ORACLE

MySQL Security

류수미
MySQL Principal Solution Engineer
JAPAC, MySQL Global Business Unit
2021년 10월 21일

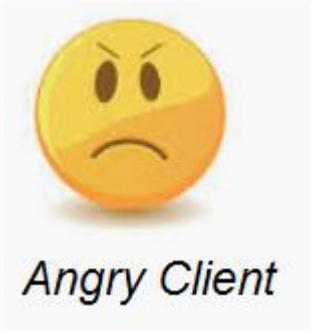
Safe Harbor Statement

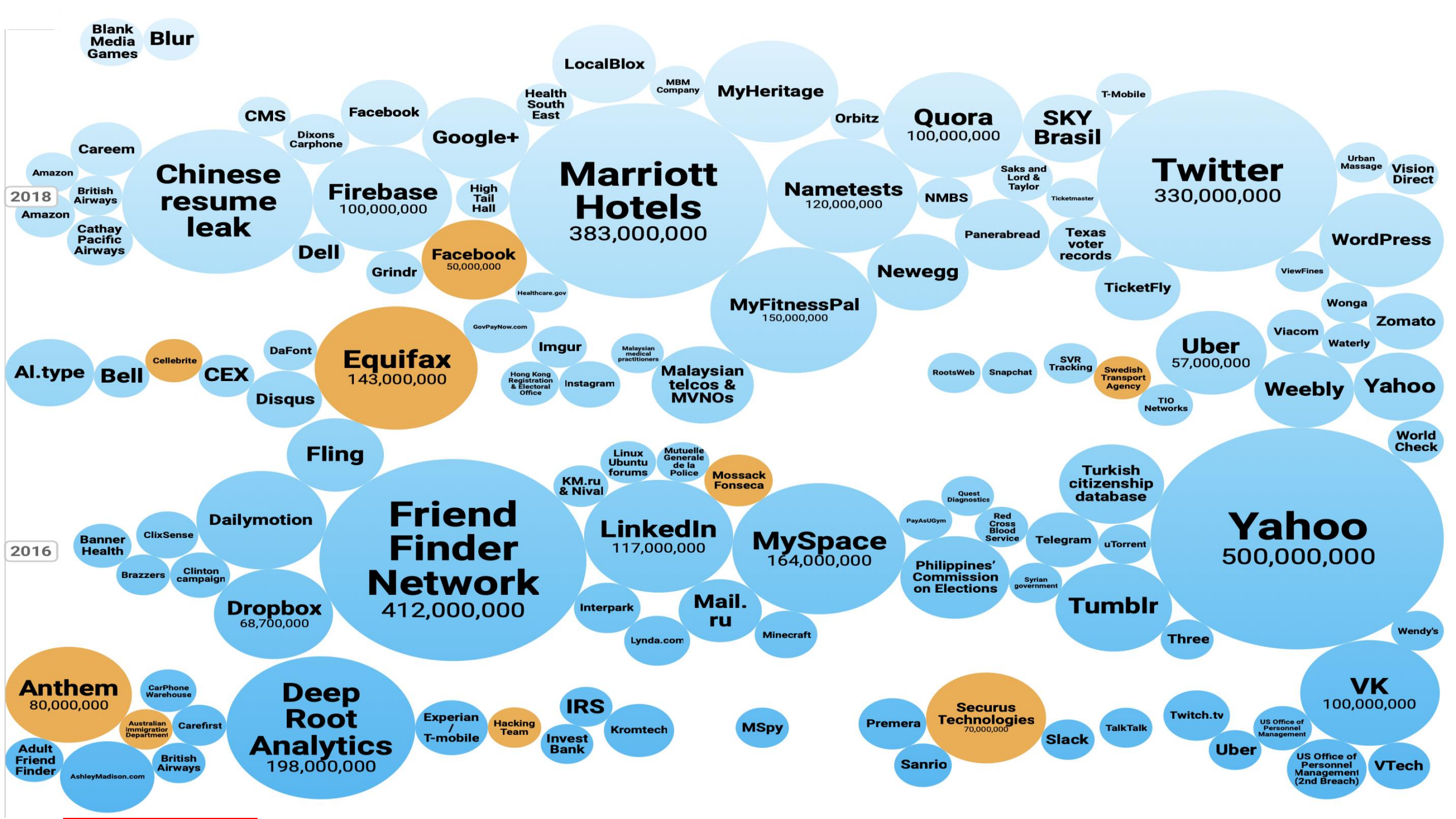
The following is intended to outline our general product direction. It is intended for information purposes only, and may not be incorporated into any contract. It is not a commitment to deliver any material, code, or functionality, and should not be relied upon in making purchasing decisions. The development, release, timing, and pricing of any features or functionality described for Oracle's products may change and remains at the sole discretion of Oracle Corporation.

