

멀티클라우드 환경에서의 데이터 보호

CONTROL YOUR CLOUD



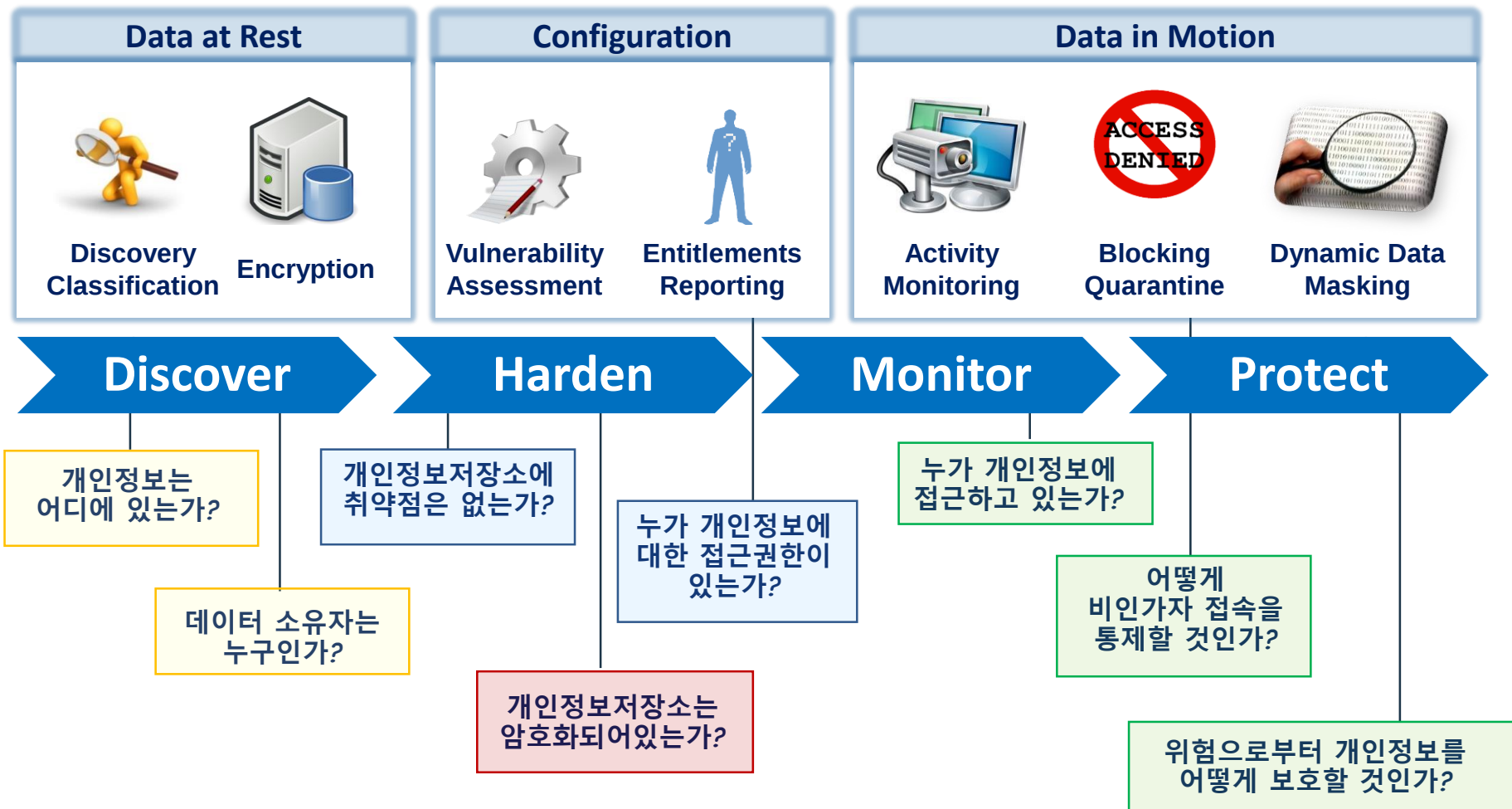
2018/12/05
조가원 실장
IBM Korea



기업의 데이터 보안 전략



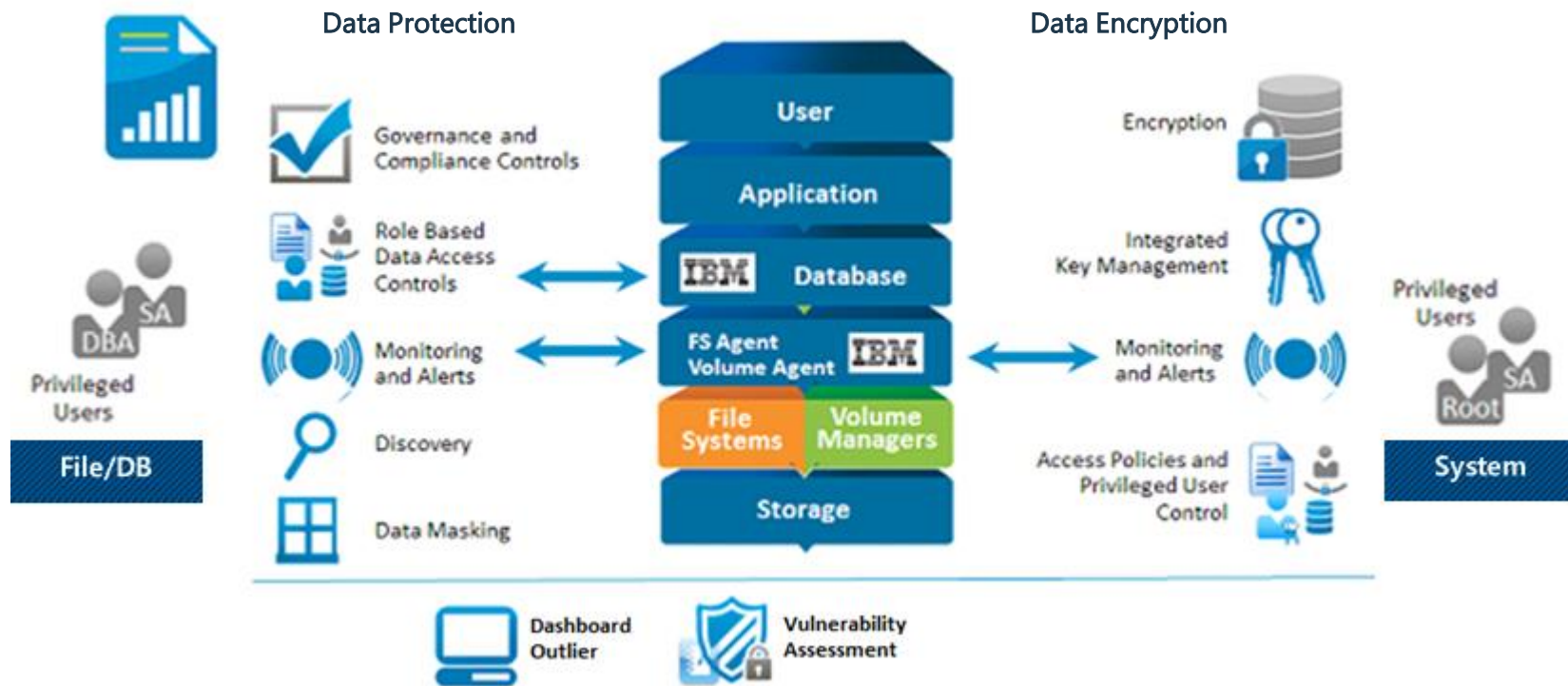
개인정보에 대한 체계적인 관리 보호



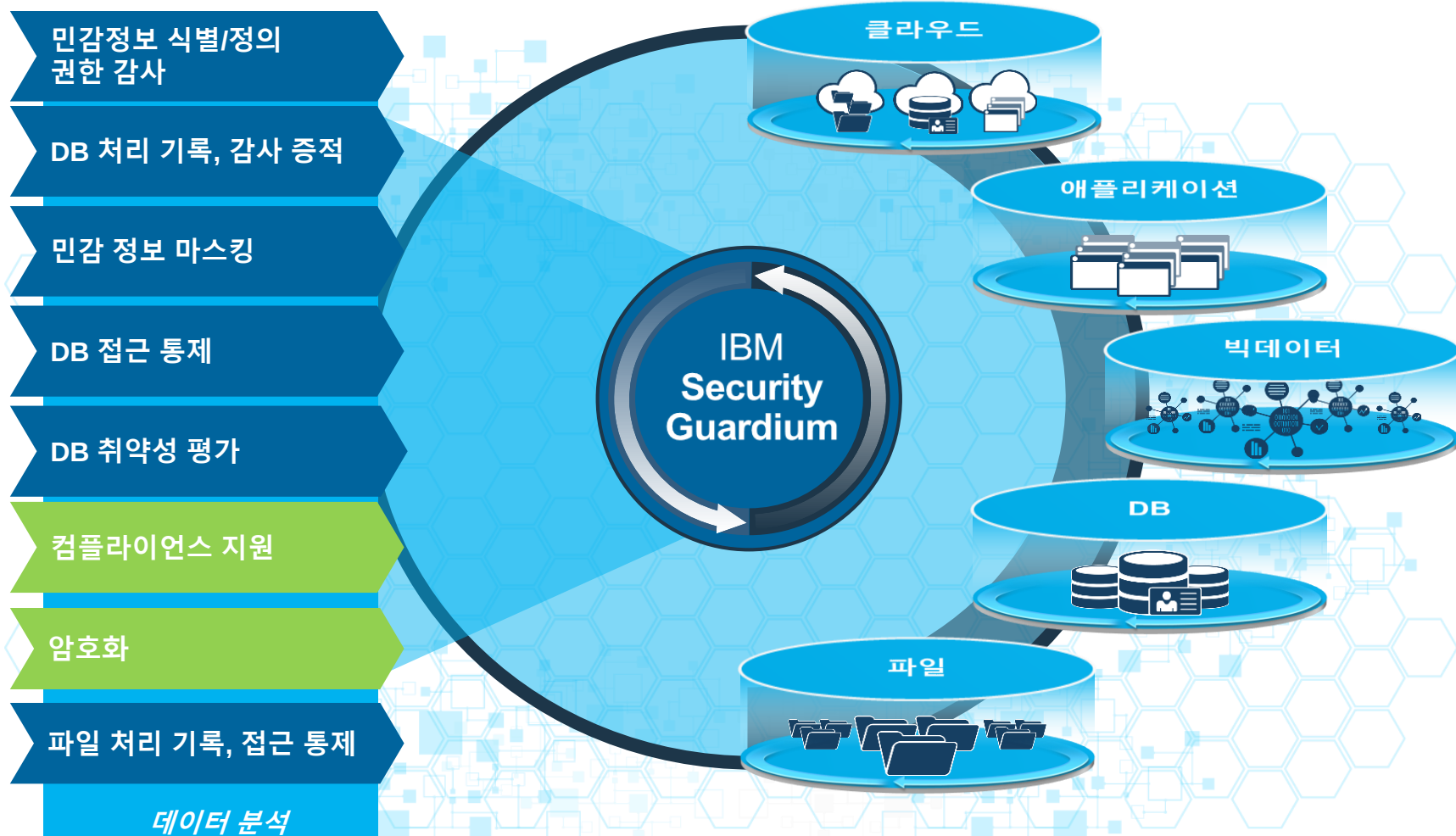
안전한 데이터 보호를 위한 IBM Guardium

- IBM Guardium은 개인정보 식별을 기반으로 암호화를 비롯하여, 권한/접근 기록 감사, 접근 통제 및 DB 취약성 평가 등을 통해 법적 규제를 충족하고 개인정보를 보호하는 데이터 보안 솔루션입니다.

