imperva

WAAP – 간단하게, 유연하게, 강력하게

(Web Application & API Protection)

eGISEC 2023

Agenda

1. **Gartner는 왜 WAF를 WAAP으로 대체하였는가?**
2. 간단하게, 유연하게 – WAAP는 어떻게 동작하며, 무엇을 할 수 있는가?
3. 간단하게, 유연하게, 강력하게 – IMPERVA WAAP

Gartner는 왜 **WAF**를 **WAAP**로 대체하였는가**?**

Gartner WAF MQ Report

2014 ~2018

Gartner MQ WAF 2014

Gartner MQ WAF 2015

Gartner MQ WAF 2017

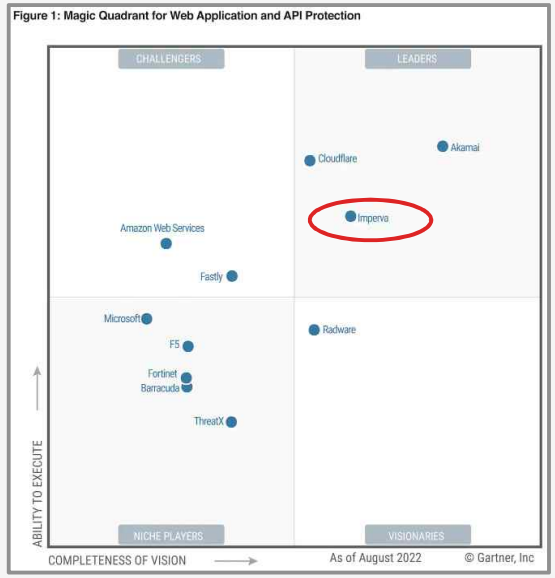
Gartner MQ WAF 2018

Gartner MQ WAAP 2019

Gartner MQ WAAP 2020

Gartner MQ WAAP 2021

Gartner MQ WAAP 2022

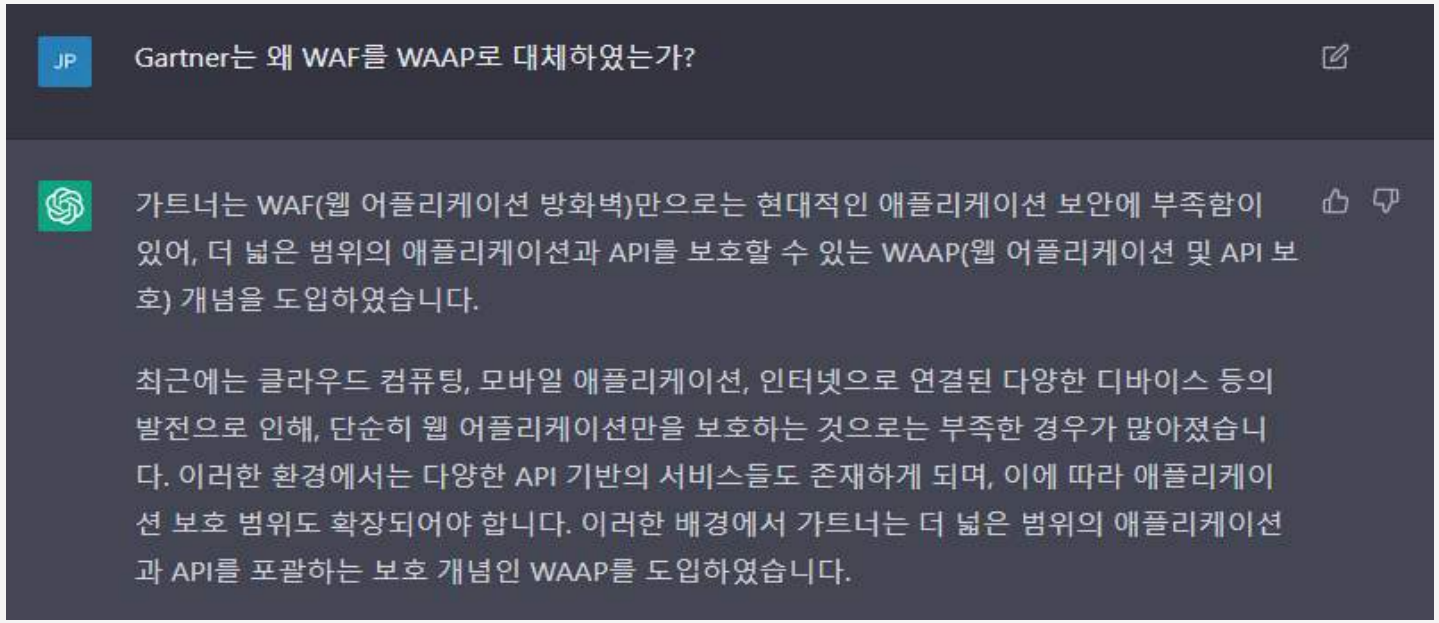


Gartner WAAP MQ Report

2019 ~2022

Gartner는 왜 WAF를 WAAP로 대체하였는가?

Gartner는 왜 WAF를 WAAP로 대체하였는가? – Chat GPT에 질문하여 보았습니다.



WAAP (Web Application & API Protection)

WAAP는 애플리케이션을 보호하기 위하여 필요한 웹방화벽을 비롯한 4가지 핵심 기능을 서비스 형태로 제공합니다.

Gartner

WAAP 4 Core Features (Gartner는 아래의 4가지 기능을 WAAP의 핵심 기능으로 정의 합니다.)

- WAF(Web Application Firewall)
- DDoS(Distributed Denial-of-Service) Protection
- Bot Management
- API Protection

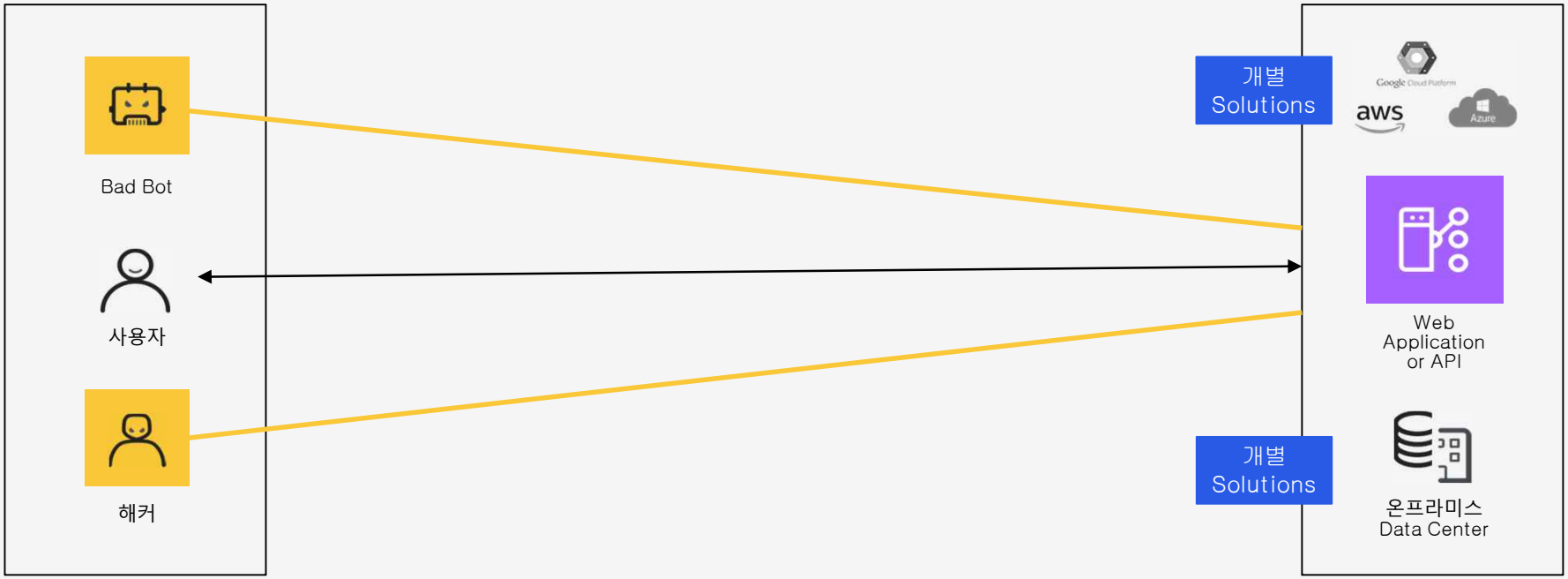
Garter가 생각하는
다양한 위치에 존재하는, 다양한 서비스를 제공하는, 다양한 기술을 사용하는 애플리케이션을 보호하기 위하여 필수적이라고 생각하는 기능

