Kona Site Defender

기업의 과감한 혁신을 뒷받침하는 통합 보안 솔루션

두려움 없이 혁신하는 기업만이 하이퍼커넥티드 세상에서 성공할 수 있습니다.

디도스, 웹 애플리케이션, DNS 인프라 공격은 오늘날 기업들이 마주한 대표적인 보안 위협입니다. 이런 공격들은 갈수록 대담해지고 있으며 모든 지역과 산업에 걸쳐 발생하고 있습니다. 이로 인해 다운타임이 발생하고 대역폭 비용이 증가하며 기밀 정보가 손실되기도 합니다. 하지만, 이런 보안 위협과 리스크에도 불구하고 소비자와 기업의 웹 콘텐츠 소비는 점차 증가하고 있습니다. 하이퍼커넥티드 세상에서 성공하길 원하는 기업들은 공격자들을 끊임없이 감시하는 데 시간을 허비하는 대신 웹 콘텐츠를 확장하는 데 역량을 집중해야 합니다. 기업들은 보안 위협에 대한 우려 없이 혁신을 달성할 수 있어야 합니다.

특징

Akamai는 매일 28Tbps 이상의 웹 트래픽을 처리하고 있습니다. 수십 혹은 수백Gbps 규모의 공격도 Akamai 네트워크에서 쉽게 처리됩니다.

Kona Site Defender(KSD)는 모든 유형의 디도스 공격, 웹 애플리케이션 공격, 오리진을 직접 겨냥한 공격 등을 모두 방어하고 Akamai Fast DNS 솔루션(옵션)은 DNS 인프라를 표적으로 한 공격을 방어합니다. KSD는 Akamai Intelligent Platform을 기반으로 구축되어 있는데 이 플랫폼은 100여 개 국가에 1,300여개의 네트워크와 20만대 이상의 서버를 보유하고 있습니다.

디도스 방어 KSD는 Akamai Intelligent Platform을 통해 디도스 공격을 방어합니다. 애플리케이션 레이어 측면의 디도스 트래픽은 흡수되고, 네트워크 레이어 측면의 디도스 공격 (SYN Floods, UDP Floods 등) 트래픽은 차단되며 네트워크 엣지에서 정상 트래픽만 허용되도록 설계되어 있습니다.

KSD는 모든 서버에 구축되어 있기 때문에 중단 없는 보안 서비스를 제공할 수 있으며, 포트 80(HTTP) 또는 포트 443(HTTPS) 트래픽만 허용합니다. 사용 요금 상한선이 있기 때문에 디도스 공격 트래픽이 증가해도 과도한 비용을 부담할 필요가 없습니다. 또한 고객의 요구사항에 따라 유연한 캐싱이 가능하기 때문에 오리진으로부터의 부하 분산을 최대화합니다.

Akamai Intelligent Platform은 전세계적으로 광범위하게 분산되어 있고 뛰어난 확장성을 갖고 있기 때문에 고객사 웹사이트 100% 가용성을 항상 유지할 수 있습니다. Akamai는 매일 평균 12Tbps의 트래픽을 처리하며 일일 최대 트래픽이 26Tbps를 넘는 경우도 있습니다. KSD는 오리진에 도달하는 최적의 경로를 유지한 상태에서 공격을 방어하기 때문에 성능 저하 없는 보안 서비스를 제공합니다. 또한, 고객사 오리진이 아닌 공격 요청이 발생한 지점으로부터 불과 몇 네트워크 홉 내에서 공격을 차단합니다.

애플리케이션 레이어 보호 KSD는 Akamai만의 독자적인 기술로 만든 WAF(Web Application Firewall)를 포함하고 있습니다. WAF는 우수한 확장성을 갖추고 있으며 애플리케이션 레이어 공격을 방어합니다. KSD는 전세계적으로 촘촘하게 구축된 20만대의 서버에 인라인 형태로 배치되어 있고 HTTP와 HTTPS 공격 트래픽을 탐지·처리하고 공격 탐지 정보를 제공 합니다. 또한 공격 트래픽이 고객사 오리진에 도착하기 전에 공격 발생지와 가까운 곳에서 공격을 차단합니다. WAF는 애플리케이션을 보호하기 위해 하기와 같은 'Kona 룰 세트(KRS)'를 포함하고 있습니다.

