IBM DB보안 솔루션
InfoSphere Guardium

Agenda

1. 개인정보보호법 규준에 따른 기술 조치
2. DB 암호화 – IBM Guardium Data Encryption
3. DB 감사/모니터링 – IBM Guardium Data Monitoring
4. WHY IBM Guardium? (법제 규준/제안 솔루션 특장점/구축)
5. 사례

정보관리에 관한 비즈니스 요건의 양면성 (공유와 보호)

The need to share documents

- 규제 요건에 대한 충족
- 확장 된 가치 사슬의 정보 공유 (계약자, 파트너, 아웃소싱 서비스 제공 업체)를 통해 생산성을 향상을 도모

The need to protect documents

- 수행업무에 국한된 최소한의 필요한 정보를 공개
- 업계의 특정 개인 정보 보호 규정 (PCI-DSS, PII, PHI, HIPAA, FOIA, 개인정보보호에 대한 법률 등) 준수

정보 공급 사슬

Reduce the Cost of Data

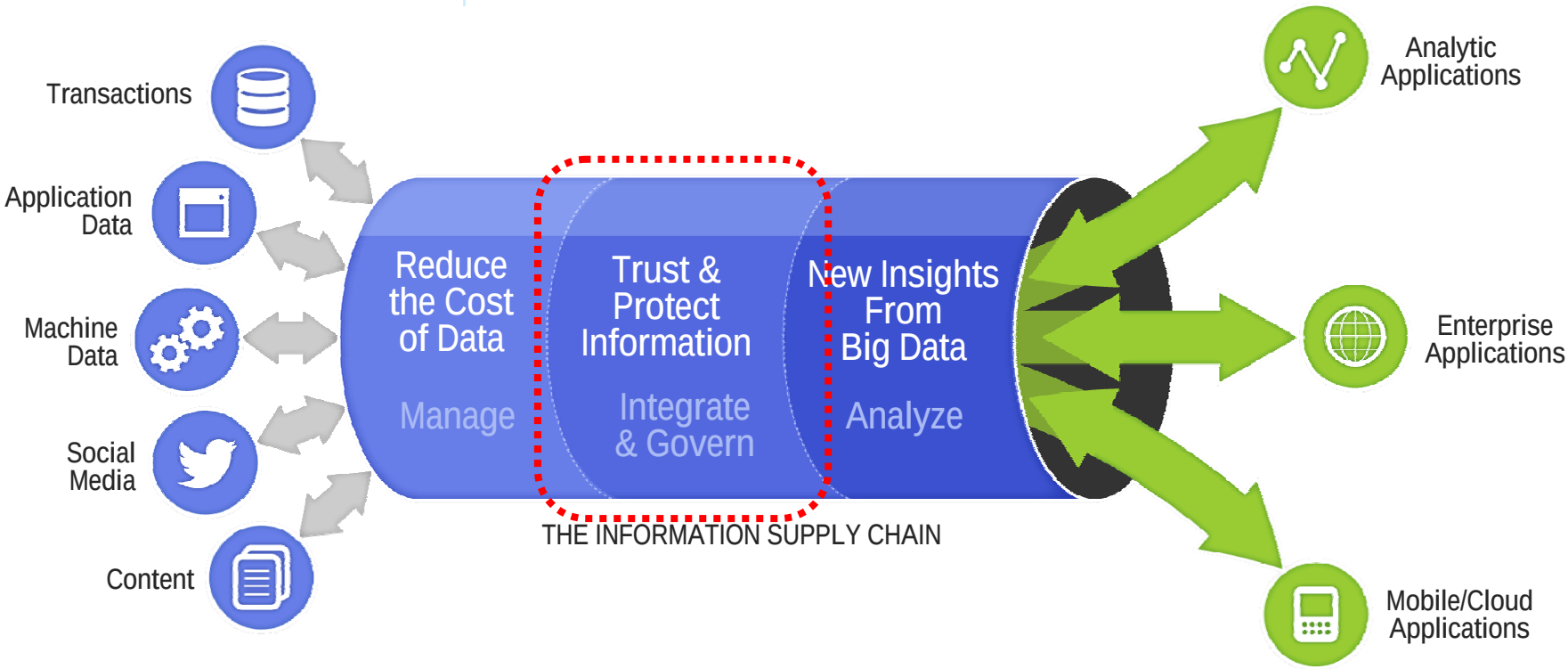
1. Replace Oracle Database
2. Enhance the Value of Your Data Management System
3. Archive Data to Reduce Cost
4. Increase Efficiency of Application Dev & Test
5. Data Warehouse Augmentation

Trust and Protect Information

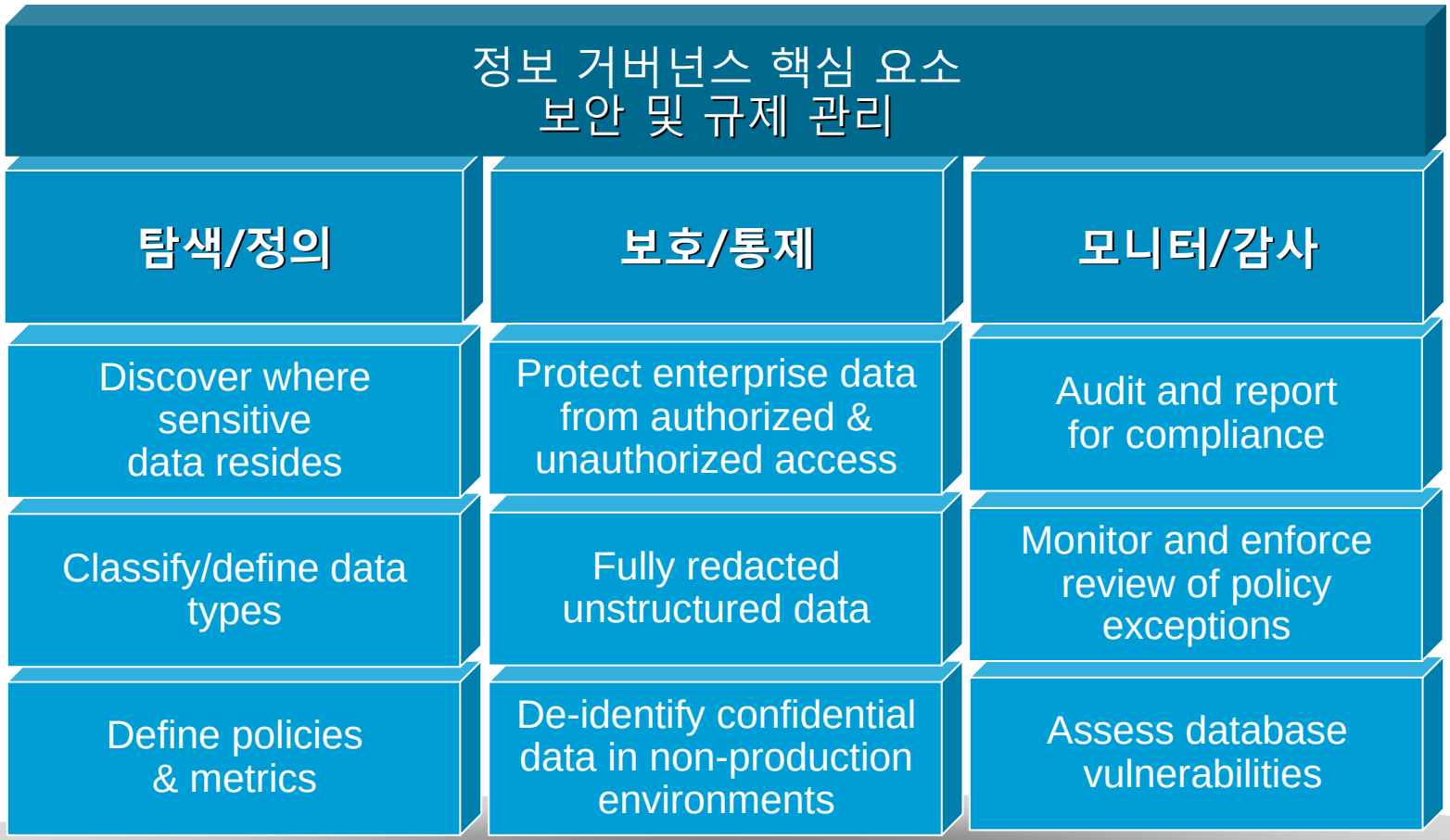
1. Trusted Information for Big Data and Data Warehousing
2. Act on a Trusted View
3. Consolidate & Retire Applications
4. **Secure & Protect Enterprise Data**

New Insights From Big Data

1. Rapid Warehouse Deployment for Deep Analytics
2. Real-Time Warehouse for Operational Analytics
3. Exploit New Data Sources



정보 거버넌스를 통한 보안/규제 관리 통찰력의 실행



> 데이터 보안 전략은 ***데이터베이스 감사 및 모니터링, 패치 관리, 데이터 마스킹, 접근 제어, 탐색/분류, 그리고 변경 관리를*** 포함해야 합니다 .
>
> *-- Why Enterprise Database Security Strategy Has Become Critical, Forrester Research, Inc, July 13, 2011*

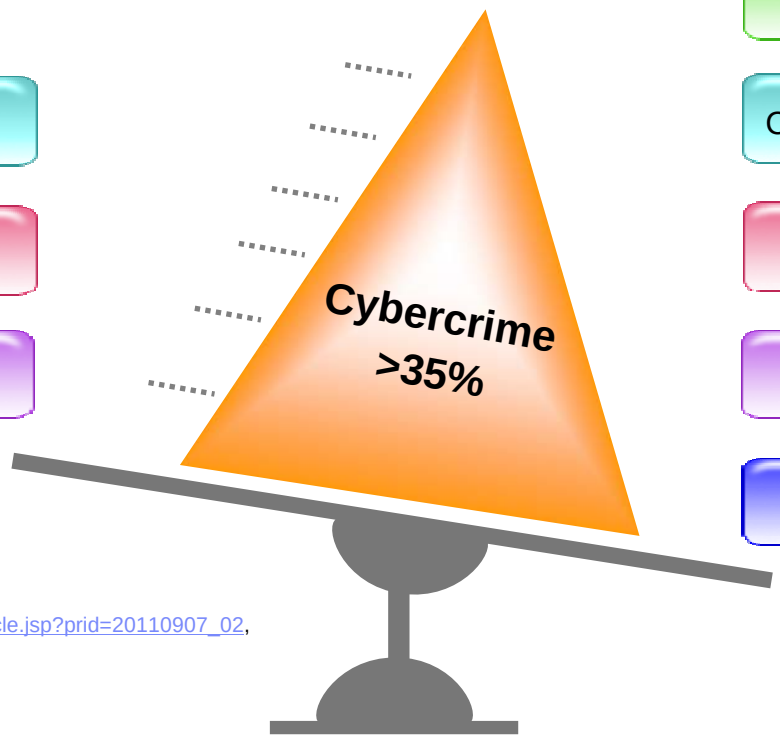
Agenda

1. **개인정보보호법 규준에 따른 기술 조치**
2. DB 암호화 – IBM Guardium Data Encryption
3. DB 감사/모니터링 – IBM Guardium Data Monitoring
4. WHY IBM Guardium? (법제 규준/제안 솔루션 특장점/구축)
5. 구축사례 및 Q&A

