클라우드 웹 서비스의 보호

IMPERVA INCAPSULA

2018. 9. 20

IMPERVA KOREA 김웅섭 이사



No.1 Cloud DDoS Mitigation Solution

INCAPSULA Web Site Protection

Agenda

I. **DDoS 공격 추이**

II. INCAPSULA 특징

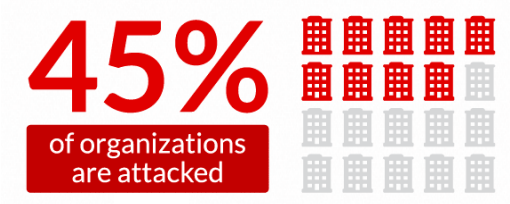
III. INCAPSULA 웹 보호

IV. 기능 비교 및 결언

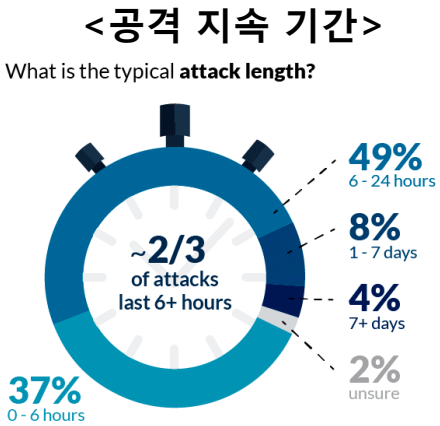
DDoS Attack Landscape

- 49%의 DDoS 공격은 6-24 시간 동안 지속됨
- 기업의 DDoS 공격 피해액은 시간당 4천만원
- 한번의 피해액은 고객 평균 대략 5억

