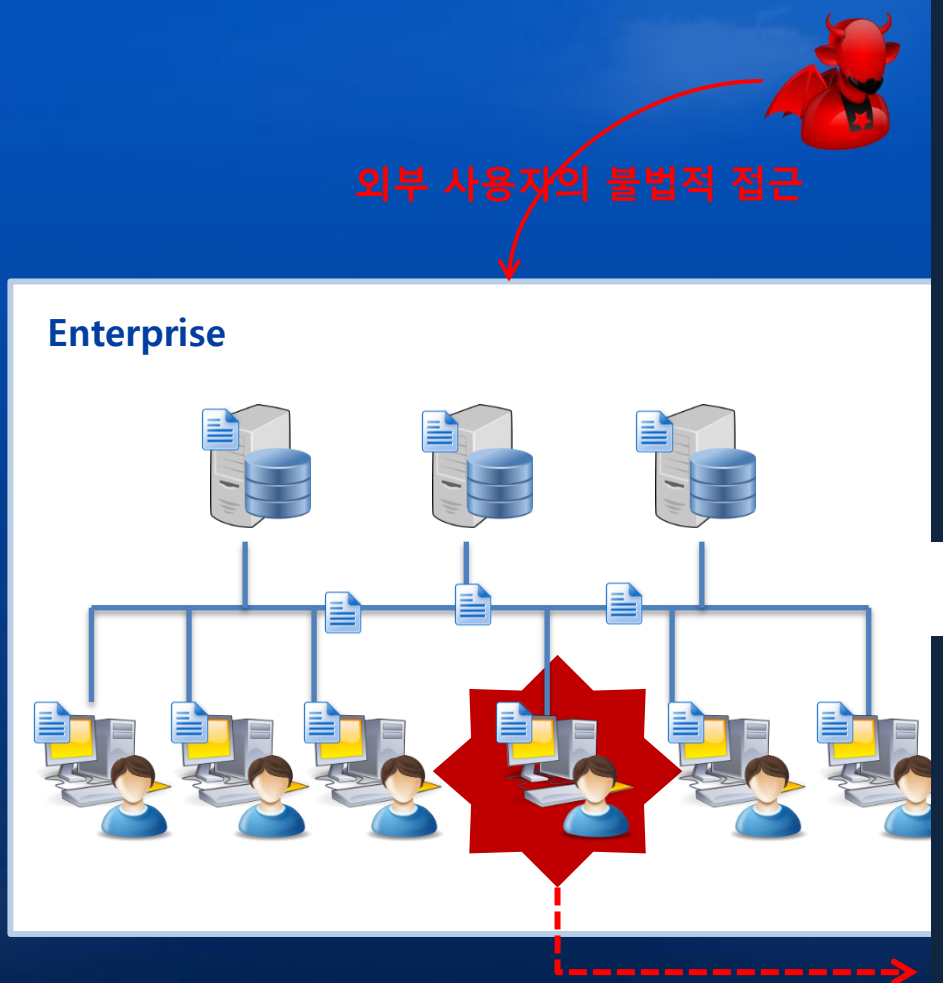
Fasoo

내부 데이터 보안 관리 전략

파수닷컴 | **김용길** 상무

내부 데이터 보안

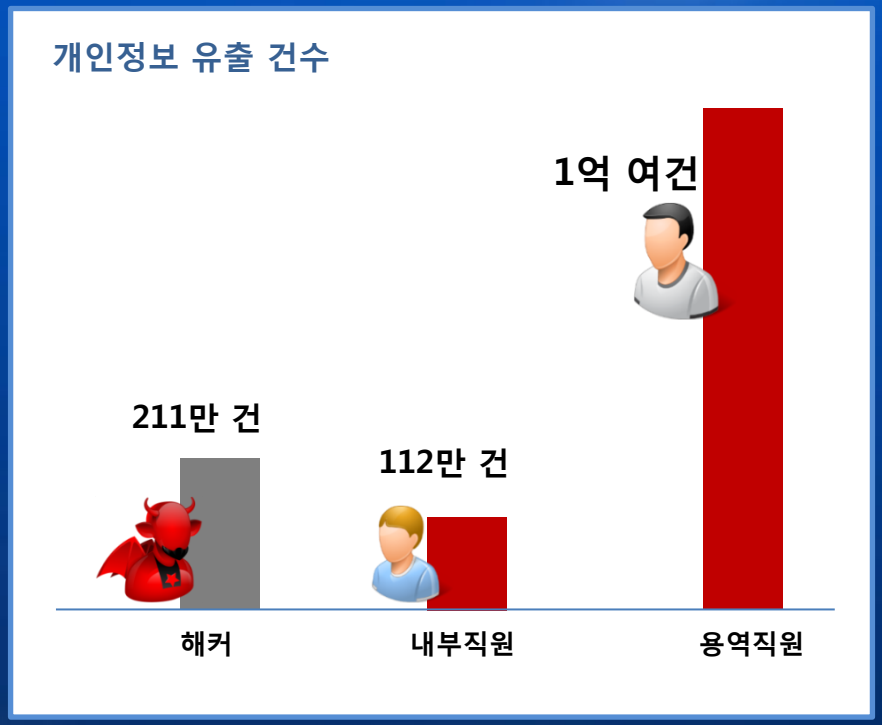


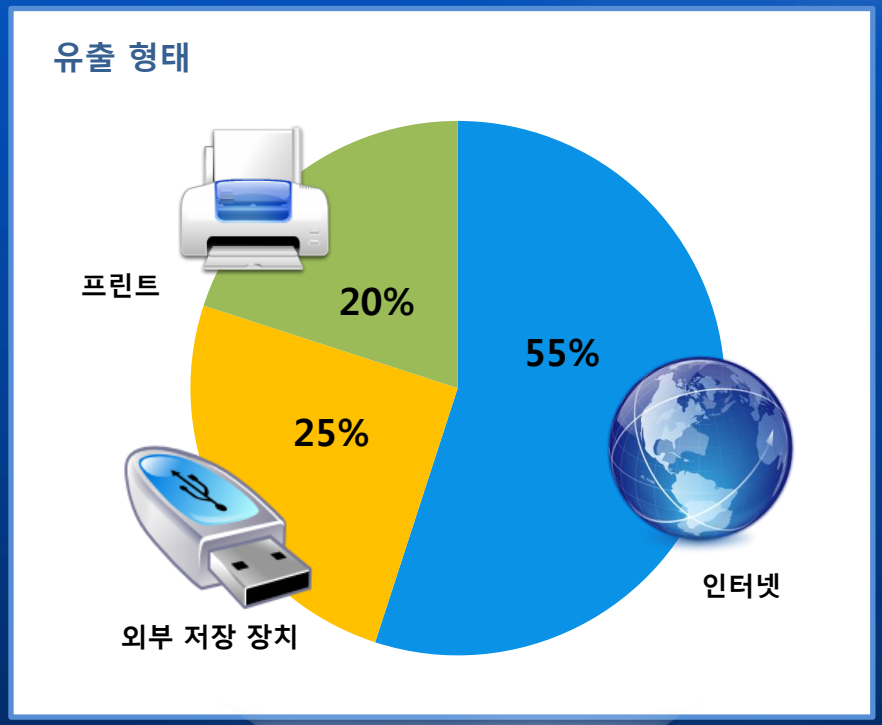
- 전통적인 내부 데이터 보안 이슈
- 스파이웨어 배포, 취약점 공격 등 공격방식에 대한 보안 필요
- APT 등 고도의 해킹 기술로 발전
- 방화벽 등 장비 보안, 웹서버 보안 제품 등 다양한 개념의 제품 출시

- 적절한 권한을 보유한 사용자가 접근 가능한 데이터를 불법적으로 유출 시도
- 실제 내부자료 유출 사고의 대부분을 차지
- 유출 사건 발생 후 상당한 시일 경과 후 인지하는 경우가 대부분
- 권한보유자의 유출 시도라는 차원에서 적절한 보안 대응이 상당히 어려움

내부 데이터 유출 사고 원인

[금융기관 정보유출 사고 유형별 내역('09 ~ '13년 중),금감원]





