2013 개인정보 보호를 위한
데이터베이스 보안 세미나

IBM

전사 데이터 보호를 위한 IBM InfoSphere Guardium

한국IBM 정보관리사업부
민 선미 부장(smmin@kr.ibm.com)
2013.10.29

Agenda

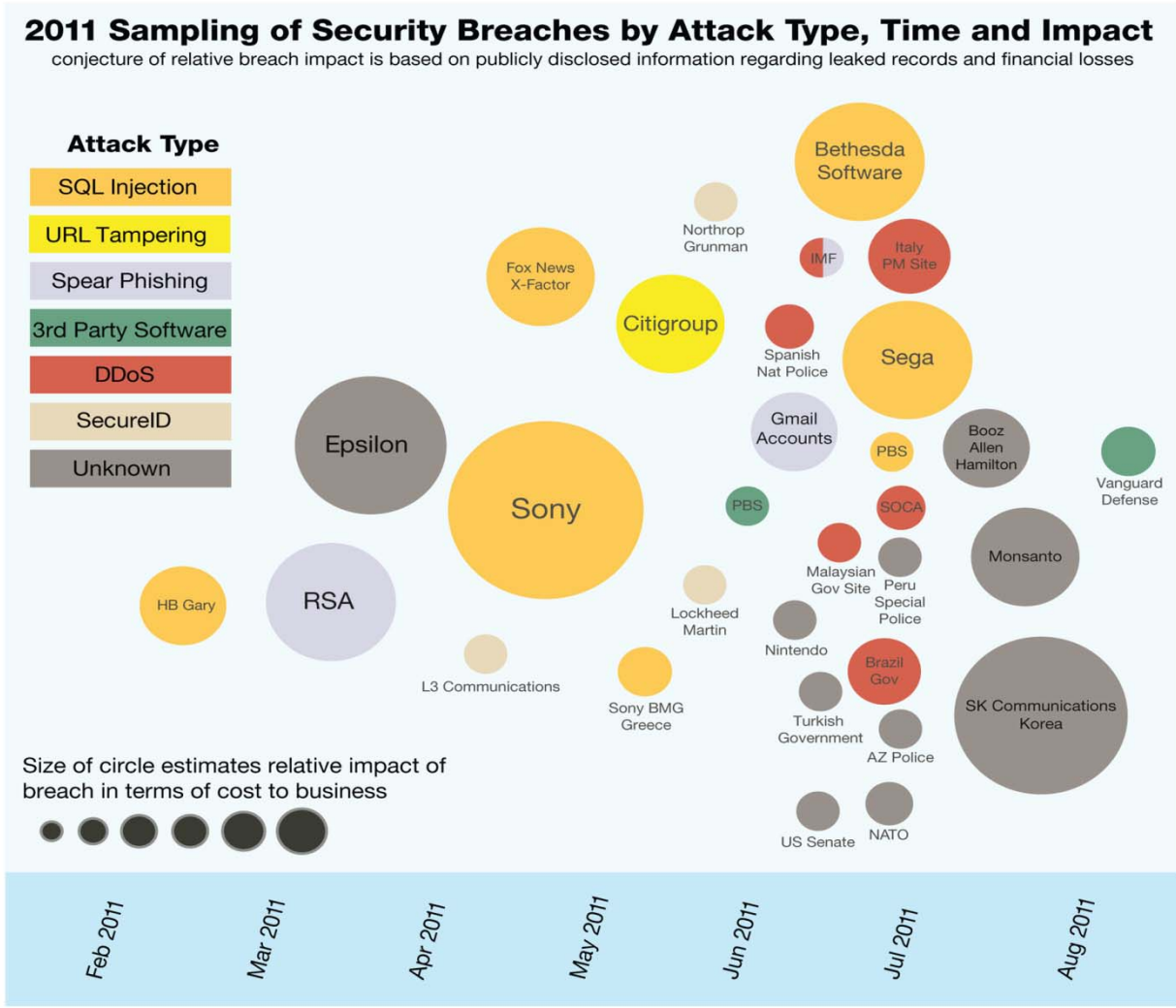
- 데이터를 둘러싼 환경
- 전사 데이터 암호화를 위한 IBM 솔루션
- 전방위 DB 보호를 위한 IBM 솔루션
- 사례 및 결론

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

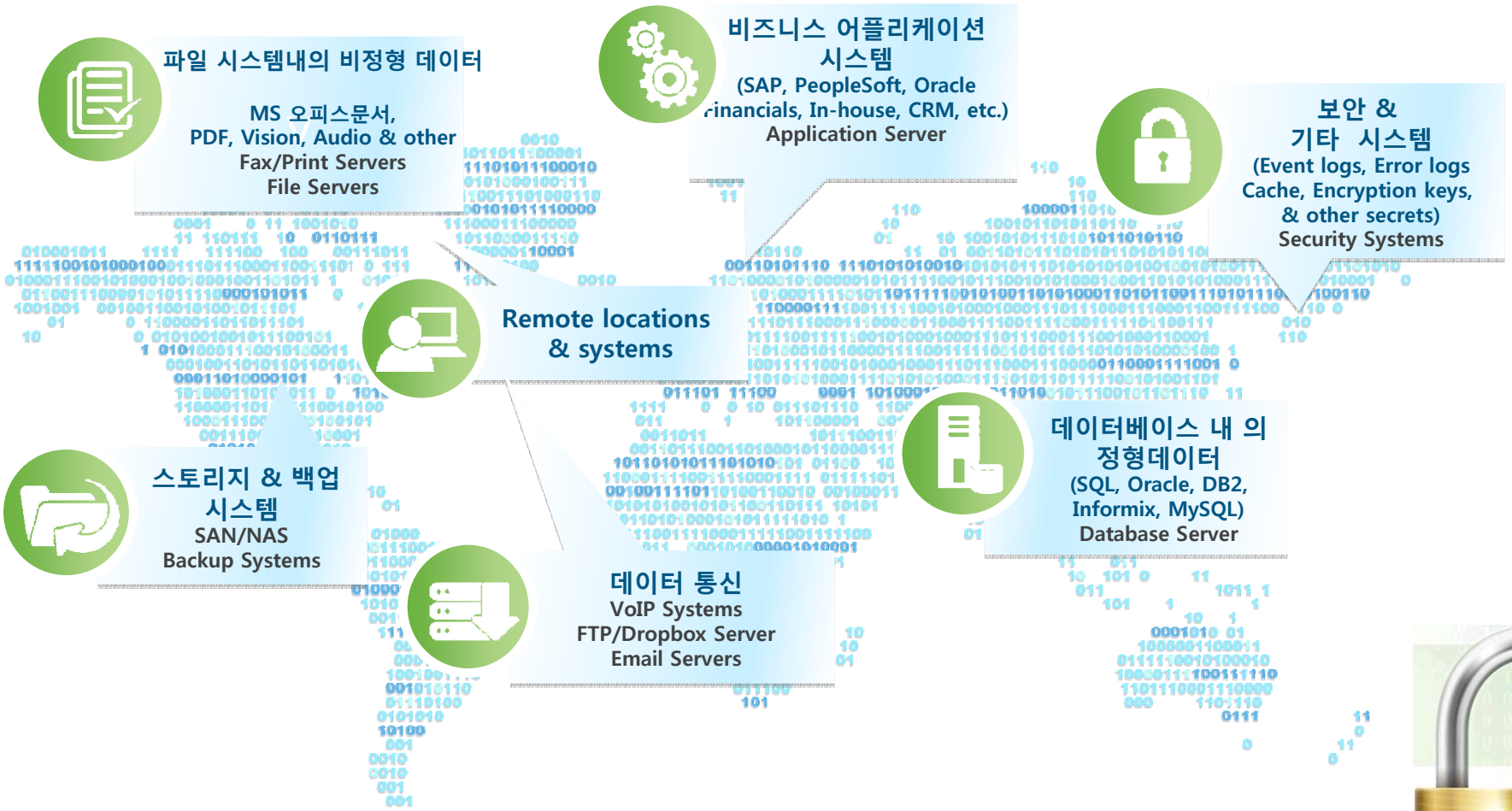


Source: IBM X-Force® Research and Development

기업 전사 내 산재된 데이터

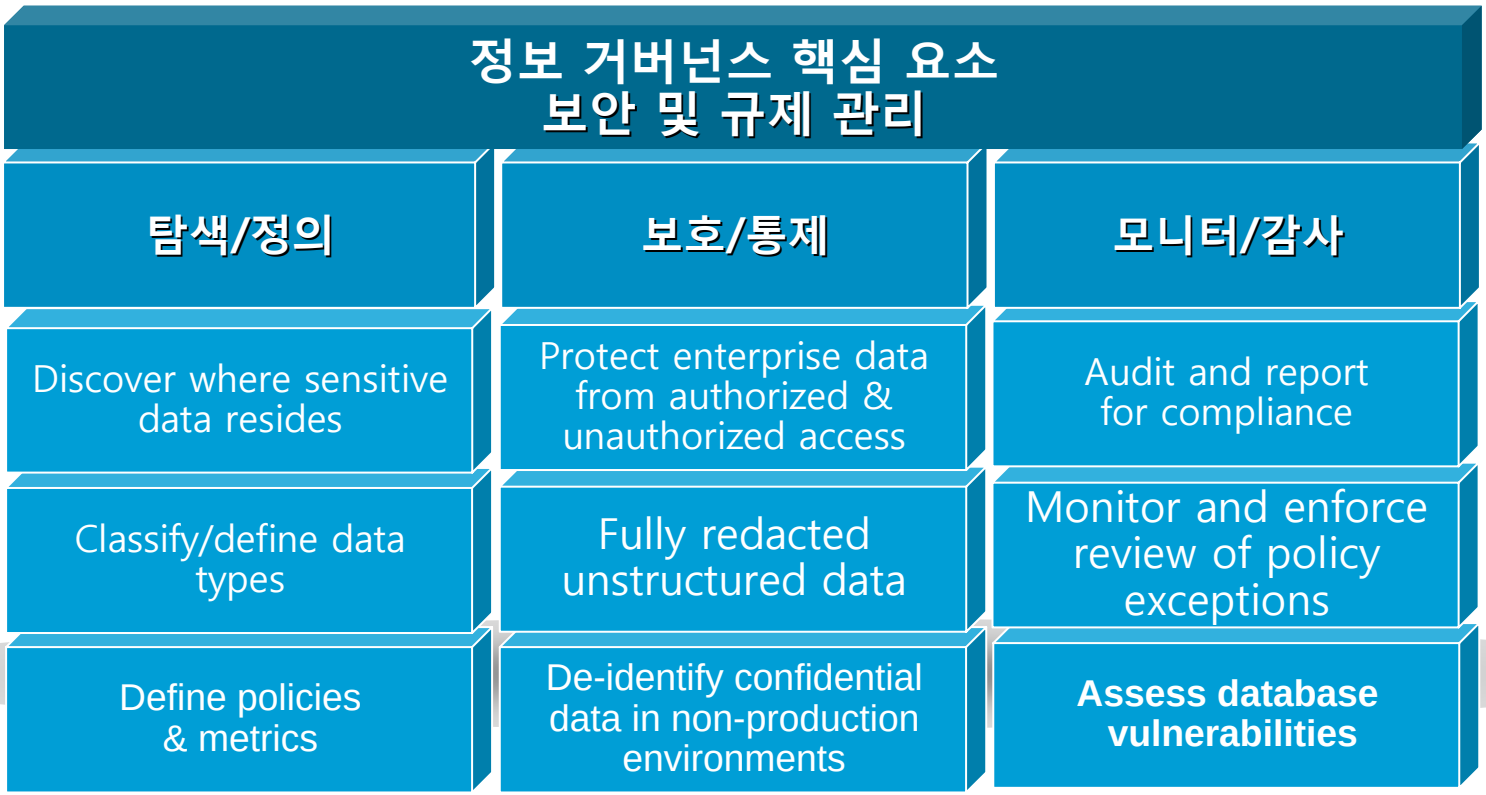
Traditional security controls not scalable

