디지털 트랜스포메이션을 통한
비즈니스 혁신과 4차 산업혁명 대응을 위한

# GIT 솔루션즈 데이

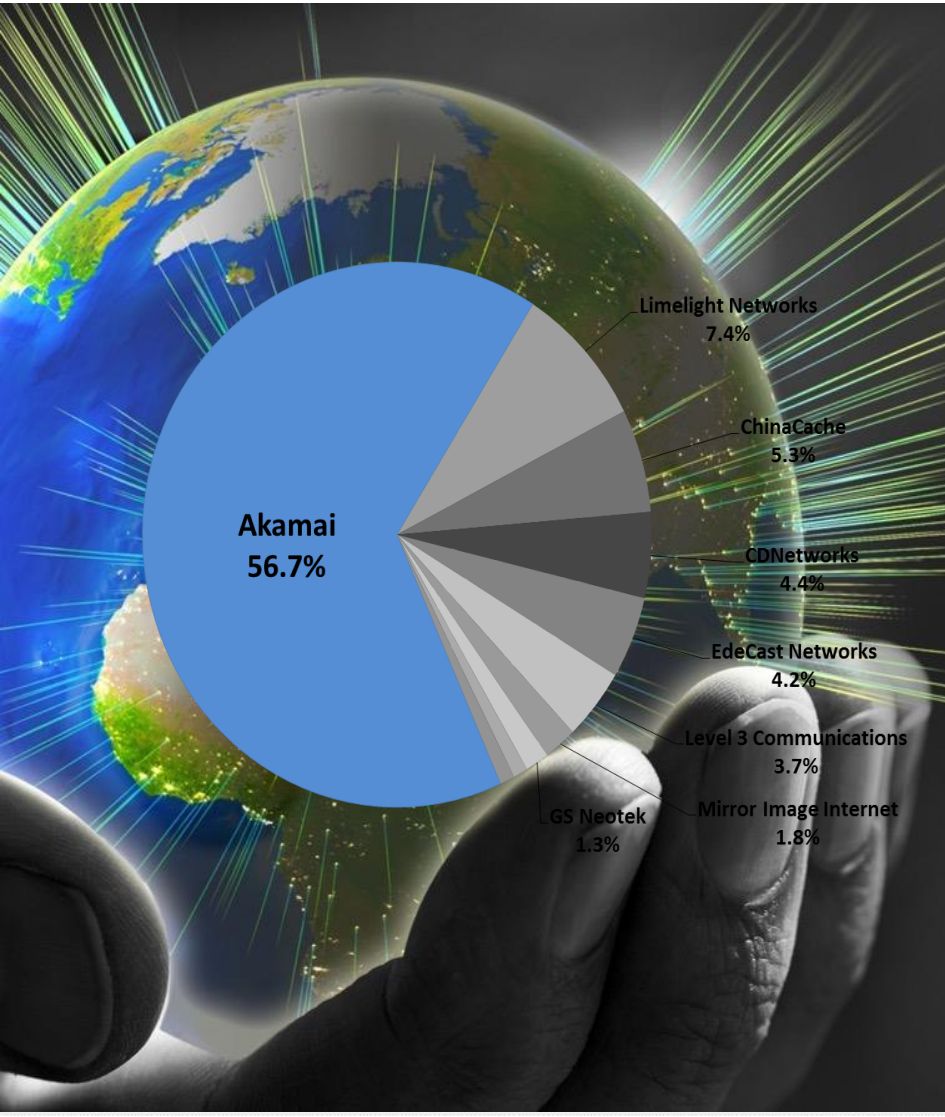
## 아카마이 솔루션을 이용한 선재적 위협 방어

2018.10.17 / 클라우드 보안팀 이신우

# 목차

# 아카마이 소개

# 아카마이 개요




아카마이 = 하와이어로 “Smart”란 뜻

**세계 최대의 커버리지**

- ✓ 240,000+ servers
- ✓ 1,300+ networks
- ✓ 3,400+ locations
- ✓ 130+ countries
- ✓ 1,100+ Cities

**세계 최대의 웹 트래픽 처리용량**

- ✓ 전세계 웹 트래픽의 15 ~ 30 %
- ✓ 최대 60Tbps의 트래픽 수용 기록
- ✓ 초당 3천만 Hit 이상
- ✓ 일 100PB 이상
- ✓ 1.2 Tbps 이상의 DDoS 공격 차단

- 전세계 임직원 6,000명+, 2017년 매출 3조원, NASDAQ(AKAM)
- 2008년 한국 지사 설립. 약 75명의 전문인력이 한국 고객 지원 중

Akamai
FASTER FORWARD

# 아카마이 역량

## 경험

**19**년 **DDoS** 및 **웹 공격** 방어 경험

## 인프라

글로벌 웹트래픽의 ~**30** 퍼센트

플랫폼 상의 트래픽 기록 **63** Tbps

매주 **40** ~ **50** 건의 DDoS 공격 방어

**2,300** Gbps의 공격 처리 용량 확보

## 고객

**1,350** 사 이상의 보안 고객

금융

이커머스

And more...

**2018**

**100** 개의 전세계 **은행**에서 아카마이 보안 솔루션 도입

**2018년 평창 올림픽, 2016년 리오올림픽, 2014년 소치 올림픽**과 **슈퍼볼 XLVIII**을 포함한 최대 규모의 온라인 이벤트 방어

## 사례

**1.35** Tbps

Akamai 단일 공격으로 차단한 최대 규모의 DDoS 공격

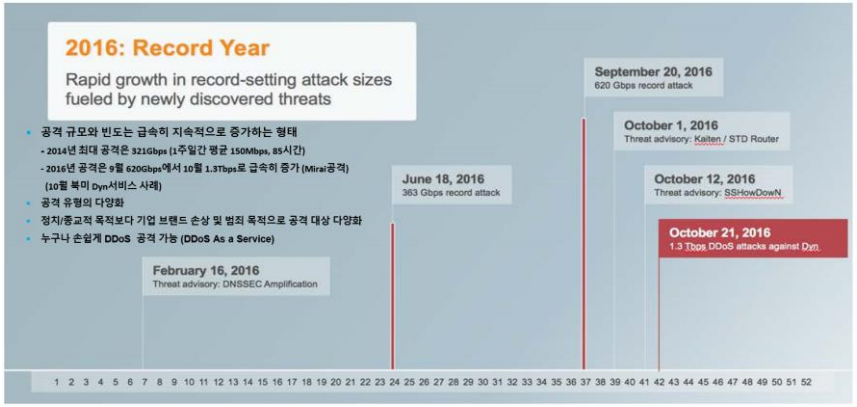
# 레퍼런스

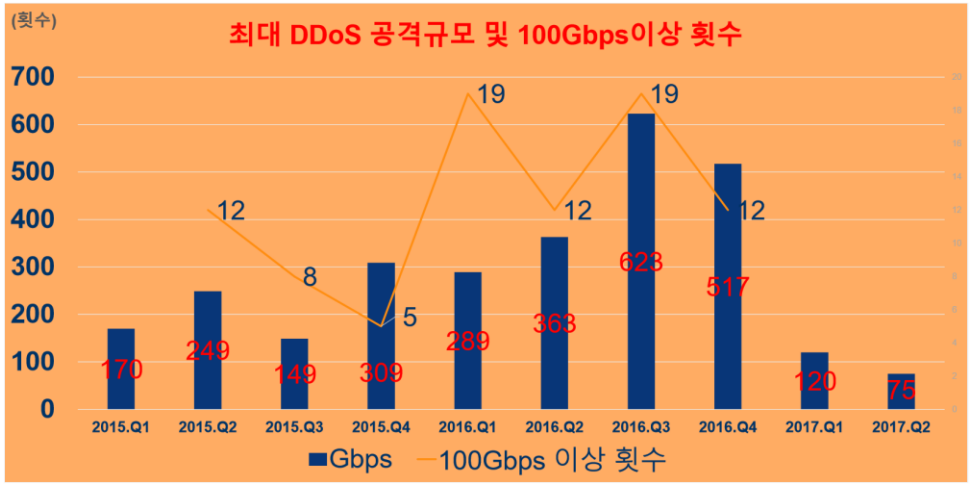
**인터넷을 활용하는 공공, 금융, 엔터프라이즈 및 모든 미디어, 커머스 고객사(6,000+)**

