DDoS 공격을 0초 안에 차단할 수 있습니까?

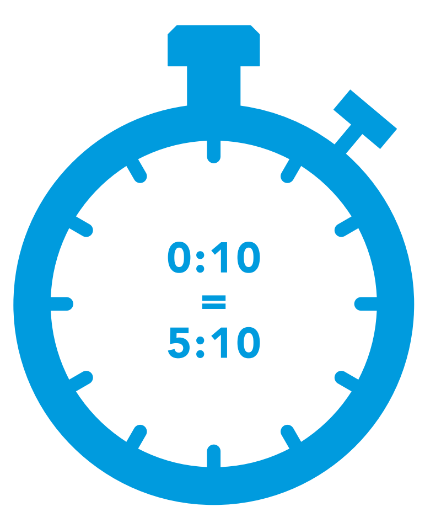
TTM(TIME TO MITIGATE) 정확하게 파악하기

TTM는 유한해야 합니다. DDoS 공격이 시작된 시점과 자산 또는
애플리케이션이 보호되는 시점 사이의 시간입니다.

모든 벤더사의 서비스 수준 협약(SLA)이 이것을 의미하지는 않습니다.
시작되고 중단되는 시점을 정확히 파악해야 합니다.

다음과 같은 벤더사의 일반적인 시나리오에 주의하세요.

벤더사 A



벤더사 A의 컨트롤 기능은 DDoS 공격을 확인하기 전에 5분 이상 트래픽 폭증을 분석해야 합니다.

10초 TTM SLA는 공격이 확인된 후에 시작됩니다.

벤더사 B

벤더사 B의 약관은 TTM을 방어 컨트롤을 배포하는 시간, 즉 대응으로 정의합니다.

공격을 차단하는 데 중점을 둔 SLA가 없습니다.

벤더사 C

벤더사 C의 TTM SLA는 탐지 및 방어 자동화에 집중합니다.

정교한 공격을 차단하는 수동적인 맞춤형 방어 기술은 SLA에 포함되어 있지 않습니다.

약관 이해

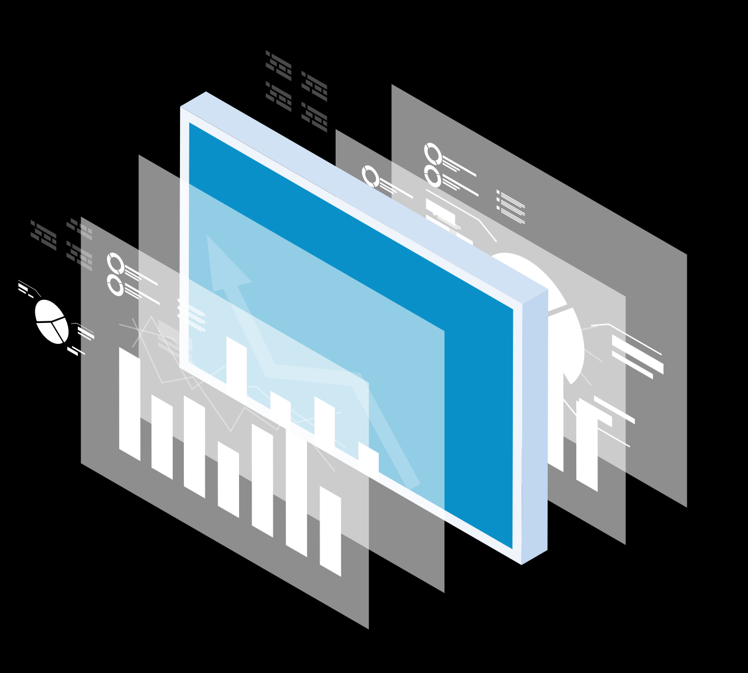
면밀히 살펴야 하는 문구

대응 시간

지속적인 DDoS 공격 ...

사후 탐지

AKAMAI의 공격 방어 시간



0이 0초를 의미하는 경우

Akamai의 선제적 방어 컨트롤은 DDoS 공격을 차단하도록 설계되어 공격 사실을 알기도 전에 이를 방어합니다. 이것이 바로 Akamai Intelligent Edge Platform의 역량입니다.

공격 탐지 시간 + **방어 컨트롤 적용** 시간 + **공격 차단** 시간 = **업계 최고의 공격 방어 시간**

DDOS 를 방어하는 8단계

Akamai는 업계에서 가장 빠른 TTM을 제공하며 위협 연구원, 인시던트 매니저, 보안 아키텍트, 최첨단 방어 기술이 강력하게 결합된 역량을 갖추고 있습니다. Akamai의 SOCC (Security Operations Command Center)는 다음 단계를 실행합니다.