전세계 사이버 범죄시장은 블랙마켓(마약시장)보다 큼

Global Black Market on Drugs
$288B

- Marijuana
- Cocaine
- Heroin

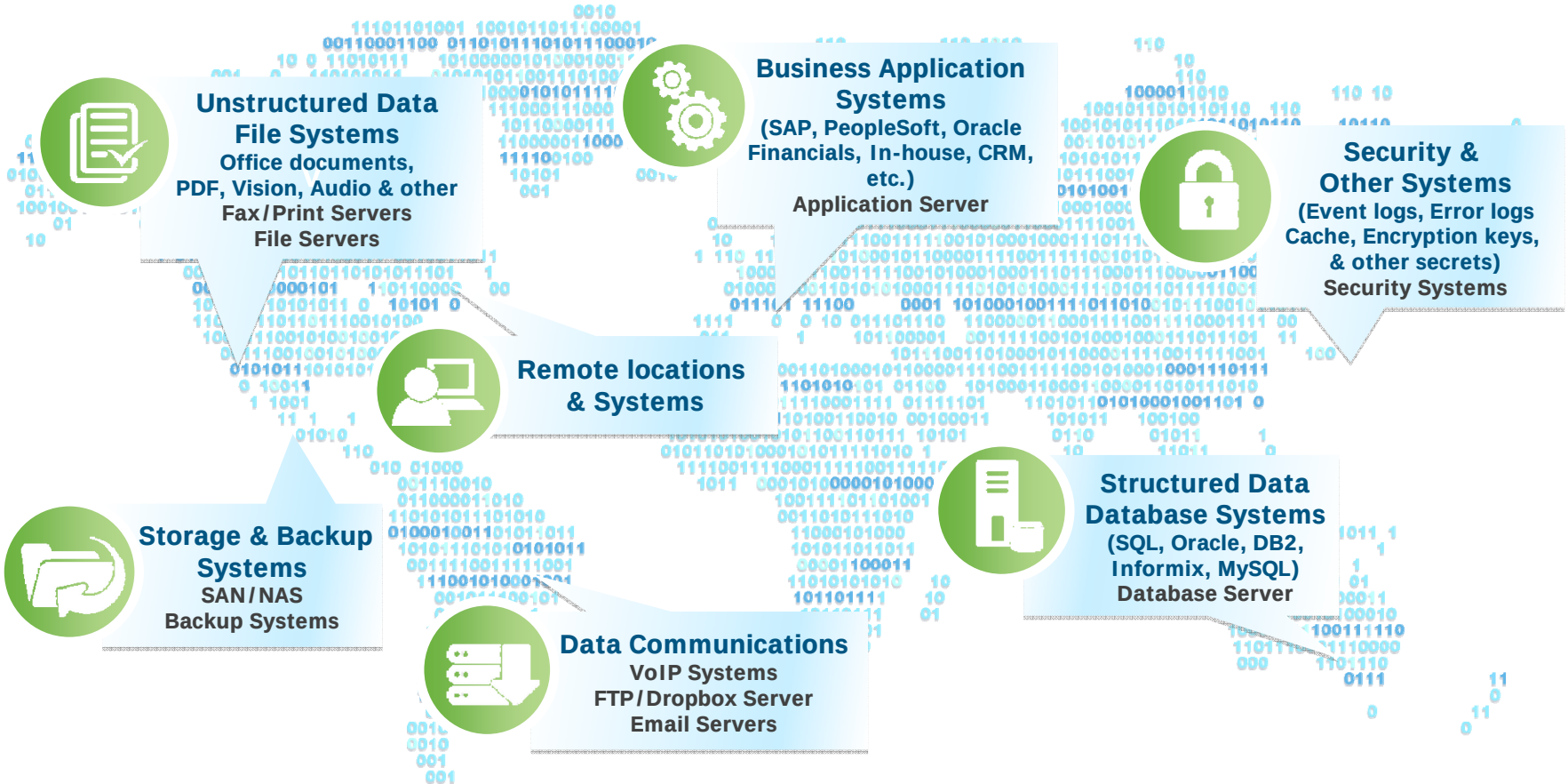


Cost of Global CyberCrime
$388B

- Online Scams
- Credit Card Fraud
- Phishing
- Malware
- Virus

http://www.symantec.com/about/news/release/article.jsp?prid=20110907_02, 2011년

개인정보보호와 보안되어야 할 데이터는 어디에 존재할까?
Protection of high value data



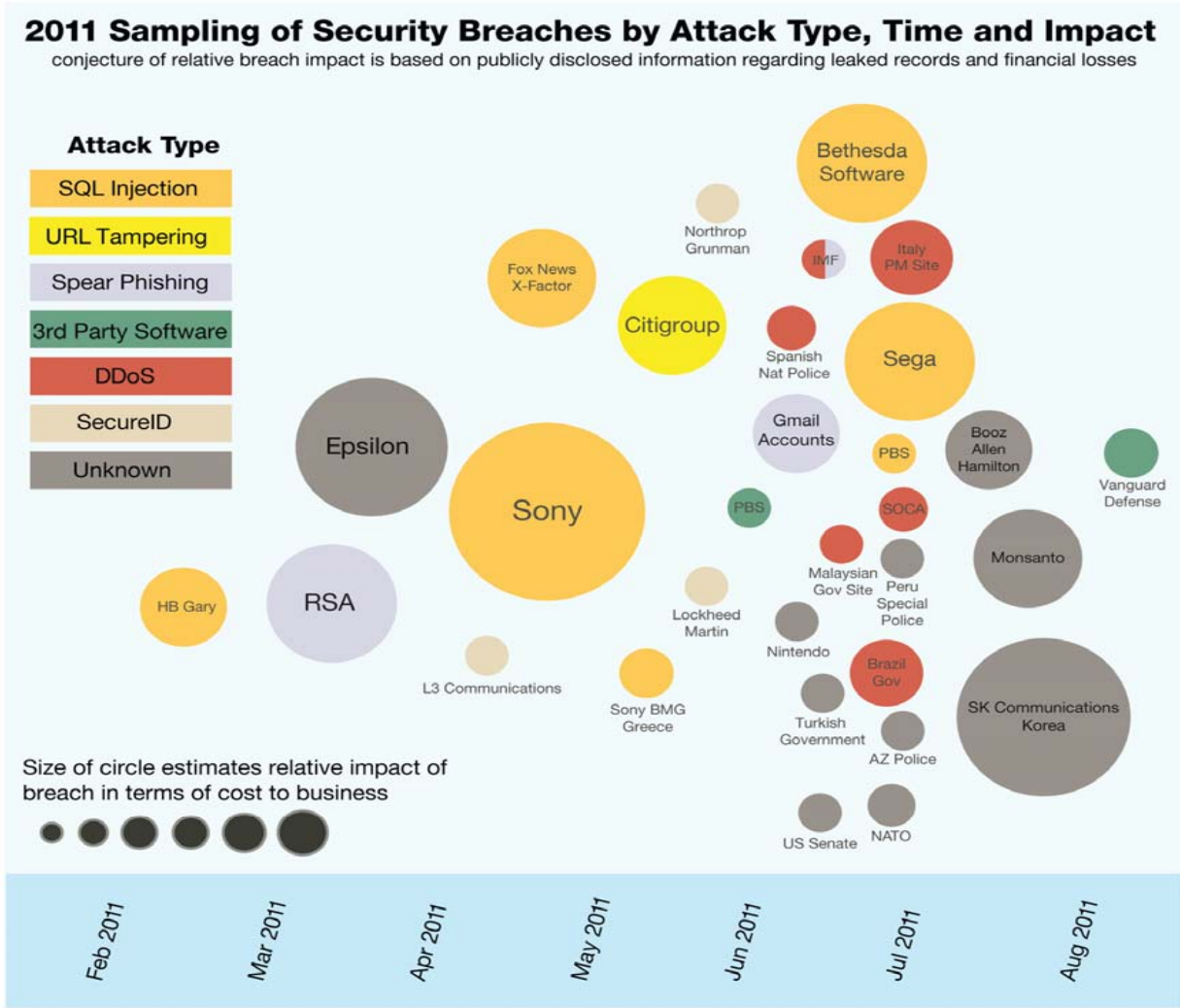
Sensitive data is EVERYWHERE

증가하는 보안 이슈 및 사고

외부 위협
전형적인 공격자가 아닌 외부의 공격자들로부터의 위험 증가

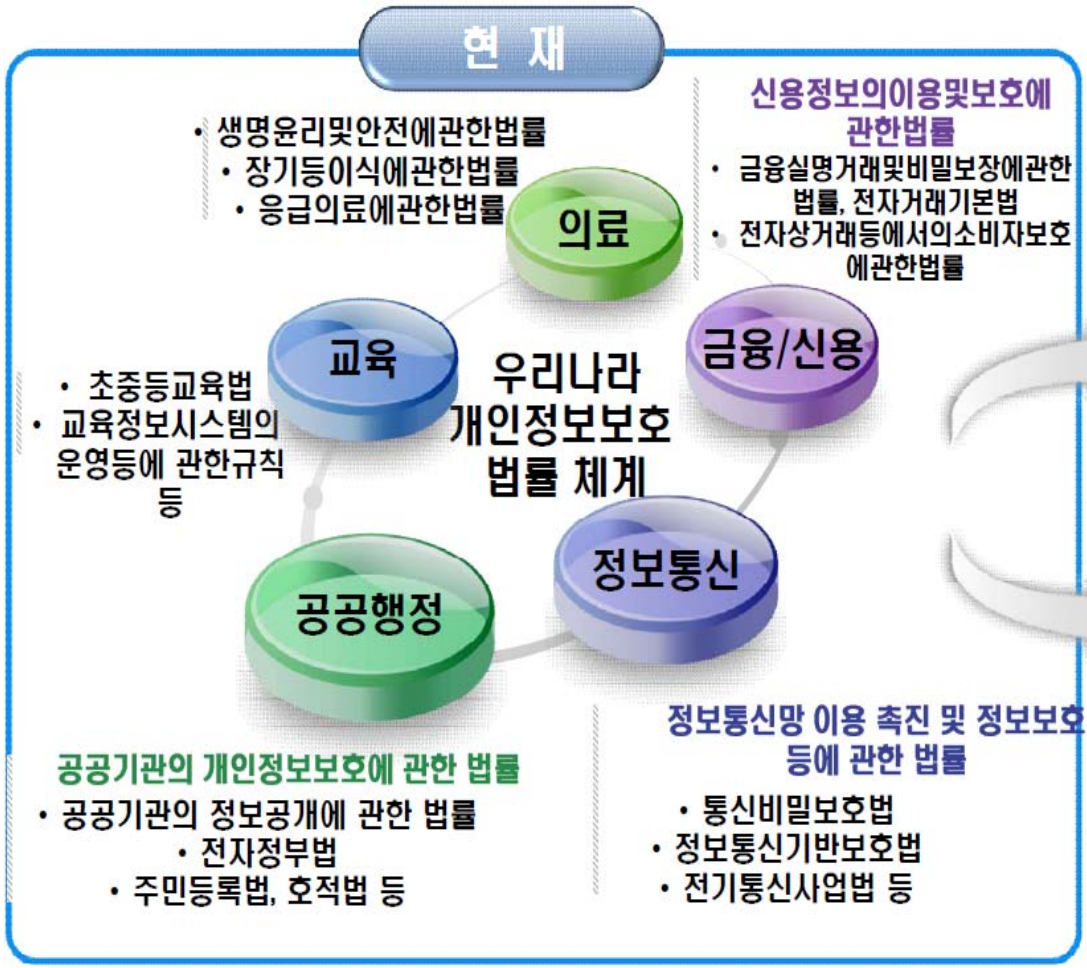
내부 위협
부주의하거나 악의적인 내부자 행동으로 인한 지속적인 위험

컴플라이언스
지속적으로 증가하는 법 규제를 준수하기 위해서는 성장 필요



Source: IBM X-Force® Research and Development

컴플라이언스 대응: 개인정보보호법 제정



제정안

개인정보 보호법
(법률 제10465호)
- 2011년 3월 제정, 9월 시행
- 현재까지 법제 변화중

개인정보 보호법

생존하는 개인에 관한 정보로서 성명, 주민등록번호(고유 식별 번호) 및 영상 등을 통하여 개인을 알아볼 수 있는 정보. (해당 정보만으로는 특정 개인을 알아볼 수 없더라도 다른 정보와 쉽게 결합하여 알아볼 수 있는 것을 포함한다.)

개인정보보호법에 필요한 관리적/기술적 보호 조치

개인정보 내부관리계획 목차 (예시)

제1장 총칙
제1조(목적)
제2조(적용범위)
제3조(용어 정의)
제2장 내부관리계획의 수립 및 시행
제4조(내부관리계획의 수립 및 승인)
제5조(내부관리계획의 공표)
제3장 개인정보관리책임자의 의무와 책임
제6조(개인정보관리책임자의 지정)
제7조(개인정보관리책임자의 의무와 책임)
제8조(개인정보취급자의 범위 및 의무와 책임)
제4장 개인정보의 처리단계별 기술적·관리적 보호조치
제9조(물리적 접근제한)
제10조(출력 복사시 보호조치)
제11조(개인정보취급자 접근 권한 관리 및 인증)
제12조(개인정보의 암호화)
제13조(접근통제)
제14조(접근기록의 위변조 방지)
제15조(보안프로그램의 설치 및 운영)
제5장 정기적인 자체감사
제16조(자체감사 주기 및 절차)
제17조(자체감사 결과 반영)
제6장 개인정보보호 교육
제18조(개인정보보호 교육 계획의 수립)
제19조(개인정보보호 교육의 실시)

1. 개인정보보호책임자 지정 및 전담조직 강화
2. 개인정보보호 정책 지침 등 규정 정비
3. 개인정보보호 컴플라이언스 활동 강화
4. 전사적인 개인정보보호 관리체계 수립 및 이행
5. 개인정보처리시스템의 안전성 강화
6. 개인정보취급에 대한 관리 감독 및 교육 강화

필요한 관리적/기술적 보호조치 내용

	정보 보호 관리 체계 구축	
계정 접근관리 (최소 5년)	계정/권한 관리보호 조치	통합 권한 관리
	인증: PKI, 보안 토큰, 휴대폰 인증, OTP	
DB암호화	DB 암호화/마스킹	암호화
접근통제	시스템/네트워크/End-Device 보안 -침입 차단/탐지/방지 시스템 -웹 방화벽 시스템 -보안 운영 체제	데이터 마스킹
	애플리케이션 보안	데이터 유출 방지
	불필요한 데이터에 대한 폐기	라이프사이클관리
로그관리 (최소 1년)	접속 로그 기록 -접근 기록 및 실시간 모니터링 솔루션 -접속기록 백업 솔루션	DB 모니터링/로깅
보안프로그램	내부정보 유출 방지 -자료 유출 방지 시스템 -문서 암호화 시스템	문서 마스킹
	악성 프로그램 방지 -백신 소프트웨어 -패치 관리	
	출력/복사 보호조치 - 디지털 워터마킹	

개인정보보호법 암호화 관련 법제 검토

✓ **개인정보 규정의 모호함: "개인정보", "개인기록", "고유식별번호" 모두 포함해야 한다.**

[수정권고안] 개인정보란 생존하는 개인에 관한 정보 또는 그 정보의 묶음으로서, 그 정보 속에 포함되어 있는 개인의 성명, 식별번호나 부호, 또는 지문/사진/화상과 같은 당해 개인의 고유한 식별자에 의하여 개인을 식별할 수 있는 정보를 말한다. 이 개인정보에는 당해 개인에게 내린 다른 사람의 평가나 의견이 모두 포함된다.

이제 시작이다!!!

✓ **"처리"의 개념적 적정성 관련 법률고도화:**

처리란 정보의 수집, 생성, 기록, 저장, 보유, 가공, 편집, 검색, 출력, 정정, 복구, 이용, 제공, 공개, 파기 및 그 밖에 이와 유사한 일체의 행위를 말한다. (제2조 제2호)

-→ 이는 개인정보가 저장소에 위치한 상태로 보호받는 조치를 하는것 뿐 아니라, 실제 처리 과정에서도 암호화 등의 조치가 선결과제로 유권해석 된다.

개인정보보호법 암호화 관련 법제 검토

✓ **입법체계 평가를 통한 향후 입법 심화 및 수정에 대한 동향**

- 현재 대두되는 입법체계 수정 및 보충 방안은

  1) 분리형 일반법제정론

  2) 통합형 일반법제정론

  3) 통합형 기본법제정론

  으로 대두되고 있다.

- 이중 현재 특장점에 의한 법제연구원의 권고 방안은 **"통합형 일반법제정론"**으로 무게가 쏠리고 있다.

- 공공부문과 민간부문을 **통합한 입법체계를 지향하면서도** 일반적으로 개인정보의 취급자가 준수해야 할 의무와 정보주체의 각종 권리 등에 관한 실체적 사항은 물론 권리행사의 방법과 절차, 피해구제, 감독기관 등 절차적 사항까지 폭 넓게 규정하자는 입장이다.

