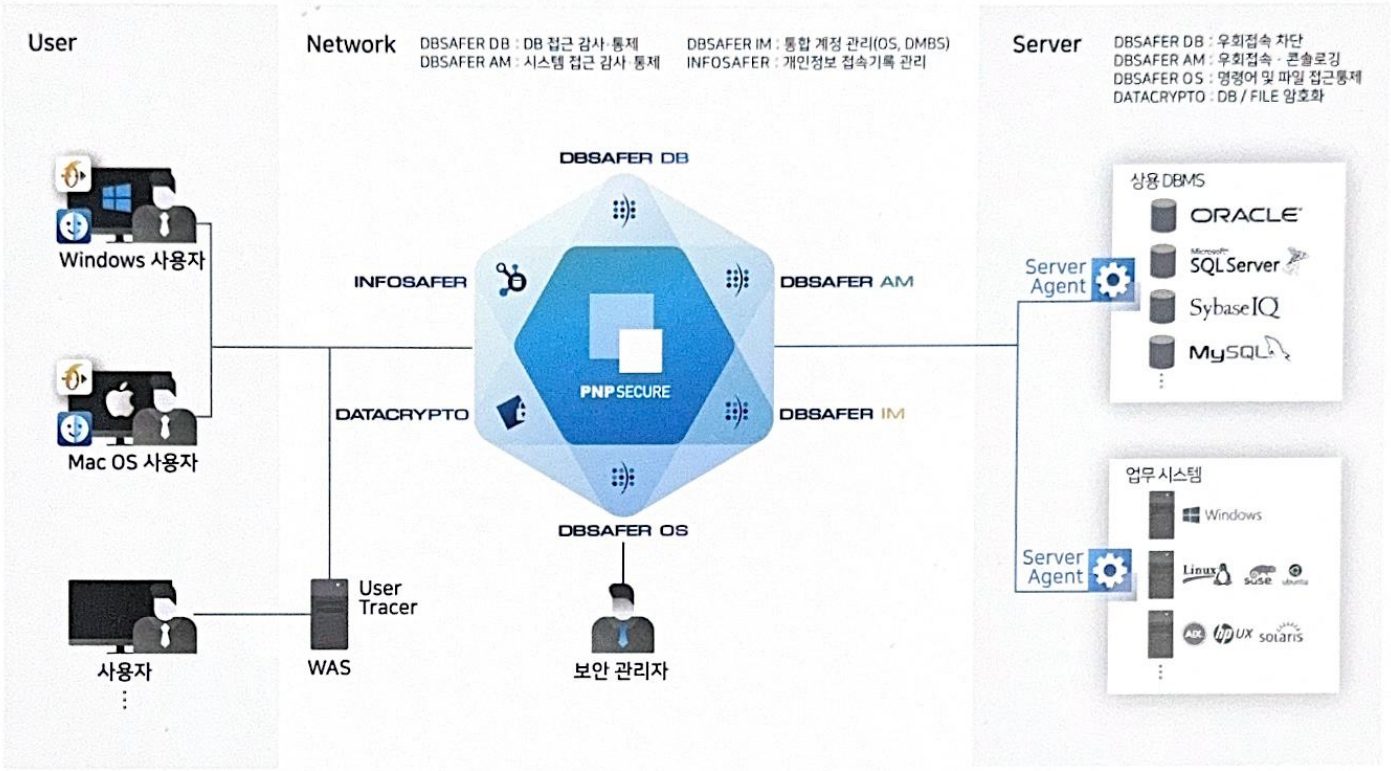
강화된 개인정보보호 관련 법률 등 다양한 컴플라이언스 충족

국내 · 외 5,000여 고객사에서 검증된 독보적인 기술력과 안정적인 기술지원

국내 최초 Unified-IAM(U-IAM, 통합 계정 및 접근 제어) 개념의 솔루션

제품 구성

(주)피앤피시큐어는 대한민국 최초의 DB보안 솔루션인 DBSAFER를 시작으로 다양하고 독보적인 기술을 탑재한 정보보안 솔루션을 개발했습니다. 최근 강화되고 있는 정보보안 컴플라이언스는 과거와 같이 DB 한 부분에 국한된 것이 아니라 보호 대상인 PC와 Network 그리고 Server 등 유기적으로 연계된 모든 분야를 대상으로 하고 있어 보안 제품으로 하여금 고도의 기술력을 갖추도록 요구하고 있습니다. (주)피앤피시큐어는 정보보안 관련 컴플라이언스와 클라우드 등 최신 업무시스템을 만족하는 뛰어난 기술력을 바탕으로 각종 서버와 DB서버에서 생성·저장되는 정보를 보호하고, 유통 · 가공하는 구간까지 통제하는 Unified-IAM(U-IAM, 통합 계정 및 접근 제어) 솔루션을 개발 · 공급하고 있습니다.



주요 연혁

(주)피앤피시큐어는 최고 수준의 정보보안 전문가와 개발자들이 세계 최고의 정보보안 솔루션을 개발 및 공급하고자 설립했습니다. 오늘날 세계 시장은 네트워크 환경을 기반으로 E-Business를 경쟁적으로 확대함으로써 새로운 정보보안 시장을 형성해가고 있습니다. 이에 (주)피앤피시큐어는 전 세계에서 정보보안의 표준으로 신뢰할 수 있는 솔루션을 개발·공급하는 기업으로 나아가고 있습니다.

2020~2022
국제 정보보안의 표준
- 청년 친화 강소기업 6년 연속 선정
- 장영실 기술혁신상, SW산업발전유공 국무총리 표창 수상
- DBSAFER OS V7.0 AIX 7.2 외 3건의 국제공통평가기준(CC) 인증 획득

2018~2019
대한민국 정보보안의 대명사
- 장영실상, 과학의날 대통령 표창, 과과학기술진흥유공자 장관 표창 수상
- 신기술 실용화 유공기업 국무총리상, 대한민국 ICT 대상 수상
- INFOSAFER V1.1 국제공통평가기준(CC) 인증 획득

2014~2017
DB 보안을 넘어 정보보안 다각화
- INFOSAFER, DATACRYPTO, DBSAFER OS 등 신제품 출시
- DBSAFER Enterprise V5.0 국제공통평가기준(CC) 인증 획득
- 과학의 날 대통령 표창, 신기술실용화 국무총리 표창, 모범납세자 국세청장 표창

2009~2013
대한민국 DB 보안의 선두
- 모범중모범중소기업 표창, 장영실상 수상
- 발명의 날 발명진흥회장상, 신기술실용화 지식경제부 장관상 수상
- DBSAFER V3.0 국제공통평가기준(CC) 인증 획득

2003~2008
대한민국 DB 보안의 시작
- [특허등록] <데이터베이스 감시 및 보안방법 및 장치>
- 세계 최초 <게이트웨이방식의 DB보안프로그램> DBSAFER V1.0 출시
- (주)피앤피시큐어 설립

PNPSECURE

CC인증 GS인증 특허등록

- **내부회계관리제도**(신외감법) 만족
- **개인정보 보호법** 만족
- **전자금융감독규정** 만족(금융위원회 고시)
- **ISMS, ISMS-P 인증 요건** 만족

DB 접근제어(통제) | 디비세이퍼 DB

DBSAFER DB의 필요성 디비세이퍼 DB(DBSAFER DB)는 최신 정보보안 관련 법률을 완벽히 준수합니다.

개인정보의 안전성 확보조치 기준(행정안전부 고시)

· 제4조(내부관리계획의 수립·시행) 개인정보의 안전한 처리를 위하여 내부관리 계획 수립 · 시행 필요
· 제5조(접근 권한의 관리) 권한 부여, 변경 또는 말소에 대한 내역 기록과 안전한 패스워드 관리 설정 필요
· 제6조(접근 통제) 접속 권한 제한 및 불법 접속 탐지
· 제7조(개인정보의 암호화) 개인 정보 암호화 및 네트워크 구간 암호화
· 제8조(접속기록의 보관 및 점검) 접속 기록에 대한 위 · 변조 방지

전자금융감독규정(금융위원회 고시)

· 제27조(전산원장 통제) 전산원장에 대한 변경 전 · 후 내용 자동기록 및 보존

DBSAFER DB의 개요

디비세이퍼 DB(DBSAFER DB)는 국내 시장 점유율 1위인 최고의 데이터베이스 접근제어 솔루션으로 개인정보 DB에 대한 접근 및 권한 통제, SQL 감사 및 로깅 등을 통해 개인정보 유출을 사전에 차단하고 발생 위험을 최소화합니다.