1. 상시 가동형 DDoS 모니터링으로 조기에 공격을 **탐지**합니다.
2. 준비된 런북을 사용해 고객에게 **알림을 전달**합니다.
3. 상시 가동형 라우팅을 통해 고객 트래픽을 **관리**합니다.
4. 트래픽을 **분석**하고 공격 기법을 확인해 방어 조치를 적용합니다.
5. 오탐률 및 미탐률 간의 최적화를 위해 적용된 방어 조치를 **미세 조정**합니다.
6. 새로운 공격 기법을 **식별**합니다.
7. 트래픽을 **분석**하고 새로운 공격 기법을 식별해 지속적으로 방어 조치를 적용합니다.
8. 적용된 방어 조치를 **최적화**하여 공격 변화를 무력화 시킵니다.

TTM이 지연되었을 때 발생하는 리스크

다운타임으로 인해 어떤 **결과**가 발생합니까?

0:01
1초 후 웹 기반 자산 또는 애플리케이션을 사용할 수 없게 됩니다.

0:10
10초 후에 고객이 겪는 불편이 증가하고 직원 생산성이 감소합니다.

5:00
5분 후 브랜드 평판이 손상되고 매출 손실이 발생합니다.

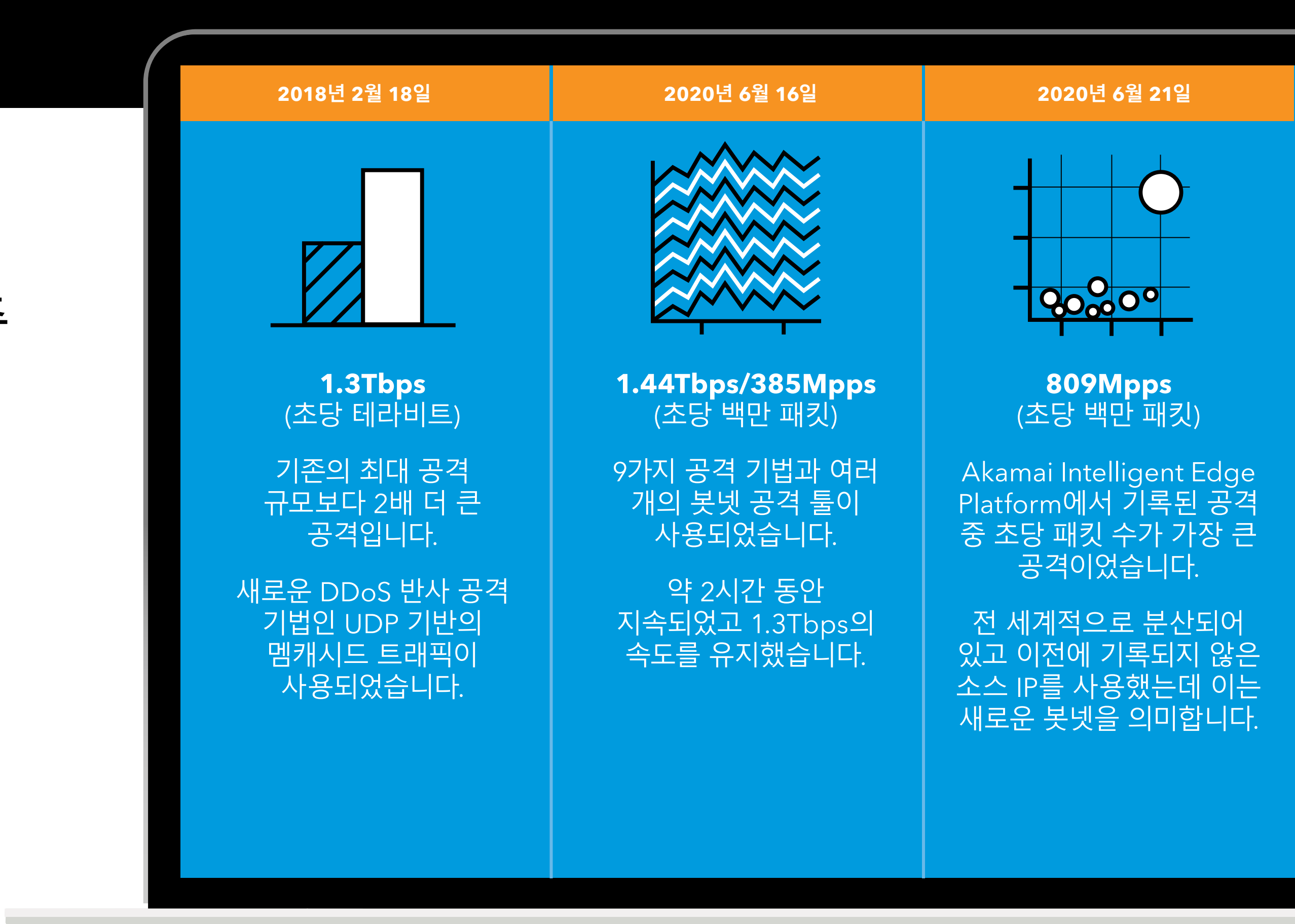
DDOS 대응 체계 평가

- 벤더사가 얼마나 빨리 공격을 탐지할 수 있습니까?
- 중요한 애플리케이션을 사용할 수 있습니까?
- 부수적인 피해가 발생합니까?
- 정상 사용자들이 영향을 받습니까?
- 벤더사가 얼마나 빨리 방어 대응 조치를 적용할 수 있습니까?
- 벤더사가 얼마나 빨리 트래픽 분석을 시작할 수 있습니까?

AKAMAI 위협 인사이트

규모 증가 **복잡성** 가중 **위험성** 증가

DDoS 공격이 기록적인 수준으로 증가하고 있습니다. 2020년 DDoS 공격의 규모와 복잡성이 증가했고 공격 기법의 수와 조합은 전례 없는 수준입니다.



2018년 2월 18일	2020년 6월 16일	2020년 6월 21일