전방위 데이터 보안 솔루션 IBM Guardium



IBM Guardium의 데이터 보호 전략 ANALYZE. PROTECT. ADAPT



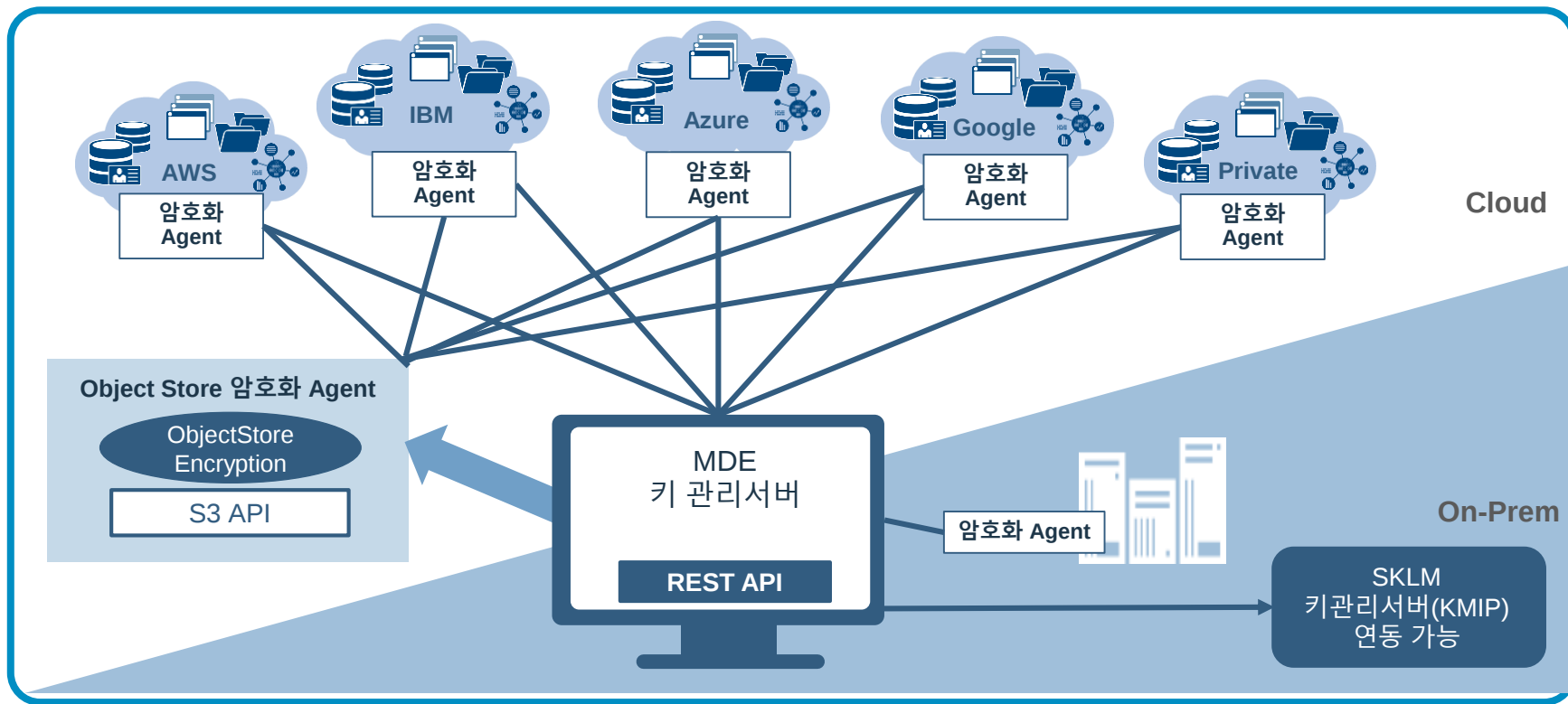


멀티 클라우드 데이터 암호화



멀티 클라우드 암호화 솔루션 Multi-Cloud Data Encryption

- 다양한 멀티 클라우드 상의 파일, 볼륨, 오브젝트 스토리지 암호화를 지원하며, 손쉬운 프로비저닝 및 Agent 적용이 가능합니다. 클라우드 간 암호화 데이터 전송, 클라우드 상의 안전한 데이터 저장 관리를 위한 암호화 분리 기능을 제공합니다.



