개인정보보호법과 전방위적 데이터 보안

2011/08/26

조가원 전문위원, 한국IBM

Agenda

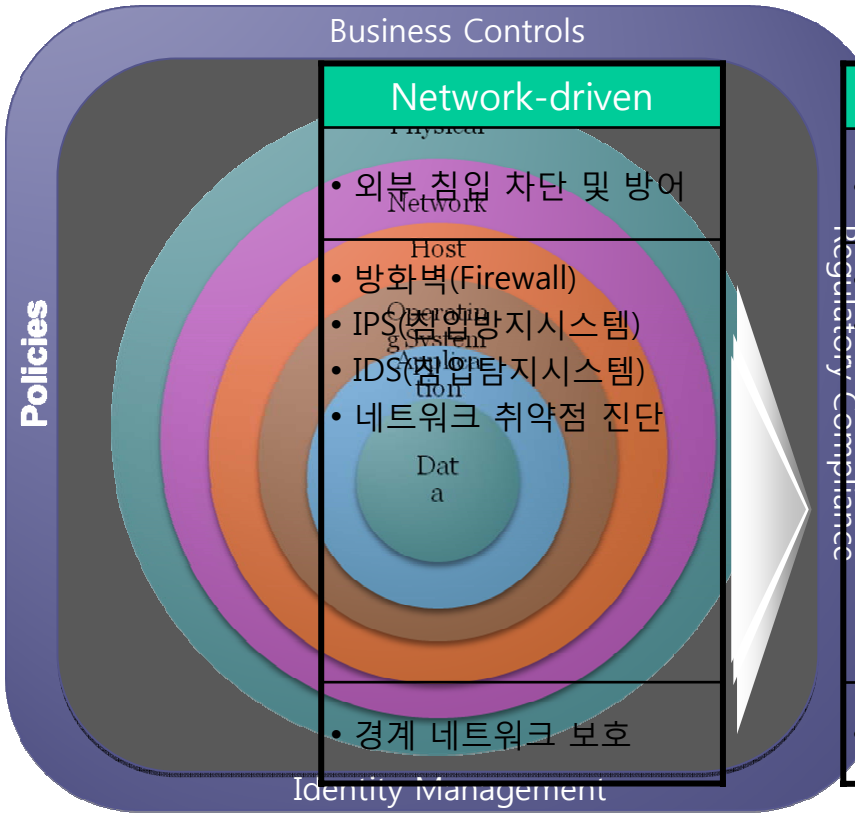
- 데이터 보안 현황
- 개인정보보호법과 데이터 보안
- IBM의 데이터 보안 영역별 솔루션
- 전방위 데이터 보안 솔루션 Guardium
- 사례 및 결론

IBM

데이터를 둘러싼 현황

"A fortress mentality will not work in cyber. We cannot retreat behind a Maginot Line of firewalls." - William J. Lynn III, U.S. Deputy Defense Secretary

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) - Network DLP - Endpoint DLP • 데이터 암호화 - 암호화 - 마스킹
• 경계 네트워크 보호	• 서버/어플리케이션 보호	• 단말 데이터베이스 보호

Regulatory Compliance

Agenda

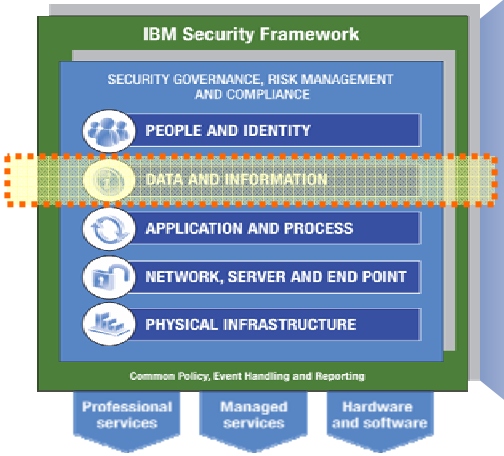
- 데이터 보안 현황
- 개인정보보호법과 데이터 보안
- IBM의 데이터 보안 영역별 솔루션
- 전방위 데이터 보안 솔루션 Guardium
- 사례 및 결론

IBM

IBM 보안 프레임워크와 데이터 보안

IBM was named the **"Best Security Company"*** by SC Magazine

Source: SC Magazine award, March 2, 2010



GRC

거버넌스, 위험 관리와 컴플라이언스
보안과 개인 정보 보호를 위한 강력한 기반의 설계와 배포

사람과 아이덴터티
기업 자산에 접근하는 사용자와 관련된 위험 완화

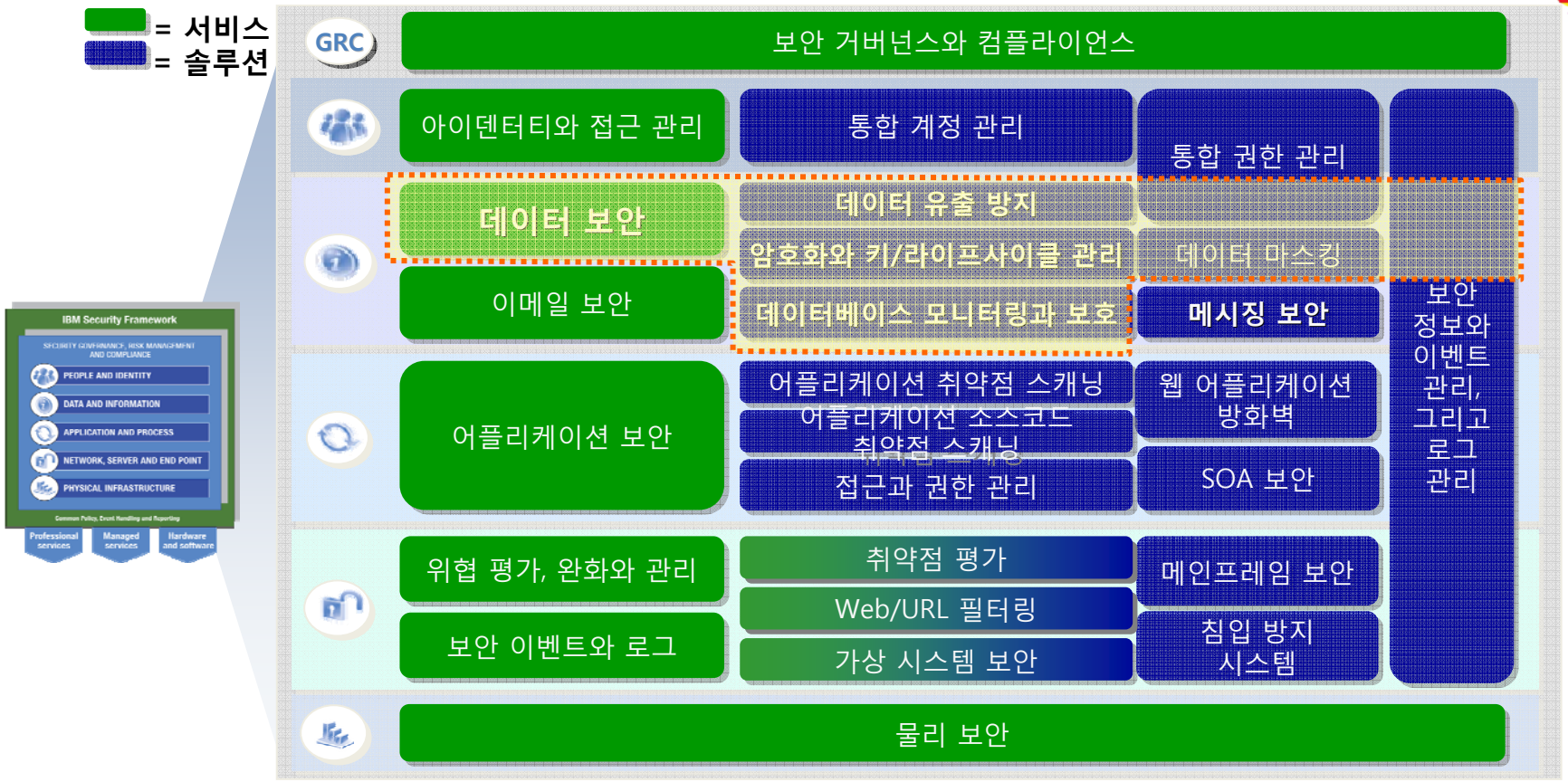
데이터와 정보
민감한 데이터의 접근과 사용에 대한 통제의 이해, 배포, 적절한 테스트