- **공공/민간부문의 부문별 차등이나 민간 내에서의 업종의 차등이 없이 규제한다는 것이 "통합형 일반법제정론"이다.**
  이는 프라이버시권을 침해한다는 점과 그것이 위법하다는 점에는 ***부문이나 산업의 차이, 취급자의 규모와 상관없으므로 모두 개인정보처리업무를 행함에 있어서 동일한 법적 규율을 받아야 한다는 취지이다.***

- 민감한 고유식별자는 취급자의 구분이 중요한 것이 아니라, 취급되는 개인정보에 따라 차등 적용되어야 한다.

개인정보보호법 규준에 따른 기술 조치

- 개인정보 보호법 발효 (2011년 9월 30일) – 개인정보에 대한 기술적 보호 조치 (개인정보 – 고유식별정보 에 대한 DB 암호화 조치) 의무화에 대한 준수 및 기업의 가장 소중한 자산인 고객정보(DB)에 대한 유출 통제 및 차단 방안 마련이 필요한 실정 임

기업이 대비해야 하는 사항

법률적인 준수 사항 대비

- **개인정보 보호법 발효 (2011년 9월 30일) – 개인정보에 대한 기술적 보호 조치**
- **개인정보 보호법 계도기간 만료(2012년 3월 31일) 에 따른 실태조사에 대한 대비 필요**
- **개인정보 보호법 및 개별법에 따라 개인정보 및 고유 식별 정보에 대한 암호화 필수!!!**

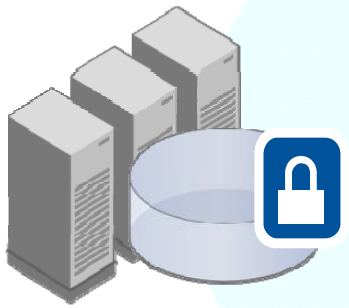
기업의 정보 보안 체계 구축

- **기업의 중요한 자산 (고객정보, 및 기밀정보)에 대한 유출 통제 및 차단 방안 체계 구축 필요**
- **외부의 악의적인 침입 및 공격으로부터 고객정보를 보호 방안**
- **고객정보 유출 시 발생할 수 있는 소송 및 피해 최소화 방안**

개인정보보호법 규준에 따른 기술 조치

- 개인정보 보호법 발효 (2011년 9월 30일) – 개인정보에 대한 기술적 보호 조치 (개인정보 – 고유식별정보 에 대한 DB 암호화 조치) 의무화에 대한 준수 및 기업의 가장 소중한 자산인 고객정보(DB)에 대한 유출 통제 및 차단 방안 마련이 필요한 실정 임

고객정보(DB) 보안에 따른 Pain point & Issue



보안 대상 및 솔루션 선정

- **어떤 기술을 사용하여 무엇을 암호화 할 것 인가?**

파급 효과 최소화

- **구축에 따른 기업의 업무 환경의 파급효과를 어떻게 최소화 할 것인가?**

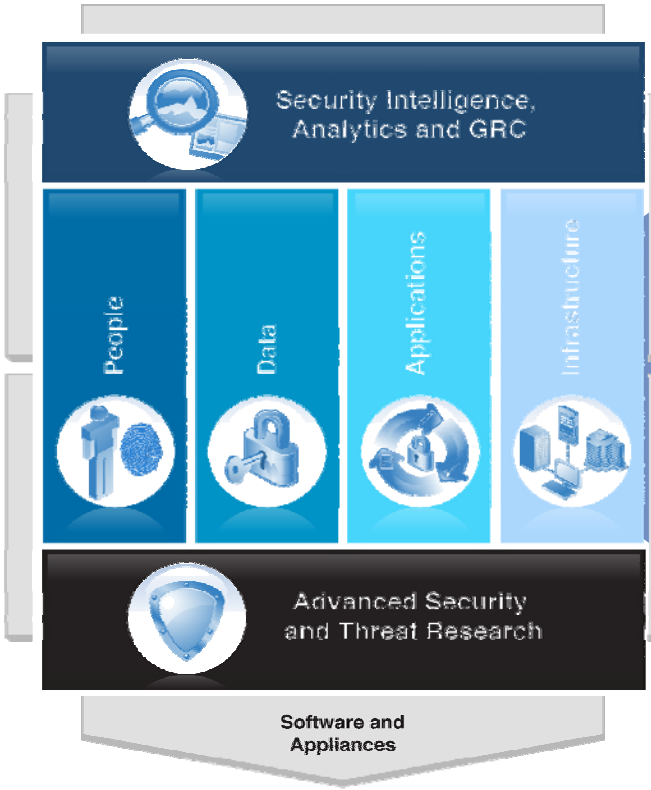
속도 및 성능 이슈

- **보안 기술 적용에 따른 속도 및 성능 이슈 발생 (CPU/Memory 사용량 증가)에 따른 이슈 발생 가능성은?**

보안적용 및 운영

- **고객정보DB에 대한 보안 적용 및 운영할 수 있는 전문적인 지식과 능력 확립 방안은 무엇인가?**

전사 보안을 위한 IBM Security Framework



사람
기업 자산에 접근하는 사용자와 관련된 위험 완화

데이터
민감한 데이터의 접근과 사용에 대한 통제의 이해, 배포, 적절한 테스트

어플리케이션
어플리케이션의 보안성 유지, 악의적 사용과 사기 방지, 실패에 대한 강도 제공

물리적 인프라스트럭처
물리적 인프라스트럭처의 원하는 상태를 갖는 행동 가능한 지능 제공과 향상

데이터 보안

- 데이터 유출 방지
- 통합 권한 관리
- 암호화와 키/라이프사이클 관리
- 메시징 보안
- 데이터베이스 모니터링과 보호
- 데이터 마스킹

이메일 보안

보안 정보와 이벤트 관리, 로그 관리

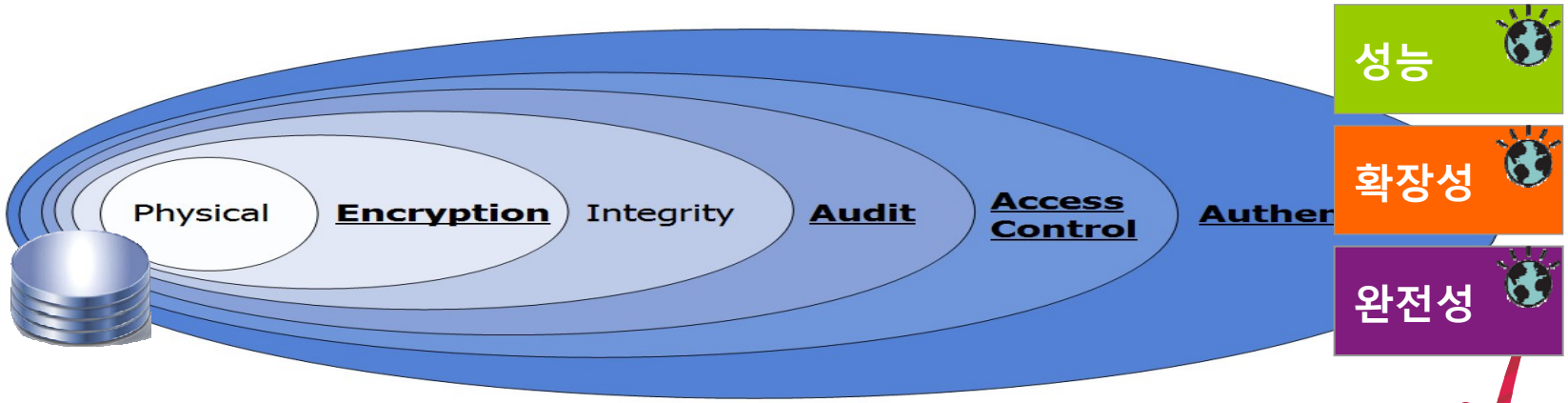
고객정보 (DB) 보호 방안

DB 암호화	DB 모니터링/Access Control	애플리케이션서버&Client
• DB 파일 단위 암호화 • 테이블 내 칼럼단위 암호화 • 암/복호화 키관리 메커니즘 • 데이터 유출 시에도 강력한 암호화 방식으로 해독 불가 • DB암호화에 의한 데이터 유출 원천 차단	• 미권한자 데이터 Masking • 의심사용자 일정기간 격리 • 애플리케이션 제어 • DB 사용자 접속 제어 • DB 테이블, 컬럼별 제어 • 수행 명령어 제어 • DB 접속 시간제어 • 접근 권한별 접속제어 • 사후 감사	• Network Access Control • 보안 프로그램 (Antivirus) 설치 • 계정 및 비밀번호 관리 • 애플리케이션 제어 • 사후 감사

보안 성숙도 및 안전성

100% ← 0%

기업의 전사 보안 체계 구축 흐름



Network-driven	Application-driven	Data-driven
▪ 외부 침입 차단 및 방어	▪ 어플리케이션을 보호	▪ **데이터 보호**
▪ 방화벽(Firewall) ▪ IPS(침입방지시스템) ▪ IDS(침입탐지시스템) ▪ 네트워크 취약점 진단	▪ 웹 방화벽 ▪ 어플리케이션 취약점 진단	▪ **데이터베이스 모니터링** **- 로깅** **- 감사** ▪ **데이터 유출방지 (DLP)** ▪ **데이터 암호화** **- 암호화** **- 마스킹**
▪ 경계 네트워크 보호	▪ 서버/어플리케이션 보호	▪ 단말 데이터베이스 보호

전사 데이터 보안을 위한 지원 영역

데이터 보안의 5가지 핵심 영역

1 DB 내 민감한 데이터의 식별

민감한 데이터 및 전사 데이터 연관도 자동 탐색

- *업무 데이터 그룹 정의를 위한 논리적인 데이터 연관도 파악*
- *민감한 데이터 자동 탐색*
- *데이터 프로토타입 및 로직에 대한 리버스 엔지니어링*

InfoSphere Discovery & InfoSphere Guardium

2 비운영 환경 내 실 데이터 변환

개발, 테스트 DB 내 민감한 데이터 보호

- *테스팅 시 민감한 데이터 보호를 위한 베스트 프랙티스*
- *실제적인 유사 데이터를 사용하여 일관성 있는 정보 변환*
- *비운영 환경 내 내부유출자 및 외부 침입자의 정보 유출 방지*

InfoSphere Optim Data Masking

3 DB 모니터링 /취약성 평가

이기종 환경 내 DB 정보 보호를 위한 필수 안전망 제공

- *지속적인 실시간 데이터베이스 활동 모니터링*
- *미승인 접근 및 유해 활동 탐지를 위한 정책 기반 DB 접근제어*
- *DB 보안 취약성 평가*
- *DB 변경 내역 감지 및 접근 차단*

InfoSphere Guardium DAM & VA Solution

4 DB 환경 암호화

고성능 데이터 암호화

- *Data Encryption tool*
  - *-애플리케이션 변경 없이 테이블 단위 암호화*
  - *-DBA와 보안담당자의 직무 분리*
  - *-통합적이고 중앙 집중적인 정책 및 키 관리*
- *DB2 Built-in 함수*
  - *-컬럼 단위 암호화*

InfoSphere Guardium Data Encryption

5 비정형 데이터 문서 내 주요 정보 변환

문서/양식 내 민감한 데이터에 대한 보호

- *텍스트, 그래픽, 양식 기반 데이터에 대한 정보 변환 지원*
- *자동화를 통한 효율성 향상 및 수작업 대비 비용 절감 효과*
- *정책 기반 사용자 별 데이터 조회 통제*

InfoSphere Guardium Data Redaction

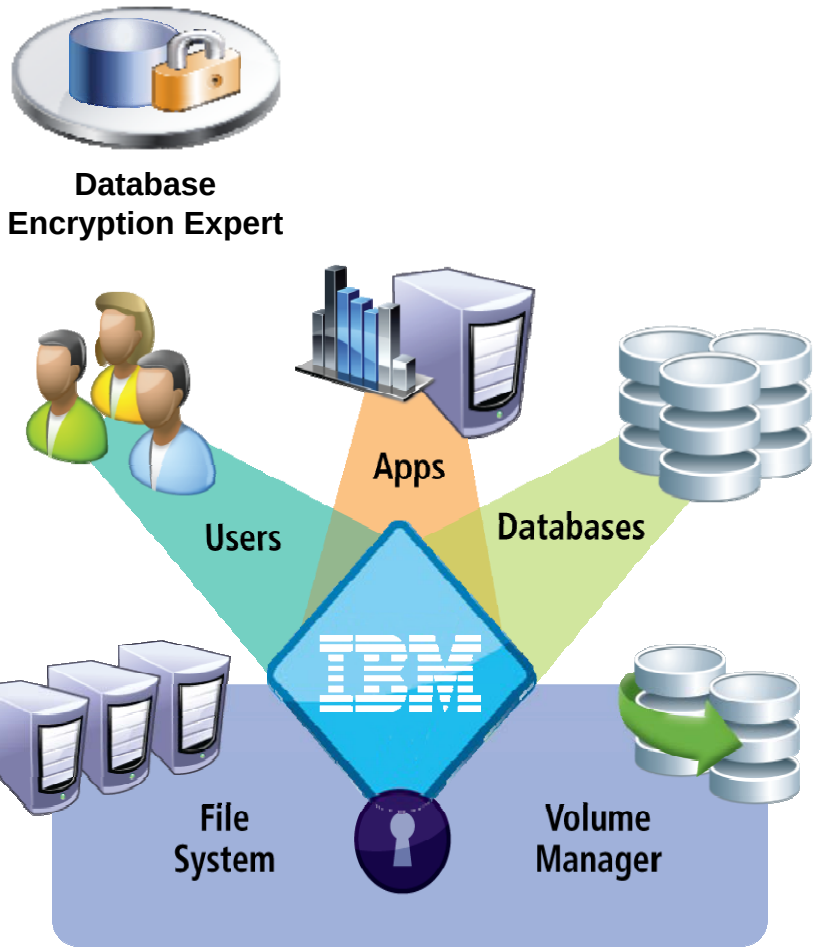
법적 규제 준수

Agenda

1. 개인정보보호법 규준에 따른 기술 조치
2. **DB 암호화 – IBM Guardium Data Encryption**
3. DB 감사/모니터링 – IBM Guardium Data Monitoring
4. WHY IBM Guardium? (법제 규준/제안 솔루션 특장점/구축)
5. 구축사례 및 Q&A

IBM InfoSphere Guardium Data Encryption

IBM Guardium Data Encryption (GDE) 는 데이터 암호화 및 암호화 Key 관리를 위한 포괄적인 솔루션을 제공합니다. 기업에서 사용하는 모든 주요 플랫폼 (Linux, Unix, Windows) 및 클라우드 환경의 암호화를 지원하며, 암호화를 통하여 기업의 데이터를 보호하고 규제 준수를 강화합니다.