안전한 멀티 클라우드 암호화 지원

관리 서버



데이터 접근
정책 수립



설정, 배포 및
Agent 관리



키 생성, 배포, 전환 등
관리



컴플라이언스, 감사
대비 로그 관리

암호화 Agent



볼륨 암호화



파일 암호화



Object Store
암호화

다양한 서버 보호



Bare Metal
Servers



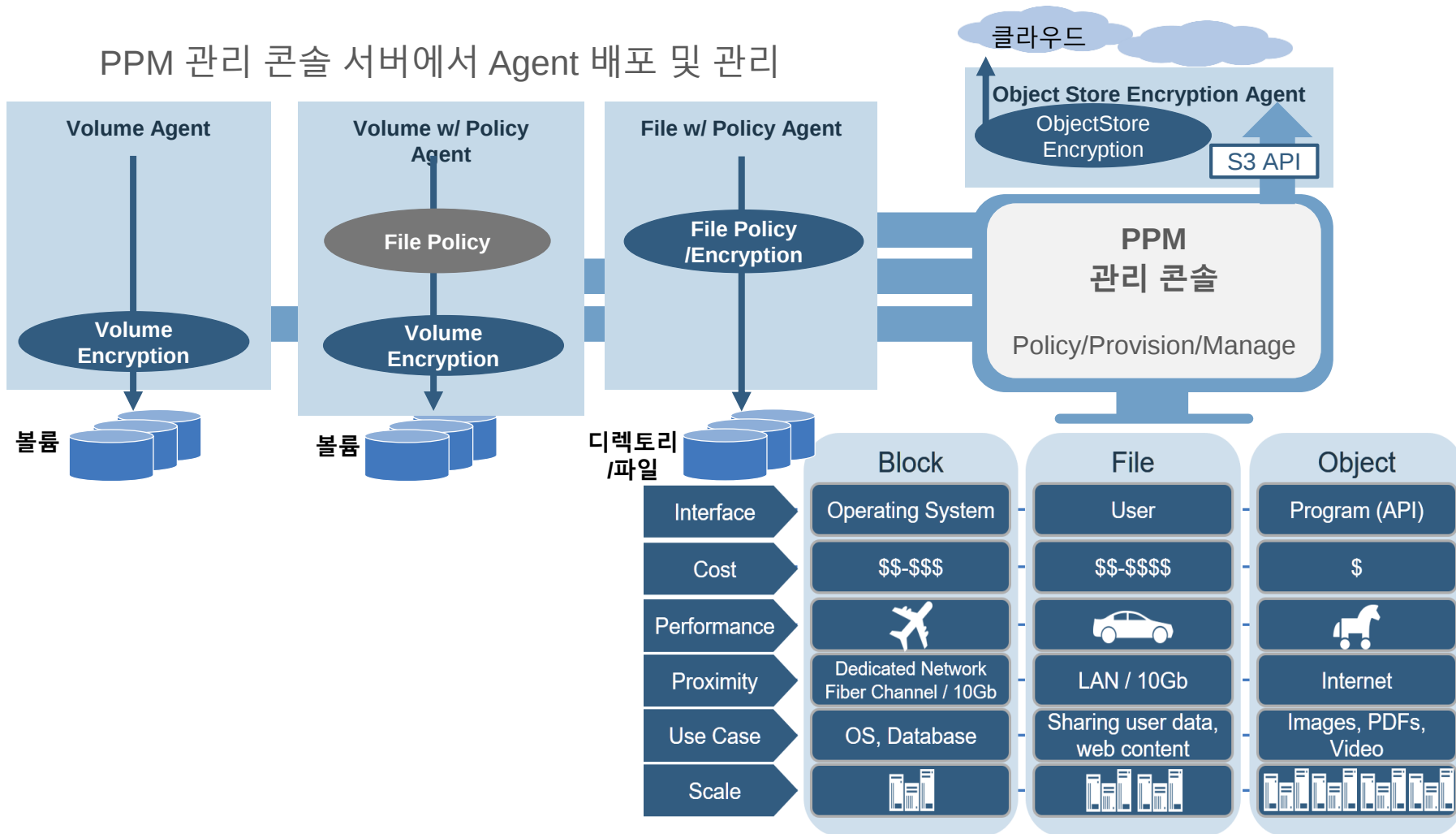
Virtual
Machines



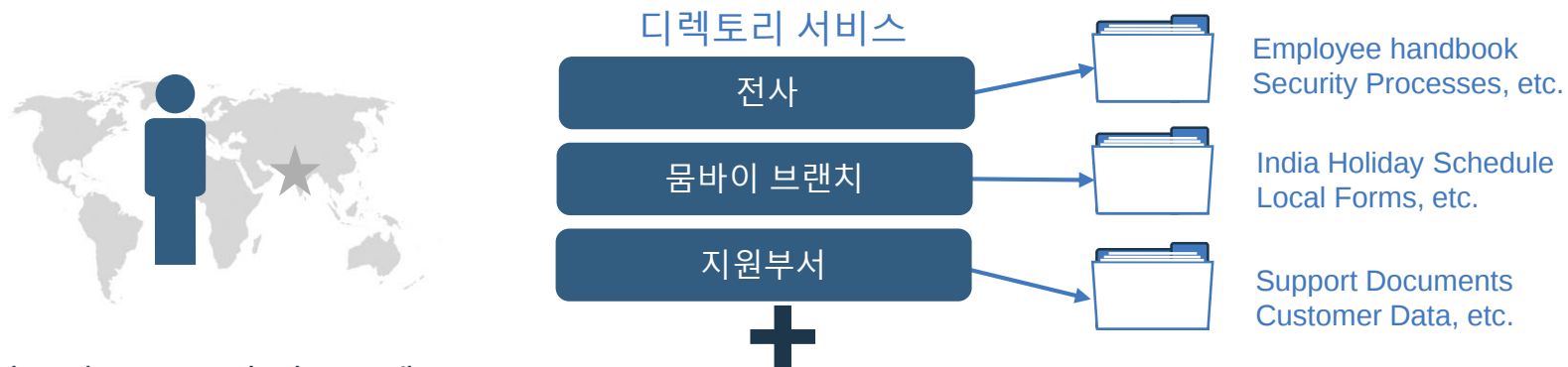
애플리케이션
/데이터베이스

특장점 > 중앙 관제 기반의 다양한 암호화 옵션

PPM 관리 콘솔 서버에서 Agent 배포 및 관리



특장점 > 사용자, 정책 기반 데이터 접근 통제 관리



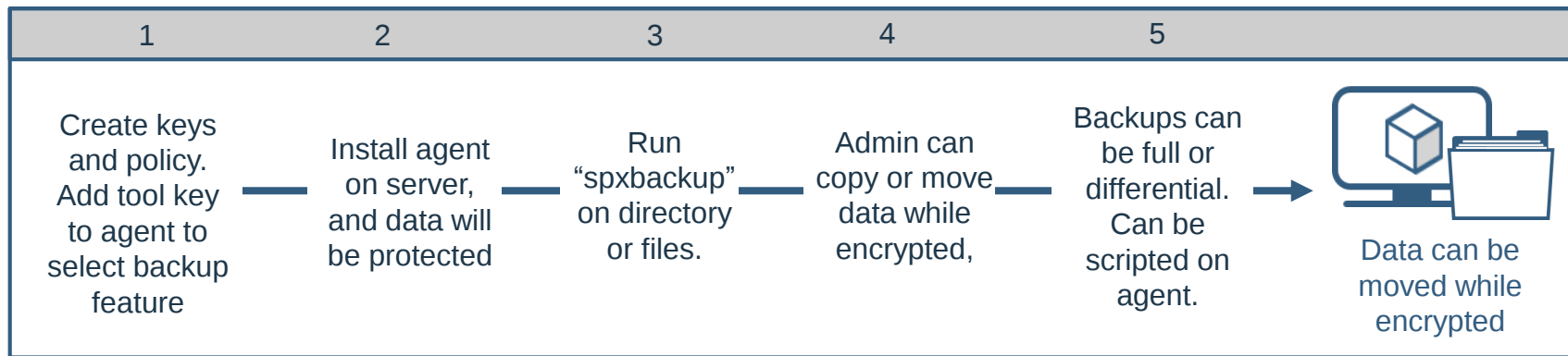
사용자, Group별 접근통제 > MDE Policy for /support/cust_data

User	Group	Action	Operation
ravi		Read and Write	Deny and Log
	All Support	Read and Write	Permit and Log
everyone_else		Read and Write	Deny and Log

프로세스별 접근 통제 > MDE Policy by Policy

User	Group	Process	Action	Operation
	DBA_team	DB_Manager	Read and Write	Permit and Log
b_admin		Data_Backup	Read and Write	Permit and Log
everyone_else			Read and Write	Deny and Log

