정보 유출 방지를 위한 IBM Information Governance 방안

Information Governance 차원의 전사적 정보 보안

2011/05/18
구자일, Industry Solution, IBM Korea

IBM Security Summit
IBM Security Solutions. Secure By Design.

Agenda

- Information Governance
- Enterprise Information Management Blueprint
- IBM Security Framework
- Structured Data – Guardium
- Unstructured Data – FileNet , Content Collector, eDiscovery

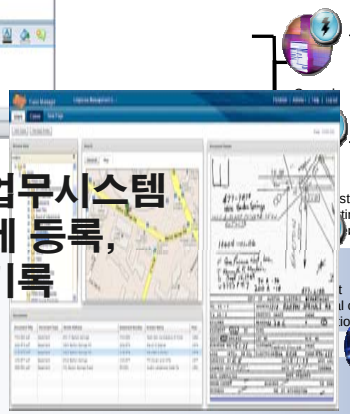
우리는 다양한 경로 정보를 받고,
만들고,
유통하고 있다.

어디서 만들어졌고,
어디에 남아 있는지..
그리고, 정상적으로 파기 되었는지..
당신은 알고 있는가?

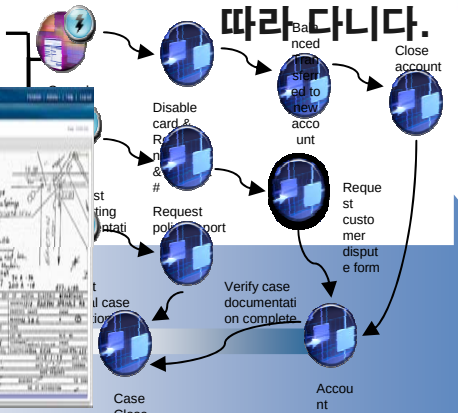
우리는 다양한 경로 정보를 받고, 만들고, 유통하고 있다.

커뮤니케이션 협업 과정에서 배포되고 복사본이 생긴다.

업무시스템에 등록, 기록

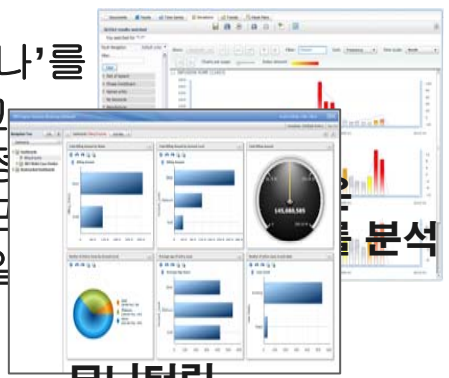


복잡한 프로세스에서 컨텐츠가 따라다니다.



다양한 정보의 흐름을 감사하기 어렵다

일하는 '나'를 둘러싸고 다양한 정 복잡한 프 속에서 일



분석

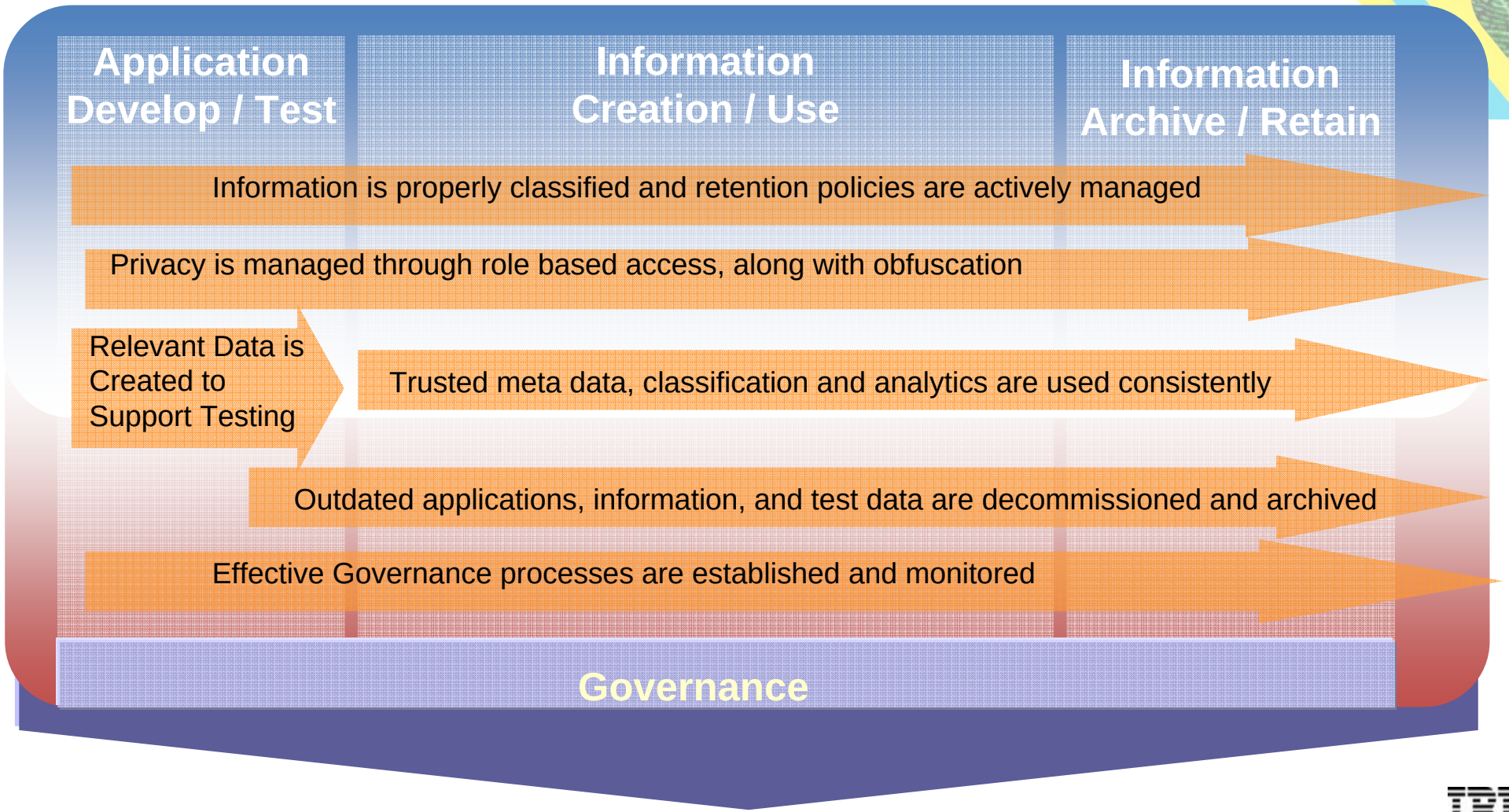
모니터링 통제 관리

감사자

그래서, 단순한 Point 솔루션이 아닌

기업 내 정보 흐름 관점에서 정보 유출 방지를 고려 해볼 필요가 있다.

정보의 유통 관점에서 정보 유출 방지를 고려 해볼 필요가 있다

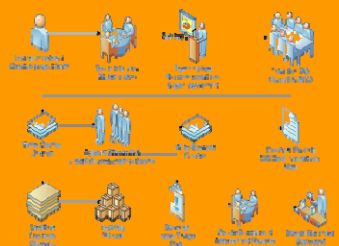


Information Governance는 기업의 모든 정보를 최적화 할 수 있도록 하는 조직적으로 통합된 사람, 프로세스 그리고 기술

INFORMATION GOVERNANCE

People

Process



Technology

Governance Program 핵심 목적

- 정보 관리 의사 결정 가이드
- 일관되게 정의되고 잘 이해가 되는 것을 안전한 정보(Ensure Information)
- 기업의 정보 데이터의 사용률 및 신뢰성 증가
- 정보 보호 및 규제 준수

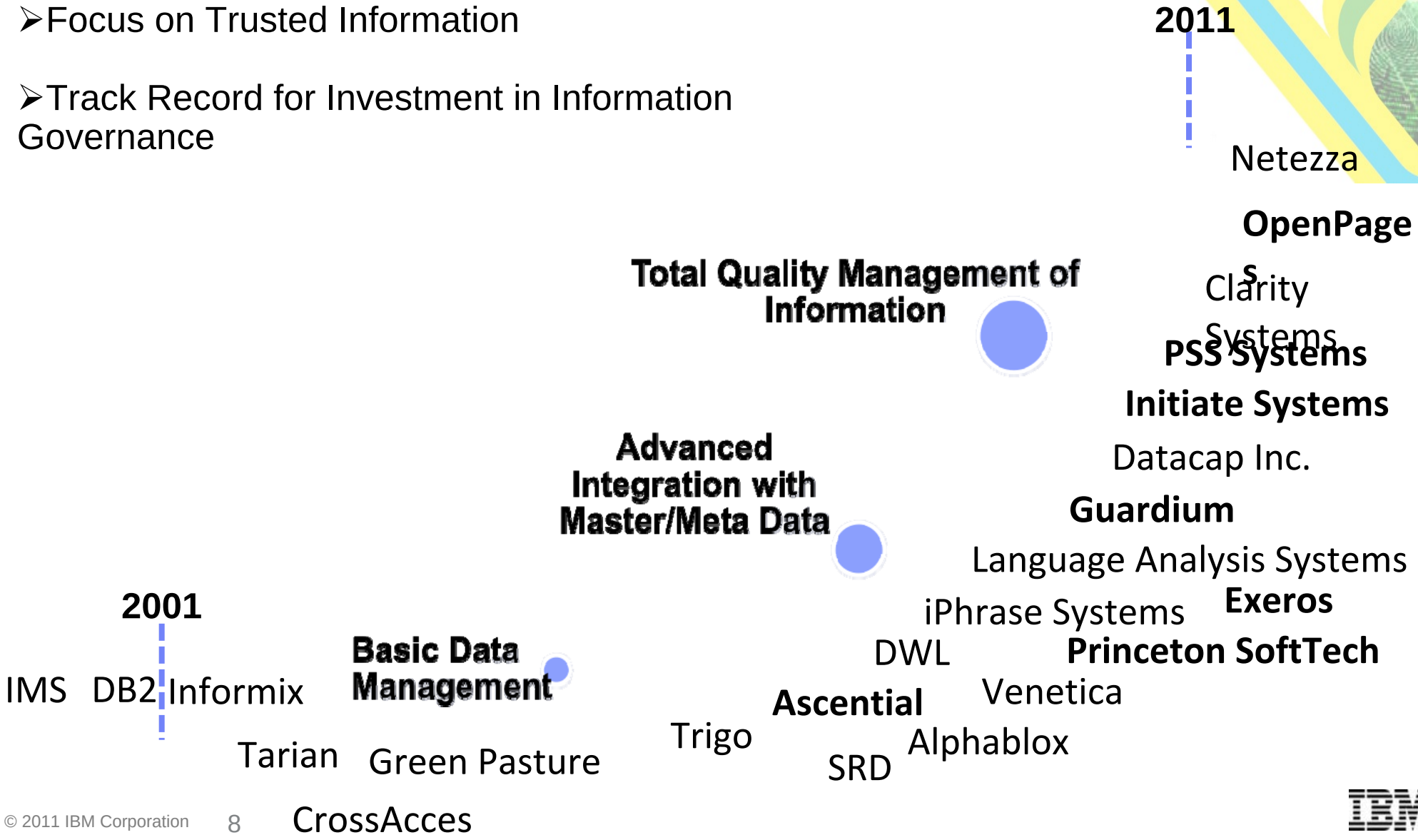
Governing the creation, management and usage of enterprise data is not an option any longer. It is:

Expected by your customers ◆ Demanded by the executives ◆ Enforced by regulators/auditors

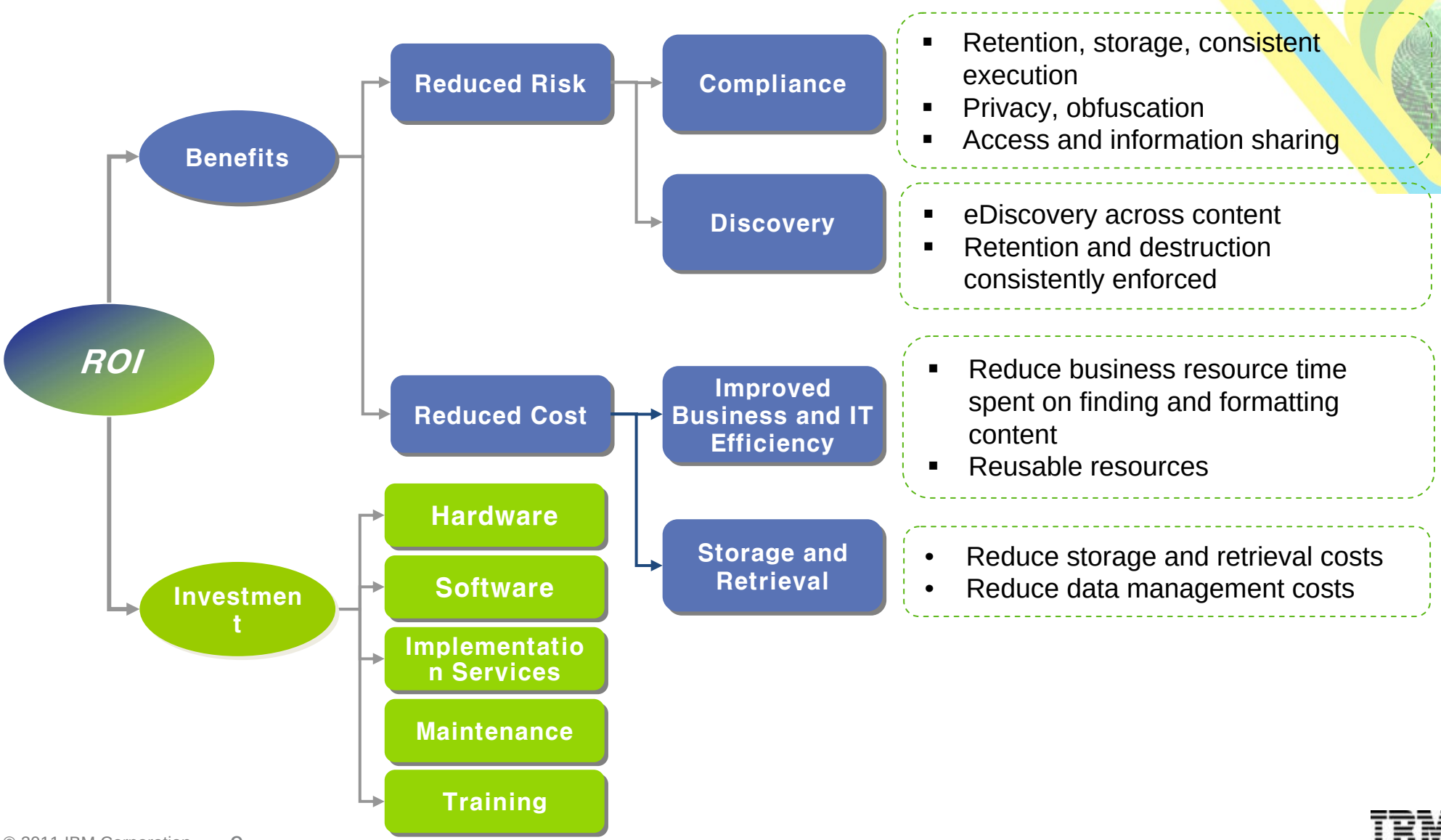
IBM Information Governance Portfolio

"Rapid Improvements in Business Performance"

