WEEDS BlackBox Series

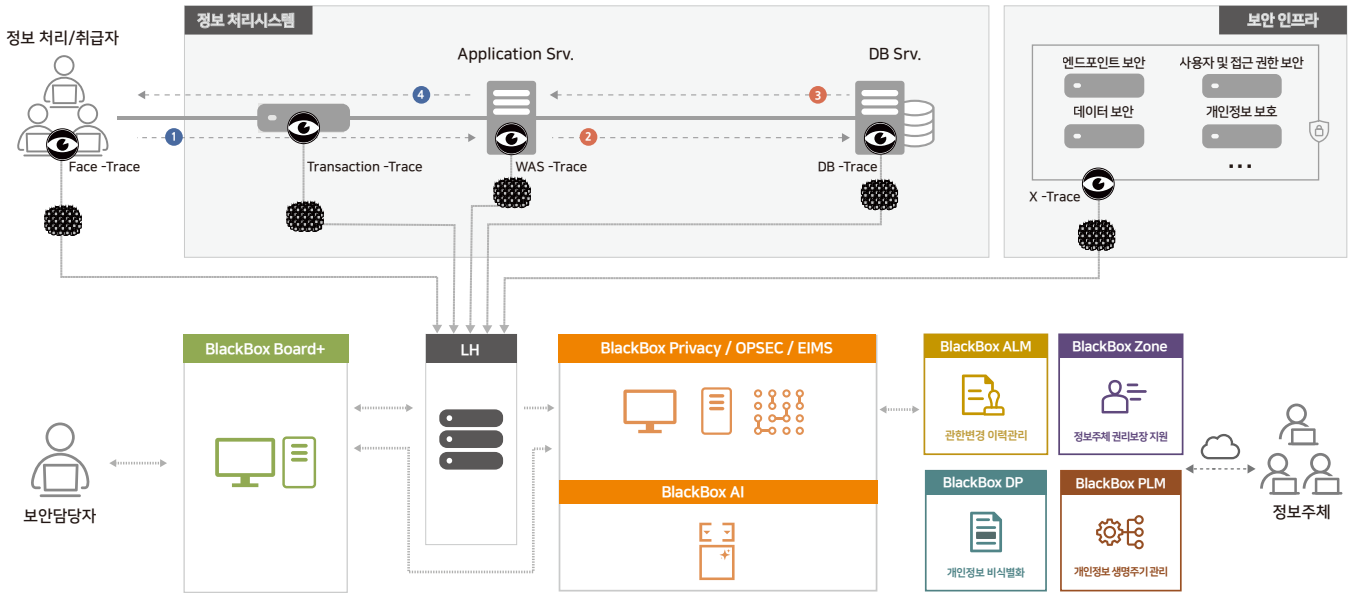
국내 최초 출시!
고객수 1위
판매액 1위
판매량 1위

AI 기반 내부자 행위 분석 및 위험 관리 플랫폼

About WEEDS BlackBox Series?

WEEDS Blackbox Series는 AI 기반 내부자 행위 분석 및 위험 관리 플랫폼(AI-driven Insider Behavior Analysis & Risk Management Platform)으로, 내부 정보시스템에서 발생하는 모든 업무 활동에 대한 전사적 가시성을 확보하고 이상 행위를 식별하여 조직의 핵심 정보 자산을 보호하며 관련 법규 및 컴플라이언스 준수를 지원합니다.

시스템 구성



WEEDS BlackBox Series 제품군

제품명	주요기능
BlackBox Privacy	개인정보 접속기록 관리 및 이상행위 탐지·대응
BlackBox OPSEC	중요 내부정보 처리이력 관리 및 이상행위 탐지·대응
BlackBox EIMS	기업 내부정보 처리 및 보안위협 탐지·대응 통합관리
BlackBox AI	AI 기반 내부자 이상행위 분석·탐지
BlackBox DP	개인정보 비식별화
BlackBox Board+	내부정보 부정사용 상시 감사 및 통합 소명 관리
BlackBox ALM	정보처리시스템 접근권한 변경 이력 관리

BlackBox Privacy

BlackBox Privacy는 관계 법령에서 요구하는 의무사항을 충실히 준수할 뿐만 아니라, 각종 인증심사와 평가 기준, 정부 보안 정책에 효과적 으로 대응할 수 있도록 체계적으로 지원합니다.

도입 근거 및 필요성

개인정보보호법 준수

법 제29조(안전조치의무), 시행령 제30조(안전성 확보 조치) 및 고시 제8조(접속기록의 보관 및 점검)에 따라, 개인정보 처리자는 개인정보처리 시스템에 대한 모든 접속기록을 누락이나 유실 없이 온전하게 생성하고 안전하게 보관 · 관리하며 정기적 으로 점검해야 합니다.