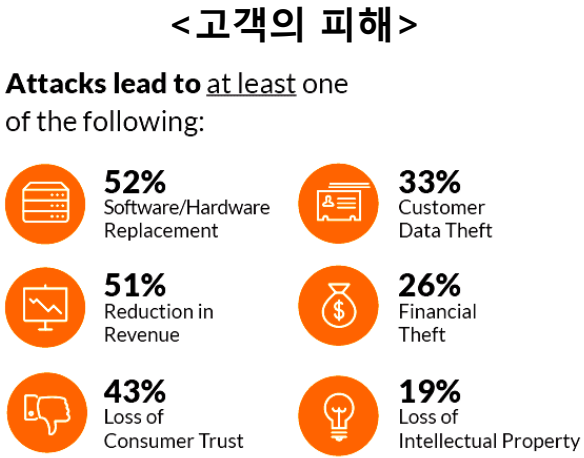
<DDoS 피해 기업>



<공격 지속 기간>



<고객의 피해>



<출처>
Global DDoS Threat Landscape Incapsula Report

Copyright © 2018 Samsung SDS All rights reserved

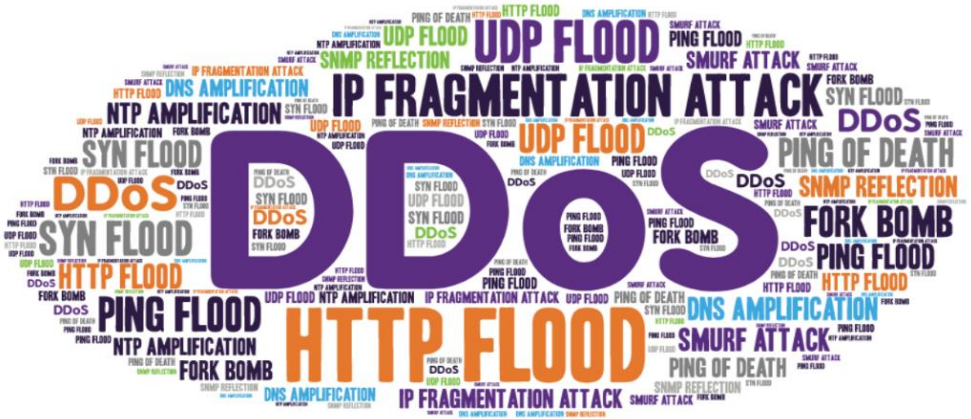
DDoS 공격 유형

다양한 유형(L3~L7) 및 큰 볼륨의 DDoS 공격이 발생되어 더 이상 On-Premise 장비로 방어 불가

Volumetric Attack

L4 Protocol Attack

Application Attack

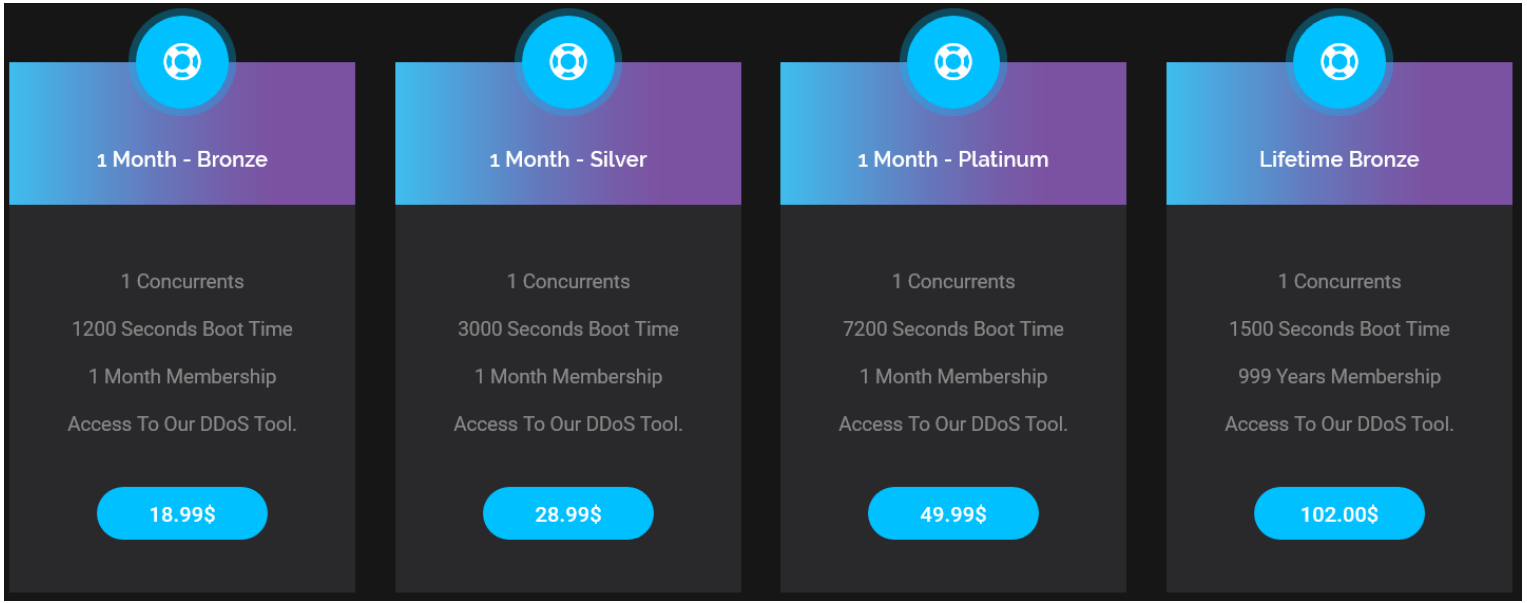


Copyright © 2018 Samsung SDS All rights reserved

DDoS Attack Evolution



DDoS As A Service – Web Stressor



Copyright © 2018 Samsung SDS All rights reserved

Definition of Cloud Scrubbing Solution

1. 고객 IP 센터에서 광고
2. BOT에 의한 공격 발생