| ENTERPRISE | COMMERCE | HIGH TECH | MEDIA & ENTERTAINMENT | PUBLIC SECTOR |
|---|---|---|---|---|
| 7 of the Top 10 World Banks | 90 of the Top 100 Retailers | 10 of the Top 12 Security Software Companies | All of the Top 30 Media Companies | All branches of U.S. Military |

# 국내외 보안 이슈

# 글로벌 보안 이슈 – 2016년 미라이 봇넷의 등장

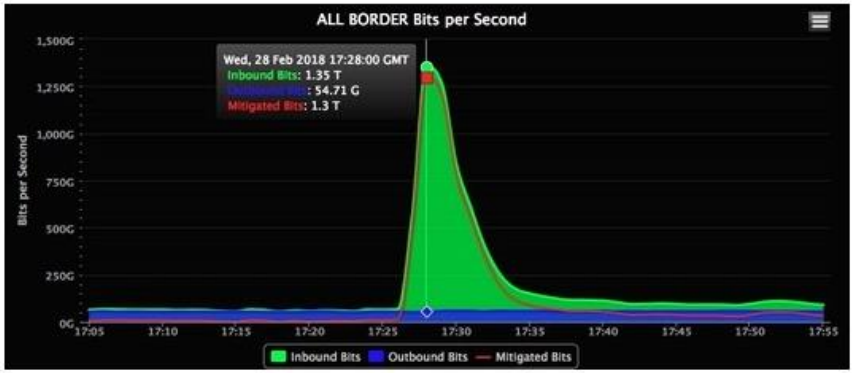




IoT 봇넷 기반 DDoS 공격 툴의 등장으로 DDoS 공격이 단일 사업체가 감당 할 수 없는 수백 Gbps 규모로 증가

# 글로벌 보안 이슈 – 2018년 슈퍼사이즈 DDoS

LILY HAY NEWMAN SECURITY 03.01.18 11:01 AM

## GITHUB SURVIVED THE BIGGEST DDOS ATTACK EVER RECORDED




Real-time traffic from the DDoS attack. AKAMAI

깃허브(Github)를 타깃으로 순간 트래픽이 1.35테라bps에 달하는 DDoS 공격이 발생했다. 이는 지금까지 발생했던 DDoS 공격들 중에서 가장 큰 규모의 DDoS 공격으로 조사됐다.
지난 2월 28일 오후 12시 15분 대규모 디도스 공격이 시작되면서, 깃허브는 공격을 저지하려 노력했지만 간헐적으로 사이트가 끈기는 현상이 발생했다.
10분 내, 깃허브는 DDoS 보안장비업체인 아카마이에 도움 요청을 했으며, 8분 뒤 공격자는 공격을 철회했다.
이번 공격으로 사이버 공격 규모가 점점 커지고 있다는 것을 알 수 있다. 작년에 DNS 서비스 업체인 Dyn이 받은 DDoS 공격과 비교해 볼 수 있는데, 당시 공격의 순간 트래픽은 1.2테라bps였다.

TECHNOLOGY

## Arbor Networks reports record-breaking 1.7Tbps DDoS attack

The record for the largest recorded denial of service attack appears to have been broken less than a week after it was set.

Arbor Networks reported on Monday in a blog post that a 1.7 -terabit-per-second attack took place targeting the customer of a U.S. based internet service provider. Arbor Networks did not specify the victim beyond that description, but said that the ISP had proper defenses in place and that no outages were reported.

"It's a testament to the defense capabilities that this Service Provider had in place to defend against an attack of this nature that no outages were reported because of this," the company wrote.

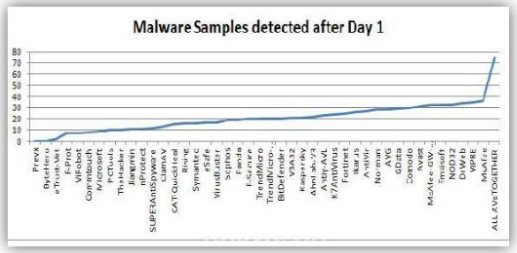
The attack used the same technique that was used in the 1.35Tbps attack on GitHub on Feb. 28, Arbor Networks said. In both cases, attackers used memcached servers to amplify the requests they were sending to their targets.

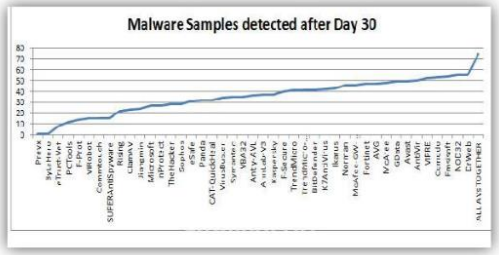
Arbor Networks says more large attacks using the memcached tactic should be expected as long as there is an open supply of memchached servers to be exploited. Memcached servers are systems that cache data in order to speed up networks and websites.