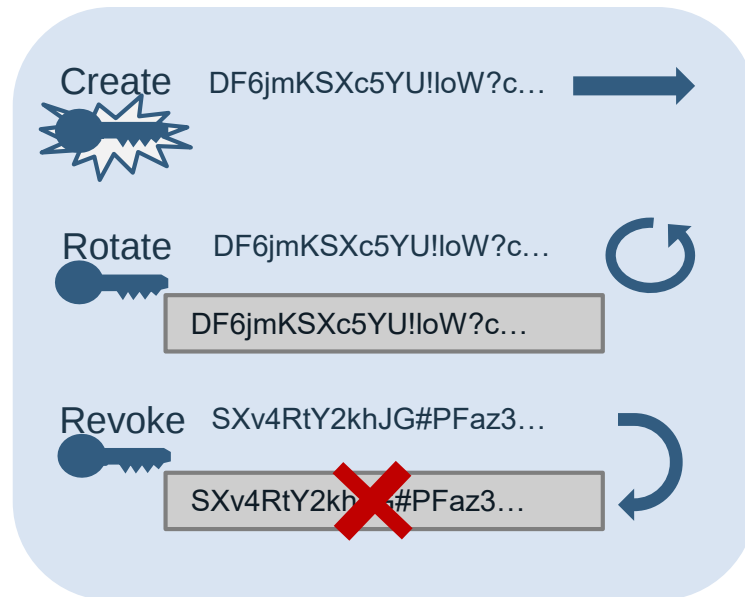
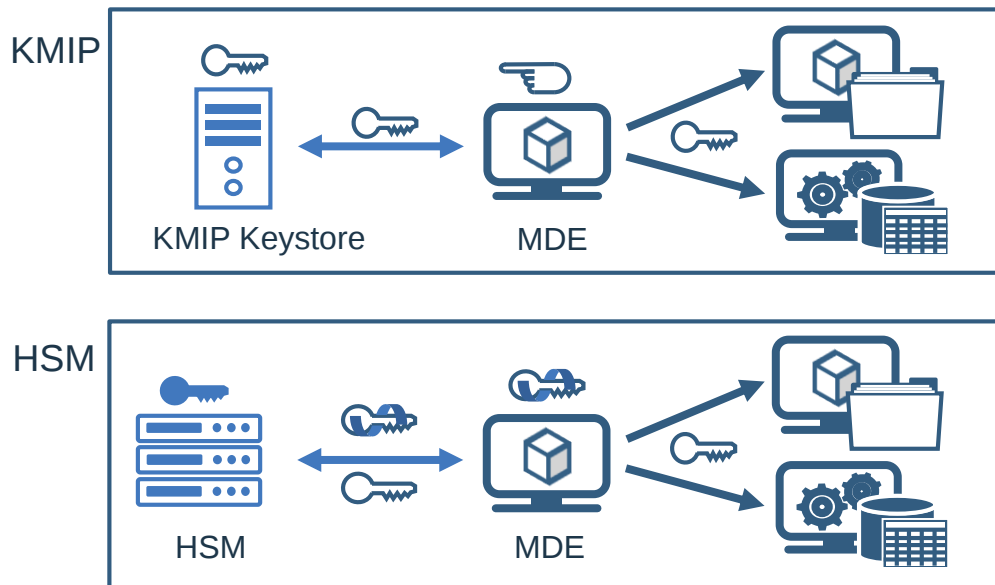
특장점 > Encrypt-in-Place 암호화



- 기존 디렉토리 암호화 지원
 - Encrypt-in-place: 운영 환경에 대한 암호화 영향 없음
 - 이중 암호화 방지 및 암호화 전후 변환 체크섬 검증
 - 암호화 내역에 대한 감사 로그
 - 사용중인 미 암호화 내역에 대한 리스트 및 전체 암호화 파일 개수 검증
 - 개인정보보호법, PCI, HIPPA 등 규제 준수를 위한 감사 증적 자료로 활용
 - 암호화 데이터의 관리 및 백업
 - Spxbackup/spxrestore 기능을 통한 키 변환 영향도 없는 백업/복원 관리

특장점 > 안전하고 손쉬운 키관리

- 표준 키 관리 프로토콜 KMIP(Key Management Interoperability Protocol) 지원
- HSM(Hardware Security Module) 연동 지원
- 손쉬운 키 관리
 - 규제 준수를 위한 Key Rotate 및 Schedule 지원(재 암호화 불필요)



Only Gemalto Luna HSM is validated and supported for MDE 2.2 through extended PKCS#11. Roadmap HSM validation / integration is customer / market driven
Only key storage in IBM SKLM and Gemalto KeySecure are validated and supported for MDE 2.2 through KMIP.