간단하게, 유연하게

- WAAP는 어떻게 동작하며, 무엇을 할 수 있는가**?**

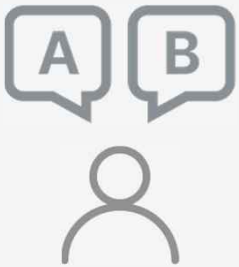
Before – 모든 위치에 개별 솔루션를 설치하는 운영

Application이 운영되는 모든 위치에 WAF, DDoS 등 개별 보안 제품 들이 별도로 설치되어 운영 됨



Before – 모든 위치에 개별 솔루션를 설치하는 운영

Application을 문제없이 안전하게 운영한 다는 것은 대부분의 기업들에게 그렇게 간단하지 않습니다.



Too many

관리 업체

Too many

모니터링 할 보안 도구

Too many

검토할 알림

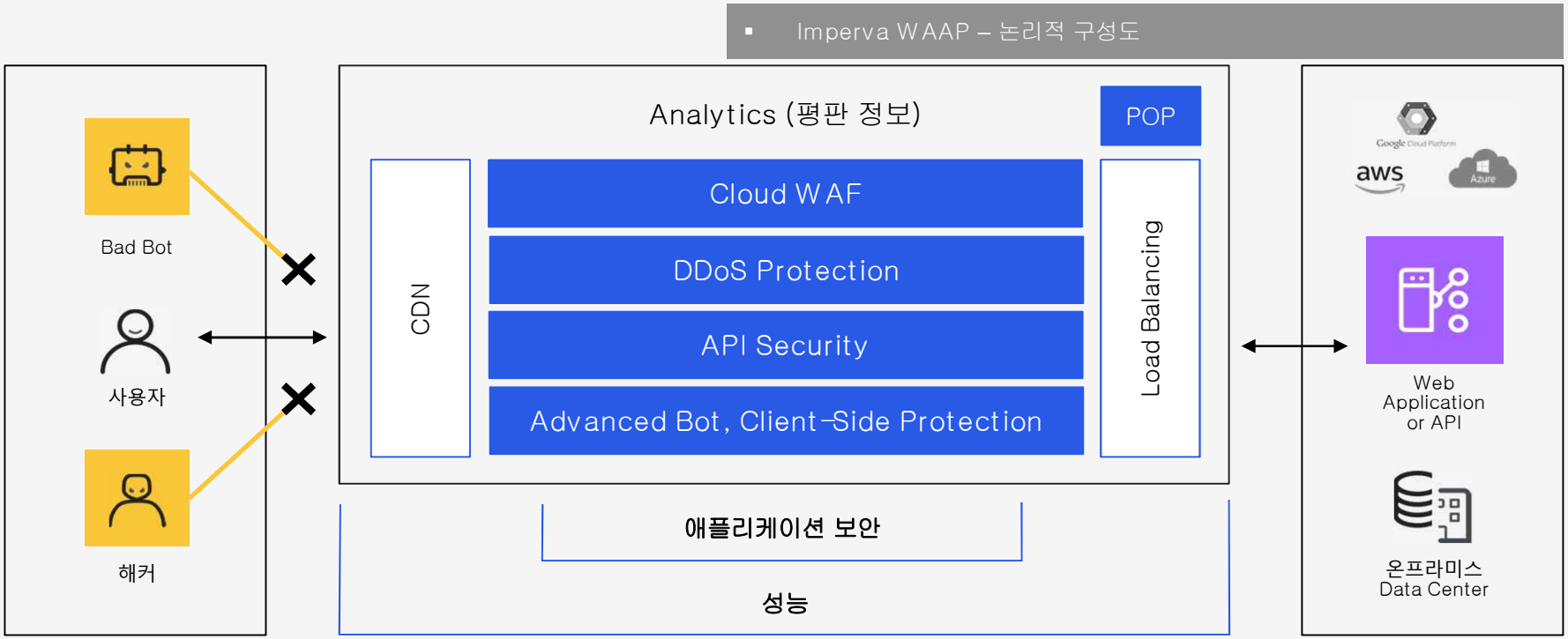
Too few

계속해서 더 많은 것을 요구

간단하고, 유연하고, 강력한 무언가 필요

After – WAAP를 통한 통합운영

다양한 환경에서 운영중인 Application 들을 WAAP를 통하여 통합 운영



After – WAAP를 통한 통합운영

전세계에 구축된 WAAP POP에서 유해한 트래픽을 차단하고 정상적인 Traffic만 통신을 허용

Global WAAP POP

사용자

Google Cloud Platform

aws

Azure

Web Application or API

온프레미스 Data Center

- Imperva의 경우 전세계에 51+ 이상의 WAAP 전용 POP를 운영하고 있습니다.

간단하게, 유연하게, 강력하게

- **IMPERVA WAAP**

Imperva WAAP 도입사례 – A사

WAAP 서비스 도입을 검토하던 A업체는 아래와 같이
제품의 기술력 및 서비스 품질, 글로벌 인프라(POP 등) 등을 종합적으로 고려하여 최종적으로 Imperva WAAP 서비스 도입을 결정하였습니다.

WAAP 사용 검토

- Multi Cloud 및 Hybrid Cloud 사용 계획
- 운영 효율성 / 확장성 / TCO 검토
- WAAP 사용 결정

WAAP 서비스 제공 업체 조사

- HW WAF만 제공하는 기업 / WAAP를 제공하지만 HW HWF 비중이 높은 기업 제외
- HW WAF 제품 없이 WAAP 서비스을 제공하는 기업 (A사, C사, G사 등) 검토
- HW WAF 경험이 있으면서 WAAP 서비스 비중이 높은 기업 (Imperva, B사, F사 등) 검토

WAAP 서비스 업체 평가

- Gartner 등 해외 시장 조사 업체들의 평가 검토
- Globel Infra 검토 (POP, 한국내 POP 보유 등)
- POC 수행

imperva

Imperva WAAP 도입사례 – B사

WAAP 서비스 도입을 검토하던 B업체는 아래와 같이
제품의 기술력 및 서비스 품질, 글로벌 인프라(POP 등) 등을 종합적으로 고려하여 최종적으로 Imperva WAAP 서비스 도입을 결정하였습니다.

