# 하나로 끝내는 WAF 평가 체크리스트

## 애플리케이션과 API 보안 요구사항에 적합한 솔루션을 찾는 툴

적합한 WAF(Web Application Firewall) 또는 WAAP(Web Application and API Protection) 벤더사를 찾는 과정을 간소화하세요. 이 포괄적인 체크리스트를 사용해 WAF 및 WAAP 공급업체를 평가하고, 솔루션이 보안, 성능, 재정, 운영 요구사항을 충족하는지 확인하세요.

## 보안 기능

### 애플리케이션 보안

- SQL 인젝션, XSS, LFI, SSRF 등 **OWASP 상위 10대 취약점에 대한 적용 범위**를 확인하세요. 보호 기능을 사용자 정의하고 자동으로 배포할 수 있는지 확인하세요.
- 솔루션이 **평판이 좋지 않은 IP**의 트래픽을 사전에 제어하고, 이전의 **예외가 남용된 경우** 경고하는지 평가하세요.
- **허용 목록과 차단 목록의 유연성**을 평가하세요. IP, 지리적 위치, ASN, TLS 지문과 같은 속성을 상호 연관시켜 효과적인 정책을 만들 수 있습니까?

### DDoS 방어

- 벤더사가 DNS, 레이어 3/4, 레이어 7을 포함한 애플리케이션과 API에 대한 **멀티레이어 DDoS 방어**를 제공하는지 확인하세요.
- 솔루션이 애플리케이션 보안을 위한 **행동 기반 DDoS 탐지**를 제공하는지 확인하세요.
- **요청 한도** 관리가 얼마나 정밀해야 할지 결정하세요. 자동적으로 설정합니까, 아니면 수동으로 설정합니까? 이러한 수단으로 증폭 공격과 Slow POST 공격으로부터 보호할 수 있습니까?
- DDoS 공격을 받는 도중 **부하를 줄이고** 성능을 향상시키는 기능을 검토하세요.
- DDoS 공격을 받는 도중 트래픽 증가로 인해 발생할 수 있는 **추가 비용**을 파악하세요.
- **L7 DDoS 방어가 자동화되어** 팀의 시간과 전문성을 낭비하지 않아도 되는지 확인하세요. 특정 트래픽 프로필 또는 리스크 허용 범위에 맞춰 **보호를 조정**할 수 있습니까?

### 제로데이 악용 보호

- WAF가 **알려진 CVE에 대한 기존 보호 기능**을 갖추고 있으며, 신속한 적응을 통해 새로운 제로데이 악용을 방어할 수 있는지 확인하세요. 솔루션의 **제로데이 방어 이력**과 응답 시간을 조사하세요.
- 고객으로서 **특정 CVE에 대한 보호**를 제공받는지 확인하세요.

### API 보안

- 솔루션이 인젝션 공격, DoS, 사양 위반으로부터 **API 엔드포인트를 보호**하는지 확인하세요.
- **API 검색** 여부를 확인하세요. 새로운 API와 수정된 API를 자동으로 탐지할 수 있습니까? API에 대한 보호를 얼마나 쉽게 적용할 수 있습니까?
- 민감한 데이터를 보호하고 데이터 유출을 방지하기 위해 **PII 탐지 및 알림**을 확인하세요.

### 봇 보안

- WAF가 봇 디렉토리와 정의를 사용해 **자동화된 위협을 탐지하고 방어**하는지 확인하세요. 봇 디렉토리의 규모는 어느 정도입니까? 새로운 봇과 수정된 봇이 얼마나 자주 업데이트됩니까?
- 툴에 어떤 **봇 정의**가 있는지 확인하세요. 봇 정의를 **직접 만들 수** 있습니까?
- 솔루션에 사용자 경험을 방해하지 않는 **CAPTCHA 또는 인간 검증 메커니즘**이 포함되어 있는지 확인하세요. 최종 사용자가 계속 진행하려면 CAPTCHA/검증과 상호 작용해야 합니까?

