

N·PAS

NURIERSYSTEM
PROTECTION SYSTEM FOR
ANTI SCRAPING



솔루션 배경

최근 해킹 / 정보 탈취에 악용되는 ‘악성 봇’으로 인한 스크래핑으로 산업계 피해 심각

계정 탈취, 디도스 공격, 웹 스크래핑, 데이터 탈취를 위한 ‘악성 봇’ 공격 급증

불법적인 스크래핑으로 웹 서비스에 지장을 주거나 데이터를 탈취하고 트래픽을 폭증시켜 비용을 증가시킴

기업의 손실과 이미지 하락

불법적인 스크래핑 증가로 고객 데이터 유출, 서버 성능 감소로 인해 서비스 지연과 불편을 야기하고 금전적 손실과 고객의 신뢰도를 잃게 됨



불법 스크래핑(scraping)과 봇이란?

- 스크래핑: 웹사이트나 시스템의 내용을 그대로 가져와서 필요한 데이터를 추출해 내는 행위
- 봇: 웹사이트를 스크래핑하는 자동화된 기계로 포털사이트, 가격비교 사이트 등에서 주로 이용
- 불법 스크래핑: 운영자 정책(robots.txt, 이용 약관)을 무시하고 스크래핑을 하는 행위

솔루션 필요성

| N-PAS는 원치 않는 스크래핑에 대해 고객사의 데이터를 보호해 드립니다.



불법 스크래핑 방지



서비스 안정성 확보



시스템 과부하 방지



API 남용 방지

솔루션 구성

| N-PAS는 서비스 이용자의 주요 정보를 프로파일 형태의 데이터로 저장해 탐지에 활용합니다.



주요 기능

트래픽 모니터링

- 네트워크 트래픽 모니터링
- 트래픽 사용량 통계 모니터링
- 사람/정상 봇/악성 봇 분류 모니터링



정책 수립

- 사람/정상 봇/악성 봇에 따른 정책 적용
- 일정 트래픽 이상일 경우, 차단 정책 적용



탐지결과 실시간 응답

- 악성 봇 블랙리스트 작성
- 실시간 탐지와 응답 수행
- 다양한 보안 시스템과 인터페이스



피드백

- 사람/정상 봇/악성 봇에 따른 정책 적용
- 일정 트래픽 이상일 경우, 차단 정책 적용



도입 효과



데이터 및 비즈니스 보호

- 불법 스크래핑 방지를 통한 기업자산 보호
- 안전한 사용자 계정 및 업무상 중요한 데이터 보호



서비스 성능 보장과 고객 민원 해소

- 서비스 성능 보장과 서비스 안정성 확보
- 서비스 속도저하와 중단을 사전에 방지하여 사용자 만족도 제고



시스템 과부하 방지

- 불법 스크래핑에 의한 인프라 및 네트워크 자원의 독점 해소
- 시스템 안정성 보장으로 비정기 유휴자원 확보



API 남용 방지

- API 서버 및 웹/앱 서버에 대한 트래픽 검증과 필터링을 통한 불법 접근 차단

서비스 구현 환경 | 누리어시스템은 공공, 기업, 금융 등 다양한 분야 고객들의 사이버 안전에 최선을 다합니다.

서비스 환경	솔루션 방식	클라우드 방식
서비스 제공	<ul style="list-style-type: none">· 실시간 모니터링· 실시간 분류· 실시간 정책 적용· 실시간 차단· 블랙리스트 관리· 결과 모니터링	<ul style="list-style-type: none">· 실시간 모니터링· 실시간 분류· 실시간 정책 적용· 실시간 차단· 블랙리스트 관리· 결과 모니터링
지원 정책	<ul style="list-style-type: none">· 자체 정책에 따른 데이터 저장· 인터페이스· 교육 및 지원	<ul style="list-style-type: none">· 빠른 설치· 데이터 사용에 따른 청구· 별도 데이터 보존 정책· 인터페이스· 교육 및 지원

솔루션 문의

박환성
부장

경영사업본부

010·3206·2057
hspark@nurier.co.kr

한경택
대리

경영사업본부

010·9590·8377
kthan0529@nurier.co.kr