Kona 룰 세트

KSD 룰은 사전 정의되어 있고 구성 가능한 애플리케이션 레이어 방화벽(WAF) 룰을 다수 포함하고 있습니다. WAF룰은 프로토콜 위반, 요청 한도 초과, HTTP 정책 위반, 악성 로봇, 다양한 인젝션 공격 및 명령어 기반 인젝션 공격, 트로이 백도어, 아웃바운드 데이터 유출 등에 따라 분류되어 있는데 정기적으로 업데이트 됩니다. 이 일련의 룰은 'Kona 룰 세트(KRS)'라고 불립니다.

KSD로 얻을 수 있는 혜택

- 다운타임·변조·데이터 도난의 위험 감소
- 매출·고객 충성도·브랜드 가치 유지
- 공격 발생 시에도 성능 유지
- 공격 트래픽 급증에 따라 발생되는 비용 감소
- 보안 하드웨어 및 소프트웨어에 대한 자본 비용 감소

운영 및 기술 측면의 혜택

- 기존 IT 인프라와 원활하게 통합
- 디도스 공격 중에도 업타임 및 가용성 최대화
- 웹 애플리케이션 인프라 방어
- 오리진을 겨냥한 직접 공격 방어
- DNS 인프라의 가용성 확보
- 온디맨드 방식으로 확장
- 최신 애플리케이션 보안 정보 제공

Kona Site Defender

Kona 룰 세트는 가장 최근에 발생한 보안 위협 및 공격을 처리함으로써 고객사를 보호합니다. Akamai 위협 연구팀(Threat Research Team)은 정기적으로 이 룰을 업데이트하고 KSD를 사용하고 있는 모든 고객사에 업데이트된 룰을 적용합니다. Kona 룰은 Low Orbit Ion Cannon, High Orbit Ion Cannon, HULK, Dirt Jumper, Havij SQL Injection Tool, Netsparker, ApacheBench, Webhive 등의 공격을 방어할 수 있으며 다음과 같은 내용을 포함하고 있습니다.

- 각각의 룰 점수를 합산해서 리스크 총점을 산출하는데 이 과정을 'anomaly scoring'이라 부릅니다. 이 리스크 총점을 바탕으로 탐지(Alert) 혹은 거부(Deny) 결정을 내립니다.
- 다계층 정규식(cascading regular expression) 룰이 HTTP 요청·응답 헤더와 HTTP POST 요청·응답 바디를 조사함으로써 SQL 인젝션과 XSS 등의 공격을 방어합니다.
- 룰을 간편하게 업그레이드하기 위해 다음과 같은 여러 기능이 제공됩니다.
  - » 기존 고객이 WAF 정책을 최신 Kona 룰로 업그레이드할 수 있는 업그레이드 마법사
  - » 기존의 룰을 이용해 공격을 방어하면서 동시에 새로운 Kona 룰 세트로 튜닝할 수 있는 평가 모드(evaluation mode)
- 고객사의 변경 제어 프로세스를 유지하면서 신규 룰을 적용할 수 있도록 뒷받침하는 룰 버전 기술

네트워크 레이어 제어 고객이 정의한 IP 화이트리스트 및 블랙리스트를 적용할 수 있는 기능입니다. 리스트 업데이트 현황은 Akamai 글로벌 네트워크를 통해 전파되는데 불과 몇 분밖에 소요되지 않기 때문에 공격에 신속하게 대응할 수 있습니다. 또한 특정 IP 주소에서 들어오는 요청을 차단함으로써 애플리케이션 레이어 공격으로부터 고객사 오리진을 보호하고 지역별 차단(geo blocking)을 실시하는 기능도 있습니다. 토르 출구 노드(Tor exit node)와 같은 고객사가 지정한 리스트를 포함해 최대 10,000개의 CIDR이 지원됩니다. IP 차단 API는 블랙리스트와 화이트리스트를 모두 자동으로 업데이트하고 처리합니다.