3. 각 센터에서 공격 차단
4. 정상적인 트래픽만 전달



공격 진원지와 가까운 곳의 방어센터에서 공격을 차단하는 분산 방어 솔루션

Copyright © 2018 Samsung SDS All rights reserved

Agenda

I. DDoS 공격 추이

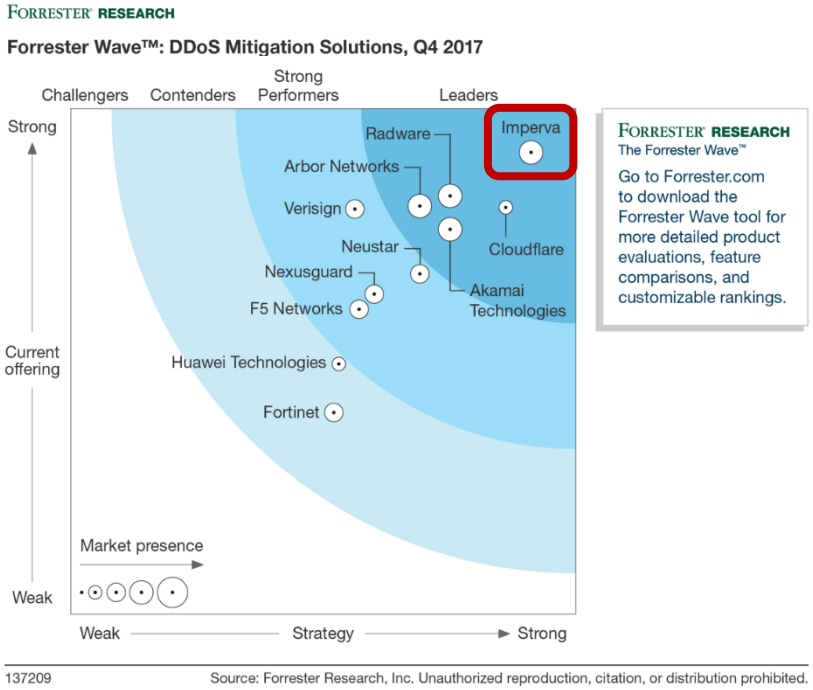
II. INCAPSULA 특징

III. INCAPSULA 웹 보호

IV. 기능 비교 및 결언

외부기관 평가

Forrest Wave DDoS Mitigation Solution 및 Gartner MQ WAF 분야 Leader



<Forrester Wave™ 2017 Q4>



<Gartner Magic Quadrant August 2018>

Copyright © 2018 Samsung SDS All rights reserved

SLA

DDoS Mitigation 솔루션 업체 중, 가장 빠른 SLA (가용성 및 빠른 차단 능력) 제공

99.99%

Uptime

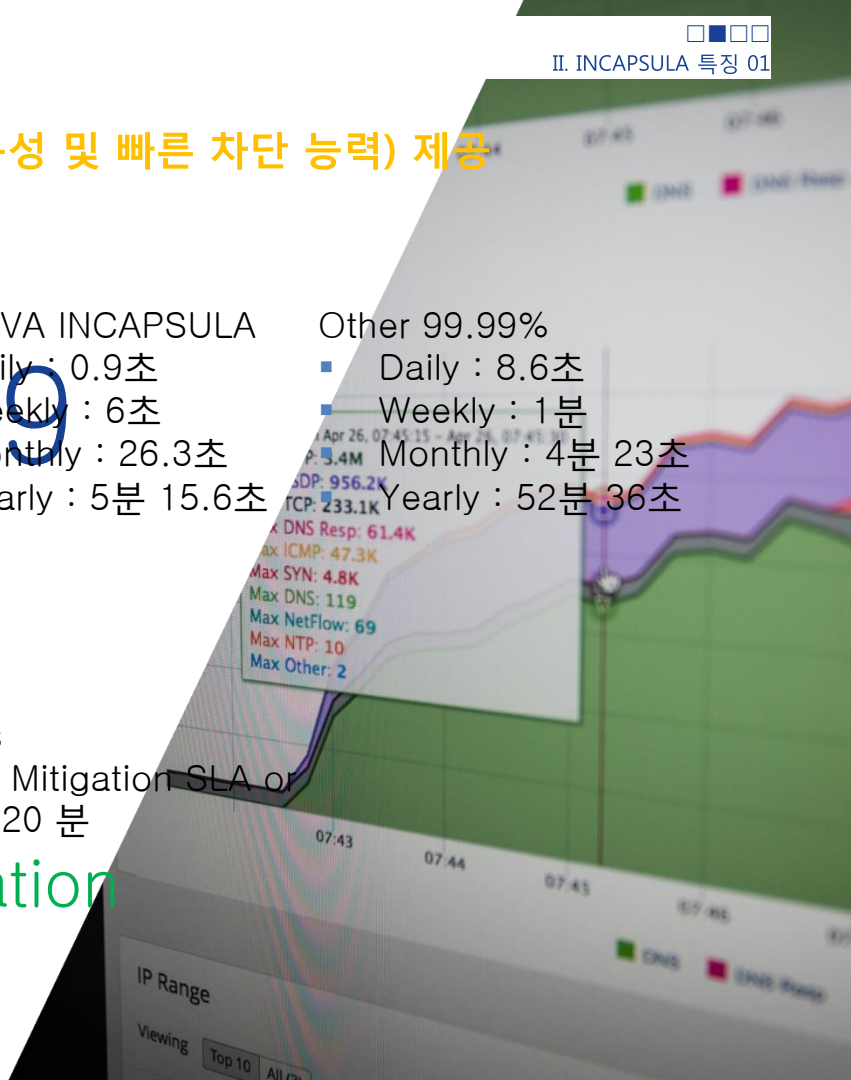
IMPERVA INCAPSULA
- Daily : 0.9초
- Weekly : 6초
- Monthly : 26.3초
- Yearly : 5분 15.6초