유출주체

유출형태 및 경로

접근 권한을 가진
내부자의 고의적 유출

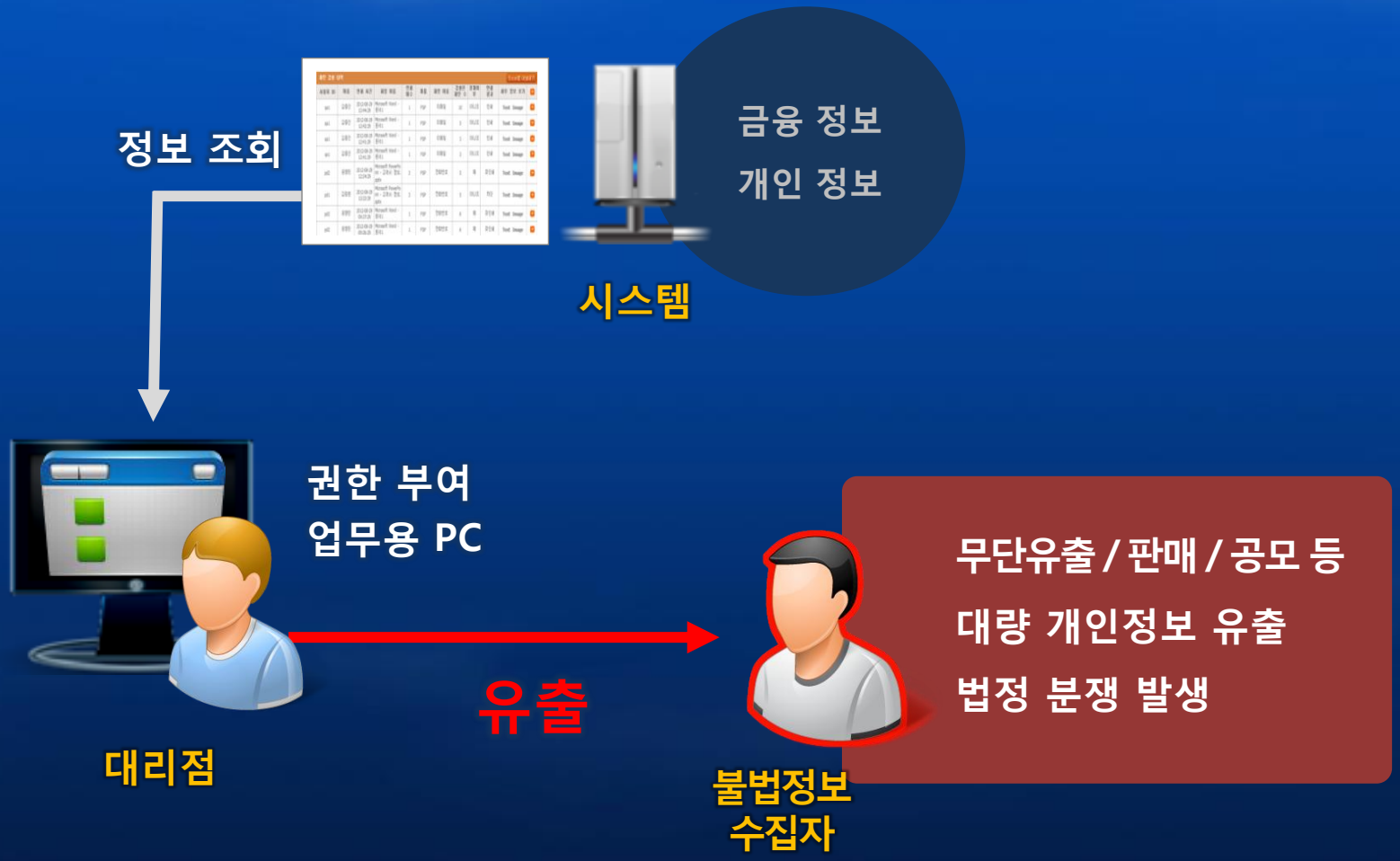
보호되지 않은 파일형태
다양한 경로를 통한 유출

Fasoo

사례 : 협력직원 유출

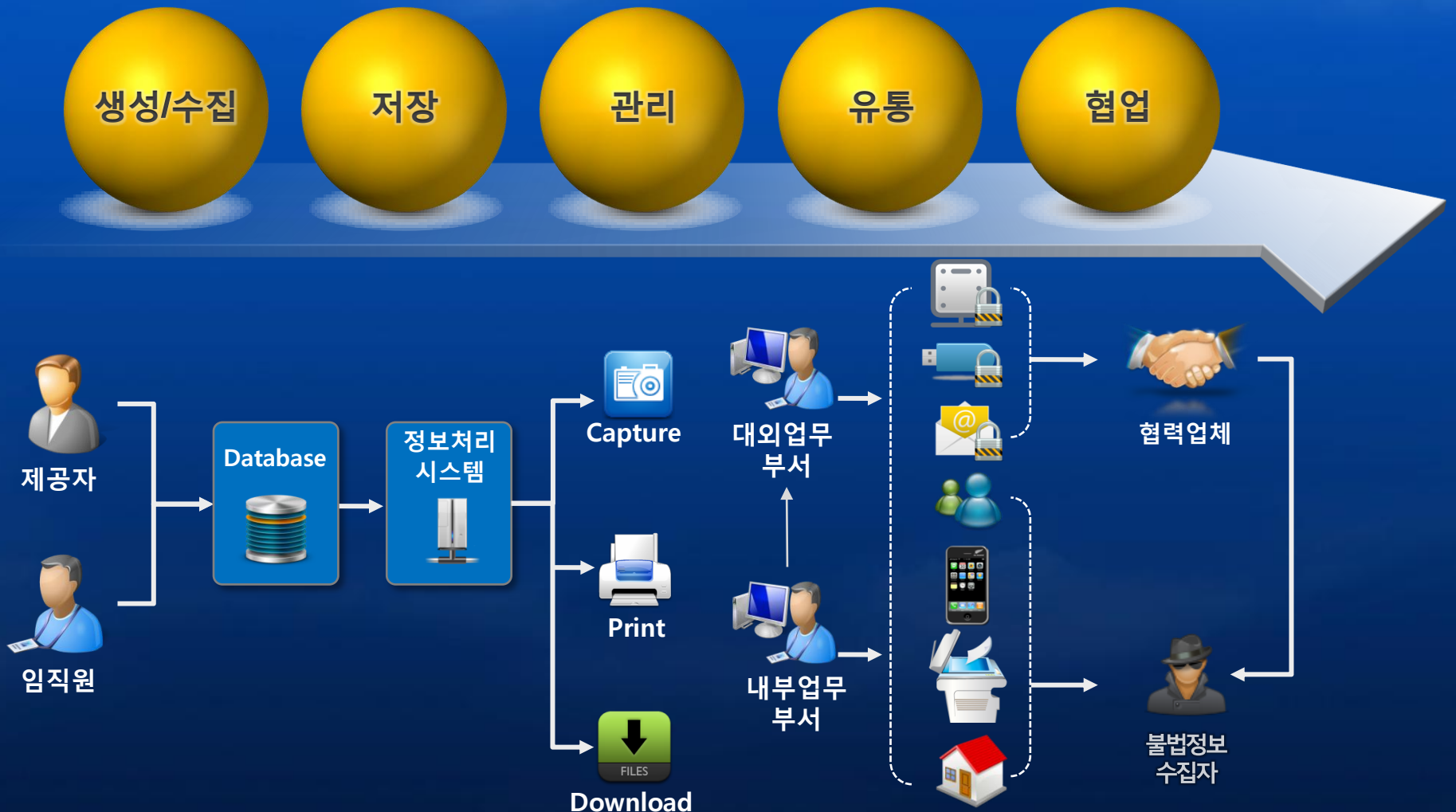

금융 정보
개인 정보
카드 정보
DB 접근
DB 저장
금융 정보
개인 정보
카드 정보
내부직원
DB
협업
유출
무단유출 / 판매 / 공모 등
대량 개인정보 유출
법정 분쟁 발생
협력업체
불법정보
수집자

사례 : 대리점 정보조회 유출



Fasoo

내부 데이터의 Life Cycle



Fasoo

내부 데이터의 Life Cycle의 보안위협

Fasoo

내부 데이터 보안 솔루션

외부유출차단
(DLP)

외부업체

DB 보안
(암호화/
매스킹)

출력물 보안
(프린트보안/
워터마킹)

출력물

BYOD 보안
(MDM/MAM)

BYOD

010
111
1100110
1101101
1100001

내부 데이터
암호화
(DRM)

사용자 행태 분석
(Behavior Analysis)

내부 권한
사용자

외부반출

매체 보안
(보안USB)

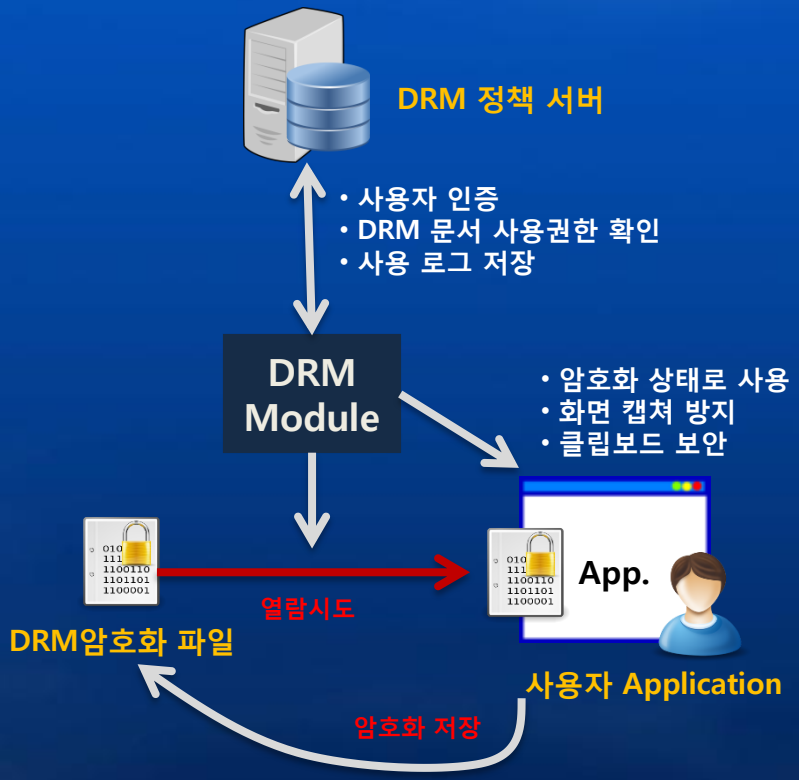
Fasoo

내부데이터 보안 솔루션 별 특징