2018년 맴캐시드 서버를 이용한 기록적인 슈퍼사이즈 규모의 Amplification DDoS 공격 등장

# 글로벌 보안 이슈 – 시그니쳐 기반 보안의 한계





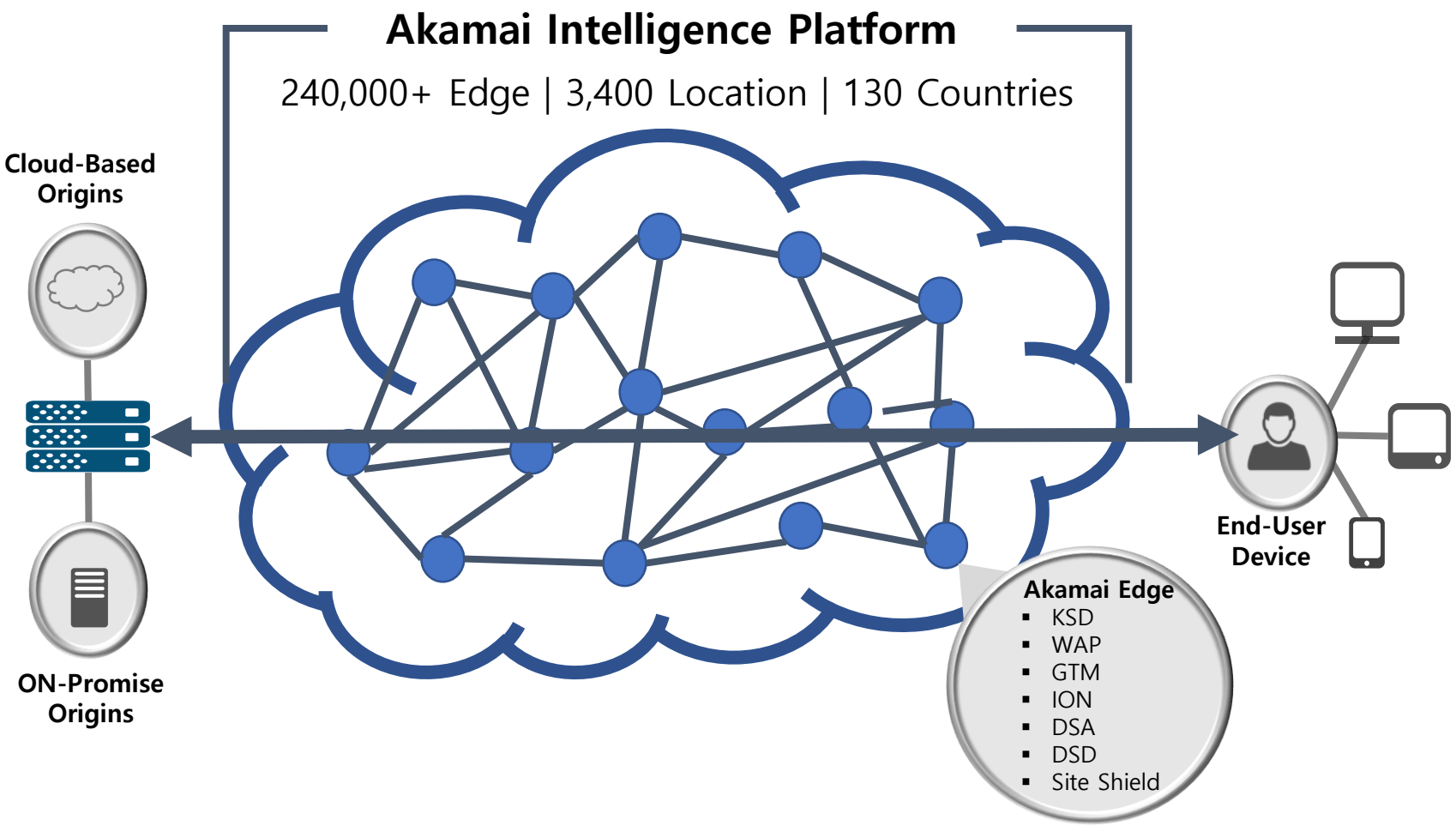




- 공개된 malware 대상으로 1일 동안 AV 테스트 결과 가장 높은 탐지율을 보인 백신도 50% 미만
- 동일한 malware 대상으로 30일 동안 AV 테스트 결과 탐지율은 역시 50% 수준
- 시그니처 방식의 한계로 인해 기존에 알려진 malware도 100% 차단하기 어려운 것이 AV의 현 상황

매일 15만개 이상 등장하는 새로운 악성 코드에  시그니쳐 방식의 대응으로는 한계에 봉착

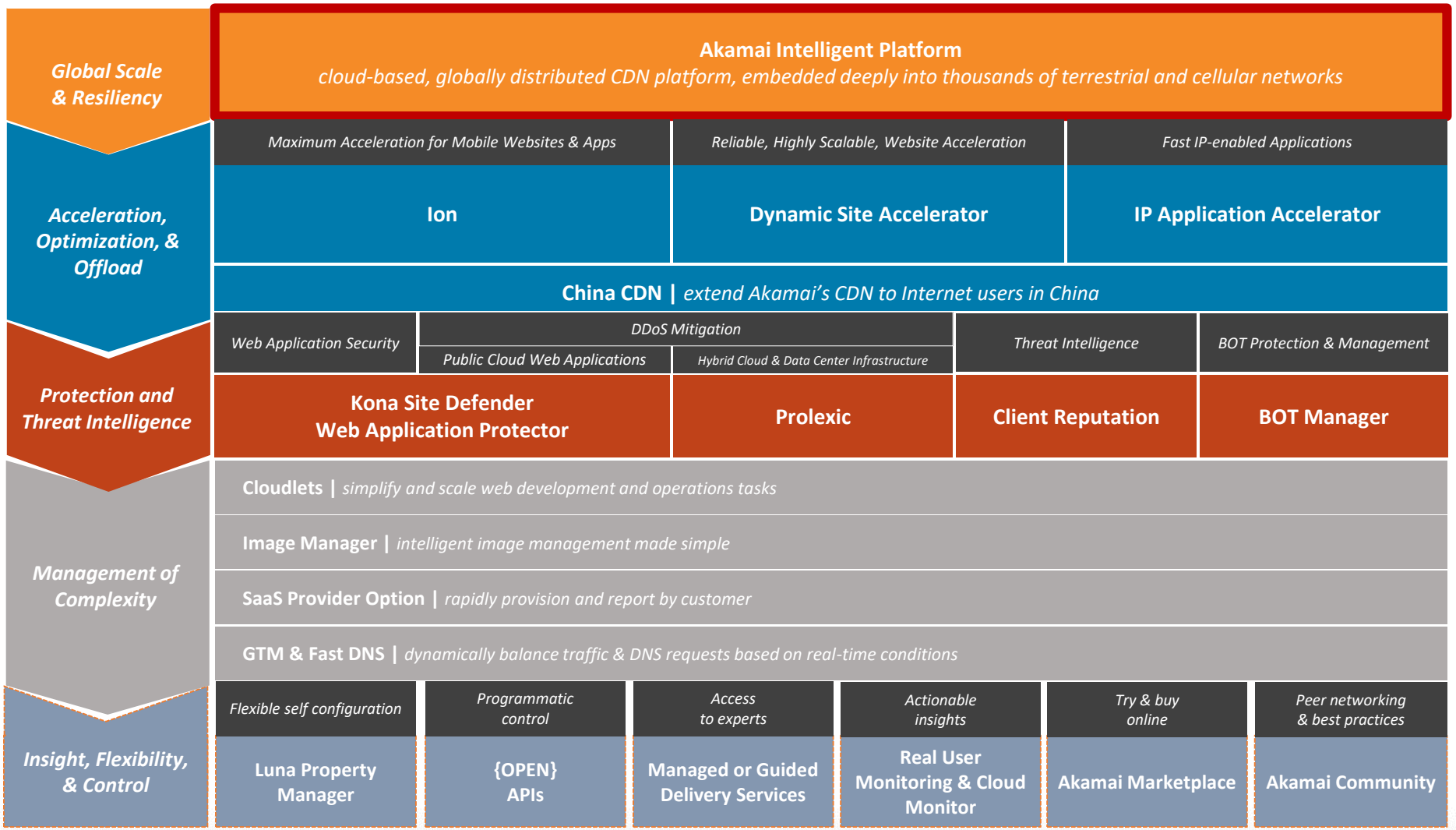
# Akamai Intelligence Platform

# Akamai Intelligence Platform




Akamai Intelligence Platform 은 모든 아카마이 서비스의 근간이 되는 Global Service Platform 입니다.