Other 99.99%
- Daily : 8.6초
- Weekly : 1분
- Monthly : 4분 23초
- Yearly : 52분 36초

10초

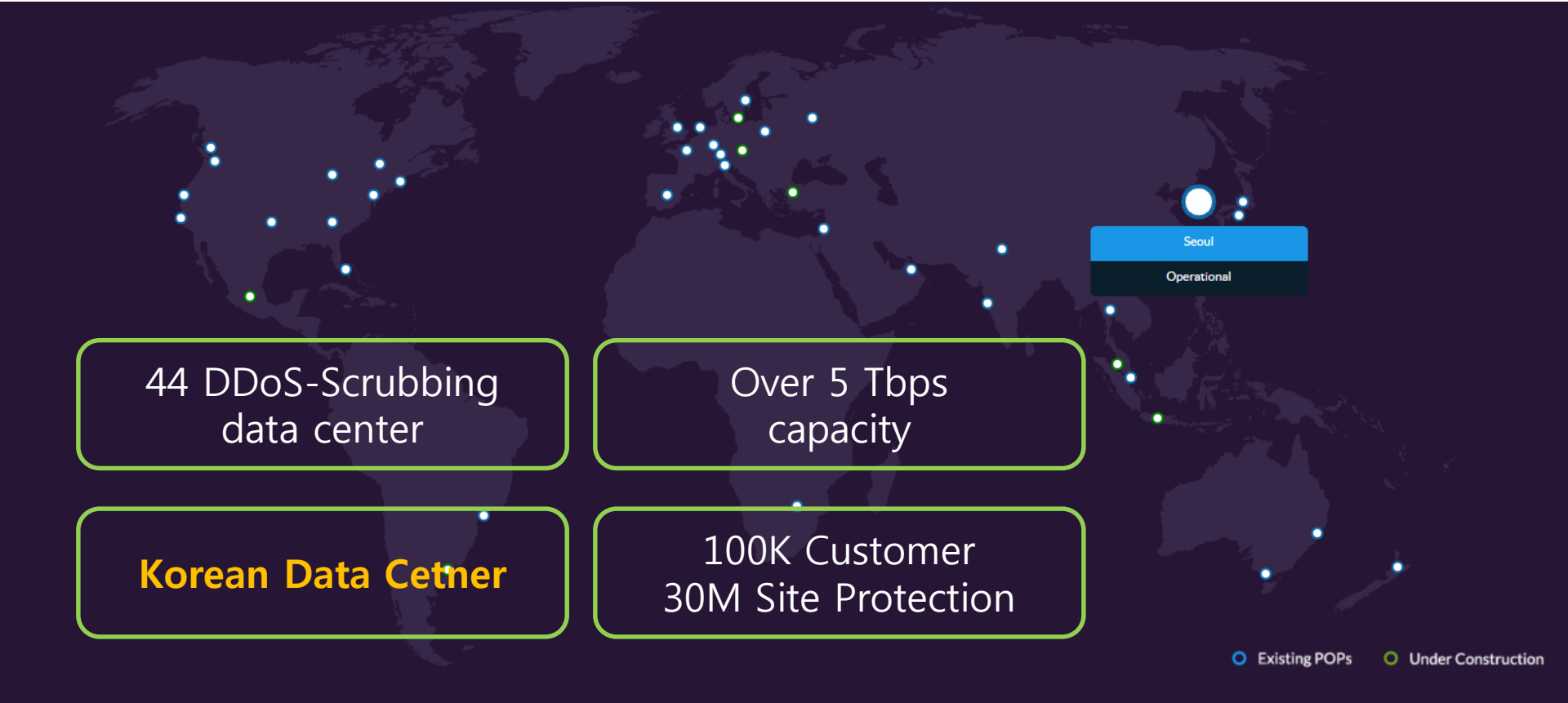
Time to Mitigation

Others
- No Mitigation SLA or
- 5~20 분



Global Data Center 및 높은 방어 용량

전세계 44개의 Scrubbing Center 운영 및 5Tbps의 방어 용량 제공



보안에 최적화된 설계

DDoS 및 웹 사이트 방어 중심의 솔루션 디자인





자체 개발 솔루션

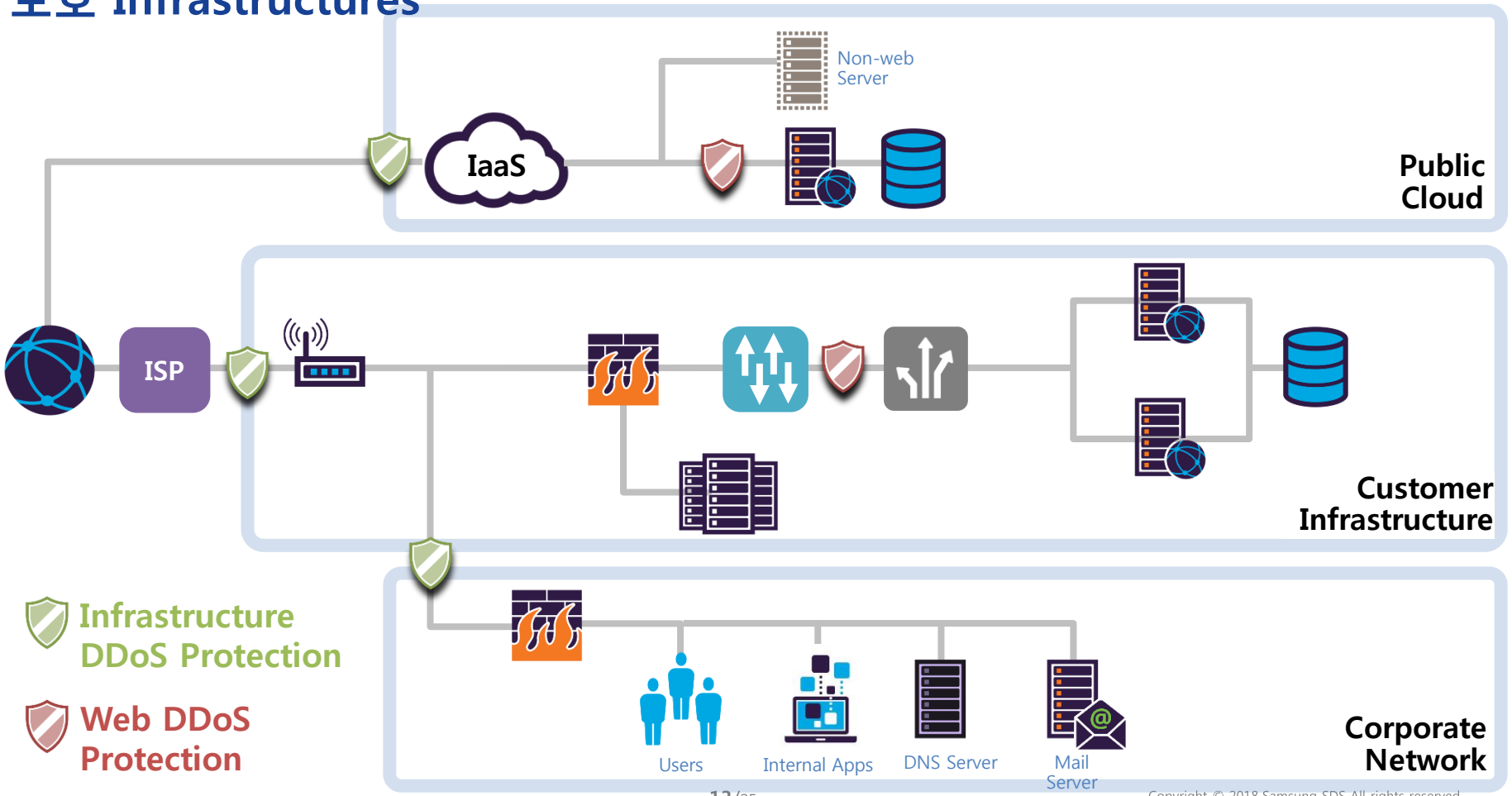
- 모든 프로토콜에 대해 L3 ~ L7의 모든 공격 방어
- 자동 방어 (사용자 개입 없음)
- 빠른 보안 업데이트
- 빠른 Mitigation 시간
- 개인정보 보호
- 비 표준 HTTP 지원