특장점 > 실시간 모니터링 및 관리편의성

- 관리콘솔 설정 및 관리 내역에 대한 로그
- 암호화 정책 및 에이전트 정의, 생성 및 배포 관리 로그
- 데이터 암호화 로그
- 한글 UI 지원



IBM Multi-Cloud
Data Encryption



Keys

Policy

Agents

Jobs

Events

Users

Settings

Last 10 Events

Reload

System Events

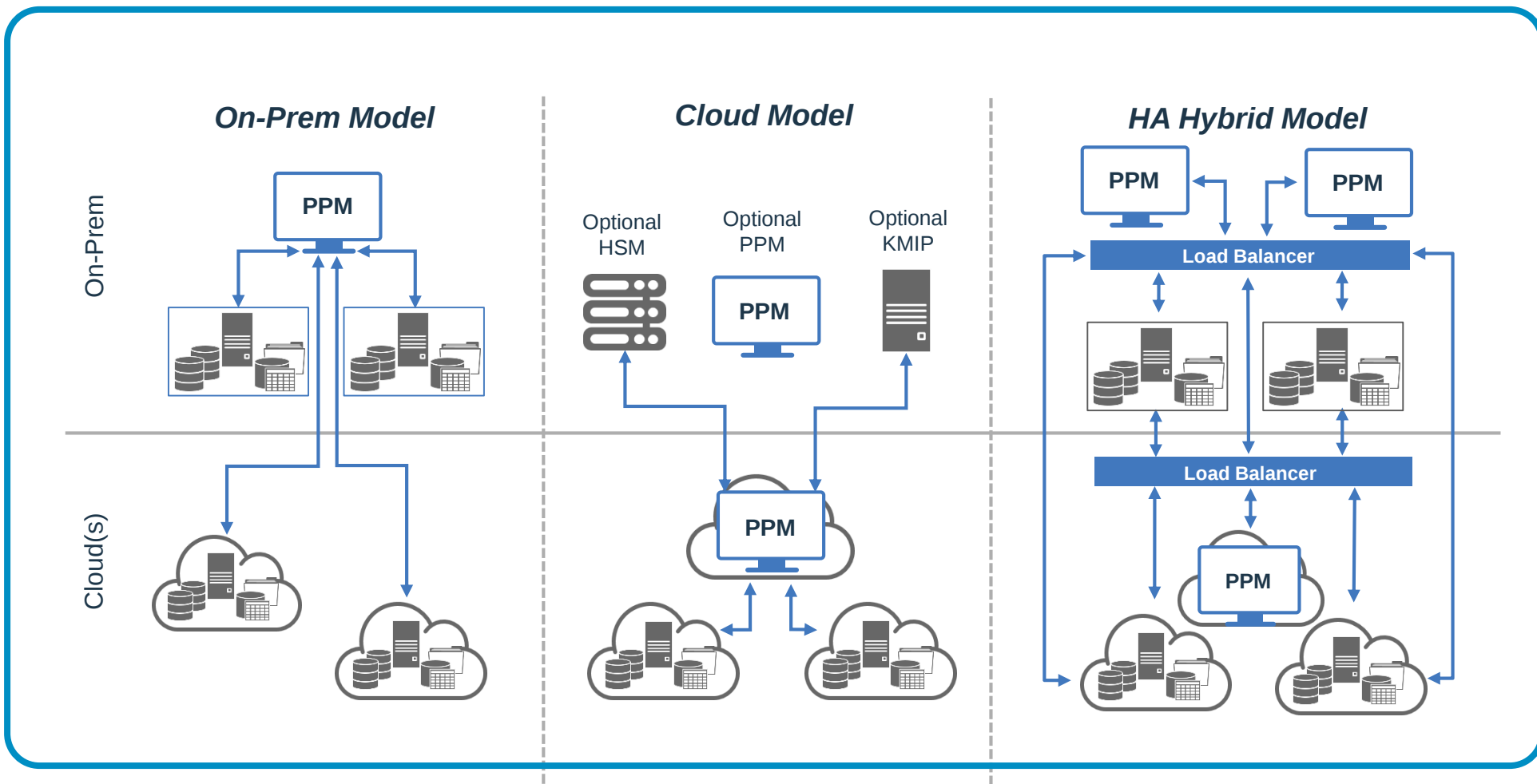
Info

Timestamp	Severity	Source	Description
2017-06-16 16:52:24.103	INFO	AUDIT	Policy look-up deny[path: E:\Data\Protected] [ui
2017-06-16 16:51:38.102	INFO	SYSTEM	Policy was deployed to agent 10.6.60.96.
2017-06-16 16:51:38.101	INFO	SYSTEM	Protection deployment job for agent 10.6.60.96
2017-06-16 16:51:38.100	INFO	AUDIT	User admin created a job to deploy policy to age

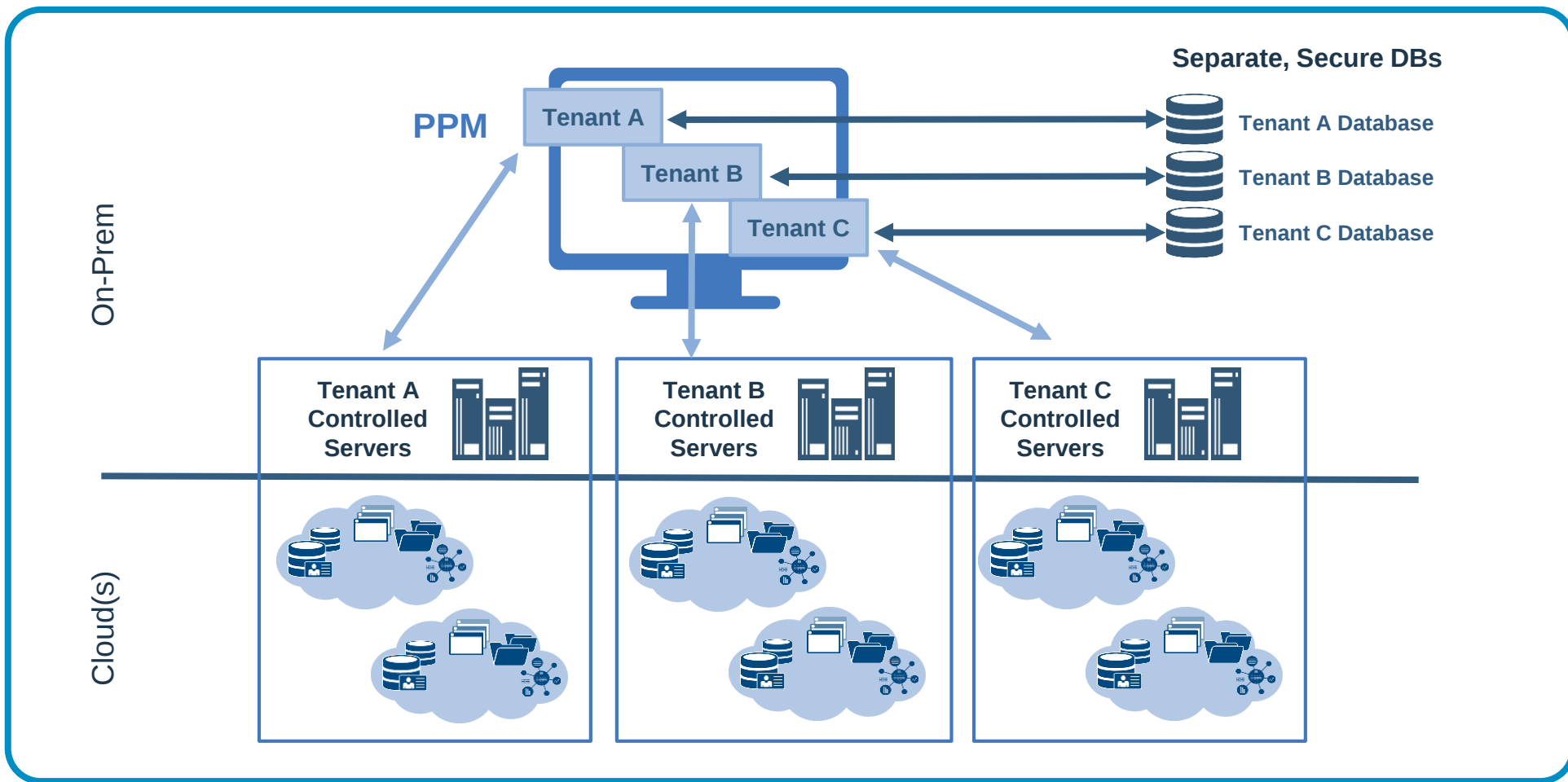
Language

- English
- deutsch
- English
- español
- français
- italiano
- 日本語
- 한국어
- português
- русский
- 普通话
- 國語