**데이터는 다양한 양식과, 상태로 다양한 위치에 존재합니다.
전통적인 보안 관제 방식은 이러한 다양성을 충족하기 어렵습니다.**



정보 거버넌스를 통한 보안/규제 관리 통찰력의 실행

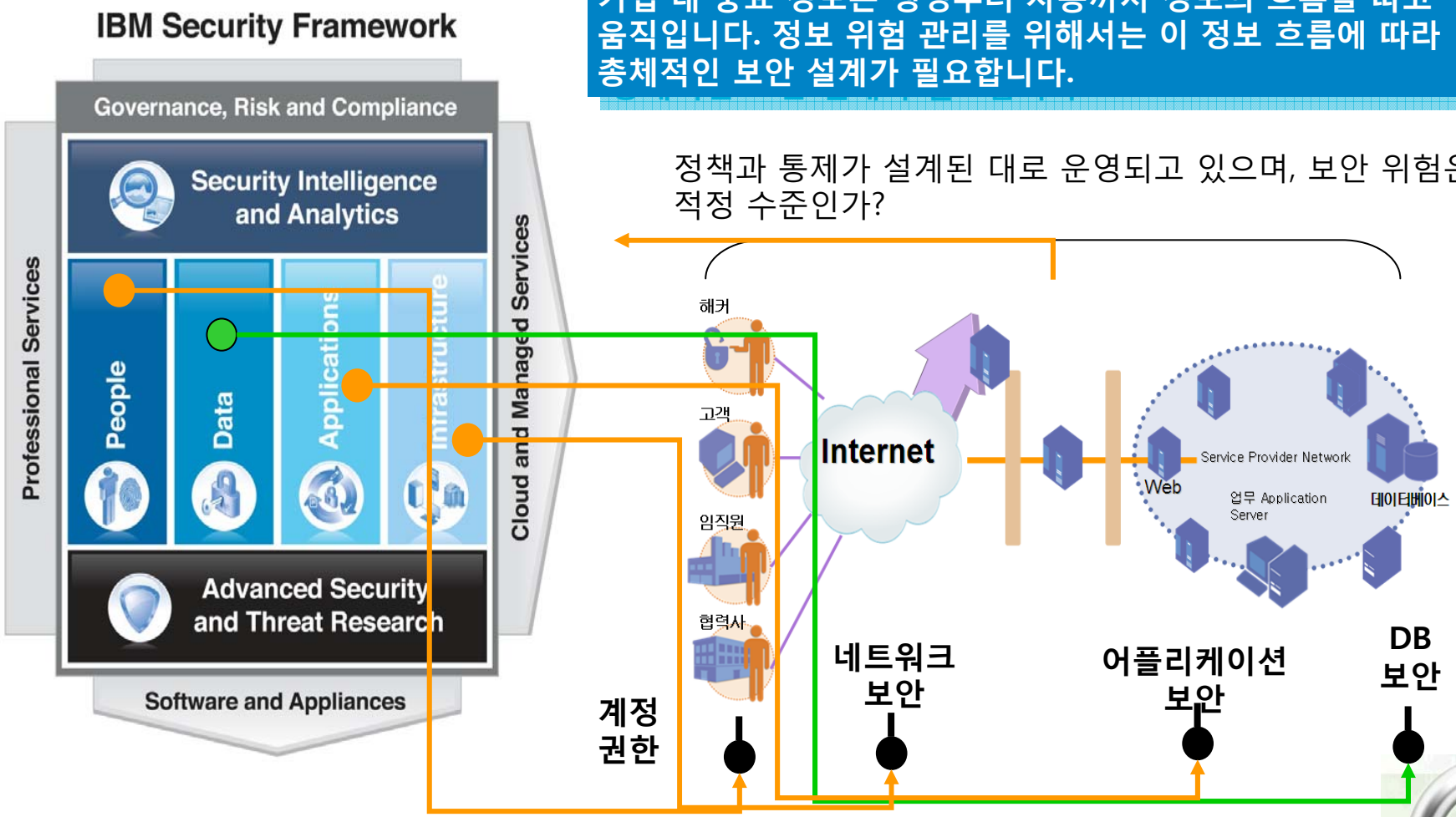
데이터 보안 전략은 ***데이터베이스 감사 및 모니터링, 패치 관리, 데이터 마스킹, 접근 제어, 탐색/분류, 그리고 변경 관리를*** 포함해야 합니다 .



-- Why Enterprise Database Security Strategy Has Become Critical, Forrester Research, Inc, July 13, 2011

전사 보안을 위한 IBM Security Framework

기업 내 중요 정보는 생성부터 사용까지 정보의 흐름을 따고 움직입니다. 정보 위험 관리를 위해서는 이 정보 흐름에 따라 총체적인 보안 설계가 필요합니다.



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/Info Sphere 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 데이터 암호화

고성능 데이터 암호화

- *애플리케이션 변경 없이 테이블 단위 암호화*
- *DBA와 보안담당자의 직무 분리*
- *통합적이고 중앙 집중적인 정책 및 키 관리*

InfoSphere Guardium Data Encryption

5 비정형 데이터 문서 내 주요 정보 변환

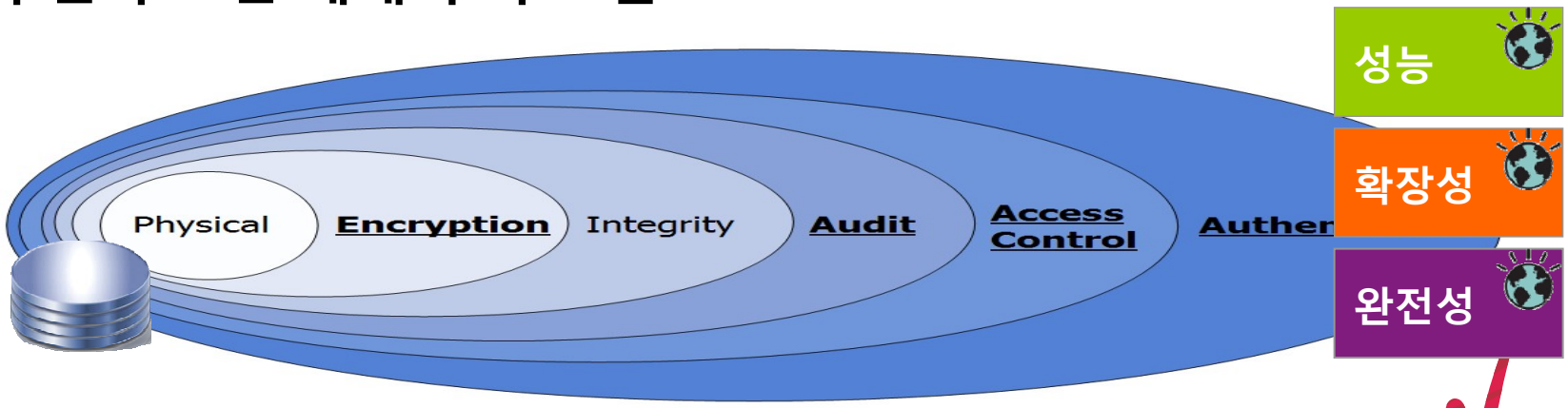
문서/양식 내 민감한 데이터에 대한 보호

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

InfoSphere Guardium Data Redaction

컴플라이언스 및 다양한 법적 규제 준수

기업의 전사 보안 체계 구축 흐름



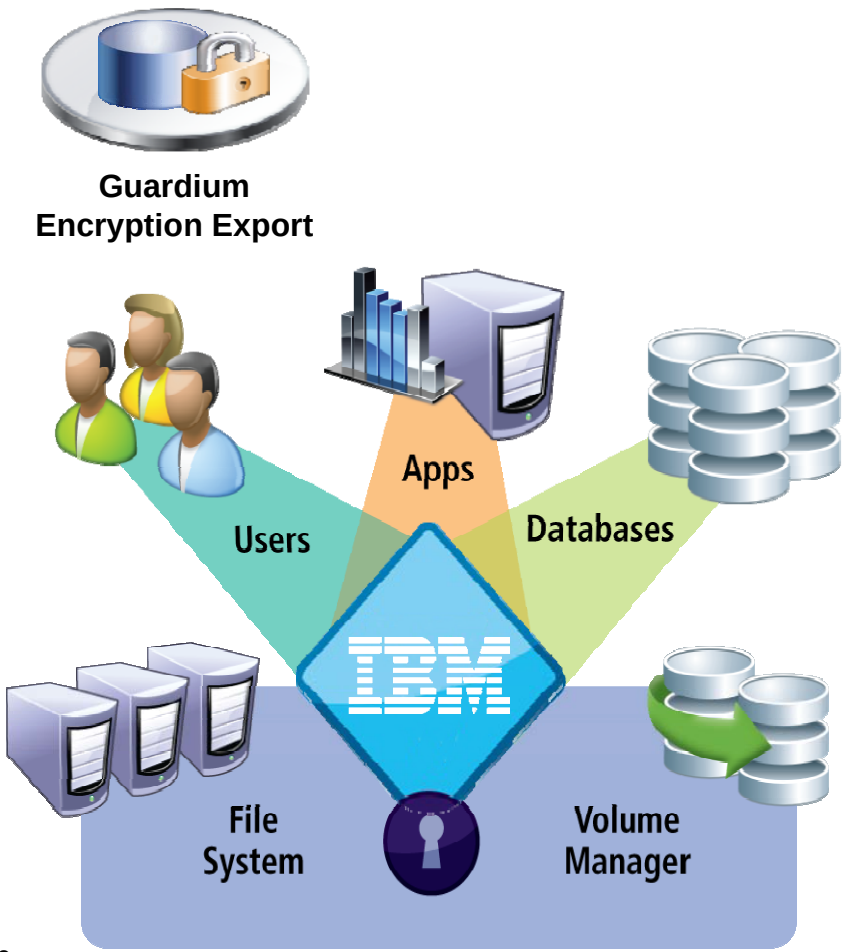
Network-driven	Application-driven	Data-driven
• 외부 침입 차단 및 방어	• 어플리케이션을 보호	• 데이터 보호
• 방화벽(Firewall) • IPS(침입방지시스템) • IDS(침입탐지시스템) • 네트워크 취약점 진단	• 웹 방화벽 • 어플리케이션 취약점 진단	• 데이터베이스 모니터링 • - 로깅 • - 감사 • 데이터 유출방지 (DLP) • 데이터 암호화 • - 암호화 • - 마스킹
• 경계 네트워크 보호	• 서버/어플리케이션 보호	• 단말 데이터베이스 보호

