대량의 고객정보 관리 취약점과 유출 대응방안

SOFTCAMP

보안 위협의 사례

실제 사고사례

보안의 패러다임 변화가 필요

3.20
3.20일 국내 은행 등 금융전산 사고
- APT 공격

1억4백만명
국내 3개 카드 사
- 2014년 사상 최대의 고객정보 유출
- 외주 직원을 통해 고객정보 유출

6,000만
부정결제사고 카드 사 회원 수
- 수백 건의 소액결제(30만원 미만) 해킹

X2
알려진 1억 2천만 건 보다 2배 이상 개인 정보 누출사고

개인정보 유출사건에 따른 보안강화 3대 핵심사항

고객정보 유출방지를 위한 금융회사 유의사항

1. 고객정보관리 내부통제 부문

① 고객정보 접근통제 및 권한 관리 철저

- 고객정보 조회 권한을 직급별, 업무별, 내·외부 직원 별로 차등 부여하고 과다조회 부서 및 직원에 대해서는 정기·수시 점검
- 고객정보를 USB메모리 등 이동저장매체에 저장하거나 외부 전송하는 수단에 대한 통제 강화
- 조회한 고객정보의 PC저장 및 출력 시 기록을 유지하고 정기적으로 점검

② 고객정보 이용 및 제3자 제공현황 모니터링 강화

2. 외주업체 보안 관리

① 아웃소싱 상주직원의 시스템에 대한 접근통제를 강화

- DB접속권한 제한, DB작업내역 자동저장, 외부반출 통제 등 아웃소싱 직원의 자료유출 경로 차단을 위한 대책 수립

② 외주업체의 고객정보 이용 통제

3. 고객정보 보호를 위한 정보기술 부문

① 시스템 개발 시 고객정보 사용에 대한 보안통제를 강화

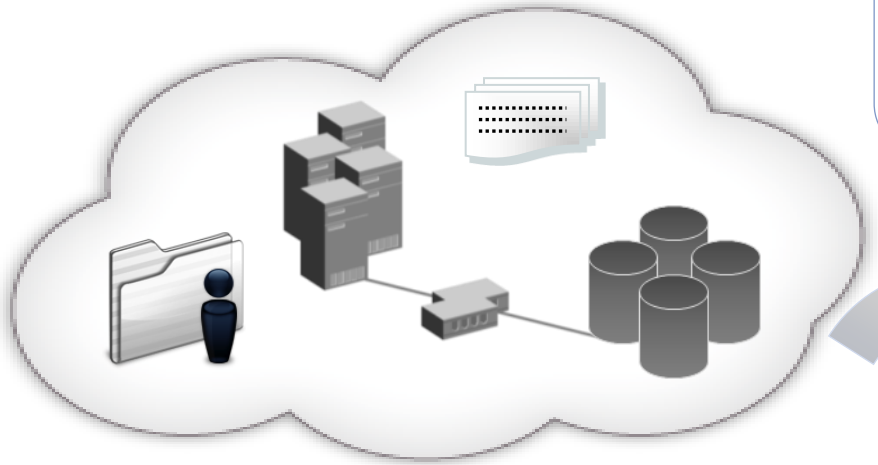
② 내·외부직원의 PC 및 인터넷 사용에 대한 보호조치 강화

- 직원 PC에 고객정보 및 금융거래정보의 불필요한 보관을 금지하고, 업무상 불가피한 경우에는 정보유출 방지대책을 수립

(출처, 개인정보유출사건에 따른 금감원, 금융회사에 대해 정보보호 강화 강력히 주문 세부 사항(별첨내용), 2014년 01월, http://www.fss.or.kr)