## 위협 인텔리전스와 자동화

### 위협 인텔리전스

- 공급업체가 위협 인텔리전스에 **퍼스트파티 데이터**를 사용해 써드파티 지연과 잠재적인 데이터 변조를 방지하는지 확인하세요.
- 공급업체 **위협 탐색팀**의 규모와 새로 등장하는 리스크를 모니터링하는 보안 전문가들의 글로벌 네트워크를 확인하세요.
- 인텔리전스 데이터베이스에서 처리하는 **데이터의 양과 관련성**을 평가하세요. 귀사와 유사한 업계의 데이터나 자주 사이버 공격의 표적이 되는 기업의 데이터가 포함되어 있습니까?

### 자동화

- WAF가 **구식 룰세트 기술**을 사용하는지 확인하세요. 고급 휴리스틱과 머신 러닝을 통한 자동 업데이트와 같은 최신 기술을 사용합니까?
- 룰세트가 자동으로 업데이트되어 **수동 개입이 필요하지 않은지** 확인하세요. 자동 업데이트가 전 세계적으로 적용됩니까? 이전에 적용된 업데이트를 제거하거나 **라이브 트래픽에서 테스트**하는 데 어떤 옵션이 있습니까?
- 개입하지 않아도 솔루션이 사용자의 환경에 맞춰 보호 기능을 맞춤화하는지 확인하세요. 솔루션이 기업의 라이브 트래픽 프로필을 기반으로 보안 정책을 지속적으로 **셀프 튜닝**합니까?
- 솔루션이 **오탐**을 어떻게 제어하는지 평가하세요. 오탐을 줄이는 것과 **정상 트래픽 방해**를 최소화하는 것 사이에서 균형을 어떻게 유지합니까?

## 가시성 및 보고

### 정밀한 가시성

- WAF가 다중 솔루션 환경을 포괄하는 맞춤형 대시보드와 보고 기능을 통해 성능과 **위협에 대한 자세한 가시성**을 제공하는지 확인하세요.
- WAF를 운영할 때, 보안팀은 대부분의 시간을 데이터 콘솔에서 보냅니다. 이용할 수 있는 **사용자 지정 기능**, 사전 예방적 분석 기능, **보고의 정밀성**을 살펴보세요.
- 솔루션이 효과적으로 애플리케이션 트래픽과 **API 트래픽을 모니터링**하고, 남용을 탐지하고, API 스프롤에 대한 자세한 인사이트를 제공할 수 있는지 평가하세요.

### 실시간 알림 및 사전 예방적 분석

- 중요한 위협을 거의 실시간으로 팀에 알리는 **실시간 알림** 기능이 있는지 확인하세요. 알림은 이해하기 쉽고 신속한 대응을 위해 심각도, 출처, 공격 종류와 같은 특정 기준에 따라 사용자 정의할 수 있어야 합니다.
- 공격이 발생하는 위치, 시기, 방법에 대한 **사전 분석된 인사이트**를 제공해 보안팀의 부담을 줄이는 솔루션을 찾으세요. 또한 솔루션은 보안 태세를 개선하기 위한 **다음 단계를 추천**해야 합니다.

## 플랫폼 및 아키텍처

### 글로벌 도달 범위

- WAF가 향상된 성능과 보안을 위해 글로벌 네트워크 엣지 또는 CDN 서비스에 대한 접속을 제공하는지 확인하세요. 주요 위치와 고객의 위치를 포함할 수 있도록 솔루션의 **글로벌 가용성**을 리서치하세요.

### 클라우드 및 하이브리드 지원

- 솔루션이 **클라우드 애그노스틱**인지, 멀티 클라우드, 하이브리드, 온프레미스 환경을 지원할 수 있는지 확인하세요. CDN 기반이라면 솔루션이 CDN을 넘어 오프-엣지 보안을 지원할 수 있는지 확인하세요.