Agenda

- 데이터를 둘러싼 환경
- **전사 데이터 암호화를 위한 IBM 솔루션**
- 전방위 DB 보호를 위한 IBM 솔루션
- 사례 및 결론

IBM InfoSphere Guardium Data Encryption

Guardium Data Encryption은 데이터 암호화 및 암호화 Key 관리를 위한 포괄적인 솔루션으로서 기업에서 사용하는 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
애플리케이션 수정 없음

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

중앙 관리
클라우드 환경에서의 암호화 제공
모든 DBMS를 중앙에서 관리

암호화 KEY 관리
별도의 분리된 안전한 Key 서버
FIPS 140-2 키 관리 인증 기술 기반

암호화 후 성능보장
암호화 후 최소 성능 Impact
인덱스 검색 등 조회 변화 없음

Guardium Data Encryption 특징

정형 및 비정형 데이터 암호화

- **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

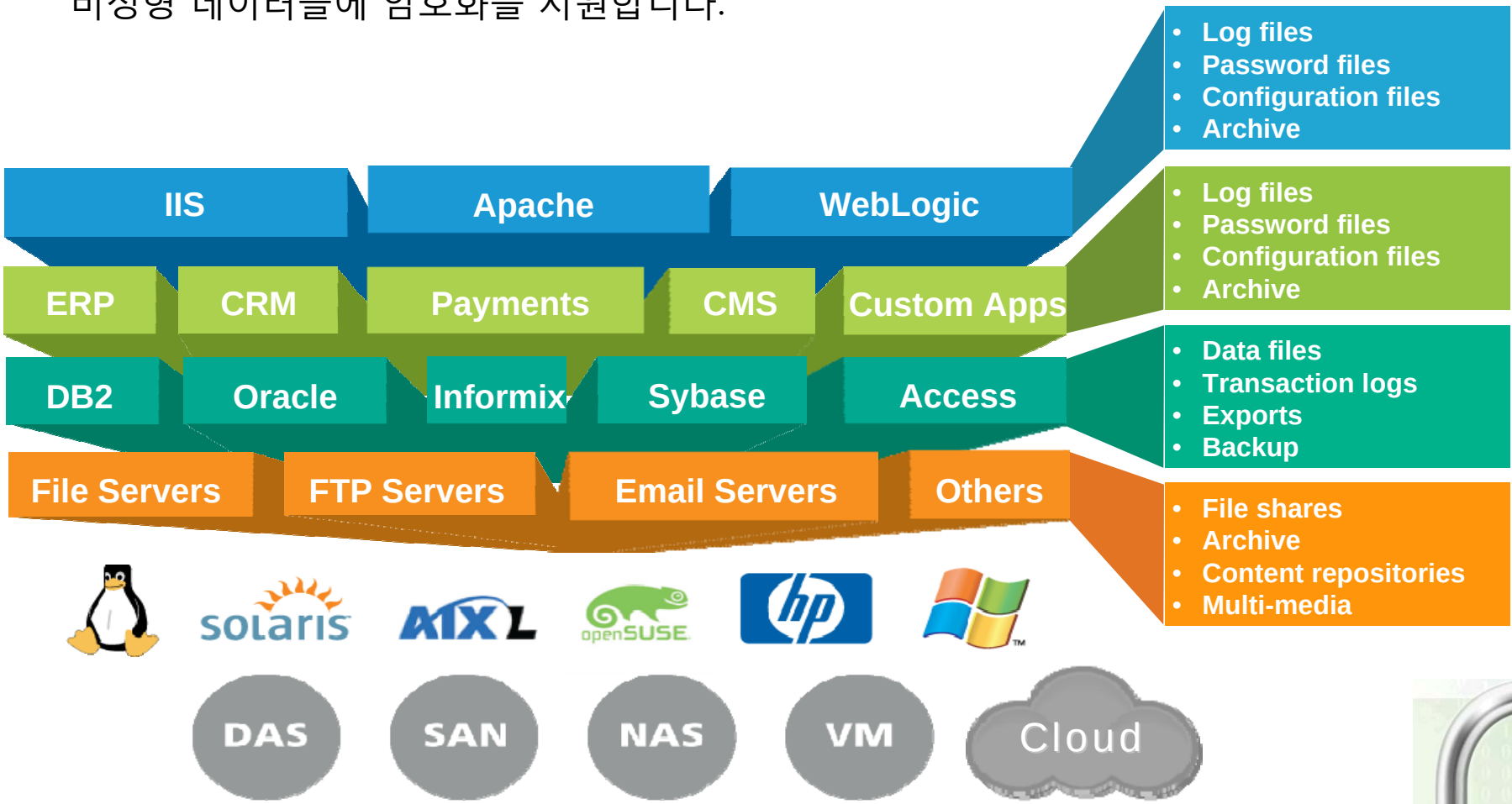
- **Big Data 암호화 지원**
- **기존 IT 인프라스트럭쳐/애플리케이션 코드 수정 없음**
- **온라인 및 오프라인 백업 환경 지원**
- **사용자 조회 일관성 보장**

전사 내 다수 DB에 대한 중앙 통제 관리

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

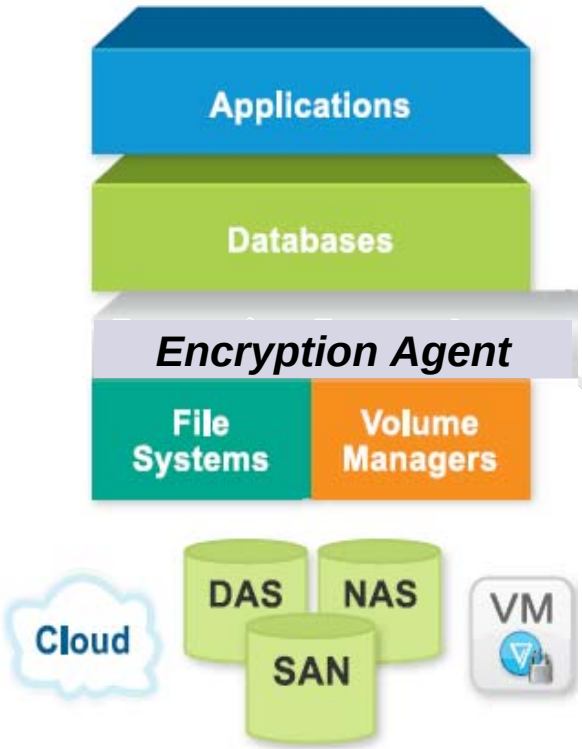
Guardium Data Encryption 적용범위

- Guardium Data Encryption은 다양한 DBMS 뿐만 아니라 미들웨어 , 다양한 어플리케이션 및 file server, ftp server 등의 데이터와 백업파일 및 DB 설정정보까지 저장되는 정형 및 비정형 데이터들에 암호화를 지원합니다.



Guardium Data Encryption 구성 아키텍처

- Guardium Data Encryption은 암호화 대상서버에 설치되는 Agent 와 별도의 Appliance 암호화 서버로 구성되며, File System 및 Volume에 대한 암호화를 지원합니다.



Security Server
- 중앙집중 및 자동화된 Key Management
- High Availability Cluster 지원
- 강력한 권한분리

HTTPS

HTTPS

Web 통합콘솔

Data Encryption Agent
- 투명한 적용
- Linux, Unix, Windows 지원
- 권한사용자 제어
- Software 기반 암호화

Guardium Data Encryption 특장점 –Key 보호 및 직무분리

- Guardium Data Encryption은 암호화 서버에서 자체적으로 Key 관리를 수행하며, 관리자들을 위한 직무분리 기능을 지원합니다.