대량 데이터의 특성

데이터베이스 내의 데이터는 End Point로 저장되면서 대량 비정형 데이터로 변경



데이터베이스 서버

End Point 저장

End Point로 저장된 데이터 중 고객정보와 기업의 중요 데이터는 유출 방지를 위해 보호해야만 함

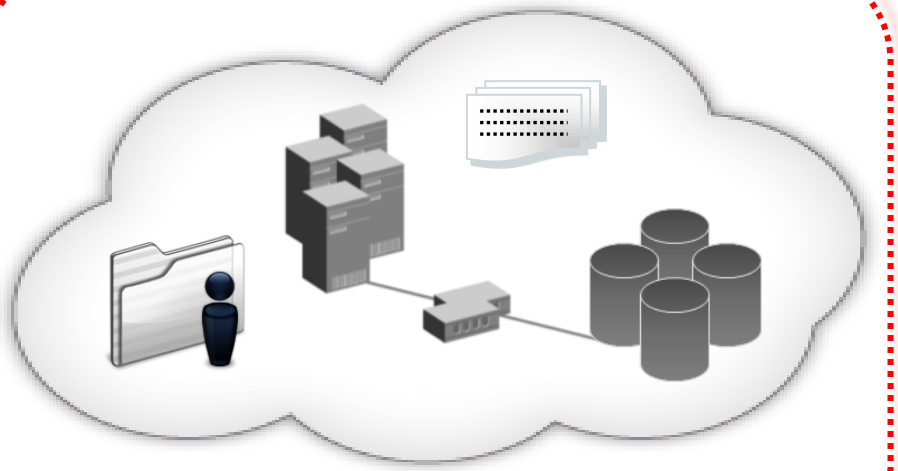
고객정보(개인정보)는 개인정보보호법 및 정보통신망법에 의거 PC에 저장되어서는 안되며, 업무 상 PC에 저장할 경우, 암호화하여 저장해야 함

→ 업무 연계를 위한 특화 솔루션 필요

비정형 데이터

DB보안의 한계점

DB 보안?



데이터베이스 서버

DB 암호화

- 대용량 DB 접근도구 및 개발도구 등 업무 연계를 위해 개발자, IT 담당은 평문 데이터로 다운로드 받음
- 사용자 PC에는 복호화 된 데이터로 저장

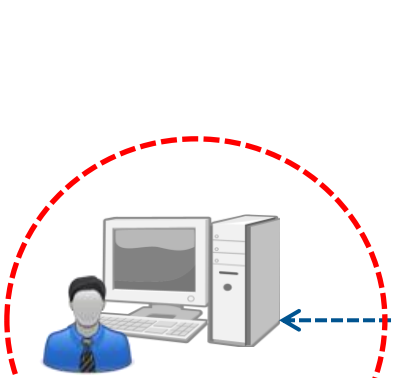
DB 접근제어

- 접근제어 및 통제를 우회하여 공격 시, 고객정보가 포함된 대량의 데이터 유출
- 실제, 유출된 대부분의 대량 고객정보 데이터는, 접근이 인가된 사용자가 다운로드 받은 후 유출

DB보안의 한계점은 대량의 고객정보 유출로 이어짐

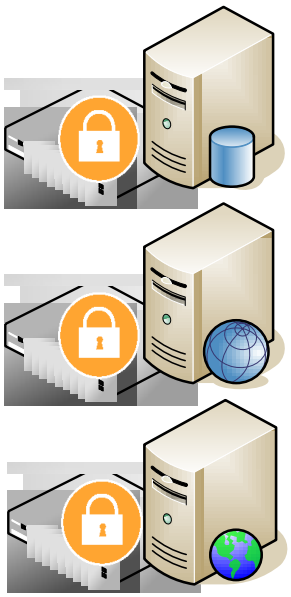
- DB 암호화를 적용하여도 대용량 DB 접근도구 및 개발도구 등 업무 연계를 위해서는 평문 데이터로 다운로드
- DB접근제어를 적용하여도, 접근이 인가된 사용자는 비정형 데이터로 PC에 저장할 수 있으므로, 대량의 고객정보가 유출될 위험 존재(대부분의 유출 사례)

DB 암호화가 적용된 고객정보 유출



인가 사용자
(개발자, IT 담당)