WAAP 사용 검토

- Multi Cloud 및 Hybrid Cloud 사용 계획
- 운영 효율성 / 확장성 / TCO 검토
- WAAP 사용 결정

WAAP 서비스 제공 업체 조사

- Gartner MQ 리더 그룹에 있는 업체들을 대상으로 설명회 진행

WAAP 서비스 업체 평가

- POC 수행 (간단한가? 유연한가? 강력한가?)
- 서비스 종류 및 가격의 합리성 검토

imperva

WAF(Web Application Firewall) 기능

2014년 부터 2022년 까지 Gartner WAF, WAAP 리포트에서 연속으로 Leader로 선정된 업체는 Imperva가 유일 합니다.

WAF(Web Application Firewall) 기능

Imperva WAAP 서비스가 제공하는 WAF 기능은 아래와 같이 다계층 방어 구조를 가지고 있습니다.

다계층 방어 구조

접근 통제
Blacklist IP 등록, 국가별 차단

Bot 차단
자동화 공격, **Bad Bot, Scraper, Spammer** 차단

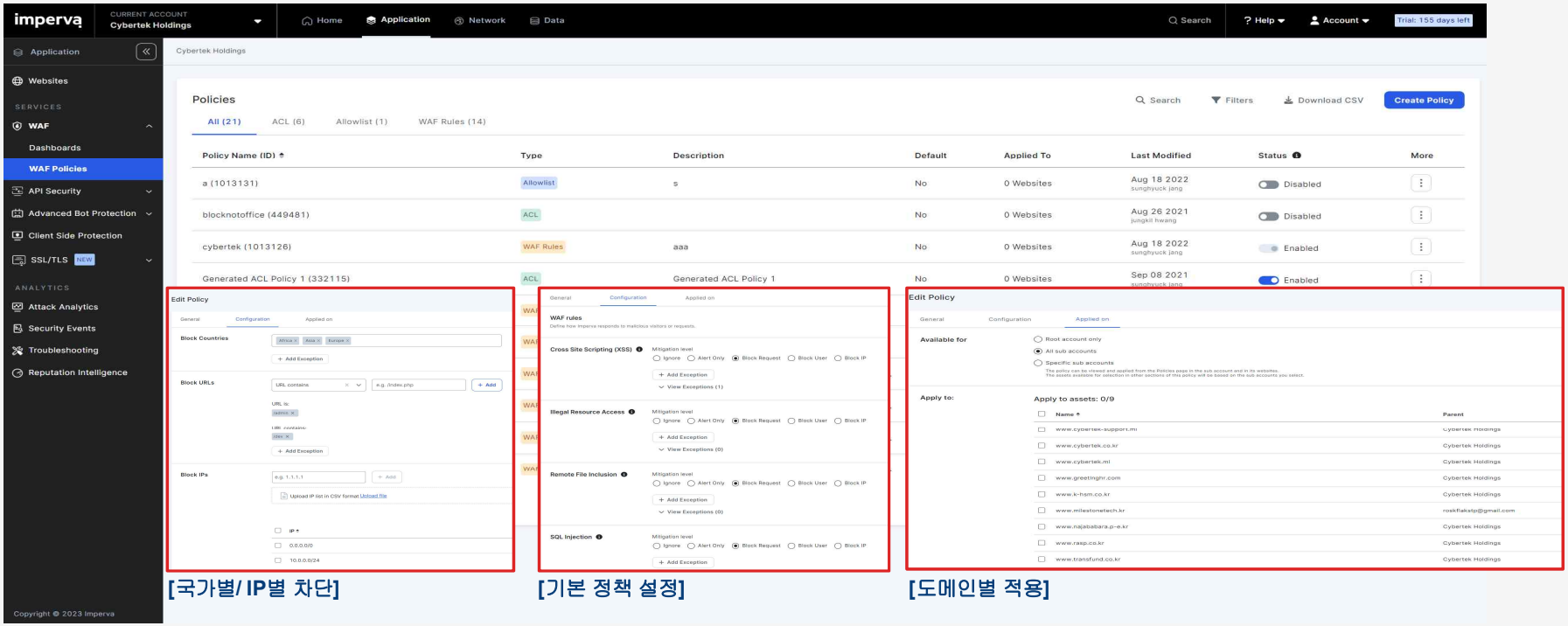
WAF
해킹 공격 차단
OWASP 상위 **10**개 공격**(SQLi, XSS** 등**)**

사용자 정의 정책
애플리케이션 공격 차단

WAF(Web Application Firewall) 기능

오랜 경험 및 기술력으로 바탕으로 관리자의 업무를 최소화할 수 있는 단순하고 직관적인 UI를 제공합니다.

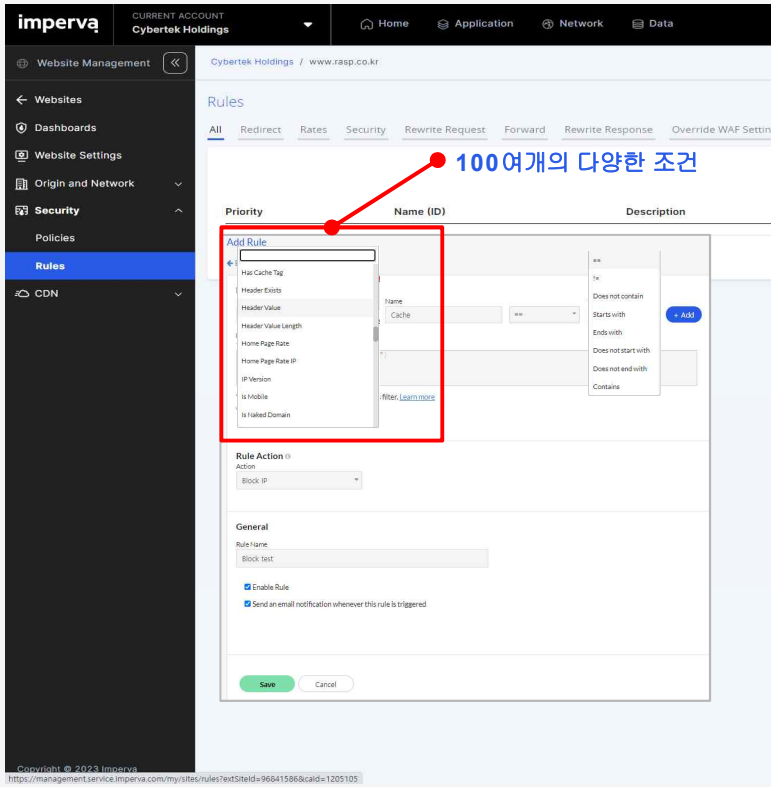
단순하고 직관적인 UI



[국가별/ IP별 차단] [기본 정책 설정] [도메인별 적용]

WAF(Web Application Firewall) 기능

사용자가 세부적인 Rule을 설정할 수 있는 Custom Rule 기능을 제공합니다.