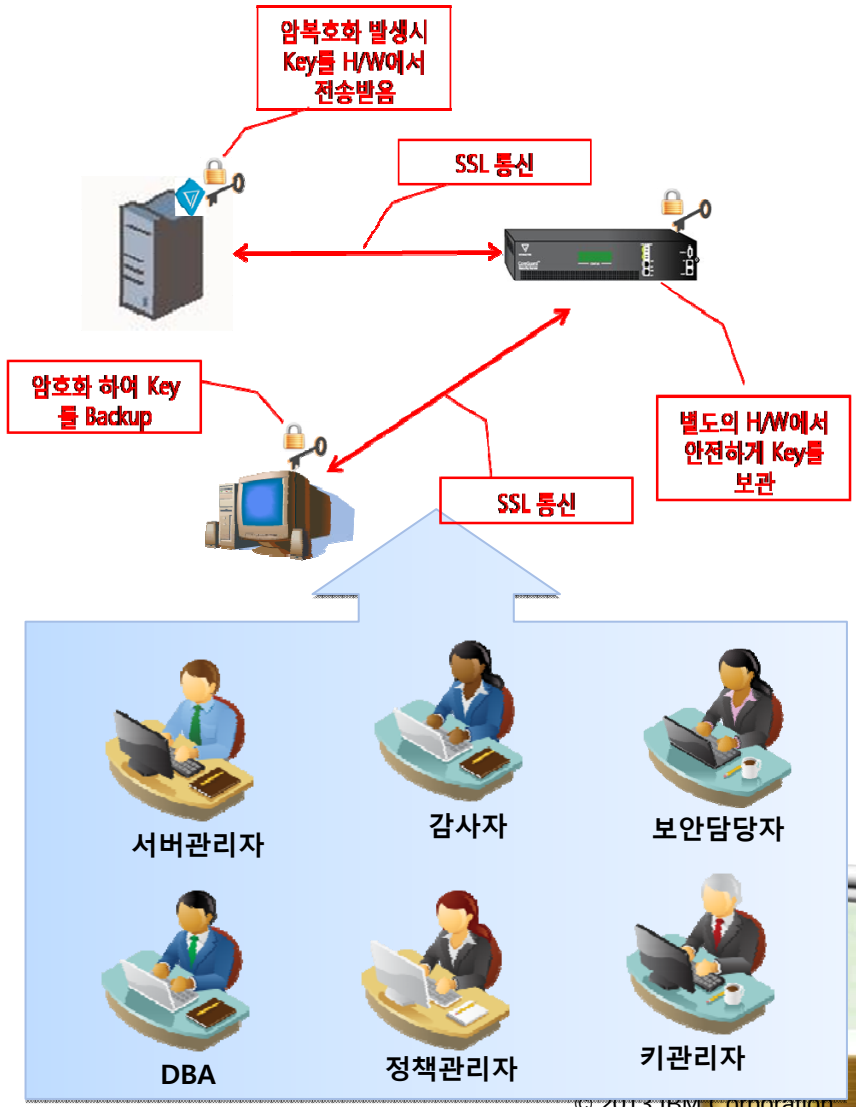
기술규준 충족 – 키관리/ 직무분리

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

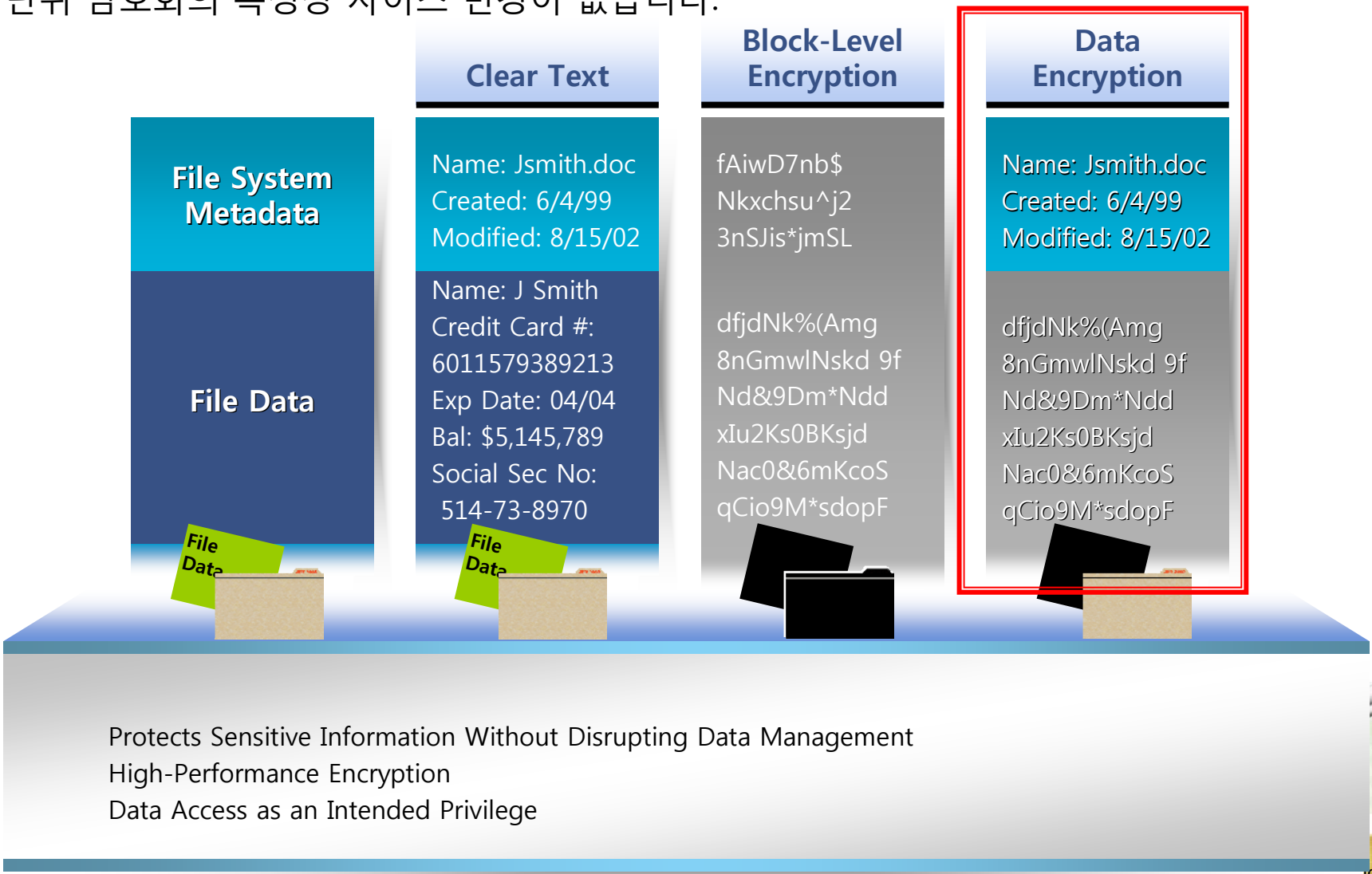
Key를 File로 Backup시 암호화해서 Backup하게 되며, 복호화를 위한 Master key는 Appliance에서만 보관하고, 어떠한 user도 Master key에는 접근이 불가능

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



Guardium Data Encryption 특장점 –데이터암호화 기술

- Guardium Data Encryption은 MetaClear기술을 적용하여 고성능 암호화를 지원하며, 블록 단위 암호화의 특성상 사이즈 변경이 없습니다.



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

Agenda

- 데이터를 둘러싼 환경
- 전사 데이터 암호화를 위한 IBM 솔루션
- **전방위 DB 보호를 위한 IBM 솔루션**
- 사례 및 결론

IBM InfoSphere Guardium Database Activity Monitor

- Guardium Database Activity Monitor는 전사 환경 내 다양한 데이터베이스에 대한 실시간 모니터링 및 로깅 기능을 통해 감사에 대응하고, 비인가자에 대한 접근 제어 및 마스킹 등의 침입 탐지 및 유출 방지를 제공하기 위한 전방위 DB 보호 솔루션입니다.

우수한 성능

- 특허받은 Software Tap 기술을 통한 CPU 부하 최소화

전 방위 접속경로 모니터링 및 제어

- 로컬 데이터베이스 접근 추적을 위한 특허 기술
- 내부 및 네트워크 접근에 대한 전 방위 보안 제공
- 비 인가자 또는 비인가 트랜잭션에 의한 접속차단 및 이력제공