솔루션	동작방식/보안대상	특징
매체 보안 (보안USB 등)	PC에 접속하는 외부장비에 저장하는 내부 데이터를 암호화하여 자료 이동 방어	. DLP 기능의 부분옵션으로도 사용 . 권한을 가진 사용자의 유출 시도에 대한 방어 어려움
외부유출차단 (DLP)	외부전송 발생 시, 파일 내부 스캔 후 주요 정보 포함된 경우 전송을 차단하고 로깅	. PC 하드 유출, 노트북 유출 등에 대한 방어 불가 . 특정 정보 Masking 후 전송 시도 우려
출력물 보안 (인쇄 워터마킹 등)	내부데이터 출력 시, 출력 내용을 기록하고, 출력물 상에 출력자 정보 등을 표현	. 파일 전송 등을 방어하는 다른 보안솔루션과 함께 사용하는 보조적인 보안 제품
사용자 행태분석 (Behavior Analysis)	사용자 행태를 실시간 모니터링하여, 이상 징후(대량 복사, 대량 다운로드) 발생 시 동작을 차단하고 로깅, 관리자 통보	. 유출 전 완벽한 차단을 목적으로 하기보다는 장기적인 현상을 모니터링 하거나 유출 사후에 상황과 검증 목적으로 활용
내부데이터 암호화 (DRM)	기업/조직 내부에서 유통되고 생성되는 주요 데이터를 생성시점부터 전체 라이프사이클에 대한 암호화 지원	. 가장 강력한 내부데이터 보안 방안 . 개별 Application 에 대한 지원 필요 . 파일 별 사용 권한 관리 기능