- Focus on Trusted Information
- Track Record for Investment in Information Governance



Reduce both risk and costs



Enterprise Information Management Blueprint

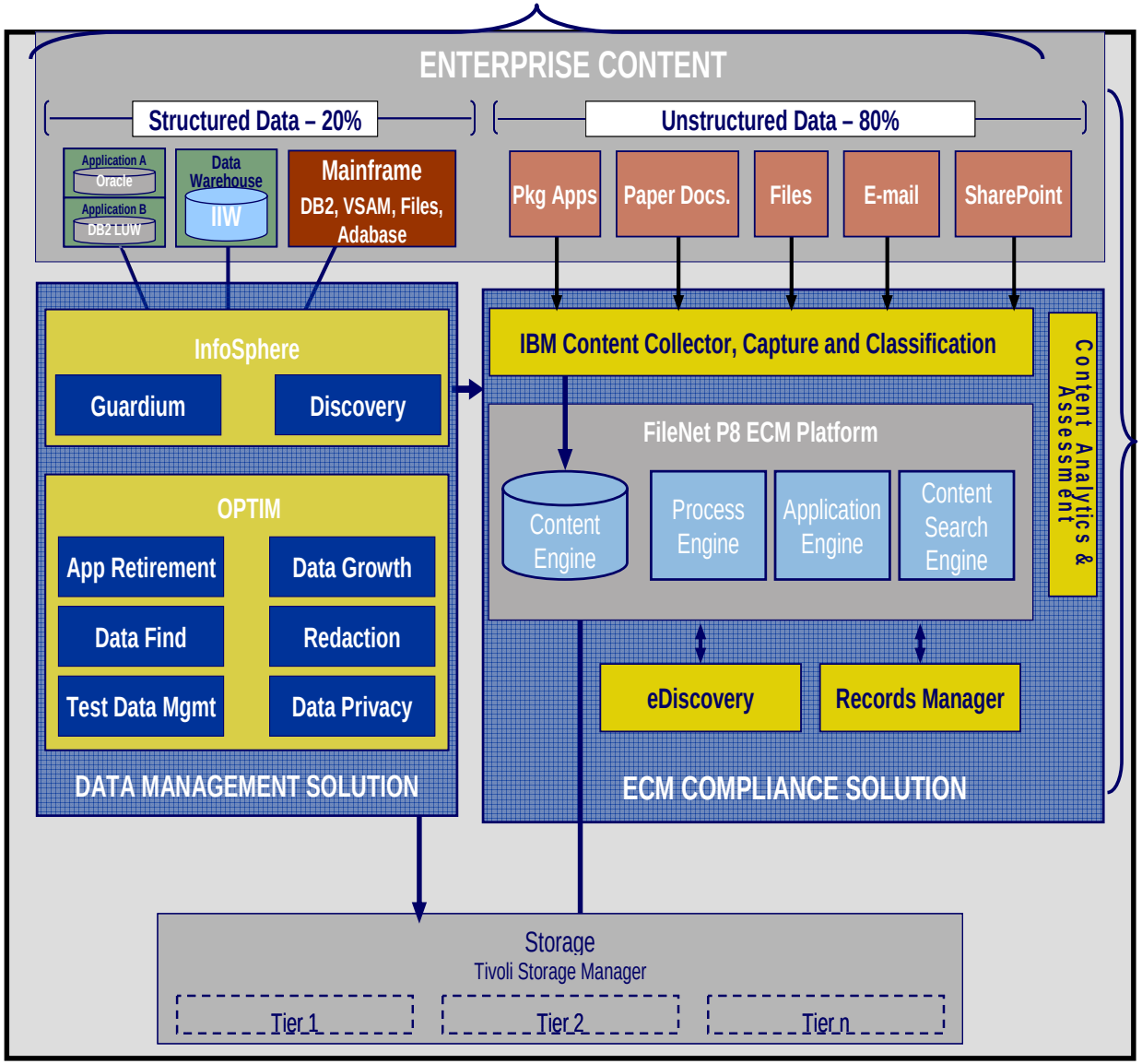
Line of Business Applications

Governance

- Insurance Industry Data Models
- Security
- Discovery
- Data Privacy

Application / Information Retirement

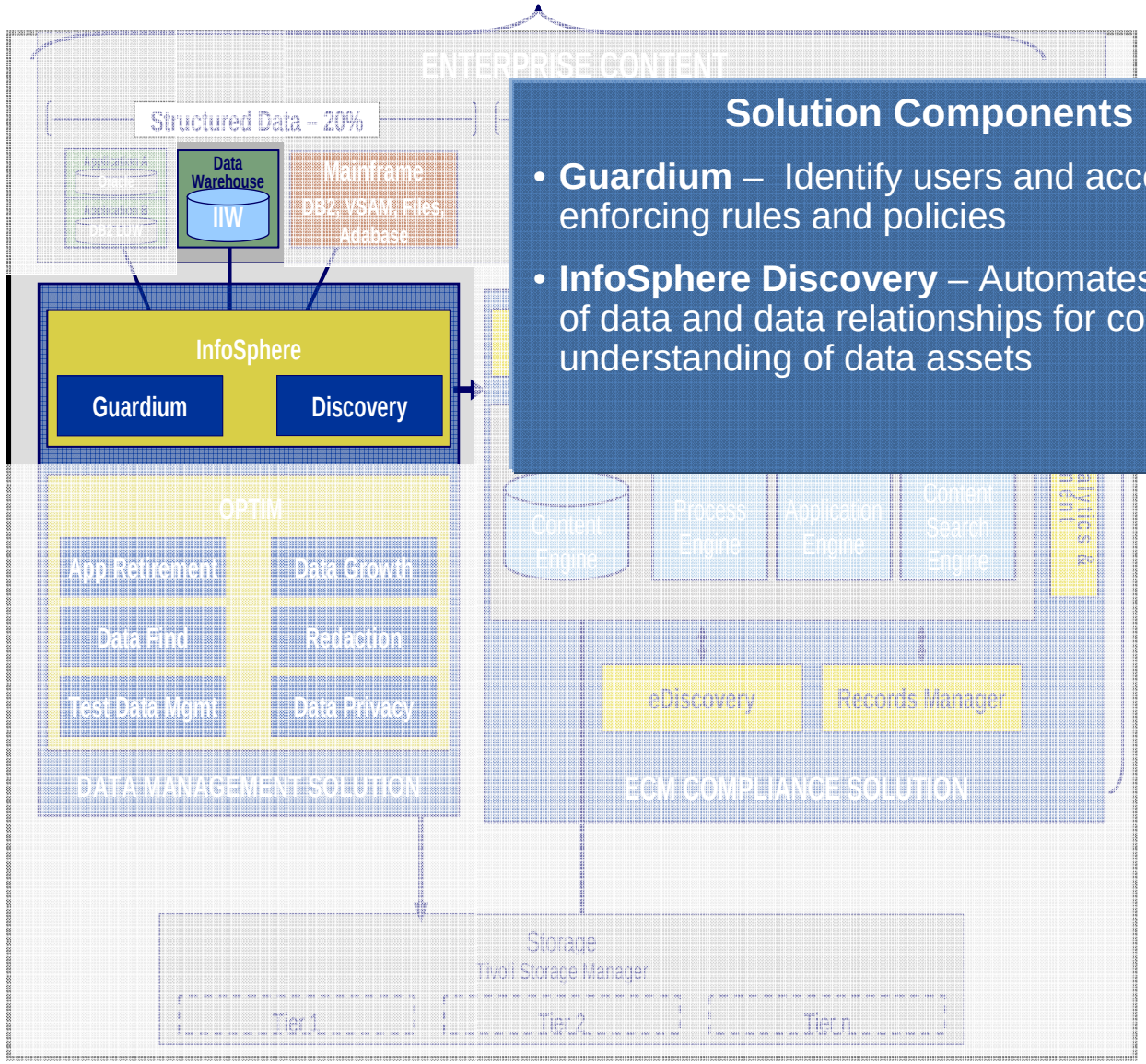
- Decommission Applications and information
- Test Data Management
- Data Growth



Active Information

- Collect and Classify
- Records Management
- Data Privacy
- Security
- eDiscovery

EIM Blueprint solution components

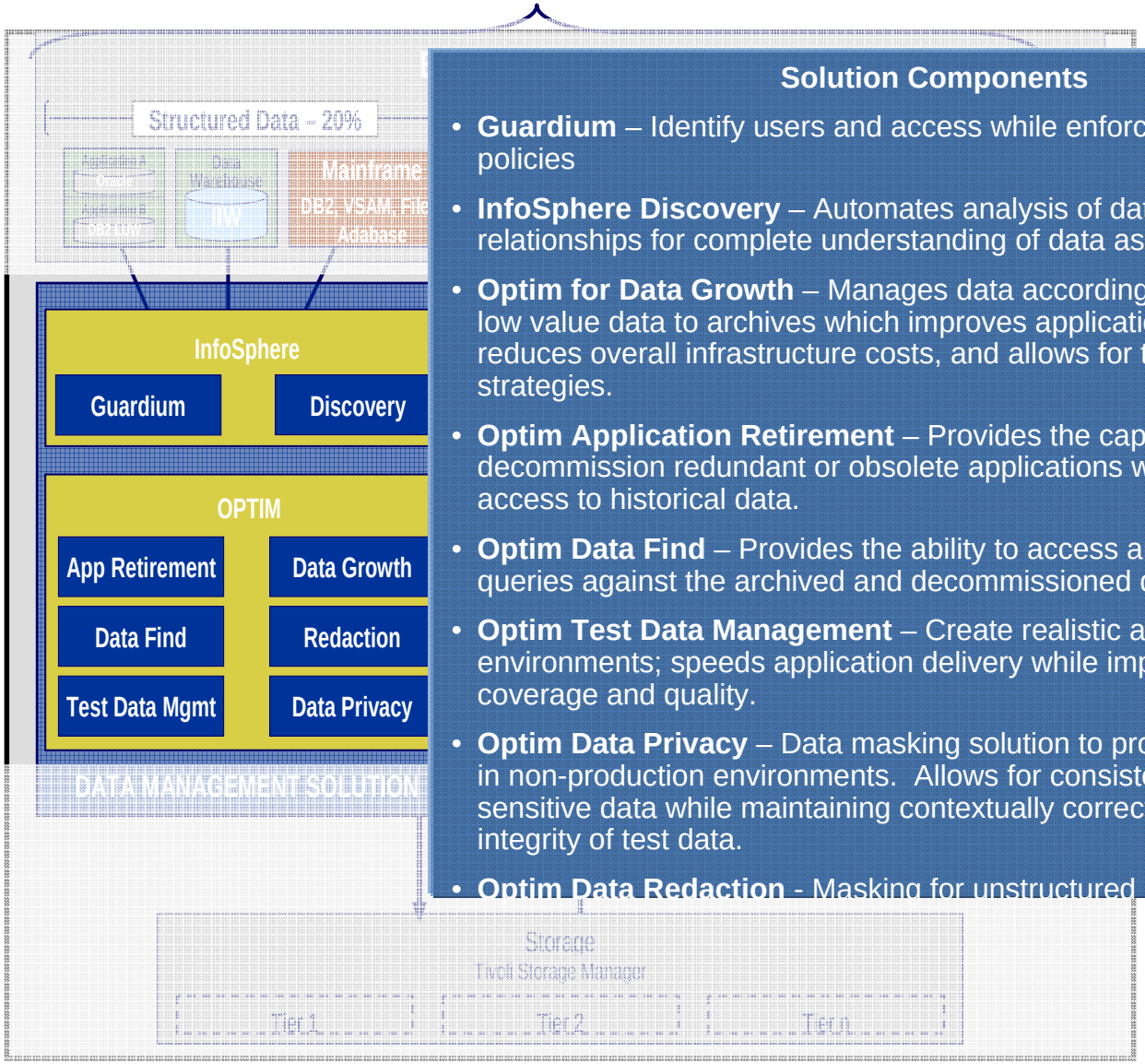


Solution Components

- **Guardium** – Identify users and access while enforcing rules and policies
- **InfoSphere Discovery** – Automates analysis of data and data relationships for complete understanding of data assets

EIM Blueprint solution components

Line of Business Applications



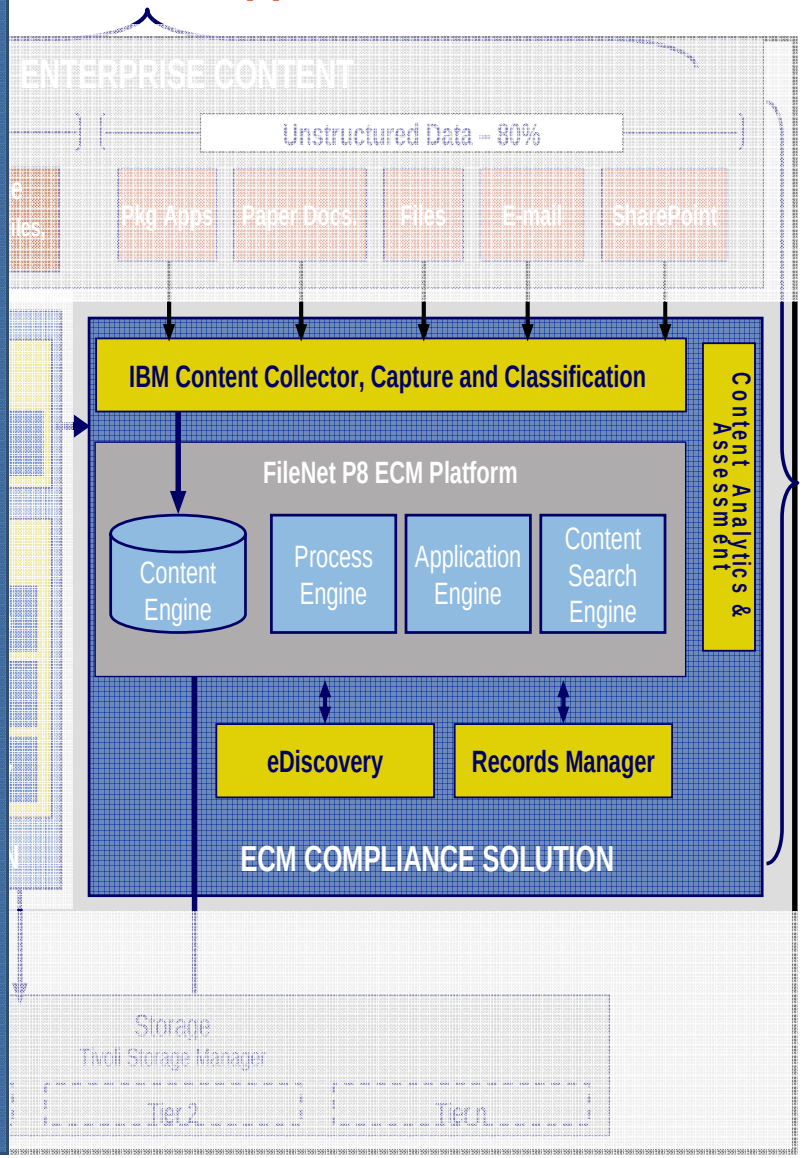
Solution Components

- **Guardium** – Identify users and access while enforcing rules and policies
- **InfoSphere Discovery** – Automates analysis of data and data relationships for complete understanding of data assets
- **Optim for Data Growth** – Manages data according to its value, moving low value data to archives which improves application performance, reduces overall infrastructure costs, and allows for tiered storage strategies.
- **Optim Application Retirement** – Provides the capabilities to decommission redundant or obsolete applications while retaining access to historical data.
- **Optim Data Find** – Provides the ability to access and run advanced queries against the archived and decommissioned data.
- **Optim Test Data Management** – Create realistic and manageable test environments; speeds application delivery while improving test coverage and quality.
- **Optim Data Privacy** – Data masking solution to protect sensitive data in non-production environments. Allows for consistent obfuscation of sensitive data while maintaining contextually correct data to preserve integrity of test data.
- **Optim Data Redaction** - Masking for unstructured documents and data.