평문 데이터



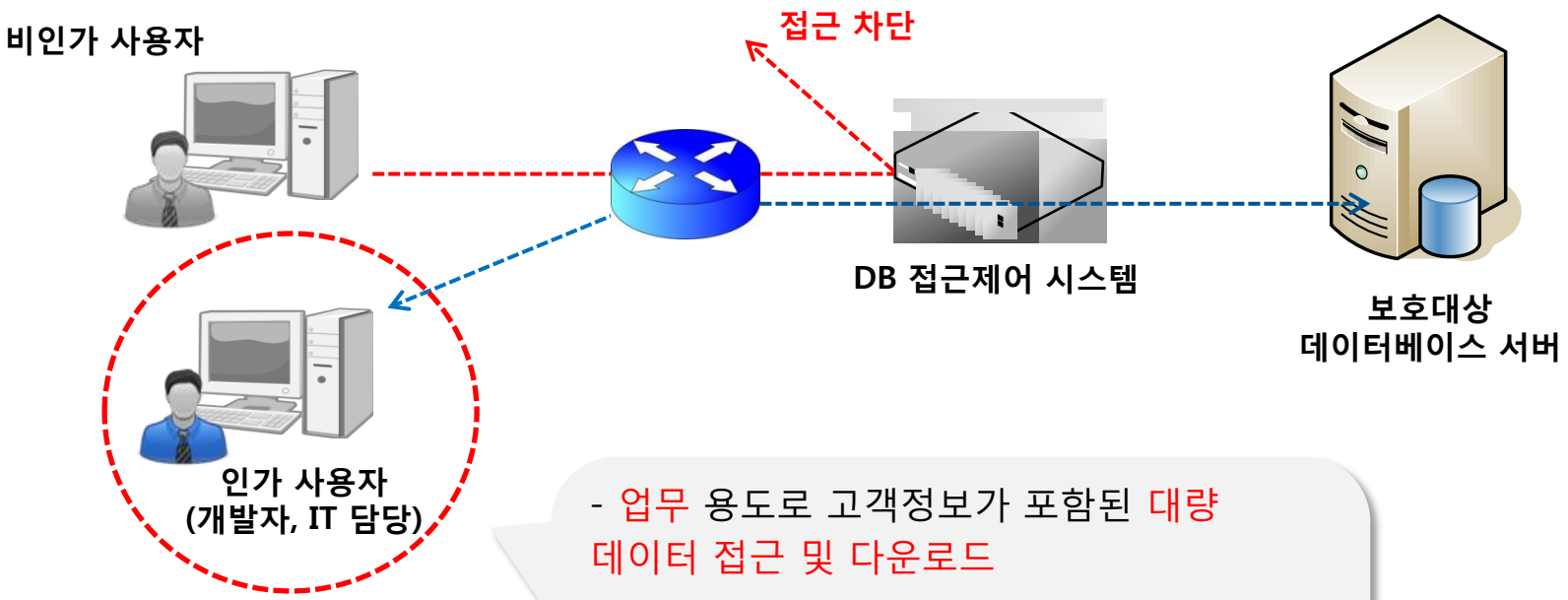
고객 DB

업무 DB

웹 서버 DB

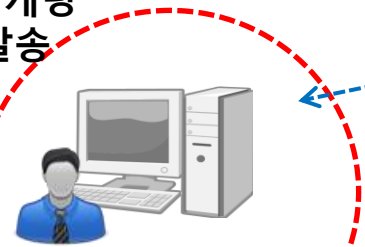
- Toad, Orange, SAS 등의 대용량 DB 접근도구 및 개발도구 등 업무 연계를 위해 다운로드 받은 데이터를 복호화하여 저장
- 저장된 비정형 데이터는 부주의 또는 악의적인 행위에 의해 쉽게 외부로 대량 유출

DB 접근 권한 인가자를 통한 고객정보 유출



- 업무 용도로 고객정보가 포함된 대량 데이터 접근 및 다운로드
- 인가된 사용자가 내려 받는 데이터는 암호화 되지 않은 비정형 데이터
- 저장된 비정형 데이터는 부주의 또는 악의적인 행위에 의해 쉽게 외부로 대량 유출