# Akamai Service Map




아카마이의 모든 서비스는 Intelligence Platform 위에서 정교하게 조직 및 운영 되고 있습니다.

# Akamai Cloud Security Service Map

## Akamai Cloud Security Service

| | WEB Service | DATA Center | Enterprise |
|---|---|---|---|
| 서비스 가용성 확보 | **KSD(Kona Site Defender)**<br>웹서비스 보안을 위한 토탈 솔루션<br>네트워크 및 어플리케이션 공격을<br>CDN 인프라를 활용해 성능 및 안전성 보장 | **Prolexic Routed**<br>라우팅을 이용한 IP 우회 서비스로<br>대용량 DDoS 방어에 최적화된 솔루션<br>글로벌 7개 SC(Scrubbing Center)를<br>통한 분산 처리 | **ETP(Enterprise Threat Protection)**<br>기업내 사용자의 외부 사이트에 대한<br>DNS 요청을 확인 하여 Bot, Malware<br>및 C&C 서버로의 접속 시도를 사전에<br>차단하는 DNS 보안 솔루션 |
| 보안 강화 | **WAP(Web Application Protector)**<br>간소화 된 형태의 웹방어 솔루션<br>전문 보안 인력 확보가 어려운<br>중/소규모의 웹서비스 보안 강화<br><br>**Bot Manager**<br>각종 자동화 된 Bot 으로 인한<br>보안 침해 및 사이트 성능 저하에 대해<br>효율적으로 대응 할 수 있는 솔루션 | **Prolexic Connected**<br>라우팅을 이용한 IP 우회 서비스<br>Routed 서비스와 달리 전용선을<br>이용해 오리진과 통신 하며 Routed 서비스<br>트래픽 제한 해결 가능 | **EAA(Enterprise Application Access)**<br>사내 인프라에 대한 외부접속을<br>단순화 하여 보안을 강화한<br>Remote Access 지원 솔루션 |

FastDNS (글로벌 분산된 DNS 서비스로 기업의 DNS 인프라 확장 가능 100% 가용성 SLA)

글로벌 130개국, 1300개 PoP, 24만대 Edge - Akamai Intelligence Platform

아카마이 보안 서비스 Cloud Security 상품군은 인터넷 비즈니스에 필요한 모든 형태의 강력한 보안을 제공 합니다

# Akamai 보안 서비스 평가

Magic Quadrant

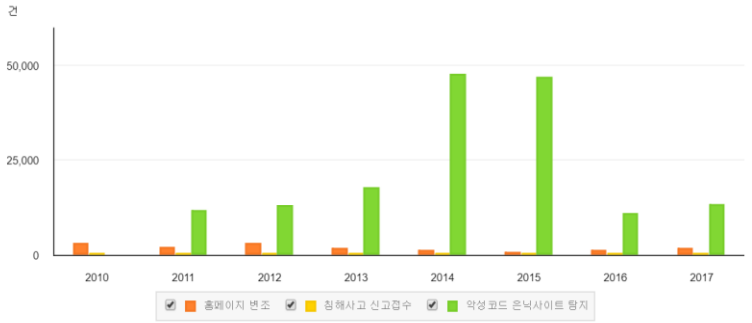


뛰어난 성능 인정 받아 가트너 2018 리포트, Frost wave 2018 2Q 리포트에서 클라우드 베이스로는 유일하게 WAF 부분 LEADERS 로 선정

# Akamai CI & NLTA

# 선재적인 보안 위협 대응의 필요성


해킹사고 건수



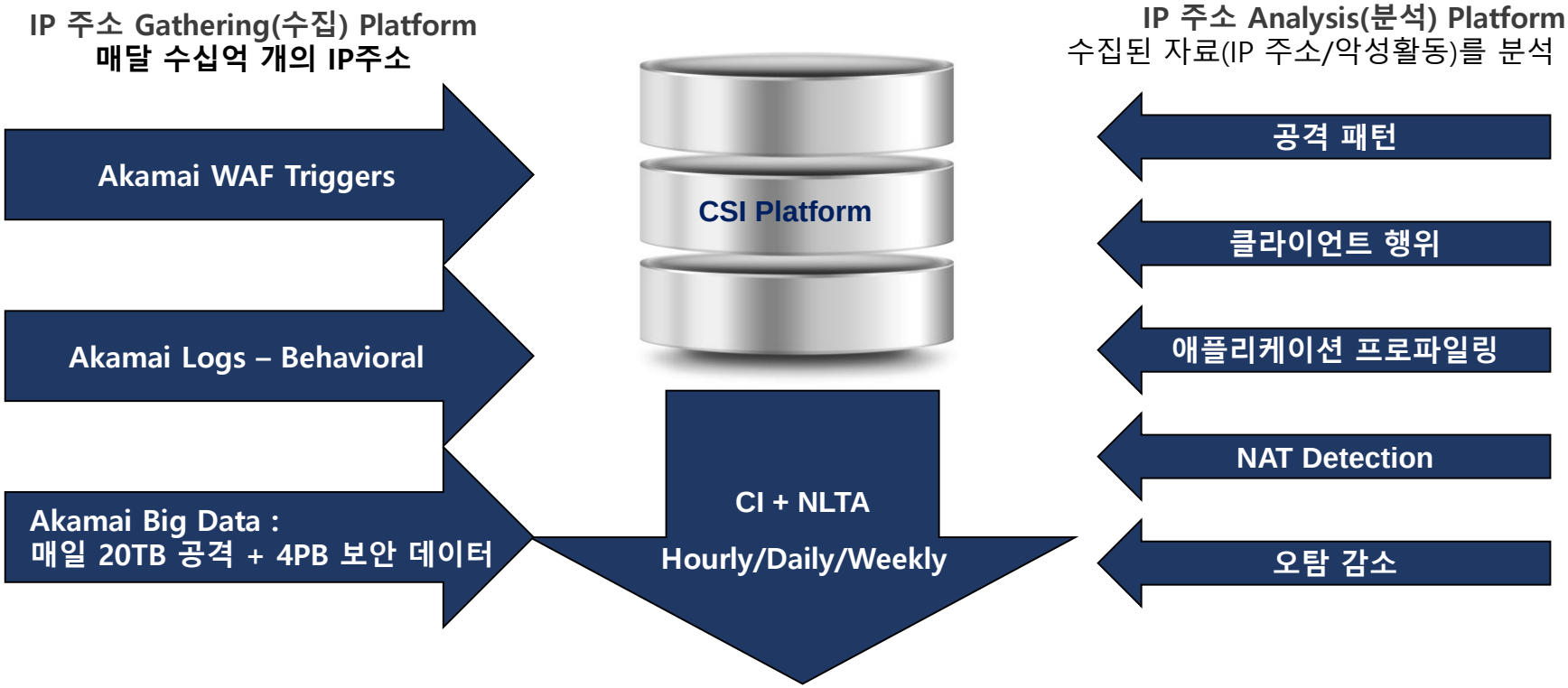

| | 2010 | 2011 | 2012 | 2013 | 2014 | 2015 | 2016 | 2017 |
|---|---|---|---|---|---|---|---|---|
| 홈페이지 변조 | 3,043 | 1,854 | 3,157 | 1,700 | 1,115 | 615 | 1,056 | 1,724 |
| 침해사고 신고접수 | 53 | 63 | 91 | 82 | 175 | 225 | 247 | 287 |
| 악성코드 은닉사이트 탐지 | - | 11,805 | 13,018 | 17,750 | 47,703 | 46,850 | 11,044 | 13,347 |

출처: 한국인터넷진흥원

나날이 고도화 되어 가는 공격자들의 공격 방식에 비해 장비 위주의 보안 대응은 얼마나 실효성이 있을까?

