Kona Site Defender

웹사이트 다운타임과 데이터 유출을 차단하는 보안 솔루션!

인터넷으로 접속하는 웹사이트와 애플리케이션은 중요한 데이터에 상대적으로 쉽게 접속할 수 있는 엔트리 포인트를 제공하는 반면 공격 대상이 되기도 합니다. Kona Site Defender(KSD)는 웹 공격과 DDoS 공격을 방어하고 웹사이트 및 애플리케이션의 다운타임과 데이터 유출을 예방합니다. KSD를 사용하면 공격에 대한 걱정 없이 온라인 비즈니스를 안정적으로 확대해 나갈 수 있습니다.

KSD 개요

KSD는 멀티레이어 툴세트를 사용해 웹사이트와 API를 정교한 공격으로부터 안전하게 보호합니다. DDoS 방어 기능은 상시가동형으로 작동하기 때문에 공격을 실제로 방어하기 전까지 트래픽을 라우팅할 필요가 없습니다. 또한, Akamai는 전세계 웹 트래픽의 15~30%를 처리하면서 최신 보안 위협에 대한 광범위한 인텔리전스를 확보하고 있는데 이를 기반으로 룰을 지속적으로 업데이트함으로써 최신 공격에 대응해 나갈 수 있습니다. 또한, 추가적으로 보안을 강화하고 싶을 경우 Akamai 전문 서비스팀의 지원(옵션)을 받을 수 있습니다.

KSD 기능

KSD의 기능은 다음과 같습니다.

- DDoS 공격 방어
- 맞춤형 웹 애플리케이션 방화벽(WAF)
- Site Shield(오리진 직접 공격 방어)
- Adaptive Caching(적응형 캐싱)
- 사이트 장애 복구
- Access Control
- NetStorage
- 로그 전송 서비스
- SIEM 애플리케이션과 즉시 통합
- ISO 27002 컴플라이언스 관리 모듈

DDoS 방어

Akamai가 처리하는 트래픽 규모는 46Tbps를 초과했습니다. 수십에서 수백 Gbps에 달하는 초대형 공격도 Akamai Intelligent Platform™은 문제없이 처리합니다. KSD는 모든 유형의 DDoS 공격, 웹 애플리케이션 공격, 오리진 직접 공격 등을 모두 방어하고 Fast DNS 솔루션(옵션)은 DNS 인프라를 표적으로 한 DDoS 공격을 방어합니다. KSD는 Akamai Intelligent Platform을 기반으로 구축되어 있는데, 이 플랫폼은 131개 국가, 1600여 개의 네트워크, 3500개 이상의 위치에 구축된 23만 대 이상의 서버로 구성되어 있습니다. 고객의 웹 서버 및 웹 애플리케이션과 멀리 떨어져 있는 Akamai 네트워크의 엣지 서버에서 공격이 차단됩니다.

장점

비즈니스 측면의 혜택

- 다운타임·웹사이트 변조·데이터 유출 리스크 감소
- 매출·고객 충성도·브랜드 가치 유지
- 공격 발생 시에도 성능 유지
- 공격 트래픽 급증으로 인한 손실 감소
- 보안 하드웨어 및 소프트웨어에 대한 자본 지출 감소

기술 측면의 혜택:

- 기존의 IT 인프라와 원활하게 통합
- DDoS 공격을 받는 중에도 업타임 및 가용성 최대화
- 웹 애플리케이션 인프라 방어
- 오리진 직접 공격 방어
- 온디맨드 방식으로 확장
- SIEM 애플리케이션에서 **포괄적으로 위협 파악**
- 최신 애플리케이션 보안 정보 제공

Akamai Intelligent Platform은 리버스 프록시로 설계되었으며 포트 80(HTTP)과 443(HTTPS)에서 오는 트래픽만 허용합니다. 모든 네트워크 레이어(레이어 3 및 4) DDoS 공격이 자동으로 차단되는데, 여기에는 ICMP, SYN, ACK, RESET, UDP Flood, UDP Fragment와 같은 트래픽이 포함됩니다.