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

네트워크, 서버와 단말
기반 인프라스트럭처에 대한 위험 완화를 통해 서비스 가용성 최적화

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

IBM 보안 프레임워크와 데이터 보안 지원 영역



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
		데이터 유출 방지
	애플리케이션 보안	
	불필요한 데이터에 대한 폐기	라이프사이클관리
로그관리 (최소 1년)	접속 로그 기록 -접근 기록 및 실시간 모니터링 솔루션 -접속기록 백업 솔루션	데이터베이스 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	

Agenda

- 데이터 보안 현황
- 개인정보보호법과 데이터 보안
- IBM의 데이터 보안 영역별 솔루션
- 전방위 데이터 보안 솔루션 Guardium
- 사례 및 결론

IBM

데이터 보안 영역별 솔루션 구성

■로깅/감사/컴플라이언스 리포트
: Infosphere Guardium DAM

■민감한 데이터 검색: Infosphere Discovery, Infosphere Guardium
■데이터 이용내역 모니터링: Infosphere Guardium DAM
■사전 데이터 보호/접근제어 : Infosphere Guardium S-GATE
■취약성 평가: Infosphere Guardium Vulnerability Assessment

데이터베이스
모니터링과 보호

데이터
유출 감지

키/라이프사
이클 관리

■비활성데이터의 폐기:
Infosphere Optim
Decommissioning

데이터 보안

암호화

■칼럼 단위 암호화: 자체 DBMS내 고유 Encrypt 함수 사용 혹은 전용 암호화 솔루션
■DB 레벨 암호화: DB2, Informix- Infosphere Guardium Encryption Expert, 이외 3rd Party제품

문서 마스킹

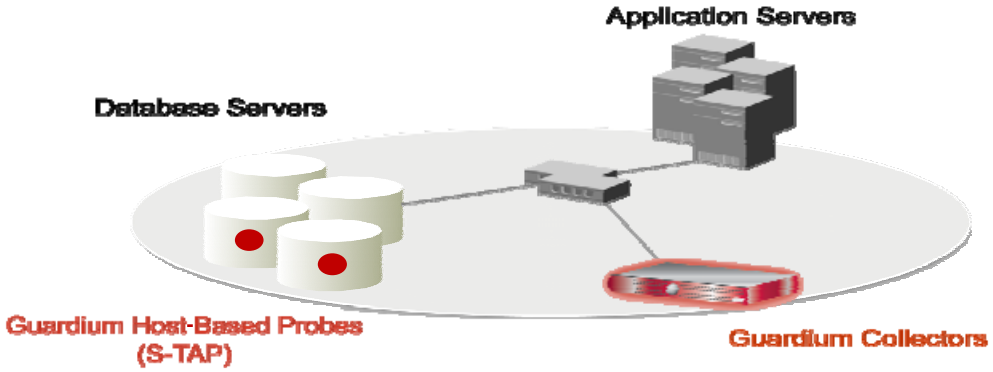
■문서 데이터 적정 알고리즘 적용을 통한 대체: Infosphere Guardium Data Redaction

데이터 마스킹

■운영 데이터 마스킹: Infosphere Guardium DAM Redaction
■비운영 환경내 데이터 마스킹: Infosphere Optim Data Privacy

IBM

실시간 DB 모니터링 – Infosphere Guardium DAM



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

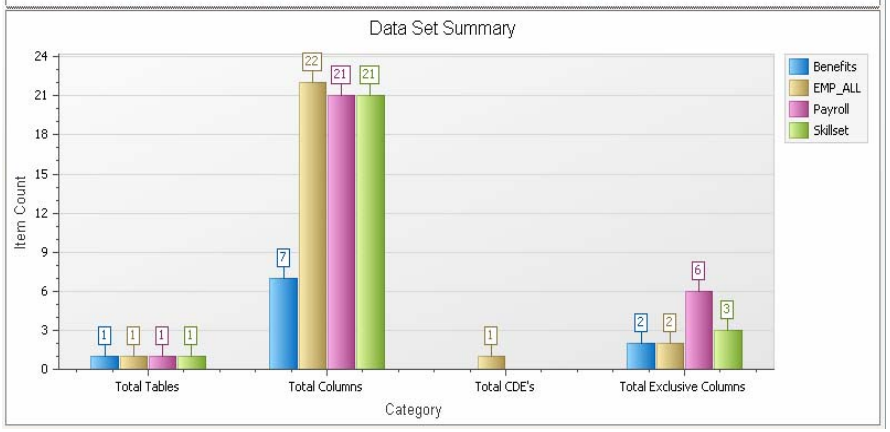
- Activity logs 는 DBA 나 침입자에 의해 영향 받지 않음
- 자동화된 컴플라이언스 레포팅,결제상신 (SOX, PCI, NIST, etc.)
- 실시간 정책 & 감사 세분화
  - *Who, what, when, where, how*

민감한 정보 탐색 및 정의 – Infosphere Discovery

- 데이터베이스 내 다양한 데이터 분석을 통해 데이터의 연관도 및 민감한 데이터를 검색

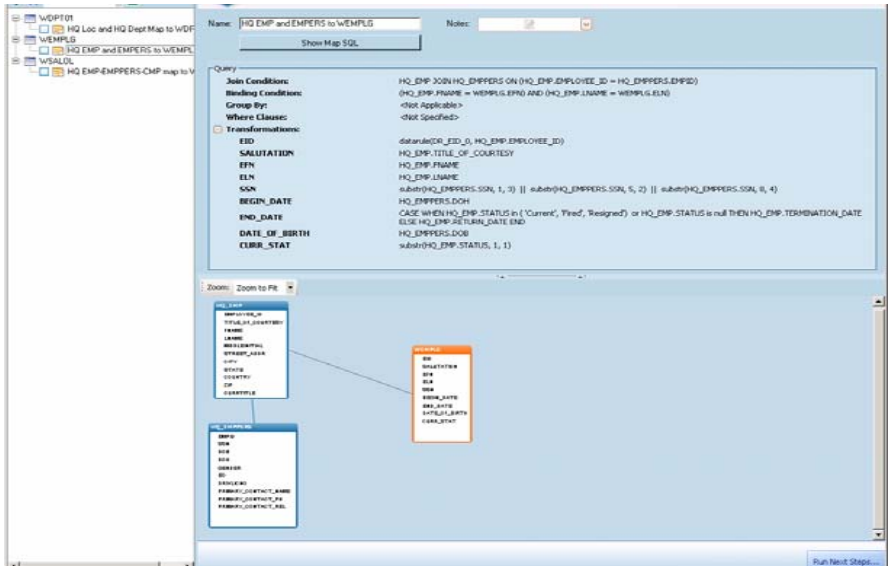
< 알려진 구조의 Sensitive 데이터 식별 >

Data Set	Total Tables	Total Columns	Total CDE's	Total Exclusive Columns
Benefits	1	7	0	2
EMP_ALL	1	22	1	2
Payroll	1	21	0	6
Skillset	1	21	0	3