DATA 암호화
데이터 유출 원천적 차단
정형 및 비정형 데이터 암호화

투명한 연동
쉬운 설치 및 구현
Source Code 수정 없음

OS 접근제어
OS User & Process 접근제어
File system & Volume 에 대한 접근제어

중앙 관리
클라우드 환경에서의 암호화 제공
모든 DBMS를 중앙에서 관리

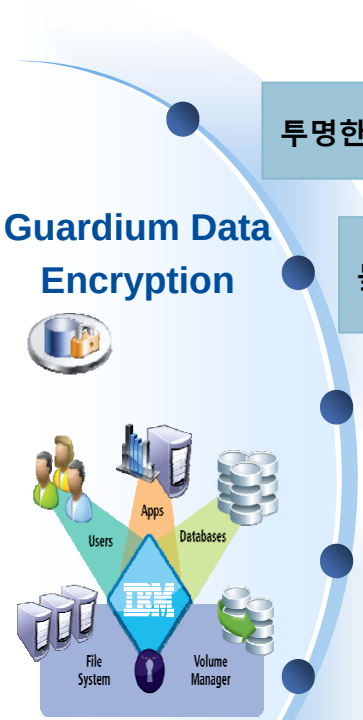
암호화 KEY 관리
자체 HSM 기능을 수행
FIPS 140-2 Level 2/3 키 관리 인증

암호화 후 성능보장
암호화 후 최소 성능 Impact

Guardium Data Encryption 솔루션 특장점

- Guardium Data Encryption 은 아키텍처 구성부터 우수한 성능 및 보안기술을 통해 안전한 데이터 보안을 구현할 수 있는 제품 입니다.

Guardium Data Encryption 특징



투명한 연동	OS, DB , Storage 등의 인프라가 변경되지 않음 ▪ DB 구조나 스키마에 영향을 주지 않아 애플리케이션 수정이 필요하지 않음
높은 호환성	▪File 단위 암호화를 지원하며, 다양한 DBMS의 종류와 버전을 지원함
암호화 기술	▪ 데이터 관리에 영향을 미치지 않는 기밀 데이터 암호화 ▪ 고성능 암호화 지원을 위한 탁월한 아키텍처
KEY 관리 암호화 알고리즘	▪3DES, AES128/256, ARIA128/256 등 강력한 암호화 알고리즘 제공
중앙화 된 관리	▪ 단일 UI 로 다수의 서버 중앙 통제 관리 ▪ 주요 데이터에 대한 암호화 키 관리의 중앙화 및 HA 지원
고성능 보장	▪ 초기 마이그레이션 시 파일 copy와 같은 수준의 암호화 성능 제공 ▪ 조건범위검색을 지원하며 암호화 전후 성능 저하 최소화

우수한 성능 및 보안성

안전한 키관리 알고리즘

투명한 연동성

어플리케이션 및 운영환경 변경 최소화

높은 호환성

FILE 단위 암호화지원
다양한 DBMS 및 OS 지원

Guardium Data Encryption 특징

정형 및 비정형 데이터 보안

- **고성능 암호화**
- **접근제어/직무 분리**
  사용자/그룹, 파일/폴더/raw device, 프로세스, 위치, I/O 타입, 시점 별 정책 및 접근제어
  인프라 변경 없이 System Admin 마스터 사용자에 대해서 접근 제어 가능
- **로깅/감사 수행**
  - ✓ 암호화 정책, 키 관리 이력
  - ✓ 암호화 내역
  - ✓ 데이터 접근 이력

DB, 애플리케이션, 스토리지에 대한 투명성 제공

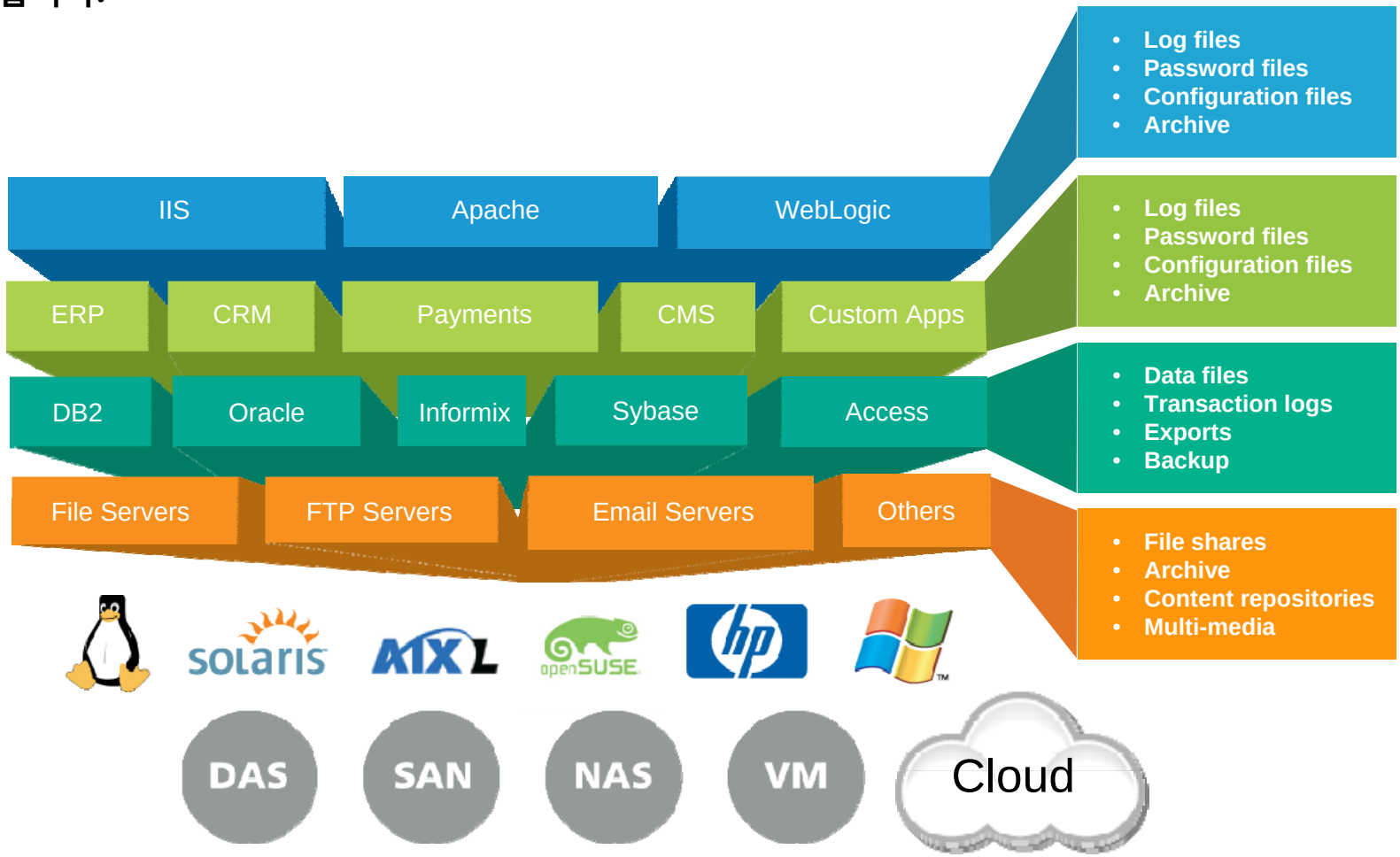
- **Big Data 암호화 지원**
- **기존 IT 인프라스트럭쳐/애플리케이션 코드 수정 없음**
- **온라인 및 오프라인 백업 환경 지원**
- **사용자 조회 일관성 보장**

전사 내 다수 DB에 대한 중앙 통제 관리

- **암호화 정책 및 암호키 관리**
- **감사 로그/리포트**
- **가용성 보장**

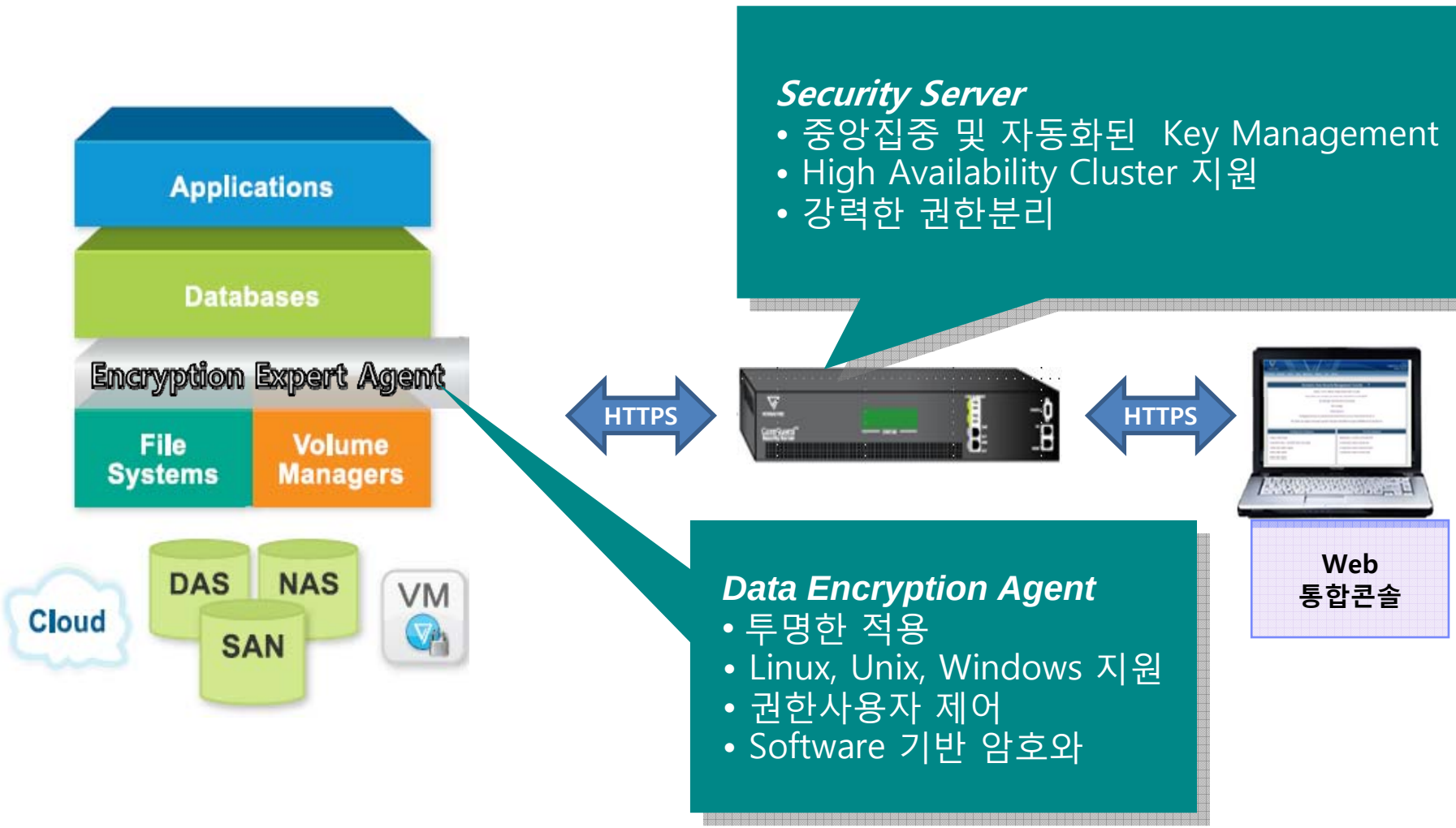
Guardium Data Encryption 적용범위

GDE는 다양한 DBMS 뿐만 아니라 미들웨어 , 다양한 어플리케이션 및 file server, ftp server 등의 데이터와 백업파일 및 DB 설정정보까지 저장되는 모든 정형 및 비정형 데이터들에 암호화를 적용 할 수 있습니다.



Guardium Data Encryption 구성 아키텍처

GDE 는 대상서버에 설치되는 Agent 와 Appliance로 구성되며, File System 및 Volume에 대한 암호화를 지원합니다.



Guardium Data Encryption 지원 플랫폼

GDE 는 정형 및 비정형 데이터의 암호화를 지원하며 다양한 DBMS, OS 환경을 지원합니다.