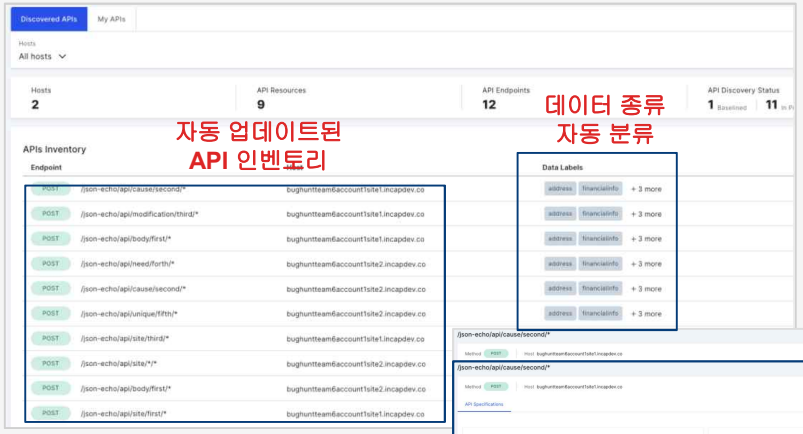


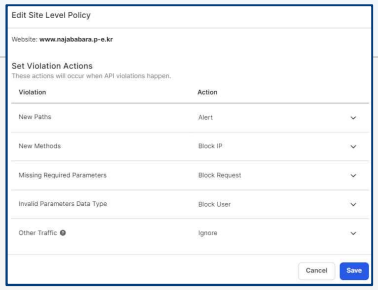
- 사용자 정의 정책 생성 기능 제공
  (100여개의 다양한 조건을 이용하여 제어 정책 작성)

  - HTTP 요청 Method
  - 헤더 값
  - URL 파라미터
  - 클라이언트 타입 (e.g., Browser, Search Engine, Feed Fetched, etc.)
  - IPs / Geo-locations
  - 세션 레벨과 IP의 요청 횟수
  - Cookie / JavaScript 지원 여부
  - 500여 가지의 탐지 시그니처
    (e.g., GoogleAds, CroneTask, WordPress bots, etc.)

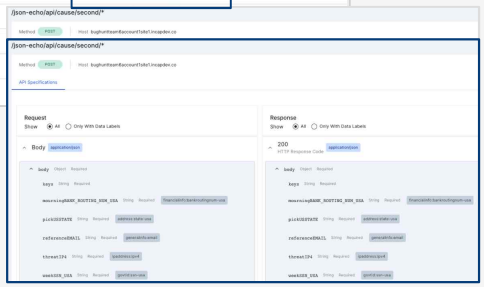
API Security 기능

Imperva WAAP 서비스는 기본적인 API 보안 기능을 제공하고 있으며, 지원 범위를 확대하고 있습니다.





기존 웹방화벽용 정책+API 전용 보안 정책 적용

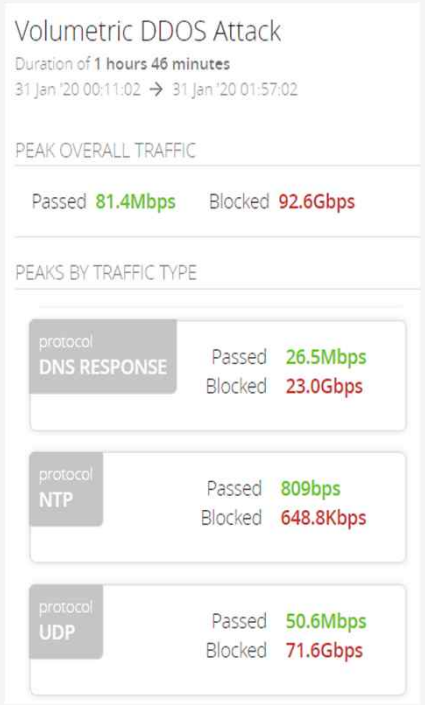


API 스키마 종류
자동 학습

DDoS 방어 기능 - 특장점

Imperva WAAP DDoS 방어 – 높은 가시성

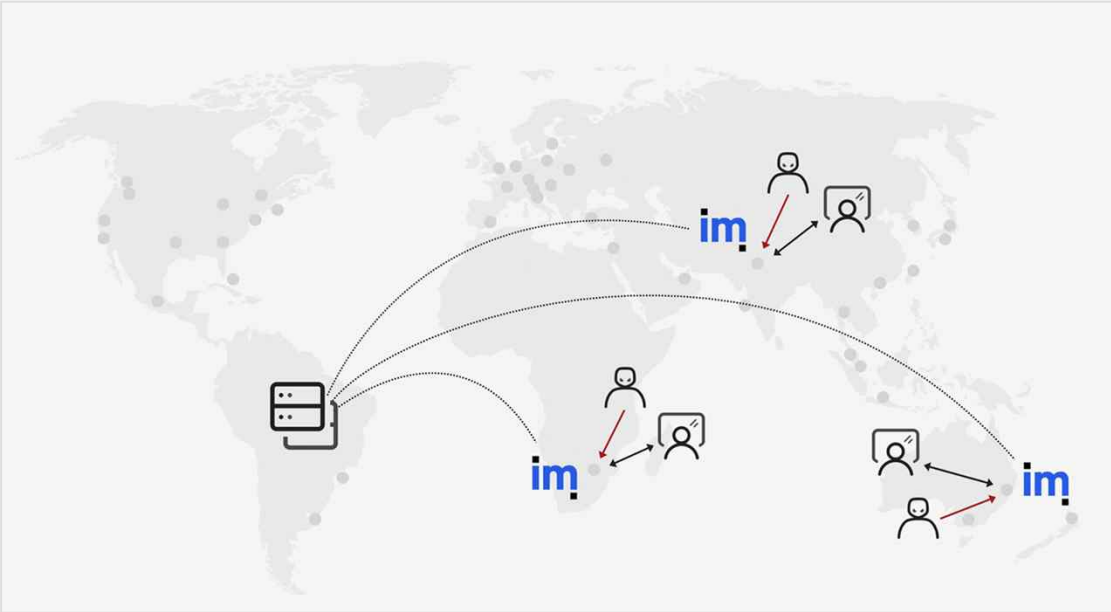
정확한 탐지 능력	빠른 속도 및 차단	사용의 편의성	높은 가시성
▪ 싱글 스택 (L3~L7 보호) ▪ 심층 검사 및 보호 ▪ 임퍼바 위협 평판 인텔리전트 ▪ 공격량과 상관 없이 Unlimited 방어 제공	▪ 국내 PoP ▪ 3초 완화 SLA ▪ SD-NOC/SOC (99.999% SLA) ▪ 고급 에지 라우팅 ▪ 글로벌 메시 구성	▪ 모든 보안 서비스를 통합 관리할 수 있는 콘솔 ▪ 사전에 설정 된 보안 룰셋 제공 ▪ 관리형 정책 제공	▪ 실시간 콘솔 및 즉각적인 알림 제공 ▪ 네트워크 트래픽 및 어플리케이션 분석 제공 ▪ L3~L7까지 상관분석 (Attack Analytics) ▪ SIEM 연동