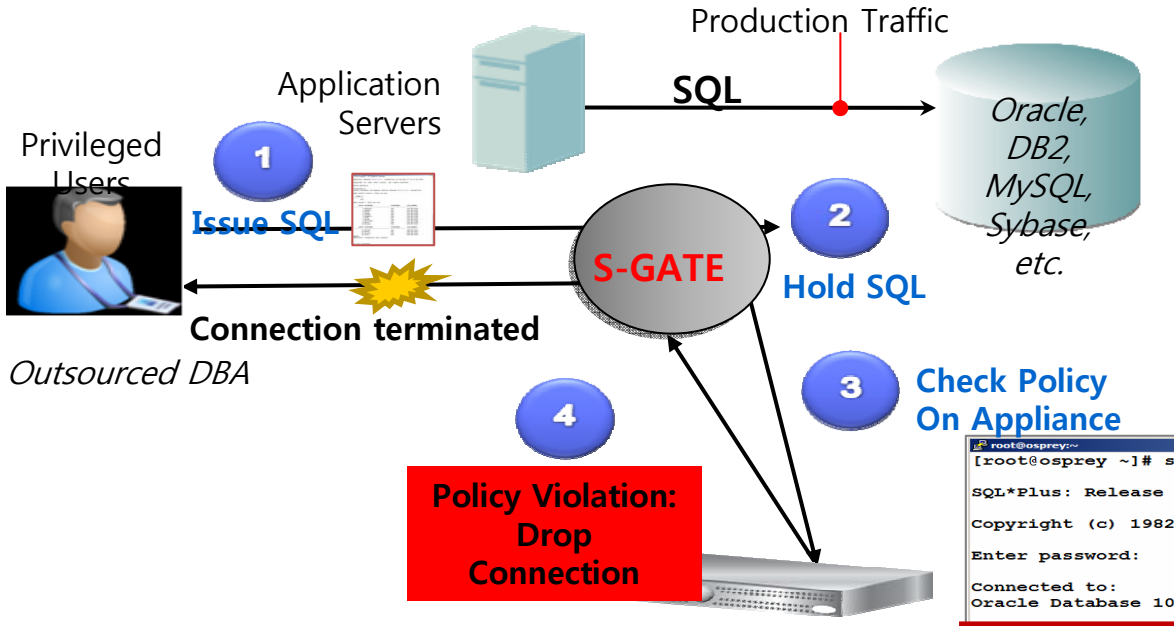
- 동시에 다양한 데이터를 분석
- 다양한 시스템에 존재하는 데이터에 대해 알려진 구조의 Sensitive data와 일치하는 것을 찾아냄

< 숨겨진 Sensitive 데이터의 발견 >



- 한 필드내 부분적으로 숨겨진 sensitive data의 발견
- 복수개의 컬럼에 분산된 Sensitive data의 발견
- 변환된 sensitive data의 발견