# Akamai CI & NLTA 개요

## Akamai CSI(Cloud Security Intelligence)




**악성으로 판단한 IP 주소**

✓ 위험 지수(Risk Score)명시

Akamai Intelligence Platform의 빅데이터를 바탕으로 보안에 위협이 되는 IP에 대한 정보를 분석 및 수집

# Akamai CI (Client Intelligence)

## CI(Client Intelligence)

✓아카마이 보안 서비스를 사용 중인 고객 서비스를 공격한 IP 정보

✓IP 주소별 행동 패턴을 분석하여 IP주소에 대한 Risk 점수(Scoring)를 산정한 자료

## IP Address 별 악성활동 이력 내용

✓웹 공격 이력(WEBATCK) – SQLi, RFI, LFI, XSS 등의 웹 해킹을 시도한 이력이 있는 IP

✓DoS 공격 이력(DOSATCK) – L7 레이어 DoS 공격을 시도한 이력이 있는 IP

✓웹스크래퍼(WEBSCRP) – 웹에서 대량의 자료를 유출 하려고 시도한 이력이 있는 IP

## Data Feed 형식

CSV 형식

```
#EventTime,IP,Country,ASN,Category,Score,Evidence
1464007200,184.154.164.186,US,32475,WEBATCK,7,XSS
1461800400,184.154.164.186,US,32475,WEBATCK,7,SQLi
1461505500,184.154.164.186,US,32475,WEBATCK,7,XSS
1461354000,184.154.164.186,US,32475,WEBATCK,7,XSS
1461476400,184.154.164.186,US,32475,WEBATCK,7,XSS
1461541200,184.154.164.186,US,32475,WEBATCK,7,SQLi
```

JSON 형식


```
{
 "ip":"209.147.85.108",
 "reputation":{
  "WEBSCRP":[
   {
    "score":3,
    "ts": 1462066920,
    "events":[
     {
      "code":"433468",
      "properties":{
       "eventType":"scrapingUsingSuspiciousUA",
       "requestsCount":109,
       "hostsCount":6
      },
      "targets":{
       "industries":{
        "Akamai":[
         {
          "subvertical":"Cruise lines",
          "vertical":"Hotel & Travel"
         }
        ]
       },
       "span":"30days"
      }
     }
    ]
   }
  ]
 },
 "lastSeen":1462369620,
 "source":{
  "country":"US",
  "region":"PA",
  "network":"11194",
  "city":"SELLERSVILLE"
 }
}
```


| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 |
|---|---|---|---|---|---|---|---|---|---|

(Risk Score 범위: 1-10 ->점수가 높을수록 High Risk)

Akamai Client Intelligence 는 아카마이 서비스에 대한 공격 정보를 수집 활용한 보안 위협 DB 입니다.

# Akamai NLTA (Network Layer Threat Actors)

## NLTA(Networ Layer Threat Actors)

✓아카마이 인프라를 공격 하거나 Scan 한 이력이 있는 IP 정보

✓IP 주소별 행동 패턴을 분석하여 IP주소에 대한 Risk 점수(Scoring)를 산정한 자료

## IP Address 별 악성활동 이력 내용

✓DoS 공격 이력(DOSATCK) – L3/L4 DoS 또는 DDoS 공격을 시도한 이력이 있는 IP

✓스캐닝 툴(SCANTL) – 포트 취약점을 스캔 하려고 한 이력이 있는 IP

## Data Feed 형식

**Client IP : 클라이언트 IP가 핵심이고 다음 속성을 포함한다는 데 유의해야 합니다.**
**Category : 위험 유형을 설명한 컨테이너 개체**
**Name : 위협 행위자 유형인 "검사자" 또는 포트 스캐너"**
**Details : 위협 세부 정보에 해당하는 컨테이너 개체**
**Targets : 대상 세부 정보에 해당하는 컨테이너 개체**
**Ports : 다수의 대상 포트와 프로토콜(예: "UDP80", "TCP23")**
**Source : 클라이언트 IP의 위치 정보에 대한 EdgeScape™ 파생 정보에 해당하는 컨테이너 개체**
**Country : ISO 2자 국가 코드**
**Network : 클라이언트 IP를 포함하는 네트워크의 익명 시스템**
**Score : 번호 클라이언트 IP에 할당된 점수(1-10, 10이 가장 높은 심각도)**
**Observations : 클라이언트 IP의 관찰 정보에 해당하는 컨테이너 개체**
**Destination_IPS : 클라이언트 IP가 대상으로 지정한 대상 IP 개수**
**Packets : 이 클라이언트 IP에서 기록된 패킷 수**
**Last_Seen : 클라이언트가 Akamai 플랫폼에서 마지막으로 확인한 시간의 유닉스 에포크**

**Example line**


```
{
"101.229.39.85": {
    "category": {
      "name": "prober",
      "details": {
        "targets": {
          "ports": [
            "TCP23",
            "TCP2323"
          ]
        }
      },
      "source": {
        "country": "CN",
        "network": "4812"
      },
      "score": 10,
      "observations": {
        "destination_ips": 426,
        "packets": 855
      },
      "first_seen": 0,
      "last_seen": "1494432493"
}
```


Akamai NLTA 는 아카마이 서비스 인프라에 대한 공격 정보를 수집 활용한 보안 위협 DB 입니다.