목차

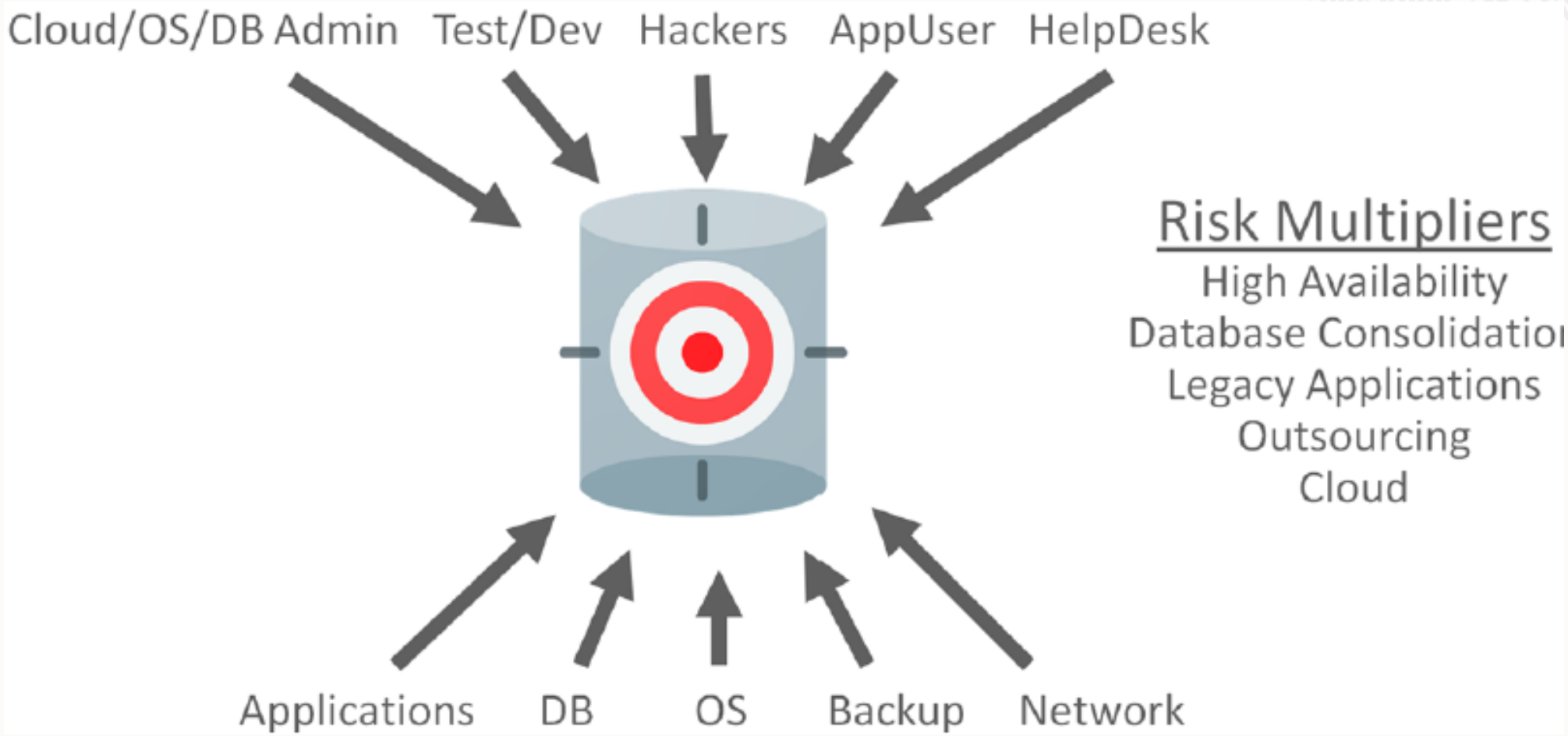
1. 보안 과제
2. MySQL 보안 기능
3. MySQL Enterprise 보안 기능
4. MySQL Security 데모