ISMS-P 인증심사

개인정보처리시스템 접속기록 관리는 ISMS-P 인증심사에서 매우 중요한 점검 항목으로, 일반적인 시스템 로그나 DB 접근 제어 만 으로는 요구 수준에 부합하기 어렵습니다. BlackBox Series는 법적 의무사항은 물론 위험행위 탐지, 내부자 위협 대응, 사후 감사를 가능하게 함 으로써 인증심사를 충족할 수 있도록 지원합니다.

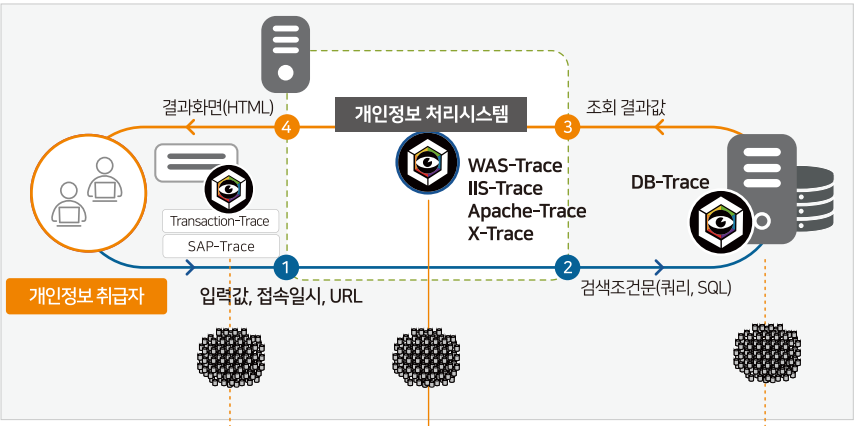
공공기관 개인정보 보호수준 평가

2025년 평가부터는 AI 등 신기술을 활용한 개인정보 리스크 관리체계를 구축한 경우 최대 10점의 가점을 부여하고 있습니다. AI 기술을 활용 하여 방대한 접속기록을 분석하고 숨겨진 위험을 정교하게 찾아내는 BlackBox Series를 도입한 공공기관은 평가에서 보다 나은 결과 를 기대할 수 있습니다.

국가 망 보안체계(N2SF)

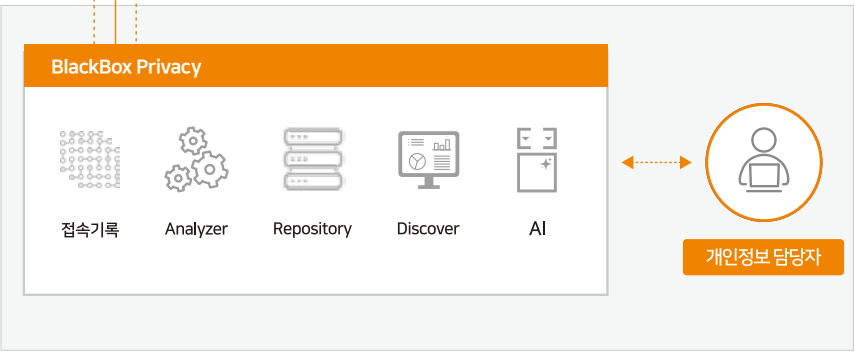
BlackBox Series는 변화하는 보안 환경에 대응하기 위해 국가정보원이 제시한 새로운 국가 망 보안체계(N2SF) 기준을 고려하여 설계 되었으며, 또한 정부 · 공공기관의 보안 인프라와 유연하게 연동되고 안정적으로 통합될 수 있도록 지원합니다.

개인정보 접속기록 생성



- **모든 정보처리 환경에 대한 접속기록 생성 지원**
  - JAVA, ASP, PHP 등 모든 WEB환경
  - CS환경 (2Tier, 3Tier 환경)
  - DB 직접 사용 환경 (콘솔작업 및 배치작업 등)
- **관련 법규 및 기준고시 완벽 충족**
  - 취급자 식별정보(ID), 접속일시, 접속지 정보
  - 수행업무 자동 정의 및 기록
  - 정보주체정보(이름, 주소 등) 기록
  - 검색조건문(SQL) 기록

차세대 개인정보 접속기록 분석 · 관리



- **접속기록의 안전한 보관**
  - 보관기관 1년(5만명 기준 2년) 법규 충족
  - MAC코드 관리기능을 통한 위변조 방지 관련 법규 충족
- **AI기반 비정상행위 및 다운로드 자동 탐지**
  - 빅데이터 기반 접속기록 다차원 통합분석
  - 자체개발 AI기반의 비정상행위 분석 및 탐지
- **접속기록 추적, 점검 및 관리**
  - 행위기반 추적, 사용자 및 사용정보 기반 추적 도구 제공
- **다양한 보고서 기능**
  - 각종 정기점검용 보고서, 개인정보 책임자용 보고서
  - 수준진단 등 업무별 전용 보고서