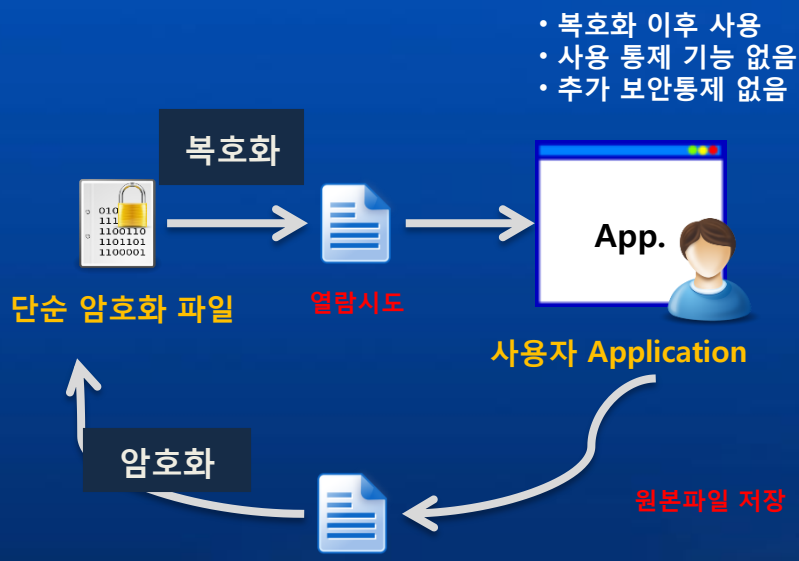
DRM 과 단순 암호화

DRM



- 생성 시점 부터 지속적인 암호화 상태 유지
- DRM 모듈에 의한 사용자 인증, 권한관리 가능
- 사용자 문서 사용 이력 추적

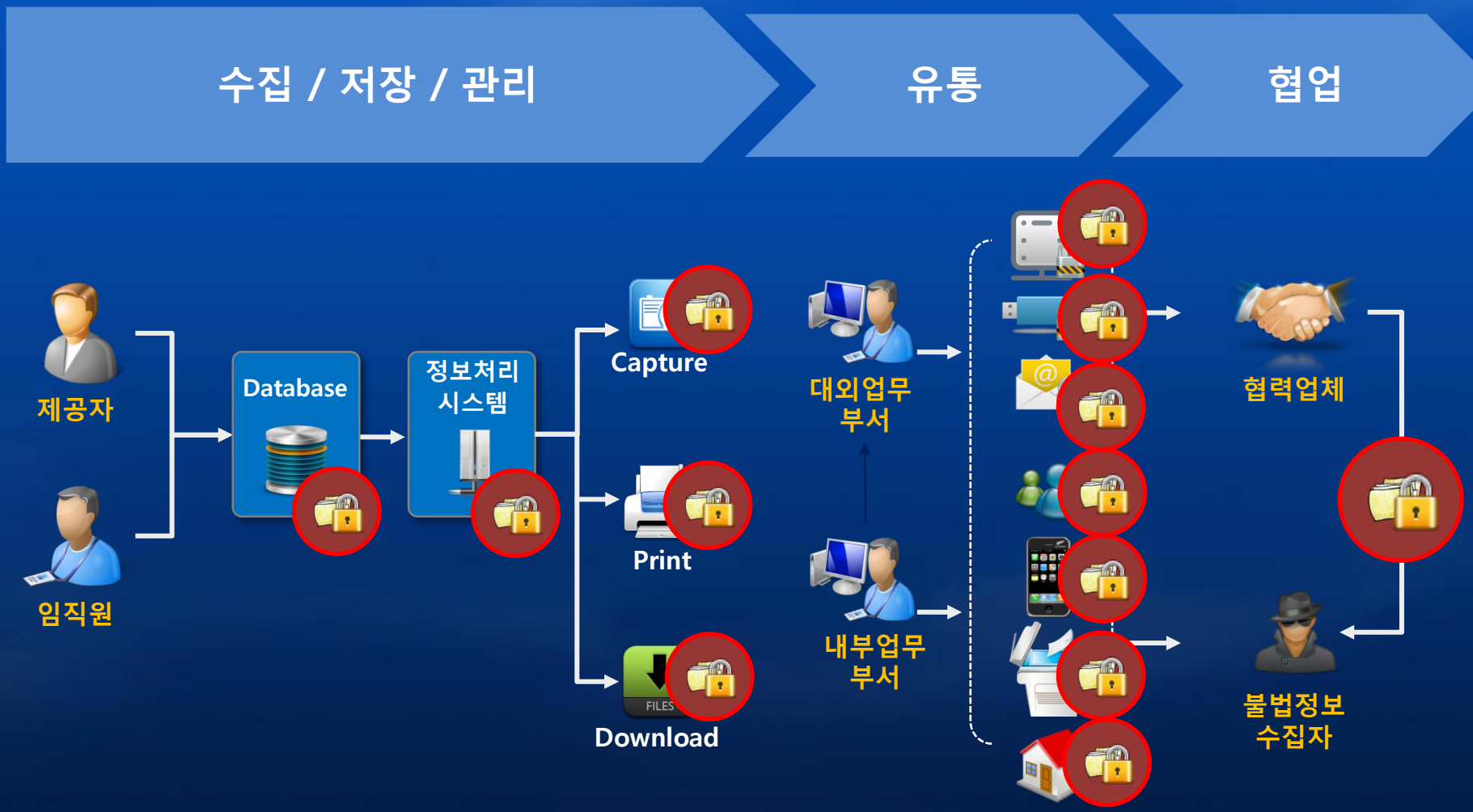
단순 암호화



- 명시적인 복호화 이후 문서 사용
- 사용자의 의도에 따라 보관 시 암호화 보안 기능
- 사용을 위한 복호화 이후에 대한 보안 방안 전무

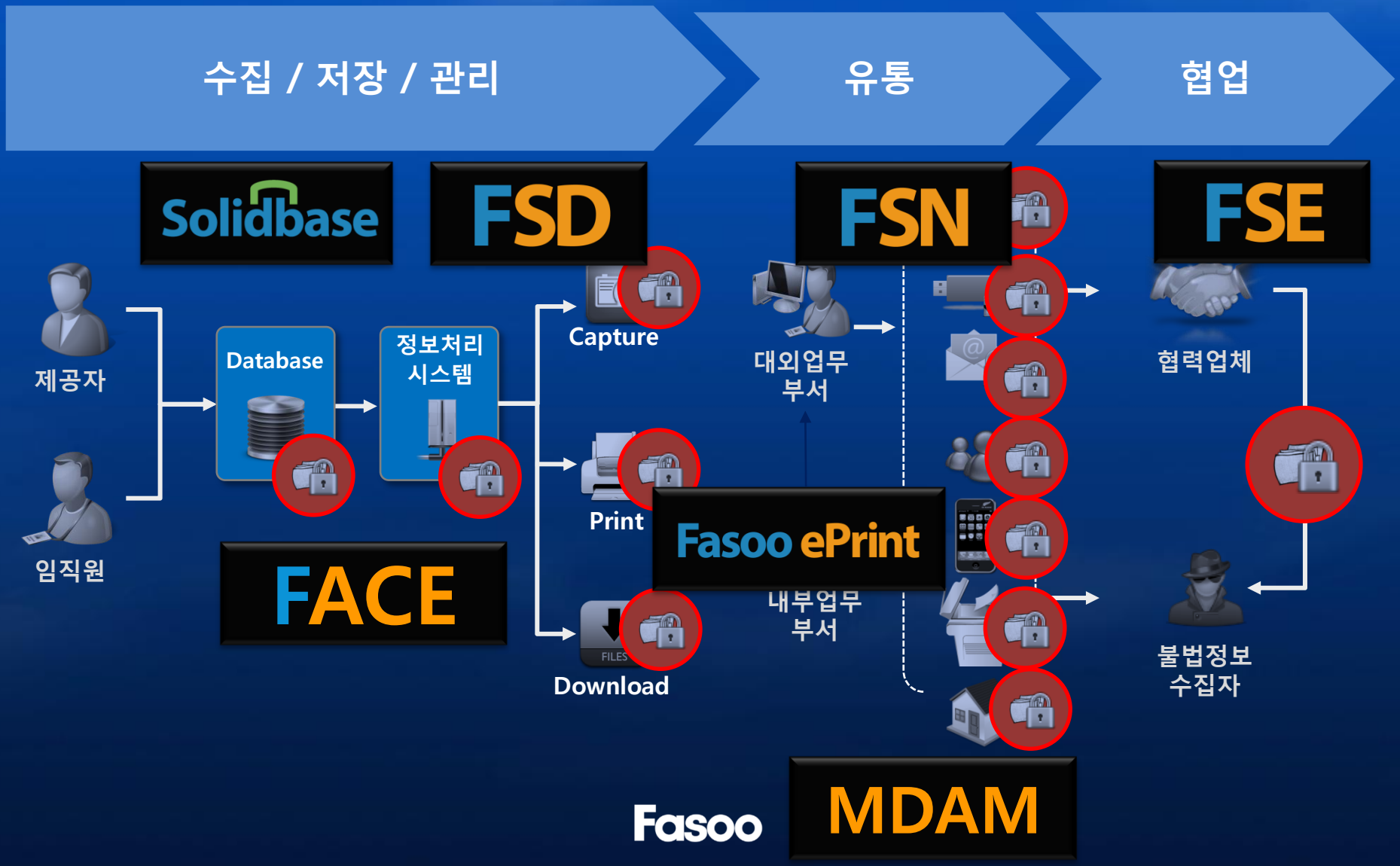
Fasoo

내부 데이터 보안의 기본: 지속적인 암호화