보안 과제




2018
2016
Blank Media Games
Blur
LocalBlox
MBM Company
MyHeritage
Health South East
Facebook
CMS
Dixons Carphone
Google+
Orbitz
Quora
100,000,000
T-Mobile
SKY Brasil
Careem
Amazon
Chinese resume leak
Firebase
100,000,000
High Tail Hall
Marriott Hotels
383,000,000
Nametests
120,000,000
NMBS
Saks and Lord & Taylor
Ticketmaster
Twitter
330,000,000
Urban Massage
Vision Direct
British Airways
Amazon
Cathay Pacific Airways
Dell
Grindr
Facebook
50,000,000
Panerabread
Texas voter records
WordPress
Newegg
ViewFines
TicketFly
Healthcare.gov
GovPayNow.com
MyFitnessPal
150,000,000
Wonga
Zomato
Viacom
Waterly
Uber
57,000,000
Al.type
Bell
Cellebrite
CEX
DaFont
Disqus
Equifax
143,000,000
Imgur
Malaysian medical practitioners
Hong Kong Registration & Electoral Office
Instagram
Malaysian telcos & MVNOs
RootsWeb
Snapchat
SVR Tracking
Swedish Transport Agency
TIO Networks
Weebly
Yahoo
Fling
World Check
Linux Ubuntu forums
Mutuelle Generale de la Police
Mossack Fonseca
KM.ru & Nival
Turkish citizenship database
Quest Diagnostics
PayAsUGym
Red Cross Blood Service
Telegram
uTorrent
Yahoo
500,000,000
Dailymotion
Friend Finder Network
412,000,000
LinkedIn
117,000,000
MySpace
164,000,000
Philippines' Commission on Elections
Syrian government
Banner Health
ClixSense
Brazzers
Clinton campaign
Dropbox
68,700,000
Interpark
Mail.ru
Lynda.com
Minecraft
Tumblr
Three
Wendy's
Anthem
80,000,000
CarPhone Warehouse
Australian Immigration Department
Carefirst
Deep Root Analytics
198,000,000
Experian / T-mobile
Hacking Team
IRS
Invest Bank
Kromtech
MSpy
Premera
Securus Technologies
70,000,000
Sanrio
Slack
TalkTalk
Twitch.tv
Uber
US Office of Personnel Management
US Office of Personnel Management (2nd Breach)
VK
100,000,000
VTech
Adult Friend Finder
AshleyMadison.com
British Airways

복잡성 심화에 따른 보안 위기 확대



데이터 보안 및 개인 정보 보호 규정의 확산

NCUA | 50 State Privacy Laws | Patriot Act | GLBA

FS-ISAC | FFIEC | Dodd Frank | NY DFS500

CIS Benchmarks™

공통 요구사항

- ❑ 지속적인 모니터링 (Users, Schema, Backups, etc)
- ❑ 데이터 보호 (Encryption, Privilege Management, etc.)
- ❑ 데이터 보관 (Backups, User Activity, etc.)
- ❑ 데이터 감사 (User activity, etc.)

규제 준수

규정

- PCI – DSS: 결제 카드 데이터
- HIPAA - 의료 데이터 보호
- Sarbanes Oxley, GLBA, 미국 애국자법:
  금융 데이터, NPI "개인 식별 금융 정보"
- FERPA – 학생 데이터
- EU 일반 데이터 보호 지침: 개인 데이터 보호(GDPR)
- 데이터보호법(영국): 개인 정보 보호

요구사항

- 지속적인 모니터링(사용자, 스키마, 백업 등)
- 데이터 보호(암호화(Encryption), 권한 관리 등)
- 데이터 보관 (백업, 사용자 활동 등)
- 데이터 감사 (사용자 활동 등)

93%

예방 가능한 보안 침해 -
Online Trust Alliance(인터넷 협회)