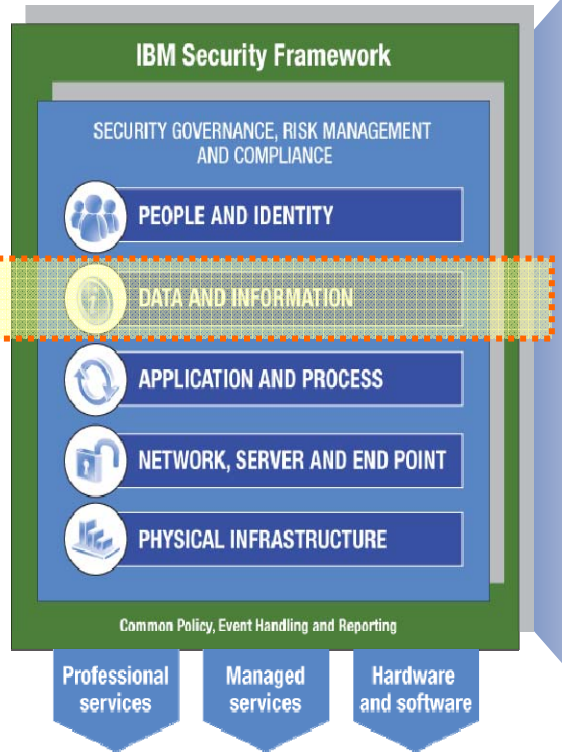
EIM Blueprint solution components

Solution Components

- **Content Collector** – Collects and controls documents on network file shares, SharePoint and email with support for de-duplication capabilities to help further reduce IT infrastructure costs.
- **Classification Module** – Content-based classification with a traditional rule-based classification that analyzes the full text of documents and emails
- **Records Management** - Enables organizations to securely capture, declare, classify, store and dispose of electronic and physical records.
- **eDiscovery** - Enables legal professionals and litigation support specialists to conduct early case assessments, prepare for Meet and Confer discussions, and refine the collection of case-related ESI to help dramatically reduce eDiscovery review costs.



IBM Security Framework



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

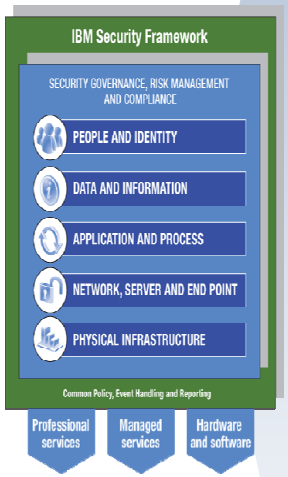
어플리케이션과 프로세스
어플리케이션의 보안성 유지, 악의적 사용과 사기 방지, 실패에 대한 강도 제공

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

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

= 서비스

= 솔루션



GRC

보안 거버넌스와 컴플라이언스

아이덴터티와 접근 관리

통합 계정 관리

통합 권한 관리

데이터 보안

Guardium

컨텐츠(메일,전자문서) 보안

Content Collector / FileNet

어플리케이션 보안

어플리케이션 취약점 스캐닝

웹 어플리케이션 방화벽

어플리케이션 소스코드 취약점 스캐닝

접근과 권한 관리

SOA 보안

위협 평가, 완화와 관리

취약점 평가

메인프레임 보안

Web/URL 필터링

보안 이벤트와 로그

가상 시스템 보안

침입 방지 시스템

보안 정보와 이벤트 관리, 그리고 로그 관리

물리 보안

Structured Data – Guardium

포괄적인 Database 보안솔루션:
InfoSphere Guardium 8

InfoSphere Guardium 8
- Continuous, real-time monitoring of all database activities to:

- 1. 데이터 침해 방지
  - 사이버 범죄자 및 내부 범죄자
  - 고객 데이터 및 기업 기밀 보호
- 2. Data Governance 보장
  - privileged user 의 승인되지 않는 민감한 데이터의 변경 방지

- 3. Compliance 비용 절감
  - 자동화 및 중앙 집중화된 제어를 통해:
    - DBMS platforms (Oracle, DB2, SQL Server, …)
    - Enterprise applications (ERP, CRM, HR, analytics, …)
    - Compliance initiatives (SOX, PCI, data privacy)
    - Business units & distributed data centers
  - 최소 성능 impact
  - 데이터베이스 및 applications 의 변경이 필요 없음

거버넌스, 위험 관리, 컴플라이언스

- 보안 전략 설계
- 모의 해킹 & 취약점 평가
- 보안 컴플라이언스 평가
- 보안 사고 대응

GRC

사람과 아이덴터티

- 아이덴터티 관리
- 어플리케이션 접근 통제
- 자원 접근에 대한 관리, 감사 그리고 보고

데이터와 정보

- 데이터 접근 관리와 모니터링
- 데이터 유출 방지
- 민감한 데이터 암호화
- 핵심 데이터베이스 보호
- 메시징 보안과 컨텐츠 필터링

어플리케이션과 프로세스

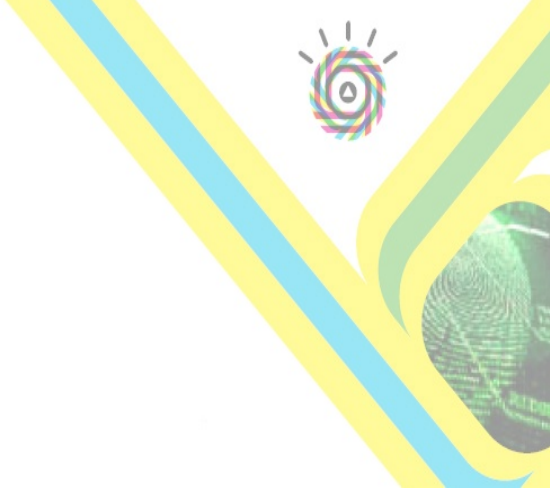
- 어플리케이션 개발 내에 보안 프로세스 보증
- 어플리케이션 취약점 탐색
- 내장된 어플리케이션 접근 통제
- SOA 보안 제공

네트워크, 서버 그리고 단말

- 서버, 단말, 네트워크, 메인프레임 보호

물리적 인프라스트럭처

- 비디오 감시 제공
- 명령 제어 센터 구축
- 수집된 비디오 분석
- 모든 자산을 아우른 보안 관리



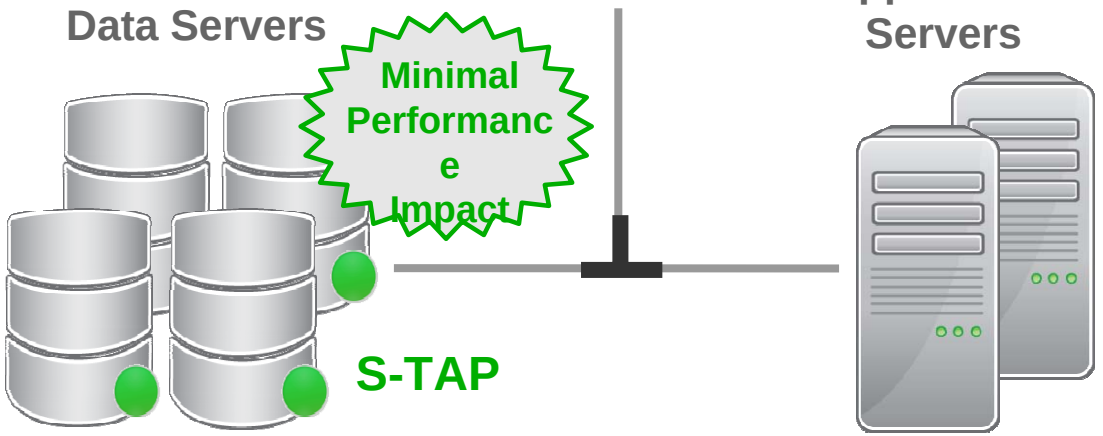
Structured Data – Guardium

포괄적인 Database 보안솔루션:
InfoSphere Guardium 8 Overview

InfoSphere Guardium 8:
다양한 엔터프라이즈 환경을 위한 Solution

Guardium Collector

Support for Popular Databases and Application Systems



- IBM DB2
- Informix
- Microsoft SQL Server
- MySQL
- Oracle Database
- Sybase
- Teradata
- Microsoft SharePoint
- Netezza
- PostgreSQL

- Linux
- Windows
- AIX
- Solaris
- HP-UX
- UNIX

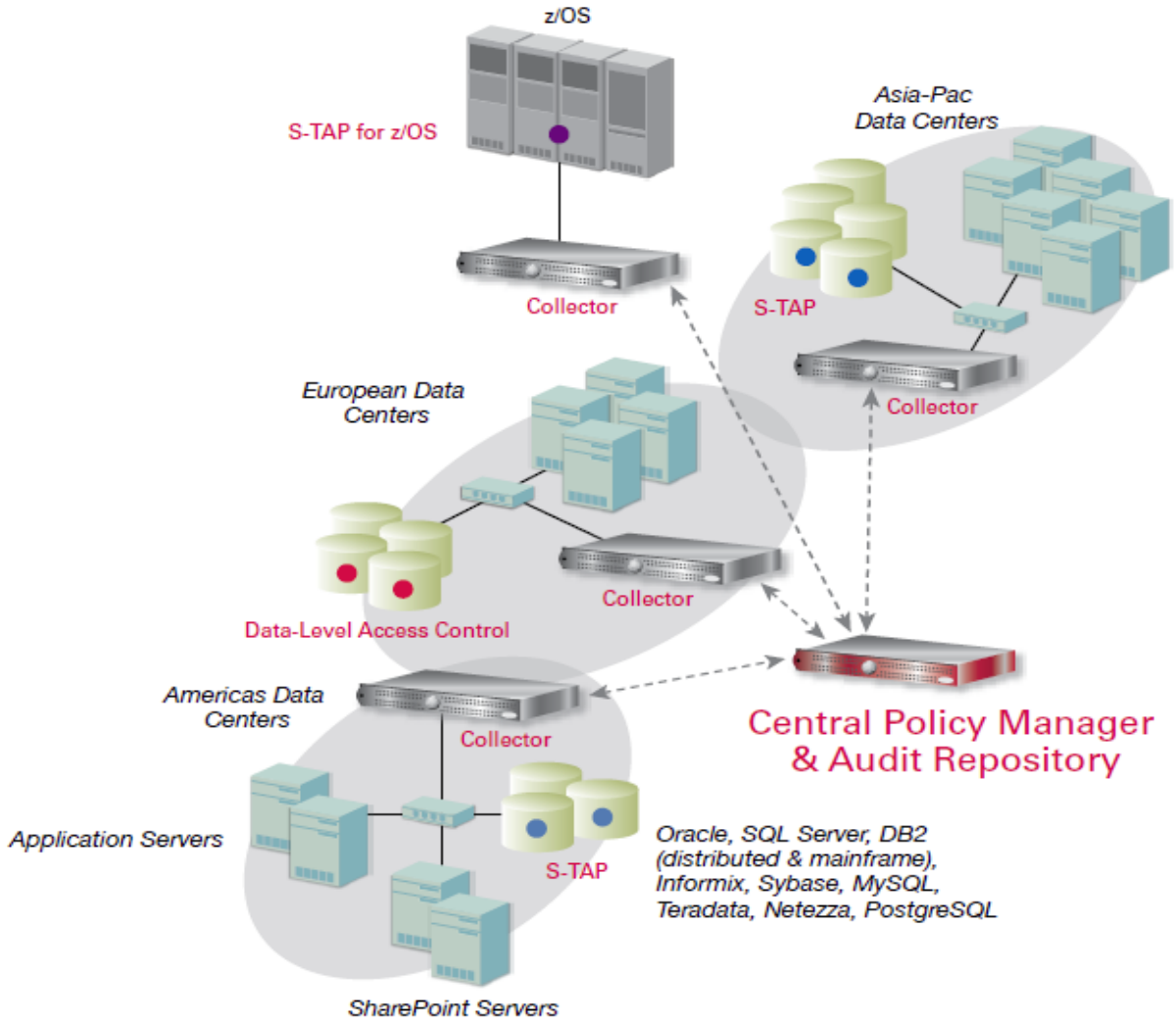
- WebSphere
- Cognos
- Oracle E-Business Suite
- Oracle JD Edwards EnterpriseOne
- Oracle | PeopleSoft
- Oracle | Siebel
- SAP

Collector Non-invasive hardened appliance enforces policies and performs logging

S-TAP Light-weight DBMS-independent software agent monitors database

InfoSphere Guardium 8:
보안 네트워크 확장 및 관리가 유연한 Multi-Tier 구조

- **확장된 분산 환경에서 Multiple S-Tap 과 Collector 사용가능**



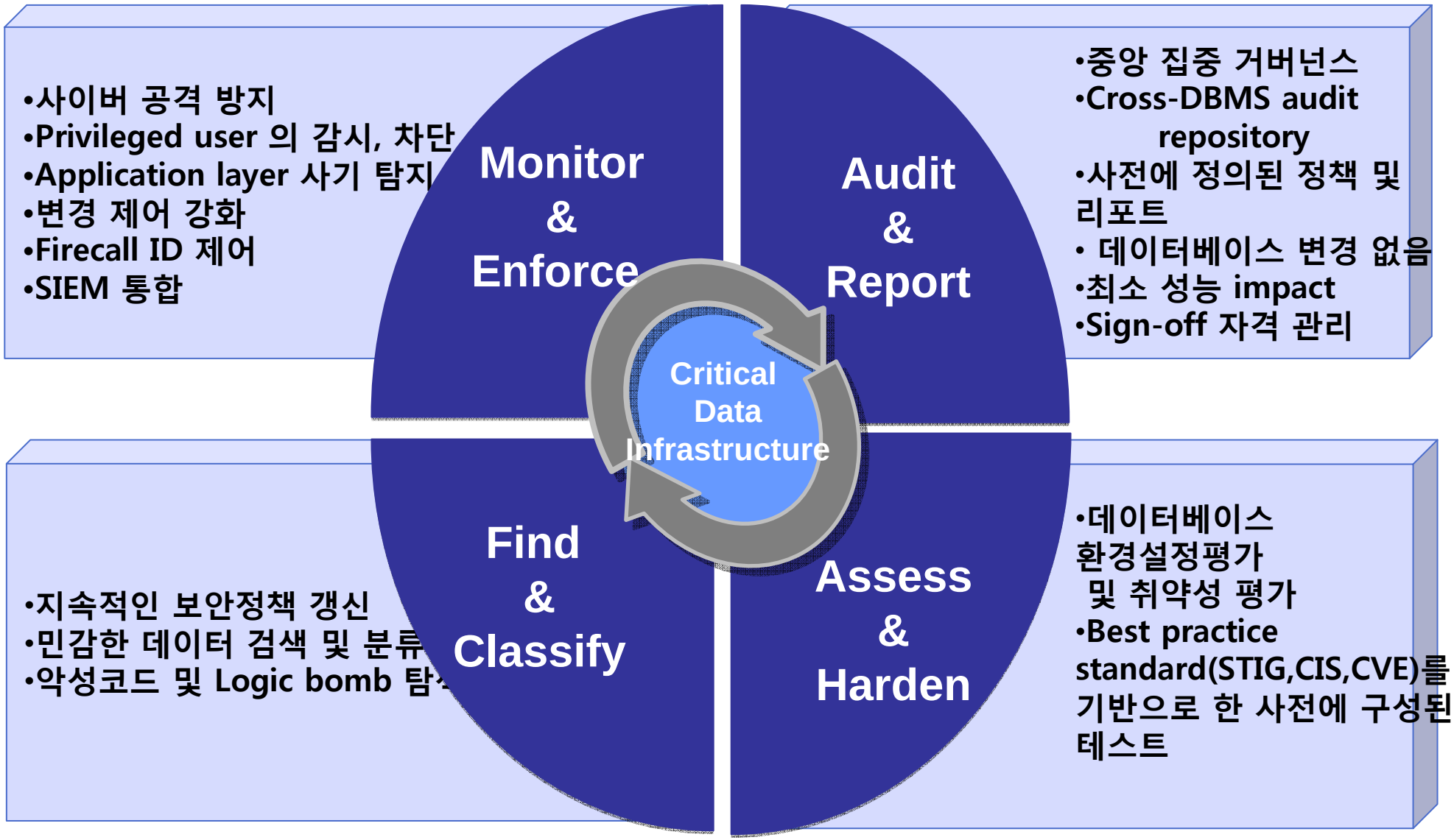
기업의 데이터 환경은 기업 정책,정부규정,업계 표준에 맞는 Information Governance 가 필요