# Akamai CI & NLTA 활용의 예

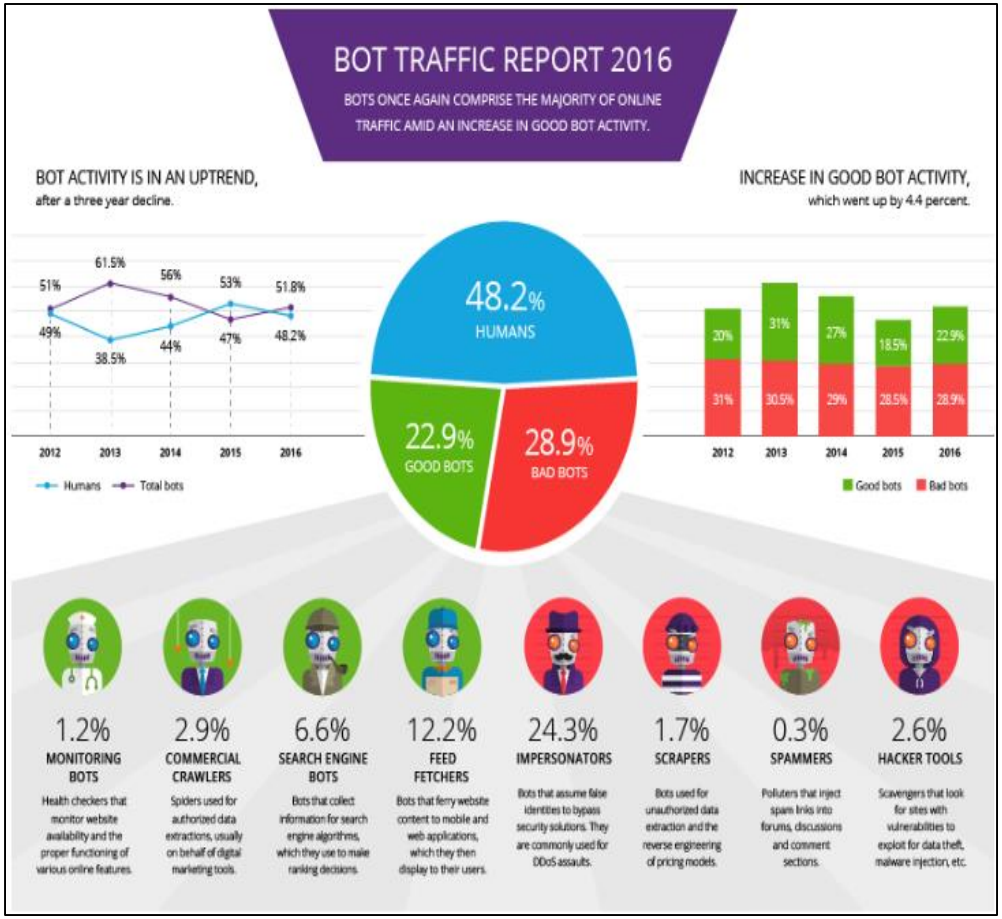

- ❑ 대한민국 정부산하 K모 기관 도입 사용(2017년~ 현재)
- ❑ 싱가포르 경찰청 도입 사용(2016년~ 현재)
- ❑ 일본 경찰청 도입 사용(2015년~ 현재)
- ❑ 미 연방 정부의 15개 장관급 내각 기관 중 14개 기관(2014년 ~ 현재)
  - ✓ 미국 주경찰청
  - ✓ 미국 국가정보기관
  - ✓ 미국 국방성
  - ✓ 전세계 모든 미군기지 보안 센터 등

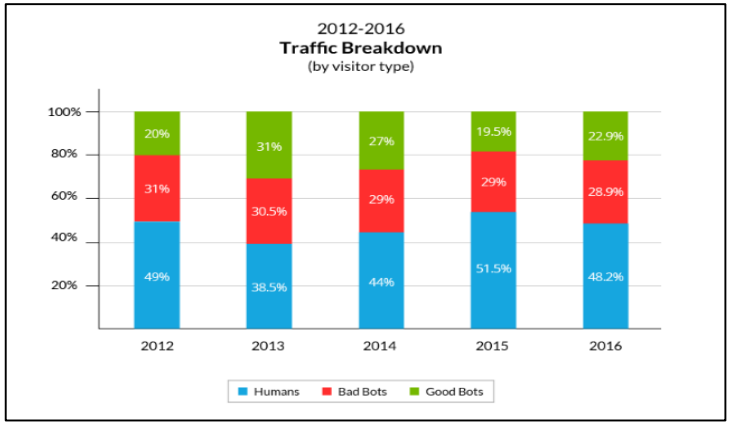


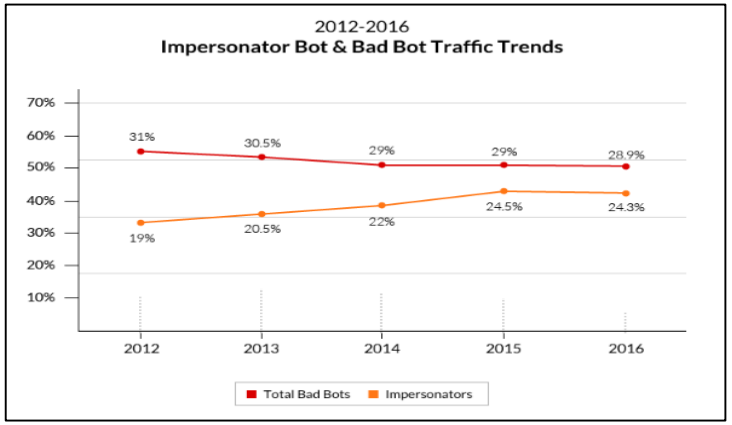
Akamai CI & NLTA 는 현존하는 최고의 보안위협DB 로서 귀사의 인프라 보안에 한층 더 깊이를 제공 할 수 있습니다.

# Akamai Bot Manager

# 자동화 된 Bot 의 의한 위협 증가



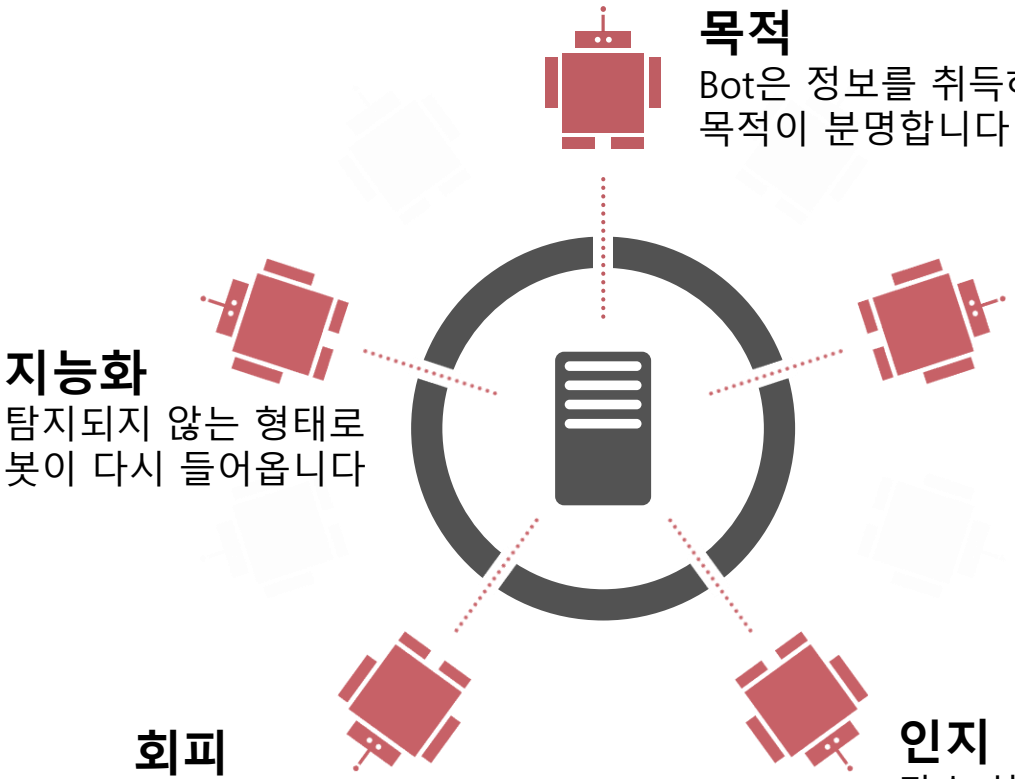

출처: Incapsula Bot Report 2016

일반적인 웹사이트에 대한 Bot 접속은 평균 50% 를 상회 하고 있으며 이중 28.9%가 악의적인 목적을 가지고 있습니다.

