LogCenter

Log Life cycle 전 과정을 관리부터
이상징후 탐지까지 해결!

로그수집/로그모니터링에서 통합 분석까지 한 번에!
통합로그 관리를 통한 시스템/보안 관리 및 IT컴플라이언스 준수를 가능하게
해주는 최적의 SIEM(Security Information & Event Management)시스템

제조사 : ㈜이너버스

LogCenter

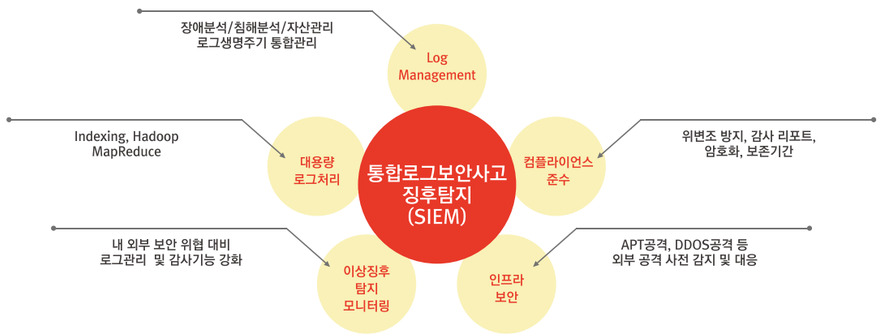
도입배경

기업은 왜 통합로그관리 시스템을 도입해야 하는가?

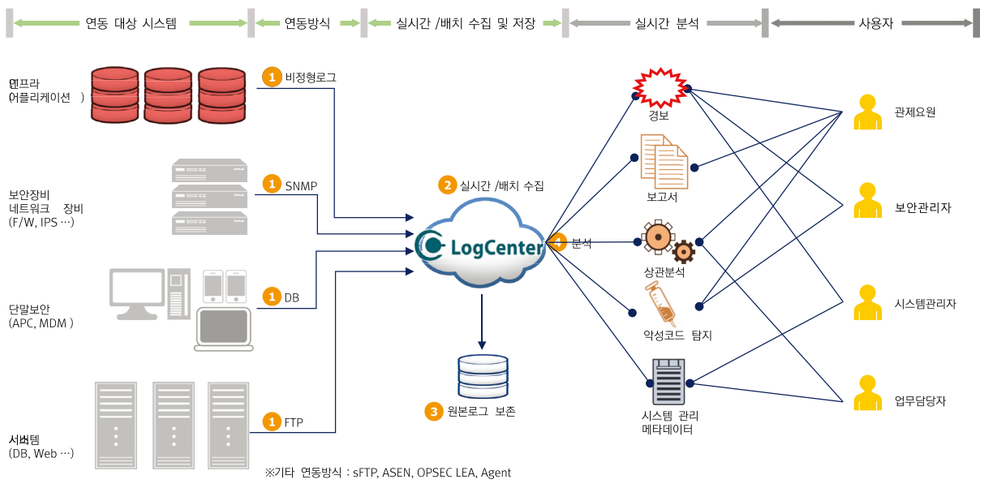
최근 기업은 로그 분석을 통한 효율적인 분석과 모니터링에 많은 어려움을 겪고 있습니다.

- 대용량/이기종 로그의 수집 및 관리
- 컴플라이언스 준수 사항 대응
- 로그분석을 통한 활용 및 이상징후 탐지

시장요구 사항



구성도



주요 기능

수집 및 저장	원본 로그의 위변조 방지	보고서	다양한 형태의 보고서
검색	지능형 고속 검색	관리	강력한 권한 관리
분석	문법을 활용한 다차원 상관분석	협업	보안 이슈 증적관리 및 협업
모니터링	사용자정의 시각화 보드	컴플라이언스 준수	상관분석 모니터링

특장점

아키텍처 (Architecture)	대용량 데이터의 처리기술 빠른속도 및 정합성 Hyper Full-Text Indexing 기술적용 로그데이터의 모든 키워드 를인덱스 파일로 저장 장비 1대로 1일 대용량로그(200GB) 처리 지원	시각화 및 컨텐츠	사용자 관점의 유연한 V-Board 다양한 위젯, 세부 탐지 직관적인 Topology Map 다양한 콘텐츠가 포함된 위젯 마켓 콘텐츠의 지속 업데이트 Know-how가 포함된 룰/시나리오 협업과 연계 한 차세대 모니터링 기술적용
협업	처리 내역 증적관리 모니터링 내역에 대한 보안 증적관리 장애 및 사고 처리에 대한 협업 알람 항목의이슈트레킹 유관 부서 또는 담당자의 협업 체계		

도입효과

LogCenter는 BigData처리, 상관분석 기술을 융합하여 로그관리 및 이상징후 탐지 기술을 제공합니다.

컴플라이언스 준수 및 보안 정책 강화

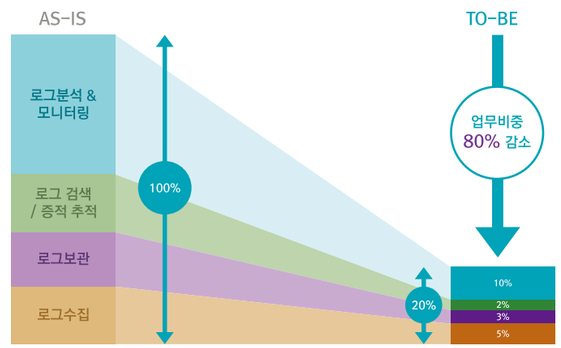
- 개인정보보호법,정보통신망법 등 각종 법률 및 가이드라인 준수
- 서비스 장애 발생 시 고속검색을 통한사후감사 체계 확보
- 로그의 위변조방지를 위한 무결성 및기밀성 보장

IT 인프라 운영 효율 개선

- 다양한 수집방식을 이용한 로그 수집
- 대용량 로그의 고속 검색으로신속한 대응 체계 정립
- 보안 이벤트 및 로그 통합으로로그 관리의 효율성 향상
- 로그 관리의 자동화 구현

대용량로그 처리 기반 분석 /모니터링 기틀 확립

- 중요 로그에 대한 라이프 사이클 관리
- 실시간 분석 환경 구현 및 로그 현황 모니터링
- 이기종 로그의 효율적 분석을 위한 탐지정책 지원
- 보안사고 시 법적인 증거 및 감사자료 제시



기존 로그관리 업무를 최소 1/5(20%)로 획기적으로 감소시킵니다.