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

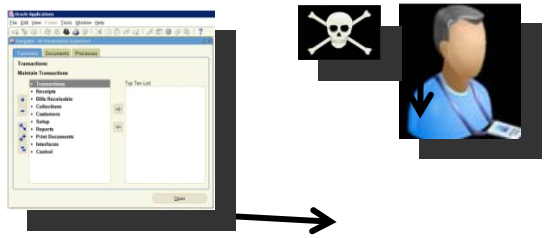
대부분의 솔루션은 처리비용이 많이 들고, 번거로운 수동 process 에 의존함

설계작업으로 직무 분리의 시행
포괄적이고 사용하기 쉬운- 패키지화 된(out-of-box) 레포팅 기능 제공
Compliance 워크플로우 자동화를 이용한 운영비용 감소
모든 데이터 환경을 위한 중앙 집중식 정책으로 Governance 단순화

InfoSphere Guardium 8:
데이터 보안 Lifecycle을 위한 전 영역 지원



Monitor & Enforce :
탐색과 예방 컨트롤을 위한 세분화 된 정책기능



APPUSER

Application Server 10.10.9.244

Database Server 10.10.9.56

Rule #1 Description: non-App Source AppUser Connection

Category: Security | Classification: Breach | Severity: MED

Not ☐ Server IP / and/or Group: Production Servers

Not ☑ Client IP / and/or Group: Authorized Client IPs

Not ☐ Client MAC | Net. Protocol | and/or Group

Not ☐ DB Name

Not ☐ DB User: APPUSER

Field Name

Object: INVENTORY

Command: DROP TABLE

Min. Ct.: 0 | Reset Interval (minutes): 0

Continue to next Rule ☐ | Rec. Vals. ☑

Action: ALERT PER MATCH

Notification

☒ Notification Type MAIL Mail User marc_gamache@guardium.com

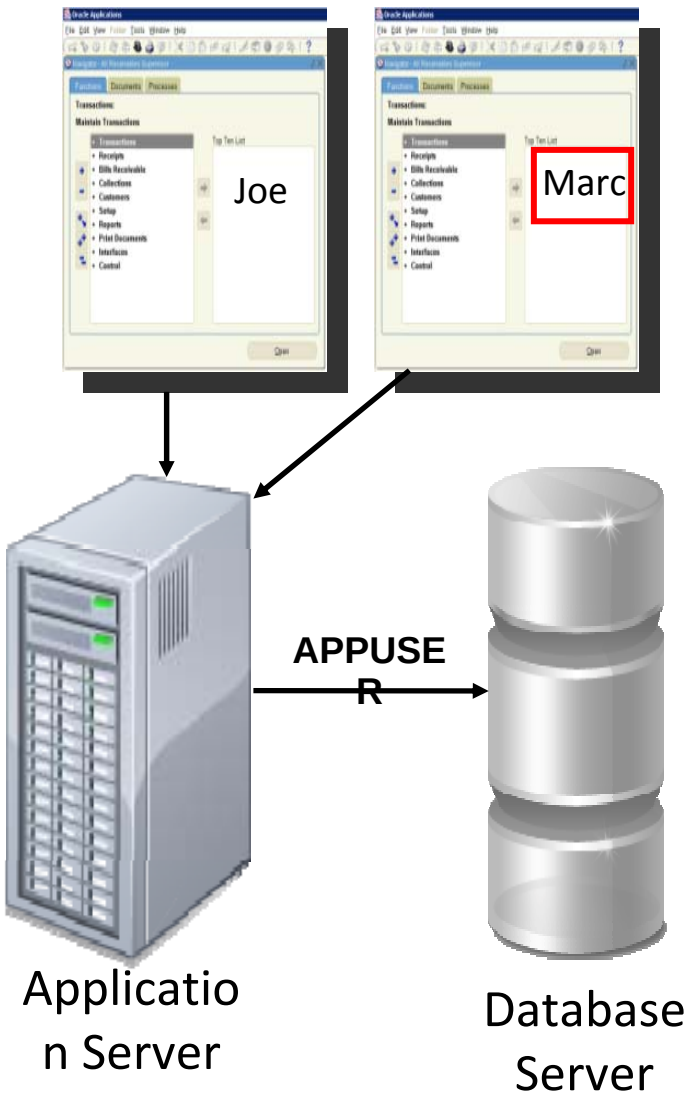
ALERT DAILY
ALERT ONCE PER SESSION
ALERT PER MATCH
ALERT PER TIME GRANULARITY
ALLOW
IGNORE RESPONSES PER SESSION
IGNORE SESSION
IGNORE SQL PER SESSION
LOG FULL DETAILS
LOG FULL DETAILS PER SESSION
LOG FULL DETAILS WITH VALUES
LOG FULL DETAILS WITH VALUES PER SESSION
LOG MASKED DETAILS
LOG ONLY
RESET
S-GATE ATTACH
S-GATE DETACH
S-GATE TERMINATE
S-TAP TERMINATE
SKIP LOGGING

Sample Alert

From: GuardiumAlert@guardium.com Sent: Wed 4/15/2009 8:00 AM
To: Marc Gamache
Cc:
Subject: (c1) SQLGUARD ALERT

Subject: (c1) SQLGUARD ALERT Alert based on rule ID non-App Source AppUser Connection
Category: security Classification: Breach Severity MED
Rule # 20267 [non-App Source AppUser Connection]
Request Info: [Session start: 2009-04-15 06:59:03 Server Type: ORACLE Client IP 192.168.20.160 ServerIP: 172.16.2.152 Client PORT: 11787 Server Port: 1521 Net Protocol: TCP DB Protocol: TNS DB Protocol Version: 3.8 DB User: APPUSER
Application User Name
Source Program: JDBC THIN CLIENT Authorization Code: 1 Request Type: SQL_LANG Last Error:
SQL: select * from EmployeeTable

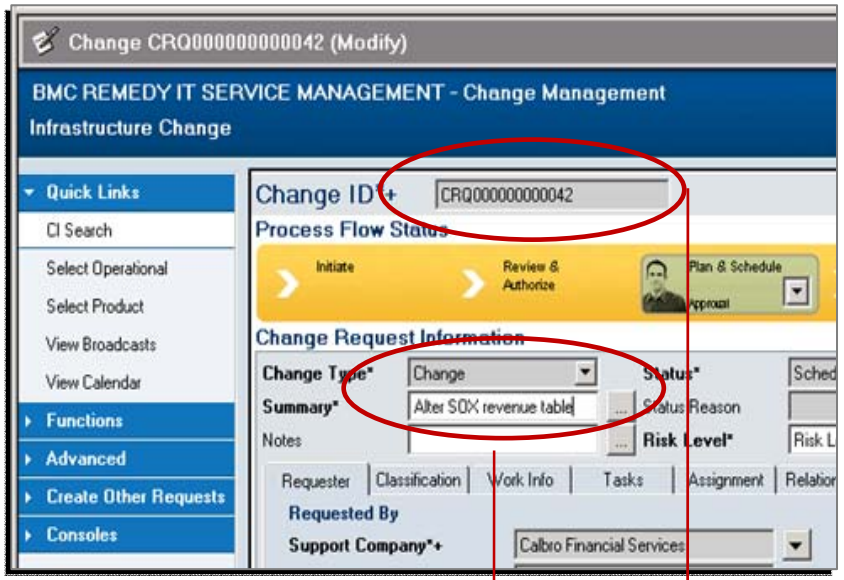
Monitor & Enforce : Application Layer 의 사기식별기능



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
- 그러나 누가 트랜젝션을 시작 했는 지 알 수 없음 (connection pooling)
- 해결책 : Guardium 은 특정 SQL 과 조합된 application user 와 함께 추적
  - 주요 application 및 custome application 을 지원
  - (WebSphere ,Oracle EBS, PeopleSoft, SAP, Siebel, Business Objects, Cognos…)
  - Application 변경 필요없음
  - User ID 의 결정적 추적
  - Time-based 의 추측에 의존하지 않음

Monitor & Enforce :
통제정책 변경강화



1.Ticket ID 를 가진 DBA actions 을 식별

2.승인된 변경에 대한 관찰된 값을 비교관찰

3. 허가되지 않은 변경 또는 유효하지 않은 Ticket ID 를 가진이가 변경할 경우 적색으로 표시

Start Date: **2009-01-22 15:00:00** End Date: **2009-01-22 16:00:00**

Timestamp	Server Type	risk_level	priority	description	change_id	change_id_entered	Assigned To	DB User Name	Client IP	Server IP	Sql
2009-01-22 15:41:55.0	ORACLE	0	0			crq000000000232	allen	SYSTEM	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_rev float
2009-01-22 15:08:21.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_east add total_revenue float
2009-01-22 15:08:29.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_central add total_revenue float
2009-01-22 15:08:36.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_west add total_revenue float
2009-01-22 15:08:44.0	ORACLE	0	3	Alter SOX revenue table	CRQ000000000042	crq000000000042	allen	ALLEN	192.168.8.129	192.168.8.129	Alter table sox_sales_international add total_revenue float
2009-01-22 15:12:39.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	alter table allen.sox_sales_east add sum_total float
2009-01-22 15:14:19.0	ORACLE	0	0					SYSTEM	192.168.8.129	192.168.8.129	insert into allen.sox_sales_east (i,customer,zipcode,revenue,total_revenue,sum_total) values(?,?,?,?,?,?

Find & Classify:
과도하거나 불필요한 데이터에 접근

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

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

Is this normal?

What did he see?

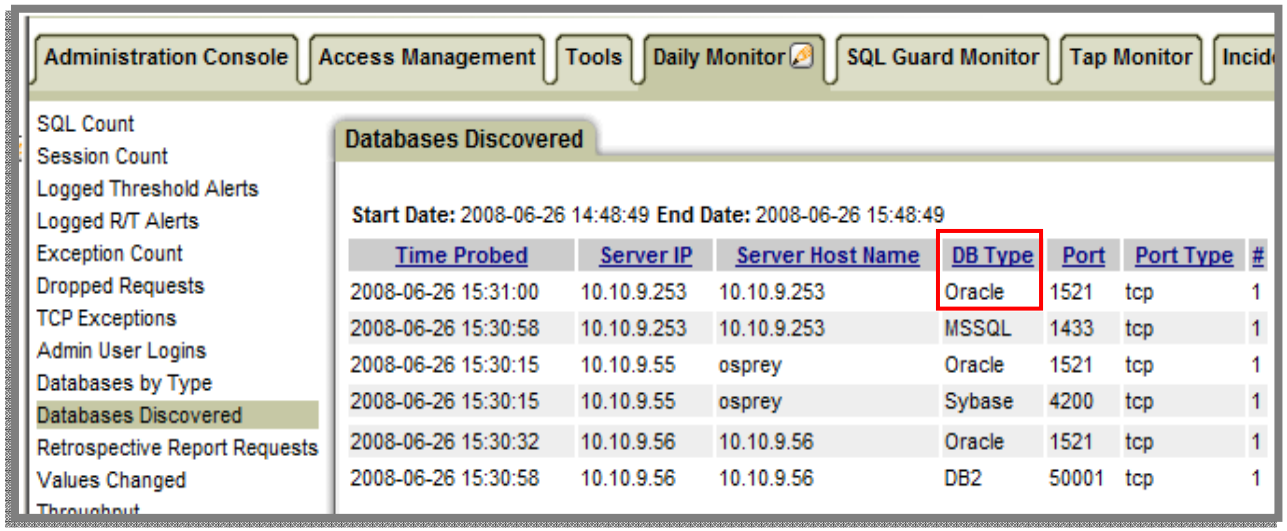
HARRY	select * from ar.creditcard where i<?	**********0002, **********0003, **********0004
JOE	select * from ar.creditcard where i<?	**********0001
JOE	select * from ar.creditcard where i<?	**********0002, **********0003, **********0004, **********0005, **********0006, **********0007, **********0008, **********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