Rate Control Akamai 서버와 고객사 오리진으로 들어오는 요청률을 모니터링하고 제어함으로써 애플리케이션 레이어 디도스 공격을 방어하는 기능입니다. KSD는 폭주하는 사용자 요청을 단 몇 초 이내에 처리할 수 있습니다.

Site Shield 고객사 오리진을 공중망(public internet)으로부터 숨길 수 있는 기능입니다. Akamai Professional Service를 통해 Site Shield 맵을 설정할 수 있고 고객사가 Luna나 API를 통해서도 직접 설정 가능합니다. Site Shield는 기존 인프라를 보완할 뿐만 아니라 오리진을 직접 겨냥한 공격을 방어합니다.

Security Monitor 이 기능은 보안 위협에 관한 정보를 실시간으로 제공하고 공격자, 공격 대상, 어떤 방어 기능에 의해 공격이 탐지되었는지, 어떤 요청 때문에 방어 기능이 작동되었는지 등 공격 탐지와 관련된 세부 정보를 제공합니다. 룰 튜닝 및 공격 조사와 관련된 요청·응답 헤더 정보 역시 이 기능을 통해 확인 가능합니다.

Rule Update Service Akamai Professional Service팀이 정기적으로 KSD와 WAF 설정을 검토하는 기능입니다. Security Monitor 로그의 오탐을 분석하고 KSD, 오리진 설정 튜닝, 최적화 등에 대해 고객사에 제안해 드립니다.

Fast DNS 최종 사용자가 웹 사이트에 직접 접속하도록 하기 위해 설계된 신뢰성, 안전성, 확장성이 우수한 기능입니다. Fast DNS는 전세계적으로 광범위하게 분산된 Akamai Intelligent Platform의 2차 권한 네임 서버(ANS)를 기반으로 합니다. 기존의 DNS 관리 프로세스를 변경할 필요가 없으며 안전성·보안성·확장성이 뛰어난 DNS 레졸루션을 제공합니다.

Client Reputation(옵션) 이 모듈은 악성 공격자의 공격을 한층 견고하게 방어하고 한층 더 높은 수준의 가시성을 확보해 줍니다. Client Reputation은 공격 기법이 아닌 웹 클라이언트 즉, 위협의 원인을 차단하는 데 집중합니다. Akamai는 매 분기마다 수십억 개의 IP 주소를 확인하는데 Client Reputation은 고급 알고리즘을 이용해 웹 클라이언트에서 수집된 데이터를 분석하고 악의적 공격자를 식별합니다. 악의적인 웹 클라이언트가 3가지 악의적 행동(웹사이트 스캐닝, 일반적인 웹 공격 개시, 디도스 공격)에 가담할 가능성을 기준으로 점수가 매겨집니다.

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 Professional Service는 고객사가 전략 변경에 맞게 혁신을 주도해 나갈 수 있도록 지원합니다.

Akamai FASTER FORWARD

전세계 콘텐츠 전송 네트워크(CDN) 분야를 이끌고 있는 Akamai는 빠르고 안전하며 신뢰할 수 있는 인터넷 환경을 제공합니다. Akamai는 웹 성능, 모바일 성능, 클라우드 보안, 미디어 전송과 관련된 우수한 솔루션을 공급하고 있으며 이 과정에서 사용 기기나 장소에 상관없이 소비자, 기업, 엔터테인먼트 경험을 최적화하는 방법을 크게 바꿔놓고 있습니다. Akamai의 인터넷 전문가들과 솔루션이 어떻게 기업의 성장을 뒷받침하고 있는지 자세히 알아보려면 Akamai 홈페이지(www.akamai.co.kr) 혹은 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 Akamai(@Akamai)를 팔로우하십시오.

Akamai는 미국 매사추세츠주 케임브리지에 본사를 두고 있으며 전세계 40여 개의 지사를 운영하고 있습니다. Akamai의 우수한 솔루션과 서비스를 사용하는 기업들은 전세계 고객들에게 우수한 웹 경험을 제공할 수 있습니다. Akamai 코리아는 서울시 강남구 강남대로 382 메리츠타워 21층에 위치해 있으며 대표번호는 02-2193-7200입니다.

2015년 4월 발행.