LEVELTHREE

Aientrophy

제품 기술 소개서

Product Technical Overview

Invisible Protection against Silent Threats

웹 애플리케이션을 대상으로 하는 자동화된 위협(매크로, 봇, 크롤링)을 실시간으로 탐지하고 차단하는 AI 기반 보안 솔루션입니다. 사용자 경험에 영향을 주지 않는 비침습적(Non-intrusive) 방식으로 동작합니다.

버전	3.0	상태	프로덕션 운영 중
작성일	2026-02-21	문서 분류	공개 (Public)

< 50ms 탐지 지연 시간	1 Line 연동 코드	Zero PII 개인정보 수집 없음	100% 서비스 가용성

Section 1

위협 현황 및 기술적 배경

전체 인터넷 트래픽의 51%가 자동화된 봇이며(Imperva Bad Bot Report 2025), 이 중 악성 봇이 37%를 차지합니다. 글로벌 피해 규모는 연간 수십억 달러에 달하며, 최신 봇은 인간의 마우스 궤적, 키 입력 타이밍, 스크롤 패턴까지 모방하여 기존 규칙 기반 방어 체계를 우회합니다.

지표	수치	출처 / 비고
전체 봇 트래픽 비율	51%	자동화된 봇이 인간 트래픽을 최초로 초과 (Imperva Bad Bot Report 2025)
악성 봇 트래픽 비율	37%	전년 대비 5%p 증가 (2023년 32% → 2024년 37%). 6년 연속 증가 추세
AI 기반 봇 비중	급증	AI 도구(LLM, 자동화 프레임워크) 확산으로 정교한 봇 공격 급격히 증가

1.1 주요 위협 유형

위협 유형	공격 방식	비즈니스 영향
매크로 매점매석	자동화 스크립트가 티켓/한정 상품을 실제 사용자보다 10~50배 빠르게 선점	정상 고객의 구매 기회 박탈, 브랜드 신뢰 하락
데이터 스크래핑	가격, 상품 정보, 콘텐츠를 대규모 자동 수집	경쟁 우위 상실, 서버 비용 증가
크리덴셜 스터핑	유출된 ID/PW 조합을 대규모 자동 테스트하여 계정 탈취	금전적 피해, 개인정보 2차 유출
AI 봇 진화	마우스 움직임, 키 입력 역학, 페이지 체류 시간 등 인간 행동 패턴을 AI로 모방	기존 CAPTCHA/규칙 기반 탐지 무력화

1.2 설계 원칙

원칙	설명
비침습성 (Non-intrusive)	호스트 애플리케이션 코드를 직접 수정하지 않습니다. SDK 삽입만으로 동작합니다.
Fail-Open (50ms 타임아웃)	보안 시스템 장애 또는 타임아웃 발생 시 트래픽을 허용합니다. 서비스 가용성 최우선.
Zero PII	민감한 개인식별정보(PII)를 수집하지 않습니다. GDPR/CCPA 준수.

Section 2

다계층 탐지 아키텍처

4개의 독립적 탐지 계층이 동시에 작동합니다. 각 계층은 서로 다른 신호를 분석하며, 단일 기법으로 전체 방어를 우회하는 것이 불가능한 구조입니다.

Figure 1. 다계층 탐지 아키텍처 — L4(외곽)에서 L1(내부)까지 단계적 필터링

계층	탐지 영역	분석 대상	처리 방식
L1	**행동 생체인식**	마우스 궤적 엔트로피, 속도/가속도 분산, 키 입력 간격(Flight Time), 체류 시간(Dwell Time)	내부 알고리즘
L2	**자동화 도구 탐지**	WebDriver 속성, HeadlessChrome UA, Navigator 불일치, 플러그인/WebGL 검사	6계층 다면 검출
L3	**세션 행동 분석**	요청 간격 변동 계수, 페이지 전환 속도, 폼 완료 시간, 동일 IP 다중 계정 접근	내부 알고리즘
L4	**능동적 방어**	Honeypot 필드, 비가시적 요소 상호작용, DOM 변조 감시, isTrusted 검증	즉시 차단

Section 3

자가 진화형 방어 시스템

정적 규칙으로는 진화하는 AI 봇에 대응할 수 없습니다. Aientrophy는 공격 AI와 방어 AI가 스스로 대결하며 학습하는 Self-Play 방식을 채택합니다.