Find & Classify:
데이타베이스 구성변경 감사기능

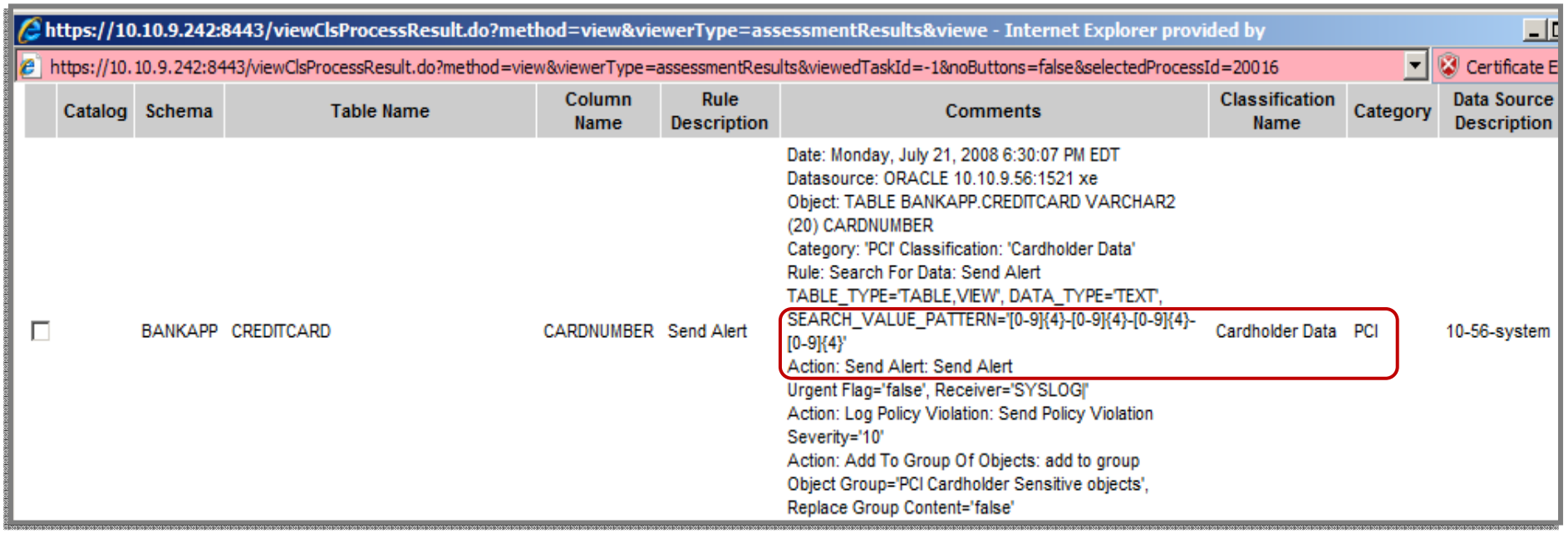
$ORACLE_HOME/soap/bin/.*	File Pattern	12h	✓	✓
$ORACLE_HOME/sysman/admin/OMSRepositoryConstraints.properties	File Pattern	12h	✓	✓
$ORACLE_HOME/sysman/config/.*properties	File Pattern	12h	✓	✓
$ORACLE_HOME/xdk/admin/xml.properties	File Pattern	12h	✓	✓
ORACLE_BASE	Environment Variable	12h	✓	⊘
ORACLE_HOME	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
- 200+ 이상의 모든 주요 운영체제/ DBMS 구성을 위한 사전구성, 사용자 지정 템플릿을 제공

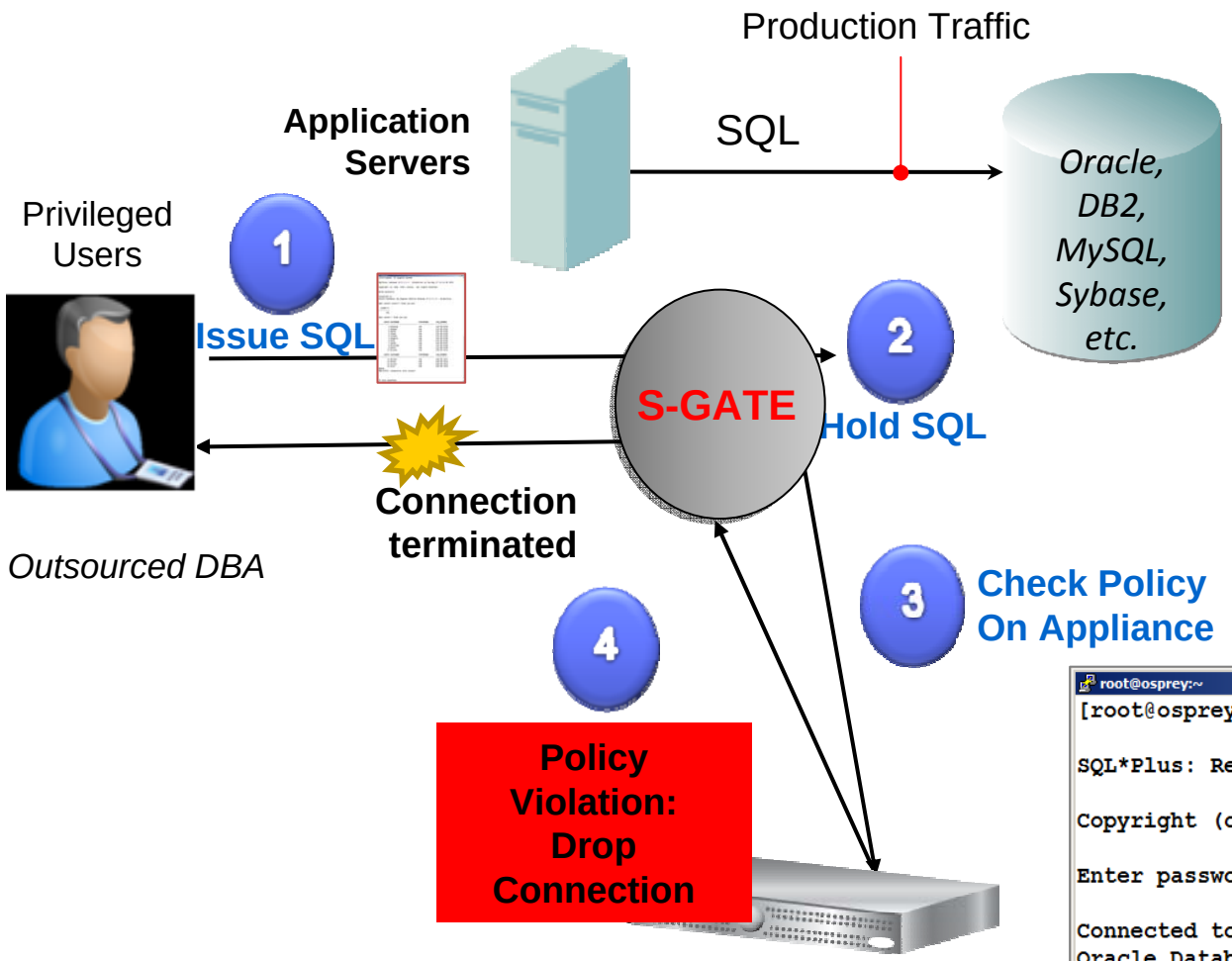
Find & Classify:
민감한 데이터를 분류 및 탐색 -발견하기



- 데이터베이스 탐색
- 민감한 데이터 탐색
- 정책 기반 Action 수행
  - ✓ Alerts 수행
  - ✓ sensitive objects 의 group 으로 추가