위장 전술로 사용되는 **DDoS** 공격 방어 중에도 실제 최종 목표 및 공격을 세부적으로 파악 가능

DDoS 방어 기능 – Imperva DDoS 대응 Infra

전세계 51+ DDoS 대응 POP를 통하여 공격자와 가장 가까운 곳에서 3초이내에 신속하게 대응



3초 DDoS 완화 SLA (밴드 계약 필요)

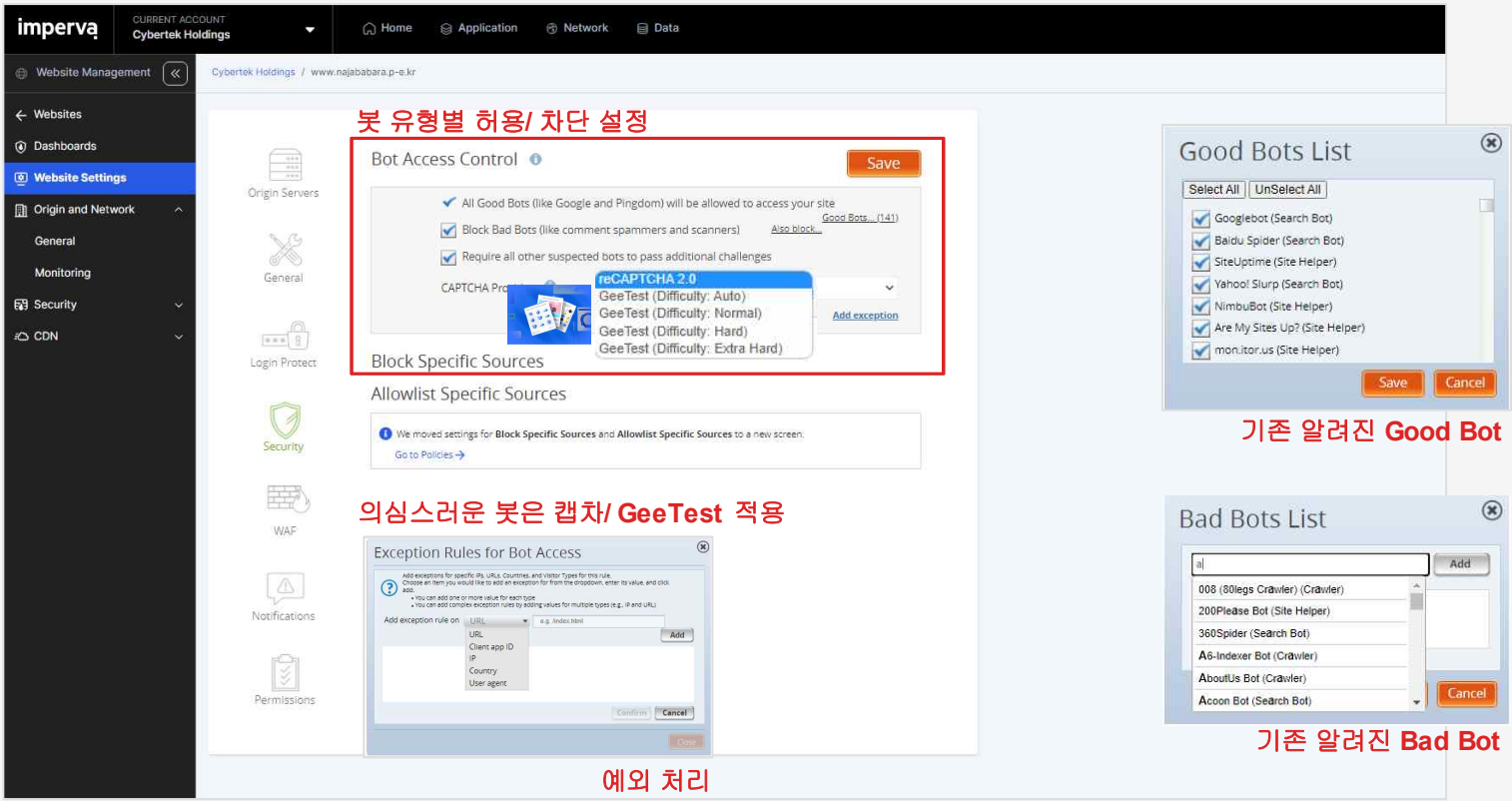
99.999% uptime 가용성 보장

+10 Tbps 처리용량

50+ 글로벌 스크러빙 센터

Bot Management 기능

Imperva가 지속적으로 Update하는 Bot DataBase를 기반으로 식속하게 실제 사용자와 Bot을 구분하고, 다양한 2차 대응 수단 제공



Imperva WAAP 과금정책

Imperva는 오직 정상 Traffic만을 대상으로 하는 95th Percentile 정책을 운영 합니다.

- 전체 트래픽에서 Clean Traffic만 과금 대상
- Blcoked(차단) Traffic은 과금 대상에서 제외

- Peak Traffic 5%를 제외하고 95%의 Peak Traffic을 기준으로 하여 과금

imperva

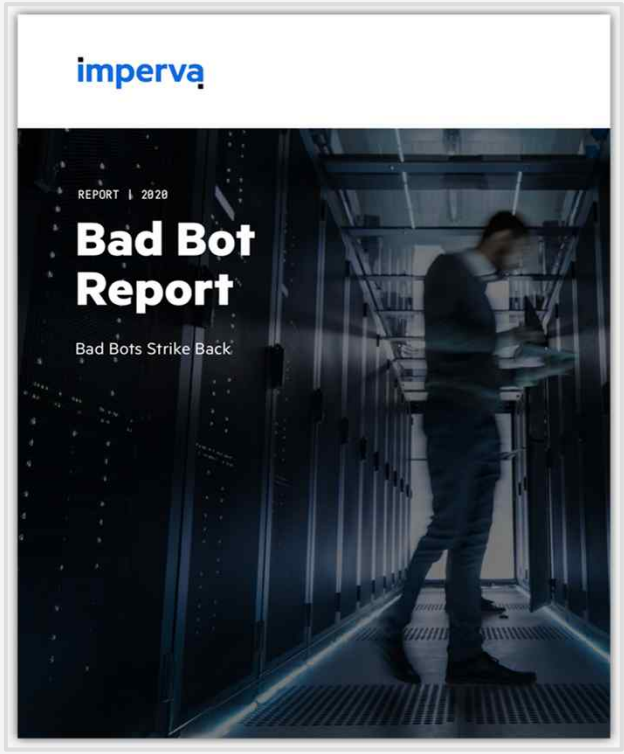
Advanced 기능 설명

ABP(Advanced Bot Protection)