피할 수 있는 주요 사고 원인

- 내부, 서드파티, 클라우드 기반의 시스템과 서비스 등 전체적인 위험 평가의 결여
- 알려진 취약점 또는 공개된 취약점에 대해 즉시 패치를 적용하지 않았거나, 취약점 보고서를 확인했지만 처리할 방법이 없는 경우
- 잘못 구성된 장치/서버
- 암호화되지 않은 데이터 또는 암호화 키의 관리 및 보호 미흡
- 제품의 수명 주기 종료(EOL) 후 지원되지 않는 장치, 운영 체제, 애플리케이션 사용
- 직원의 실수 및 우발적인 공개 — 데이터, 파일, 드라이브, 장치, 컴퓨터의 분실 및 부적절한 폐기
- 악성 전자메일 차단 실패
- 사용자가 비즈니스 전자메일 사칭 공격(BEC) 및 소셜 악용에 굴복

고객사의 보안팀에 물어봐야 할 열 가지 질문

- 보안 팀과 데이터 관리/운영 팀이 잘 조율되어 있습니까?
- 무료 데이터베이스가 확산하는 상황에서 이 환경을 규제할 강력한 거버넌스 또는 청사진이 있습니까?
- 데이터베이스 로그인이 기업 표준 및 거버넌스를 충족합니까?
- 내부 침해에 대비해서 보호하고 있습니까?
- 데이터베이스를 노리는 해커가 웹 페이지를 통해 직접 침입하여 SQL 인젝션 공격을 할 수 있습니까?
- 파트너에게 보기 기능을 제공하는 경우 개인 식별 정보를 마스킹할 수 있습니까?
- 문제를 발견한 후 누가 데이터에 액세스하고 있는지 추적할 수 있습니까?
- 침해가 발생한 데이터 보안 조건 및 변경사항에 대해 경고할 수 있습니까?
- 데이터는 암호화되어 있습니까?
- GDPR이나 CPPA와 같은 규정 표준을 준수/위반에 대한 여러분 회사의 위험 수준은 어느 정도입니까?

MySQL Database를 보호하는 방법?

데이터베이스 보안 위험 관리에 대한 4가지 접근 방법

공통 요구사항

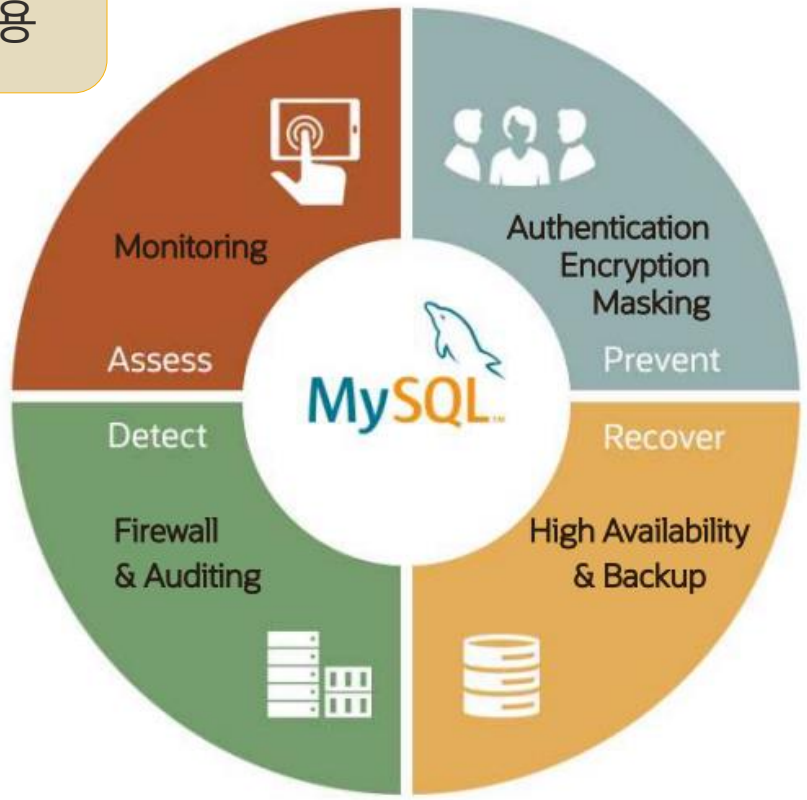
- ❑ 지속적인 모니터링 (Users, Schema, Backups, etc)
- ❑ 데이터 보호(Encryption, Privilege Management, etc.)
- ❑ 데이터 보관 (Backups, User Activity, etc.)
- ❑ 데이터 감사 (User activity, etc.)