Audit & Report:
실시간으로 사전에 정책위반사항 방지기능 제공



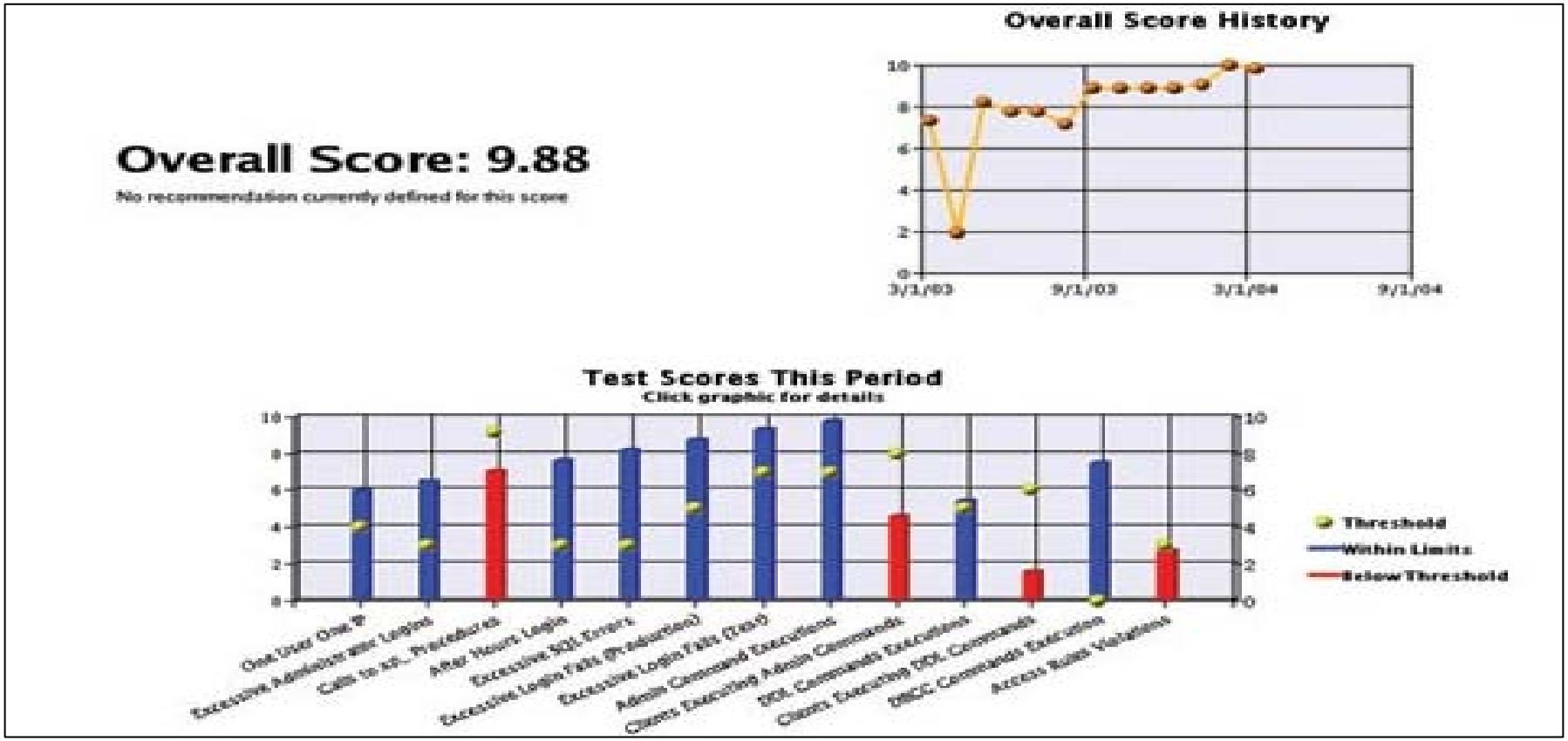
- 데이타베이스 변경없음
- Application 변경없음
- Inline application 의 트래픽 방해 없음

```
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

Assess & Harden :
보안 취약점 평가

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

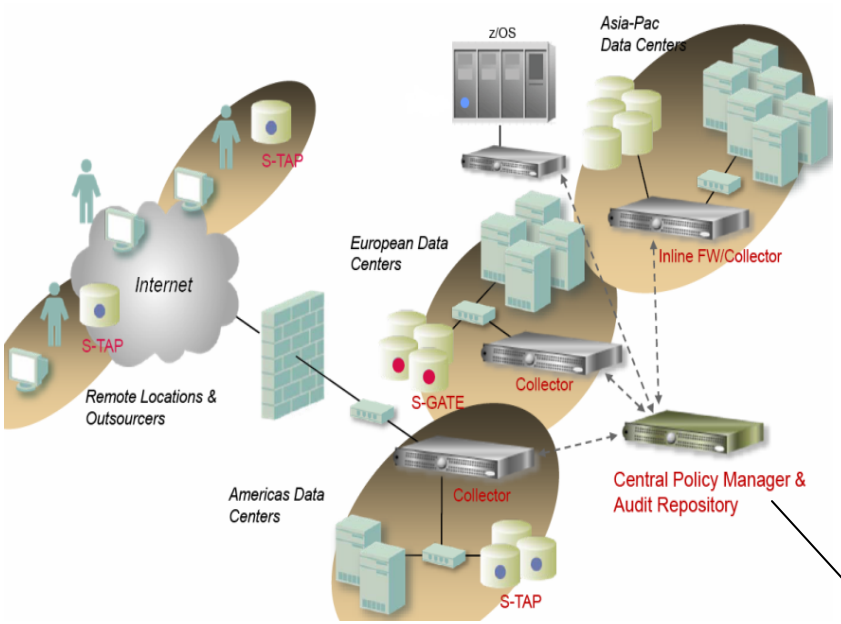


InfoSphere Guardium 8 Summary

가장 완벽한 Database 보안 솔루션 / Reducing Risk,Simplifying Compliance & Lowering Audit Costs

- 새로운 확장된 플랫폼/애플리케이션/DB 지원
  - - System z
  - - SharePoint
  - - SAP
  - - PostgreSQL
  - - Netezza
- 새로운 접근 제어 기능
  - - 향상된 차단기능 : Firecall-ID management & quarantine
  - - Entitlement reporting
- 새로운 audit & compliance 감시 기능
  - - Advanced compliance workflow automation
- 새로운 취약성 평가 (Vulnerability assessment) 테스트기능 강화
- Tivoli (TSIEM) 과의 통합
- 가용성 ,성능향상에 기반을 둔 여러 가지 확장된 기능

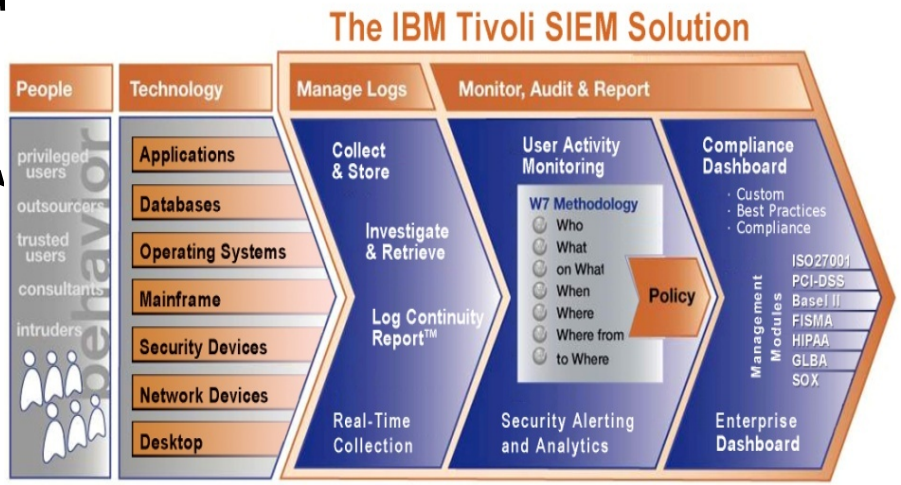
TSIEM & Guardium



- 세분화된 데이터베이스 모니터링 및 보호
- 낮은 오버헤드; 로깅 저장 부하 감소
- 데이터베이스 위치와 분류
- 데이터베이스 평가 및 경화
- 자동 준수보고 및 워크플로우
- 수출 알림 및 TSIEM에 핵심 데이터

Syslog-CEF
Feed

- 통합 Guardium 알림 및 데이터
- 엔터 프라이즈 준수 및 감사
- 법의학
- 로그 관리
- 컴플 라 이언스 관리 모듈을위한 ISO27001, GLBA, 삭스, HIPAA 등

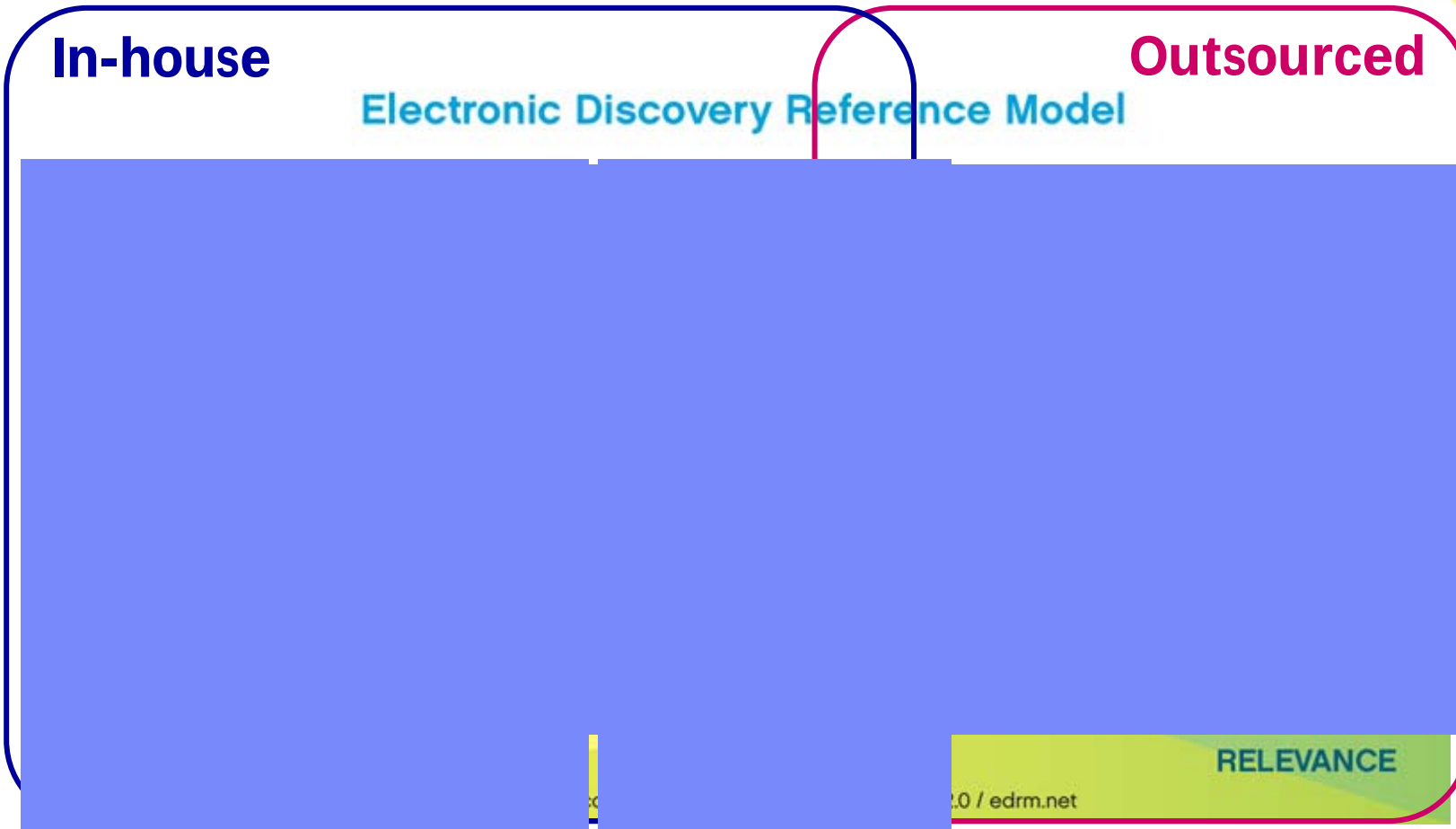


Unstructured Data – eDiscovery

소송(기소), 조사 그리고 감사에 필요한
식별(Identifying), 위치 파악, 디지털 증거 또는 전자적
보관 정보(ESI, Electronically stored information), 자료
등을 취합, 분석하는 모든 과정:
InfoSphere eDiscovery

Best Practices for e-discovery

민첩하게(Agile) 선재적 대응(Proactive & Defensible)하게 도와주는 IBM eDiscovery solutions

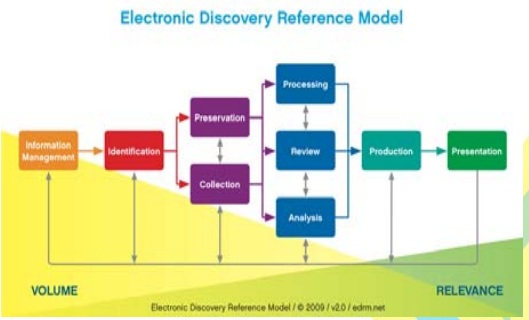


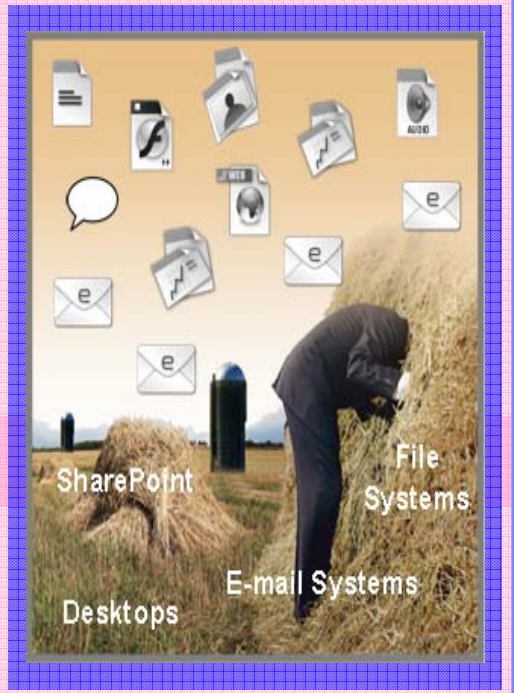
선재적 대응
(Defensible Process)
운영 효율 및 위험 감소

사전 정보관리**(Proactive Information Management)**
전자 검색 비용 및 위험을 줄이기 위한

민첩한(빠른) 결과
(Agile e-discovery Response)
전략적 통찰력과 빠른 대응

수작업에 의존적인 eDiscovery





어지럽게 산재, 분실/손실 위험, 불필요하게 보관

소송지원 (Litigation Support)

기업 법률 (Corporate Legal)

수작업, 비교적 비용이 많이 소요, 오류 발생 가능성이 높은 검색(분석) 프로세스

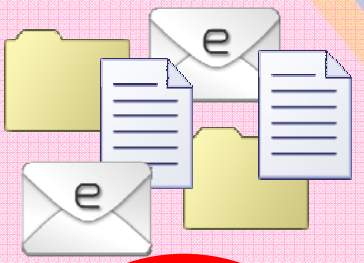
Service Providers

사용자 (Business Users)

IT / RIM

일관성 없는 정보 집합(Inconsistent information)

