 플랫폼 전반에 걸쳐 클라우드 소싱된 공격 인텔리전스를 기반으로 공격의 주체, 빈도, 심각도에 대한 가시성 제공
- 포트 80 및 443을 사용하는 웹 트래픽에 대한 리버스 프록시
- SSL/TLS 암호화를 통한 네트워크 개인정보 보호

## 카테고리 2: 적응형 웹 애플리케이션 및 DDoS 방어

웹 애플리케이션 보안은 기존의 시그니처 기반 탐지보다 더 발전된 형태의 적응형 웹 애플리케이션 및 DDoS 보안으로 정확도와 안정성이 가장 높은 보안을 제공해야 합니다.

- 비정상 및 리스크 기반 점수 책정으로 시그니처 기반 공격 이외의 다양한 공격 탐지
- 머신 러닝과 데이터 마이닝, 휴리스틱 기반 탐지 기능으로 빠르게 변화하는 위협 식별
- 보안 연구원이 지속적으로 제공하는 실시간 위협 인텔리전스를 기반으로 자동 웹 애플리케이션 방화벽 (WAF) 룰 업데이트
- 프로덕션으로 배포하기 전에 라이브 트래픽에 신규 또는 업데이트된 WAF 룰을 테스트하는 기능
- SQL 인젝션, XSS, 파일 인클루전, 명령어 인젝션, SSRF, SSI, XXE를 포함한 다양한 공격 방어
- 고객의 특정 요구사항에 맞춰 사전 정의된 맞춤형 룰
- 반복적인 애플리케이션 활동으로 웹 서버 처리 용량을 초과하도록 설계된 애플리케이션 레이어 L7 증폭 DoS(Denial-of-Service) 공격 차단
- 지속적인 설정과 업데이트가 필요 없는 완전한 매니지드 WAF 룰
- 개별 IP 주소와 공유 IP 주소 모두에 대한 Client Reputation 점수 책정 및 인텔리전스 제공
- 특정 트래픽 패턴을 신속하게 방어하는 맞춤형 룰(가상 패치)
- 자동화된 봇 트래픽 또는 과도한 봇 트래픽을 막기 위한 요청 전송률 제한
- 오리진을 직접 겨냥하는 표적 공격 방어
- 다중 네트워크 목록을 통해 특정 IP, 서브넷, 지역의 트래픽을 차단 또는 허용하는 IP 및 지리적 위치 기반 제어
- 취약점 스캐닝, 웹 공격 툴 등 자동화된 클라이언트 차단

### 카테고리 3: API 가시성, 보안, 제어

API 보안은 웹 애플리케이션 보안의 중요한 부분으로 자리잡았습니다. API 취약점을 방어하고 리스크가 높은 공격면을 줄이기 위해 강력한 API 검색, 보안, 제어 기능을 갖춘 WAAP 솔루션이 필요합니다.

- 알려지지 않거나 또는 변화하는 API를 자동 검색 및 프로파일링(API 엔드포인트, 특징, 정의 포함)
- API 기반 공격을 탐지하기 위해 XML 및 JSON 요청을 자동으로 검사
- 사용자의 특정 요구사항을 충족하는 맞춤형 API 검사 룰
- 허용 가능한 XML 및 JSON 형식을 사전 정의해 API 요청의 크기와 종류, 깊이를 제한하는 기능
- 리소스를 소진하도록 설계된 '로우 앤 슬로우(Low and Slow)' 공격(예: Slow POST, Slow GET)으로부터 API 백엔드 인프라 보호
- API 수준의 실시간 알림, 리포팅, 대시보드
- API 키를 기반으로 하는 API 엔드포인트의 전송률 제어(스로틀링)
- IP 및 지리적 위치를 기반으로 한 API 네트워크 목록 (허용 목록/차단 목록)
- 버전 관리를 통한 API 라이프사이클 관리
- JWT(JSON Web Token) 검증을 통한 보안 인증 및 권한 확인
- 키(key)에 따라 허용된 API 요청 정의(개별적으로 정의된 각 키에 대한 할당량)로 소비량 완전 제어
- 표준 API 정의(Swagger/OAS 및 RAML)를 사용한 API 온보딩

## 카테고리 4: 유연한 관리

투자 효과를 극대화하고 운영 효율성을 개선하려면 간편하고 자동화된 워크플로우가 필요합니다. 신규 애플리케이션 또는 변화하는 애플리케이션을 보호하고, 새로운 WAF 룰을 채택하고, API로 보안 기능을 확장하려는 원활하고 직관적인 프로세스가 필요합니다.

- 보안 설정 작업을 CI/CD 프로세스로 통합하기 위한 Open API 및 CLI(명령줄 인터페이스)
- 온프레미스 및 클라우드 기반의 SIEM(보안 정보 및 이벤트 관리) 애플리케이션과의 통합
- 완전한 테스트 환경 및 변경 제어 실행 능력
- 트래픽에 자동으로 적응하는 셀프 튜닝 보안 기능
- 실시간 대시보드, 보고, 휴리스틱 기반 알림 기능
- 세부 공격 텔레메트리에 접속하고 보안 이벤트를 분석할 수 있는 중앙 집중식 UI(사용자 인터페이스)
- 탁월한 제어 또는 완전 자동화된 보안을 통해 WAAP를 관리하는 유연성
- 보안 관리, 모니터링, 위협 차단 업무의 부하를 분산하거나 해당 역량을 강화하는 완전한 관리형 보안 서비스

Akamai Connected Cloud를 통해 매일 수백만 건의 웹 애플리케이션 공격, 수십억 건의 봇 요청, 수조 건의 API 요청으로부터 인사이트를 확보합니다. Akamai는 높은 수준의 인사이트를 고급 머신 러닝 및 위협 리서치와 결합함으로써 새로운 위협을 포착하고 지속적으로 발전하며 혁신적인 기능을 개발하고 있습니다.

자세한 내용은 [akamai.com](https://akamai.com)를 방문하거나 Akamai 영업 담당자에게 문의하시기 바랍니다.