위험 및 취약점 확인, 필요한 보안 제어 적용

Assess
- MySQL Enterprise Monitor

여전히 존재하는 유출 가능성 – 감사, 모니터링, 경고

Detect
- MySQL Enterprise Audit
- MySQL Enterprise Firewall



암호화, 사용자 제어, 액세스 제어 등 사용

Prevent
- MySQL Enterprise Authentication
- MySQL Enterprise Firewall
- MySQL Enterprise Encryption
- MySQL Enterprise Data Masking

보안 사고로 인해 서비스가 중단되지 않도록 함

메인 데이터베이스가 중단되더라도 RTO 및 RPO 목표를 보장하여 기업을 보호

Recover
- MySQL Enterprise HA
- MySQL Enterprise Backup

MySQL 보안

MySQL 보안

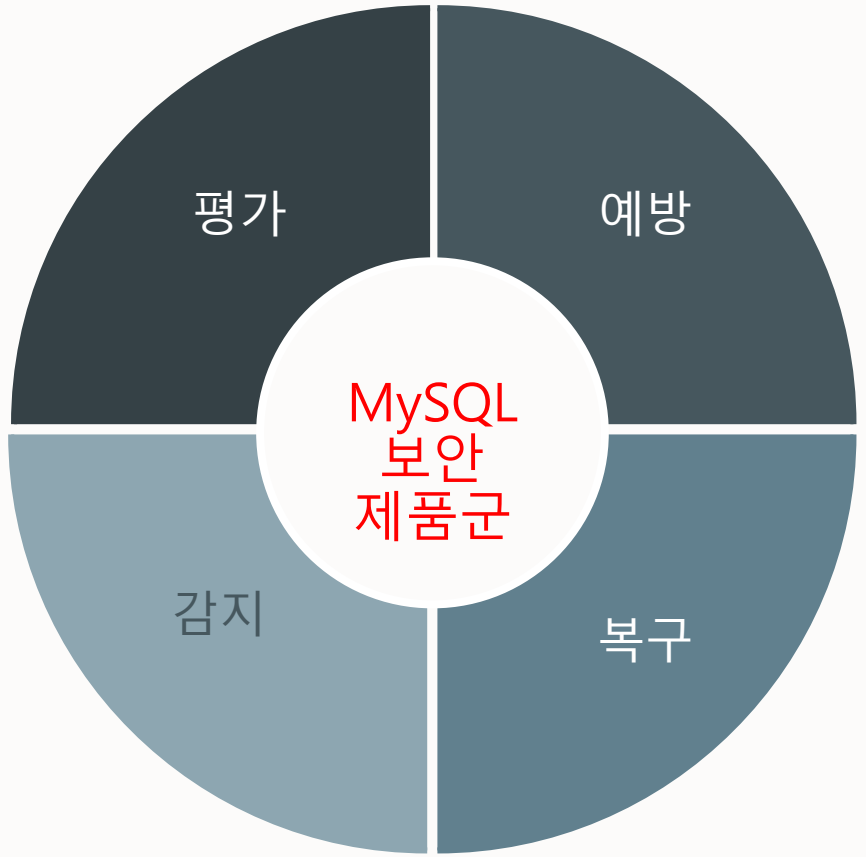
MySQL 전체 에디션

- MySQL Community Edition
- MySQL Standard Edition
- MySQL Classic Edition
- MySQL as an Embedded Database
- MySQL Enterprise Edition
- MySQL Cluster CGE

