WAREVALLEY

DBMS

SOLUTION

PARK

www.warevalley.com

WARE VALLEY

Log Catch

개인정보 접속기록 통합관리 솔루션

Log Catch V2

보안 책임자는 기업내 보유한 개인정보 보호의 필요성이 증가함에 따라 개인정보사용자/취급자에 대한 개인정보 접속 기록을 관리하고, 이를 규제하기 위한 각종 컴플라이언트들을 끊임없이 이해하고 따라가야 합니다.
Log Catch는 기업내 관리해야 할 대상 서버와 데이터베이스 자산을 탐색하고, 데이터베이스 내에 개인정보를 자동으로 식별합니다.

WAS를 통해 개인정보가 저장된 데이터베이스에 대한 작업을 로그로 수집하고, 개인정보 사용을 분석하여 개인정보 접속 기록 생성 및 보안관점의 감사로그와 다양한 통계 정보를 제공합니다. 또한 이상 징후를 식별하고 관리자에 실시간으로 알림, 소명관리 기능을 제공함으로써, 보안관리자가 개인정보 접속기록 관리 및 보안 관리까지 할 수 있도록 도와드립니다.

WHY Log Catch

- 3Tier 환경에서 다수의 WAS로부터 실시간 로그를 수집
- 5W1H 육하원칙 기준으로 수집 로그 가공 저장 및 검색
- 다양한 통계 정보와 보안관점의 대시보드 정보 제공
- 개인정보보호 컨플라이언스 기준 다양한 보고서 제공
- 이상 징후(대량 정보조회) 탐지 및 알림, 소명 기능 제공
- Server, DBMS 자산탐색 및 Database내 민감정보 식별

02

민감정보 접속기록 관리는
어떻게 하고 있습니까?

Log Catch KEY FEATURES

Log Catch는 개인정보 접속기록 관리 대상이 되는 시스템을 자동 탐색하고, 개인정보를 식별 합니다. WAS Agent를 통해 개인정보에 대한 작업을 수집로그로 저장하고, 이를 분석하여 다양 한 가공 로그를 생성하여 통계 정보와 보안경보를 제공하는 통합로그관리 솔루션입니다. 또한 웨어밸리의 DB 접근제어 솔루션과의 연동으로 DB접근제어 솔루션의 감사로그를 분석하여 개인 정보 접속기록을 생성할 수 있습니다.

자산 탐색

엔터프라이즈 환경에서 운영되고 있는 자산을 탐색하여, 서버와 데이터베이스를 식별하여 로그 수집 대상으로 등록하여 관리합니다. 또 스케줄러를 설정하여 주기적으로 탐색함으로써 새로운 서비스의 출현을 감지하고 로그수집 대상으로 식별하는 업무를 지원합니다.

개인정보 / 민감정보 식별

개인정보를 가진 민감정보 위치를 파악하고 지속적으로 관리하는것은 정보보안 활동의 가장 중요한 업무입니다. Log Catch는 개인정보 접속기록의 대상인 데이터베이스내의 개인정보 저장 항목을 식별 하여 등록할 수 있도록 지원하며, 자동화된 스케줄러를 지원해 개인정보의 추가/삭제 등의 변경 추이를 관리합니다.

Database	Oracle, Microsoft SQL Server, IBM DB2, Sybase ASE/IQ, MySQL, MariaDB, PostgreSQL, Tibero, Altibase, PetaSQL

개인정보 접속기록 생성 및 관리

WAS 시스템을 통해 DBMS 저장된 개인정보에 누가, 언제, 어디서 접근하고 변경한 작업 로그를 실시 간으로 수집하고, 저장된 로그를 5W1H(육하원칙)에 따라 분석·가공하여 개인정보 사용에 대한 접속기록 생성 및 다양한 통계정보를 생성합니다.

Log Catch가 수집하여 분석 제공하는 접속 기록의 유형은 아래와 같습니다.

개인정보 접속기록	접속시간, 업무 시스템, 사용자 아이디와 IP 주소, 소속, 접속URI, 쿼리, 쿼리를 통해 조회된 정보, 조회된 개인정보의 rows수, 개인정보 칼럼명, 쿼리 결과에 포함된 개인정보 유형(패턴)정보
통계 정보	통계 종합 리포트 및 및 개인정보 접속기록 리포트를 출력, 정기적인 보고서 출력을위한 스케줄러를 제공합니다.

실시간 위험 탐지 및 경보

보안경보 정책 설정을 통해 실시간으로 개인 정보 사용에 대한 위험 탐지 및 경보를 발생시켜 관리자에 알림 기능을 제공합니다. 조회건수 설정을 통한 등급별 과다조회, 업무시간외 접근, 미등록 사용자 계정, 미등록 사용자 IP를 통한 개인정보 조회, 미등록 메뉴/기능/URI를 통한 개인정보 접근에 대해 경보를 발생합니다.

이상 징후 및 소명 관리

분석한 개인정보 접속기록을 3 Sigma rule 기법을 통한 기간(24시간, 주, 월, 년)별 통계데이터 학습을 통해 이상 징후를 감지하고 관리자에게 알림 기능을 제공합니다. 이상 징후를 발생시킨 사용자에게 자동 소명 요청 및 관리 기능을 제공하여, 보안 관리자가 개인정보 자산에 대한 보안 측면의 관리가 가능 하도록 도와줍니다.