특장점 및 차별성

1 검색 조건문(쿼리, SQL), 정보주체정보(이름,ID) 완벽 기록

개정 기준 고시 충족을 위해 "검색조건문(SQL)" 및 "정보주체정보(이름)" 기록이 반드시 필요

2 개인정보 다운로드 자동 식별

개정 기준 고시 충족을 위해 개인정보 다운로드 식별 및 사유확인 필요

3 수행업무 자동 정의 및 기록

- 수행업무 수작업 정의 및 현행화 작업에 의한 관리자 불편 해소

4 정확한 개인정보 취급행위 선별 및 취급 개인정보 식별

- 패턴필터링의 오류(오탐, 과탐 등)를 최소화 하기 위하여 SQL 결과의 컬럼 기반으로 식별

5 JDBC드라이브 교체 등 심각한 환경변화 없이 접속기록 생성

JDBC드라이브 교체, 변경은 시스템에 매우 큰 영향을 유발하며 대상 시스템이 보안솔루션에 종속되는 문제를 일으킴

6 일체의 유실, 누락없는 접속기록 생성

7 조회 결과값, 결과화면까지 기록

- 결과화면(HTML)만 기록시 운영 시 다양한 한계 및 불편 발생

8 개정된 "개인정보의 안전성 확보조치 기준 고시" 충족

- 기준 고시 및 보호수준평가 ISMS-P, 영향평가 등 완벽 대응

9 개인정보 처리 전사 가시성 확보 및 시스템화된 준법체계 제공

공공시스템 운영기관의 개인정보 접속기록 보관 및 점검 완벽 지원!

개인정보보호위원회 고시 「개인정보의 안전성 확보조치 기준」 제17조

① 공공시스템 접속기록 등을 자동화된 방식으로 분석하여 불법적인 개인 정보유출 및 오용·남용 시도를 탐지하고 그 사유를 소명 하도록 하는 등 필요 한 조치를 하여야 한다.

Blackbox Series 지원사항

일원화된 컴플라이언스 준수 프로세스

접속기록 생성부터 이상행위 탐지, 소명 처리, 최종 보고서 생성까지 전 과정을 하나의 시스템으로 통합 지원

AI 기반 스마트 탐지

단순 임계치 기반 탐지를 넘어, 탐지된 이상행위에 대한 학습을 통해 비정상 행위를 식별

원스톱 소명 워크플로우

이상행위 탐지 시 자동 알림을 발송하며, 전용 인터페이스를 통해 사유 입력 및 증빙 자료 제출을 즉시 처리합니다.

② 공공시스템운영기관은 공공시스템이용기관이 소관 개인정보 취급자 의 접속기록을 직접 점검할 수 있는 기능을 제공하여야 한다.

Blackbox Series 지원사항

독립적 점검 환경

전용 아키텍처와 권한 통제를 통해 이용기관별로 분리된 접속기록 점검 환경을 제공하며, 이용기관별 취급자의 접속기록만 안전하게 조회·점검 가능

맞춤형 운영 및 보고

기관별 특성에 맞춘 점검 필터 설정이 가능하며, 각 이용 기관별로 표준 보고서를 자동으로 생성하여 행정 효율 증가

맞춤형 라이선스 정책

이용기관 수(기관 및 사용자)에 알맞는 라이선스 정책과 세분화된 관리자 권한 체계를 지원하여 운영기관의 비용과 관리 부담의 최소화

BlackBox AI

Blackbox AI는 위즈코리아의 자체 개발 AI 모델 'GUREUM'이 학습한 데이터를 기반으로 이상행위를 분석·탐지합니다. 방대한 접속 기록과 탐지 데이터를 분석하여 기존 보안 방식으론 확인하기 어려운 고위험 이상행위와 내부자 위협을 탐지하여, 보안 담당자를 지원하는 지능형 보안 AI Agent로 동작합니다.

특징 및 장점

AI 자체개발 모델

23년간 축적된 내부정보 보안 기술과 노하우로 개발된 위즈코리아의 자체 AI 모델입니다.

AI모델 기반의 이상 행위 자동 탐지 기능

- 자체 AI 모델 GUREUM을 통한 고객 업무·보안 증적 자동 학습
- 고객 환경에 특화된 이상 행위 식별 및 내부 위험 자동 탐지

학습 데이터 자동 관리 기능

최신 데이터를 자동으로 수집, 전처리하고 불필요하거나 오래된 학습 데이터를 자동으로 정리

폭넓은 확장 가능

기존 AI플랫폼을 사용하는 것과 달리 새로운 위협과 변형된 위협에도 신속하게 대응 가능한 고객 맞춤형 AI 모델입니다.