Figure 2. 자가 진화형 방어 — 공격/방어 AI의 Self-Play 학습 구조

3.1 기존 접근법 비교

항목	규칙 기반 (기존)	Aientrophy
업데이트 방식	수동 규칙 추가 (보안팀 의존)	보안팀의 검토하에 AI가 자동으로 공격 패턴 학습 및 규칙 갱신
AI 봇 대응	인간 행동 모방 봇 탐지 불가	행동 생체인식 + 내부 알고리즘으로 미세 패턴 탐지
우회 난이도	규칙 패턴 분석 후 우회 가능	4계층 독립 분석, 단일 기법 우회 불가
유지 비용	지속적 인력 투입 필요	Self-Play 기반 학습 + 보안팀 검토하에 규칙 갱신

3.2 위협 스코어링 체계

각 탐지 이벤트의 위협도가 IP 단위로 누적됩니다. 임계치 초과 시 자동으로 접근을 차단하거나 챌린지를 발급합니다.

점수 구간	대응	설명
0.0 ~ 0.3	**허용 (Allow)**	정상 사용자로 판단. 모든 요청 허용.
0.3 ~ 0.8	**챌린지 (Challenge)**	의심 행동 탐지. CAPTCHA 챌린지 발급.
0.8+	**차단 (Block)**	봇으로 판단. 해당 IP를 일정 시간 차단.

Section 4

시스템 아키텍처

클라이언트 측 보안 SDK(WebAssembly 기반)와 서버 측 분석 엔진으로 구성된 클라이언트-서버 아키텍처입니다. 핵심 탐지 로직은 WASM으로 컴파일되어 역공학이 극도로 어려우며, 모든 통신은 엔드투엔드 암호화됩니다.

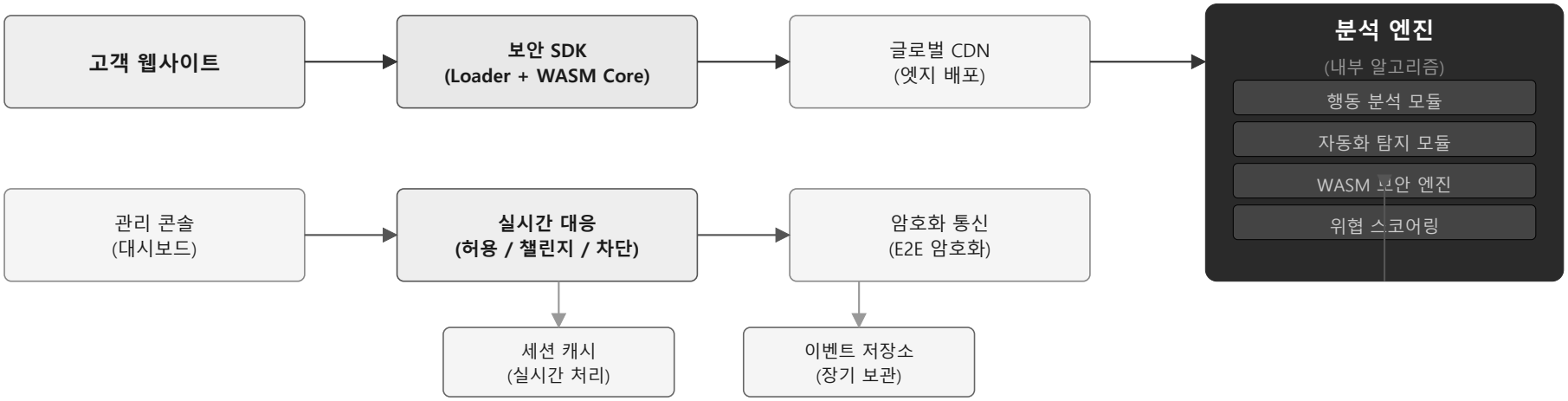

Figure 3. 시스템 아키텍처 — 클라이언트에서 분석 엔진까지의 데이터 흐름

4.1 성능 사양

항목	사양	비고
SDK 로딩 시간	< 100ms	CDN 엣지 배포 + 초경량 로더 (~1KB)
탐지 응답 시간	< 50ms	Fail-Open: 타임아웃 시 트래픽 허용
통신 암호화	E2E	엔드투엔드 암호화 적용
서비스 가용성	100%	Fail-Open 아키텍처로 무중단 보장
소스 보호	WASM	WebAssembly 컴파일 + 동적 로딩 + 난독화 + 도메인 잠금

Section 5

SDK 구조 및 연동

보안 SDK는 핵심 탐지 로직을 WebAssembly(WASM)로 컴파일하여 네이티브급 성능과 역공학 방지를 동시에 달성합니다. 2단계 동적 로딩 아키텍처를 채택하여 Loader와 WASM Core가 분리되어 있으며, Core는 암호화된 상태로 전송되어 메모리 상에서만 실행됩니다.