Fasoo

Fasoo 내부 데이터 보안 제품군



BYOD 환경에서의 내부데이터 보호

BYOD에 대응하는
모바일 보안전략 CHECKLIST

- ✔ 모바일 디바이스 내 저장된 데이터는 안전한가
- ✔ 서버와 모바일 디바이스 사이의 통신은 안전한가
- ✔ 모바일 환경에서 서버 접근을 관리, 통제하는가
- ✔ 모바일 화면이 또 다른 유출 경로가 되고 있지 않은가
- ✔ 모바일 디바이스 내 문서가 안전하게 유통되는가

Fasoo

Fasoo Mobile Data & Access Management(MDAM)

접속 허용자

Fasoo Explore

사용자 인증
접속권한 확인
암호화 전송
스크린 워터마크
캡쳐제어
접속/동작 로깅

접속 미허용자

Fasoo Explore

접속 차단

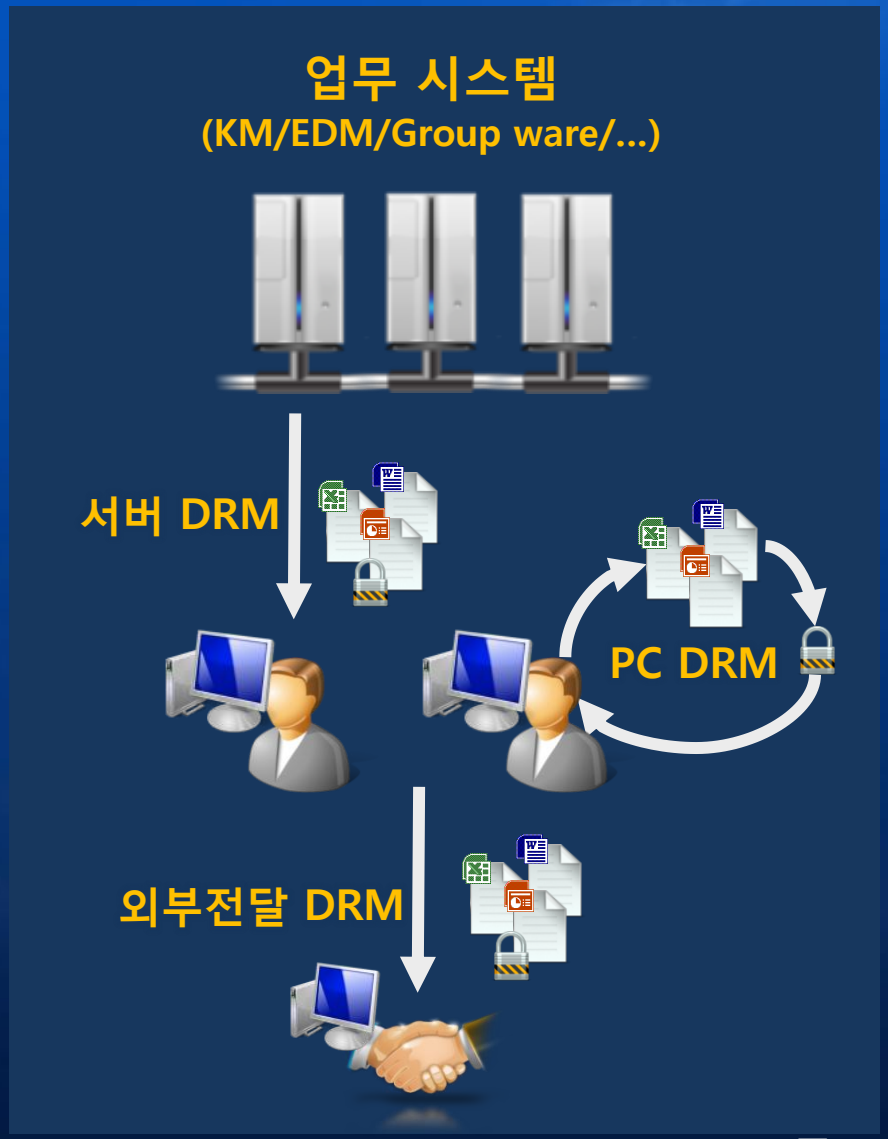
일반 브라우저
앱 접속자

Fasoo Explore

접속 차단 후 Fasoo Explore 실행

Fasoo

DRM Solution for Database Applications



Fasoo

FACE (Fasoo Application Control & Encryption)

Fasoo

FACE (Fasoo Application Control & Encryption)