정형 및 비정형 데이터 타입 지원

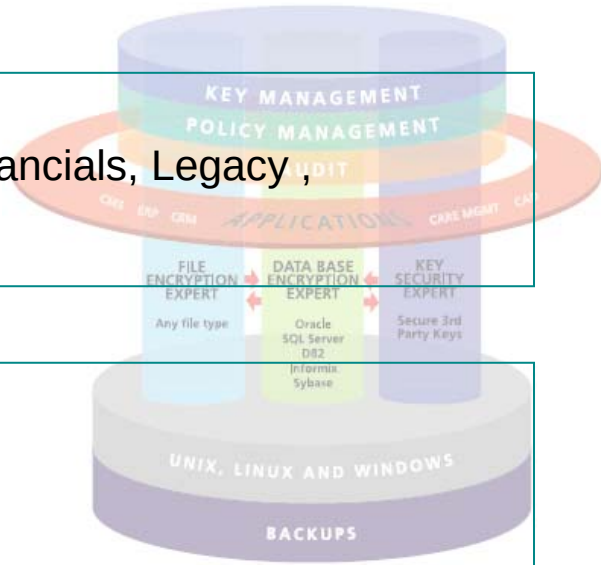
Microsoft Office documents, PDF files, or Extract-Transform-Load (ETL) data

DBMS 지원

All versions of Oracle, DB2, SQL Server, MySQL, Post-GreSQL, Informix, Sybase

Application 지원

SAP, Siebel, People-Soft, FileNet, Documentum, Oracle Financials, Legacy , custom application

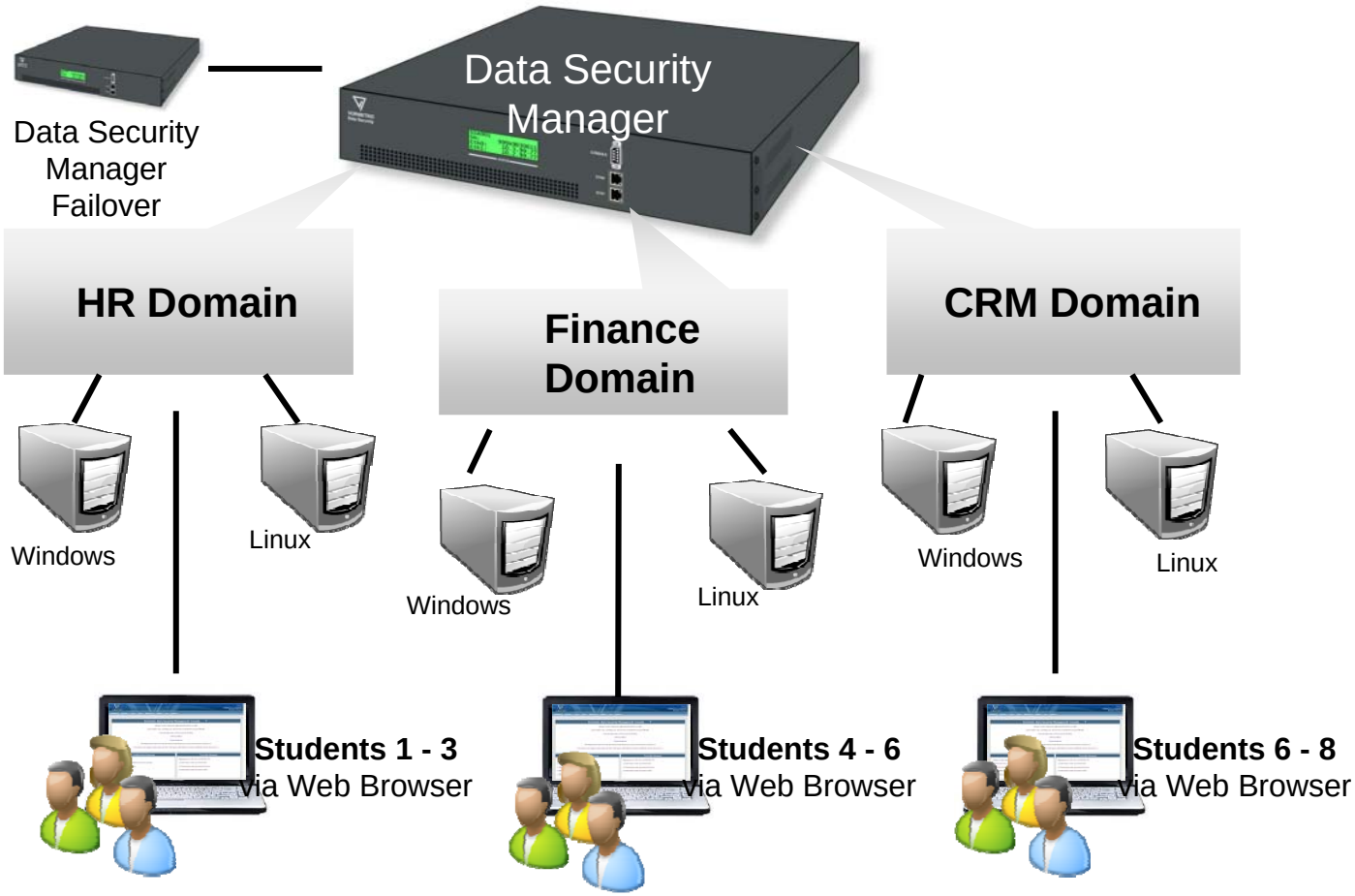


OS 지원

Windows 2000, XP, Vista, Windows Server 2003, 2008
AIX / Solaris / HP-UX
Red Hat Enterprise Linux / SuSE Linux Enterprise Server

Guardium Data Encryption 특장점 – 투명한 DB 연동

Security Server 는 Agent와 Appliance간의 TCP 통신만 가능하면, 네트워크적인 위치에 관계없이 OS, DB, 어플리케이션의 변경 없이 설치 및 연동이 가능합니다.



Guardium Data Encryption 특장점 –Key 보호 및 직무분리

GDE 는 자체적으로 Key 관리를 수행하며, 관리자들을 위한 직무분리 기능을 지원합니다.

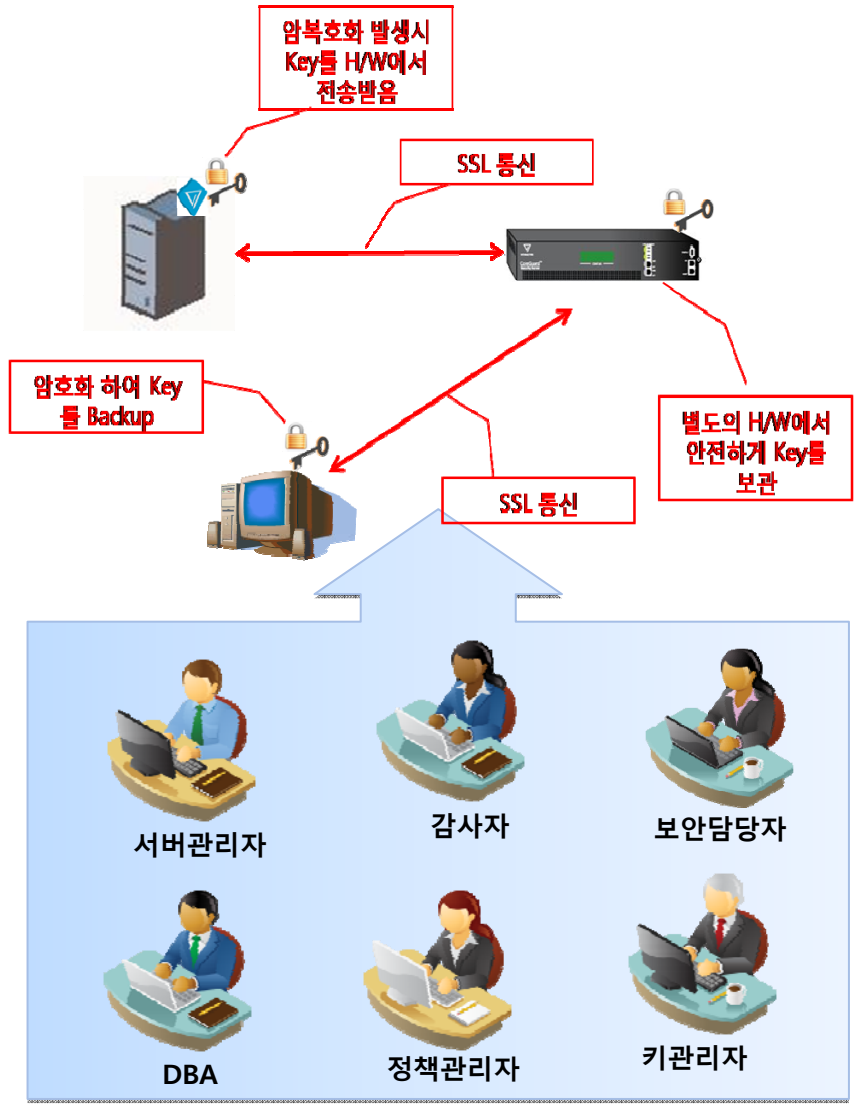
기술규준 충족 – 키관리/ 직무분리

다양한 알고리즘 지원
- AES128/256, 3DES, ARIA 128/256 알고리즘
- Guardium Security Server에서 안전하게 생성 및 관리

Appliance와 Agent간에 Secure Channel (SSL)을 이용한 안전한 Key 배포

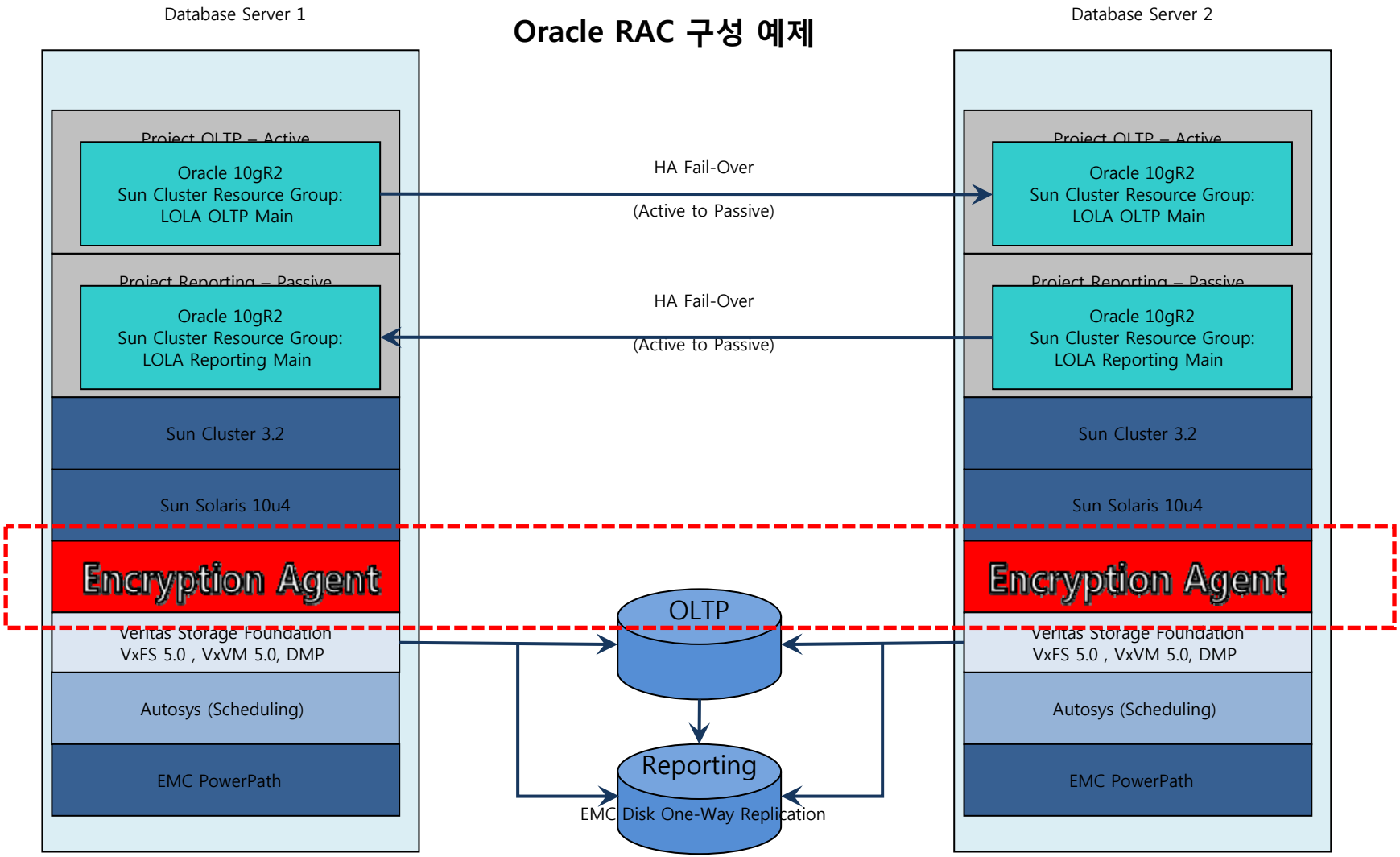
Key를 File로 Backup시 암호화해서 Backup하게 되며, 복호화를 위한 Master key는 Appliance에서만 보관하고, 어떠한 user도 Master key에는 접근이 불가능