### 안정성 및 장애 복구

- **솔루션의 안정성**을 평가하세요. 중단이나 장애가 발생하는 동안 자동으로 장애를 복구해 보호를 유지할 수 있습니까?
- 공급업체의 **최근 서비스 중단 및 대응**을 검토하세요.
- **SLA(Service-Level Agreement)**가 비즈니스 요구사항을 충족하는지 확인하세요.

## 지원 및 매니지드 서비스

### 포함된 지원 및 서비스 접속

- WAF 솔루션에 **포함된 지원 수준**과 유료로 이용 가능한 지원 수준을 확인하세요.
- **연중무휴 24시간 인시던트 대응**이 가능한지, 공격이 발생하는 동안 SOC(Security Operations Center)에 직접 접속할 수 있는지 확인하세요.
- 벤더사가 공격 대응, 설정, 직원 교체에 대한 전문 지식을 포함한 **완전 매니지드 보안 서비스**를 제공하여 내부 리소스의 잠재적 격차를 메울 수 있는지 확인하세요.

## 통합 및 DevSecOps 호환성

### API, CLI, 인프라 자동화

- **API, CLI, Terraform** 통합을 확인하여 보안 기능을 자동화하고 개발 워크플로우에 내장시킬 수 있는지 점검하세요. GitOps 및 기타 '코드로서의 인프라' 프레임워크에 대한 지원은 환경 전반에 걸쳐 일관된 보안 적용을 위해 매우 중요합니다.

### SIEM 통합

- WAF가 향상된 모니터링, 보고, 인시던트 대응을 위해 Splunk 또는 QRadar와 같은 **SIEM 툴과 원활하게 통합되는지** 확인하세요.

## 비즈니스 성과 및 효율성

### 확장성 및 성능

- 성능 저하 없이 대량의 트래픽을 처리할 수 있도록 솔루션이 **자동으로 확장되는지** 확인하세요. 과부하가 걸렸을 때 솔루션이 지연 시간을 일으키거나 취약해지는 시점은 언제입니까?
- **100% 가용성** SLA를 확인하고, 솔루션이 캐싱 및 트래픽 가속과 같은 성능 향상 기능을 제공해 애플리케이션을 개선할 수 있는지 평가하세요.

### 통합 관리

- 공급업체가 클라우드, 온프레미스, 하이브리드 등 **모든 환경에서 보안 정책을 관리할 수 있는** 단일 창 인터페이스를 제공하는지 평가하세요. 솔루션이 현재 스택과 통합될 수 있는지, 보안팀과 개발팀 모두에게 원활한 경험을 제공할 수 있는지 확인하세요.

### 비용 효과

- 솔루션이 **WAF, DDoS, 봇 관리, API 보안을 단일 벤더사로 통합**하여 복잡성을 줄이고 관리 비용을 절감할 수 있는지 확인하세요. 보안 효과와 운영 비용 간의 균형을 평가해 전반적인 가치를 결정하세요.

## 벤더사의 신뢰성

### 서비스 및 안정성 이력

- 지난 5년 동안 공급업체의 **중단 및 서비스 지장 이력**을 검토하세요.
- 회사가 **재정적으로 안정적인지** 확인하세요. 이윤을 내고 있습니까? 사업 기간은 얼마나 됩니까? 어떤 규모와 종류의 고객을 대상으로 서비스를 제공합니까?

### 평판 및 리뷰

- 검증된 리뷰와 고객 후기를 리서치해 업계의 유사한 기업이 **해당 벤더사를 신뢰**하는지 확인하세요. 현재 고객의 사용 사례가 귀하의 요구사항과 일치합니까?
- 애플리케이션 및 API 보안 솔루션에 대해 Gartner, Forrester와 같은 **업계 분석가들이 인정**하는지 확인하세요.
- 벤더사와 논의한 후, 고객사가 된 경우 문제가 발생했을 때 벤더사의 대응 속도와 지원에 대한 **확신이 있는지** 확인하세요. 초기 온보딩 후 누가 계정을 지원할 것인지 문의하세요.

**Akamai의 WAAP 솔루션에 대해 더 자세히 알고 싶으십니까?**
**App & API Protector의 무료 체험을 시작하세요.**