다양한 운영 환경 지원

- 다양한 OS , DBMS, 애플리케이션 모니터링 및 접근제어 지원

데이터 유출 방지

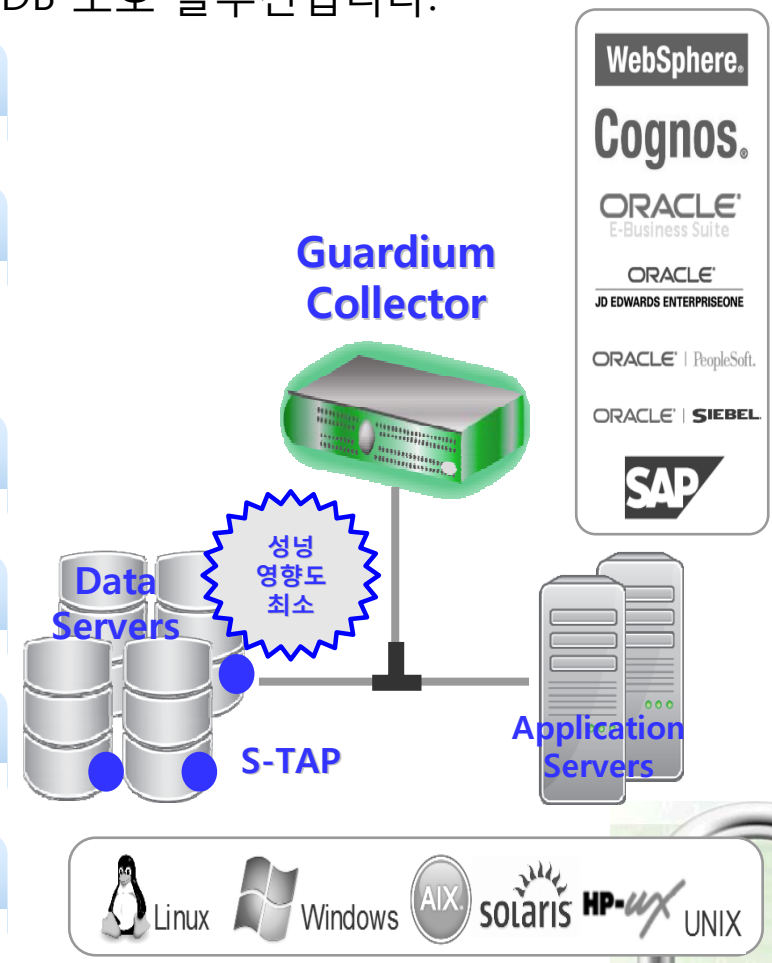
- 권한사용자 대상 정책 기반 쿼리 데이터 결과값 마스킹

다양한 보고서

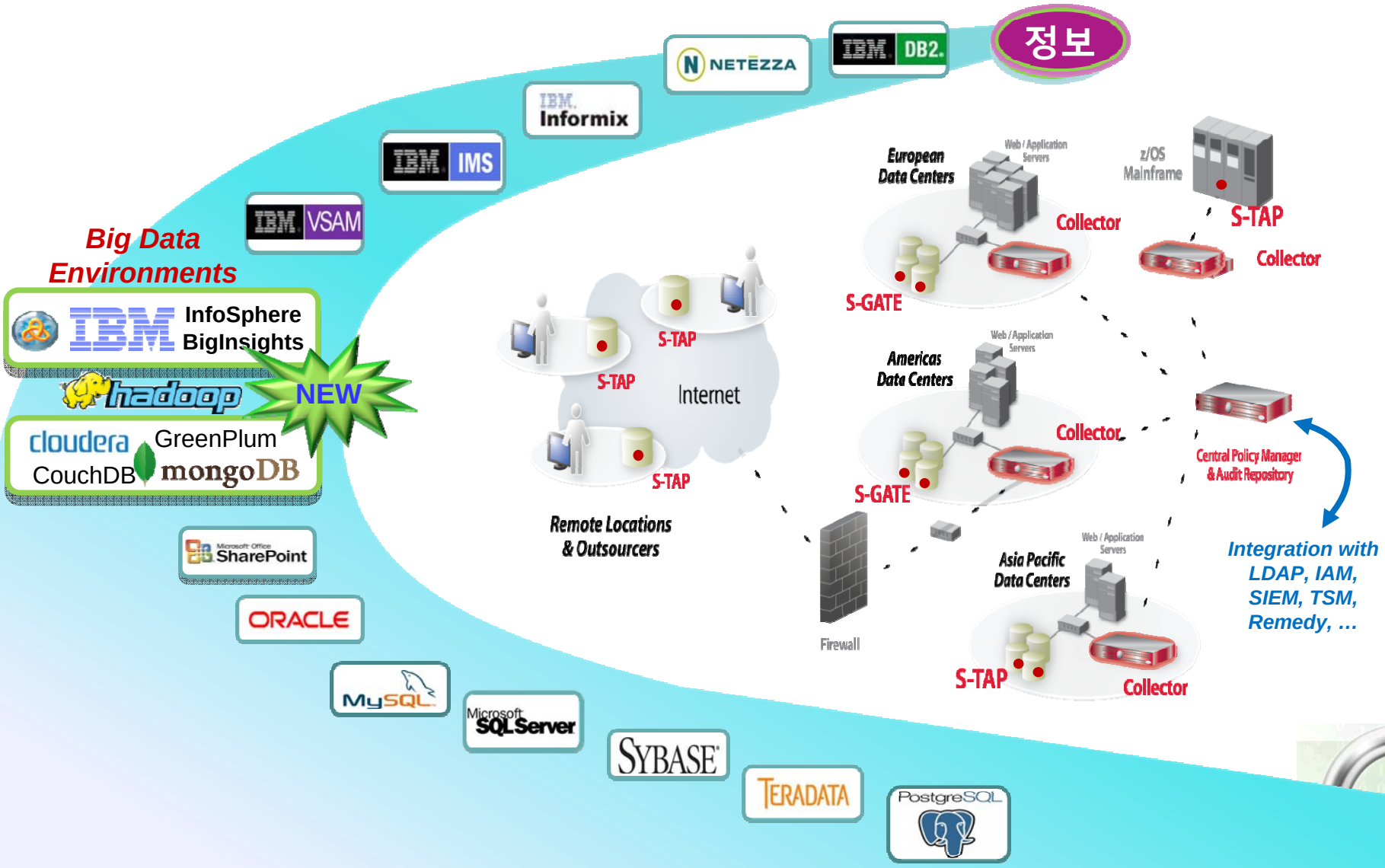
- 다양한 필터링 조건에 의한 검색 보고서 기능을 제공

유연한 외부 시스템 연계

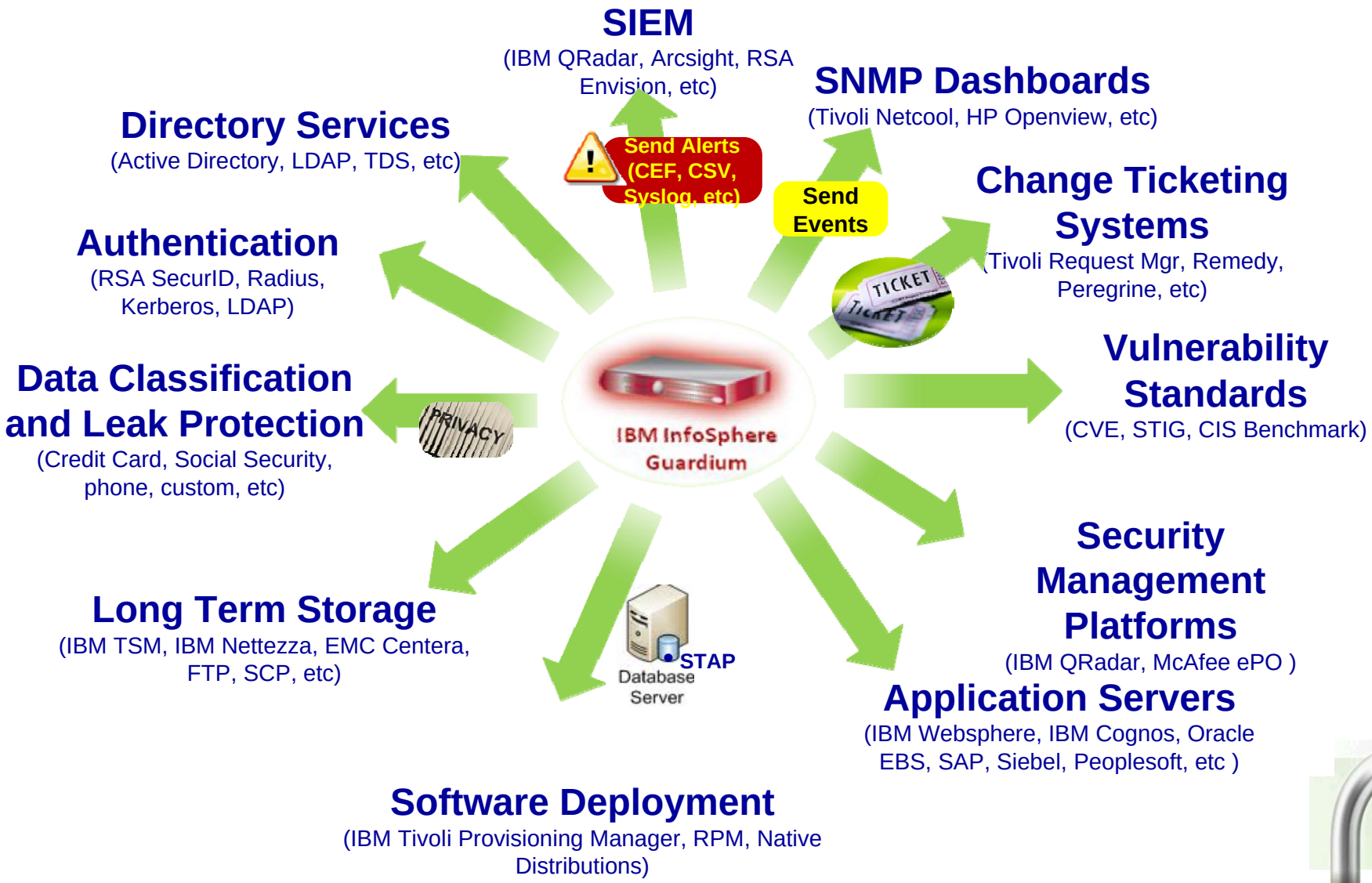
- 통합관제, 백업시스템 등 다양한 외부 시스템과의 연계 제공



다양한 전사 이기종 환경에 대한 지원



주변 인프라와의 원활한 통합



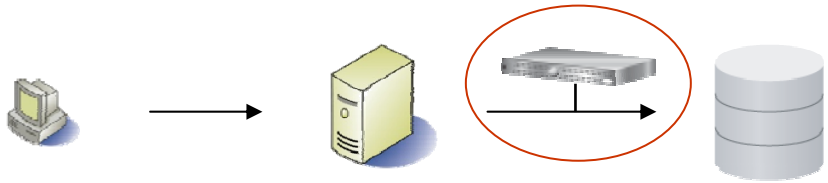
Guardium을 통한 데이터 보안 지원

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)

실시간 DB 활동 모니터링#1 – 대/내외 트랜잭션 리포팅

Database Activity Monitoring
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



Client IP
Client host name
Domain login
App user ID
Client OS
MAC
TTL
Origin
Failed logins

Server IP
Server port
Server name
Session
SQL patterns
Network protocol
Server OS
Timestamp
Access programs

ALL SQL commands
Fields
Objects
Verbs
DDL
DML
DCL
DB user name
DB version
DB type
DB protocol
Origin
DB errors
Selects

예) SQL 모니터링 주요 내용 ....
-어느 네트워크 사용자가 어떤 데이터에 접근 하는가 ?
-어느 어플리케이션이 어떤 데이터에 접근 하는가 ?
-인가되지 않은 소스 프로그램에서 Data를 어느 때 변경시키는가 ?
-어떤 종류의 DB오류가 발생하고 Data 접근은 어떻게 되고 있는가 ?
-DB관리자 또는 외부용역 직원은 어떤 DB감사 업무를 수행하고 있는가 ?
-DB스키마 또는 테이블을 누가 변경 또는 삭제 하는가 ?
-DB사용 현황(누가,언제,어떤 등)은 매일 유사한가 ?
-혹시 어떤 인가되지 않은 프로그램에서 재무 Data를 사용하지는 않는가 ?
-로그인 실패는 어디에서 얼마나 일어나고 있는가 ?
-비사용 data로 인하여 저장공간을 낭비하고 있지는 않은가 ?
-민감한 오브젝트의 노출은 없는가 ?
-누가, 언제 SQL injection 공격을 시도하는가

All SQL traffic contextually analyzed & filtered in real-time to provide specific information required by auditors

실시간 DB 활동 모니터링#2 – 이상 트랜잭션 감지

Should my customer service rep view 99 records in an hour when average is 4?

Is this normal?

DB User Name	Sql	Records
STEVE	select * from ar.creditcard where i>? and i<?	4
HARRY	select * from ar.creditcard where i<?	4
JOE	select * from ar.creditcard where i<?	99

What did he see?