암호화 키 및 정책은 정기적으로 백업하여 파일로 보관함으로, Appliance Fault 발생시 대체 장비를 통해 restore 지원



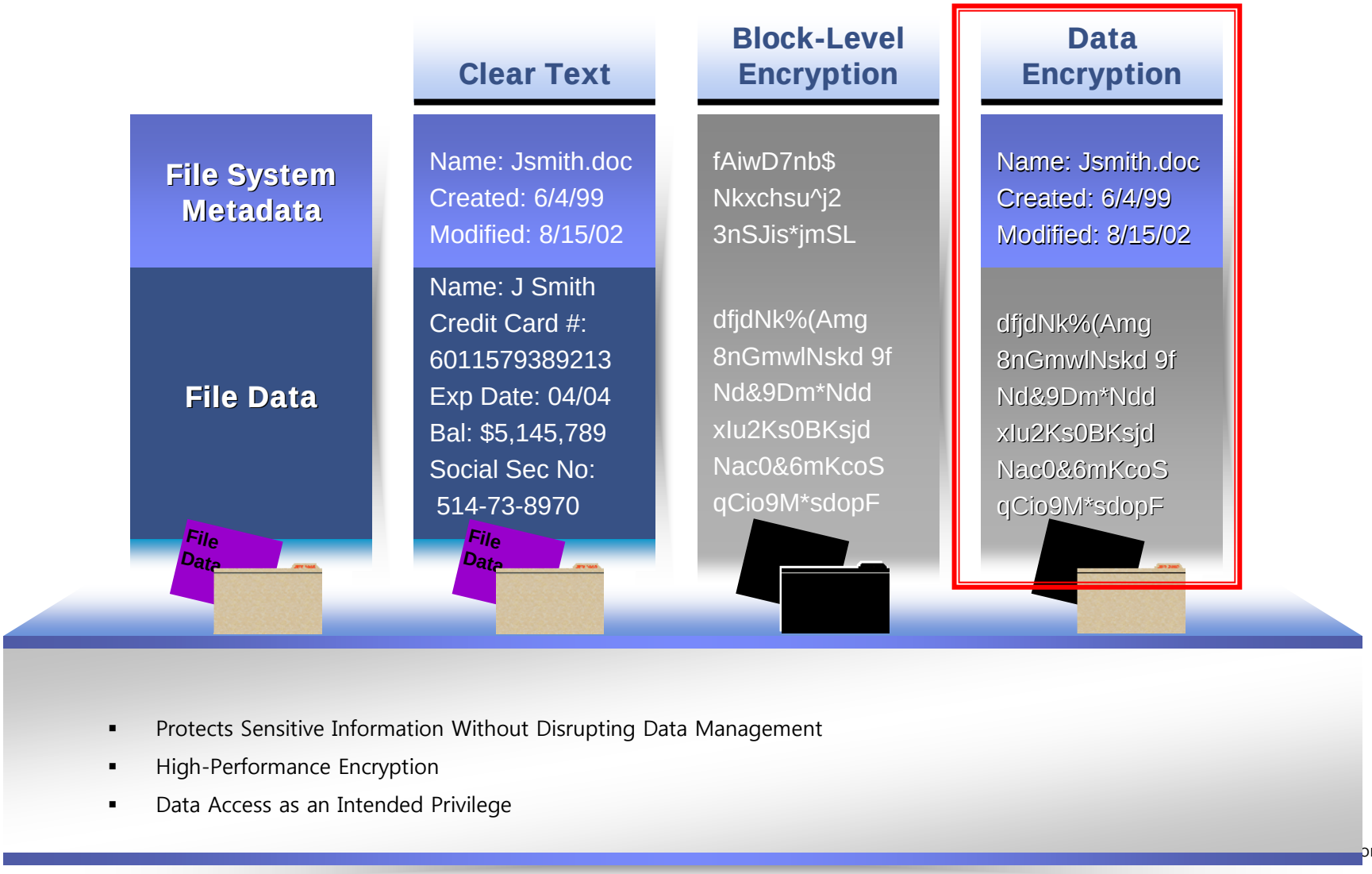
Guardium Data Encryption 특장점 – 이중화 지원

GDE 는 기존 운영환경 변화 없이 이중화 서버에 Agent 설치만으로 이중화를 지원합니다.



Guardium Data Encryption 특장점 –데이터암호화 기술

MetaClear 기술을 적용하여 사이즈 변경 없이 Block 암호화를 지원하며 , 데이터 관리 포인트에 영향을 주지 않고 기밀 정보만을 안전하게 암호화를 수행합니다.



- Protects Sensitive Information Without Disrupting Data Management
- High-Performance Encryption
- Data Access as an Intended Privilege

DB 암호화 기술

DB 암호화 기술

항 목	파일	애플리케이션	컬럼	TDE	토큰화	스위치
대상범위	정형 데이터, 비정형 데이터	정형 데이터	정형 데이터 컬럼	정형 데이터	정형 데이터 컬럼	정형 데이터, 비정형 데이터
직무분리	●	◕	◕	◕	◑	◔
투명성	●	◑	◔	◕	◑	●
애플리케이션 수정 불필요	●	◔	◔	◑	◑	◑
성능 영향도	●	◑	◔	◑	◑	◑
다양한 데이터타입	●	◔	◔	◑	◔	◑
접근 감사	●	●	●	●	●	◔
접근 제어	●	●	●	●	●	◔
인프라 변경	●	●	●	●	●	◔

● = Best ◕ = Better ◑ = Good ◔ = Fair

DB 암호화 기술

항목	파일 방식	컬럼 방식	TDE 방식
암호화 방식	•테이블스페이스, 테이블 단위로 OS 커널에서 암호화	•컬럼 단위로 DBMS(혹은 별도 서버)에서 암호화	•테이블스페이스 단위로 DB 커널에서 암호화
암호화 Key 관리	•자체 HSM 키 관리 및 보호 •중앙 집중적인 관리	•HSM 모듈 별도 필요 •중앙 관리 불가	•DBMS 내 Master Key 암호화 보관 •HSM 추가 연계 필요 •체계적인 키 관리 어려움
DBMS 변경	•DBMS 변경 없음	•DBMS내 스키마 변화 •뷰, 트리거, 인덱스 등 생성	•DBMS 커널 사용 암호화로 DBMS 시스템 부하 증가
에플리케이션 수정	•에플리케이션 수정 없음	•에플리케이션 코드 수정 필요(별도의 API 제공)	•에플리케이션 수정 없음
암.복호화 성능	•블록단위 암호화로 SQL 영향 최소화 •약 5% 이내 부하(벤치마크)	•특정 SQL(조건 검색, 범위 검색 등) 성능 저하 •평균 약 20~30% 부하	•SQL 영향 최소화 •4~8% 부하(whitepaper)
지원 환경	•Oracle, MS-SQL, DB2, IDS, Sybase 등 다양한 DB 지원, 이기종 지원 •Server OS 및 CPU 영향 받음	•Oracle, MS-SQL, DB2 등 지원 •DBMS의 종류 및 Version 영향 받음.	•DBMS 특정 버전 지원 •버전 업그레이드 필요(11g~)
암호화 시 Data Size 변동 여부	•Data Size 변화 없음	•약 10~20% 정도의 Data Size 증가	•Data Size 변화 없음
암호화 Data에 대한 보안성	•블록 단위 IV 적용 •데이터 유주 및 주적 불가능	•IV 적용 암호화 제공 •데이터 유주 및 주적 불가능	• IV 적용 암호화 제공 •데이터 유주 및 주적 불가능
구축 기간	•용이한 구현으로 단납기 지원	•상대적으로 긴 구축 기간	•용이한 구현으로 단납기 지원

Guardium Data Encryption 요약

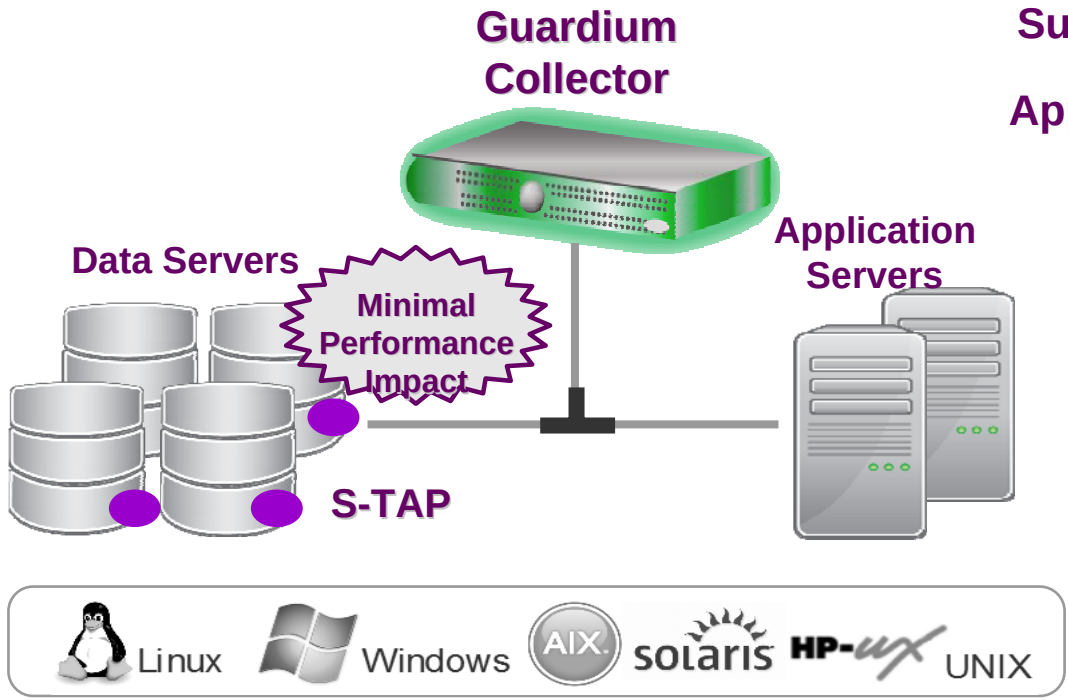
GDE 는 Data암호화 및 상황 기반의 접근제어를 통해 중요 DB Data의 유출을 차단하고 System의 무결성을 보호하는 통합 데이터 보안 솔루션입니다.

투명한 연동	• OS, DB, Storage 등의 인프라가 변경되지 않음 • 애플리케이션 수정이 필요하지 않음 • DB구조나 스키마에 영향을 주지 않음
높은 호환성	• File 단위 암호화를 지원하며, 다양한 DBMS의 종류와 버전을 지원함
암호화 기술	• 데이터 관리에 영향을 미치지 않는 기밀 데이터 암호화 • 고성능 암호화 지원을 위한 탁월한 아키텍처
KEY 암호화 알고리즘	• 3DES, AES128/256, ARIA128/256 등 강력한 암호화 알고리즘 제공
중앙화 된 관리	• 단일 UI 로 다수의 서버 중앙 통제 관리 • 주요 데이터에 대한 암호화 키 관리의 중앙화 • HA 지원
고성능 보장	• 초기 마이그레이션 시 파일 copy와 같은 수준의 암호화 성능 제공 • 조건범위검색을 지원하며 암호화 전후 성능 저하 최소화

Agenda

1. 개인정보보호법 규준에 따른 기술 조치
2. DB 암호화 – IBM Guardium Data Encryption
3. **DB 감사/모니터링 – IBM Guardium Data Monitoring**
4. WHY IBM Guardium? (법제 규준/제안 솔루션 특장점/구축)
5. 구축사례 및 Q&A

Guardium Data Activity Monitoring:실시간 DB 보안 및 모니터링

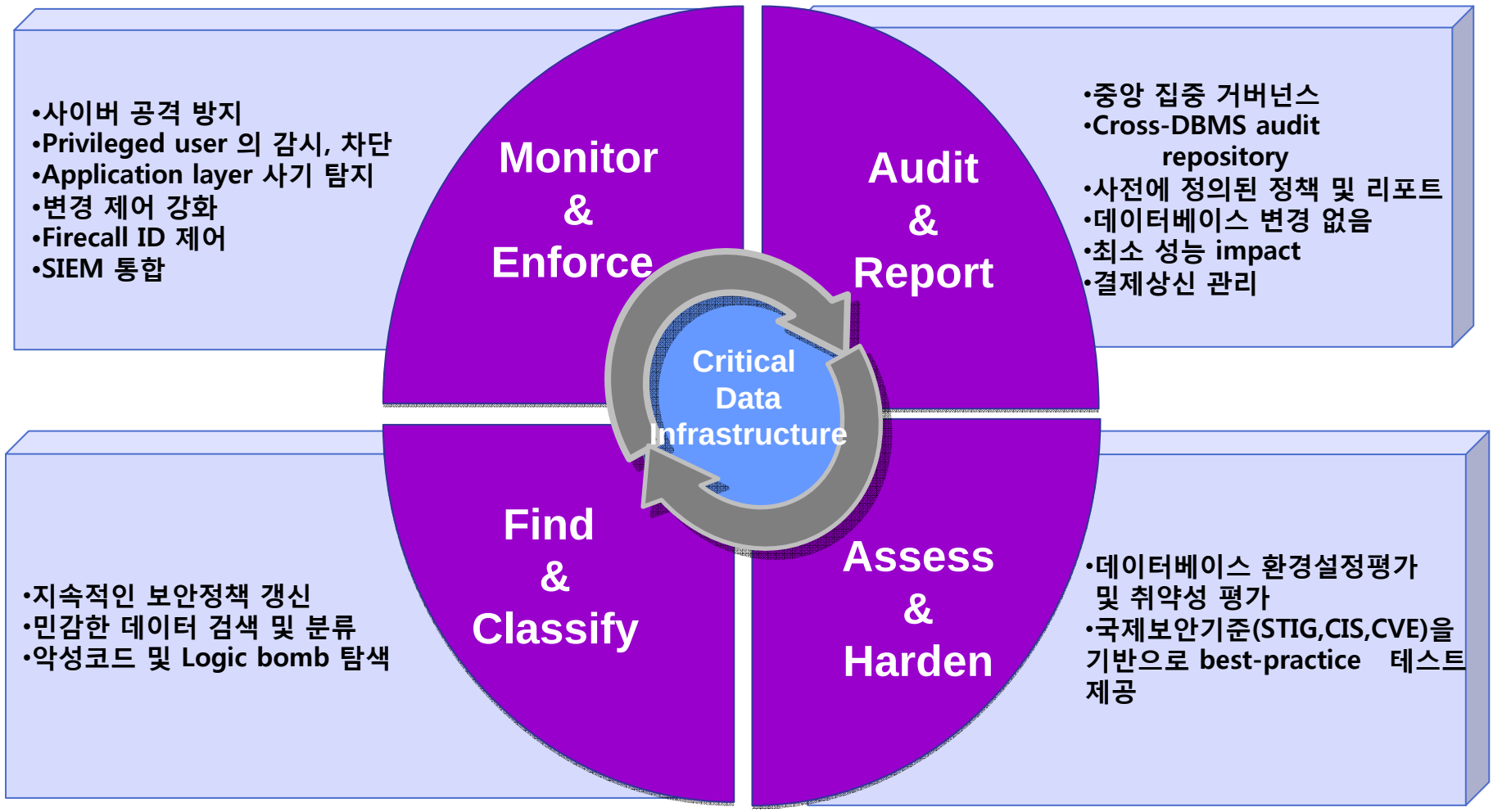


Support for Popular Databases and Application Systems

- 지속적으로 모든 데이터 베이스 활동들을 모니터(Super-user 의 local 접근포함)
- 이기종 환경 , Cross-DBMS 솔루션지원
- Native DBMS log 에 의존하지 않음
- 최소 성능 영향 (약 5% 이하)
- DBMS 나 어플리케이션 변경이 필요 없음

- Activity logs 는 DBA 나 침입자에 의해 영향 받지 않음
- 자동화된 컴플라이언스 레포팅,결제상신 (SOX, PCI, NIST, etc.)
- 실시간 정책 & 감사 세분화
  - *Who, what, when, where, how*