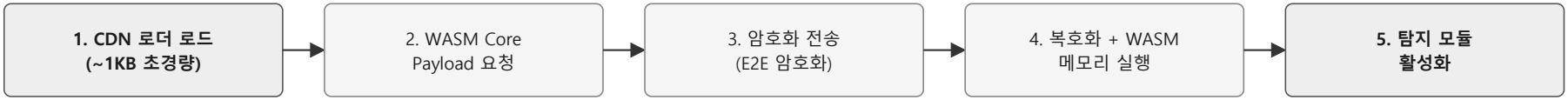

Figure 4. SDK 2단계 동적 로딩 흐름 — WebAssembly Core의 암호화 전송 및 메모리 실행

5.1 탐지 모듈

모듈	분석 대상	탐지 목표
MouseTracker	마우스 궤적의 엔트로피, 속도/가속도 분산 패턴	직선 이동, 일정 속도의 기계적 움직임
InputTracker	키 입력 간격(Flight Time), 키 체류 시간(Dwell Time)	기계적 타이핑, 초인적 입력 속도
RapidClickDetector	연속 클릭의 시간 간격 및 좌표 패턴	자동화된 클릭 봇
Honeypot	사용자에게 비가시적인 숨겨진 폼 필드 상호작용	DOM을 순회하는 폼 자동 입력 봇
InvisibleInteraction	비가시 요소 상호작용 + isTrusted 속성 검증	스크립트로 생성된 합성 이벤트
ConsoleDetector	개발자 도구 열기 여부 (3계층 감지)	실시간 디버깅 / 분석 시도
AntiDebug	디버거 문 주입 + 실행 타이밍 편차 분석	역공학 및 코드 분석 시도

5.2 연동 방법

HTML 스크립트 태그 1줄을 추가합니다. SDK가 자동으로 2단계 동적 로딩을 수행합니다.

```
<script src="https://cdn.aientrophy.com/sdk/loader.js"></script> <script> SecuritySDK.init({ clientKey: "your-key" }); </script>
```

Section 6

보안 아키텍처

일반적인 HTTPS를 넘어 애플리케이션 계층에서의 다층 보안을 적용합니다. 프록시 도구를 이용한 중간자 공격에 대응하기 위해 페이로드 수준에서 기밀성, 무결성, 신선도(Freshness)를 보장합니다.

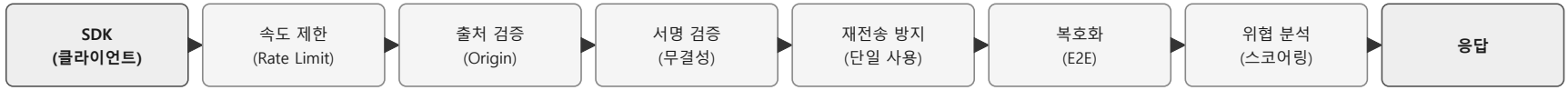

Figure 5. 요청 처리 파이프라인 — 8단계 검증 흐름

6.1 패킷 변조 방어 체계

방어 계층	기술	설명
전송 암호화	엔드투엔드 암호화	인증 태그를 포함하여 페이로드 변조 시 복호화 자체가 실패합니다.
시간 기반 방어	타임스탬프 검증	일정 시간 경과한 패킷은 즉시 폐기합니다. 캡처된 패킷의 재사용을 방지합니다.
무결성 검증	서명 기반 검증	요청 출처 인증과 데이터 무결성을 동시에 보장합니다.
재전송 방지	일회성 토큰	사용 후 즉시 폐기되는 토큰으로 동일 요청의 재전송을 차단합니다.
논리 검증	서버 측 일관성 검사	좌표-뷰포트 불일치, 불가능한 스크롤 등 조작된 데이터 패턴을 탐지합니다.
이벤트 신뢰성	브라우저 네이티브 검증	스크립트로 생성된 합성 이벤트를 식별하여 차단합니다.

6.2 소스 코드 보호

핵심 탐지 로직은 WebAssembly(WASM)로 컴파일되어 네이티브급 성능으로 실행됩니다. WASM 바이너리는 함수명·변수명·디버그 심볼이 모두 제거되며, 런타임 노이즈(원본 대비 ~40배 코드)로 분석 난이도를 비약적으로 높입니다. Loader(CDN ~1KB)와 WASM Core(서버)는 분리되어 Core는 암호화 전송 후 메모리에서만 실행됩니다. JavaScript 레이어에는 제어 흐름 난독화와 도메인 잠금을 적용하며, 3계층 안티 디버깅으로 실시간 분석을 방해합니다.