대부분 수작업



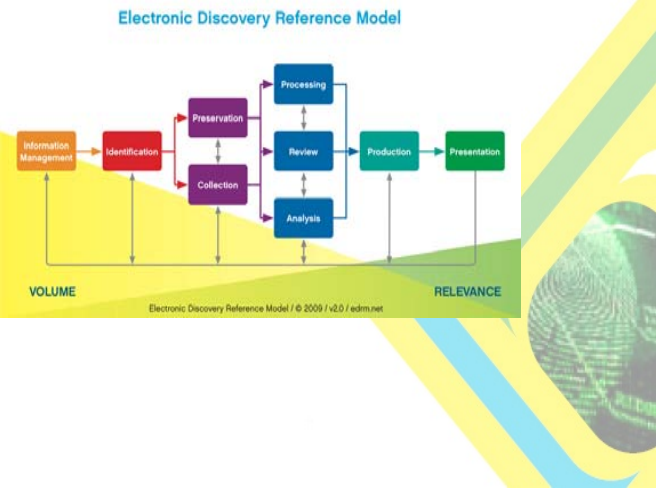
중복 자료, 엉뚱한 자료, 불안전한 정보

높은 비용 및 위험

Outside Review

Volume

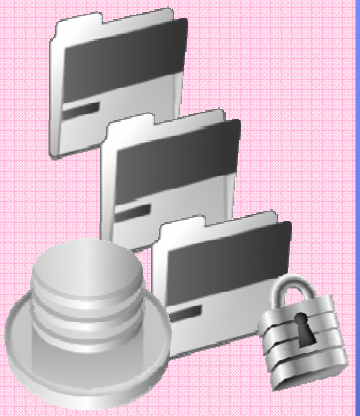
Agile and Proactive eDiscovery



어지럽게 산재,
분실/손실 위험,
불필요하게 보관

Proactive ESI Management

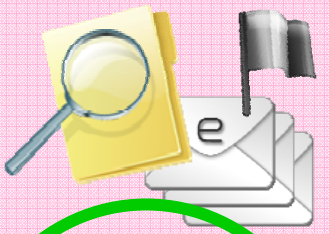
- Content Assessment
- Content Collection & Archiving
- Automatic Classification
- Records/Retention Management



조직화된,
보안성, 신뢰할
수 있는 정보

Agile eDiscovery Response

- eDiscovery Search & Analytics



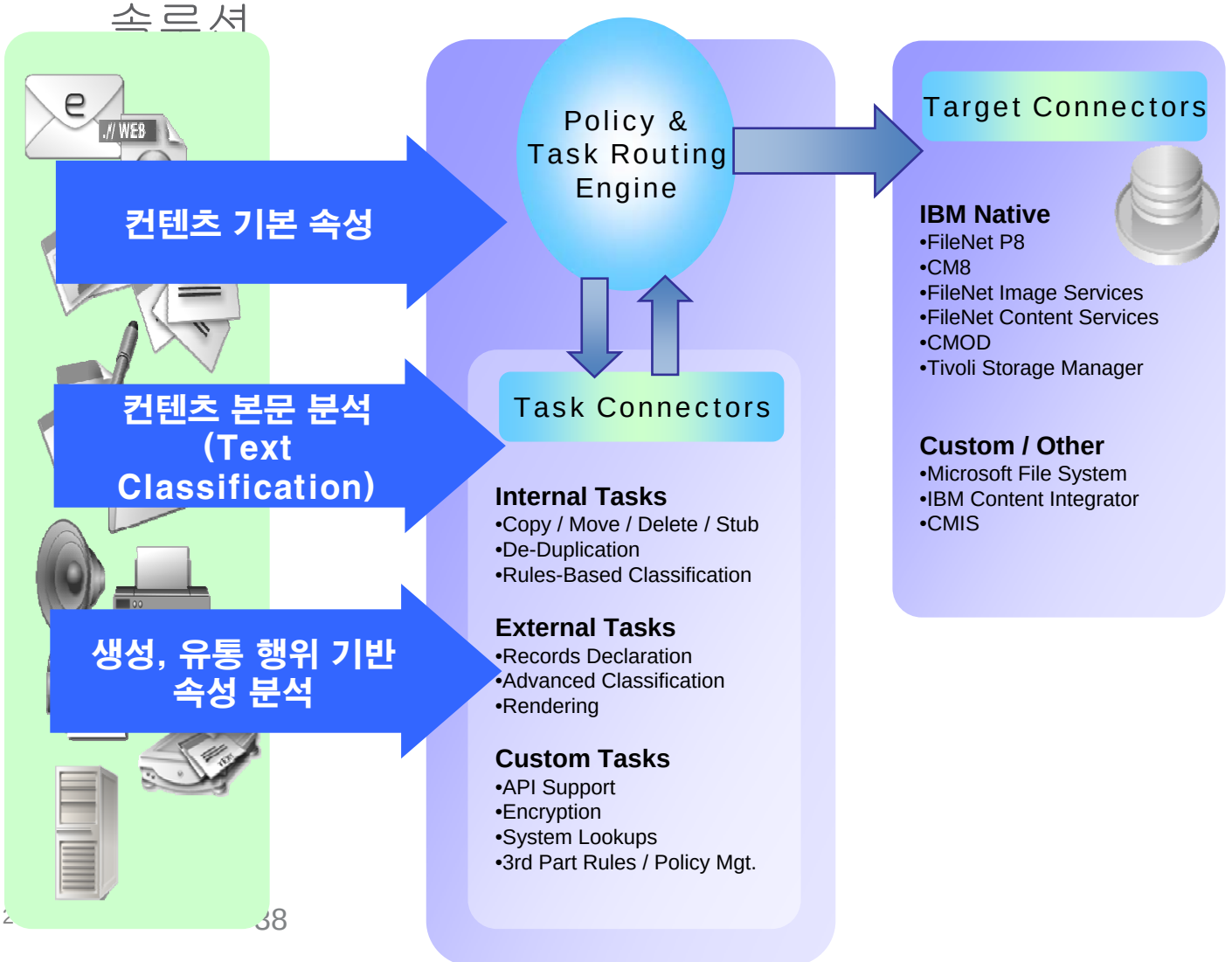
연관성,
통찰력(insightful), 검토(분석)
가능한 정보

비용 및 위험 감소

Volume

Infosphere Content Collector
단순 Archiving이 아닌 Content Collection

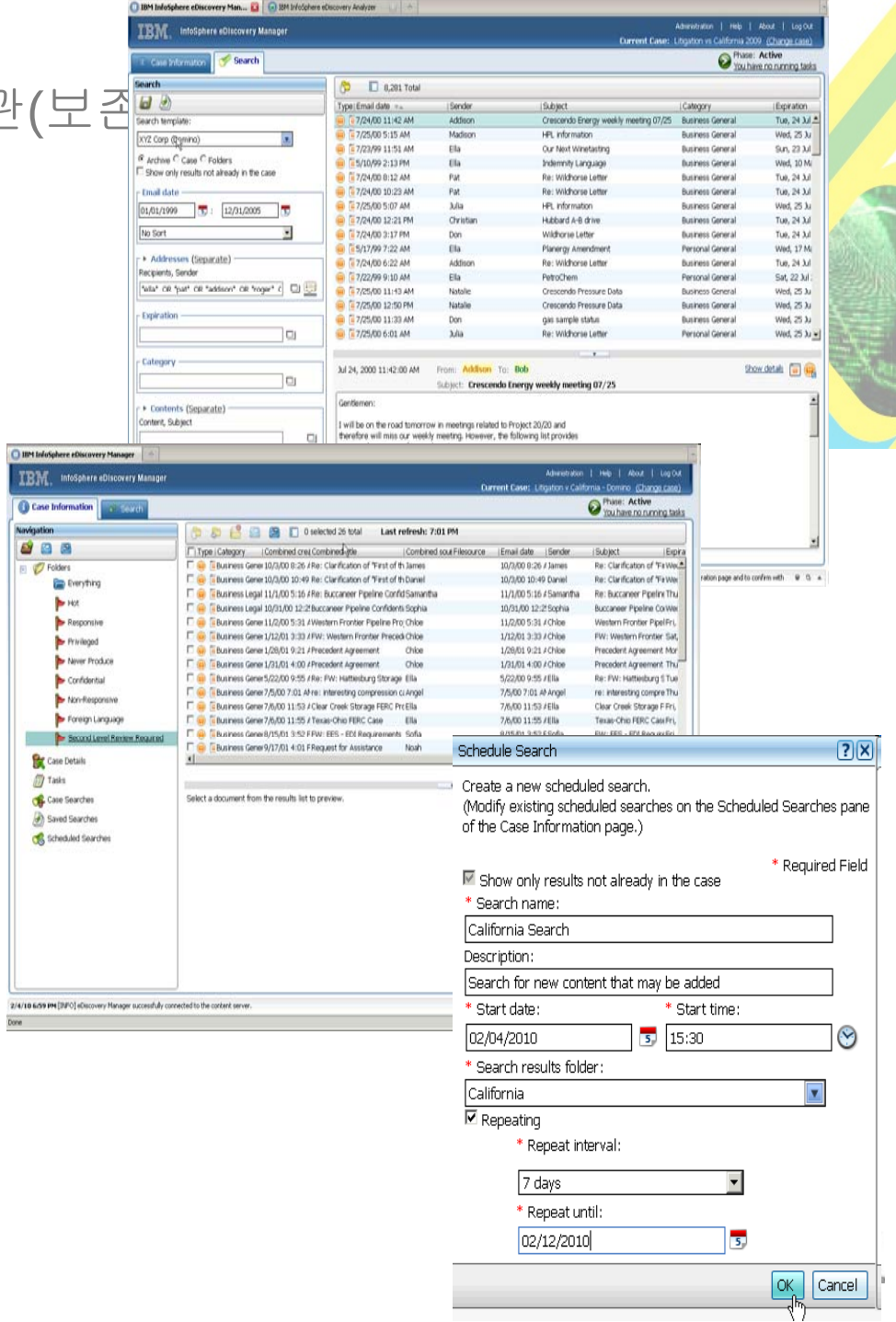
- Domino Notes 및 Exchange를 포함한 메일 시스템 뿐 아니라 File System 등 다양한 기업의 컨텐츠를 정책에 따라서 취합(Collection)하는 솔루션



- 쉽게 자료를 추출
  - 다양한 Connector 및 API를 제공하여, 기업 내 유통되는 다양한 컨텐츠를 쉽게 추출함
- 자동화된 분류
  - 분류 정책 및 계획을 직접 수립해서 적용할 수 있음
  - 다양한 추가 분류 체계 및 사용자 정의 분류체계 및 규칙 적용
- 안전한 보관하고 효율적인 저장
  - 정보 추출한 정보를 바탕으로 분류하고, 분류 정책에 따라, 장기보관, 변경/수정 불가능(Lock&Hold), 폐기 등 수행
  - 전문화된 EDMS을 통해 안전하게 보관하고 검색 조회함

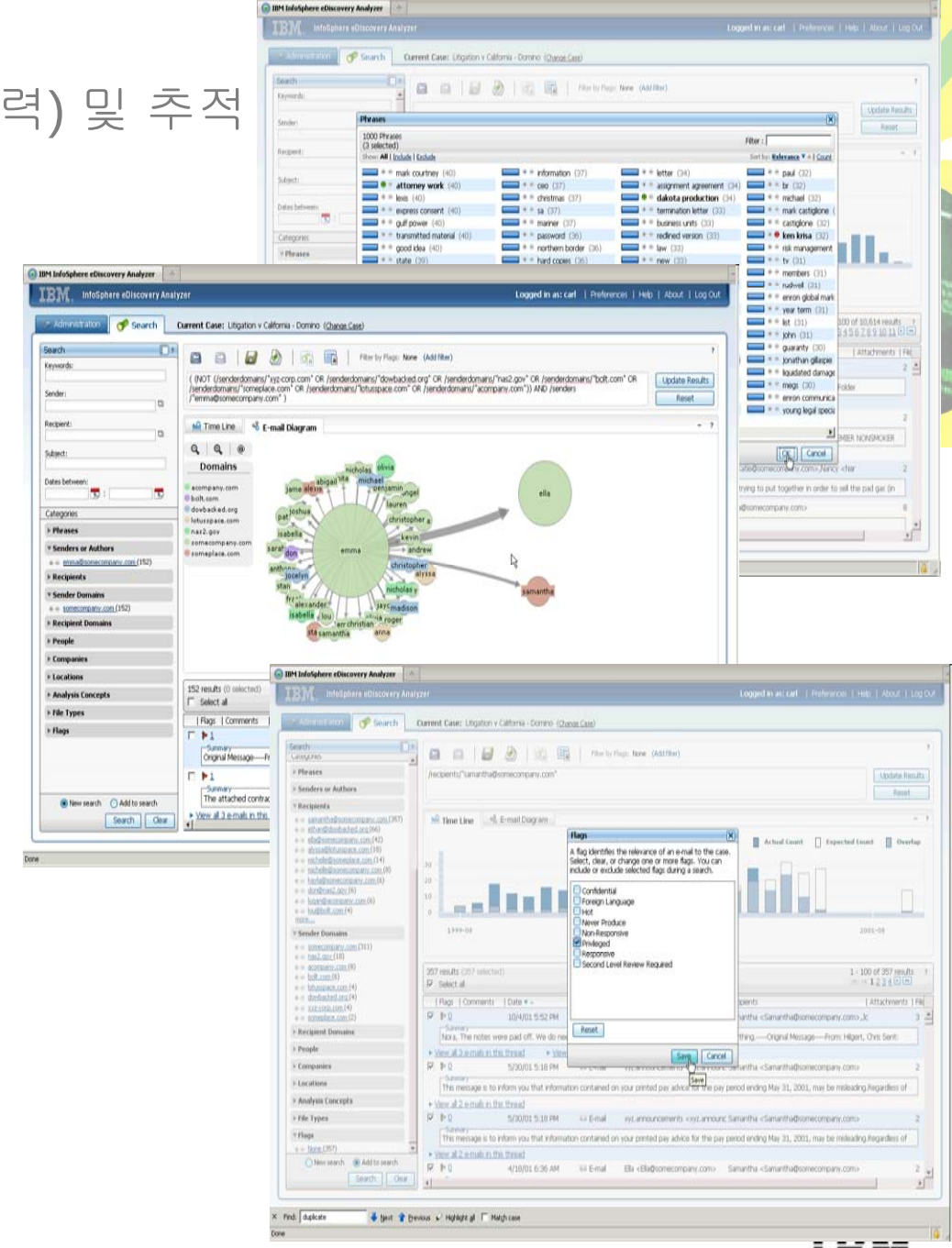
IBM eDiscovery Manager
종합적으로 검색, 조회, 취합, 연결 및 보관(보존

- eDiscovery에 대한 IT적 기능들
  - 케이스(Case)생성, 사용자 지정(권한 설정)
  - 다양한 Case별 전자 보관소(ESI) 관리
  - 검색 및 추가적인 Case 관리
  - Hold, Lock 기능
  - 미리보기(관련 정보 포함)
  - 반복적인 업무 스케줄 검색
  - 감사, 추적, 변경에 대한 보고서 및 무결성 지원
  - EDRM XML 형식 지원 (제출형식 추출-Export)



IBM eDiscovery Analyzer
Case(사건)에 대한 집중적인 분석(통찰력) 및 추적

- 변호사, 수사관, 감사자 및 지원부서를 위한 도구 - 모든 Case(사건)을 추적 분석하는데 적은 비용으로 처리 가능
  - Case(사건) 정보로부터 빠르게 핵심정보(Relevant data set)를 추출
  - 주요 사실, 커뮤니케이션 패턴 및 스레드, 핵심 증거 조각 등을 쉽게 찾도록 심층적인 분석(Insight)
  - 플래기(Flag), 동적 연결(dynamically Link) 방식, 중복 제거 및 검토를 위한 우선 순위 감지, 연관성 분석
  - 검색(Query) 결과에 대한 보고서
  - 검색 및 분석 결과에 대한 보안 및 감사 기능



Unstructured Data – FileNet

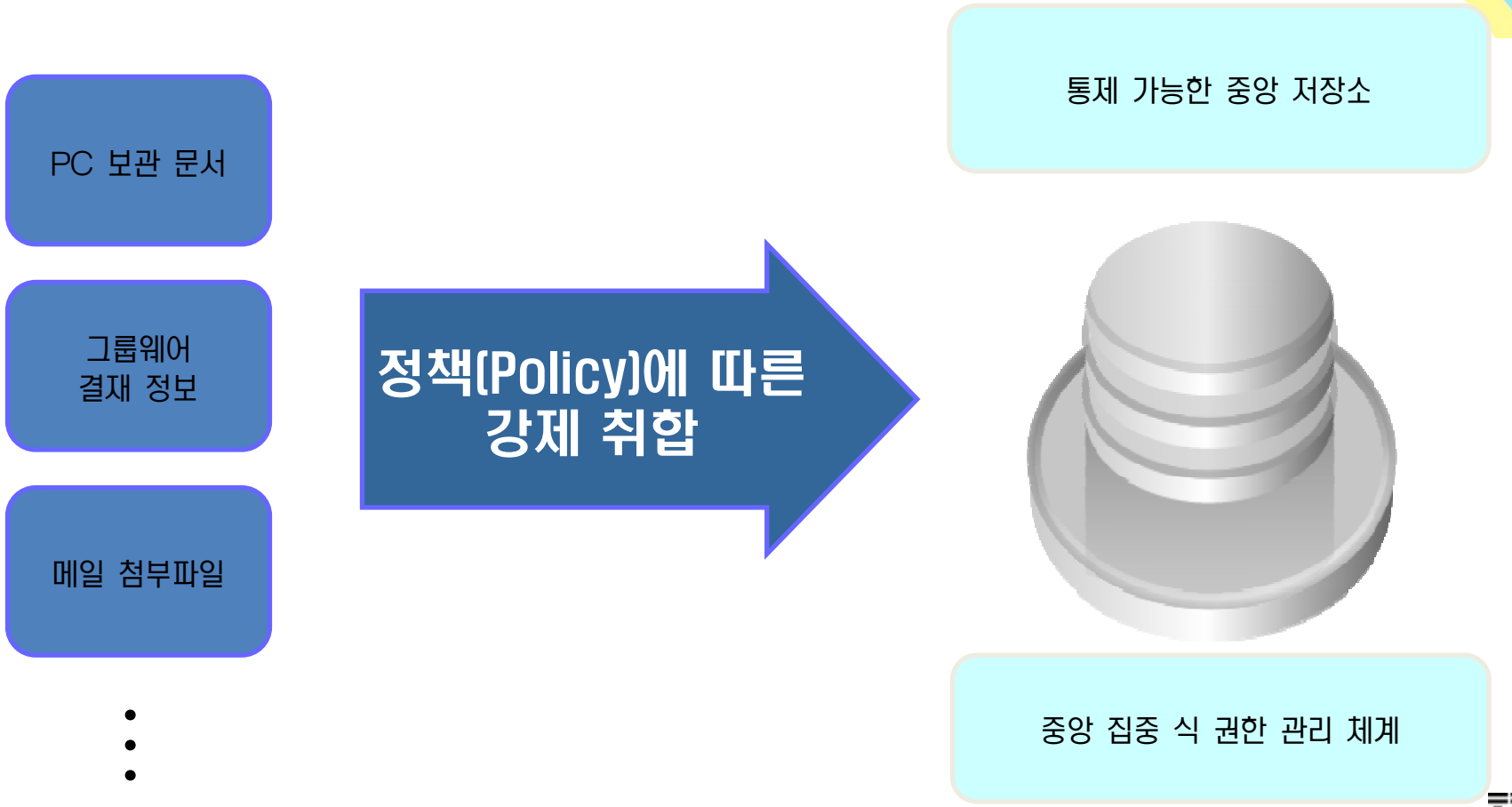
정보의 취합, 안전한 관리, 효율적인 활용

IBM FileNet P8 Content Manager, Classification Module

Records Management

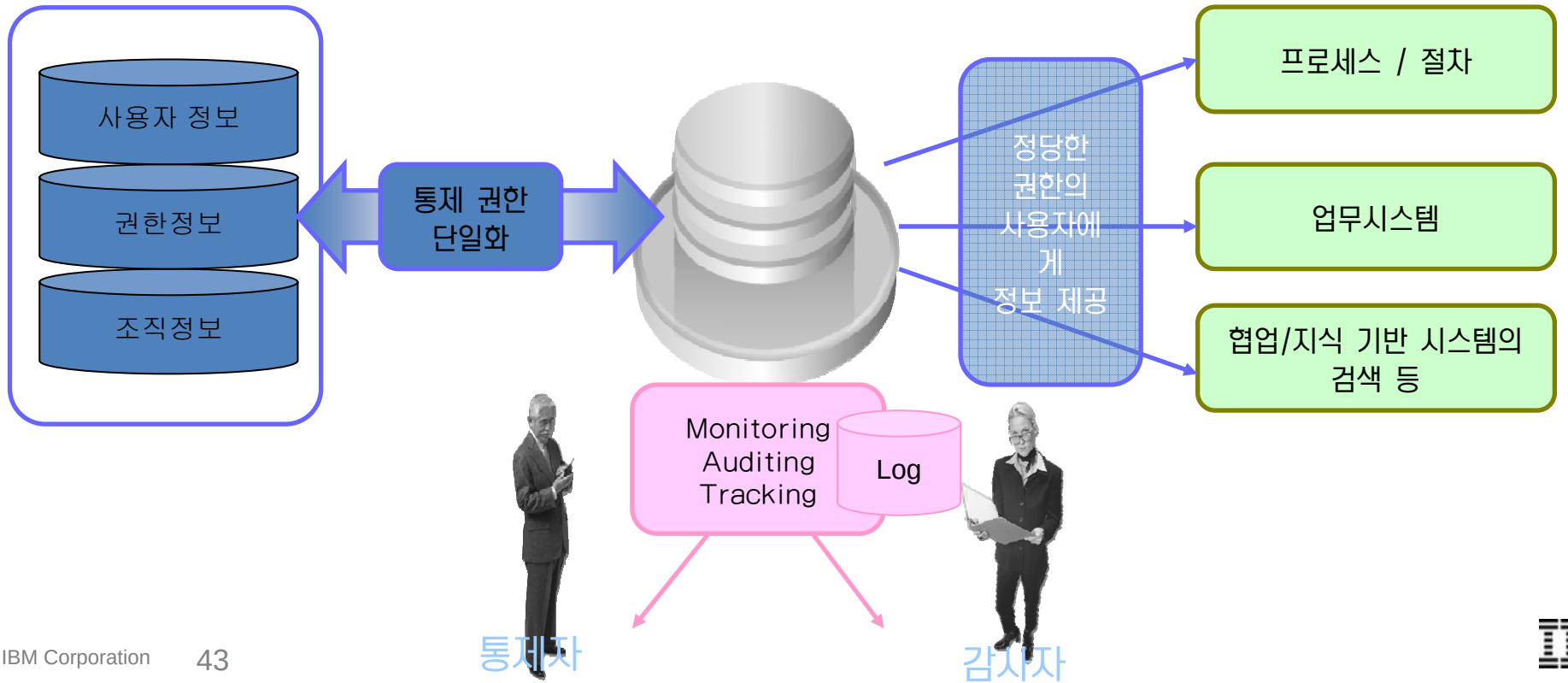
통제를 위한 취합 – 필요한 정보 강제 취합, 정보 통제