DB 접근 제어 – Infosphere Guardium S-GATE



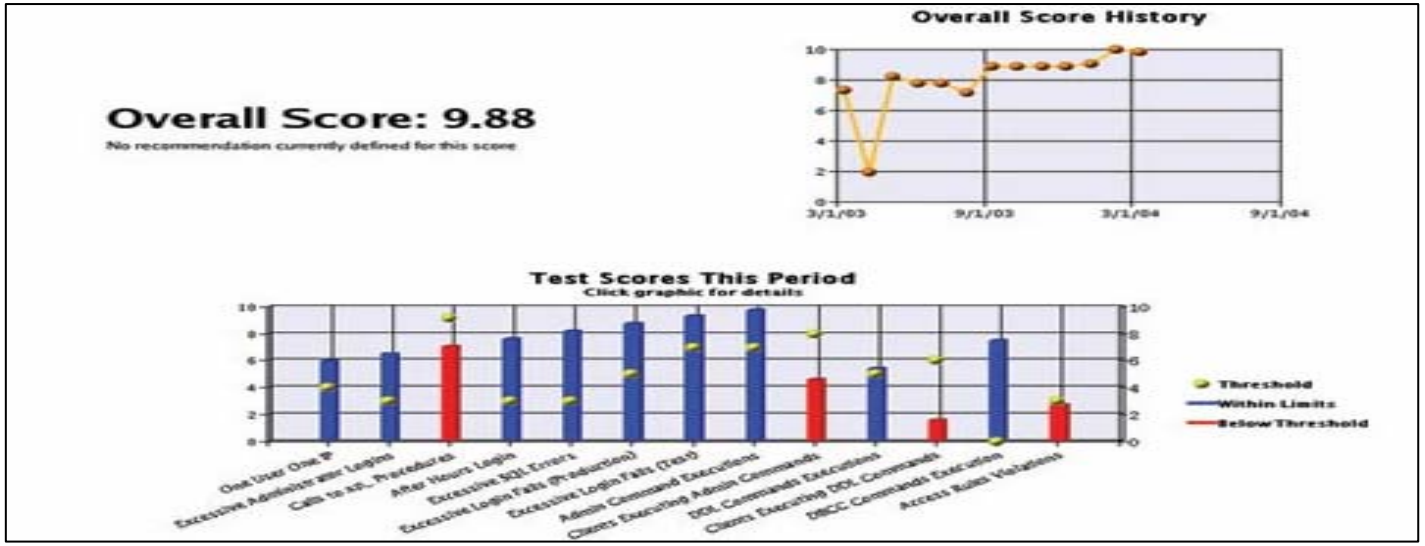
- 데이타베이스 변경없음
- Application 변경없음
- Inline application 의 트래픽 방해 없음

```
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

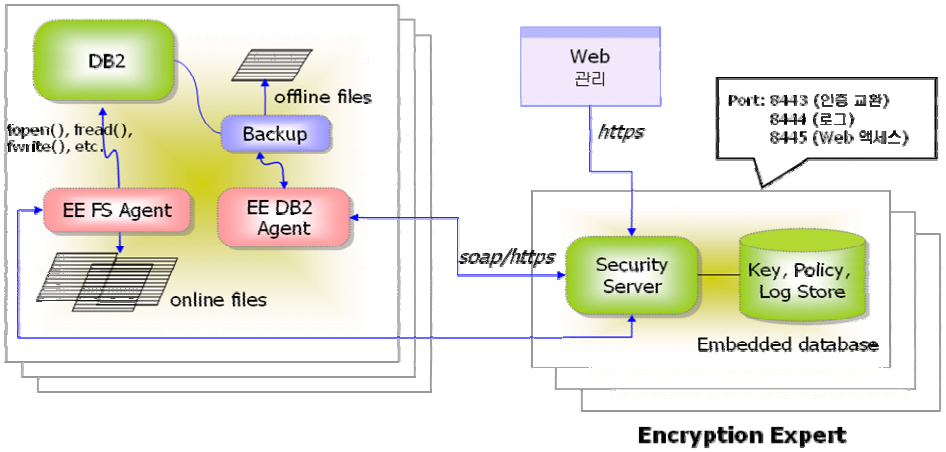
DB 보안 취약성 평가 – Infosphere Guardium Vulnerability Assessment

- 자체 DB보안 취약점 평가
- 스케줄링에 의한 주기적인 자동 리포트 생성
- 비인가 접속 사용자, SQL Error, 과도한 접속 시도, 업무 외 시간 접속 등 전반적인 DB시스템의 취약점 평가 후 지속적 대응



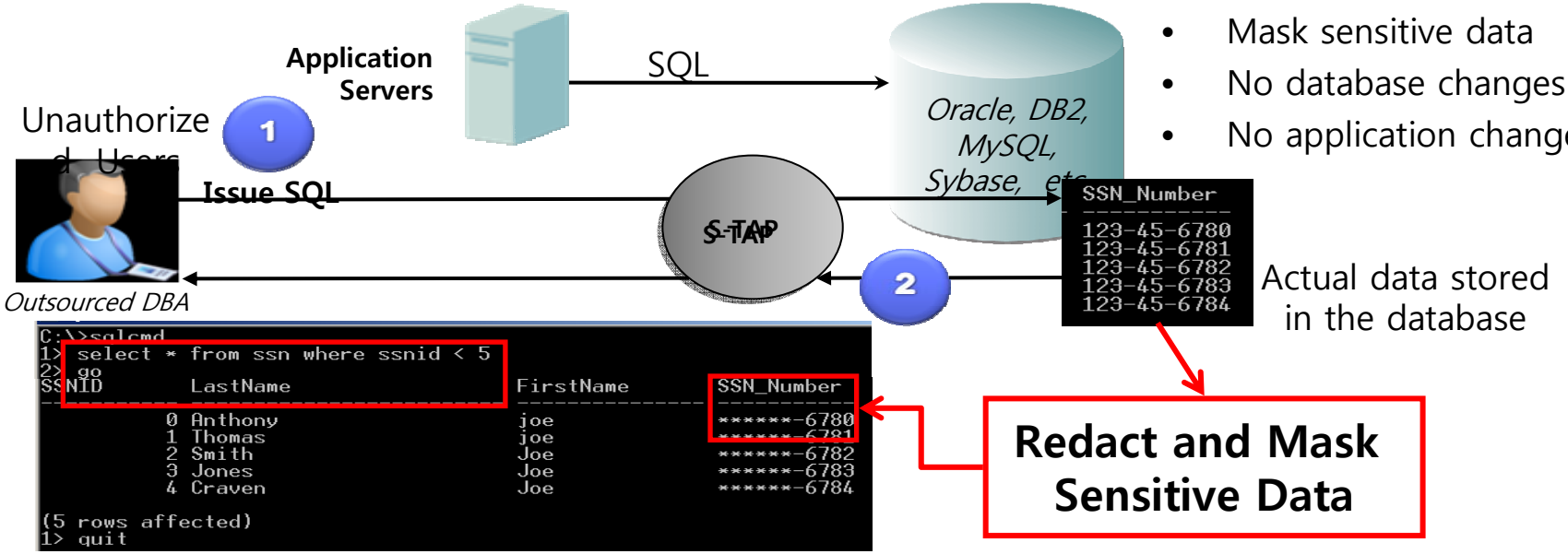
DB레벨 데이터 암호화 – Infosphere Guardium Encryption Expert

- 오프라인 데이터(데이타베이스 백업)
  - 암호화에 의한 데이터의 보호
  - 스토리지·스페이스를 절약하기 위한 데이타베이스·백업 압축
  - 복구 관리
- 온라인 데이터(데이타베이스에 보존되고 있는 데이터)
  - 암호화에 의한 데이터의 보호
  - 액세스 제어 (root 유저등도 제어 가능)
- Database 와 다른 별도의 시스템에 Security 정보 및 관리 정보 보관(보안,서버)
  - Policy/Key Management
  - 로그
- Failover



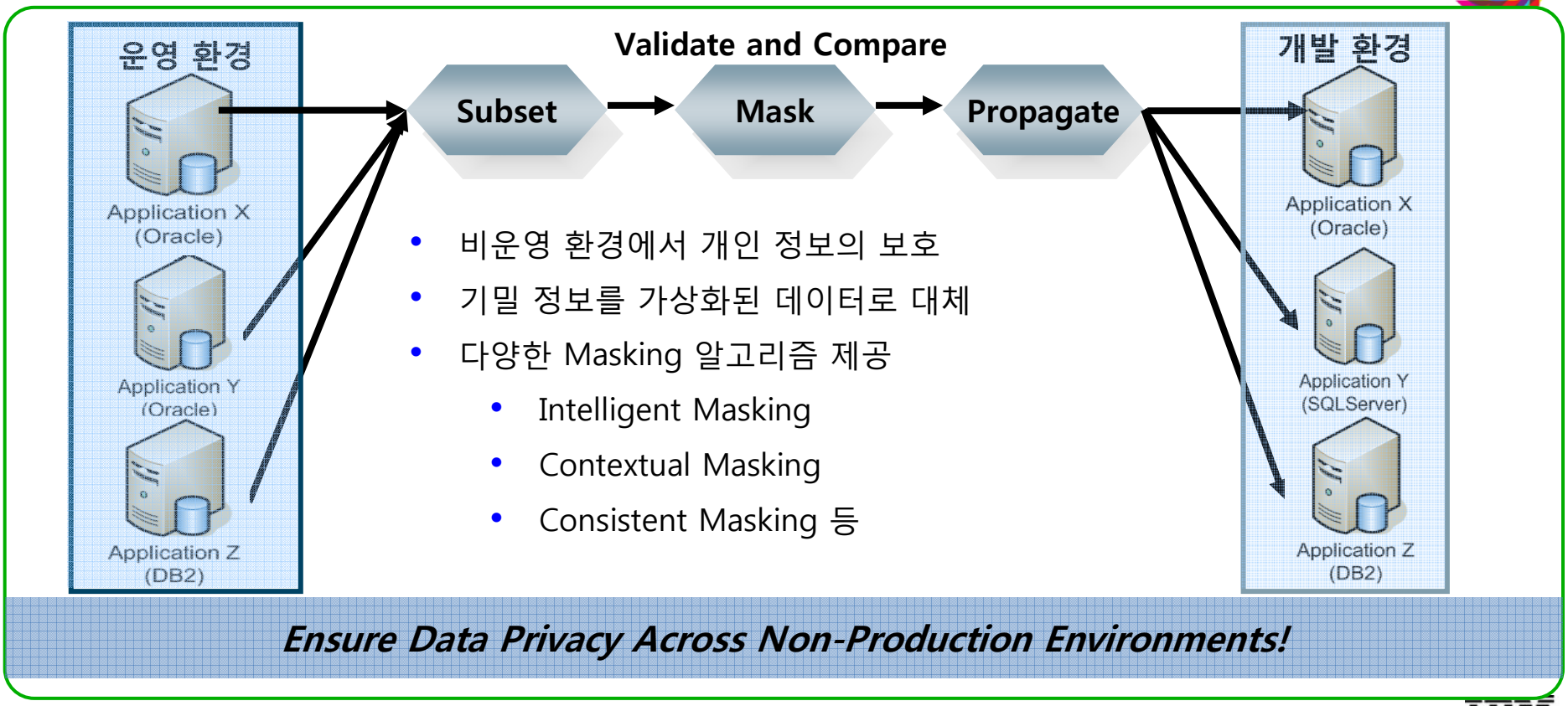
정형 데이터 마스킹 – Infosphere Guardium DAM Redaction

- 데이터베이스 내 민감한 데이터에 대해 권한 없는 사용자에게 암호화된 데이터 조회를 통해 민감한 개인 정보 보호



- Cross-DBMS policies
- Mask sensitive data
- No database changes
- No application changes

비운영 환경 내 데이터 마스킹- Infosphere Optim Data Privacy



문서 데이터 마스킹 – Infosphere Guardium Data Redaction

- 비정형 문서, 양식, 이미지 자료 중 민감한 자료 보호
  - 문서로부터 민감한 데이터 및 메타 검색/제거
  - 다양한 파일 타입 지원: PDF, TIFF, MS-Word, Txt, XML
- 컴플라이언스 비용 절감
- 사용자에 따른 무의식적인 데이터 유출 방지

Finresearch LLC
934 Fifth Ave
New York, NY 00124

September 19, 2008

James McDonald CEO
Financial National Bank
111 Massachusetts Ave
Boston MA 02140

Re: Preliminary Anti-Trust Pre-Acquisition Investigation

Finresearch LLC has conducted research of the market and legal situation in preparation for an acquisition of Northern Investments Inc. by Financial National Bank Inc., scheduled for Jan. 21, 2009. The assignment was to determine the risk of civil and/or criminal action from the Attorney General of the United States under Section 15 of the Lombard Act, 15 U.S.C. § 19 to enjoin the acquisition of Northern Investments. We were asked to assess if such an acquisition would substantially affect competition in the housing

→

[Organization]
[Address]
[Address]

[Date]

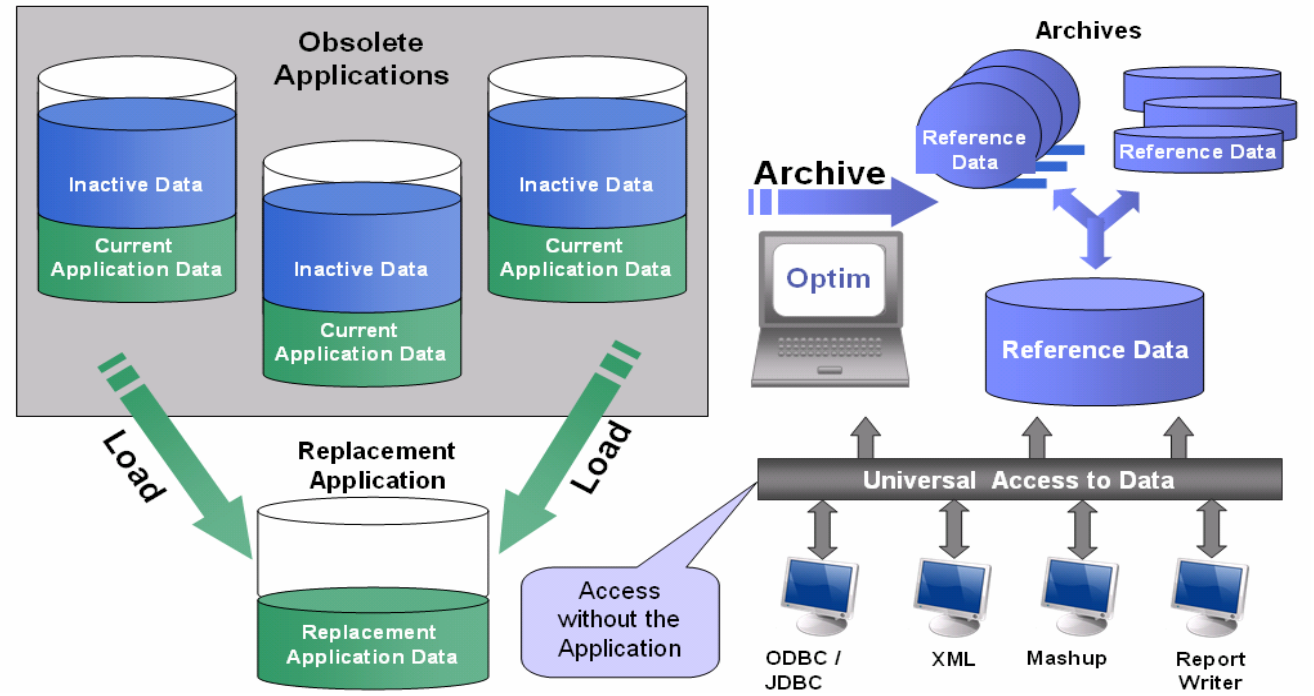
[Person] [Orga...]
[Organization]
[Address]
[Address]

Re: [Organization] Pre-Acquisition Investigation

[Organization] has conducted research of the market and legal situation in preparation for an acquisition of [Organization] [O...] by [Organization], scheduled for [Date]. The assignment was to determine the risk of civil and/or criminal action from the Attorney General of the [Location] under Section 15 of the Lombard Act, 15 [Sec.]C. § 19 to enjoin the acquisition of Northern Investments. We were asked to assess if such an acquisition would substantially affect competition in the housing

비활성 데이터 폐기/분리 – Infosphere Optim Decommissioning

- 실시간 조회 및 활용이 거의 없는 DB 및 관련 데이터에 대한 안전한 폐기 및 다양한 조회 환경 제공



Agenda

- 데이터 보안 현황
