AKAMAI 제품 설명서

App & API Protector

오늘날의 연결된 세상에서 비즈니스를 성공적으로 이끌어 나가려면 다양한 신종 위협과 진화하는 위협으로부터 웹 애플리케이션과 API를 보호해야 합니다. 하지만 클라우드 전환 여정, 최신 DevOps 사례, 끊임없이 변화하는 애플리케이션 등의 상황 속에서 디지털 상호작용을 안전하게 보호하려는 과정에서 새로운 복잡성과 도전과제가 발생합니다.

포괄적인 웹 애플리케이션 및 API 보안(WAAP) 솔루션을 배포하면 보안 기능을 적응형으로 업데이트하고 공격받는 취약점에 대한 인사이트를 선제적으로 제공함으로써 보안 체계를 강화할 수 있습니다.

Akamai App & API Protector는 웹 애플리케이션 방화벽(WAF), 봇 방어, API 보안, 분산 서비스 거부(DDoS) 방어 등 다양한 보안 기술을 하나로 통합한 단일 솔루션입니다. App & API Protector는 선도적인 WAAP 솔루션으로서 기존의 WAF를 넘어오는 위협을 신속하게 식별하고 방어해 다차원 공격으로부터 전체 디지털 자산을 보호합니다. 이 플랫폼은 구축과 사용이 용이하고, 종합적인 가시성을 제공하며, Akamai 적응형 보안 엔진을 통해 최신 맞춤형 보호 기능을 자동으로 구현합니다.

Akamai App & API Protector Hybrid를 통해 WAF 보안을 확장하세요

분산된 애플리케이션 보안을 위해 설계된 App & API Protector Hybrid는 Akamai의 검증된 핵심 WAF 기능을 온프레미스, 멀티클라우드, 오프-CDN 인프라 등 다양한 환경에 배포된 애플리케이션과 API 전반으로 확장해 일관된 보안을 제공합니다.

적응형 보안의 장점

App & API Protector는 룰세트 외에도 적응형 보안 엔진을 활용합니다. 이 혁신적인 기술을 바탕으로 보안 기능이 지속적으로 자동 업데이트되며, 클릭 한 번으로 맞춤형 정책 권장사항을 구축할 수 있습니다. 적응형 보안 엔진을 사용하면 머신 러닝, 실시간 보안 인텔리전스, 고도의 자동화, 400명이 넘는 보안 전문가와 위협 연구원이 제공하는 인사이트를 조합해 최신 방어 기능을 사용할 수 있습니다. 적응형 보안 엔진의 장점은 다음과 같습니다.

- 각 요청의 특성을 엣지에서 실시간으로 분석해 더 빠르게 위협을 탐지
- 로컬 및 글로벌 데이터를 모두 활용해 공격 패턴을 학습하고 고객별로 보안 기능 조정
- 진화하는 공격에 대응해 보안 기능을 지속적으로 업데이트하기 때문에, 미래의 위협에도 유연하게 대응

기업이 누릴 수 있는 이점

신뢰할 수 있는 공격 탐지
위협 환경에 맞춰 진화하며 DDoS, 봇넷, 인젝션, API 공격 등 기존의 위협 및 새롭게 등장하는 위협 방어

하나의 제품으로 보안 범위 확대
WAAP, 봇 가시성 및 방어, DDoS 방어, 보안 정보 및 이벤트 관리(SIEM) 커넥터, 웹 최적화, 클라우드 컴퓨팅, API 가속 등이 포함된 솔루션으로 보안 투자 효과 극대화