다양한 서비스 제공

- Infrastructure 보호
- Always-on & On-demand 제공
- Web Application 보호
- Gartner #1 웹 방화벽
- 로드 분산
- 사용자 체감 속도 향상

Copyright © 2018 Samsung SDS All rights reserved

보호 Infrastructures



Copyright © 2018 Samsung SDS All rights reserved

Agenda

I. DDoS 공격 추이

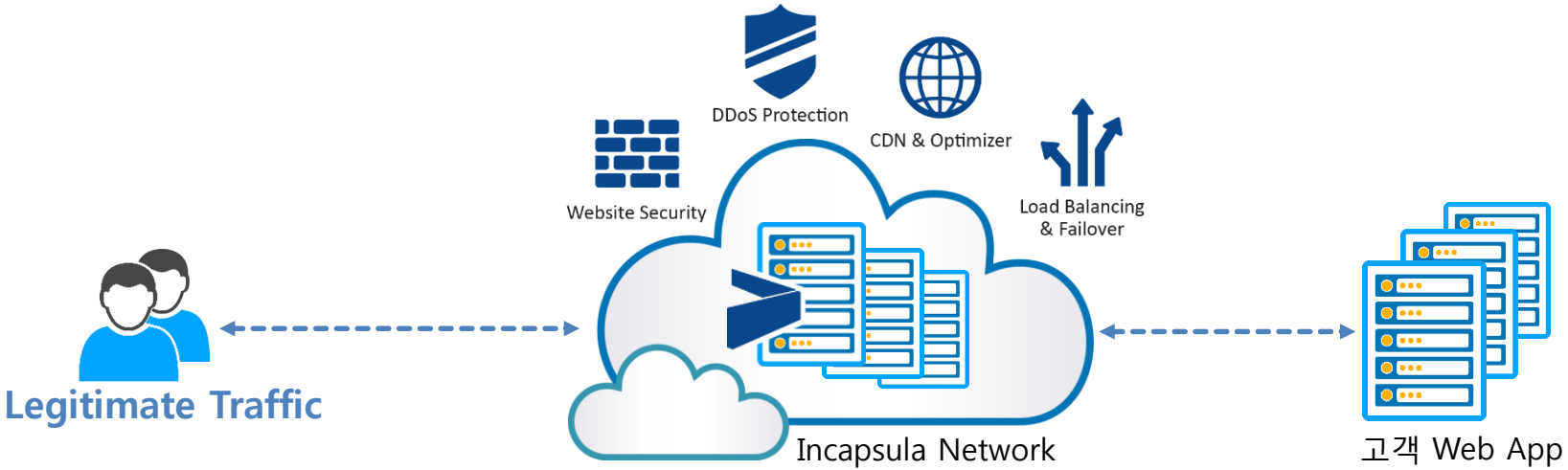
II. INCAPSULA 특징

III. INCAPSULA 웹 보호

IV. 기능 비교 및 결언

웹 어플리케이션 보호

간단한 DNS CNAME 변경을 통한 웹 어플리케이션 보안 및 성능 향상 제공



- 웹방화벽
- L3 ~ L7 DDoS Protection
- Bot mitigation
- Reputation Intelligence 제공
- CDN / Optimizer 제공