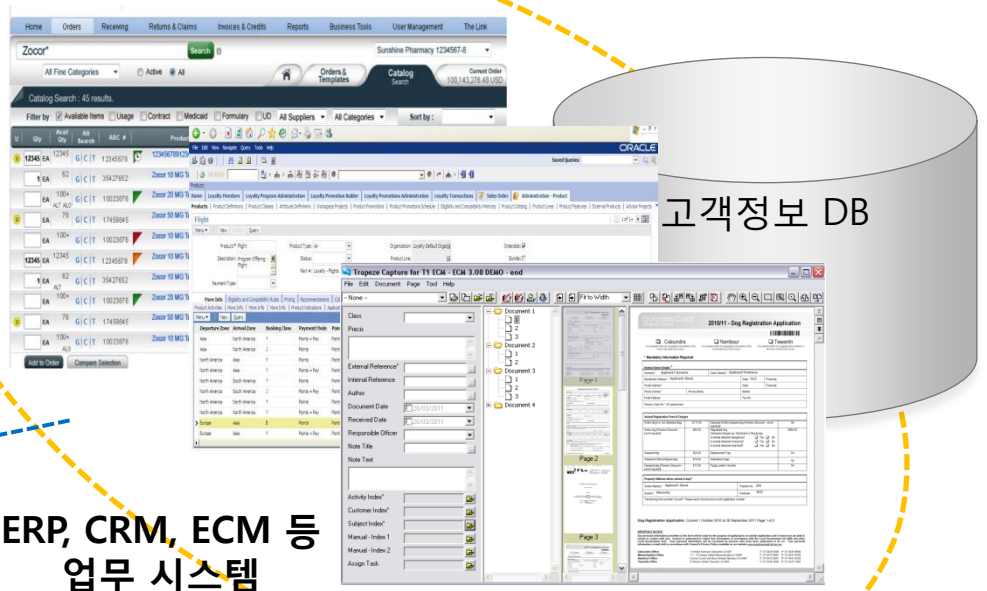
업무시스템을 통한 고객정보 유출



인가 사용자

통계, 상품개발,
Report, 마케팅
및 DM 발송

Export



고객정보 DB

ERP, CRM, ECM 등
업무 시스템

- 업무 조회 후 고객 정보가 포함된 데이터를 Office파일 또는 CSV 파일 등 비정형 데이터로 내보내기/다운로드 (암호화 미적용)
- 소량 데이터를 장기적으로 누적하여 받는 경우 감지 어려움
- 저장된 비정형 데이터는 부주의 또는 악의적인 행위에 의해 쉽게 외부로 대량 유출

대량의 고객정보 유출을 막기 위해서,

내/외부자의 부주의 또는 악의적인 행위에 의한 대량 고객정보 유출을 방지하기 위해서는,

1. 개발, IT 담당 등 인가된 사용자가 취급하는 대량 데이터의 암호화 및 유출 차단
2. DB지원 도구, 개발 도구 등 기존 업무 환경을 유지하며 암호화 및 유출 차단
3. 기업 내 모든 형태의 데이터에 대해 암호화 및 유출 차단

이 필요합니다.

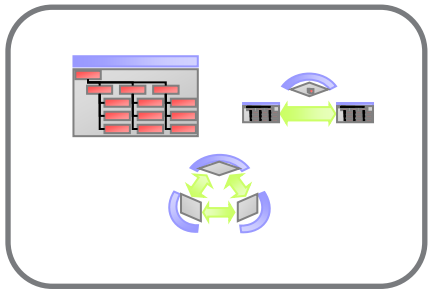
소프트캠프의 영역보안 기술 개념

| 영역보안 기술 개념

- 사용자 PC내에 보안영역을 만들어 주요 정보 및 데이터를 보안영역에만 저장
- 보안영역 자체에 대한 암호화 및 어플리케이션 통제, 파일 반출 통제 등을 통해 내부정보 유출 방지
- 보안영역 내의 정보(데이터)는 보안영역 내에서만 자유롭게 유통 가능