보고서 제공

개인정보 접속기록에 대한 통계 보고서 및 종합 보고서를 제공하며, 정기적인 보고서 생성을 위한 스케줄링 기능을 제공한다.

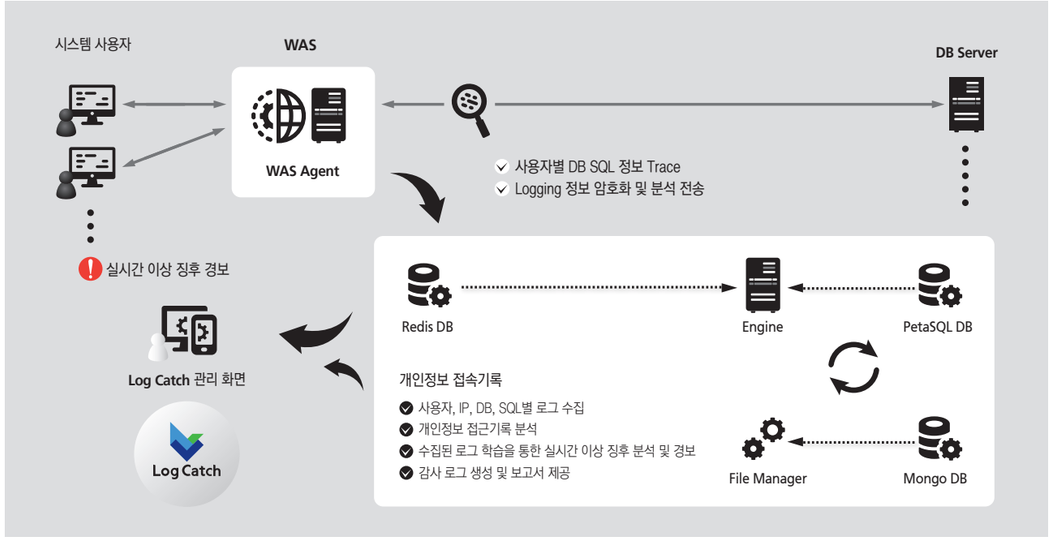
시스템 자원 모니터링

로그수집대상 시스템과 Log Catch 서버의 시스템 자원(CPU, Memory, Disk) 모니터링 기능과 주요 프로세스에 대한 health check 기능을 제공합니다. 또한 Log Catch 서버의 개인정보 수집 로그와 감사 이력을 저장하기 위한 디스크 공간에 대한 모니터링 기능을 제공하여, 개인정보 접속 이력 로그와 시스템 운영에 대한 감사로그 유실 방지 기능을 제공합니다.

개인정보 접속기록의 안전한 보관

개인정보 접속기록에 포함된 개인정보의 안전한 보관을 위해, 민감정보를 암호화하여 데이터베이스에 저장합니다.

Log Catch FLOW



PROTECT
YOUR
EVERYDAY
INFO

Log Catch 구성 및 운영환경

구성 방식

Log Catch Agent는 로그수집대상 WAS에 설치하여 운영됩니다. 따라서 수집대상 WAS가 다수인 경우, 다수의 Log Catch Agent가 로그를 수집하여 한대의 Log Catch Server로 수집로그를 전송하는 형태로 구성할 수 있습니다.

로그수집 에이전트	WAS를 통한 데이터베이스 접속 및 작업에 대하여 실시간 로그를 수집합니다.
관리 콘솔	수집대상 데이터베이스 및 WAS 업무시스템 관리를 수행할 수 있으며, 분석한 개인정보 접속 이력 및 보안 경보를 조회할 수 있습니다. 실시간 대시보드를 통해 통계 정보를 확인하고 이상징후 현황 실시한 모니터를 통해 보안경보를 확인함으로써 실시간 보안성 확보를 제공합니다.
탐색 에이전트	탐색 에이전트는 다음 기능을 지원합니다. · 서버/데이터베이스 탐색 · 개인정보/민감정보 탐색
분석처리 엔진	Log Catch Agent 가 수집한 로그를 분석하여, 개인정보 접속기록 생성 및 통계정보, 보안 경보를 생성합니다. 3 Sigma 통계를 이용한 데이터 학습을 통해 이상징후 경보를 발생합니다.
리포트 출력 에이전트	통계 종합 리포트 및 및 개인정보 접속 기록 리포트를 출력, 정기적인 보고서 출력을 위한 스케줄러를 제공합니다.

운영 환경

Log Catch Agent	Java 기반 WAS 시스템(Java 1.6 이상) Tomcat 5.5 이상, RedHat Jboss Application Server 6.x 이상, WebLogic 8.x 이상, WebSphere 6.x 이상, Tmaxsoft JEUS 4.x 이상, Resin 3.x 이상, Windows IIS .NET 4.0 이상
Log Catch Server	CentOS 7.7 64 (Linux Kernel 3.10.0), JRE v1.8, Apache Tomcat v8.5
관리자 PC	Chrome 80.0