데이터 보안 Lifecycle을 위한 전 영역 지원



Guardium Data Activity Monitoring을 통한 데이터 보안 지원

실시간 데이터베이스 활동 모니터링	로컬접근 및 네트웍 접근에 대한 전방위 보안 제공 사전에 무단 또는 의심스러운 활동 식별 권한이 있는 사용자에 의한 승인되지 않는 접근 차단
감사 및 compliance 솔루션	자동화 및 검증활동 단순화 PCI-DSS , SOX, SAS70,ISO 27001/2 ,NIST 800-53 , Data Masking 관련
변경 제어솔루션	데이터베이스 구조,권한 및 환경구성파일의 무단변경 방지
취약성관리	누락된 패치, 잘못 구성된 권한 및 기본 계정과 같은 데이터베이스 취약점 식별 및 관련 리포트 제공
사기방지솔루션	애플리케이션 계층의 승인되지 않는 응용프로그램 사용자 활동을 식별하는 모니터링 (SAP, PeopleSoft , Oracle EBS, Cognos Etc)
데이터베이스 유출방지	민감한 데이터를 찾고, 데이터 센터 침해요인을 제거 (주민번호, 신용카드번호 등)

솔루션비교 – 모니터링 및 DB보호 솔루션

항목	경쟁사	Guardium
1. 성능 이슈	성능 저하 이슈 없음	OS 커널 방식에 따른 성능저하 최소
2. 사용자 PC 단 에이전트 설치	에이전트 설치함	에이전트 설치 필요 없음
3. Local Access Control	에이전트가 설치된 사용자 단말에 한해서 가능함	모든 접근 경로에 대한 모니터링 가능
4. 마스킹	에이전트가 설치된 사용자 단말에 한해서 가능함	가능
5. 사용자 ID + Appl. ID 접근 제어 및 로깅	불가능	가능
6. 해당 DBMS 변경감사	불가능	가능
7. 취약성 분석 기능	불가능	가능
8. 계정 스위칭 사용자 추적 기능	에이전트가 설치된 사용자 단말에 한해서 가능함	가능

Agenda

1. 개인정보보호법 규준에 따른 기술 조치
2. DB 암호화 – IBM Guardium Data Encryption
3. DB 감사/모니터링 – IBM Guardium Data Monitoring
4. **WHY IBM Guardium? (법제 규준/제안 솔루션 특장점/구축)**
5. 구축사례 및 Q&A

제안 솔루션의 우수성

- IBM InfoSphere Guardium은 운영 환경에 영향 및 부하를 주지 않고, 대내외 등 우회 경로 없는 모니터링 및 접근 통제를 지원하며, 암호화 적용 후, 기존 운영환경과의 성능 저하를 최소화 하며, 다양한 이기종의 DBMS 시스템 및 O/S 연동이 가능하고 다양한 암호화 알고리즘을 지원합니다.

모니터링 및 접근 통제

우수한 성능
- **다양한 이기종 DBMS와 연동되는 특허 받은 기술**
- **Software Tap 방식으로 CPU 부하 최소화**

전방위 접속로 제어
- **로컬 접속 및 네트워크 접근에 대한 전 방위 보안 제공**
- 비 인가자 또는 비인가 트랜잭션에 의한 접속차단 및 이력제공

유출 방지
- **권한이 있는 사용자에 의한 승인되는 않는 쿼리에 대한 결과값을 마스킹**

암호화

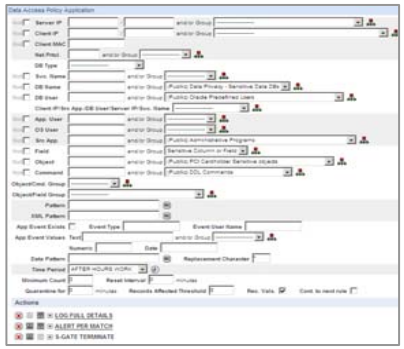
우수한 성능과 보안성
- **기존 운영환경 성능 저하를 최소화**
- **안전한 키 관리 시스템과 시스템 커널 모듈**

투명한 연동
- **운영 환경의 변화 없이 암호화 지원**
- **어플리케이션의 변경 없이 적용**

높은 호환성
- File 단위의 암호화 지원
- **다양한 DBMS 종류와 버전 지원**

IBM Guardium DB 보안 솔루션 구성 (암호화 접근제어 전체구성 방안)

- IBM Data Security – DB 암호화 및 접근제어 전체 구성 방안

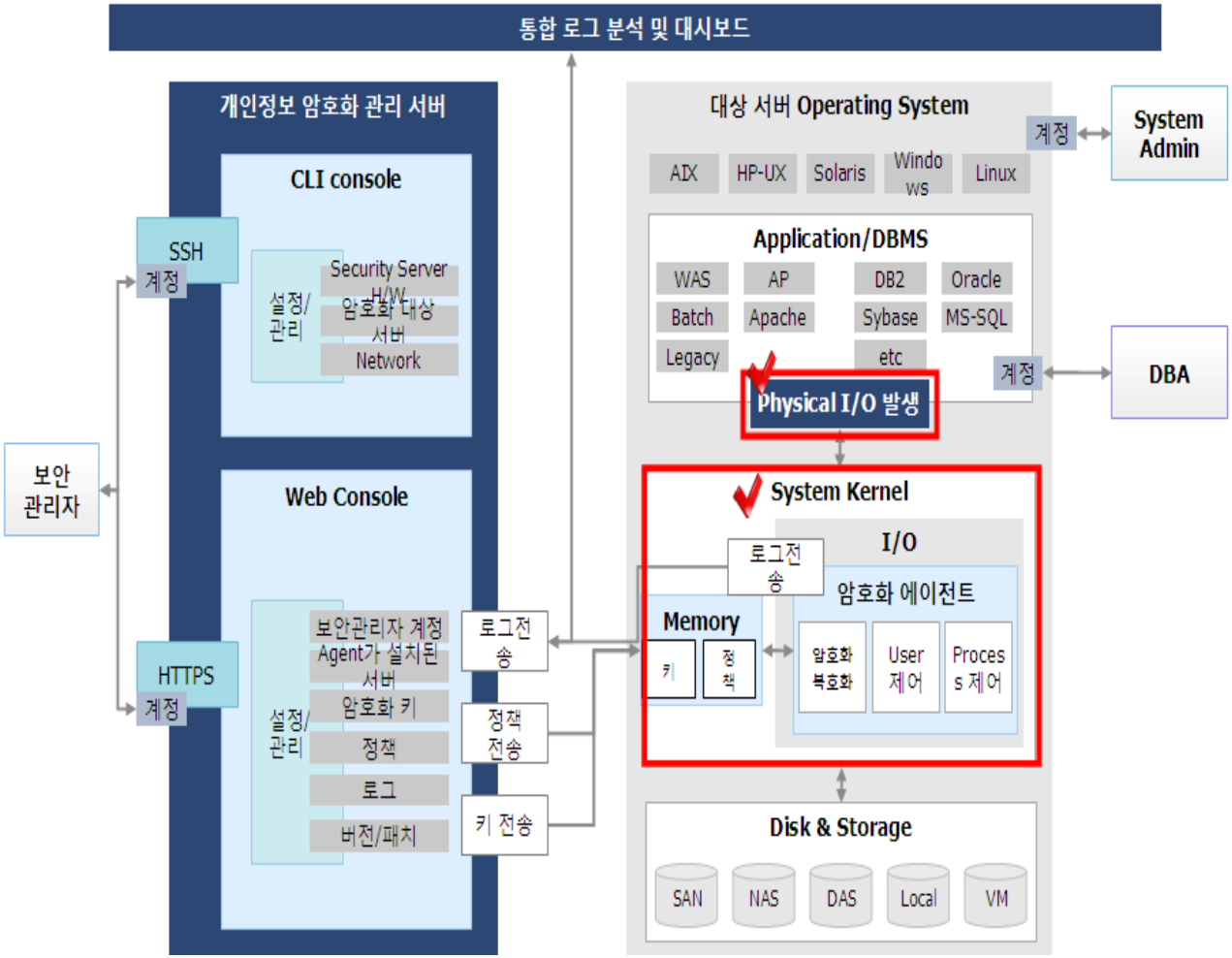


전 방위적인 접근제어에 대한 접근 감사 시스템

OS 단위에서의 모든 접근 제어 및 모니터링

- TCP, Shared Memory, Named Pipes, Bequeath
- Encryption Traffic: SSH/IPSEC, Oracle ASO, SQL Server SSL

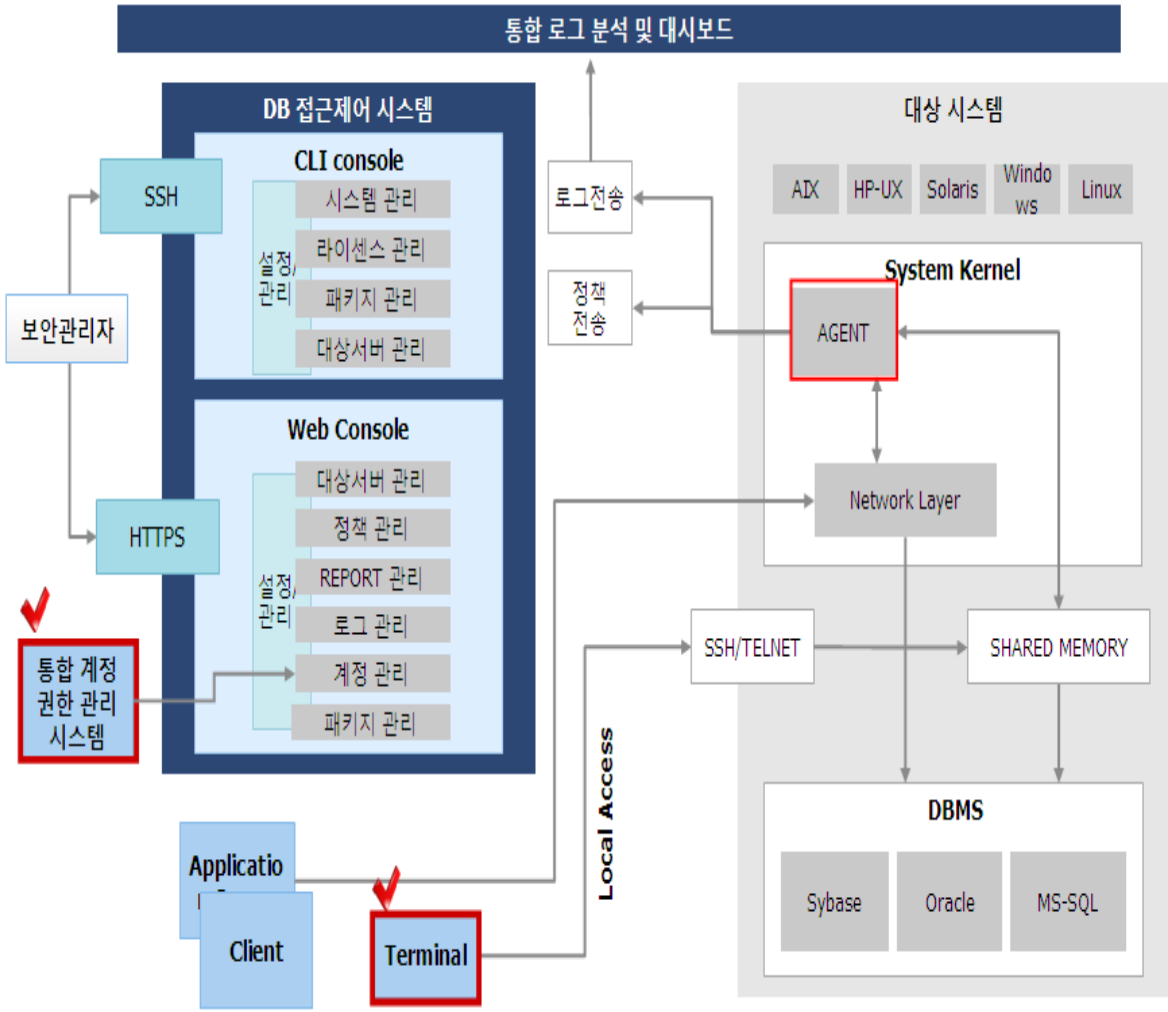
Guardium Data Encryption 구성



솔루션 특장점

- 다양한 암호화 알고리즘을 지원
- 기존 운영환경비교 최소한의 성능저하
- 안전한 키 관리 시스템과 시스템 커널 모듈
- 운영 환경의 변화 없이 암호화 지원
- 어플리케이션의 변경 없이 적용