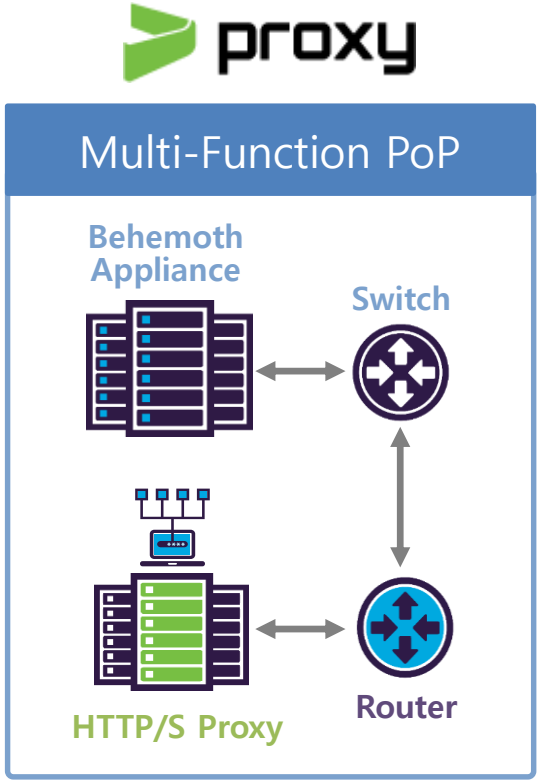
- 차단 모드로 운영됨 (Low FP)
- 사용자의 설정이 필요 없음
- 웹사이트 개수 및 Bandwidth의 옵션 제공
- DNS Protection 기본 제공 (10 Zone)

Copyright © 2018 Samsung SDS All rights reserved

웹 어플리케이션 보호

Industry Leading WAF Technology 및 업계 최고 Intelligence 제공

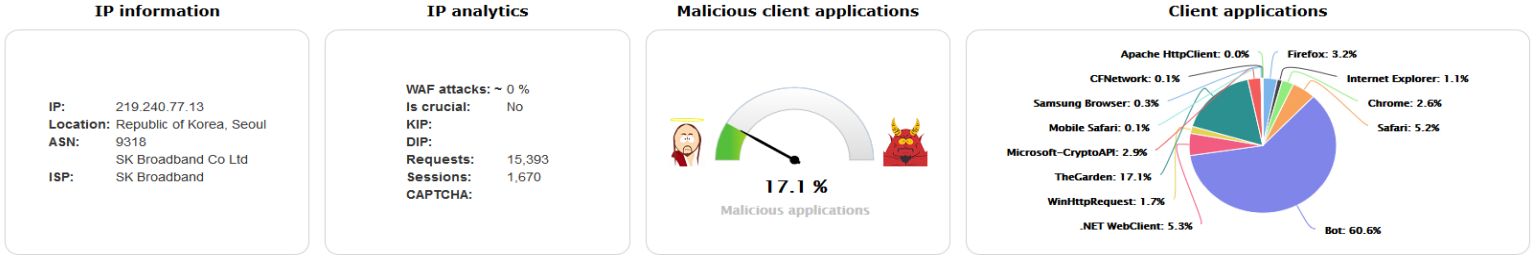
- **Web Application 방화벽**
  - Request / Response 동시 검사
  - 액세스 통제 (국가 / Reputation IP / Region / Black list)
  - Bot Mitigation / OWASP Top 10 / Hacking
  - Detail Custom Rules – Application 공격 차단
  - 백도어 탐지 및 차단 / Two Factor 인증
  - 비 표준 HTTP 지원 (In-House Application)
- **웹 옵티마이저**
  - Caches static/dynamic content
  - Optimizes content (압축, 변형, ...)
- **로드밸런서 (Data Centers / Servers)**
  - Application delivery rules
  - Manage fail-over



Copyright © 2018 Samsung SDS All rights reserved

Best Intelligence

16년의 웹방화벽 기술 Knowhow의 정교한 Intelligence 기반의 탐지 및 방어



Copyright © 2018 Samsung SDS All rights reserved

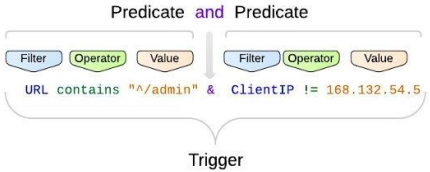
사용자 정의 정책

IncapRules 를 통한 비니지스 로직 공격 및 테크니컬 공격 탐지 및 방어

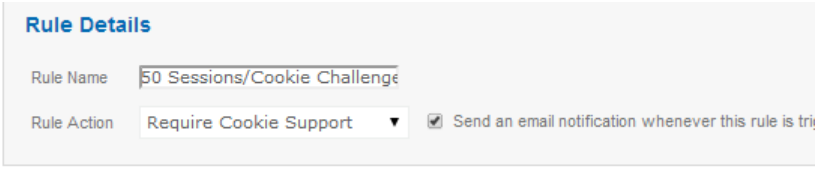


- 사용자 정의 정책 생성 기능 제공
  - HTTP 요청 Method
  - 헤더 값
  - URL 파라미터
  - 클라이언트 타입 (e.g., Browser, Search Engine,etc.)
  - IPs / Geo-locations
  - 세션 / IP 의 요청 횟수
  - Cookie / JavaScript 지원 여부
  - 500여 가지의 탐지 시그니처 (e.g., GoogleAds, CroneTask, WordPress bots, etc.)