HARRY	select * from ar.creditcard where i<?	**********0002, **********0003, **********0004
JOE	select * from ar.creditcard where i<?	**********0001
JOE	select * from ar.creditcard where i<?	**********0002, **********0003, **********0004, **********0005, **********0006, **********0007, **********0008, **********0009, **********0010, **********0011, **********0012, **********0013, **********0014, **********0015, **********0016
JOE	select * from ar.creditcard where i<?	**********0017, **********0018, **********0019, **********0020, **********0021, **********0022, **********0023, **********0024, **********0025, **********0026, **********0027, **********0028, **********0029, **********0030, **********0031
JOE	select * from ar.creditcard where i<?	**********0032, **********0033, **********0034, **********0035, **********0036, **********0037, **********0038, **********0039, **********0040, **********0041, **********0042, **********0043, **********0044, **********0045, **********0046
JOE	select * from ar.creditcard where i<?	**********0047, **********0048, **********0049, **********0050, **********0051, **********0052, **********0053, **********0054, **********0055, **********0056, **********0057, **********0058, **********0059, **********0060, **********0061
JOE	select * from ar.creditcard where i<?	**********0062, **********0063, **********0064, **********0065, **********0066, **********0067, **********0068, **********0069, **********0070, **********0071, **********0072, **********0073, **********0074, **********0075, **********0076
JOE	select * from ar.creditcard where i<?	**********0077, **********0078, **********0079, **********0080, **********0081, **********0082, **********0083, **********0084, **********0085, **********0086, **********0087, **********0088, **********0089, **********0090, **********0091
JOE	select * from ar.creditcard where i<?	**********0092, **********0093, **********0094, **********0095, **********0096, **********0097, **********0098, **********0099

자동화된 컴플라이언스 솔루션

Auditing and compliance solutions
감사 및 compliance 솔루션

-포괄적이고 사용하기 쉬운 패키지화된 리포트 기능제공
-컴플라이언스 워크플로우 자동화를 이용한 운영비용 감소
-PCI-DSS , SOX, SAS70,ISO 27001/2 ,NIST 800-53 등 관련

-기업의 데이터 환경은 기업 정책,정부규정,업계 표준에 맞는 Information Governance 가 필요

- PCI-DSS Payment Card Industry Data Security Standard
- SOX Sarbanes-Oxley Act
- EUDPD European Union Data Protection Directive

Audit Requirements	COBIT (SOX)	PCI-DSS	ISO 27002	Data Privacy & Protection Laws	NIST SP 800-53 (FISMA)
1. Access to Sensitive Data (Successful/Failed SELECTs)		✓	✓	✓	✓
2. Schema Changes (DDL) (Create/Drop/Alter Tables, etc.)	✓	✓	✓	✓	✓
3. Data Changes (DML) (Insert, Update, Delete)	✓		✓		
4. Security Exceptions (Failed logins, SQL errors, etc.)	✓	✓	✓	✓	✓
5. Accounts, Roles & Permissions (DCL) (GRANT, REVOKE)	✓	✓	✓	✓	✓

•DDL = Data Definition Language (aka schema changes)
•DML = Data Manipulation Language (data value changes)
•DCL = Data Control Language

<PCI-DSS sample>

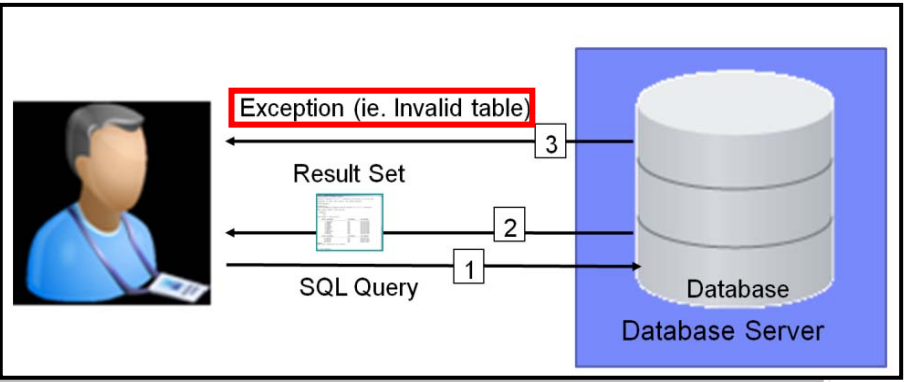
자동화된 컴플라이언스 솔루션#2 – SAP PCI 정책 예시

Policy Rules

- PCI, SAP Production

Expand All | Collapse All | Select All

1	Access Rule: Non SAP DB Server - Ignore
2	Exception Rule: Failed Login - Log Violation
3	Exception Rule: Failed Login - Alert if repeated
4	Exception Rule: SQL Error - Log
5	Exception Rule: SQL Error - Alert on Risk Indicative errors
6	Access Rule: Selects Commands, Not APP Users, Cardholder SAP Objects - Log Full Details
7	Access Rule: DDL Commands, Cardholder SAP Objects - Log Full Details
8	Access Rule: Suspicious Users - Log Full Details
9	Access Rule: Suspicious Users, Cardholder SAP Objects - Log Info
10	Access Rule: Grant Commands, Cardholder SAP Objects - Log INFO
11	Access Rule: DDL Commands, Cardholder SAP Objects - Log INFO
12	Access Rule: DML Commands - Allow
13	Access Rule: guardium://CREDIT_CARD , Unauthorized - Violation
14	Access Rule: guardium://PCI_TRACK_DATA , Unauthorized Users - Violation
15	Access Rule: Unauthorized Clients access Cardholder SAP Objects - Alert
16	Access Rule: Unauthorized Users on Cardholder SAP Objects - Alert
17	Extrusion Rule: Credit Card Numbers, Unauthorized Users - Log Violation
18	Extrusion Rule: PCI Track Data, Unauthorized Users - Log Violation



24

데이터베이스 구성변경 감사기능#1 – 환경 변수 감사/리포팅

Change control solutions
변경 제어솔루션

데이터베이스 구조,권한 및 환경구성파일의 무단변경 방지

$ORACLE_HOME/soap/bin/.*	File Pattern	12h	✓	✓
$ORACLE_HOME/sysman/admin/OMSRepositoryConstraints.properties	File Pattern	12h	✓	✓
$ORACLE_HOME/sysman/config/.*properties	File Pattern	12h	✓	✓
$ORACLE_HOME/xdk/admin/xml.properties	File Pattern	12h	✓	✓
ORACLE_BASE	Environment Variable	12h	✓	⊘
ORACLE_HOME	Environment Variable	12h	✓	⊘
ORACLE_SID	Environment Variable	12h	✓	⊘
TNS_ADMIN	Environment Variable	12h	✓	⊘
select * from dba_db_links	SQL Script	12h	✓	⊘

- 보안에 영향을 미칠 수 있는 파일, 환경변수 , 레지스트리 설정, 스크립트 등 변경사항들을 추적
- 500 + 이상의 모든 주요 운영체제/ DBMS 구성을 위한 사전구성, 사용자 지정 템플릿을 제공

데이터베이스 구성변경 감사기능#2 – 구성 파일 감사/리포팅

```
[tec156] root:/oracle/POC/102_64/network/admin>cat tnsnames.ora
# tnsnames.ora Network Configuration File: /oracle/POC/102_64/network/admin/tnsnames.ora
# Generated by Oracle configuration tools.

#################
# Filename......: tnsnames.ora
# Created.......: created by SAP AG, R/3 Rel. >= 6.10
# Name..........:
# Date..........:
# @(#) $Id: //bc/700-1_REL/src/ins/SAPINST/impl/tpls/ora/ind/TNSNAMES.ORA#4 $
#################

LISTENER_POC.WORLD =
  (ADDRESS = (COMMUNITY = SAP.WORLD)(PROTOCOL = TCP)(HOST = tec156)(PORT = 1528))


POC.WORLD =
  (DESCRIPTION =
    (ADDRESS = (COMMUNITY = SAP.WORLD)(PROTOCOL = TCP)(HOST = tec156)(PORT = 1528))
    (CONNECT_DATA =
      (SERVER = DEDICATED)
      (SERVICE_NAME = POC)
    )
  )

LISTENER_POC.WORLD =
  (ADDRESS = (COMMUNITY = SAP.WORLD)(PROTOCOL = TCP)(HOST = tec156)(PORT = 1521))
```

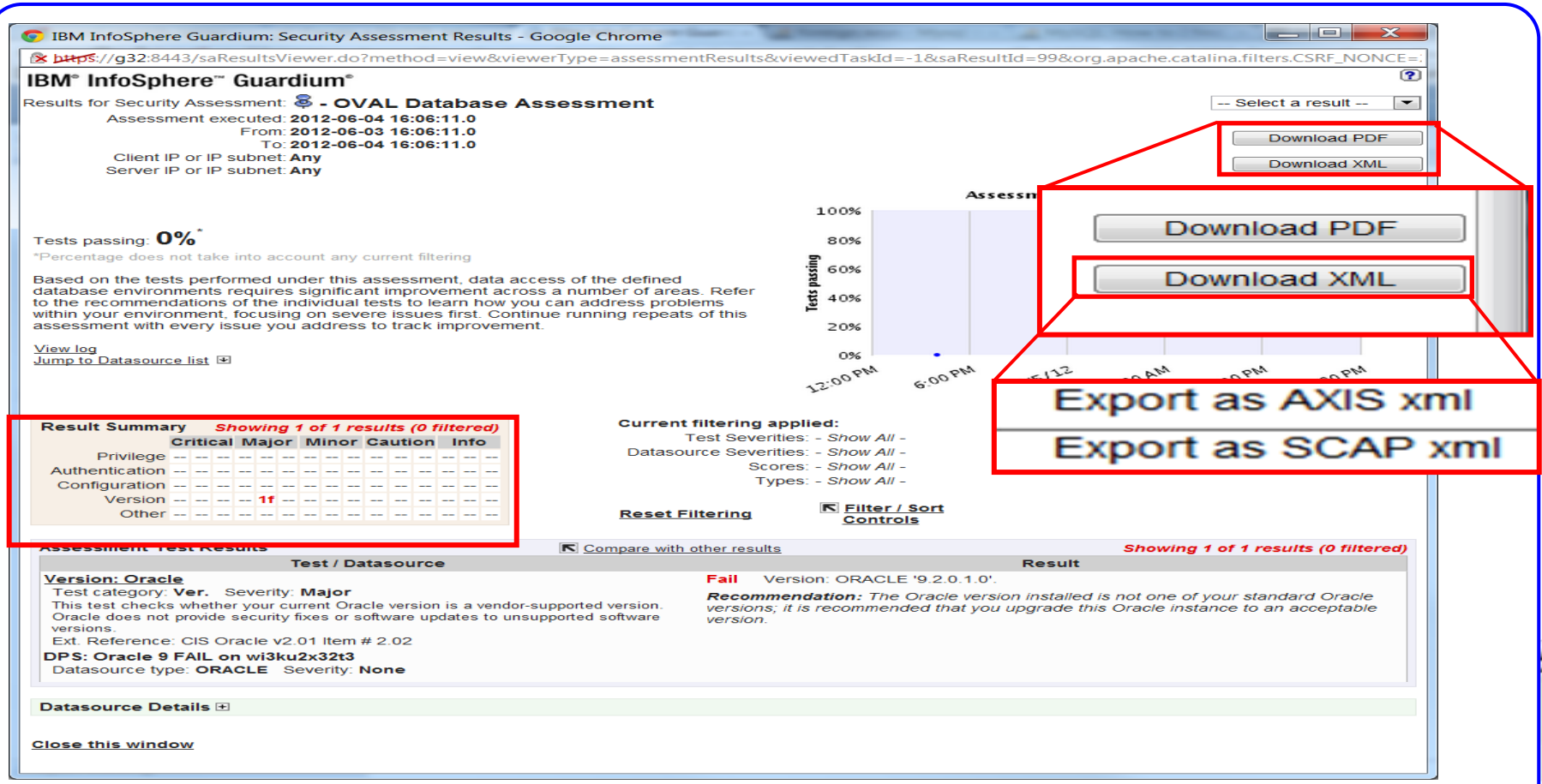
8:30

	Saved Data	Last Modified
10.10.13.156 /oracle/POC/102_64/network/admin/tnsnames.ora	# tnsnames.ora Network Configuration File: /oracle/POC/102_64/network/admin/tnsnames.ora # Generated by Oracle configuration tools. ################# # Filename.....: tnsnames.ora # Created.....: created by SAP AG, R/3 Rel. >= 6.10 # Name.....: # Date.....: # @(#) $Id: //bc/700- 1_REL/src/ins/SAPINST/impl/tpls/ora/ind/TNSNAMES.ORA#4 $ ################# LISTENER_POC.WORLD = (ADDRESS = (COMMUNITY = SAP.WORLD)(PROTOCOL = TCP) (HOST = tec156)(PORT = 1528)) POC.WORLD = (DESCRIPTION = (ADDRESS = (COMMUNITY = SAP.WORLD)(PROTOCOL = TCP) (HOST = tec156)(PORT = 1528)) (CONNECT_DATA = (SERVER = DEDICATED) (SERVICE_NAME = POC))) LISTENER_POC.WORLD = (ADDRESS = (COMMUNITY = SAP.WORLD)(PROTOCOL = TCP) (HOST = tec156)(PORT = 1521))	2011-09-20 18:45:39.0