- 개인정보보호법과 데이터 보안
- IBM의 데이터 보안 영역별 솔루션
- 전방위 데이터 보안 솔루션 Guardium
- 사례 및 결론

IBM

실시간 DB 모니터링 솔루션 Infosphere Guardium

•실시간 데이터베이스 활동 모니터링 통하여 기업정보의 보호 강화 및 가치향상을 위해 광범위하게 사용되는 솔루션

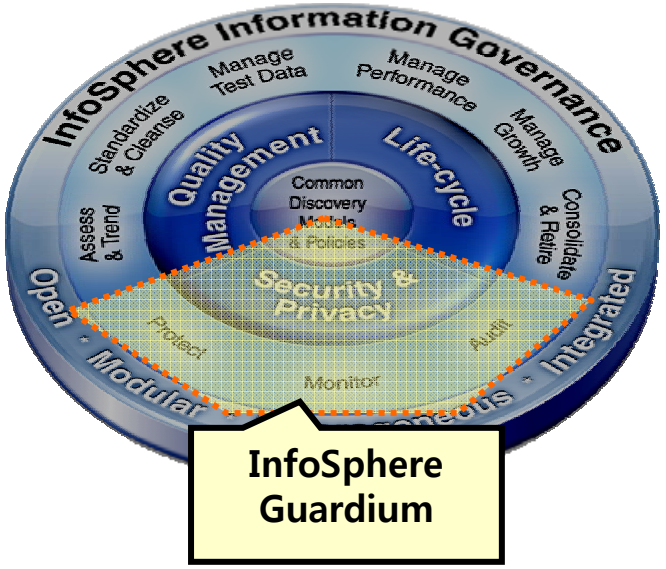
•Database Activity Monitoring (DAM) 및 높은 가치의 데이터베이스를 보호하는 Market leader 제품

•포괄적인 컴플라이언스 자동화 시스템

• 확장성이 뛰어난 아키텍처 로 다양한 이기종 환경 지원

•데이터 접근 및 모니터링-제어를 위한 특허 받은 업계를 선도하는 Software Agent 솔루션

IBM's Information Governance portfolio 의 핵심 제품
이기종 환경을 위한 지속적인 지원



InfoSphere Guardium 8:
데이터 보안 Lifecycle을 위한 전 영역 지원

InfoSphere Guardium을 통한 데이터 보안 지원

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
Auditing and compliance solutions **감사 및 compliance 솔루션**	자동화 및 검증활동 단순화 PCI-DSS , SOX, SAS70,ISO 27001/2 ,NIST 800-53 , data privacy 관련
Change control solutions **변경 제어솔루션**	데이터베이스 구조,권한 및 환경구성파일의 무단변경 방지
Vulnerability management **취약성관리**	누락된 패치, 잘못 구성된 권한 및 기본 계정과 같은 데이터베이스 취약점 식별 및 관련 리포트 제공
Fraud prevention solutions **사기방지솔루션**	애플리케이션 계층의 승인되지 않는 응용프로그램 사용자 활동을 식별하는 모니터링 (SAP, PeopleSoft , Oracle EBS, Cognos Etc)
Database leak prevention **데이터베이스 유출방지**	민감한 데이터를 찾고, 데이터 센터 침해요인을 제거 (주민번호, 신용카드번호 등)

실시간 데이터베이스 활동 모니터링

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

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, SOX, BASEL II, EUDPD

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**

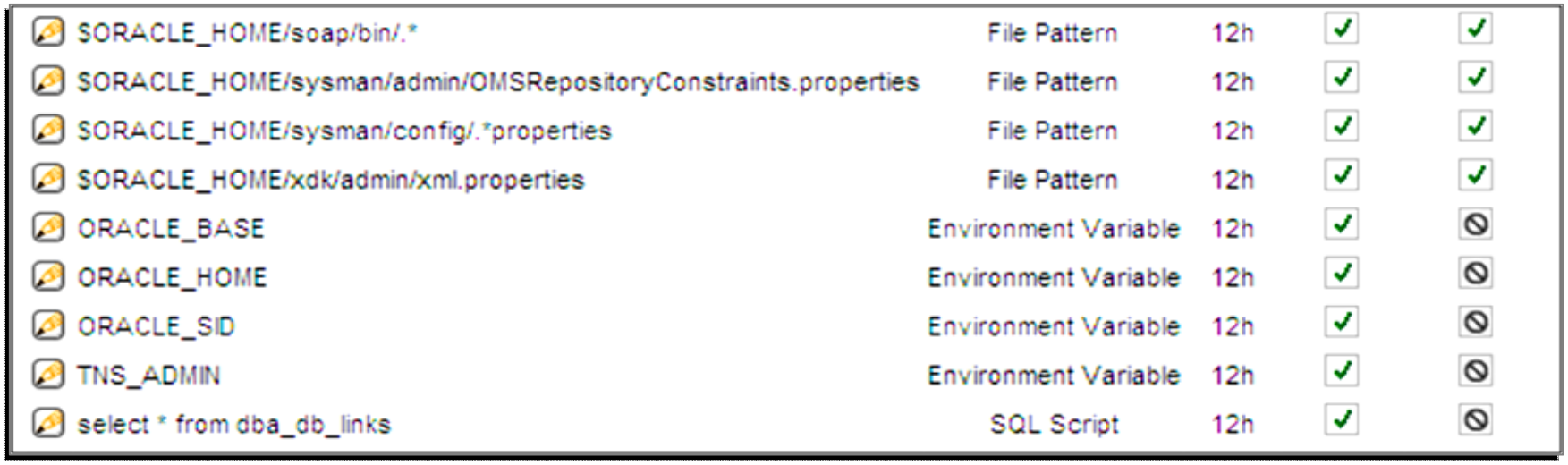
2	Do not use vendor defaults for system passwords	Comprehensive suite of DBMS-specific tests based on industry standards (CIS, STIG)
	• Configure system parameters to prevent misuse	• Checks for default passwords, unpatched systems, misconfigured privileges, etc.
	• Encrypt non-console admin access	• Audits usage and alerts on misuse
		• Locks configurations after vulnerabilities remediated
		• Monitors encrypted traffic (Oracle ASO, SSL, etc.) without need for key storage
3	Protect stored cardholder data	Real-time, database leak prevention
		• Continuous, real-time, policy-based monitoring with proactive security (alerts, blocking)
		• Compensating control for column-level encryption
		• Auto-discovers & classifies stored data; identifies sensitive data in query result stream
6	Maintain secure systems	Centralized vulnerability and configuration assessment
	• Establish a process to identify security vulnerabilities	• Ensures current patches applied & vulnerable SPs identified; "virtual patching"
	• Follow change control procedures for all configuration changes	• Alerts on all configuration changes, inside and outside databases
	• Separation of duties (development, test and production)	• Enforces separation of duties with real-time alerting and granular access controls
7	Restrict access to cardholder data	Proactive, real-time access control (independent of native DBMS controls)
		• Policies defined by source IP or application, OS or DB user, time, SQL command, object, etc.