- IncapRules기본 - 필터/트리거/Action



- 정책 생성 화면

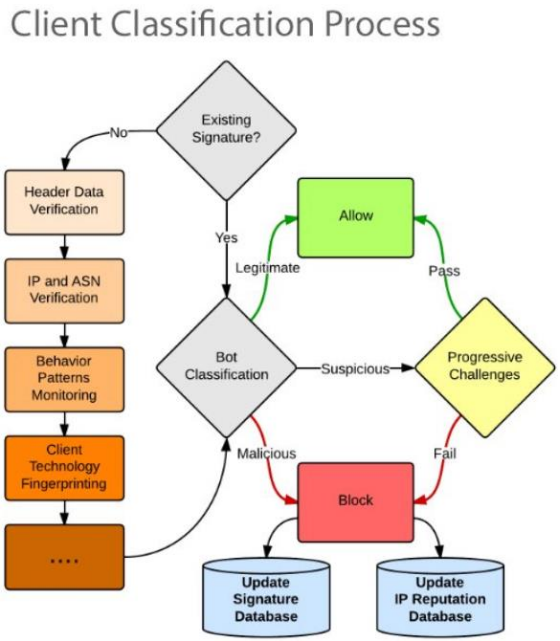




Copyright © 2018 Samsung SDS All rights reserved

BOT Protection

800여개의 BoT Database로 고객 웹 어플리케이션 보호



2 Jun 2018 07:12:48	Safari from United States	52.41.211.72 | 1 hits | HTTP/1.1 **Entry Page:** / (GET) **User Agent:** Magic Browser **Served Via:** Tokyo, Japan **Session Id:** 407001890042125103 DDoS Actions Less

URL: / (GET)
Status: Client was sent a JavaScript security check, request was suspended
Incident ID: 407001890042125103-128235813540924377
DDoS (Request suspended)

Add to whitelist

JS Test DDoS

2 Jun 2018 06:15:15	Bot (Unclassified) from United States	104.238.248.15 | 2 page views | 3 hits | Supports Cookies | HTTP/1.1 **Entry Page:** / (GET) **User Agent:** Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.0) **Served Via:** Los Angeles, CA **Session Id:** 224001420035045400 DDoS Actions Less

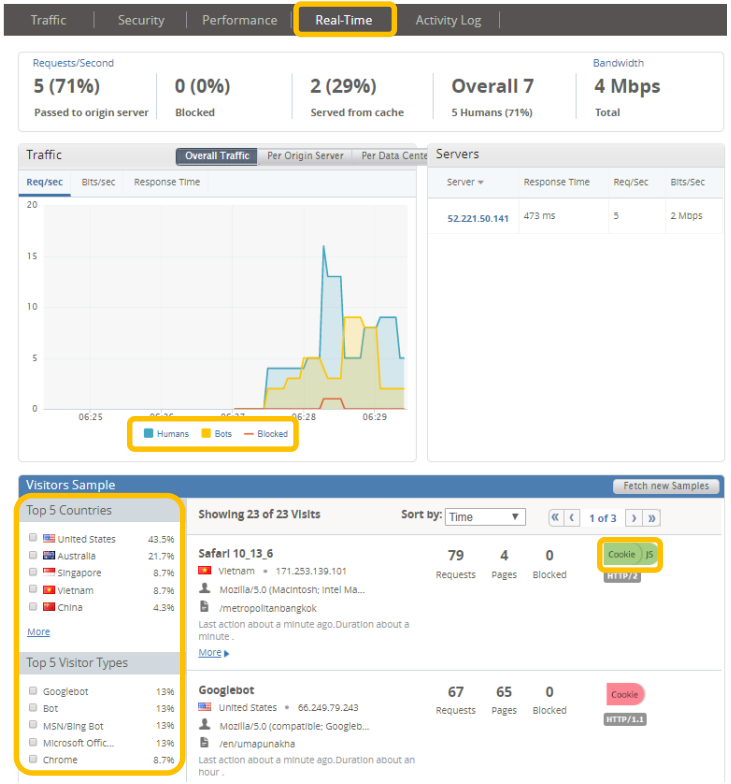
URL: / (GET)
Status: Client was sent a Cookie security check, request was suspended
Incident ID: 224001420035045400-45359961376557283
DDoS (Request suspended)