Section 7

산업별 적용 및 관리 콘솔

7.1 산업별 활용 사례

산업	주요 위협	Aientrophy 적용 효과
티켓 / 예약 서비스	매크로 매점매석, 대기열 우회, 봇 팜	실시간 봇 탐지로 한정 상품에 대한 공정한 접근 보장
이커머스 & 리테일	가격 스크래핑, 재고 매점매석, 계정 탈취	다계층 탐지로 자동화 공격 원천 차단, 결제 사기 방지
커뮤니티 & 플랫폼	스팸 봇, 콘텐츠 무단 수집, 자동 가입	행동 분석 기반 스팸/봇 탐지, API 남용 방지
금융 서비스	크리덴셜 스터핑, 자동 이체 시도, 계정 탈취	세션 행동 분석 + 다계층 탐지로 이상 접근 즉시 차단

7.2 관리 콘솔

관리자는 웹 기반 콘솔에서 실시간 위협 현황을 모니터링하고, 보안 정책을 조정할 수 있습니다.

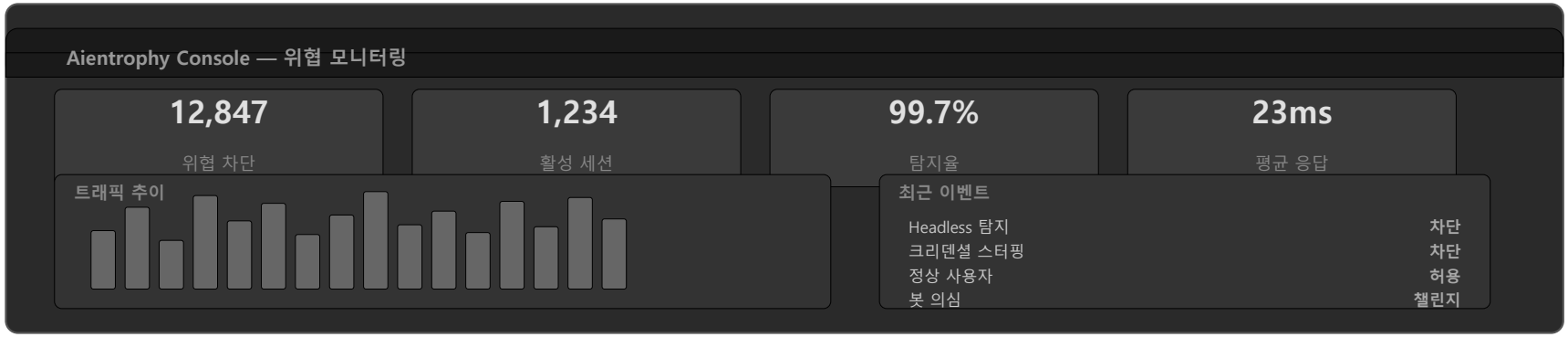

Figure 6. 관리 콘솔 대시보드 와이어프레임

Section 8

배포 현황 및 검증 결과

8.1 인프라 배포

구성 요소	배포 환경	상태
Backend Server	AWS Elastic Beanstalk (Docker)	운영 중
Official Site	AWS Amplify	운영 중
Client Console	AWS Amplify	운영 중
SDK (CDN)	AWS CloudFront	운영 중
npm 패키지	@aientrophy/sdk v0.1.1	배포 완료

8.2 기술 스택

레이어	기술
SDK	TypeScript, AssemblyScript → WebAssembly (.wasm), Vite, Terser
Backend	Node.js 20, Express, TypeScript
Frontend	Next.js, React 19, Tailwind CSS
Infrastructure	AWS (EB, RDS, ElastiCache, CloudFront, S3, Amplify)

8.3 보안 검증 결과

검증 항목	결과	비고
패킷 변조 방어 테스트	**30/30 통과**	암호화 무결성, 타임스탬프, 논리 검증 등 6개 범주
서명 기반 무결성 검증	**7/7 통과**	상수 시간 비교, 타임스탬프 만료 포함

검증 항목	결과	비고
재전송 방지 검증	**5/5 통과**	일회성 토큰 사용 후 폐기 확인
SDK 단위 테스트	**7/7 통과**	Vitest 기반 단위 테스트
서버 단위 테스트	**3/3 통과**	Jest 기반 단위 테스트
인간형 봇 오탐 방지	**5/5 통과**	Level 2 봇 (인간 행동 모방) 오탐 없음 확인
기계적 봇 탐지	**탐지 성공**	Level 1 봇 (직선 이동, 즉각 타이핑) 탐지 확인

Aientrophy

Invisible Protection against Silent Threats

웹사이트	문의	관리 콘솔
aientrophy.com	info@aientrophy.com	console.aientrophy.com

LEVELTHREE