		• Blocks any unauthorized user, including administrators, from accessing cardholder data
		• Compensating control for unsegmented networks
8	Assign a unique ID to each person with computer access	Complements native DBMS controls with external, cross-DBMS controls
	• Enforce password policies	• Alerts on credential sharing, failed logins, account creation, privilege escalation
	• Limit repeated access attempts	• Verifies password policies are enforced; can lock accounts or terminate sessions
10	Track and monitor access to cardholder data	Continuous, granular auditing with scalable architecture to handle high transaction volumes
		• Fine-grained audit trail of all database activities (SELECT, DDL, DML, DCL, logins, logouts, etc.)
		• Does not rely on native trace or audit logs: minimal perf. impact (2-3%), enforces sep. of duties
		• Tracks all network and local connections, including direct access by DBAs (shared memory, etc.)
		• Audit information stored securely in hardened appliance to prevent anti-forensics or tampering
		• Identifies fraud by resolving end-user IDs in connection-pooling apps (SAP, Cognos, PeopleSoft, etc
		• Integrates with LDAP, IAM, TCIM, TSM, SIEM, change management, CMDBs, etc.
		• Compliance workflow automation (electronic sign-offs, escalations) demonstrates oversight process
		• PCI Accelerator provides pre-configured reports based on best practices
11	Regularly test security systems and processes	Integrated vulnerability scanning, file integrity monitoring & behavioral vulnerability testing
	• Run internal and external vulnerability scans	• Includes hundreds of pre-configured vulnerability tests for all major DBMS/OS combinations
	• Deploy integrity monitoring to detect modif. of critical sys. files	• Tracks changes to DB configuration files, environ./registry variables, executables and OS files
12	Maintain an Information Security Policy	Robust automated controls for enforcing information security policies
	• Monitor/analyze alerts and distribute to appropriate personnel	• Real-time alerts, correlation alerts, centralized aggregation of all audit data, SIEM integration
	• Monitor and control all access to data	• Automated sign-offs demonstrate formal oversight process
		• 100% visibility & control over all database transactions (with blocking)

<PCI-DSS sample>

데이타베이스 구성변경 감사기능

Change control solutions
변경 제어솔루션

데이터베이스 구조,권한 및 환경구성파일의 무단변경 방지

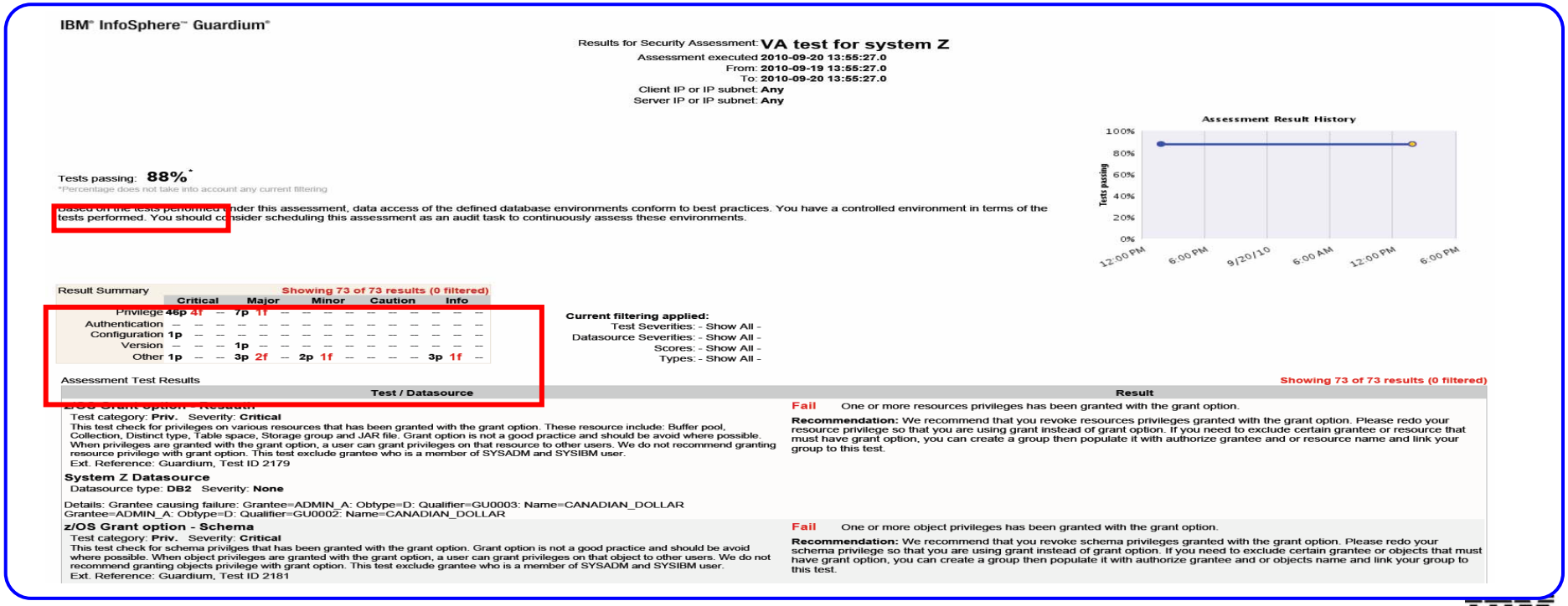


- 보안에 영향을 미칠 수 있는 파일, 환경변수 , 레지스트리 설정, 스크립트 등 변경사항들을 추적
- 500 + 이상의 모든 주요 운영체제/ DBMS 구성을 위한 사전구성, 사용자 지정 템플릿을 제공

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 등 전반적인 DB 시스템의 취약성 평가서 제공



IBM® InfoSphere™ Guardium®

Results for Security Assessment: **VA test for system Z**
Assessment executed **2010-09-20 13:55:27.0**
From: **2010-09-19 13:55:27.0**