업무 영역보안을 통한 고객정보 보호의 특화 요건 대응

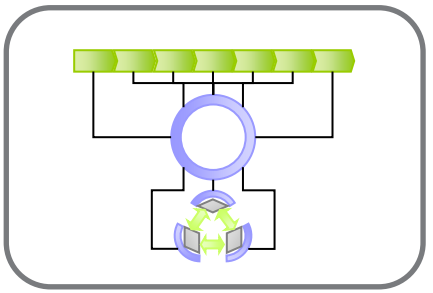
어플리케이션/데이터의 다양성



다양한 파일 형식과 다양한 어플리케이션의 유기적인 상호 연동 보장

데이터 생성시점부터 폐기까지의 전 구간에 완벽한 보안 방안 제공

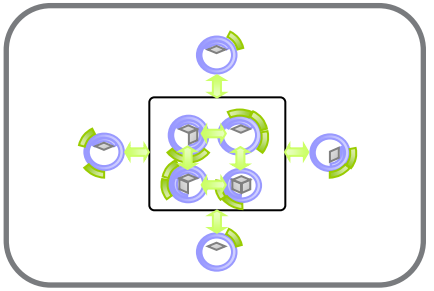
업무 데이터 보안 관리



사용자 단의 업무영역 또는 DB서버로부터 다운로드 받은 데이터 보안 관리

대용량 파일 보안 방안 최적화