취약성 분석 및 보고서 제공

Vulnerability management
취약성관리

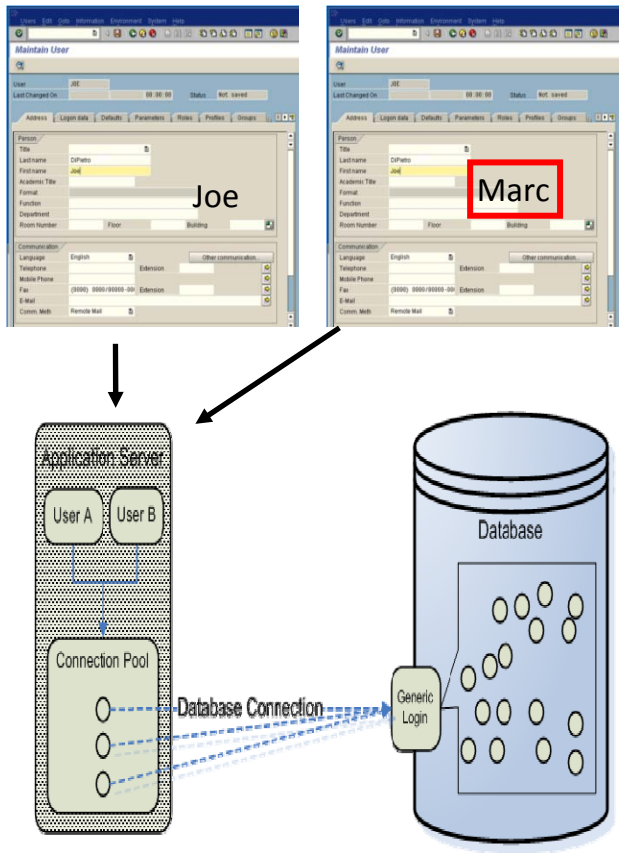
누락된 패치, 잘못 구성된 권한 및 기본 계정과 같은 데이터베이스 취약점 식별 및 관련 보고서 제공
비인가 접속사용자, SQL 에러,과도한 접속시도,업무시간 외 접속 등 전반적인 DB 시스템의 취약성 평가서 제공



사기방지:어플리케이션 계층의 사기식별기능

Fraud prevention solutions
사기방지솔루션

어플리케이션 계층의 승인되지 않는 응용프로그램 사용자 활동을 식별하는 모니터링
(SAP, PeopleSoft , Oracle EBS, Cognos Etc)



DB User Name	Application User	Sql
APPUSER	joe	select * from EmployeeRoleView where UserName=?
APPUSER	joe	select * from EmployeeTable
APPUSER	marc	insert into EmployeeTable values (?,?,?,?,?,?,?,?)

이슈: Application server 는 데이터베이스에 접근하기 위해 일반적인 서비스 계정을 사용

BUT 누가 트랜잭션을 시작했는지 알 수 없음(connection pooling)

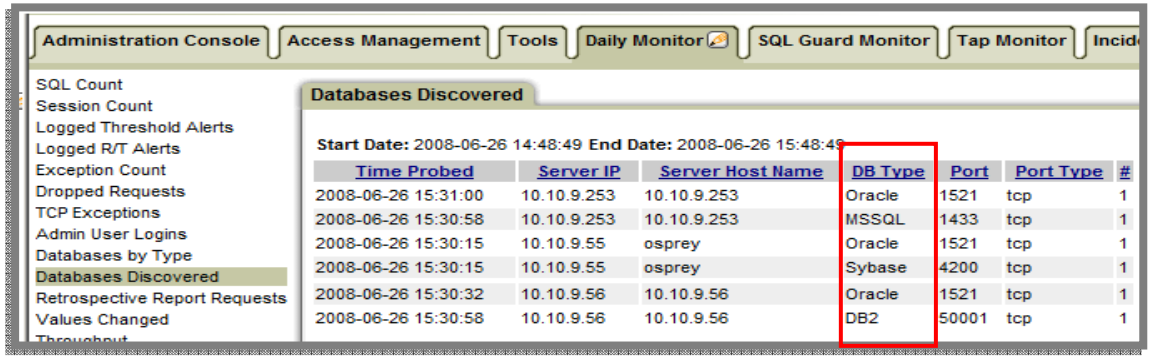
해결책 : Guardium 은 특정 SQL 과 조합된 **application user** 와 **함께 추적**

- ✓ 주요 application 및 custom application 을 지원
  (WebSphere ,Oracle EBS, PeopleSoft, SAP, Siebel, Cognos 등)
- ✓ Application 변경 필요 없음
- ✓ User ID 의 결정적 추적
- ✓ Time-based 의 추측에 의존하지 않음

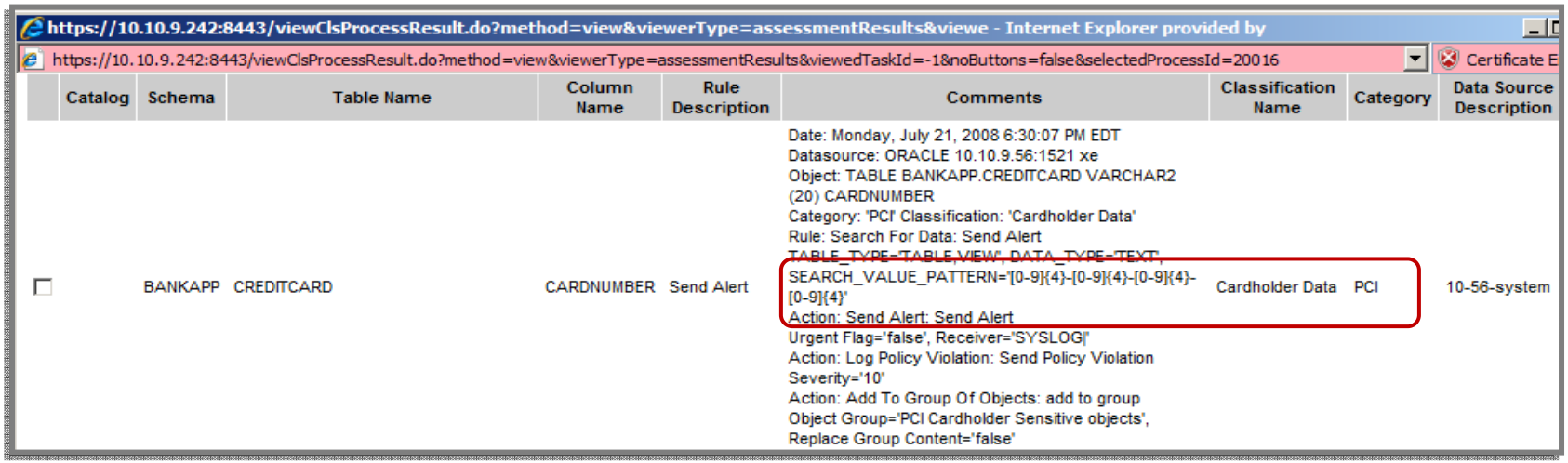
데이터베이스 유출방지#1 – DB, 민감 데이터 식별

Database leak prevention
데이터베이스 유출방지

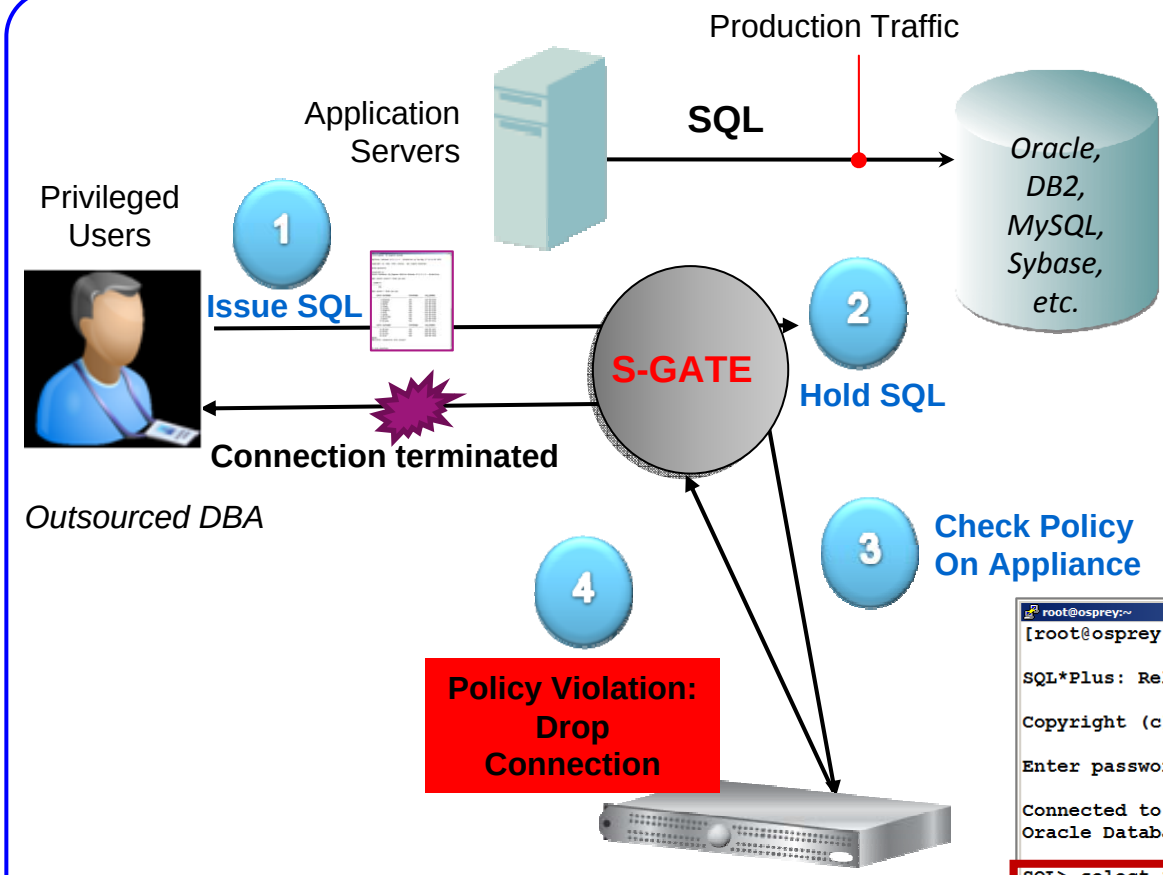
민감한 데이터를 찾고, 데이터 센터 침해요인을 제거
(주민번호, 신용카드번호 등)