# 자동화 된 Bot 의 의한 위협 증가


자동화 된 악성 Bot 에 의한 공격은 우리의 일상 생활에서 느낄 수 있도록 증가 하고 있으며 위협이 점점 심각해 지고 있습니다.

# Akamai Bot Manager – 관리의 필요 필요성



**목적**
Bot은 정보를 취득하려는
목적이 분명합니다

**지능화**
탐지되지 않는 형태로
봇이 다시 들어옵니다

**차단**
정보 취득을 차단
해 봅니다

**회피**
봇 운영자는 탐지와 차단을
회피하기 위해 봇을
재프로그래밍 합니다

**인지**
단순 차단은 봇 운영자에게
차단 되었다 라는 것을
인지하게끔 합니다

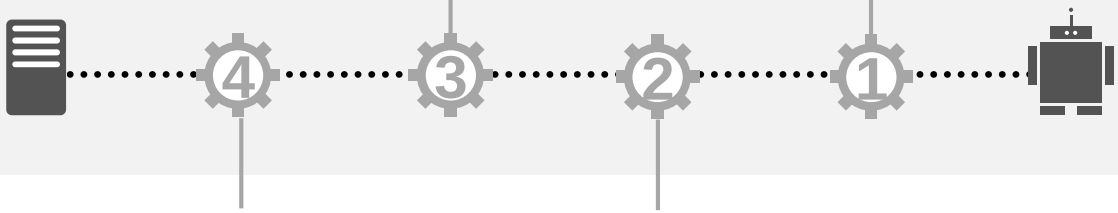
효과적인 봇 차단을 위해서는 봇 사용자가 원하는 정보를 탈취한 것으로 보이게 위장 하는 **봇 관리 능력**이 필요 합니다.

# Akamai Bot Manager – 관리의 방법

- 단순히 Block 하지 않고 Good 과 Bad Bot을 관리
- 비즈니스 영향도에 따라 Bot을 분류
- 전문적인 Bot 트래픽 관리
- Bot 트래픽을 모니터링하고 보고서 작성


✓ **Action**
- Basic (Monitor, Block)
- Drop
- Rate (Delay 1-3s, Slow 8-10s)
- Serve (다른 origin, 다른 content, 캐시)
- **조건에 따른 Action 적용**

✓ **Bot 트래픽 감지**
- 아카마이 카테고리 사용
- 고객 카테고리 설정 가능
- 실시간 감지 (형태, rate 분석)
- **브라우저 검증**

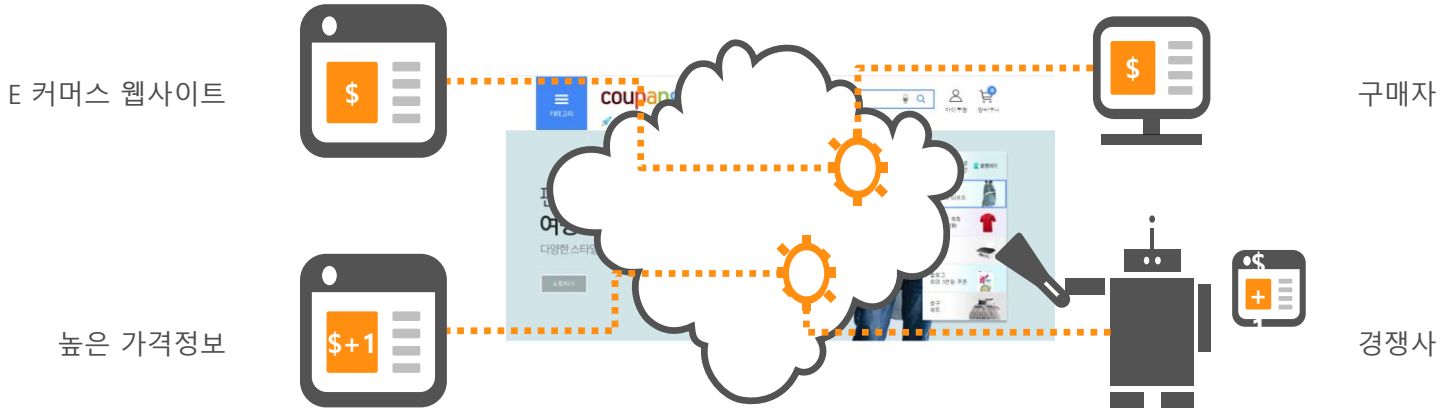



✓ **분석 및 Reporting**
- Security Center
- Bot Activity report
- Bot Analysis report

✓ **15개의 다른 카테고리로 분류**
- Akamai 카테고리는 계속 업데이트
  - Web search, SEO, Aggregator
  - RSS, Social, BI, Monitoring 등..
- 고객 카테고리는 Customizing 가능
- 실시간 감지하여 서로 다른 Action 수행

Akamai Bot Manager 는 봇 탐지, 분류, 관리, 리포트 등 봇 트래픽 관리를 위한 상세 기능을 제공 합니다.

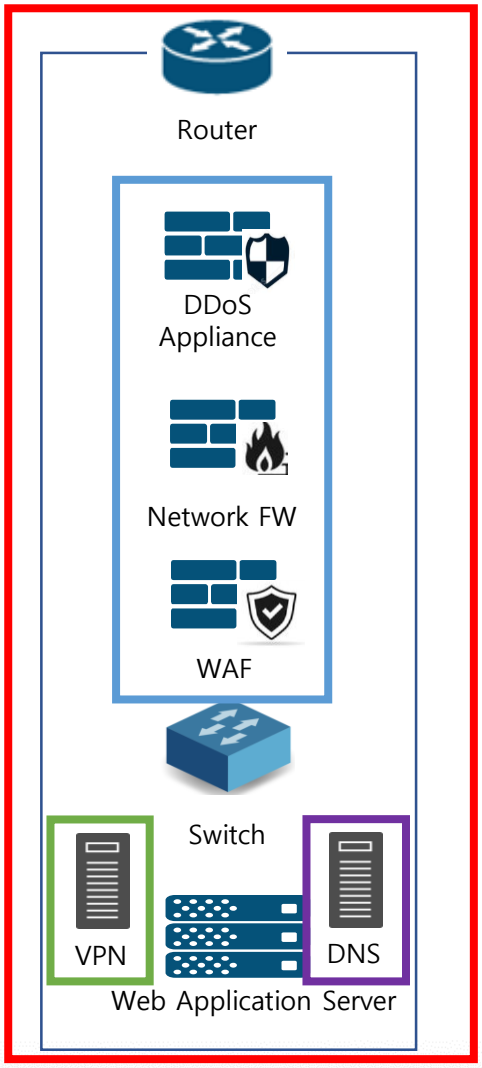
# Akamai Bot Manager – 관리의 예시


Akamai Bot manager 는 고객사의 서비스 형태나 미리 설정된 내용에 따라 여러가지 형태로 봇에 대한 응답을 관리 할 수 있습니다.