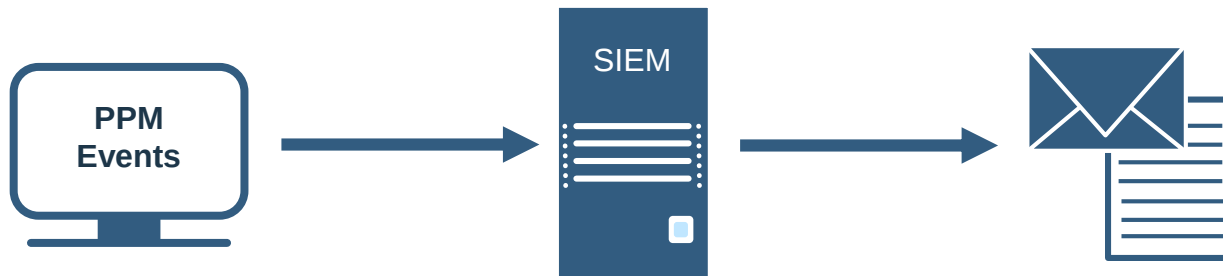
아키텍처 > 다양한 환경과 멀티테넌시를 지원하는 유연한 구성 지원



아키텍처 > 다양한 환경과 멀티테넌시를 지원하는 유연한 구성 지원



아키텍처 > SIEM 솔루션과의 연동



splunk >

Search last

_time	msg	src
2017-07-26 13:36:12	Policy look-up deny [path:/protected/passwd][uid:user02][gid:user02] [process:/usr/bin/head][rule:1][flags:32,768]	10.6.1.49
2017-07-26 13:35:04	Policy look-up deny [path:/protected/passwd2][uid:user02][gid:user0] [process:/usr/bin/cp][rule:1][flags:1]	10.6.1.49

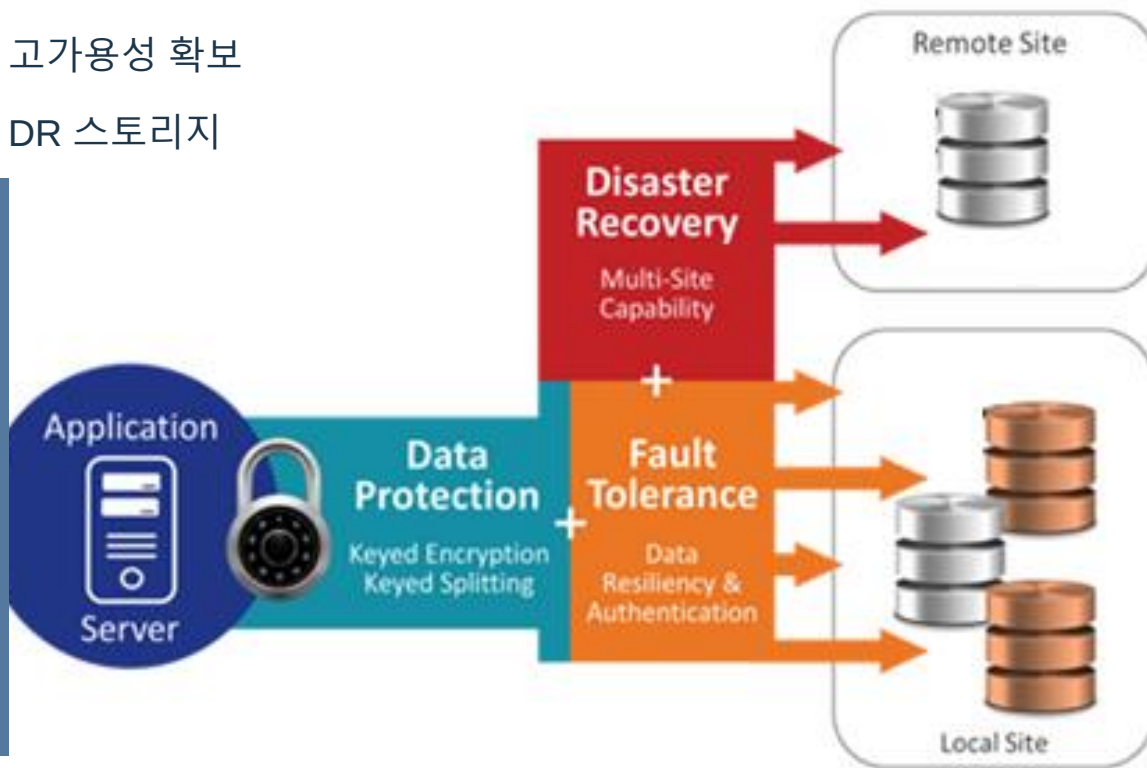


MDE 활용 사례



MDE 활용 사례

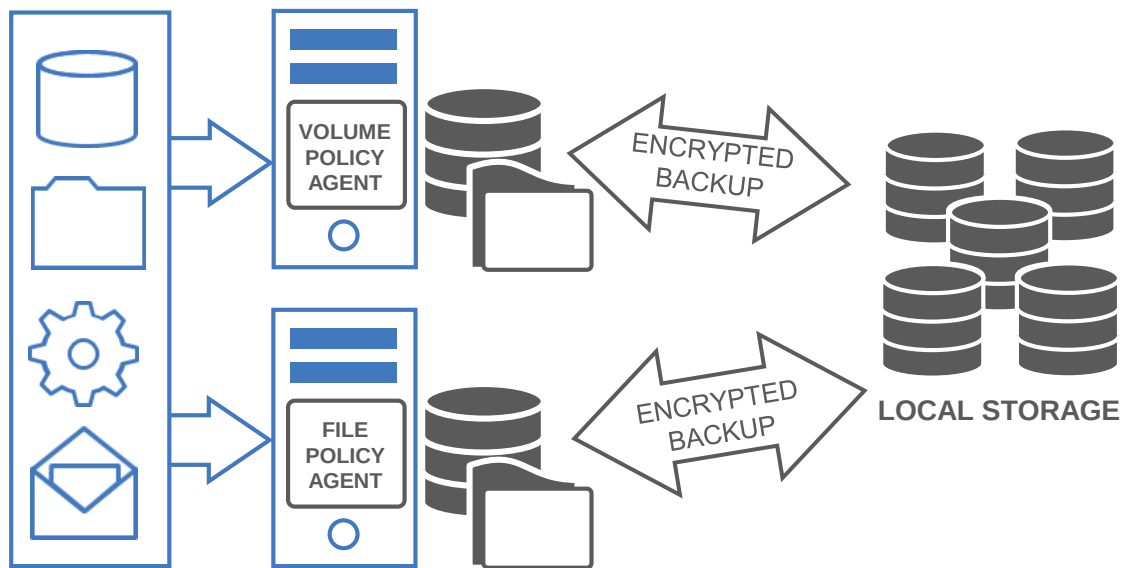
1. 컴플라이언스 지원
2. 안전한 데이터 백업
3. 오브젝트 스토리지 암호화 및고가용성 확보
4. 랜섬웨어 대비 클라우드 기반 DR 스토리지