- 기업의 정책상 필요하다면, 잠재적 위험이 될 수 있는 정보(모든 종류의 컨텐츠)를 접근 통제 할 수 있어야 한다. 접근 통제하는 방법은 정보를 강제로 중앙 보관소에 보관하는 방법과 중앙에서 접근권한이 통제되는 방법이 있다



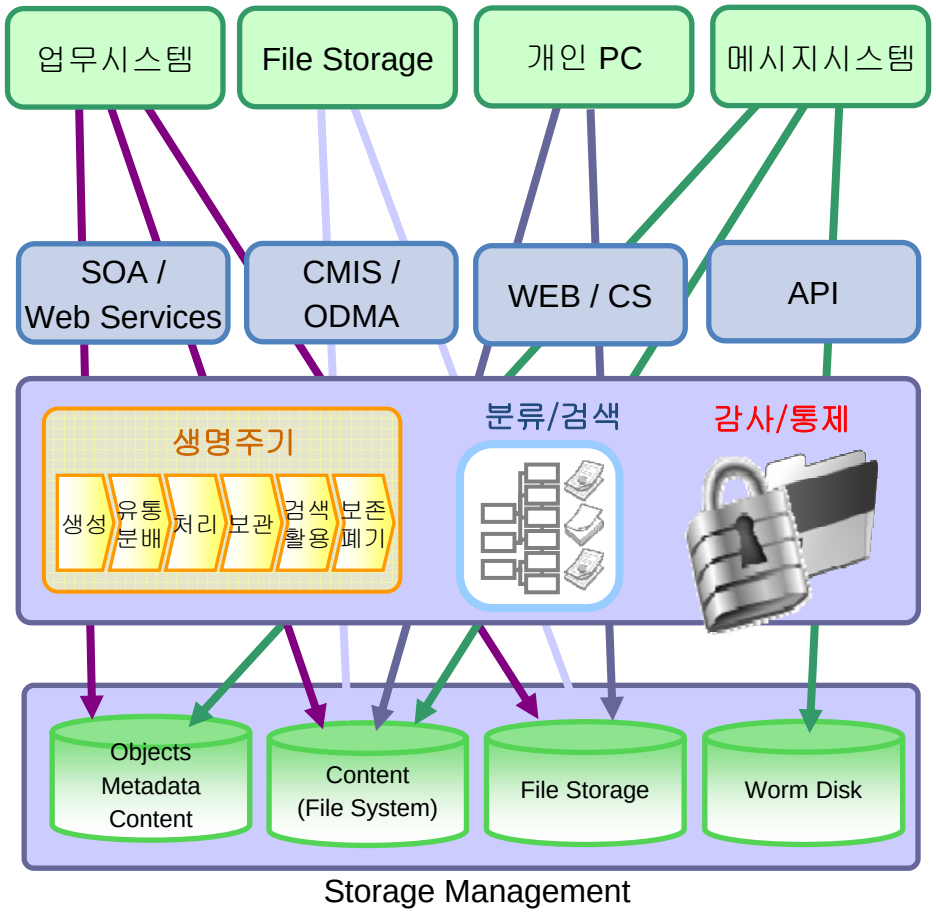
통제를 위한 관리 – 정책에 따른 정보의 통제 / 모니터링 및 분석

- 전사 정보 통제 규정(Rule) 및 정책(Policy)을 반영하여, 통제 가능한 중앙 저장소가 필요하다. 이 정책에는 전사적 조직(IT 및 비 IT모두), 프로세스가 반영되어 유기적으로 연동 되어야 한다.
- 정책의 위반, 자동화된 경고, 사후 대응을 위한 모니터링, 정보 분석 등이 기능이 필요하다.



ECM 관점에서 취합

- 표면적 자료 취합이 아닌, 중복 없이, 재사용 가능한 컨텐츠 통합



- 컨텐츠 표준화
  - 기업의 컨텐츠 생성/유통/폐기에 대한 표준화
  - 컨텐츠 보관에 대한 정형화
- 효율적인 인터페이스
  - 표준 프로토콜 및 개발환경에 대응하기 위한 다양한 방식의 연계
- 생명주기 관리
  - 생성 후 유통 및 폐기에 이르는 컨텐츠의 생명주기 관리 및 통제
- 다양한 분류 체계 및 검색
  - 사용자가 필요로하는 자료를 쉽고 빠르게 검색
  - 다양한 조직, 업무에 맞도록 가상화된 분류체계
- 모니터링, 사후 감사, 통제
  - 현 사항에 대한 실시간 모니터링
  - 사고, 감사 등의 사유로 Auditing
  - 접근 제어 및 기업의 다른 권한 체계 연동
- 확장성 있는 통합 저장소
  - 정보를 적절하게 분류해 중요도, 보존기간 등을 고려해 다양한 Cost의 스토리지에 보관

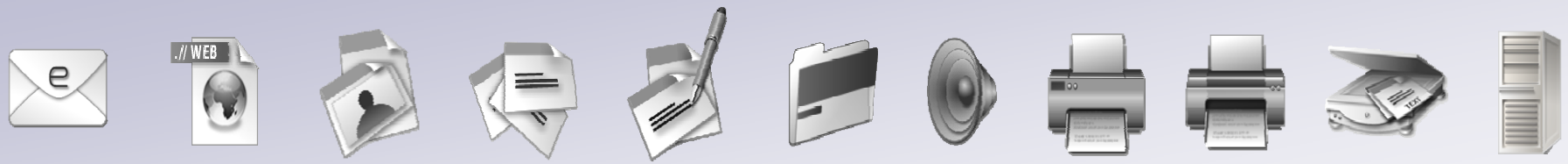
ECM 관점에서 통합 관리

- 취합된 정보는 안전하고, 증명 가능하게 보관되어야 하며, 다양한 곳에서 재 사용 가능 하도록 표준화되어 있어야 한다.

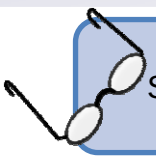
통제 되고 있음 확인, 위험 요소 관리, 법규 준수 증명(eDiscovery) 등에서 다양하게 사용

직접 사용	표준 인터페이스	자동 이관	자동 분류	대용량 처리
시스템 중심이 아닌 업무 중심 컨텐츠 활용	쉬고 안정적인 통합/연동	보관주기 관리 컨텐츠 관리 비용 감소	수작업부분 최소화 안전한고 적절한 보관	지식 기반 시스템 성능 향상

기업의 컨텐츠 기반(Foundation)



쉽고, 증명이 되는 정보
Holding & Locking
위조/변경 방지

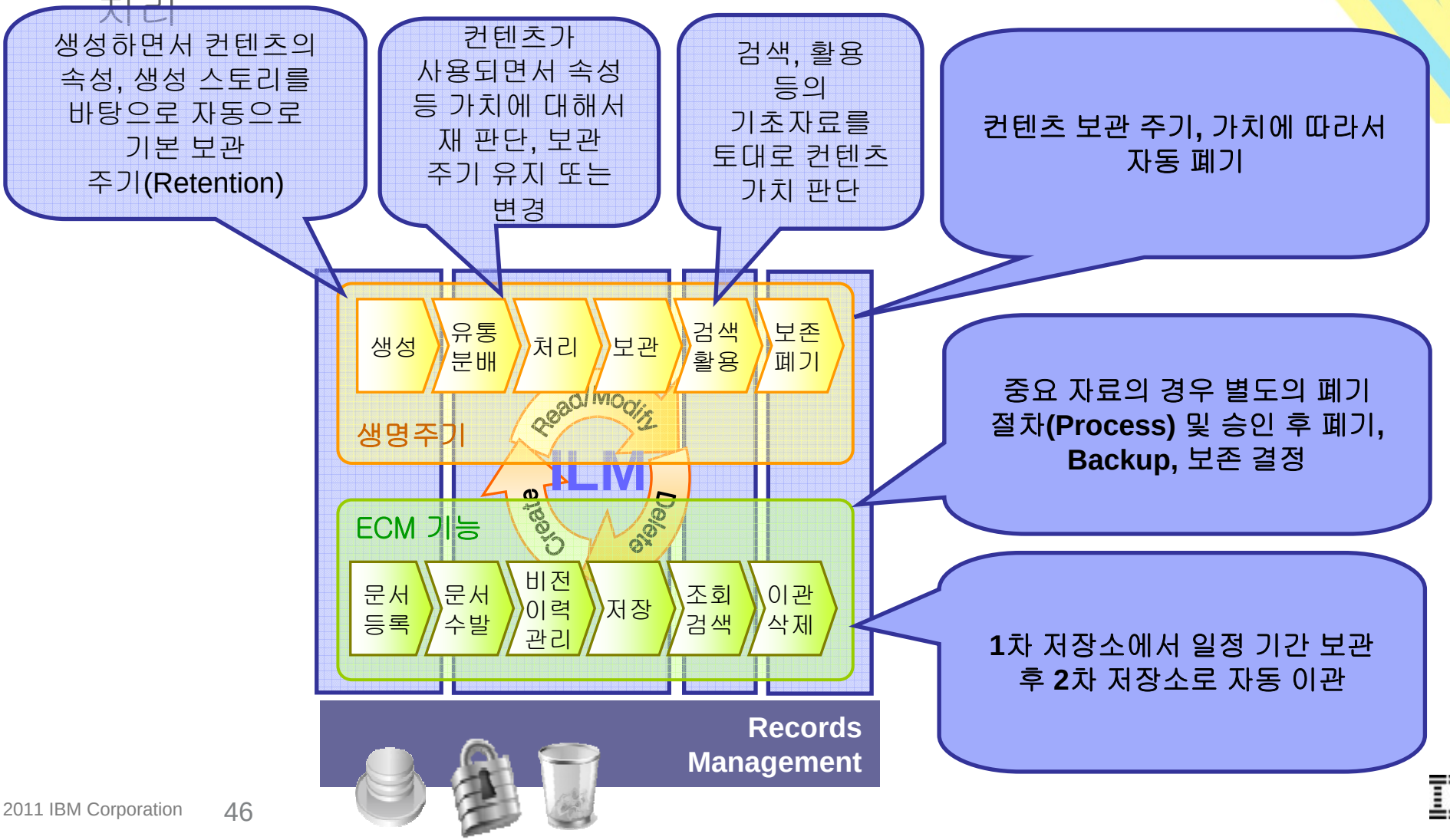


Search & Discovery

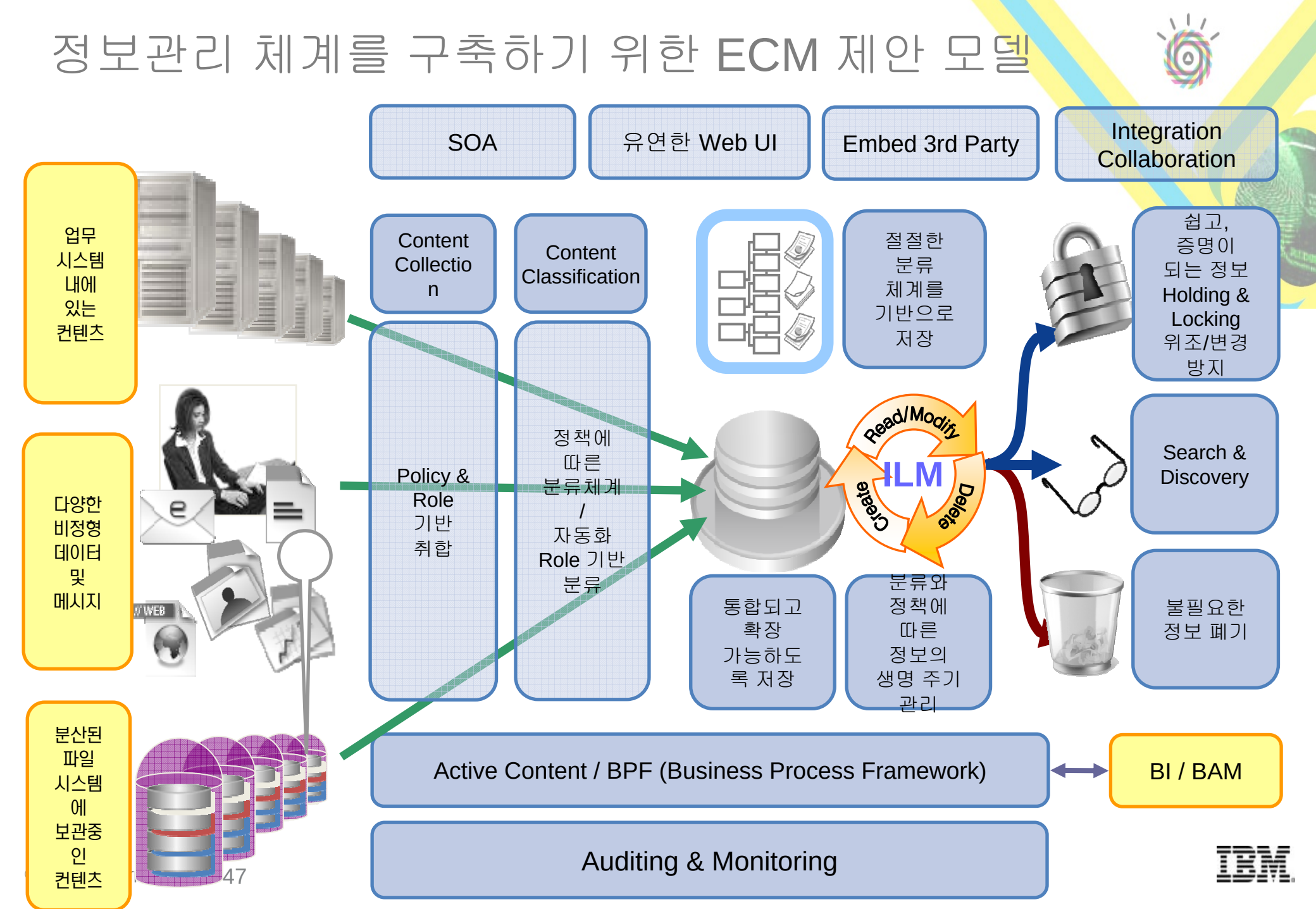
불필요한 정보 폐기
폐기 프로세스
폐기 증명

불필요한 정보는 정확히 파기

- 생성되면서부터 기본 보관주기를 가지게 되고, 유통, 활용되면서 해당 값을 판단하며, 폐시기 컨텐츠의 가치에 따라서 다양한 폐기 정책을 수립 처리



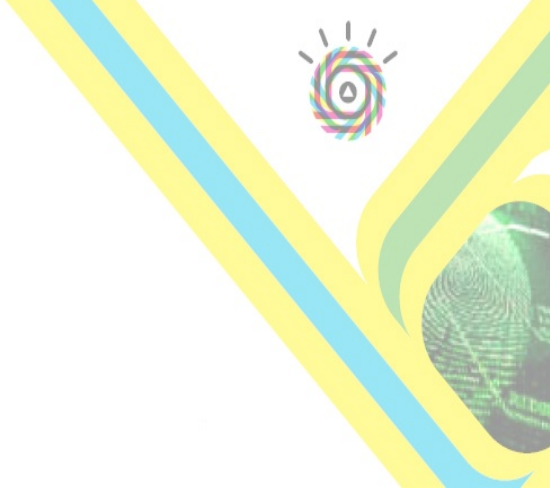
정보관리 체계를 구축하기 위한 ECM 제안 모델



FileNet P8 Platform

	Governance	Risk Management	Users
취합	정보 자산화 	잠재적 위험 제거 위한 정보 취합 	기존 PC에서 사용 보다 불편함 최소화 
관리	조직, 프로세스, 정책에 따른 정보의 접근 통제 	정보 보안 수준 상승 최신의 정보를 신뢰할 수 있도록 통제 관리 	유일본 관리 최신의 정보 제공(최종본) 
활용	기업의 모든 컨텐츠 공급자의 역할 	사후 모니터링 정보 검토(eDiscovery 	정보 공유의 장 정보 제공의 장 

Thank you.



- InfoSphere Guardium 8
- Contents Collector
- eDiscovery Manager
- eDiscovery Analyzer
- FileNet P8 Content Manager
- Classification Module
- Records Management