# Akamai Cloud Security

# Akamai Cloud Security 의 역할




## 아카마이 보안 솔루션

| | WEB Service | DATA Center | Enterprise |
|---|---|---|---|
| 서비스 가용성 확보 | **KSD(Kona Site Defender)**<br>웹서비스 보안을 위한 토탈 솔루션<br>네트워크 및 어플리케이션 공격을<br>CDN 인프라를 활용해 성능 및<br>안전성 보장 | **Prolexic Routed**<br>라우팅을 이용한 IP 우회 서비스로<br>대용량 DDoS 방어에 최적화된<br>솔루션 글로벌 7개<br>SC(Scrubbing Center)를<br>통한 분산 처리 | **ETP(Enterprise Threat Protection)**<br>기업내 사용자의 외부 사이트에<br>대한 DNS 요청을 확인 하여 Bot,<br>Malware 및 C&C 서버로의 접속<br>시도를 사전에 차단하는 DNS 보안<br>솔루션 |
| | **WAP(Web Application Protector)**<br>간소화 된 형태의 웹방어 솔루션<br>전문 보안 인력 확보가 어려운<br>중/소규모의 웹서비스 보안 강화 | | |
| 보안 강화 | **Bot Manager**<br>각종 자동화 된 Bot 으로 인한<br>보안 침해 및 사이트 성능 저하에<br>효율적으로 대응 할 수 있는 솔루션 | **Prolexic Connected**<br>라우팅을 이용한 IP 우회 서비스<br>Routed 서비스와 달리 전용선을<br>이용해 오리진과 통신 하며<br>Routed 서비스<br>트래픽 제한 해결 가능 | **EAA(Enterprise Application Access)**<br>사내 인프라에 대한 외부접속을<br>단순화 하여 보안을 강화한<br>Remote Access 지원 솔루션 |

FastDNS (글로벌 분산된 DNS 서비스로 기업의 DNS 인프라 확장 가능 100% 가용성 SLA)

전세계 137 개국, 3000+ PoP, 28만+ Edge Server 서비스 인프라

고객 내부 방어 시스템을 각각의 보안 솔루션을 이용해 성능 향상 및 대체 서비스를 제공 할 수 있습니다.

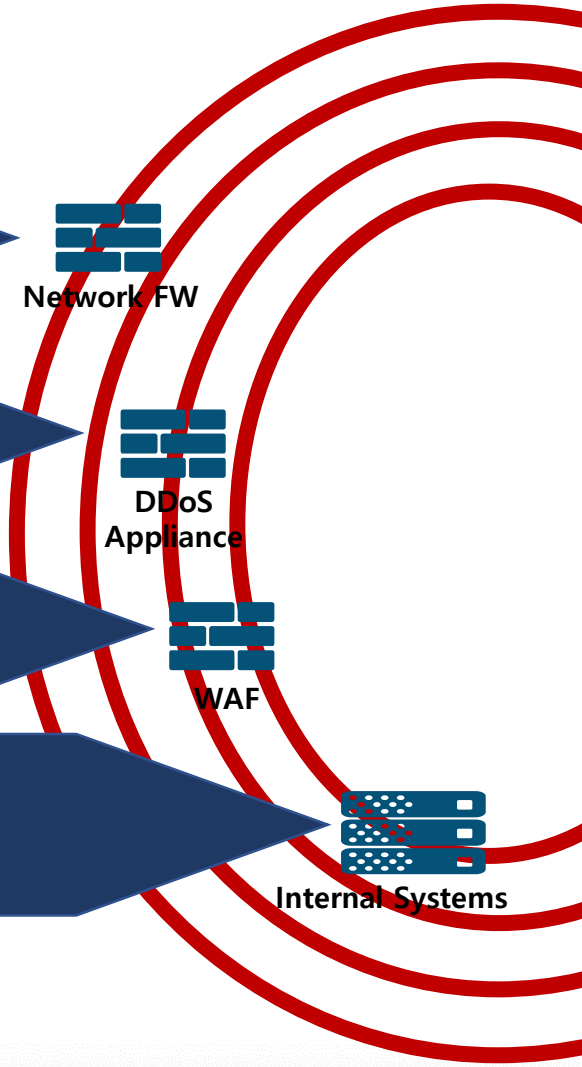
# Akamai Cloud Security 의 활용

Akamai CI & NLTA
- SIEM, ESM 에 융합 하여 관제 및 대응 강화
- Network 및 보안 장비에서 선재적으로 차단

Akamai WAF & Prolexic
- 강력한 Cloud WAF 로 웹에 대한 공격 방어
- BGP + GRE 서비스로 Data Center 공격 방어

Akamai Bot Manager
- 아카마이 봇 메니저로 봇 트래픽 관리
- 비정상 적인 봇 접속에 의한 보안 사고 예방

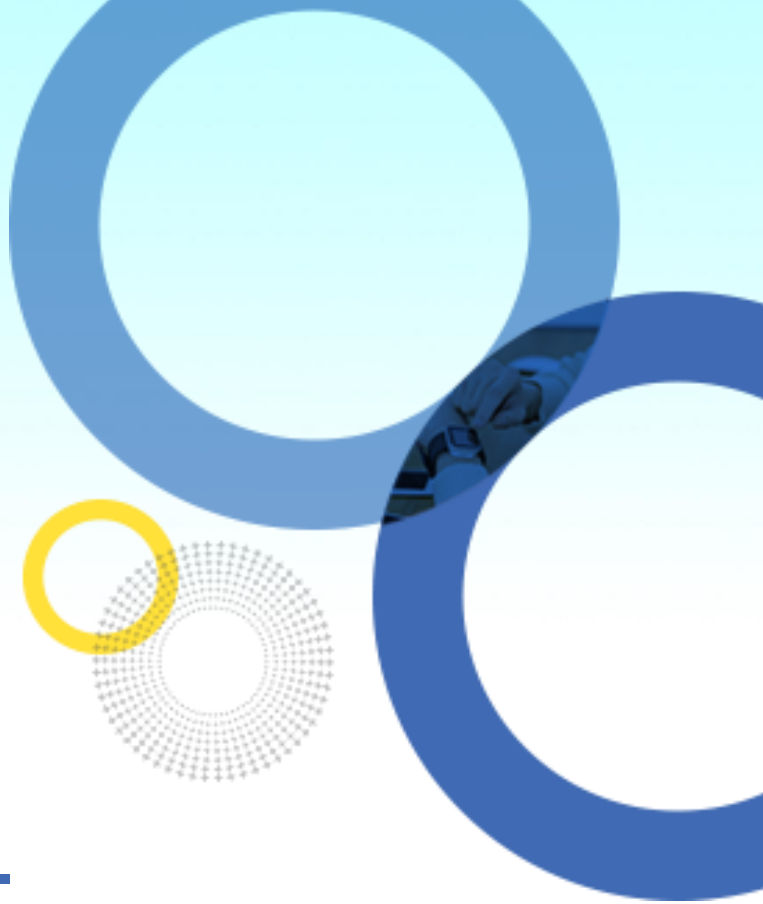
Akamai EAA + ETP
- EAA 를 통해 원격 접속에 대한 보안 제고
- ETP 를 통해 사내 보안 사고 예방 및 감시




아카마이 보안 솔루션을 활용 하여 선제적 위협 방어 체제 설립 및 내외부 보안 강화에 활용 가능

디지털 트랜스포메이션을 통한
비즈니스 혁신과 4차 산업혁명 대응을 위한

# GIT 솔루션즈 데이



감사합니다.

GiT 굿모닝아이텍(주)