관련 컴플라이언스 100% 만족

- 내부회계관리제도(신외감법) 요건
- 개인정보보호법 시행령
- 전자금융감독규정
- ISMS, ISMS-P 인증 요건

접속 / 권한 제어

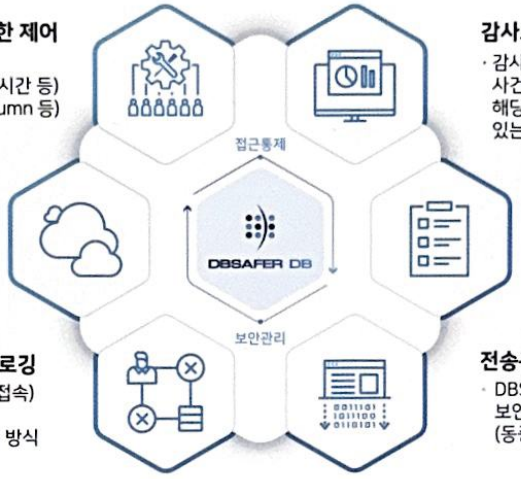
- 다양한 DBMS에 대한 접근을 중앙 관리
- 접근제어 (사번, IP, Application, DB계정, 시간 등)
- 권한제어 (DDL/DML/DCL 구문, Table/Column 등)

다양한 Cloud 환경 지원

- 멀티 클라우드 지원 (AWS, MS Azure, NAVER Cloud 등)
- On-Premise와 Cloud 환경 동시 지원 (Hybrid 방식)

우회접속 차단 및 로깅

- Gateway를 통하지 않는 우회접속(비인가접속) 차단 및 로깅
- 전산(장비)실 내에서 직접 콘솔로 접근하는 방식 차단 및 로깅



감사로깅 및 실시간 모니터링

- 감사데이터에 대하여 실시간 모니터링을 제공하며, 특정 사건에 대한 로그 분석 시에 다양한 관점에서 신속하게 해당 시점의 로그에 접근하여 정확한 자료를 확인 할 수 있는 환경을 제공

보고서 및 결재시스템 제공

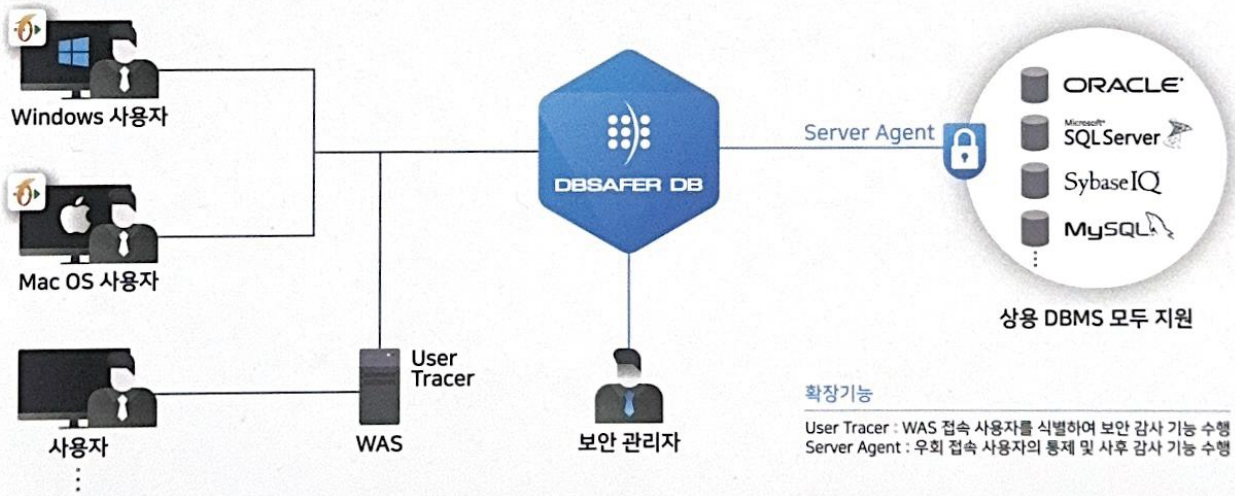
- 다양한 보고서(약 93종)를 탬플릿을 제공하여 각종 컴플라이언스에 맞춤 대응
- 결재시스템을 통하여 User ID/User IP 및 Table 단위의 조건을 조합하여 쿼리를 결재하는 기능을 제공하며, 사용자가 요구하는 내역에 대한 이력보고서를 생성

전송구간 암호화

- DBSAFER는 사용자 PC와 DBSAFER, DBSAFER와 보안대상서버의 통신 전구간에 암호화 기능을 제공 (동종업계 중 유일, 전구간 암호화 통신 제공)

DBSAFER DB의 구성

디비세이퍼 DB(DBSAFER DB)는 다음과 같은 구성을 통하여 강력한 DB 접근제어 기능을 제공합니다.



확장기능

User Tracer : WAS 접속 사용자를 식별하여 보안 감사 기능 수행
Server Agent : 우회 접속 사용자의 통제 및 사후 감사 기능 수행

DBSAFER DB의 특장점

- DBSAFER AM(시스템 접근제어)와 함께 사용할 경우 통합 접근제어가 가능하며, 통합 정책 설정, 통합 로그 관리 기능 제공
- 클라우드 환경에서 운영을 지원하며, 다양한 클라우드 DB서비스 지원 (Aurora, DynamoDB, RDS, RedShift 등)
- E-mail, SMS, OTP를 이용한 2차 인증
- 서버 내 개인정보의 자동 추적 및 식별을 통한 보안정책 적용의 자동화
- 중요 보안 대상 서버에 대한 직접 또는 우회 접근 차단 (서버to서버, DB링크 등)
- Server Agent를 이용하여 보안 서버를 우회하는 콘솔 또는 원격 접속자에 대한 통제
- 워크플로우를 통한 전산원장의 사전, 사후 감사
- 감사 로그 데이터 암호화 저장 및 저장 데이터의 무결성 보장

PNPSECURE

특허등록

- **내부회계관리제도**(신외감법) 만족
- **개인정보 보호법** 만족
- **전자금융감독규정** 만족(금융위원회 고시)
- **ISMS, ISMS-P 인증 요건** 만족

SYSTEM 접근제어(통제) | 디비세이퍼 AM

DBSAFER AM의 필요성 디비세이퍼 AM(DBSAFER AM)은 각종 보안 법률을 완벽히 준수합니다.

개인정보의 안전성 확보조치 기준(행정안전부 고시)

- 제4조(내부관리계획의 수립·시행) 개인정보의 안전한 처리를 위하여 내부관리 계획 수립·시행 필요
- 제5조(접근 권한의 관리) 권한 부여, 변경 또는 말소에 대한 내역 기록과 안전한 패스워드 관리 설정 필요
- 제6조(접근 통제) 접속 권한 제한 및 불법 접속 탐지
- 제7조(개인정보의 암호화) 개인 정보 암호화 및 네트워크 구간 암호화
- 제8조(접속기록의 보관 및 점검) 접속 기록에 대한 위·변조 방지

DBSAFER AM의 개요

디비세이퍼 AM(DBSAFER AM)은 사용자의 권한별 시스템 접근제어 및 작업 이력 감사 등을 수행하는 솔루션으로 DBSAFER DB (DB 접근제어)와 연동하여 서버에 접근하는 모든 행위에 대해 강력한 시스템 접근제어 기능을 수행합니다.

관련 컴플라이언스 100% 만족

- 내부회계관리제도(신외감법) 요건
- 개인정보보호법 시행령
- 전자금융감독규정
- ISMS, ISMS-P 인증 요건

접속 / 권한 제어

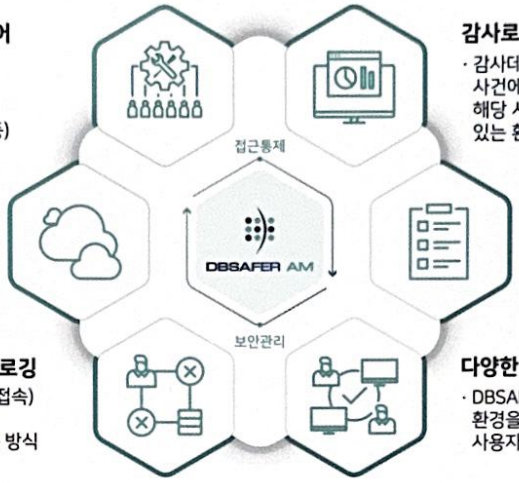
- Windows 터미널 (RDP/윈도우원격접속)
- Unix/Linux 터미널 (TELNET/SSH/시리얼포트/로컬 콘솔 등)
- 파일 전송 서비스 감시/제어 (FTP/SFTP 등)

다양한 Cloud 환경 지원

- 멀티 클라우드 지원 (AWS, Azure, Toast, NBP 등)
- On-Premise와 Cloud 환경 동시 지원 (Hybrid 방식)

우회접속 차단 및 로깅

- Gateway를 통하지 않는 우회접속(비인가접속) 차단 및 로깅
- 전산(장비)실 내에서 직접 콘솔로 접근하는 방식 차단 및 로깅



감사로깅 및 실시간 모니터링

- 감사데이터에 대하여 실시간 모니터링을 제공하며, 특정 사건에 대한 로그 분석 시에 다양한 관점에서 신속하게 해당 시점의 로그에 접근하여 정확한 자료를 확인 할 수 있는 환경을 제공