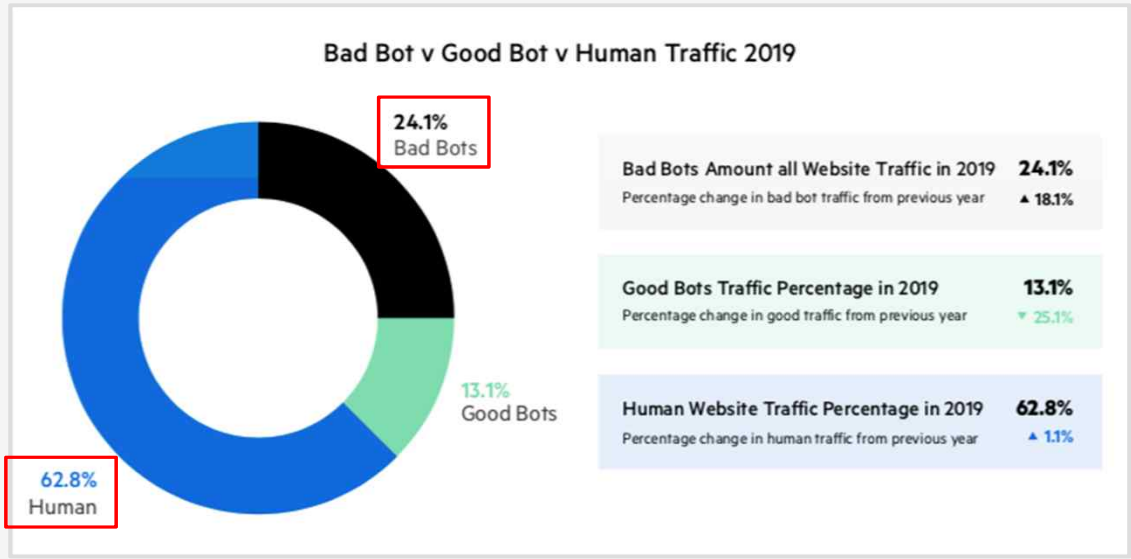
ATO(Account Takeover) 공격 대응

ABP(Advanced Bot Protection)

Imperva의 Bad Bot Report에 따르면 자동화된 Bot에 의한 공격이 지속적으로 증가하고 있습니다.



10번 접속 시 4번은 봇 접근 / 4번의 봇 접근 중 2.4회는 악성 봇 접근



ABP(Advanced Bot Protection)

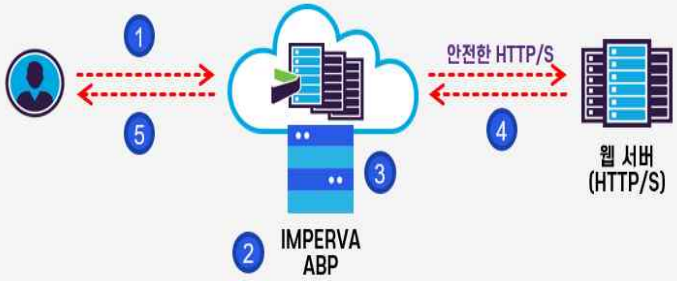
Imperva는 악성 봇 탐지의 정확성을 향상을 위하여 17가지의 ML(Machine Learning) 기법을 사용합니다.

탐지 모델	설명
Coordinated Activity Models (6)	함께 동작하는 사용자 그룹 탐지
Identity Mismatch Models (2)	자신을 여러 신분으로 표시하는 사용자 탐지
Session Characteristic Models (2)	세션이 비정상적으로 배포되는 사용자 탐지
Fingerprint Manipulation Model	클라이언트 핑거프린트를 지속적으로 변경하는 사용자 탐지
Avoid Identification Model	클라이언트 식별을 피하기 위해 클라이언트 정보를 지속적으로 변경하는 사용자
CAPTCHA Farm Model	캡차를 비정상적으로 해결하는 사용자 탐지
Wide Scraper Model	비정상적으로 사이트 이용 패턴을 보이는 사용자 탐지
Request Clustering Load balancer Model	정상적인 봇의 특징인 일정한 접속 요청 동작을 하는 사용자 탐지
Heavy Web Scraping Model	사이트의 특정 부분을 과도하게 스크래핑하는 사용자 탐지
Time Model	시간 단위로 비정상적으로 접속하는 사용자 탐지

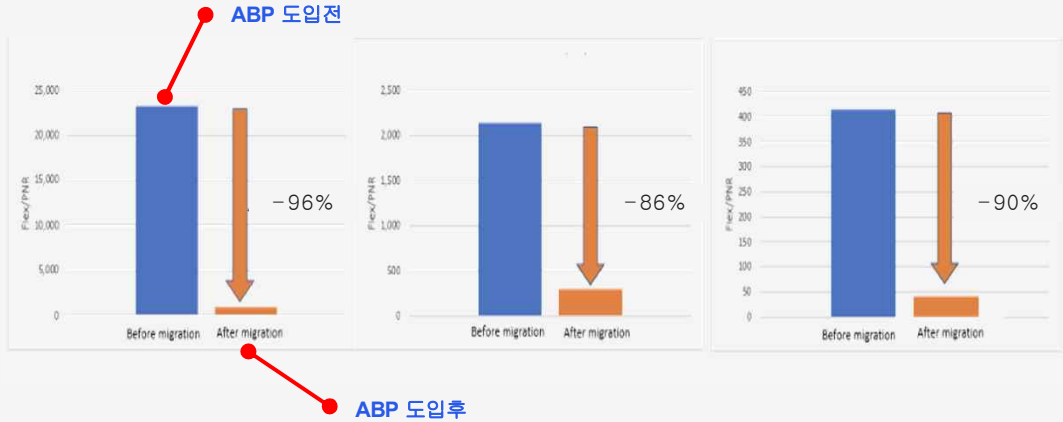
ABP(Advanced Bot Protection)

Imperva의 ABP를 도입한 기업들의 대부분이 서비스 도입후 약 90% 이상의 Bot 트래픽 감소 효과를 경험 하였습니다.

Imperva ABP 아키텍쳐



① 클라이언트는 웹서버에 데이터 요청
② ABP 서비스는 요청 헤더 감시
③ 봇으로 의심될 경우 사전 정의된 정책을 Cloud WAF에 조치사항 전달
④ Cloud WAF는 웹서버에 접속 후 데이터 수신
⑤ IMPERVA Cloud WAF는 전달된 지시에 따라 작동 (허용, 차단, CAPTCHA Challenge 등)