다양한 참여조직

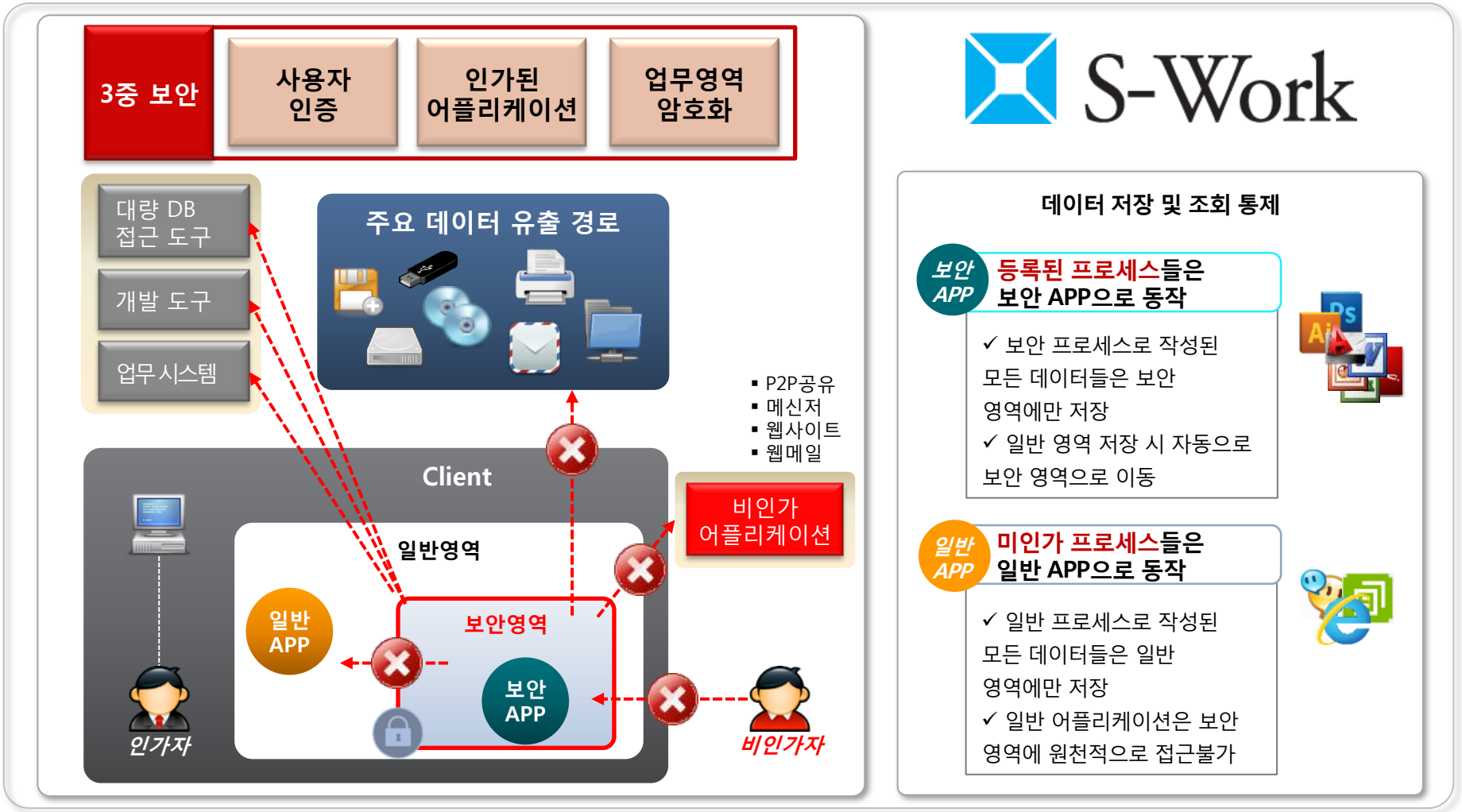


다양한 사내/외 참여 조직간의 협업 정보 공유 시 신뢰성 보장

고객정보 등 기업 내 중요 데이터의 유출 경로 차단

소프트캠프의 영역보안 솔루션

- 고객정보를 포함한 대량 데이터를 접근하는 **인가된 프로그램**(대량 DB 접근 도구, 개발 도구, 업무시스템)의 경우 **보안영역**에서만 사용 가능
- 일반영역 및 외부로의 **고객정보 및 중요정보의 유출은 철저히 차단**