보고서 및 결재시스템 제공

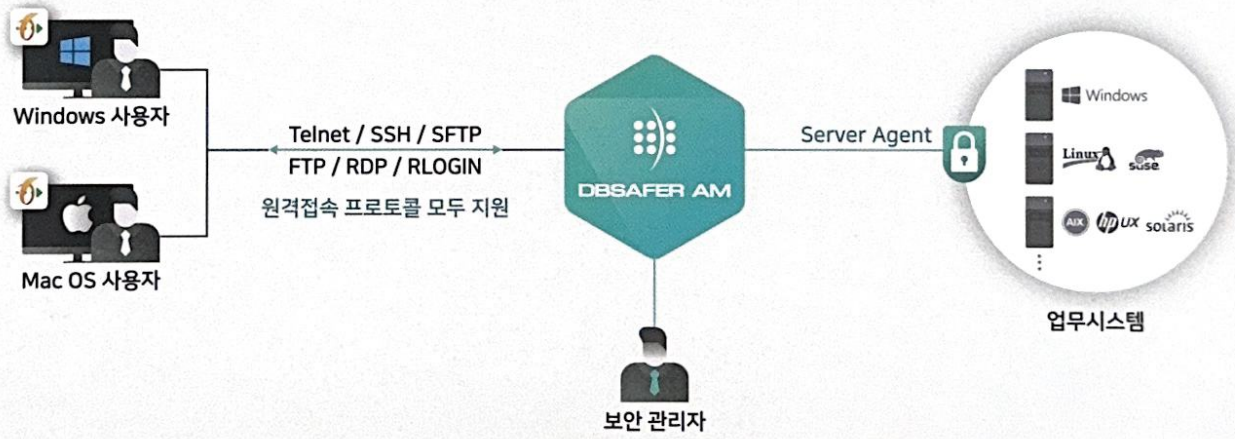
- 다양한 보고서(약 93종)를 탬플릿을 제공하여 각종 컴플라이언스에 맞춤 대응
- 결재시스템을 통하여 User ID/User IP 및 Table 단위의 조건을 조합하여 쿼리를 결재하는 기능을 제공하며, 사용자가 요구하는 내역에 대한 이력보고서를 생성

다양한 접속 환경 지원

- DBSAFER Enterprise는 기존의 접속 프로그램이나 환경을 변경하지 않는 C/S(PC NAT)방식과 Web을 통한 사용자 접속 방식 모두를 제공

DBSAFER AM의 구성

디비세이퍼 AM(DBSAFER AM)은 다음과 같은 구성을 통하여 강력한 시스템 접근제어 기능을 제공합니다.



DBSAFER AM의 특장점

- DBSAFER DB(DBMS 접근제어)와 함께 사용할 경우 통합 접근제어가 가능하며, 통합 정책 설정, 통합 로그 관리 기능 제공
- Windows Terminal(RDP), TELNET/SSH, Console등의 접속 로그에 대해 사용자 화면과 동일한 화면을 재현하는 기능과 보안사고시 메타 검색 기능 제공
- 서버 접속 관리 및 자동 로그인
- 클라우드 환경에서 운영을 지원하며, 다양한 클라우드 기능 지원 (Auto Scaling, Elastic IP 등)
- E-mail, SMS, OTP를 이용한 2차 인증
- 실시간 사용자에 대한 동영상 다중 모니터링 및 세션 통제
- 데이타마스킹 및 전송구간 암호화 제공
- 중요 보안대상 서버에 대한 직접 또는 우회접근 차단
- 사용자에 대한 접속 및 명령어 결재
- 보안 서버를 우회하는 콘솔 또는 원격 접속자에 대한 통제 및 로깅

PNPSECURE

GS인증 특허등록

- **내부회계관리제도**(신외감법) 만족
- **개인정보의 안정성 확보조치 기준** 만족(행안부)
- **ISMS, ISMS-P 인증 요건** 만족
- **금융회사 정보기술**(IT)부문 **보호업무 모범규준**
- **정보 통신 보안업무 규정**

통합 계정 관리 | 디비세이퍼 IM

DBSAFER IM의 필요성 OS 계정 및 DBMS계정의 생성, 변경, 삭제등의 계정의 Life Cycle에 대한 감사 자료를 생성 및 관리에 위한 최신 정보보안 관련 법률을 준수

개인정보의 안전성 확보조치 기준(행정안전부 고시)

- 제4조(내부관리계획의 수립·시행) 개인정보의 안전한 처리를 위하여 내부관리 계획 수립·시행 필요
- 제5조(접근 권한의 관리) 권한 부여, 변경 또는 말소에 대한 내역 기록과 안전한 패스워드 관리 설정 필요
- 제6조(접근 통제) 접속 권한 제한 및 불법 접속 탐지
- 제8조(접속기록의 보관 및 점검) 접속 기록에 대한 위·변조 방지

정보 통신 보안 업무 규정

- 제27조(사용자계정 관리) 계정 관련작업시 승인절차 필요. 불법접속 방지
- 제28조(비밀번호 관리) 접근용 비밀번호, 사용자인증, 자료별 비밀번호 관리 필요

금융회사 정보기술(IT)부문 보호업무 모범규준

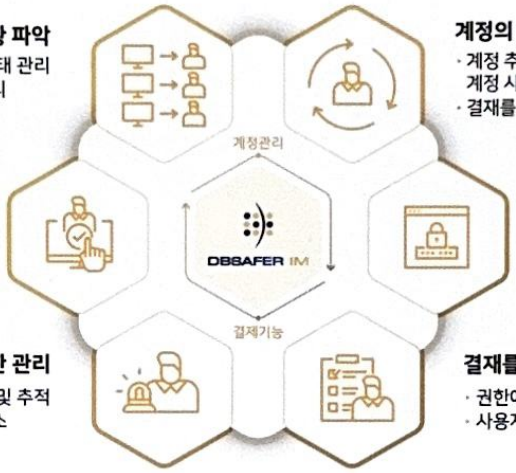
13. 정보기술부문 내부통제
⑨(내부사용자비밀번호관리) 비밀번호를 부여하고 분기 1회 이상 변경 필요

DBSAFER IM의 개요

디비세이퍼 IM(DBSAFER IM)은 불특정 다수인 관리 대상 서버의 OS 계정 및 DBMS 계정을 중앙에서 통합 관리하는 솔루션으로 계정의 Life Cycle을 관리하며, 계정을 이용하는 사용자의 접근에 대해 신청과 승인의 자동화를 통한 Work-Flow를 제공하여 조직 내 시스템의 효율적인 내부 통제를 실현합니다.

관련 컴플라이언스 100% 만족

- 내부회계관리제도(신외감법) 요건
- 개인정보의 안전성 확보조치 기준
- ISMS, ISMS-P 인증 요건
- 금융회사 정보기술(IT)부문 보호업무 모범규준
- 정보 통신 보안 업무 규정



장비 별 계정 현황 파악
- 보호대상서버 OS 및 DBMS의 계정 상태 관리
- 이상, 만료, 휴면 계정 상태 확인 및 관리

계정의 Life-Cycle 관리
- 계정 추가, 사용, 삭제, 비밀번호 변경등 계정의 전반적인 계정 사이클 관리
- 결재를 통해 계정 관리 및 사용 권한 관리

자동접속 기능 제공
- 비밀번호 노출 없이 클릭시 자동으로 접속
- TELNET/SSH/SFTP/FTP/RDP 프로토콜 등 지원

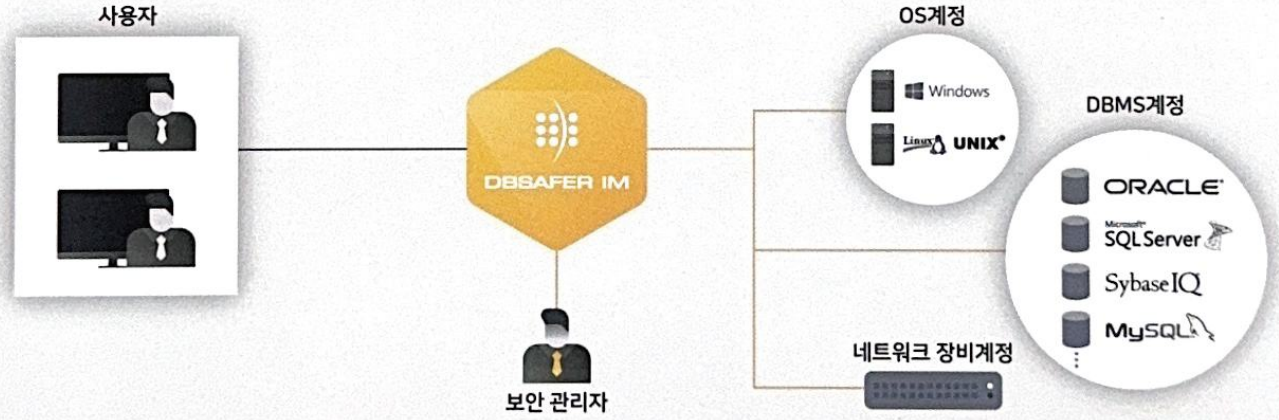
패스워드 관리 기능
- 서버별, 계정별, 계정 유형별 다양한 비밀번호 정책 설정
- 스케쥴링 기능을 통한 주기적인 비밀번호 변경
- 스크립트 기반의 유연한 비밀번호 규칙 설정

사용자 별 권한 관리
- 사용자별 접근 권한의 부여, 변경 및 추적
- 사용자 변경 사항에 따른 권한 말소

결재를 통한 사용자별 계정 발급
- 권한에 따른 사용자별 계정 권한 신청 및 결재
- 사용자 권한 신청에 대한 근거 기록 및 보관

DBSAFER IM의 구성

디비세이퍼 IM(DBSAFER IM)은 다음과 같은 구성을 통하여 통합 계정 관리 기능을 제공합니다.