자동 보안
Akamai 적응형 보안 엔진이 제공하는 셀프 튜닝 권장사항과 자동 업데이트를 통해 시간 소모적인 수동 유지 관리의 부담 감소

사용 편의성
UI 디자인을 개선해 온보딩 및 전반적인 보안 운영을 간소화하고 설정 및 문제 해결 가이드 활용

가시성 통합
Akamai 보안 솔루션의 원격 공유 텔레메트리를 통해 단일 대시보드 또는 선제적 검색 보고서로 전체 범위의 보안 지표 분석

적응형 보안 엔진은 제로터치 업데이트를 통해 많은 시간이 소요되는 수동 조정의 부담을 경감해 완벽에 가까운 자동 경험을 제공합니다. 출시 시점을 기준으로 이 기술을 통해 탐지 성능을 2배 강화하고, 오탐률을 5배 줄였습니다. 또한 머신 러닝 기반의 알고리즘을 최신으로 업데이트해 오탐률을 추가적으로 4배 줄였습니다. 보안 전문가는 안전하고 고객 친화적인 디지털 비즈니스 운영에 더 많은 시간을 할애할 수 있습니다.

신규: 행동 기반 DDoS 엔진

새로운 행동 기반 DDoS 엔진은 머신 러닝으로 구동되어 애플리케이션 레이어 DDoS 방어를 강화하고 간소화합니다. 행동 기반 DDoS 엔진의 행동 및 비정상 탐지 알고리즘은 발생 국가, 네트워크 지문 및 기타 HTTPS 요청 특성과 같은 다양한 트래픽 차원을 살펴보면서 맞춤형 보안 기능을 제공하고 애플리케이션 레이어 DDoS 공격에 대한 자동 접근 방식을 지원합니다.

행동 기반 DDoS 엔진은 트래픽 프로필 또는 기준선 생성을 위해 머신 러닝을 활용함으로써 트래픽 차원에서 효율성 및 의사 결정을 개선합니다. 다양한 민감성 수준의 점수 매커니즘을 통해 기업의 리스크 성향을 고려해 공격을 탐지하고 오탐률을 최소화할 수 있습니다.

업계 최고의 공격 탐지 기술 - 디지털 환경이 확장되면 Akamai 고객에게 제공되는 보안 기능의 깊이와 폭도 확장됩니다. App & API Protector는 적응형 보안 엔진이 제공하는 자동 업데이트 및 적응형 셀프 튜닝 외에도 DDoS, 봇, 멀웨어, 기타 공격 기법에 대해 애널리스트가 인정하는 주요 탐지 기능을 제공합니다. Akamai 위협 리서치 툴을 통해 새롭게 등장한 CVE와 진화하는 CVE에 대한 Akamai 보호 조치를 확인할 수 있습니다.

애플리케이션 보안 - App & API Protector는 기업의 요구사항에 맞게 보안을 조정할 수 있는 완벽한 방어 및 사용자 맞춤 기능을 제공합니다. Client Reputation, 클라이언트 목록, 새로운 공격 탐지 등의 효과적인 기능을 통해 공격에 선제적으로 대응하면서 보안 운영을 간소화할 수 있습니다. Akamai WAAP 솔루션의 최신 애플리케이션 레이어 방어 기능을 바탕으로 DDoS, SQL 인젝션, 크로스 사이트 스크립팅, 로컬 파일 인클루전, 서버 측 요청 위조, 기타 공격 기법을 방어할 수 있습니다.

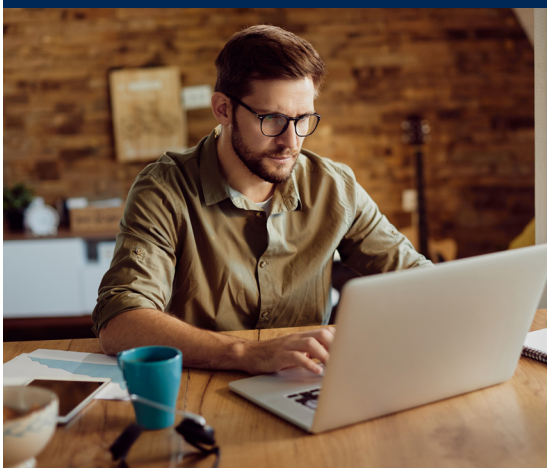
DDoS 방어 및 세분화된 전송률 제어 - 뛰어난 DDoS 솔루션으로 인정을 받은 App & API Protector는 공격을 차단해야 하는 최전선에서 DDoS 방어 기능을 제공합니다. 리스크 방어 및 리소스 절감을 위해 엣지에서 네트워크 레이어 DDoS 공격을 즉시 차단합니다. 그런 다음, 엣지에서 정교한 레이어 7 DDoS 공격을 자동으로 탐지하고 방어해 DDoS 위협의 진화하는 환경에 대비한 실시간 자동 보호 기능을 제공합니다. 세분화된 전송률 제어로 트래픽 및 공격 프로필에 맞게 DDoS 방어 기능을 사용자 맞춤화할 수 있습니다.