1.3Tbps (초당 테라비트) 기존의 최대 공격 규모보다 2배 더 큰 공격입니다. 새로운 DDoS 반사 공격 기법인 UDP 기반의 멤캐시드 트래픽이 사용되었습니다.	**1.44Tbps/385Mpps** (초당 백만 패킷) 9가지 공격 기법과 여러 개의 봇넷 공격 툴이 사용되었습니다. 약 2시간 동안 지속되었고 1.3Tbps의 속도를 유지했습니다.	**809Mpps** (초당 백만 패킷) Akamai Intelligent Edge Platform에서 기록된 공격 중 초당 패킷 수가 가장 큰 공격이었습니다. 전 세계적으로 분산되어 있고 이전에 기록되지 않은 소스 IP를 사용했는데 이는 새로운 봇넷을 의미합니다.

공격을 효과적으로 방어하려면 검증된 플랫폼, 숙련된 전문가, 정교한 프로세스와 기술이 필요합니다.

공격 방어 시간은 정상 트래픽과 사용자에게 영향을 주지 않으면서 얼마나 빨리 악성 트래픽을 식별하고 차단하는지를 의미합니다.

결국 미션 크리티컬 애플리케이션, 인프라, 브랜드 평판 보호가 성공적인 방어 역량을 평가하는 기준입니다.

지금 바로 DDOS 방어 기능을 강화하세요

Akamai가 0초 방어를 지원하는 방법을 확인하세요.

자세히 보기

Akamai는 전 세계 주요 기업들에게 안전하고 쾌적한 디지털 경험을 제공합니다. Akamai의 인텔리전트 엣지 플랫폼은 기업과 클라우드 등 모든 곳으로 확장하고 있고 고객의 비즈니스가 빠르고, 스마트하며, 안전하게 운영될 수 있도록 지원합니다. 대표적인 글로벌 기업들은 Akamai 솔루션을 통해 멀티 클라우드 아키텍처를 강화하고 경쟁 우위를 확보하고 있습니다. Akamai는 가장 가까운 곳에서 사용자에게 의사 결정, 앱, 경험을 제공하고 공격과 위협을 먼 곳에서 차단합니다. Akamai 포트폴리오는 엣지 보안, 웹·모바일 성능, 엔터프라이즈 접속, 비디오 전송 솔루션으로 구성되어 있고 우수한 고객 서비스, 애널리틱스, 24시간 연중무휴 모니터링 서비스를 제공합니다. 대표적인 기업과 기관에서 Akamai를 신뢰하는 이유를 알아보려면 Akamai 홈페이지(www.akamai.com) 또는 블로그(blogs.akamai.com)를 방문하거나 Twitter에서 @Akamai를 팔로우하시기 바랍니다. 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.

2020년 11월 발행