DBSAFER IM의 특장점

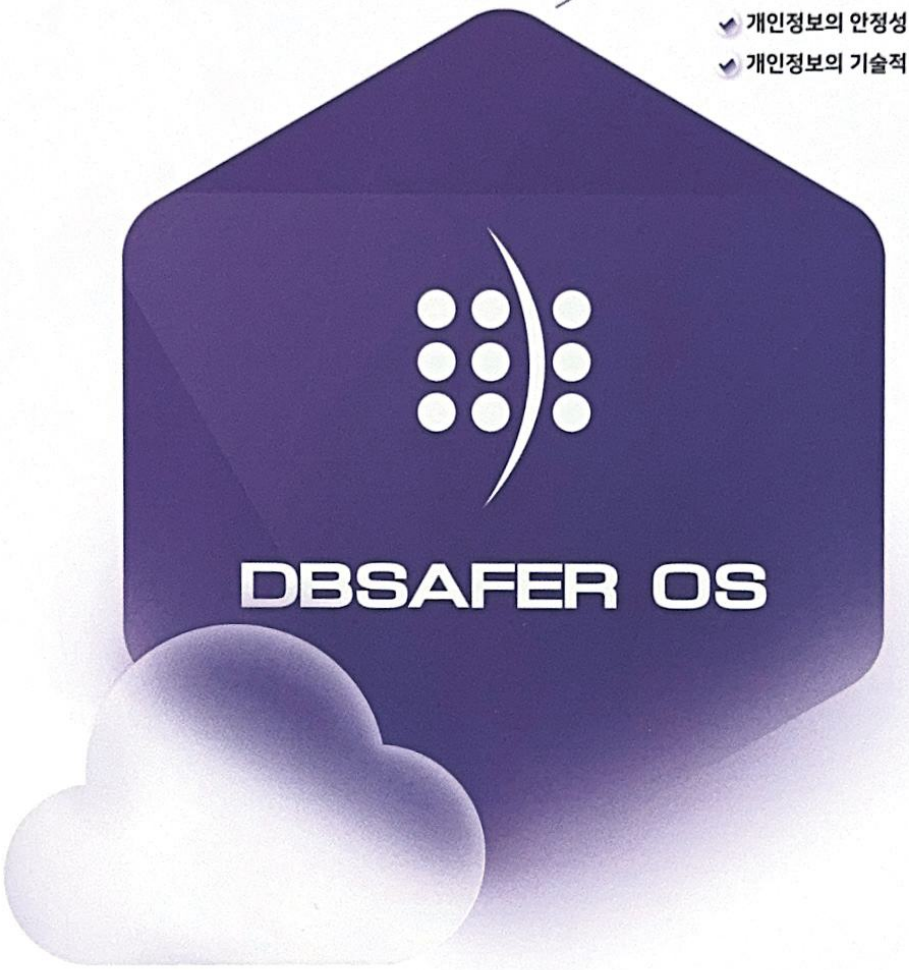
- 관리자의 업무를 최소화, 보안성 향상을 위하여 서버, DBMS, 네트워크 장비 등 이기종 장비의 계정을 자동으로 수집 및 동기화하여 통합 관리
- 불법계정(Ghost / Broken) 및 만료, 휴면 계정 등에 대하여 강력한 관리 기능 제공
- Work-Flow와 연동된 사용자 계정 신청, 업무 상신 및 결재권자 승인 기능 제공
- 정책 기반의 비밀번호 생성 및 스케쥴러에 의한 비밀번호 규칙 관리
- Role을 지원하는 DBMS는 계정의 Role 관리 기능도 같이 제공
- 관리자, 시스템, 일반사용자 계정 등 유형을 구분하여 계정 및 비밀번호 관리
- 특권 계정 관리, 감사 로그, 사용 행위 감사 로그 등을 통해 개인정보보호법, SOX, PCI-DSS, HIPAA, BASELIII 등 다양한 Compliance 준수
- 계정의 비밀번호 노출없이 서버, DBMS에 대한 자동 접속 기능 제공
- 기존 DBSAFER DB 또는 AM과의 서버, 계정에 대한 완벽한 연동 기능 제공

제품문의 sales@pnpsecure.com 대표전화 1670-9295 www.pnpsecure.com

PNPSECURE

CC인증 GS인증 특허등록

- **내부회계관리제도**(신외감법) 만족
- **전자금융감독규정** 만족(금융위원회 고시)
- **개인정보의 안정성 확보조치 기준** 만족(행안부)
- **개인정보의 기술적 관리 보호조치 기준** 만족(방통위)



OS 접근제어(통제) | 디비세이퍼 OS

DBSAFER OS의 필요성 디비세이퍼 OS(DBSAFER OS)는 관리자에 의한 내부 유출을 원천적으로 차단 할 수 있으며, 중요 DATA 유출을 방지 할 수 있습니다.

전자금융감독규정(금융위원회 고시)

- 제13조(전산자료 보호대책) 전산자료 입 · 출력 업무별 접근권한 통제
- 제17조(홈페이지 등 공개용 웹서버 관리대책) 접근통제가 취약한 웹서버 해킹공격 대응 조치
- 제26조(직무의 분리) 업무에 대하여 직무 분리 · 운영

주식회사 등의 외부감사에 관한 법률

- 제8조(내부회계관리제도의 운영 등) ① 회계정보 장부의 관리 방법과 통제 절차
  ② 회계정보를 위조 · 변조 · 훼손 및 파기시 통제 절차

개인정보의 안전성 확보조치 기준(행정안전부 고시)

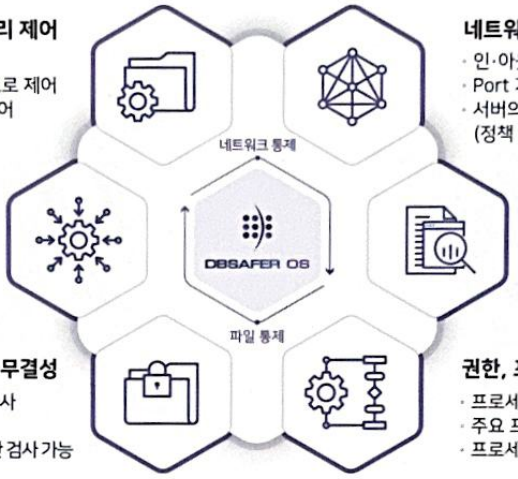
- 제4조(접근권한의 관리) 접근권한을 최소한의 범위로 업무 담당자에 따라 차등 부여
- 제6조(접근통제 시스템 설치 및 운영) 접속 권한을 IP(Internet Protocl)주소 등으로 제한하여 인가 받지 않은 접근을 제한
- 제8조(접근기록의 보관 및 위 · 변조방지) 접속기록의 위 · 변조 및 도난, 분실 방지

DBSAFER OS의 개요

디비세이퍼 OS(DBSAFER OS)는 보호대상 호스트를 다양한 위협에 대한 감시 및 보호를 하는 솔루션으로 서버의 중요 파일에 대한 접근 감시 및 변경에 대한 제어하여 서버의 무결성을 보장할 수 있습니다.