IBM Guardium Data Activity Monitoring 구성



솔루션 특장점

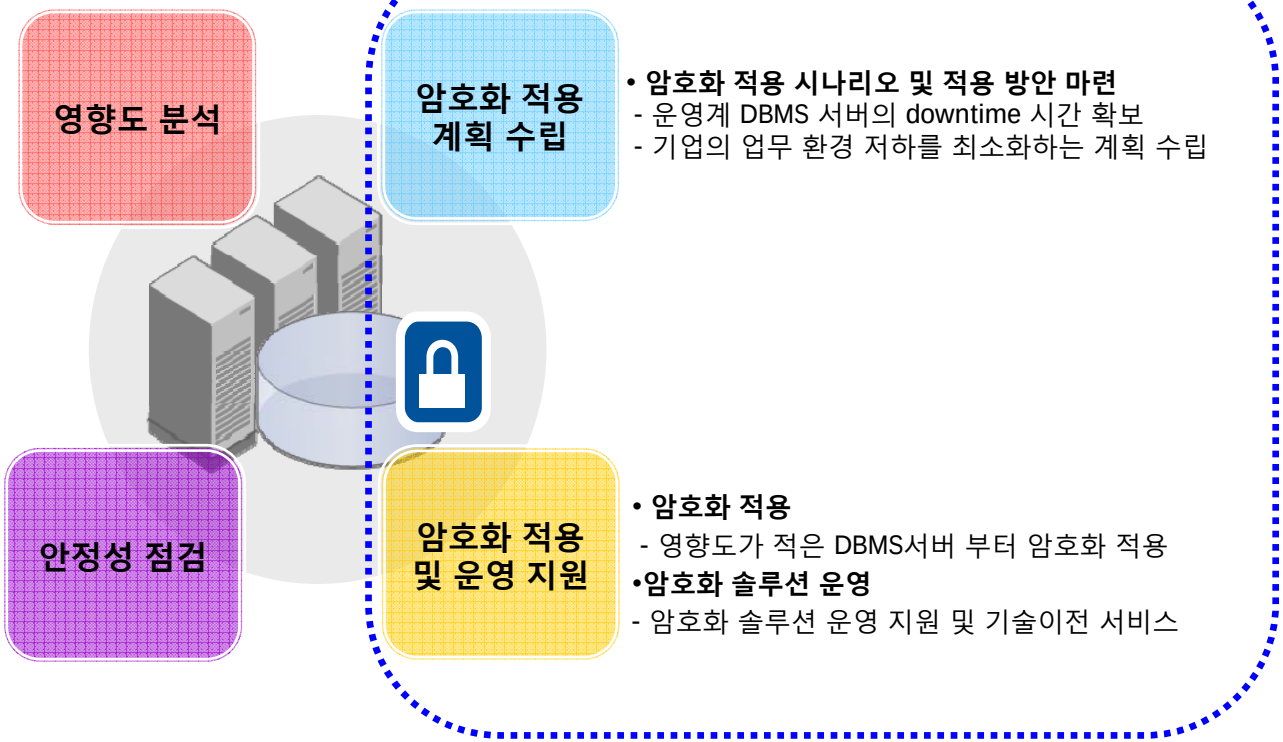
- 유일의 DBMS와 연동되는 특허 받은 기술
- Software Tap 방식으로 CPU 부하 최소화
- 로컬 접속 및 네트워크 접근에 대한 전 방위 보안 제공
- 비 인가자 또는 비인가 트랜잭션에 의한 접속차단 및 이력 제공
- 권한이 있는 사용자에 의한 승인되는 않는 쿼리문 마스킹

IBM Data Security – Why IBM

- IBM의 Data Security 서비스를 통해서 고객 정보 DB 암호화에 필요한 복잡하고 장기간의 일정을 필요로 하는 하지 않는 'Data Security 솔루션 및 구축 서비스'를 통해서 고객정보DB에 대한 암호화 솔루션 적용 및 운영을 통해서 가장 안전하고 빠른 고객정보 암호화 방안을 제시 합니다.

• 암호화 대상 테이블과 컬럼에 대한 분석
-법률적 근거에 따른 암호화 대상 선정
- 해당 컬럼을 사용하는 모든 SQL에 대한 분석 및 영향도 분석

• 파급효과 및 안정성 분석
- 고객정보 암호화에 따른 비즈니스 파급 효과 분석
- 테스트 환경 구축 및 암호화에 따른 기능 및 성능 이슈 점검



• 암호화 적용 시나리오 및 적용 방안 마련
- 운영계 DBMS 서버의 downtime 시간 확보
- 기업의 업무 환경 저하를 최소화하는 계획 수립

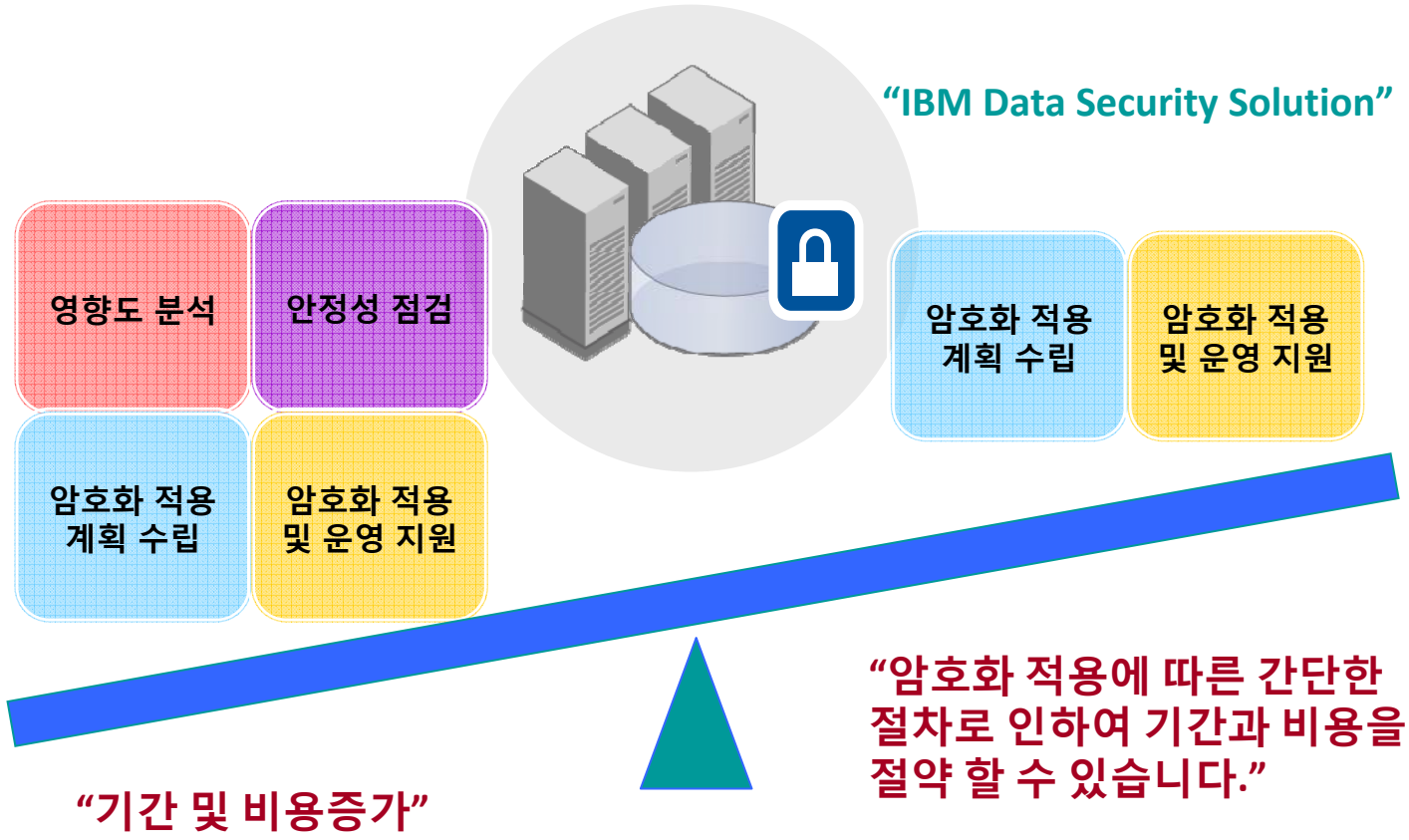
• 암호화 적용
- 영향도가 적은 DBMS서버 부터 암호화 적용

•암호화 솔루션 운영
- 암호화 솔루션 운영 지원 및 기술이전 서비스

"IBM Data Security 솔루션 및 구축 Service"

IBM Data Security – Why IBM

- IBM의 Data Security 서비스를 통해서 고객 정보 DB 암호화에 필요한 복잡하고 장기간의 일정을 필요로 하는 하지 않는 'Data Security 솔루션 및 구축 서비스'를 통해서 고객정보DB에 대한 암호화 솔루션 적용 및 운영을 통해서 가장 안전하고 빠른 고객정보 암호화 방안을 제시 합니다.



왜 "IBM Guardium"인가? – 파일방식 암호화/ 에이전트 방식 모니터링

DB 보안은 Governance (Trust & Protect)영역!!

법제고도화

2004년 발의된 묶은 법
'개인정보의 범위'에 대한 확장
변화되는 법규에 기민한 대응

운영효율

데이터 보안의 목적은 운영효율
비용과 효율성의 문제로 접근

데이터 거버넌스

보안의 관점에서 확대
빅데이터 시대의 거버넌스
다양한 데이터, 인프라 지원 필수

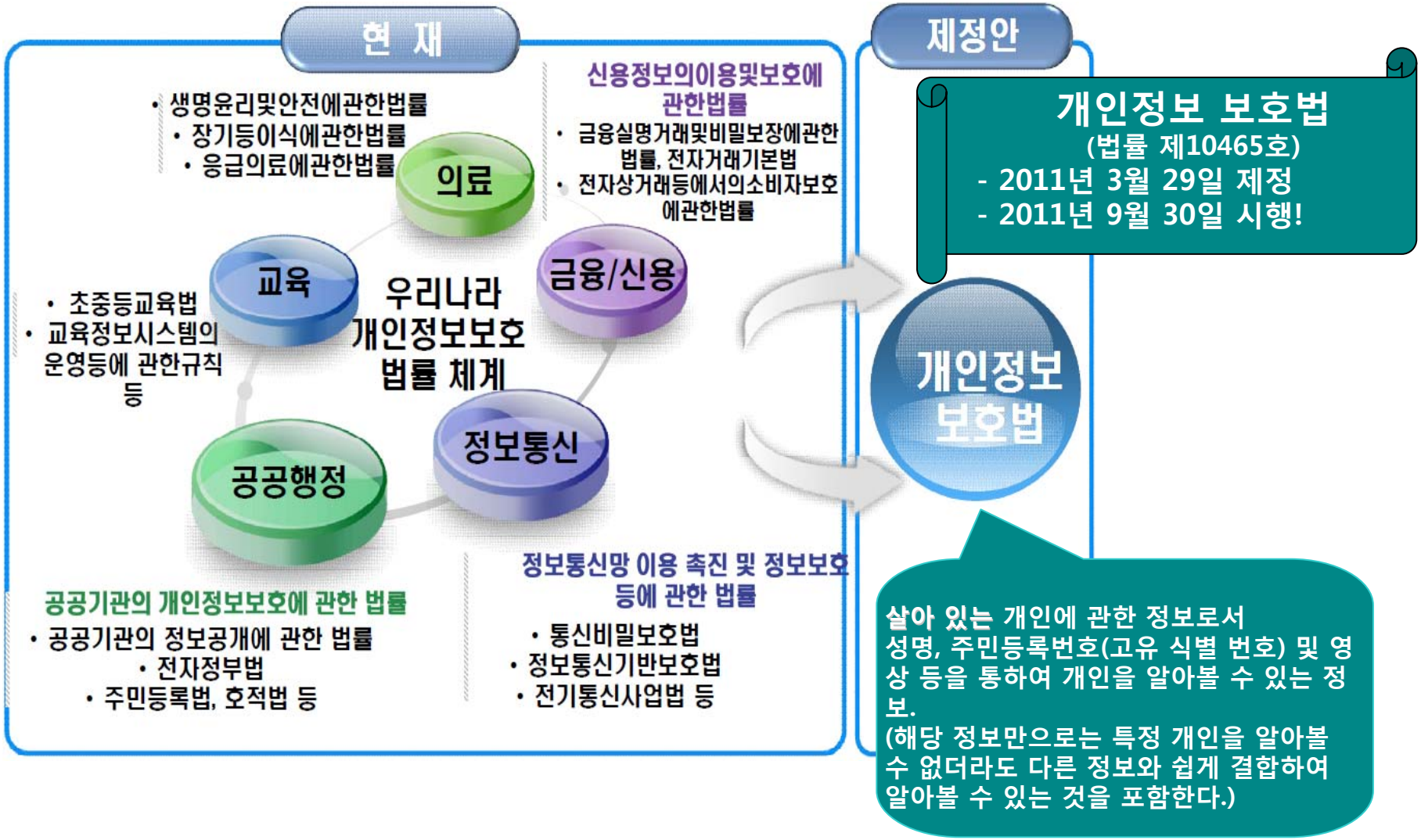
~

법제의 고도화에 따라 구속요건이 강화되거나, 추가적 범위의 확대에 따라 ***보다 확장적인 기술규준을 요구하는 것***이 국제적 추이

비즈니스 기민성과 회복능력 향상이라는 큰 개념의 이득에서 부터, 반복된 업무의 감소와 다운타임감소/ 어플리케이션 성능의 향상 등으로 인한 ***운영효율*** 까지 고려

데이터는 ***공유와 보호*** 라는 상충하는 양면성을 특징으로 하고, 빅데이터 환경에서 그 데이터의 양과 형태는 증가하지만, ***신뢰성 하락과 유출위험*** 이 양립

컴플라이언스 대응: 개인정보보호법 제정



Clients' Value

- IBM 의 Data Base Security 데이터 암호화 및 접근제어 솔루션을 통해서 가장 안전하고 생산성 저하를 최소화 할 수 있는 암호화 방안 제공하고 궁극적으로 기업이 고객정보 유출 및 통제에 대한 대응할 수 있습니다

Business Alignment

Data Base 암호화에 따른 기간 및 비용 최소화

- 암호화에 따른 사전 영향분석 및 SQL 분석 업무 필요 없음
- 암호화 기간 소요 최소화 및 애플리케이션 변경/개발 불필요에 따른 비용절감
- 기업의 업무 환경에 및 비즈니스 영향 최소화에 따른 생산성 최소화

Service Excellence

Data Base 의 암호화 및 접근제어 통합 솔루션 제공

- Data Base 암호화 및 접근제어 대한 통합된 (Integrated) 솔루션으로 제공
- 현 고객 Data Base에 대한 암호화 적용 서비스 제공
- Data Base 암호화 솔루션의 운영지원 서비스 제공

Managing Risk

기업의 고객정보 유출 통제 및 차단 및 보안 위협 대응

- 법적 규제에 대한 대응
- 고객정보에 대한 유출 통제 및 차단 방안 마련
- 고객정보 유출에 따른 피해 최소화

Agenda

1. 개인정보보호법 규준에 따른 기술 조치
2. DB 암호화 – IBM Guardium Data Encryption
3. DB 감사/모니터링 – IBM Guardium Data Monitoring
4. WHY IBM Guardium? (법제 규준/제안 솔루션 특장점/구축)
5. 사례

국내 주요 구축 사례 – DB 암호화/모니터링/ 접근제어

다양한 산업 군에 걸친 고객분들이 IBM InfoSphere Gardium을 선택해 주셨습니다.

※ 고객의 요청에 따라 상세 고객정보는 공유하지 않습니다. 양해 부탁 드립니다.