Add to whitelist

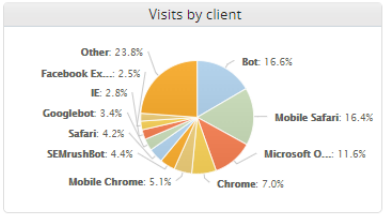
DDoS Cookie Test

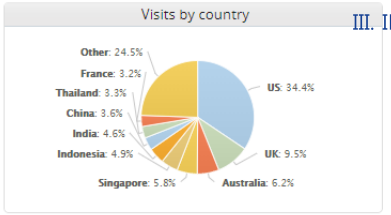
Copyright © 2018 Samsung SDS All rights reserved

Web Protection Dashboard

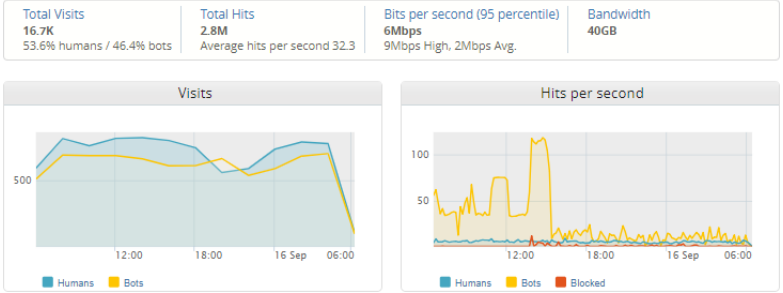


<실시간 Dashboard>

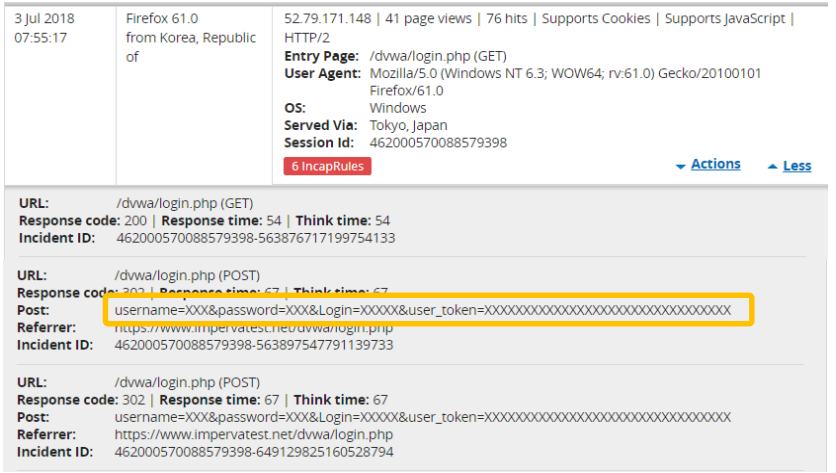




<각종 통계>



<탐지로그>



Agenda

I. DDoS 공격 추이

II. INCAPSULA 특징

III. INCAPSULA 웹 보호

IV. 기능 비교 및 결언

INCAPSULA Web Site Protection 기능 비교

기능	INCAPSULA	경쟁사
OWASP TOP 10	기본 제공	기본 제공
보안 및 안정성	Gartner 평가 1위 웹 방화벽 기술	오픈 소스인 Mod_Security를 사용, 다양한 reverse 해킹 기법 존재
데이터센터 규모	44개 스크러빙 센터 / 5Tbps / 한국 센터 운영	7개 스크러빙 센터 / 3.2Tbps / 한국 센터 없음
DNS DDoS 보호	기본 제공	추가 Product인 Fast DNS 구매
Bot Protection	기본 제공	추가 Product인 Bot Manager 구매 해야함
Backdoor Shell Protection	기본 제공	기능 없음
룰 설정 동기화 시간	5초 이내(자체 솔루션으로 빠른 동기화 제공)	45분
CDN 및 압축	기본 제공	기본 제공
리얼타임 Dashboard	O	15분 단위
오탐률	0.01%, 차단 모드로 운영	오픈 소스 기반으로 오탐률 심함, 탐지모드로 운영
신규 룰, 패치 배포	Sandbox 기반 실제 모든 사이트 대상으로 오탐 유무 확인 후 배포	3rd party인 Trustwave에서 룰 관리하여, 실제 트래픽 및 사이트에 대한 사전 테스트 불가능

Copyright © 2018 Samsung SDS All rights reserved

INCAPSULA 이용 고객

TRUSTED BY OVER 3 MILLION WEBSITES



Copyright © 2018 Samsung SDS All rights reserved

Why Incapsula

- DDoS 전용 솔루션
- 탐지부터 방어까지의 시간이 짧고 명확한 SLA 제공
- 최대 규모의 DDoS Scrubbing Center (44개 / 5Tbps)
- 한국 데이터 센터 운영
- 빠른 Latency 및 사용자 체감 속도 제공
- 개인정보 비 식별화 처리
- 비 표준 HTTP 지원하여 서비스 영향 전무