관련 컴플라이언스 100% 만족

- 내부회계관리제도(신외감법) 요건
- 개인정보의 안전성 확보조치 기준
- 전자금융감독규정
- 개인정보의 기술적 관리 보호조치 기준



파일 디렉토리 제어
- 중요 파일/디렉터리에 대한 접근 제어
- 사용자 IP, 계정, 프로세스 등 다양한 조건으로 제어
- READ/WRITE/EXECUTE 등 유형 별로 제어

네트워크 감지 및 통제
- 인·아웃바운드 접속 대한 감지 및 통제
- Port 기반으로 사용자/서버 IP 별 통제
- 서버의 Listen Port 정보를 수집해서 제공 (정책 설정 편의성 제공)

중앙관리
- 다양한 운영체제로 구성된 서버들에 대한 통합 관리
- 정책 배포/로그 수집을 중앙 서버에서 관리

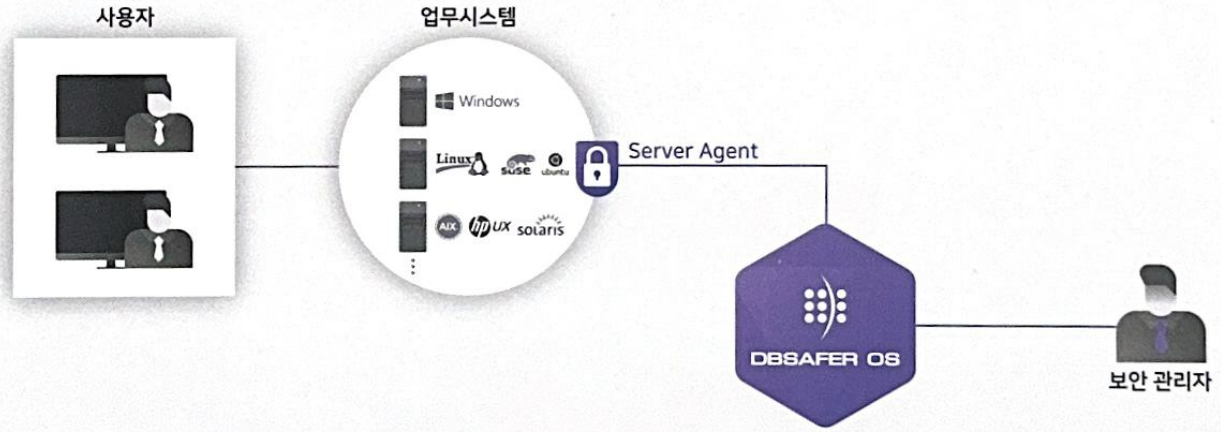
감사 로그 관리
- 중요 파일/디렉터리에 접근한 이력 로깅
- 인·아웃바운드 접속 이력 로깅
- 감사로그 위 , 변조 방지

중요 파일 무결성
- 중요 파일의 위·변조를 확인하는 무결성 검사
- 설정한 주기 별로 무결성 검사 진행
- OS 중요 파일/소스 파일 등 원하는 파일에 대한 검사 가능

권한, 프로세스 관리
- 프로세스/데몬의 강제 종료 방지 기능 제공
- 주요 프로세스 모니터링 기능 제공
- 프로세스 중지 시 자동 실행 기능 제공

DBSAFER OS의 구성

디비세이퍼 OS(DBSAFER OS)는 보호대상 호스트를 다양한 위협에 대한 감시 및 보호를 하는 솔루션으로 서버의 중요 파일에 대한 접근 감시 및 변경에 대한 제어하여 서버의 무결성을 보장 할 수 있습니다.



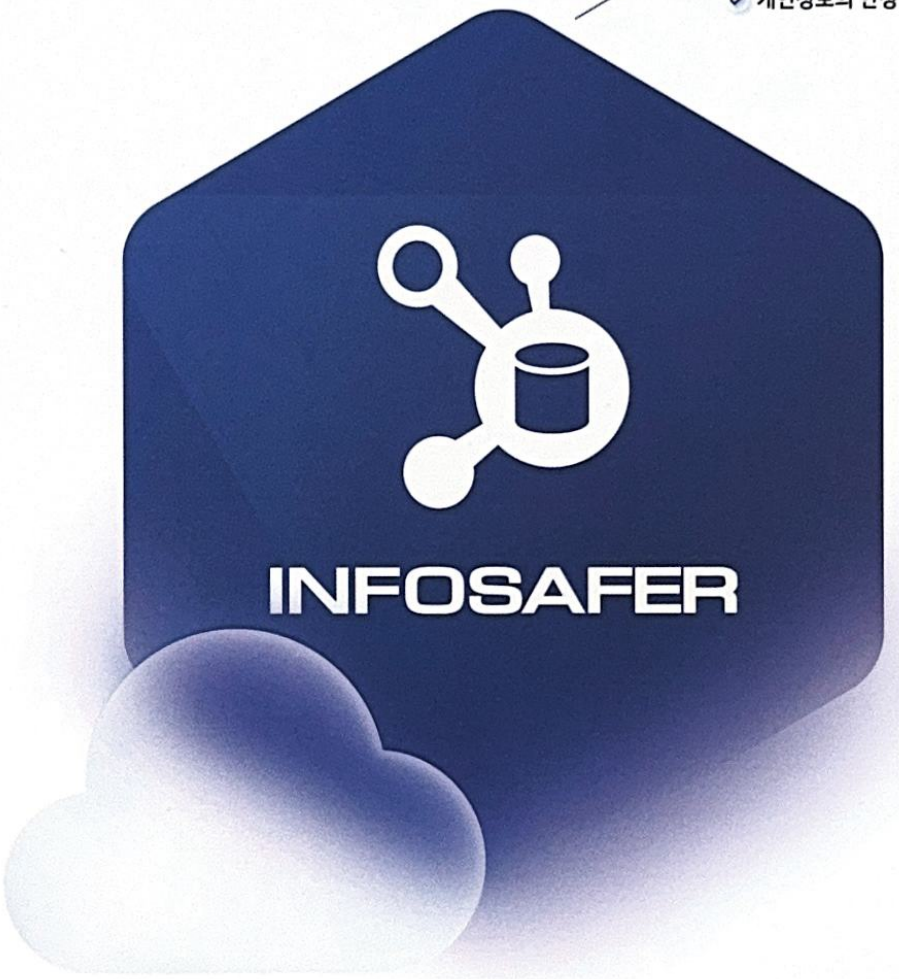
DBSAFER OS의 특장점

- DB, SYSTEM, OS가 통합된 접근제어 솔루션에서 통합 관리하여 효율성, 사용성, 편리성 증대
- 파일 접근에 대한 권한 통제 및 접근 이력에 대한 로그 검색 기능을 제공
- 정책에 따라 사용자별(IP 주소) 접근 통제, 포트 기반으로 인·아웃바운드 통제, 프로세스별 접근 통제
- 특정 디렉토리 또는 파일에 접근한 이력에 대해 감사로그 검색
- 보안장비를 경유하지 않고 접속한 세션 또는 서버에서 외부로 나가는 세션에 대한 감사로그 검색
- 특정 디렉토리 또는 파일에 대한 접근제어
- 명령어 및 프로세스 별 접근
- 사용자별(IP 주소, 접속계정, 보안계정, 실행권한) 접근제어
- 통제 정책에서 예외가 필요한 경우 별도 예외 정책부여 가능
- 인가되지 않은 접속 및 외부로 나가는 세션 통제

PNPSECURE

CC인증 GS인증 특허등록

✔ **개인정보 보호법** 만족
✔ **개인정보의 안정성 확보조치 기준** 만족(행안부)



개인정보 접속기록 관리 | 인포세이퍼 v5.0

INFOSAFER의 필요성 '개인정보의 안정성 확보 조치 기준'에 따르면 접속기록은 불법적인 접근 또는 행동의 확인을 위한 중요 자료로서, 1년 이상 안전하게 보관·관리 및 정기적 점검을 통해 비정상행위에 대해 적절한 조치를 취해야 함을 강조

개인정보의 안전성 확보 조치 기준 2019.6.7. 고시

제4조 | 내부관리계획의 수립·시행 개인정보 보호책임자는 접근권한 관리, 접속기록 보관 및 점검, 암호화 조치 등 내부 관리계획의 이행 실태를 연 1회 이상으로 점검·관리 하여야 한다.

제8조 | 접속기록의 보관 및 점검
① 개인정보처리자는 개인정보취급자가 개인정보처리시스템에 접속한 기록을 **1년 이상 보관·관리**하여야 한다.
② 개인정보처리자는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록 등을 월 **1회 이상 점검**하여야 한다.
③ 개인정보처리자는 개인정보취급자의 접속 기록이 위·변조 및 도난, 분실되지 않도록 해당 접속기록을 안전하게 보관하여야 한다.