활용 사례 > 컴플라이언스 지원

- **Payment Card Industry Data Security Standard (PCI DSS)**
- **Sarbanes-Oxley Act (SOX)**
- **Health Insurance Portability and Accountability Act (HIPAA)**
- **General Data Protection Regulation (GDPR)**
 - **Article #5 - Principles relating to processing of personal data**
 - Access controls can track who has access to what data.
 - Logs can show when data was created, who used it, and when it was deleted for audit purposes.
 - **Article #17 - Right to erasure ('right to be forgotten')**
 - Encryption offers a means to destroy personal data. By deleting the key, data is cryptographically shredded.
 - **Article #25 - Data protection by design and by default**
 - Encrypt data-at-rest and protect it from the moment of creation or collection while stored on a server asset.
 - Access can be controlled by application and monitored for permit/deny access permissions
 - Full set of RESTful API allows integration into IT process for Security by Design, Security by Default
 - **Article #32 - Security of processing**
 - Data protection at the server file or volume level, as well as object storage is compatible with most existing IT environments.
 - **Article #33 - Notification of a personal data breach to the supervisory authority**
 - Access Logging forwarded to a SIEM analytic engine for real time awareness of potential infiltration risk.
 - **Article #34 - Communication of a personal data breach to the data subject**
 - Access controls, monitoring and pseudonymisation can lessen requirements to notify unauthorized events.

Built-in Encrypted Copy / Backup / Restore



Clear Text

Encrypted / Decrypted per MDE Policy and Keys

When Nobody Controls Your Object Stores — Except You

April 18, 2018 | By Rick Robinson



In recent months and years, we have seen the benefit of low-cost object stores offered by cloud service providers (CSPs). In some circles, these are called "Swift" or "S3" stores. However, as often as the topic of object or cloud storage emerges, so does the topic of securing the data within those object stores.

CSPs often promise that their environments are secure and,



in some cases, that the data is protected through encryption — but how do you know for sure?

Ransomware Recovery: Maintain Control of Your Data in the Face of an Attack

June 12, 2018 | By Rick Robinson



Imagine the panic and concern that hits as you look at a screen that says: "All files on your computer have been locked. Please pay the ransom within 24 hours to get the key ... or else."

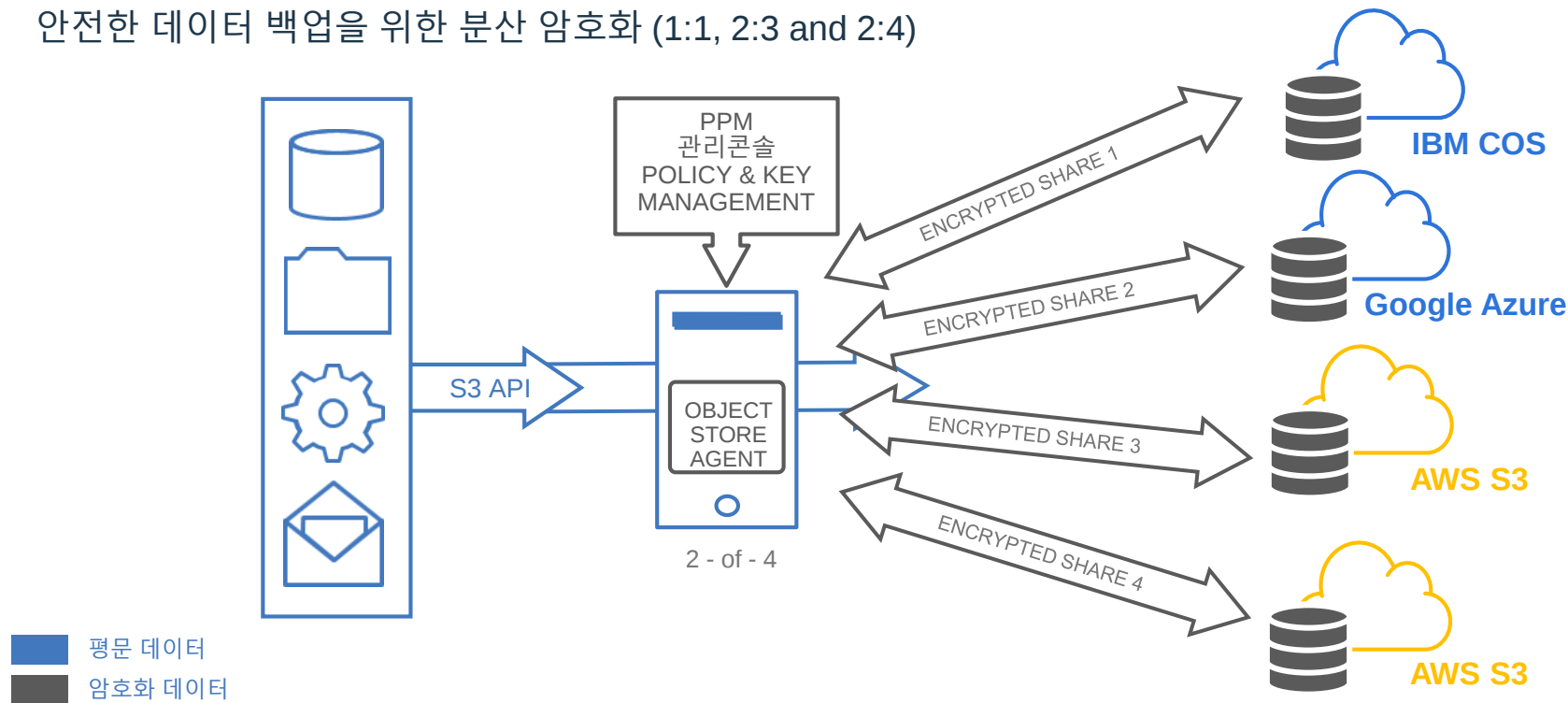
From the days of ransomware being distributed on floppy disks to modern-day attacks like WannaCry and Petya spreading around the world in minutes, this may be your



image of ransomware recovery. Ransomware either locks your computer or your data before demanding a fee in exchange for the supposed safe return of your critical assets.

활용 사례 > 오브젝트 스토리지 암호화 및 고가용성 확보

- 표준 S3 스토리지 요건 지원
- Object Store를 위한 프록시. S3 API 지원
- 안전한 데이터 백업을 위한 분산 암호화 (1:1, 2:3 and 2:4)