봇 가시성 및 방어 - 알려진 봇에 대한 Akamai의 디렉터리에 접속해 봇 트래픽에 대한 실시간 가시성을 제공합니다. 왜곡된 웹 애널리틱스를 조사하고, 오리진의 과부하를 방지하며, 봇 정의를 직접 생성해 방해 없이 써드파티 및 파트너 봇에 접속할 수 있게 됩니다. 브라우저 신분 도용 탐지, 조건부 동작, 암호화 챌린지 등 확장된 봇 제어가 이제 App & API Protector에 포함됩니다.

OWASP 상위 10대 취약점

Akamai는 OWASP 상위 10대 및 OWASP API 보안 상위 10대 리스크를 모두 방어합니다. App & API Protector와 Akamai의 보안 솔루션을 사용해 대규모 일반 위협이나 신종 위협으로부터 고객을 보호하는 방법에 대해 자세히 알아보세요.

OWASP 10대 리스크에 대한 Akamai의 보호 기능에 대해 자세히 알아보려면 백서를 다운로드하세요.



API 보안 - 업계를 선도하는 Akamai의 API 보안 솔루션은 디지털 자산의 트래픽에 대한 가시성을 제공하고, 취약점을 사전에 발견하며, 환경 변화를 식별하고, 숨겨진 공격을 막아냄으로써 보안 수준을 높입니다. App & API Protector의 API 기능을 통해 다음과 같은 장점을 누릴 수 있습니다.

- 엔드포인트, 정의, 트래픽 프로필 등 웹 트래픽 전체에서 알려진, 알려지지 않은, 변화하는 모든 API 자동 검색
- 새로 검색된 API를 클릭 몇 번으로 간편하게 등록
- DDoS, 악성 인젝션, 인증정보 도용 공격, API 사양 위반에 대한 API 보안 보장
- App & API Protector의 PII(개인 식별 정보) 보고 기능을 통해 민감한 데이터 처리를 제어해 규정 준수

가장 큰 규모의 글로벌 네트워크에서 성능 이상의 이점 제공 - Akamai 플랫폼을 활용하는 고객은 Akamai의 광범위한 글로벌 규모를 통해 경쟁 우위를 확보할 수 있으며, 글로벌 인터넷 트래픽의 상당 부분을 실시간으로 파악할 수 있습니다. Akamai는 이러한 방대한 데이터를 바탕으로 실행 가능한 위협 인텔리전스를 제공해 기업이 진화하는 보안 위협에 선제적으로 대비하고 다양한 환경에서 공격을 더욱 빠르게 탐지하고 방어할 수 있도록 지원합니다. 또한 플랫폼은 검증된 성능 강화 및 100% 가용성 서비스 수준 협약(SLA)을 제공합니다.

멀웨어 방지 기능 - 이 추가 모듈은 파일이 업로드되기 전에 엣지에서 파일을 검사해 멀웨어가 악성 파일 업로드로 기업 시스템에 유입되는 것을 탐지하고 차단할 수 있습니다. 추가 앱 또는 API 설정이 필요하지 않기 때문에 각 시스템에서 개별적으로 보안 설정을 하는 데 소요되는 시간을 절감합니다.