Kona Rule Set

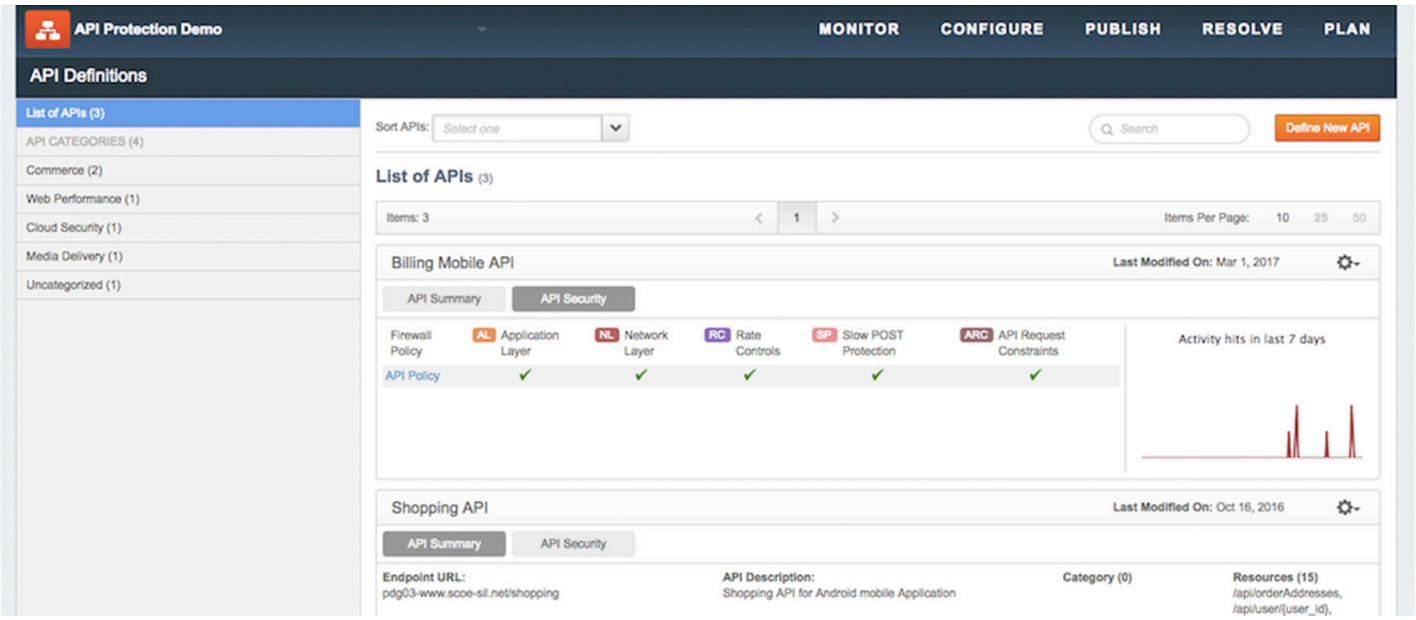
KSD는 미리 설정 가능한 애플리케이션 레이어 방화벽 보호 기능을 다수 포함하고 있습니다. KSD 룰은 프로토콜 위반, 요청 한도 위반, HTTP 정책 위반, 악성 로봇, 일반 인젝션 공격, 명령어 인젝션 공격, 트로이 백도어, 아웃바운드 데이터 유출 등으로 분류되어 있고 각 룰은 정기적으로 업데이트됩니다. 이 일련의 룰은 'Kona 룰 세트(KRS)'라고 불립니다.

KRS는 가장 최근에 발생한 보안 위협과 공격에 대응함으로써 수많은 고객사를 보호합니다. Akamai 위협 연구팀(Threat Research Team)은 정기적으로 룰을 업데이트하고 KSD를 사용하고 있는 모든 고객사에 업데이트된 룰을 적용합니다.