개인정보의 안전성 확보조치 기준 해설서

- 개인정보취급자가 개인정보처리시스템에 접속하여 개인정보를 처리한 경우, 수행한 업무 내역에 대하여 식별자, 접속일시, 접속지를 알 수 있는 정보, 수행업무 등의 접속기록을 1년 이상 저장하고 정기적으로 확인·감독하여야 한다.
  - **정보주체에 대한 접속기록까지 보관·관리하고 정기적으로 확인·감독하는 경우 불법적인 접근 및 비정상 행위에 대한 조치 등을 강화**할 수 있다. (정보주체정보 로깅)
- 개인정보처리자는 개인정보의 유출·변조·훼손 등에 대응하기 위하여 개인정보처리시스템의 접속기록을 월 1회 이상 정기적으로 점검 하여야 한다.
  - 이를 통해 **비인가된 개인정보 처리, 대량의 개인정보의 조회, 정정, 다운로드, 삭제 등의 비정상 행위를 탐지하여 적절한 대응조치를 할 필요**가 있다
- 개인정보처리자는 개인정보처리시스템의 접속기록이 위·변조 및 도난, 분실되지 않도록 안전하게 보관하여야 한다.
  - 즉, 정기적으로 접속기록 백업을 수행하여 개인정보처리시스템 이외의 별도의 보조저장 매체나 별도의 저장장치에 보관하는 등의 조치가 필요하다.
  - 접속기록에 대한 위·변조를 방지하기 위해서는 CD-ROM 등과 같은 덮어쓰기 방지 매체를 사용하는 것이 바람직하다.
  - 접속기록을 수정 가능한 매체(하드디스크, 자기 테이프 등)에 백업하는 경우에는 무결성 보장을 위해 위·변조 여부를 확인할 수 있는 정보를 별도의 장비에 보관·관리할 수 있다.

INFOSAFER v5.0의 개요

인포세이퍼(INFOSAFER) v5.0은 개인정보 접속에 대한 감시, 추적, 기록 및 소명기능을 통해 개인정보의 부정사용을 실시간으로 대응하는 정보보안 솔루션입니다.

관련 컴플라이언스 100% 만족

- 개인정보보호법 시행령
- 개인정보의 안전성 확보조치 기준

접속기록의 안전한 보관

- 로그 암호화 및 *WORM 기능을 통한 정보 위/변조 방지
- 감사 로그 원본데이터 사본과 해쉬값을 생성하여 *WORM 영역에 저장
- 원본데이터 훼손 시, 제공되는 유틸리티를 통해 복구
- 유틸리티를 통해 진위성 검증

* WORM(Write-Once Read-Many) 한번 기록된 파일은 삭제하거나 변조할 수 없도록 설계된 스토리지

개인정보 접근에 대한 위험 및 이상 징후 관리

- 개인정보취급자의 평균 개인정보 사용량 분석
- 평균 대비 사용량 증가 시 자동으로 위험사용자 인식 및 알림
- 업무 외 시간, 다중 접속, 권한 외 접근에 대한 경고 기능

소명관리 시스템

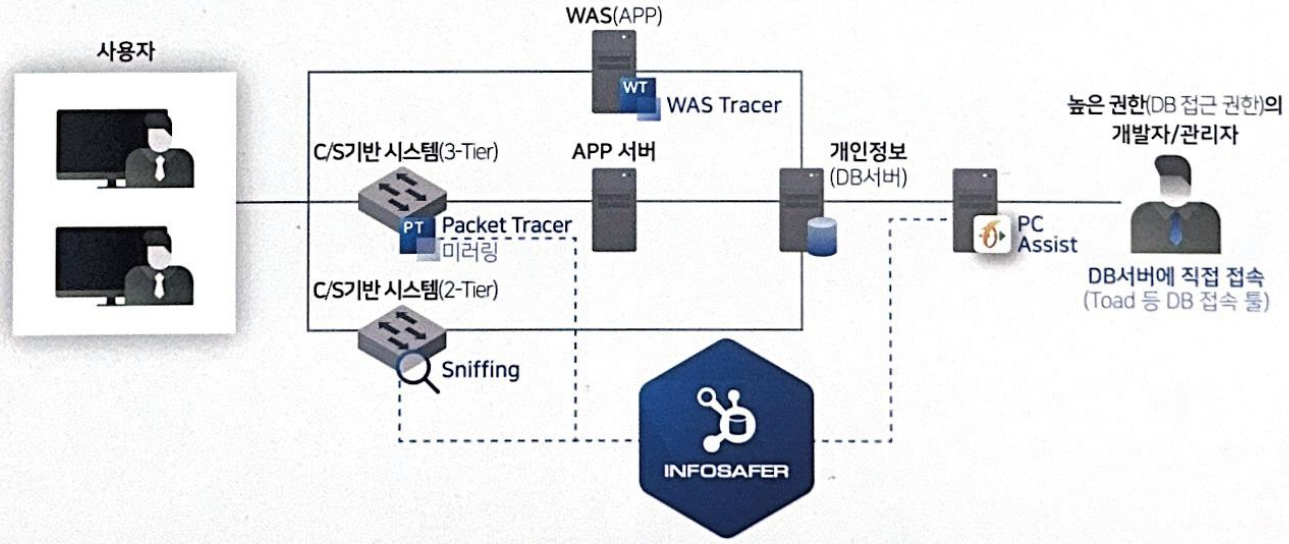
- 개인정보 접근 위험 및 이상 징후 발생 시 사용자 이메일로 소명 요청
- 관리자의 승인/반려/재소명 기능
- 메일 발송 내역에 대해 감사 증적자료로 활용

사용자 다운로드 탐지 및 로깅

- 모든 업무시스템의 다운로드 기록 관리
- WAS Tracer를 통해 쿼리와 파일 다운로드 탐지 매치/분석
- 다운로드 행위 발생 시 파일스캐너로 개인정보 포함 여부 분석
- 다운로드 탐지와 소명 기능 자동 연동

INFOSAFER v5.0의 구성

INFOSAFER v5.0은 어플리케이션 접속 사용자(3-Tier)뿐 아니라 개인정보처리DB에 직접 접속하는 등, 다양한 경로로 접근해 개인정보를 활용하는 기록을 로깅하고 이를 실시간으로 모니터링 및 관리하도록 구성 합니다.



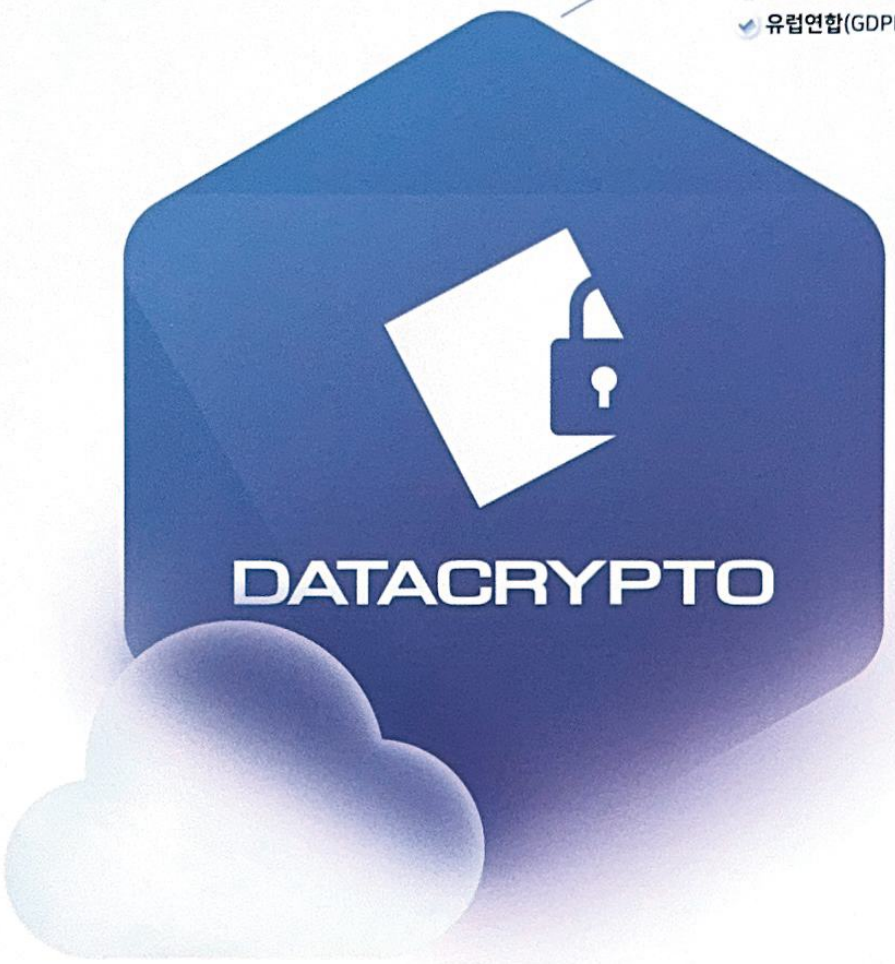
INFOSAFER v5.0의 특장점

- 모든 경로 개인정보 접속이력 완벽 로깅
  - DB 직접 접속 사용자(2-Tier) 기록 수집 / 분석
  - 어플리케이션 접속 사용자(3-Tier) 기록 수집 / 분석
- DBSCANNER 모듈을 통해 개인정보의 위치를 식별
  - 개인정보 자동 검출 / 등록
  - 스케줄링 기능 통한 개인정보 현행화 (오탐 / 괴탐 없는 개인정보접속기록 생성)