최고 수준의 방어력과 간소화된 보안 운영

App & API Protector의 주요 기능은 기업 내 운영 환경을 개선하는 동시에, 외부 고객에게는 더 나은 사용자 경험과 성능을 제공합니다.

간단한 시작 온보딩 - 뛰어난 보안 툴은 사용자가 사용할 때만 작동합니다. Akamai는 생산성과 강력한 보안을 지원하는 사용하기 쉬운 플랫폼을 구축하기 위해 최선을 다하고 있습니다. Simple Start를 활용하면 신속한 온보딩이 가능하며 몇 번의 클릭만으로 새로운 애플리케이션에 보안 기능을 적용할 수 있습니다.

대시보드, 알림, 보고 툴 - Web Security Analytics는 AI 기반 정보를 제공하는 Akamai의 공격 텔레메트리 대시보드입니다. 여기에서 보안 이벤트를 분석하고, 정적 필터와 임계치를 사용해 실시간 이메일 알림을 생성하고, Akamai 플랫폼에서 사용자 맞춤화 가능한 보고 툴을 사용해 보안 효과를 지속적으로 모니터링하고 평가할 수 있습니다.

DevOps 통합 - GitOps를 통해 DevOps 워크플로우에 보안을 원활하게 통합함으로써 보안이 빠른 개발 속도를 따라갈 수 있도록 지원합니다. CLI 또는 Terraform을 통해 제공되는 Akamai의 API를 사용하면 코드를 통해 App & API Protector를 완벽하게 관리할 수 있으며 사용자 인터페이스에서 사용할 수 있는 모든 작업을 지원합니다.

SIEM 통합 - SIEM API도 사용할 수 있으며, Splunk, QRadar, ArcSight 등에 사전 구축된 커넥터가 App & API Protector에 자동으로 포함됩니다.

포함된 솔루션 - 이제 App & API Protector는 가시성과 성능을 높이기 위해 다음과 같이 Akamai 고객에게 가장 사랑받는 제품을 제공합니다.

- **Site Shield**
  공격자가 클라우드 기반 보안 기능을 우회해 오리진 인프라를 표적으로 삼지 못하도록 차단
- **mPulse Lite**
  사용자 행동에 대한 심층적인 가시성을 확보하고, 실시간 성능 문제를 해결하며, 디지털 변화가 매출에 끼치는 영향 평가
- **Akamai EdgeWorkers**
  출시 기간을 단축하고 최종 사용자와 가장 가까운 곳에서 로직을 실행하는 등 서버리스 컴퓨팅의 장점 활용
- **Akamai Image & Video Manager**
  품질, 포맷, 크기의 완벽한 조합으로 이미지와 비디오를 지능적으로 최적화
- **Akamai API Acceleration**
  접속을 쉽게 관리하고 수요 급증 시 확장하며, API 보안을 강화해 API 성능 향상

무료 등급 제품은 사용에 제한이 있을 수 있습니다. 자세한 내용은 Akamai에 문의하세요.

최신 보안 관리

애플리케이션 환경이 복잡하고 보안 요구사항이 높은 고객의 경우, 고급 보안 관리 옵션 모듈로 자동화 및 설정을 유연하게 진행할 수 있습니다. 최신 보안 관리 옵션에는 추가 보안 설정, 전송률 정책, 보안 정책, 애플리케이션 레이어 DDoS 제어, 사용자 지정 WAF 룰, 포지티브 API 보안, IP 평판 위협 인텔리전스(Client Reputation)에 대한 접속이 포함되어 있습니다.

Managed Security Service

모든 Akamai 고객에게 연중무휴 24시간 표준 지원을 제공합니다. Akamai는 컨설팅 또는 단일 프로젝트 작업을 위한 온디맨드 전문 서비스 외에도 완전한 매니지드 WAAP 서비스, 매니지드 공격 지원 그리고 전문 보안관제센터 지원과 같은 매니지드 서비스를 제공합니다.

전문가에게 문의해 자세히 알아보세요.