Kona Site Defender

API 보호

KSD는 API를 악성 호출로부터 보호하기 위해 포지티브 및 네거티브 보안 모델을 사용합니다. 고객은 허용하고 싶은 요청과 콜을 직접 결정할 수 있고 KSD는 예외 처리된 값을 기준으로 RESTful API의 변수를 조사하고 JSON body와 경로 변수를 조사해 위험한 콘텐츠가 있는지 확인합니다. 전송률 관리(Rate Control) 기능은 API를 통해 발생하는 DDoS 공격을 방어할 수 있으며 KSD는 API에 대한 애널리틱스와 리포팅을 포함하고 있습니다.



맞춤형 룰 생성기(Custom Rule Builder)

KSD의 룰 세트는 자주 업데이트되고 Akamai의 Professional Services팀은 Security Optimization Assistance 패키지를 통해 개별 고객의 요구사항에 맞는 룰을 생성합니다. 한편, 룰을 직접 생성하고 싶어 하는 고객들을 위해 맞춤형 룰 생성기 역시 기본으로 제공됩니다. 이 생성기는 고객이 쉽게 사용할 수 있는 직관적인 인터페이스를 제공합니다. 맞춤형 룰은 WAF에서 표준 룰을 정의하기 전에 새로운 웹사이트 취약점을 빠르게 방어할 수 있는 가상 패치 역할을 합니다.

컴플라이언스 관리

KSD는 Akamai 제품을 사용하는 것이 고객의 컴플라이언스 계획에 미치는 영향을 정확하게 이해하고 검증하기 위해 ISO27002 컴플라이언스 관리 구성 요소를 포함하고 있습니다. 여기에는 ISO 27002 모듈과 관련된 일반적인 요구사항에 대응할 수 있는 핵심 내용이 포함되어 있습니다. 다른 컴플라이언스 프레임워크를 지원하는 모듈 역시 추가적으로 제공됩니다.

Akamai 생태계

Akamai는 빠르고 안전하며 신뢰할 수 있는 인터넷 환경을 제공합니다. 당사가 제공하는 포괄적인 솔루션은 전세계적으로 촘촘하게 구축된 Akamai Intelligent Platform을 기반으로 설계되었습니다. 모든 솔루션은 당사 통합 포털인 Luna Control Center를 통해 고객사별로 가시성과 통제력을 제공합니다. 또한 Akamai의 전문 서비스는 고객사가 전략 변경에 맞게 혁신을 주도해 나갈 수 있도록 지원합니다.

Akamai FASTER FORWARD

Akamai 소개

Akamai는 가장 탄탄한 신뢰를 받는 세계 최대 규모의 클라우드 전송 플랫폼으로, 고객이 사용하는 장소와 디바이스에 상관없이 안전하고 쾌적한 디지털 경험을 손쉽게 제공할 수 있도록 지원합니다. 전 세계 각지에 대규모로 분산 배치된 Akamai의 플랫폼은 130개국에서 20만 대의 서버에 배포되는 등의 독보적인 배포 규모를 자랑하며 고객에게 탁월한 성능과 위협 방어 기능을 제공합니다. 웹•모바일 성능 향상, 클라우드 보안, 기업 접속, 비디오 전송 솔루션으로 구성된 Akamai의 솔루션 제품군은 탁월한 고객 서비스와 24시간 연중무휴 모니터링의 지원을 받습니다. 금융 기관, 유명 이커머스 기업, 미디어•엔터테인먼트 사업자, 정부 기관이 Akamai를 신뢰하는 이유를 알아보려면 Akamai 홈페이지(www.akamai.com) 또는 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 @Akamai를 팔로우하십시오. 전 세계 Akamai 연락처 정보는 www.akamai.com/locations에서 확인할 수 있습니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표전화는 02-2193-7200입니다. 2017년 3월 발행.