소프트캠프의 영역보안 솔루션 기대효과

강력한 데이터 유출 방지

암호화된 보안영역의 데이터 반출 차단

- 암호화된 보안영역으로 데이터 자동 저장
- 암호화된 보안영역의 데이터 반출 차단
- 보안 어플리케이션 데이터 유출 차단

안전하고 효율적인 협업 가능

업무 상의 사내외 조직과의 협업 지원

- 사내 사용자 간 데이터 공유
- 사용자와 업무 시스템 간 데이터 공유
- S-Work가 설치된 사외 사용자와의 데이터 공유

편리하고 효율적인 관리

쉽고 편리한 관리방안 제공

- 프로세스 등록을 통한 어플리케이션 보안 연동
- 계층적인 관리체계 지원
- 통합적인 이력 관리

기존 업무환경과의 호환성

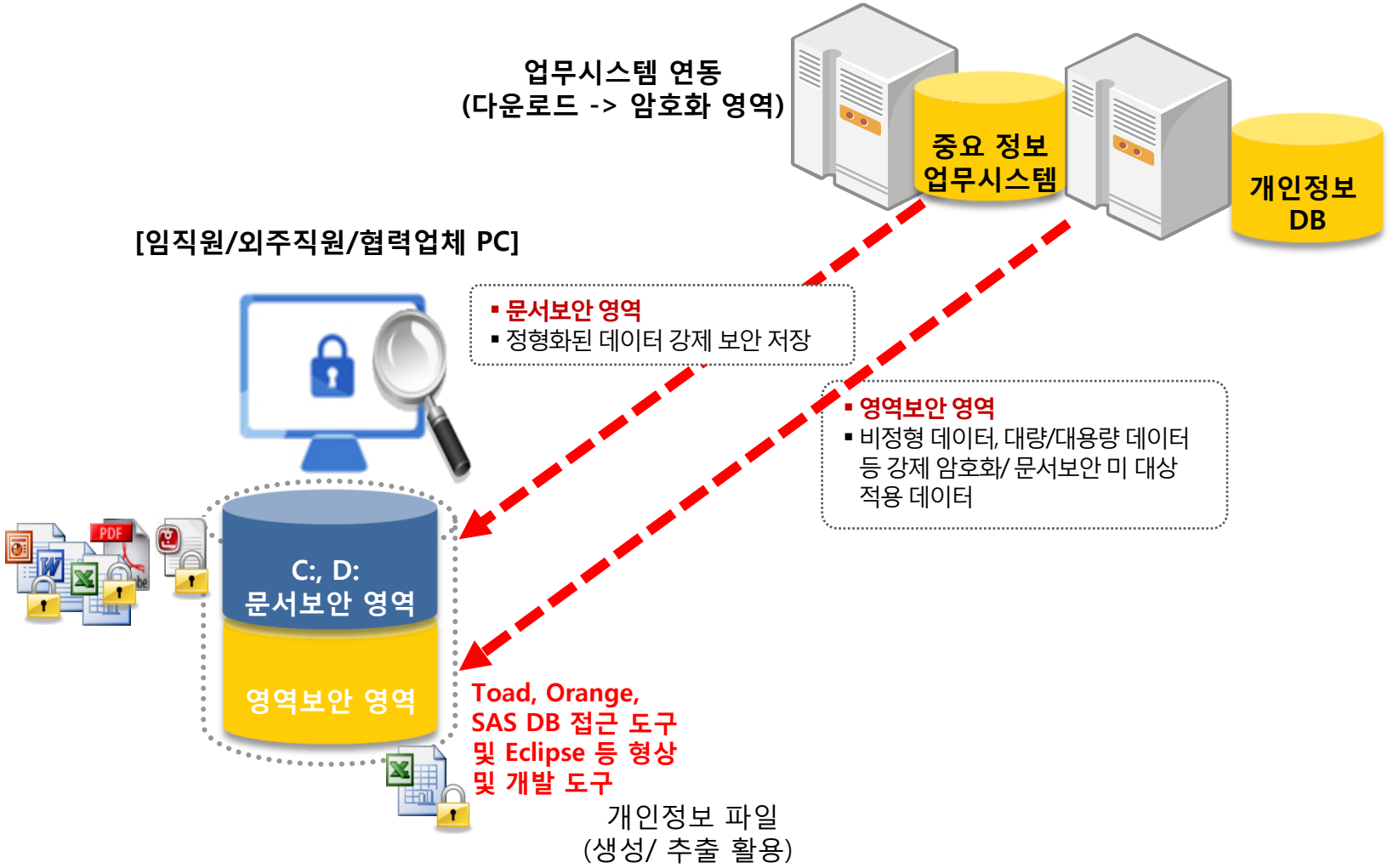
다양한 업무 시스템 및 업무용 프로그램 지원

- 어플리케이션(확장자)에 무관하게 제어/통제 가능
- 기존 업무시스템 연동을 통해 모든 업무 프로세스 상에서 일관된 보안 적용 가능

S-Work

문서보안 및 영역보안 통합 운영 방안> 통합 시스템 구성도

- 문서보안은 정형화된 문서파일에는 매우 효과적이지만, **비정형 데이터, 대량/대용량 데이터** 등의 문서보안에서 커버하지 못하는 분야는 **영역보안**으로 커버함으로써 높은 보안 수준을 구현