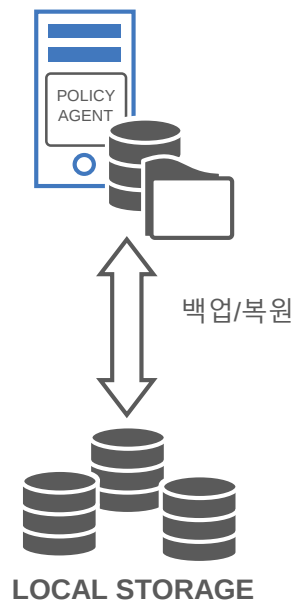
활용 사례 > 랜섬웨어 대비 클라우드 기반 DR 스토리지

암호화된 백업/복원

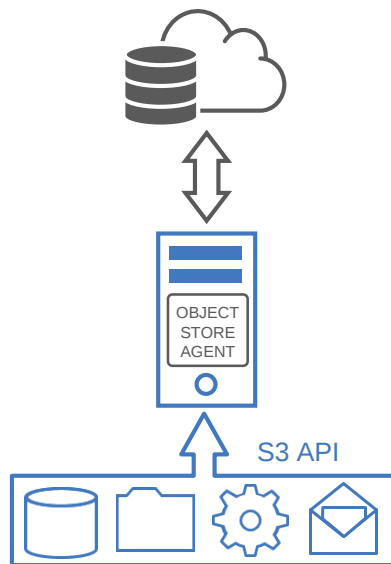


저비용 클라우드 오브젝트
스토리지 활용

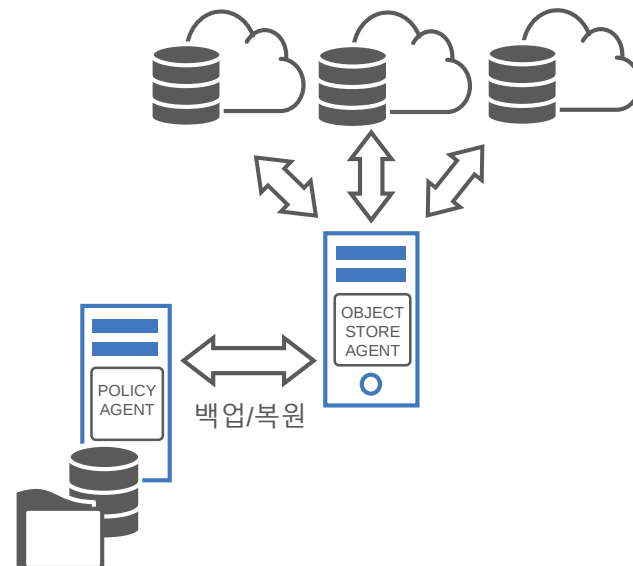
Geo Distributed Archive/Recovery



S3 OBJECT STORAGE



S3 OBJECT STORAGE



■ 평문 데이터
■ 암호화 데이터



사례 및 맺음말



고객 성공 사례



- Crohn's & Colitis Foundation of America (CCFA)

- Who?

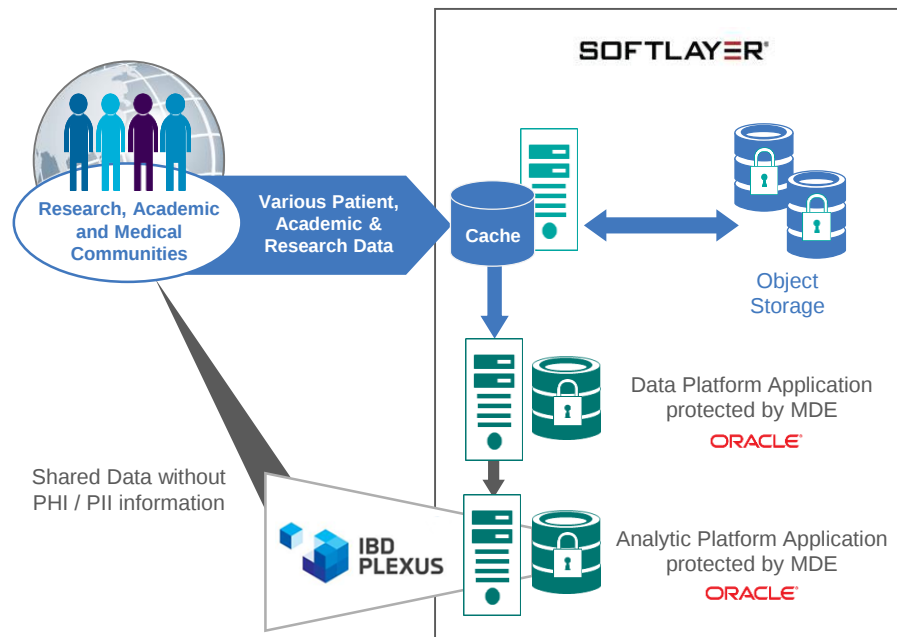
- Non-profit dedicated to finding cures for Crohn's Disease and ulcerative colitis.

- Need

- Protect patient info in public database
 - Personal Healthcare Information (PHI)
 - Personally Identifiable Information (PII)
- Comply with the federal and state privacy laws
 - HIPAA/HITECH healthcare compliance.

- Solution

- IBM Cloud hosted infrastructure for their applications
- MDE used to secure data



데이터 보안 시장을 선도하는 IBM

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

Awarded highest score in overall "Market Presence"

Awarded highest score in overall "Strategy"

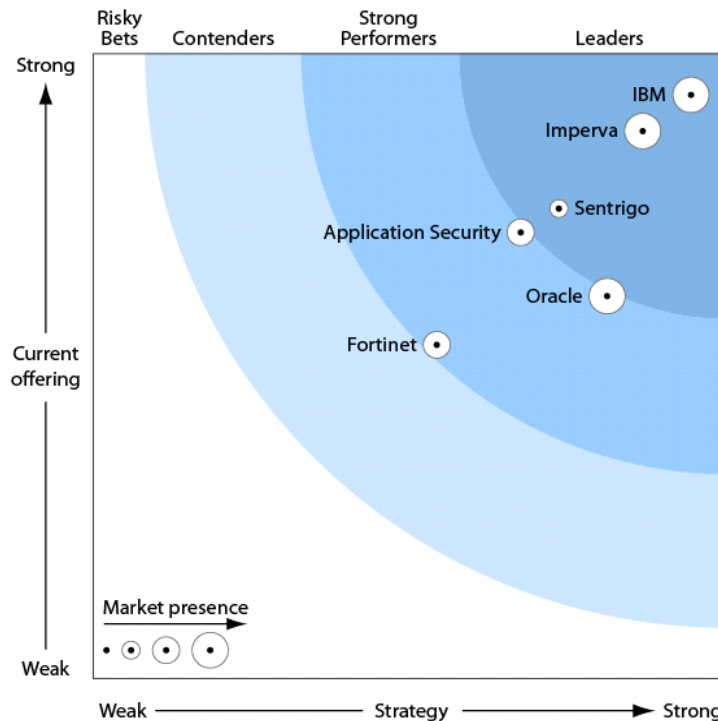
Awarded highest score in evaluation of "Current Offering"

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

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



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.

전문가들이 인정한 검증된 솔루션



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



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



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



*"Most Powerful Compliance
Regulations Tools ... Ever"*



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



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



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



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*



The most recognized name

in PCs *Protecting over 7 million
credit card transactions per year*



8 of the top 10 telcos worldwide

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





THANK YOU

FOLLOW US ON:



ibm.com/security



securityintelligence.com



xforce.ibmcloud.com



[@ibmsecurity](https://twitter.com/ibmsecurity)



youtube/user/ibmsecuritysolutions

© Copyright IBM Corporation 2016. All rights reserved. The information contained in these materials is provided for informational purposes only, and is provided AS IS without warranty of any kind, express or implied. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, these materials. Nothing contained in these materials is intended to, nor shall have the effect of, creating any warranties or representations from IBM or its suppliers or licensors, or altering the terms and conditions of the applicable license agreement governing the use of IBM software. References in these materials to IBM products, programs, or services do not imply that they will be available in all countries in which IBM operates. Product release dates and / or capabilities referenced in these materials may change at any time at IBM's sole discretion based on market opportunities or other factors, and are not intended to be a commitment to future product or feature availability in any way. IBM, the IBM logo, and other IBM products and services are trademarks of the International Business Machines Corporation, in the United States, other countries or both. Other company, product, or service names may be trademarks or service marks of others.

Statement of Good Security Practices: IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a lawful, comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective.

IBM DOES NOT WARRANT THAT ANYSYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.