- 데이터베이스 탐색
- 민감한 데이터 탐색
- 정책 기반 Action 수행
  - ✓ Alerts 수행
  - ✓ 민감데이터 그룹화



데이터베이스 유출방지#2 – 비인가자 접근제어



- 데이터베이스 변경 없음
- Application 변경 없음

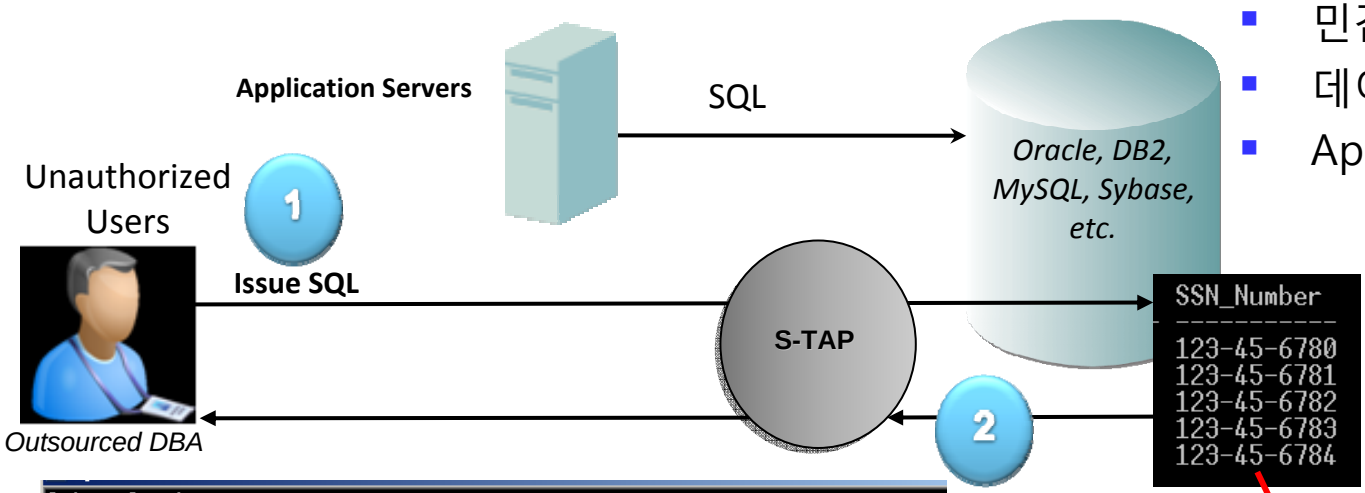
```
root@osprey:~
[root@osprey ~]# sqlplus system

SQL*Plus: Release 10.2.0.1.0 - Production on Tue May 27 01:13:32 20

Copyright (c) 1982, 2005, Oracle.  All rights reserved.

Enter password:

Connected to:
Oracle Database 10g Express Edition Release 10.2.0.1.0 - Production

SQL> select * from creditcard;
select * from creditcard
*
ERROR at line 1:
ORA-03113: end-of-file on communication channel


SQL>
```

Session Terminated

데이터베이스 유출방지#3 – 민감 데이터 마스킹

Unauthorized Users Masked when Sensitive Information Cross-DBMS, Data-Level Access Control (Redact)

- 전사/이기종 DB 지원
- 민감 데이터 마스킹
- 데이터베이스 변경 없음
- Application 변경 없음




```
C:\>sqlcmd
1> select * from ssn where ssnid < 5
2> go
SSNID       LastName                  FirstName     SSN_Number
----------- ------------------------- ------------- -----------
          0 Anthony                   joe           ******-6780
          1 Thomas                    joe           ******-6781
          2 Smith                     Joe           ******-6782
          3 Jones                     Joe           ******-6783
          4 Craven                    Joe           ******-6784

(5 rows affected)
1> quit
```

Redact and Mask Sensitive Data

User view of the data in the database

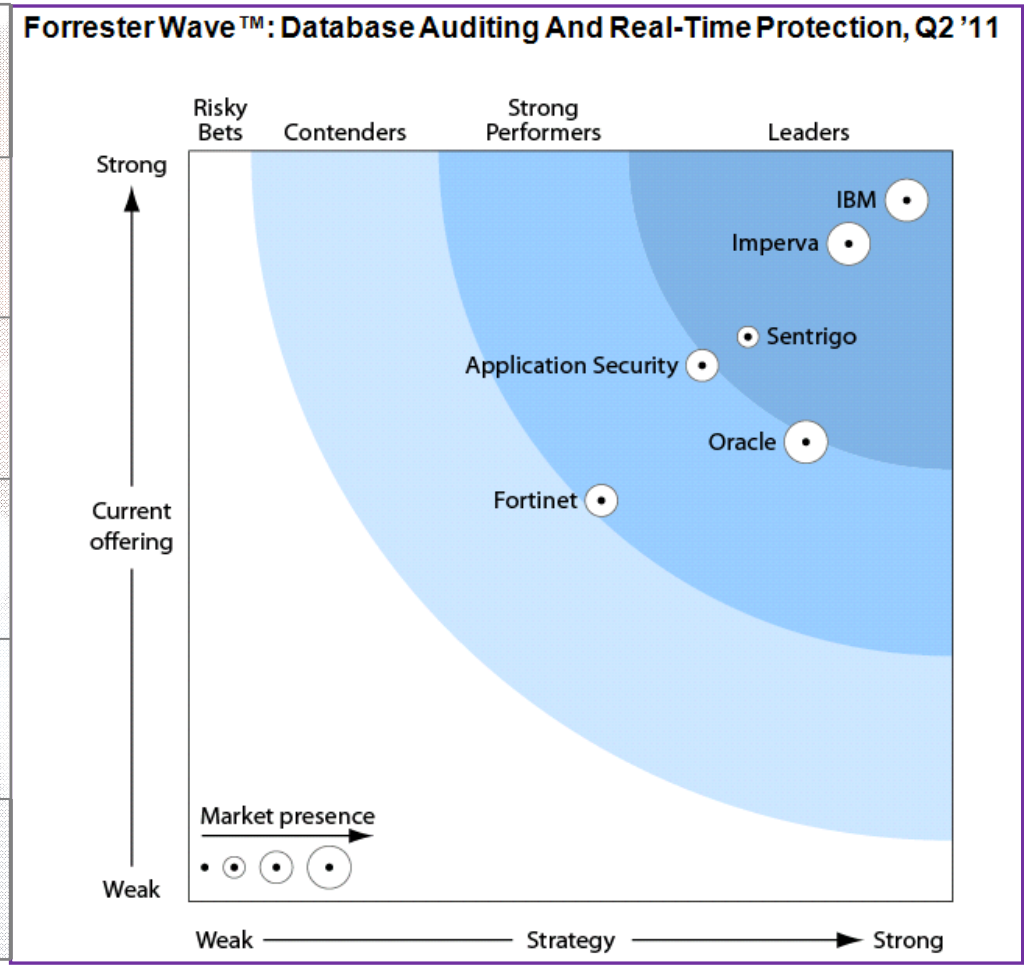
Agenda

- 데이터를 둘러싼 환경
- 전사 데이터 암호화를 위한 IBM 솔루션
- 전방위 DB 보호를 위한 IBM 솔루션
- **사례 및 결론**

데이터 보안 시장을 선도하는 IBM

Forrester에서 17개 항목 중 총 15개의 평가분야 최고점을 인정한 Guardium

Awarded highest score in overall “Market Pre sence”
Awarded highest score in overall “Strategy”
Awarded highest score in evaluation of “Curre nt Offering”
Achieved highest score possible in 8 out of 16 high-level scored categories
Achieved the top ranking in 7 high-level categories; tied for top ranking in 1 category
Evaluation based on v7, v8 introduced weeks after cutoff



Source: The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011, May 6, 2011. Forrester Research, Inc., The Forrester Wave™: Database Auditing And Real-Time Protection, Q2 2011, May 6, 2011. The Forrester Wave is copyrighted by Forrester Research, Inc. Forrester and Forrester Wave are trademarks of Forrester Research, Inc. The Forrester Wave is a graphical representation of Forrester's call on a market and is plotted using a detailed spreadsheet with exposed scores, weightings, and comments. Forrester does not endorse any vendor, product, or service depicted in the Forrester Wave. Information is based on best available resources. Opinions reflect judgment at the time and are subject to change.

업계 선도 기업들이 선택한 검증된 솔루션

5 of the top 5 global banks

*Protecting access to over **$10,869,929,241** in financial assets*

4 of the top 4 global managed healthcare providers

*Protecting access to **136 million** patients private information*

2 of the top 3 global retailers

*Safeguarding the integrity of **2.5 billion** credit card or personal information transactions per year*

Top government agencies

Safeguarding the integrity of the world's government information and defense

5 of the top 6 global insurers

*Protecting more than **100,000 databases** with personal and private information*

8 of the top 10 telcos worldwide

*Maintaining the privacy of over **1,100,000,000 subscribers***

전문가들이 인정한 검증된 솔루션

FORRESTER®

"Dominance in this space"
#1 Scores for Current Offering, Architecture & Product Strategy

ChannelWeb

"Most Powerful Compliance Regulations Tools ... Ever"

SC MAGAZINE

"5-Star Ratings: Easy installation, sophisticated reporting, strong policy-based security."

the 451 group

"Guardium is ahead of the pack and gaining speed."

InformationWeek

"Top of DBEP Class"
"Practically every feature you'll need to lock down sensitive data."

RED HERRING N. AMERICA WINNER 100

SQL SERVER MAGAZINE

2007 Editor's Choice Award in "Auditing and Compliance"

INFORMATION SECURITY MAGAZINE

"Enterprise-class data security product that should be on every organization's radar."

INFORMATION SECURITY Hotpick