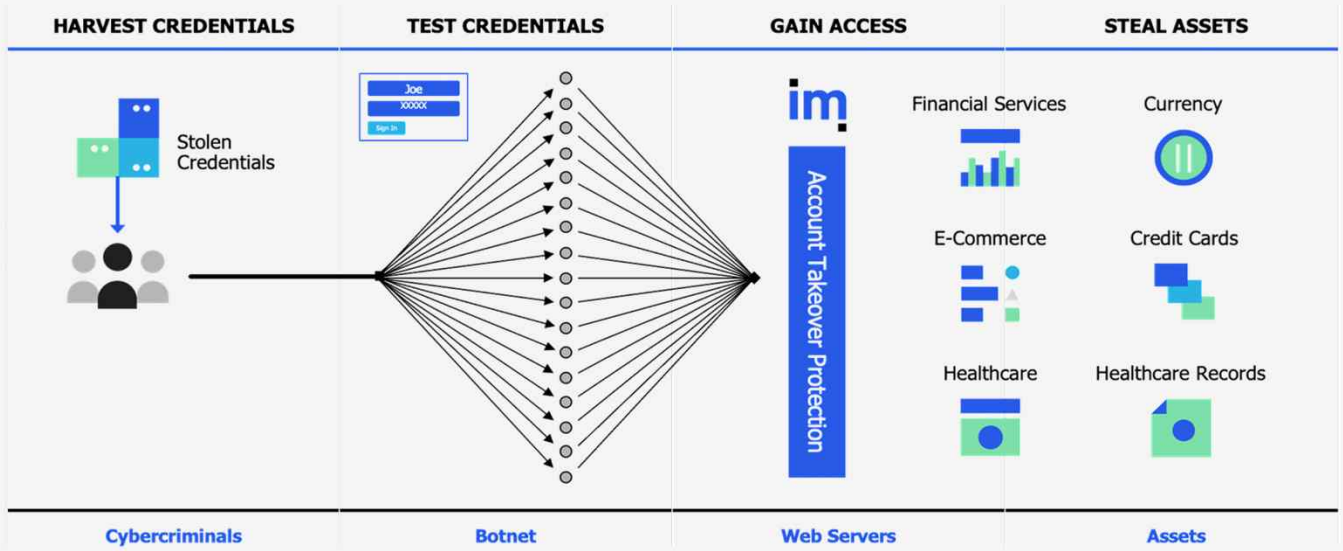


ABP(Advanced Bot Protection) 도입 후
약 90%의 봇 트래픽 및 보안 위협 감소 효과

ATO(Account Takeover) 공격 대응

ATO 공격 및 위험성

- 인터넷 사용자들이 동일한 로그인 정보를 여러 사이트에서 사용한다는 점을 악용
- **다크 웹을 통해 수집된 로그인 정보를 봇이 로그인 필드에 반복적으로 로그인하여 개인정보를 수집하는 형태의 공격**
- 계정도용 성공 시 금전적 이득, 자금 이체 또는 전자 상거래와 같은 거래를 수행하는 등 악의적인 목적으로 사용 될 수 있음.



ATO(Account Takeover) 공격 대응

ATO 공격 – Imperva의 대응

공격 확률
- 독점적인 알고리즘을 이용하여 클라이언트 프로그램, 로그인 시도 속도 및 IP 평판과 같은 요소를 고려하여 공격 가능성을 평가하는 프로필을 작성
- ATO는 위험 레벨을 각각의 계정 별로 High, Medium, Low 부여

고급 완화
- 좋은 봇과 나쁜 봇을 구분하여 봇의 비즈니스 및 보안의 순기능을 유지할 수 있도록 함

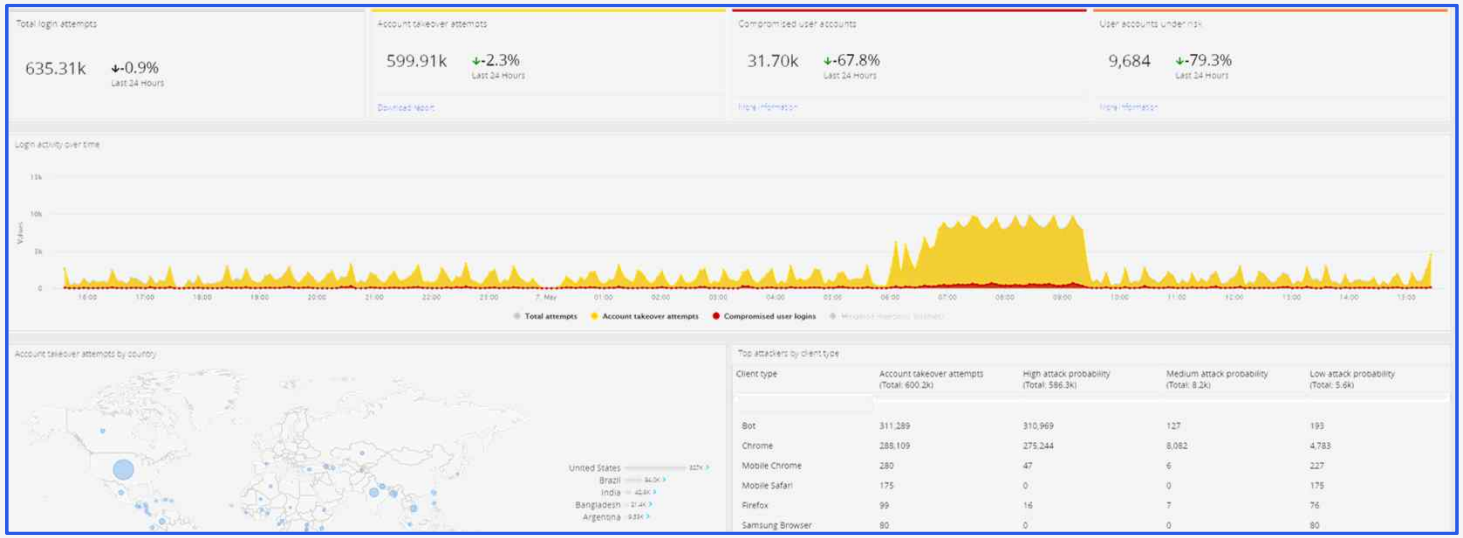
가시성
- 로그인 활동에 대한 대시보드를 통해 가시성을 제공. 사이트가 공격을 받는지, 영향을 받는 사이트 및 해킹 된 사용자 계정 리스트를 확인할 수 있음

Compromised User 판단 기준

차단 사유	설명
Bruteforce	동일한 디바이스에서 **단기간에 여러 사용자 계정으로 로그인을 실패한 경우.** Imperva 평판 및 클라이언트 분류 지표를 기반으로 장치 당 로그인 결과 비율, 사용자 이름 수 및 장치 위험과 같은 요소에 의해 결정 된다.
Password bruteforce	동일한 디바이스에서 **단기간에 서로 다른 패스워드를 입력하여 로그인에 실패한 경우.** Imperva 평판 및 클라이언트 분류 지표를 기반으로 장치 당 로그인 결과 비율, 실패한 로그인 수 및 장치 위험과 같은 요소에 의해 결정 된다.
Common password	동일한 디바이스에서 **단기간에 자주 사용되는 패스워드(예시> 123456)와 같은 사전 공격에 자주 사용되는 비밀번호로 로그인을 실패한 경우.** Imperva 평판 및 클라이언트 분류 지표를 기반으로 장치 당 로그인 실패 횟수, 비밀번호 평판 및 장치 위험과 같은 요인에 의해 결정 된다.
Common user	동일한 디바이스에서 **단기간에 로그인을 실패한 일반 사용자(예시> admin, administrator)가 많은 경우.** Imperva 평판 및 분류 지표를 기반으로 장치 당 로그인 실패 횟수, 사용자 평판 및 장치 위험과 같은 요인에 의해 결정된다.
Credential stuffing	동일한 디바이스에서 **단기간에 알려진 유출된 계정으로 과도한 로그인을 시도한 경우.** Imperva 평판 및 클라이언트 분류 지표를 기반으로 장치 당 로그인 결과 비율, 자격증명 평판 및 장치 위험과 같은 요소에 의해 결정된다.
Suspicious number of users	동일한 디바이스에서 **많은 계정이 로그인에 성공한 경우.** Imperva 평판 및 클라이언트 분류 지표를 기반으로 장치 당 로그인 결과 비율 및 위험과 같은 요인에 의해 결정된다.