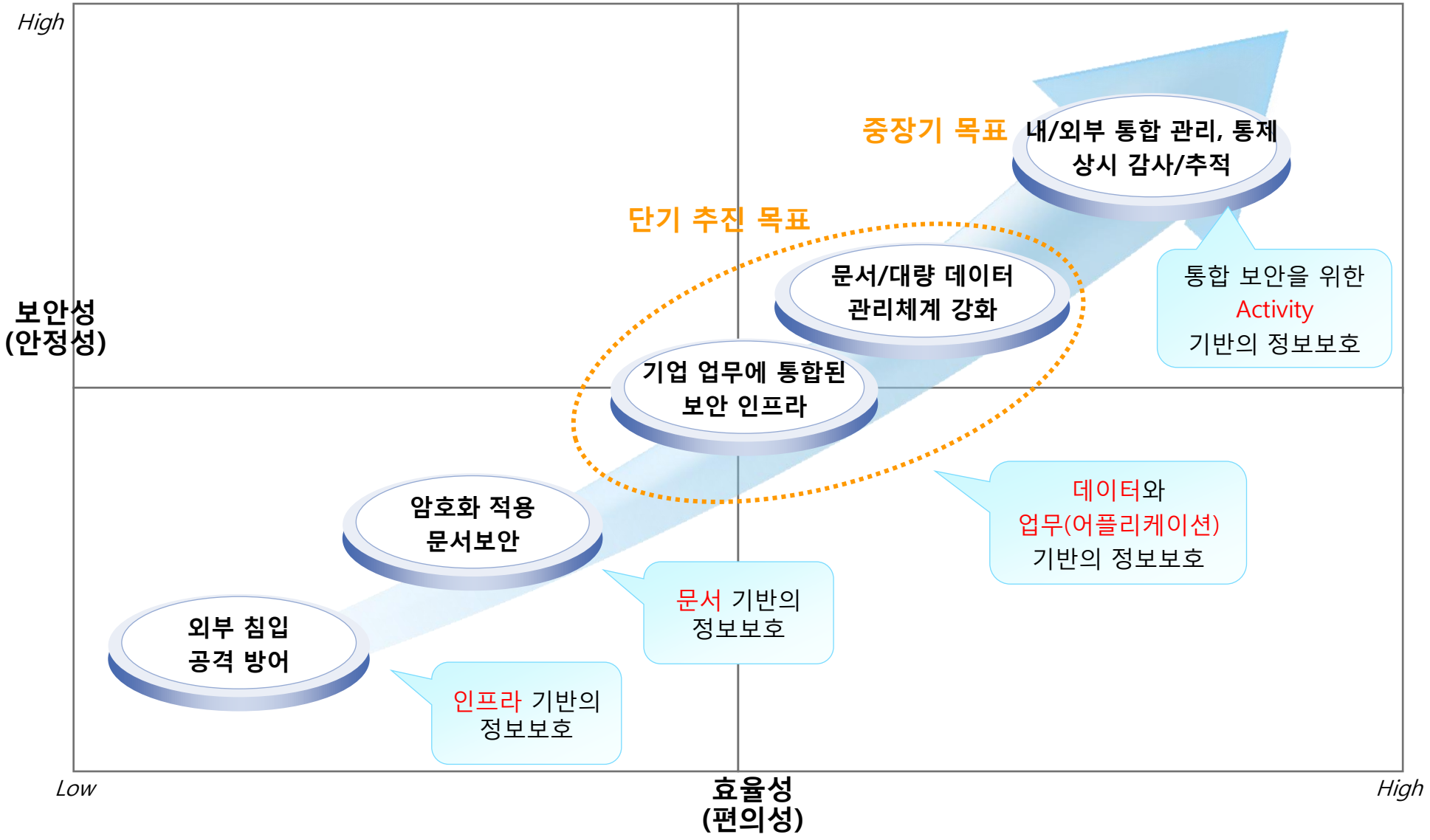


문서보안 및 영역보안 통합 운영 방안> 통합 시스템 구성도

영역보안 내 데이터는 해킹이나 사용자의 고의적인 정보 유출을 차단하며 데이터 유출이 발생할 수 있는 구간에 강력한 보안 정책을 통해 전 구간에 걸친 정보 유출 제어 및 문서보안과 연동을 통한 다중 보안 체계 구성 가능

통제 가능한 영역에서 자유로운 업무환경	속도, 대용량 암호화	업무환경이 최소로 변화된 보안 환경	Temp, Cache 영역까지 보안영역

정보보호 전략 - 단계별 보안 관리



정보보호 전략 - 단계별 보안 관리에 따른 소프트캠프 솔루션

기업 업무에 통합된 보안 인프라

내/외부 통합 관리, 통제 상시 감사/추적

문서/대량 데이터 관리체계 강화

- 외부 침입, 공격 대응
- PC가상화 기반 격리환경

- 외부 유입 파일 보안 관리
- 추적/상시 감시 및 통제

- 고객 정보 유출 방지
- 모든 컨텐츠 암호화(보안 적용 확대)
- 내부직원, 외주직원 자료 유출 경로 차단

Network Security ← → **End Point Security**

SHIELDEX

Document Security for Mobile

Document Security

SecureKeyStroke

S-Work

SoftCamp S-Work DI

MAXEON

소프트캠프는 기업의 단계적 보안 관리를 위해 Network에서부터 End Point Security를 위한 솔루션을 제공합니다.

SOFTCAMP

소프트캠프㈜
서울시 강남구 역삼동 828-7 한동빌딩 5층 (우) 135-080
Tel. 02-3453-9999, Fax. 02-3453-3033
http://www.softcamp.co.kr