To: **2010-09-20 13:55:27.0**
Client IP or IP subnet: **Any**
Server IP or IP subnet: **Any**

Assessment Result History

Tests passing: **88%***
*Percentage does not take into account any current filtering

Based on the tests performed under this assessment, data access of the defined database environments conform to best practices. You have a controlled environment in terms of the tests performed. You should consider scheduling this assessment as an audit task to continuously assess these environments.

Result Summary — Showing 73 of 73 results (0 filtered)

	Critical			Major			Minor			Caution			Info		
Privilege	46p	4f	–	7p	1f	–	–	–	–	–	–	–	–	–	–
Authentication	–	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Configuration	1p	–	–	–	–	–	–	–	–	–	–	–	–	–	–
Version	–	–	–	1p	–	–	–	–	–	–	–	–	–	–	–
Other	1p	–	–	3p	2f	–	2p	1f	–	–	–	–	3p	1f	–

Current filtering applied:
Test Severities: - Show All -
Datasource Severities: - Show All -
Scores: - Show All -
Types: - Show All -

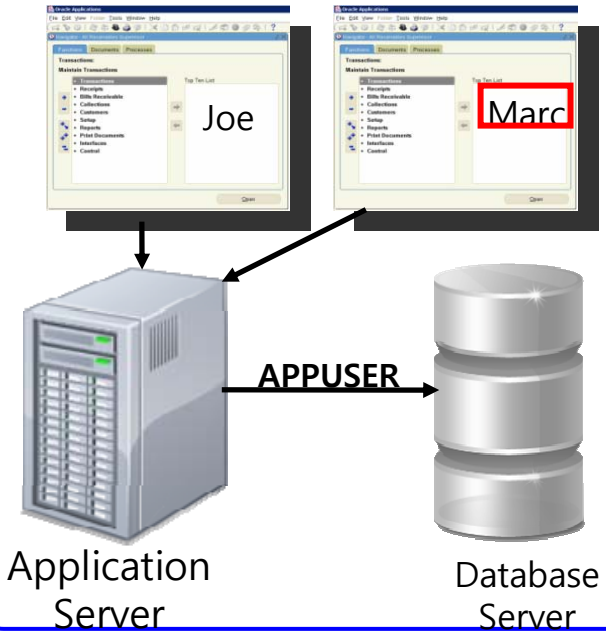
Assessment Test Results — Showing 73 of 73 results (0 filtered)

Test / Datasource	Result
Test category: **Priv.** Severity: **Critical** This test check for privileges on various resources that has been granted with the grant option. These resource include: Buffer pool, Collection, Distinct type, Table space, Storage group and JAR file. Grant option is not a good practice and should be avoid where possible. When privileges are granted with the grant option, a user can grant privileges on that resource to other users. We do not recommend granting resource privilege with grant option. This test exclude grantee who is a member of SYSADM and SYSIBM user. Ext. Reference: Guardium, Test ID 2179 **System Z Datasource** Datasource type: **DB2** Severity: **None** Details: Grantee causing failure: Grantee=ADMIN_A: Obtype=D: Qualifier=GU0003: Name=CANADIAN_DOLLAR Grantee=ADMIN_A: Obtype=D: Qualifier=GU0002: Name=CANADIAN_DOLLAR	Fail One or more resources privileges has been granted with the grant option. **Recommendation:** We recommend that you revoke resources privileges granted with the grant option. Please redo your resource privilege so that you are using grant instead of grant option. If you need to exclude certain grantee or resource that must have grant option, you can create a group then populate it with authorize grantee and or resource name and link your group to this test.