PNPSECURE

국가정보원 암호모듈 검증필 GS인증 특허등록

- **개인정보 보호법** 만족
- **개인정보의 안정성 확보조치 기준** 만족(행안부)
- **유럽연합(GDPR) 개인정보 보호법** 만족



DB / FILE 암호화 | 데이타크립토

DATACRYPTO의 필요성 금융 기관의 정보시스템 중 로그, 녹취 및 영상뿐 아니라 대외망을 연결하는 시스템에 저장되는 개인정보도 암호화 의무대상으로 지정

개인정보보호법 시행령

- 제21조(고유식별정보의 안전성 확보 조치) 고유식별정보의 안전성 확보 조치에 관하여는 제 30조를 준용, "개인정보"는 "고유식별정보"로 본다.
- 제30조(개인정보의 안전성 확보 조치) ①-3 개인정보를 안전하게 저장·전송할 수 있는 암호화 기술의 적용 또는 이에 상응하는 조치

유럽연합 개인정보보호법 (EU GDPR)

- GDPR이 정의한 '개인정보' 및 민감정보(Special categories of personal data) 대응

개인정보의 안전성 확보조치 기준(행정안전부 고시)

- 제7조(개인정보의 암호화)

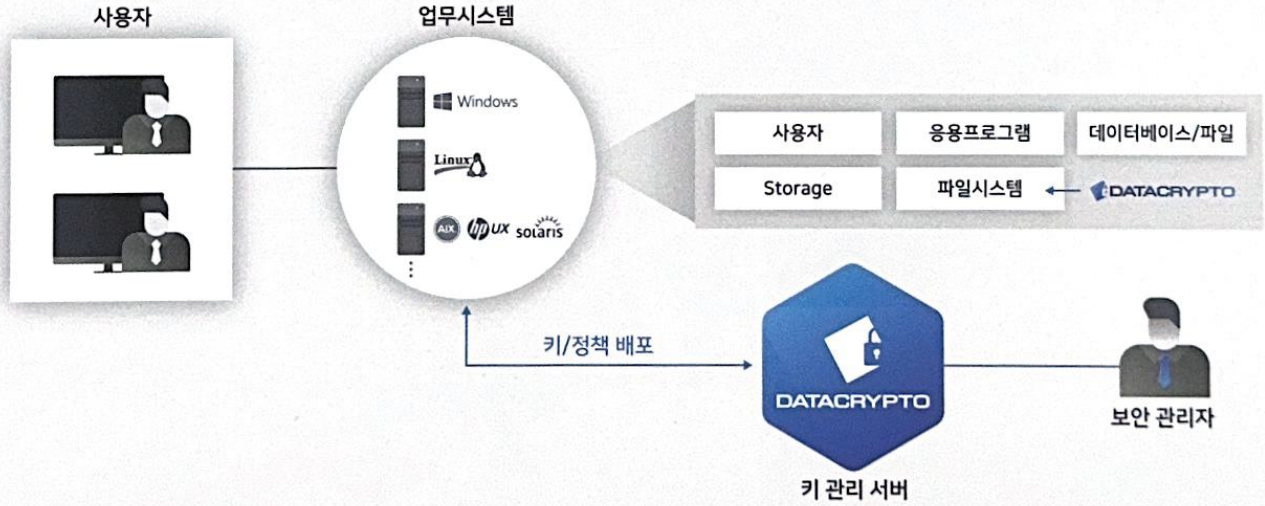
① (고유식별정보, 비밀번호, 바이오정보)정보통신망으로 송수신, 보조저장매체로 전달 시 암호화
② 비밀번호 및 바이오정보는 암호화하여 저장
③ 인터넷 구간 및 인터넷 구간과 내부망의 중간 지점(DMZ : Demilitarized Zone)에 고유식별정보 저장 시 암호화
⑥ 암호화된 개인정보를 안전하게 보관하기 위해 안전한 암호 키 생성, 이용, 보관, 배포 및 파기 등에 관한 절차를 수립·시행

DATACRYPTO의 개요

데이타크립토(DATACRYPTO)는 개인정보보호법 등 최신 컴플라이언스를 준수하는 DB/FILE 암호화 솔루션이며, 다양한 방식을 지원하여 최적화 된 암호화 방식을 제공하고 있습니다.

DATACRYPTO의 구성

데이타크립토(DATACRYPTO)는 다음과 같은 구성을 통해 별도의 어플리케이션 수정이 필요없이 암·복호화를 수행합니다.



DATACRYPTO의 특장점

- 공용 계정에 대하여 사용자를 식별하고 암·복호화 수행
- 국정원 요구사항인 암호화 알고리즘에 대하여 모두 충족
- 대용량 파일에 대한 어플리케이션 수정 없이 실시간 On-Line 암호화 방식과 Bulk 암호화 방식 지원
- 키 관리 서버를 통한 중앙 통제 및 키 관리
- 다양한 서버용 OS 및 볼륨매니저 지원 및 운영 환경 변경 없이 암호화 적용
- 사고 발생 또는 감사요구 시 추적 가능한 감사로그 제공
- 파일과 디렉토리에 대한 실시간 암 · 복호화 및 가속 기능

PNPSECURE

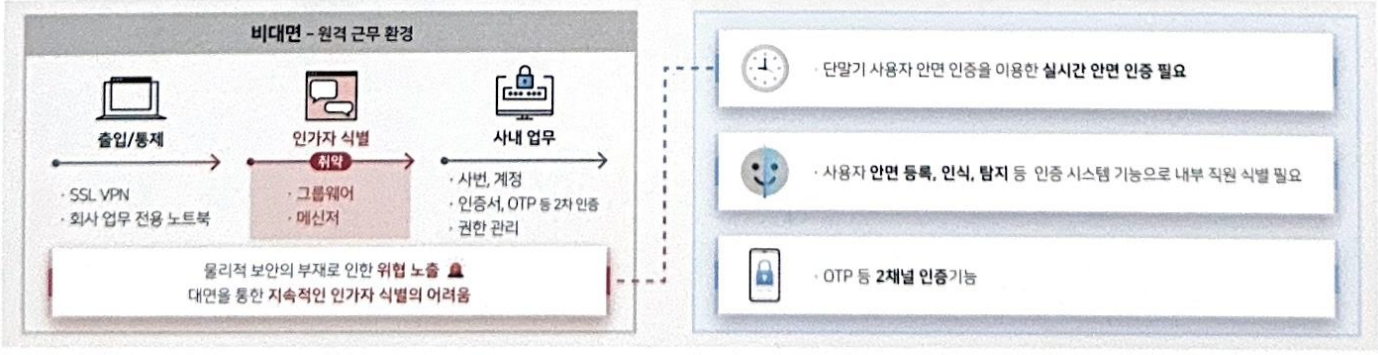
특허등록

- **전자금융 감독규정 시행세칙**(금감원)
- **금융회사 재택근무 보안 안내서**(금보원)
- **재택 · 원격근무 정보보호 6대 실천 수칙**(KISA)
- **재택근무 종합 매뉴얼**(고노부)
- **원격업무 통합보안매뉴얼**(국정원)

FaceLocker

Zero Trust 안면인식 보안 | 페이스락커

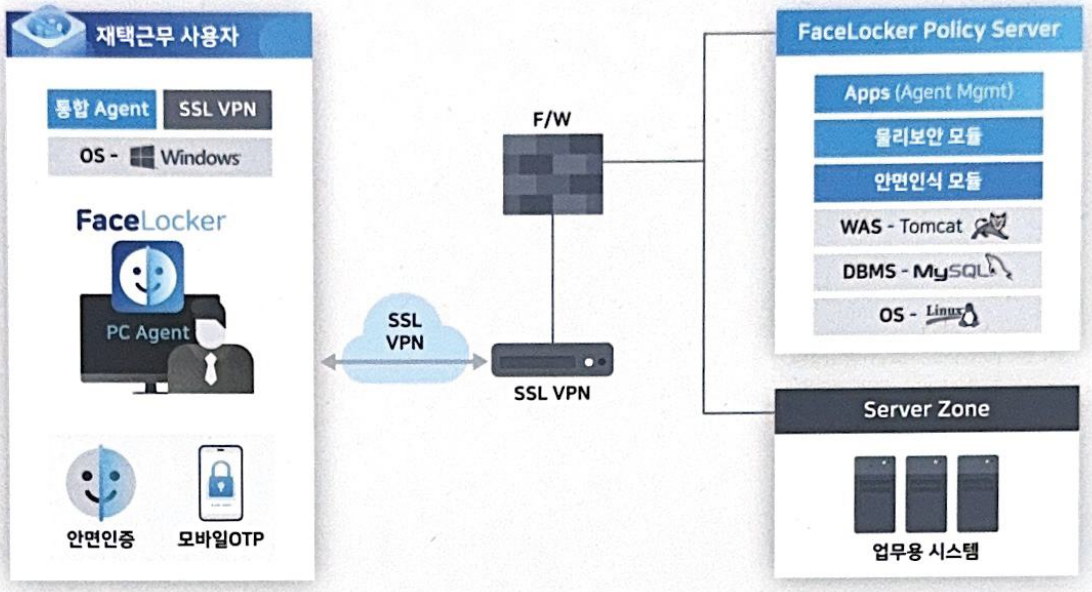
FaceLoker의 필요성 모바일오피스, 홈오피스, 공유좌석제 등 모던 오피스를 통해 생산성을 높이는 방법들이 쏟아지고 있는 지금 편리하고 안전한 제로트러스트 업무환경에 대한 필요성이 높아지고 있습니다. FaceLocker는 독자적인 안면인증 기술과 매커니즘을 통하여 제로트러스트의 지속적인 검증을 실현하며, Shoulder Surfing Attack, 핸드폰 촬영 등의 방법을 통한 정보유출을 차단합니다.