허가된 DB 어플리케이션에 대한 DRM 데이터 보안

주요 정보 저장파일 DRM 암호화

DB 프로그램에서 생성되는 파일 DRM 암호화

암호화 파일 사용 권한 통제

문서 접근 / 사용 이력 로깅

FACE (Fasoo Application Control & Encryption)

DB 어플리케이션 접근 통제

사용 가능한 DB 접근 어플리케이션 제한

비 허가 DB 어플리케이션의 DB접근 통제

사용자 별 DB 어플리케이션 허용 정책부여

FACE (Fasoo Application Control & Encryption)

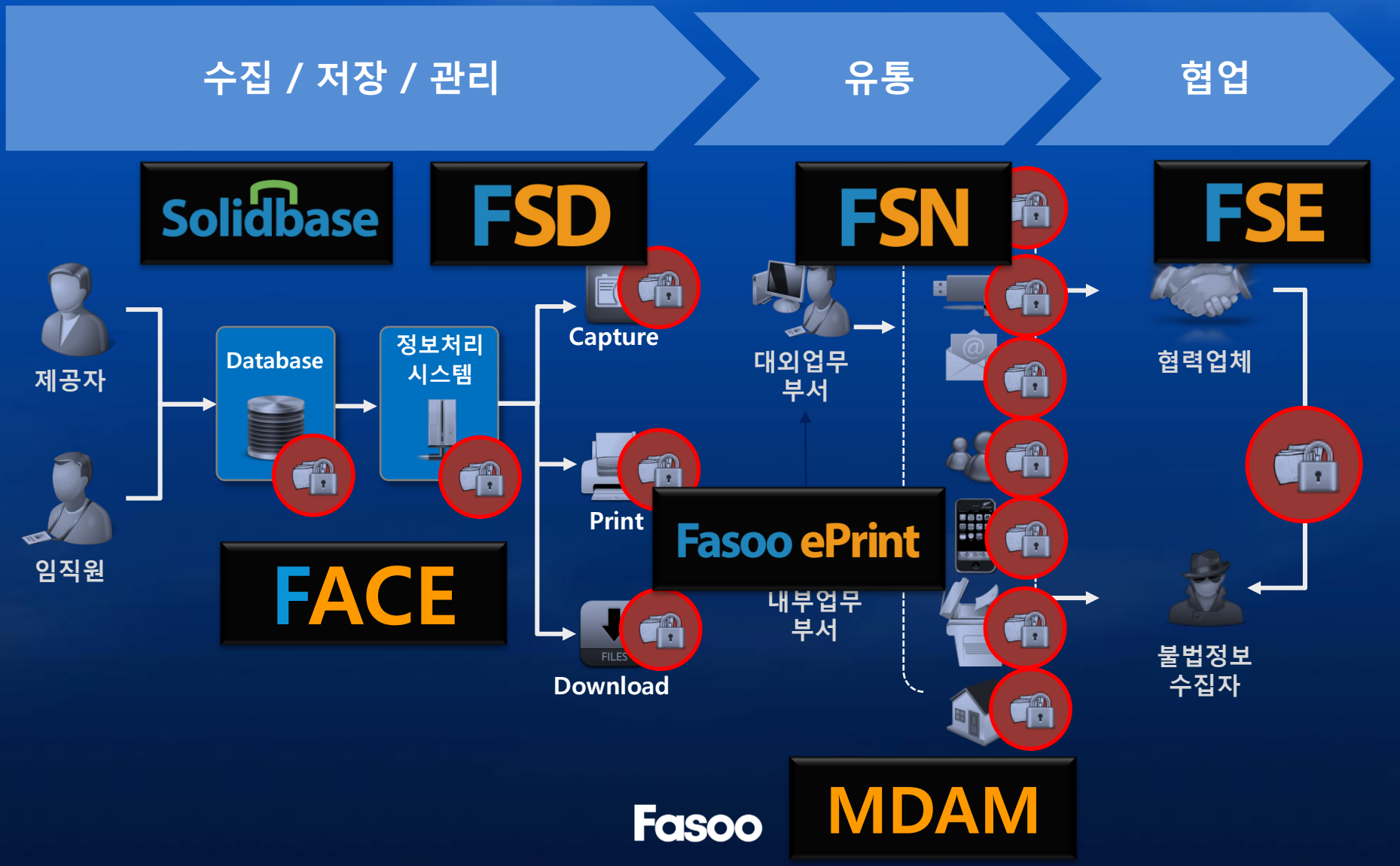
그 외 어플리케이션 적용 가능

주요서버와 통신하는 네트워크 어플리케이션 제한

허가되지 않은 FTP / 기타 Socket 모듈 등의 사용 통제

허가된 어플리케이션의 DRM(암호화, 복사방지,캡쳐방지)

Fasoo 내부 데이터 보안 제품군



내부 데이터 보안의 핵심은 데이터 자체의 보호 !

DRM, 권한관리와 지속적인 데이터 보호 방안의 핵심

Fasoo

Thank you

Fasoo