주기적, 지속적 자동 학습 및 최적화 기능

- 업무증적을 지속적으로 학습하여 위험식별 모델의 지속적, 점진적 성능 향상
- 최신의 내부 보안 위협에 지속 적응

AI 모델 운용(데이터 수집, 학습, 탐지) 모니터링 및 고도화 기능

AI 모델의 데이터 수집, 학습, 탐지 현황과 이력의 모니터링 및 감시체계 운영에 반영하는 고도화 기능 제공

BlackBox OPSEC

BlackBox OPSEC은 조직 내부의 중요 정보 자산(영업정보, 고객정보, R&D 정보 등)을 보호하기 위한 전사적 내부 정보 접근 가시성 확보 플랫폼입니다. 내부정보 처리 경로와 이상 행위를 정확히 식별하고, 내부자 위협을 선제적으로 관리하여 조직의 핵심 자산을 안전하게 보호하는 데 특화되어 있습니다.

주요 기능

내부 중요 정보 자산 식별 및 분류
중요 정보 자산의 식별 및 중요도에 따른 분류 지원

전사적 업무 증적 관리
데이터 조회, 다운로드, 수정 등 모든 업무 활동에 대한 상세 접속기록 및 행위 기록을 누락 없이 생성 및 보관

접근 및 처리 행위 가시성 확보
내부정보 접근 및 처리 과정의 가시성 제공

다양한 중요 정보 자산 보호
영업 정보, R&D 정보 등 내부 핵심 정보 자산에 대한 통합 보호 체계 제공

BlackBox EIMS

Blackbox EIMS는 Blackbox Series의 핵심 엔진 및 자체 개발 AI 모델을 기반하여 내부 정보처리시스템은 물론, 다양한 정보보안 인프라에서 개별적으로 관리되는 보안 및 시스템 로그 데이터를 통합 연계하여 종합적인 가시성을 제공합니다. 특히, 단순한 로그 통합을 넘어 AI 기반의 '내부자 행위 분석 및 위험 관리 플랫폼'으로서 역할을 수행하고, 통합된 로그 데이터를 처리, 보관, 취급, 유·반출, 기타 등 5가지 핵심 관점으로 재구성하여 정보의 흐름을 입체적으로 분석하고 조직의 보안 체계를 완성합니다.

주요 기능

전사적 로그 통합 수집 및 연계
내부 정보시스템 외 DB, WAS, OS, 네트워크 장비, 보안 솔루션(DRM, DLP, NAC 등) 등 고객 환경의 모든 이기종 시스템 로그를 수집, 통합

정보 활동 5대 관점(처리, 보관, 취급, 유·반출, 기타) 분석
단순 로그 분석을 넘어, 정보를 다루는 행위를 5가지 핵심 관점으로 분류하고 심층 분석하여 정보 흐름의 투명성 확보

통합 보안 이벤트 관리 및 분석
개별 시스템의 이벤트를 통합 관리하고, AI 기반 분석을 통해 잠재적인 보안 위협 시나리오 자동 식별

통합 대시보드 및 리포팅
전사적 보안 현황, 주요 정보 활동, 위협 탐지 이력을 한눈에 파악할 수 있는 통합 대시보드 및 맞춤형 리포팅 제공

BlackBox DP

Blackbox DP는 개인정보 비식별화·가명처리, 마스킹 등 비식별화 기술을 적용하여 개인정보 식별 가능성을 최소화하고 안전한 데이터 활용을 지원 합니다.

주요 기능

규제 준수 및 보안성 강화
가명정보 처리 가이드라인 등에 최적화된 기술 제공

전용 UI 제공
비식별화를 위한 편리한 전용 UI 제공

맞춤형 비식별화
비식별화 처리를 위한 10여가지 이상의 전용 알고리즘 지원

폭넓은 호환성
다양한 데이터소스(DB, File, API 등) 및 형식 지원

주요 고객사

우리은행 · 삼성카드 · 삼성증권 · 한국투자증권 · 한화생명 · 한국은행 · NICE평가정보
SK hynix · LG U+ · LG CNS · 삼성전자 · 롯데쇼핑e커머스 · SHINSEGAE · KT&G
국세청 · 경찰청 · 검찰 · 대한민국국회 · 세계속의 경기도 · 부산광역시 · 인천광역시
KERIS 한국교육학술정보원 · KLID 한국지역정보개발원 · LH 한국토지주택공사 · 근로복지공단 · 한국도로공사 · 한국방송통신대학교 · KISA 한국인터넷진흥원

그외 다수

WEEDS (주)위즈코리아
www.weeds.co.kr
02-786-7217
 Desing by UMI 2010, Printed 2026.03