ATO(Account Takeover) 공격 대응

ATO 공격 차단 사례 – 글로벌 게임사



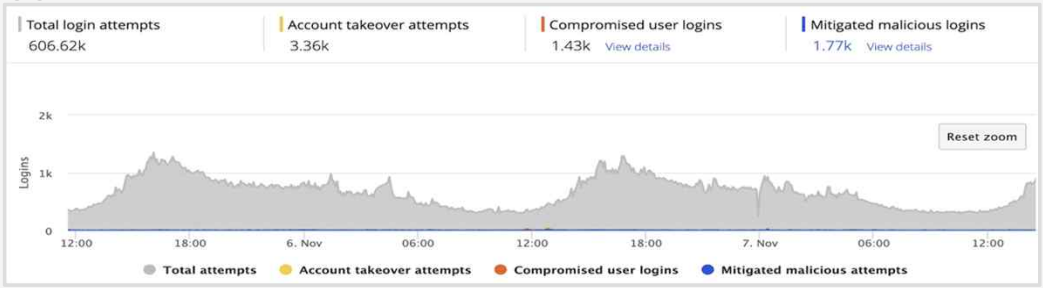
- +600k 로그인 시도
- 95% (586K) ATO(계정 탈취) 공격 시도
- 분산된 공격 시도
- 3709 IP는 익명의 프록시, 스패머로 식별됨
- 자동화된 봇 사용 식별

ATO(Account Takeover) 공격 대응

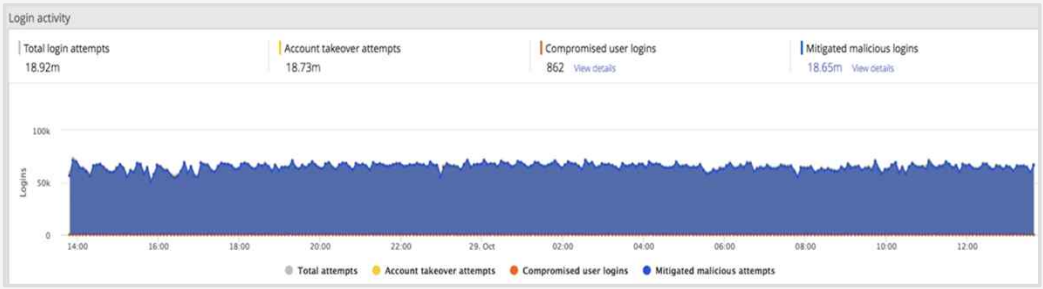
ATO 공격 차단 사례 – 글로벌 금융사

인프라를 압도하는 크리덴셜/ 계정탈취 공격 대응

정상 로그인



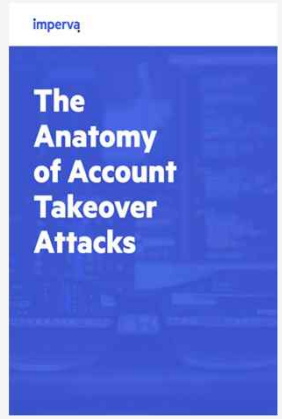
공격 로그인 활동



인프라를 앞도하는 ATO 공격

60시간 동안
44M+ ATO
시도
(12K per Sec)

99%의
로그인이 악성임



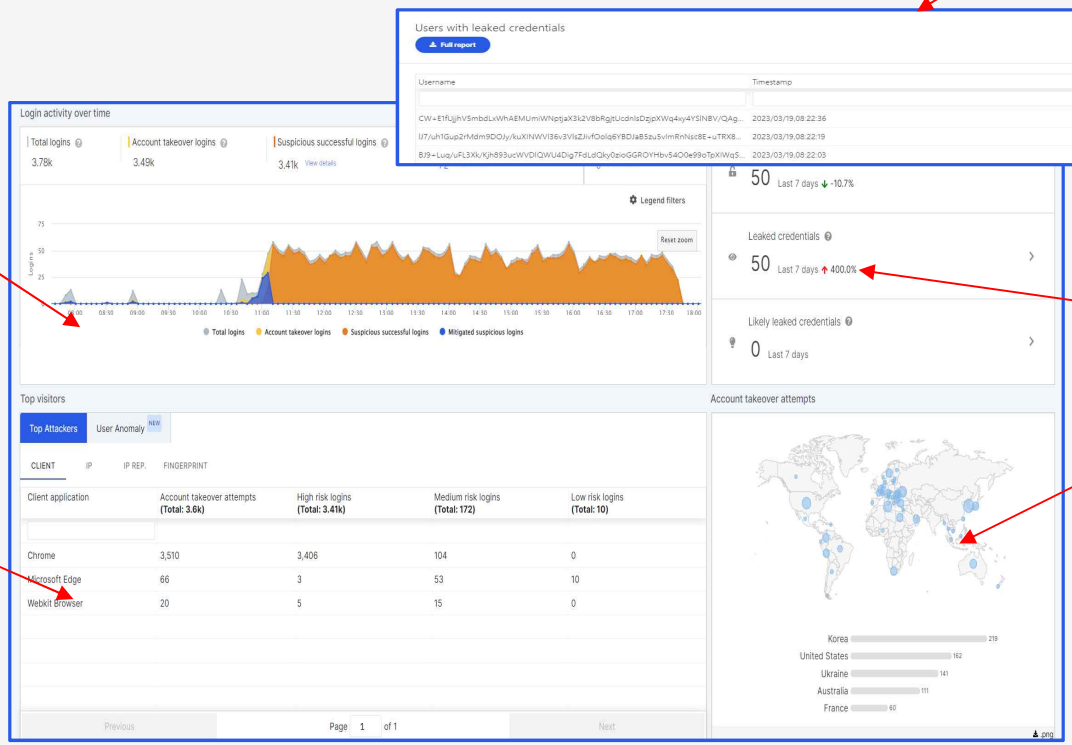
ATO(Account Takeover) 공격 대응

Imperva ATO Dashboard

공개 된 자격증명을 시도한 사용자 목록 제공. 공격 시도, 위험에 처한 사용자 및 탈취된 계정에 대한 명확한 가시성 제공

로그인 활동에 대한 그래프

Total login attempts: 모든 로그인 활동 수
Account takeover attempts: 잠재적인 **ATO** 공격 활동 수
Compromised user logins: 계정 탈취로 이루어진 로그인 수
(예시> Naver유출계정으로 DAUM 로긴시도)
Mitigated malicious logins: Imperva에 의해 차단된 **ATO** 공격



Compromised Users :
자격증명이 해킹 된 사용자 로그인 **(429),**
Users with leaked credential :
공개 된 자격증명을 사용하여 잠재적 위험을 갖고 있는 사용자 로그인**(10)**

각 클라이언트 타입, **IP, IP** 평판 별로 공격 가능성 수준을 표시

공격한 클라이언트의 정보를 국가 별로 표시

imperva

Thank You!

진네트웍스
솔루션 사업부 팀장 : 박종필
Kevin.park@jinnetworks.com