FaceLocker의 구성

- FaceLocker Agent 와 FaceLocker Policy Server로 구성

- 실시간 안면 인증(등록/인증) 및 OTP/VPN 연동 지원



FaceLocker의 주요 기능 및 특장점

생산성 향상을 위한 모던 오피스 환경에서도 편리하고 안전하게 업무를 수행할 수 있도록 진보된 안면인식 기능을 기반으로 한 제로트러스트 워크플레이스를 구현할 수 있습니다.

| 주요 기능

실시간 안면인식 기능

- 사용자 안면(얼굴) 등록 및 인증
- 실시간 안면 탐지 기능
- 사용자 안면 Fake(사진 등) 탐지 기능

화면 촬영 및 출력 차단

- 사용자 자리 이석 시 화면 차단
- 안면 미 인증 시 화면차단
- 2인 이상 인증 시 화면차단
- 핸드폰에 의한 화면 촬영 감지/차단

사용자 정책 및 관리 기능

- 역할별 사용/관리 권한 설정 기능
- 안면등록 승인/거절 기능
- 클라이언트 로그 정책위반, 클라이언트 정보, 정책 적용, 안면정보등록, 사용자 인증, 정책 반영 로그
- 관리자 로그 사용자, 역할, 접속기록, 조직, 그룹 로그

| 특장점

차세대 안면인식 기술

- 안면 인식 자체 기술 보유
- 사용자 단말에서 HW 기능으로 제공하는 Fake 탐지 기술 활용
- 안면 인식의 뛰어난 정확성과 빠른 인증 속도

이상 행위 탐지

- 디텍터 모듈이 검출한 얼굴 영역 확인 기술 보유
- 인가자 외 2인 이상인 경우의 탐지
- 사용자 자리 이석 탐지
- Local Display 제어 기능
- 핸드폰/카메라 촬영 감지

통합 관리 기능 지원

- 보안 정책 관리 기능
- 통합 로그 관리 기능
- 사용자 관리 기능
- One Time Password 기능
- 로그 & 통신구간 암호화 기능

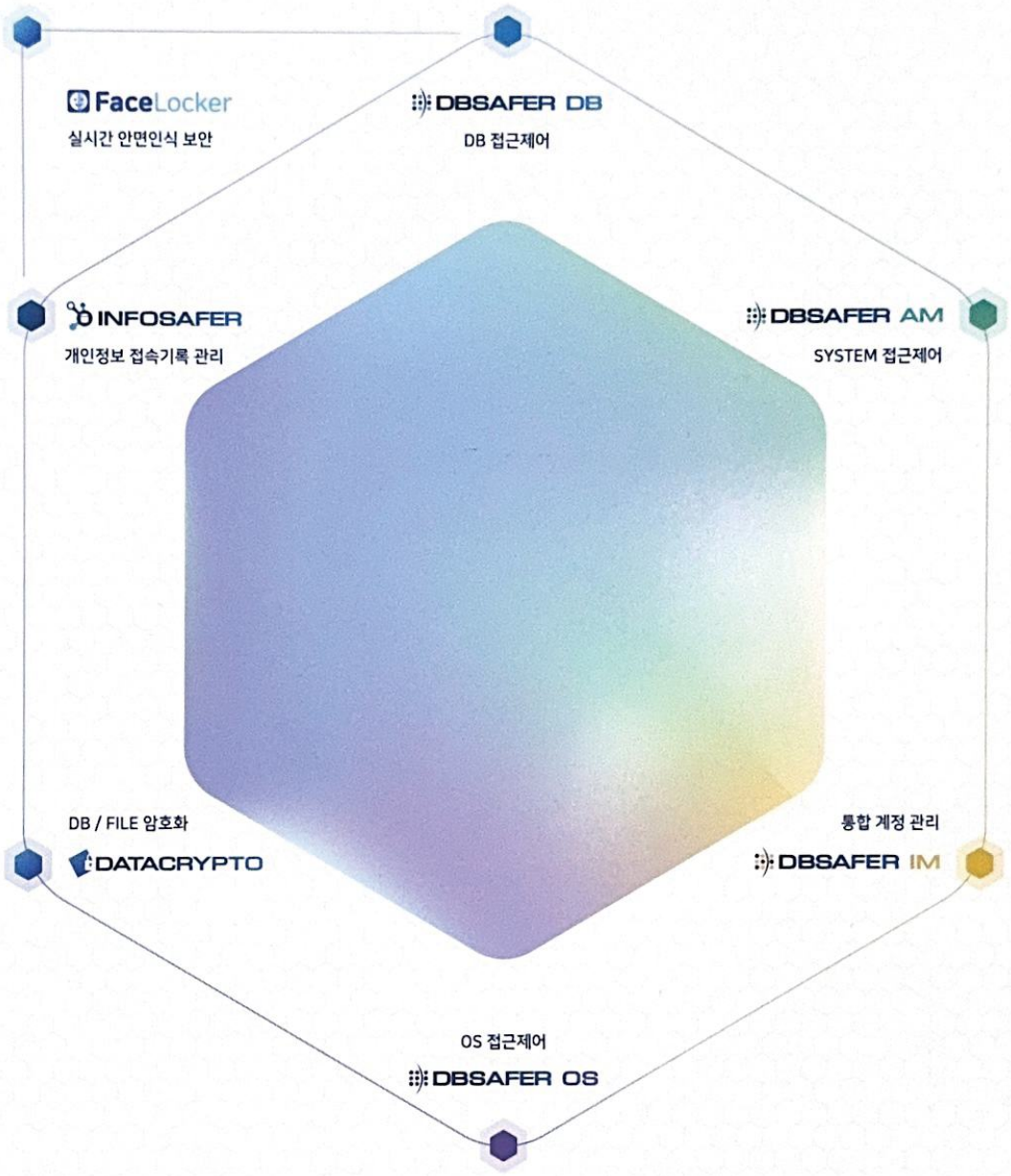
주요 인증

CC인증 | GS인증 | 신제품인증 | 신기술인증 | 우수조달제품 | 특허등록

주요 고객사

<금융·공공·기업 병원 등 국내 주요분야 5,000여 고객사>

은 행 권	신한은행	KB국민은행	IBK기업은행	standard chartered	NH NongHyup	우리은행
정 부 기 관	보건복지부	지식경제부	행정안전부	국세청	방위사업청	조달청
금 융 권	금융결제원	한국거래소	삼성생명	현대해상	보험개발원	우리투자증권
통신 / 제조	SK telecom	kt	LG U+	삼성전자	HYUNDAI MOTOR GROUP	posco
공사 / 공단	NPS 국민연금공단	한국전력공사	KOMSCO 한국조폐공사	KORAIL	K water 한국수자원공사	Incheon Airport
인터넷 기업	NAVER	위메프	TMON	ebay	kakaobank	K bank
유 통	HYUNDAI	신세계	롯데쇼핑	CJ 오쇼핑	GS SHOP	농협 하나로마트
병원 / 의료	SNUH 서울대학교병원	연세대학교 의료원	강북삼성병원	보훈공단	국민건강보험	대한적십자사
대 학	서울대학교	연세대학교	고려대학교	단국대학교	이화여자대학교	서울시립대학교
지방자치단체	서울특별시	세계속의 경기도	부산광역시	대구광역시	인천광역시	강원도
교 육 기 관	서울특별시교육청	대구광역시교육청	충청남도교육청	대전광역시교육청	부산광역시교육연구정보원	대구광역시교육연구정보원


FaceLocker
실시간 안면인식 보안
DBSAFER DB
DB 접근제어
INFOSAFER
개인정보 접속기록 관리
DBSAFER AM
SYSTEM 접근제어
DB / FILE 암호화
DATACRYPTO
통합 계정 관리
DBSAFER IM
OS 접근제어
DBSAFER OS