z/OS Grant option - Schema Test category: **Priv.** Severity: **Critical** This test check for schema privilges that has been granted with the grant option. Grant option is not a good practice and should be avoid where possible. When object privileges are granted with the grant option, a user can grant privileges on that object to other users. We do not recommend granting objects privilege with grant option. This test exclude grantee who is a member of SYSADM and SYSIBM user. Ext. Reference: Guardium, Test ID 2181	Fail One or more object privileges has been granted with the grant option. **Recommendation:** We recommend that you revoke schema privileges granted with the grant option. Please redo your schema privilege so that you are using grant instead of grant option. If you need to exclude certain grantee or objects that must have grant option, you can create a group then populate it with authorize grantee and or objects name and link your group to this test.

사기방지솔루션-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

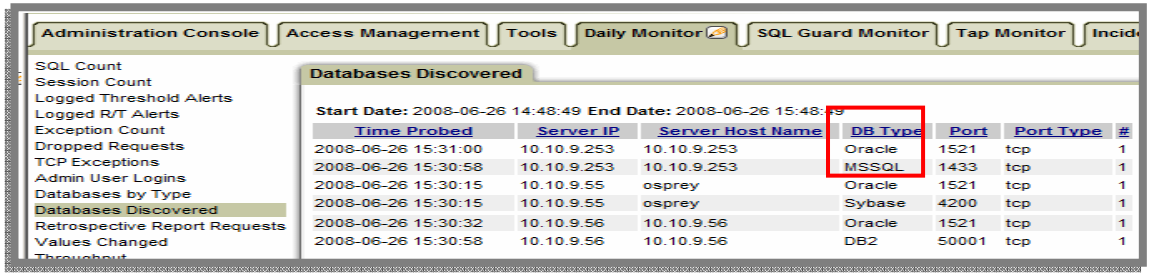
✓ BUT **누가** 트랜잭션을 시작했는지 알 수 없음(connection pooling)

- 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

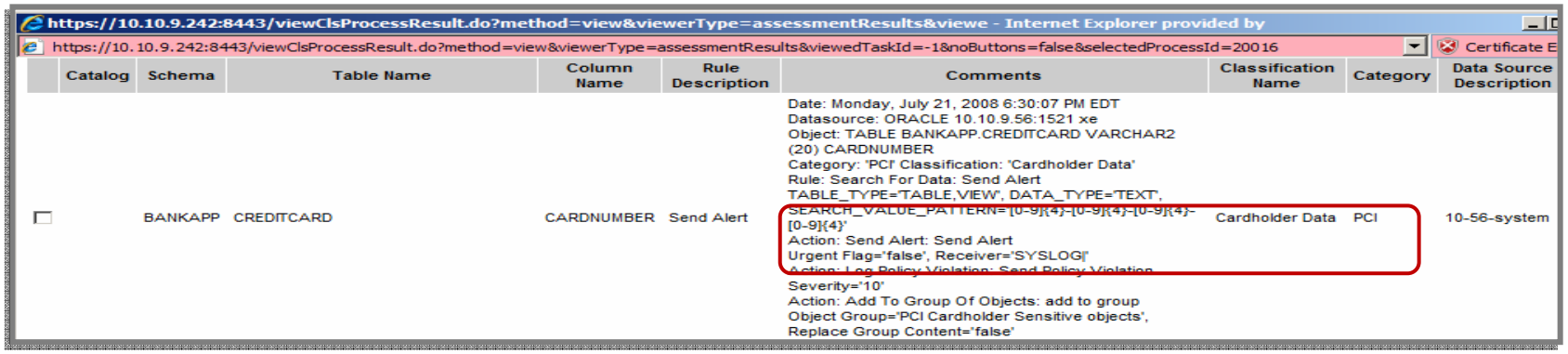
데이터베이스 유출방지

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
  - ✓ Sensitive Objects 의 group 으로 추가



데이터베이스 유출방지 (계속)

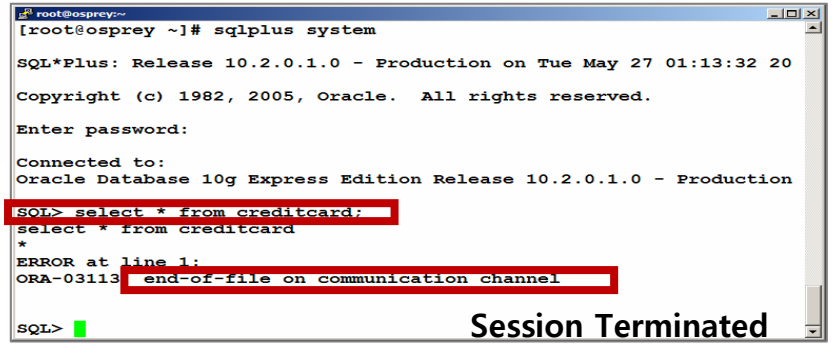
- 비정상적인 트랜잭션 감지
- 정책에 위반하는 트랜잭션의 접근 제어

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

Is this normal?

What did he see?

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

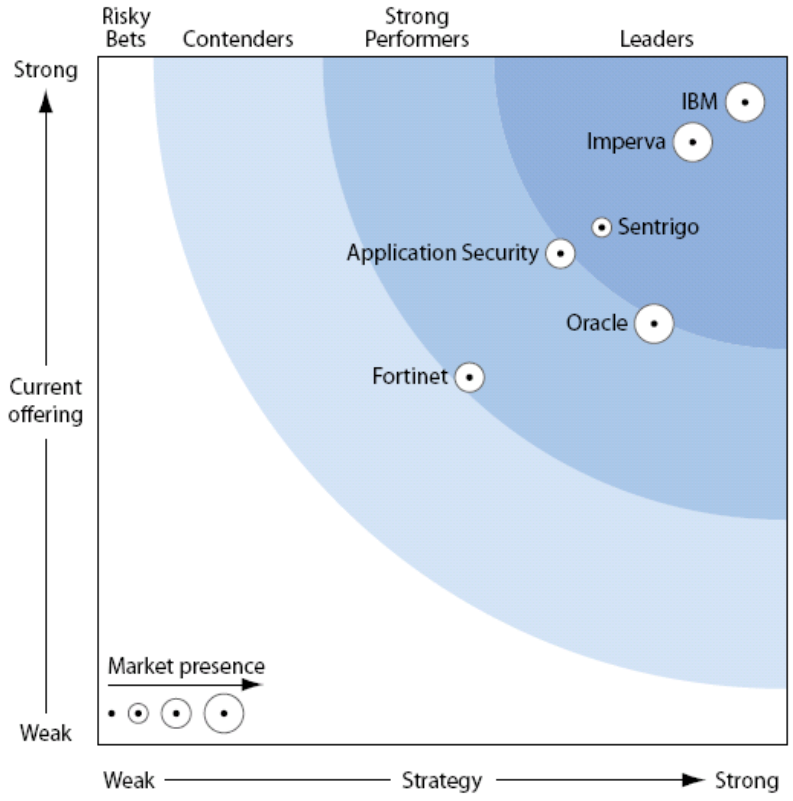


Agenda

- 데이터 보안 현황
- 개인정보보호법과 데이터 보안
- IBM의 데이터 보안 영역별 솔루션
- 전방위 데이터 보안 솔루션 Guardium
- 사례 및 결론

IBM

데이터 보안 시장을 선도하는 마켓 리더 IBM Infosphere Guardium



Source: Forrester Wave™: Database Auditing And Real-Time Protection, Q2 '11

FORRESTER®

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

SC MAGAZINE

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

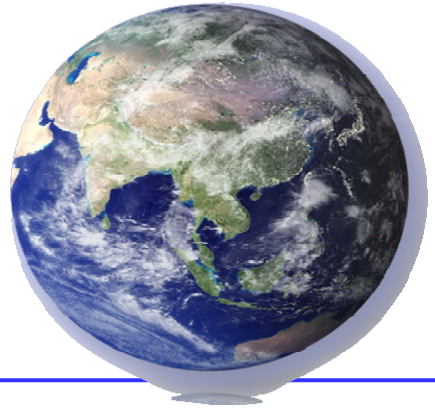
INFORMATION SECURITY MAGAZINE

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

IBM

Chosen by Leading Organizations Worldwide

- 5 of the top 5 global banks
- 4 of the top 6 global insurers
- 2 of the top 3 global retailers
- 2 of the world's favorite beverage brands
- The most recognized name in PCs
- 25 of the world's leading telcos



- Top government agencies
- Top 3 auto maker
- #1 dedicated security company
- Leading energy suppliers
- Major health care providers
- Media & entertainment brands

The Choice of Market Leaders

데이터 보안 진단 서비스

ROI 진단 워크샵 BVA

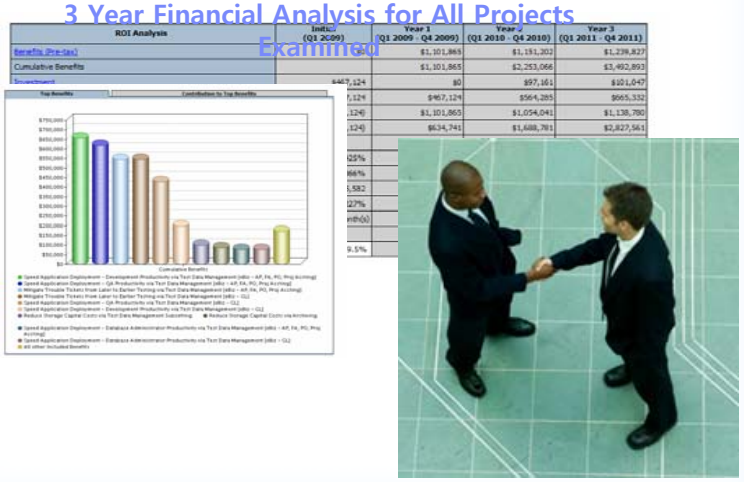
- 데이터 보안을 통해 얻어지는 비용 절감과 추가적인 매출 창출에 대한 비즈니스 이윤을 정량화할 수 있도록 분석하는 워크샵
- 전략적인 파트너쉽 고객을 위해 무료로 제공되는 프로그램

진행결과

- Alinean ROI Analyst 분석툴 사용
- 2008년 WW 80개 이상의 워크샵을 수행하여 100만 달러 이상의 비용 절감 결과를 도출

보안 진단 워크샵

- 고객사의 데이터 보안 현황을 살펴보고, 민감한 개인 정보 및 정책에 대한 이해도를 증대시키고, 데이터 보안 전략/프로젝트를 정의하여 적용할 수 있도록 지원하는 워크샵



Prison? The Guardium Redemption!

- 개인정보보호법 위반 시 수사 기관에 고발 및 징계 요청
- 개인정보보호법 위반 시 최고 5년 이하의 징역 및 5천만원 이하의 벌금
- 양벌규정: 종업원 개인의 범죄라도
  해당 기업의 대표자나 법인은 최고 7천만원까지 벌금 부과
- 개인정보보호법 위반하여 개인정보 수집 및 관리 시
  과태료는 최고 5천만원

IBM

Thank you


Smarter software for a smarter planet
smarter planet
smarter software
IBM
smarter