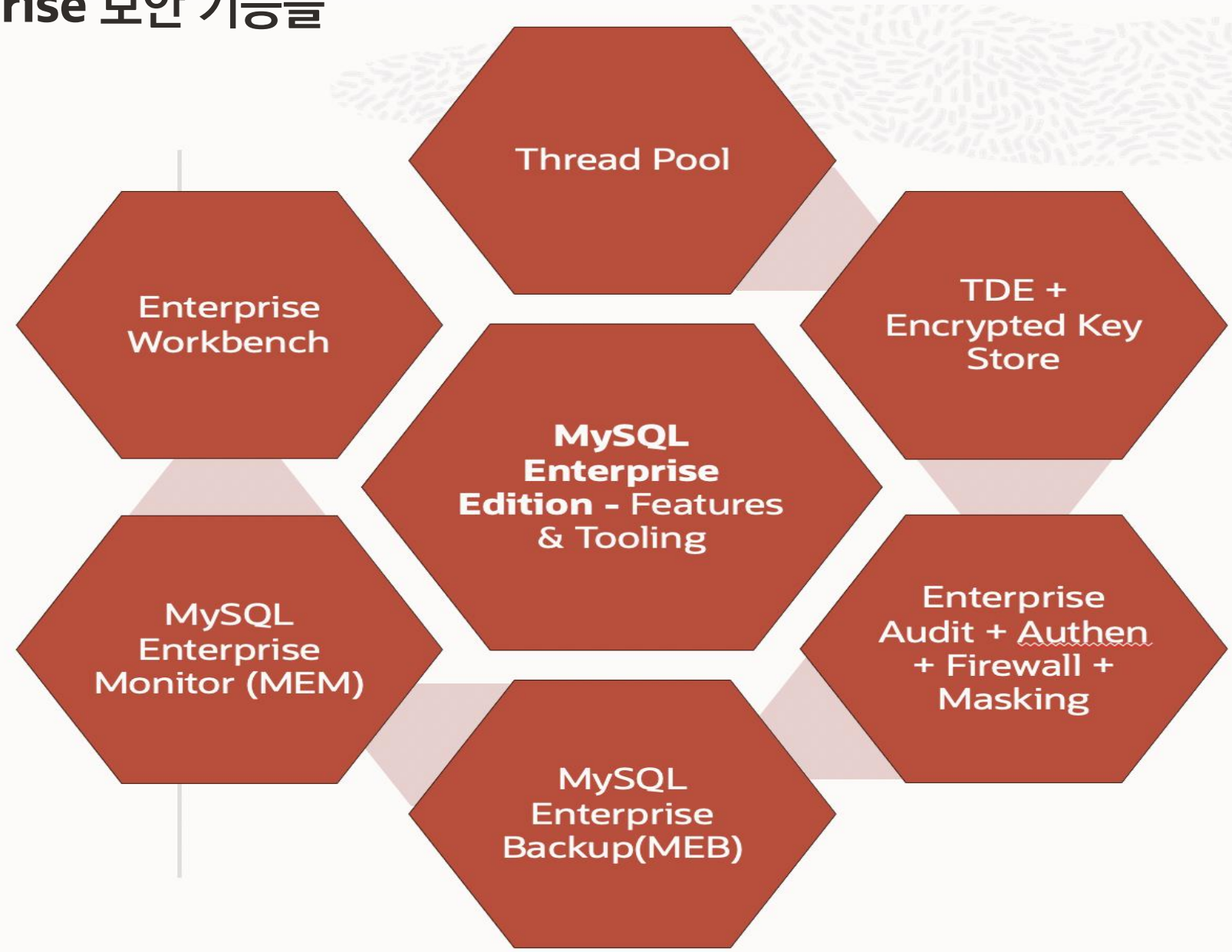
MySQL Enterprise Security

MySQL Enterprise Edition/Cluster

- MySQL Enterprise Edition
- MySQL Cluster CGE



MySQL Enterprise 보안 기능들



MySQL 보안

모든 MySQL 에디션을 위한 기본 보안 기능

MySQL 보안

- 다운로드한 패키지의 무결성을 확인하는 MD5 체크섬 및 GnuPG(GNU Privacy Guard) 서명
- 기본적으로 보안 설치
- 기본 SHA-256 인증
- 암호 검증 및 관리 구성요소
- 플러그블 방식의 인증

- 클라이언트-서버 간 연결을 TLS로 암호화
- FIPS 모드 지원
- 관리자를 위한 별도의 네트워크 인터페이스
- 계정 리소스 제한
- 사용자 롤
- 권한 부여

MySQL 보안 설치

MySQL_Secure_Installation - MySQL 설치 보안 강화

- 루트 계정에 대해 **강력한** 암호 설정
- 로컬 호스트 밖에서 액세스할 수 있는 루트 계정 제거
- 익명의 사용자 계정 제거
- 테스트 데이터베이스 제거
  - 기본적으로 모든 사용자가 액세스할 수 있는 데이터베이스
  - 익명의 사용자 포함

MySQL 암호 기능

암호 관리

- 기존 암호를 재사용하는 것이 아니라 새 암호 요구 - 변경 횟수 및/또는 사용 기간으로 제어
- 암호 재사용 정책을 계정별 설정 및 global 설정
- 암호를 변경할 때도 기존 암호를 요구

캐싱을 이용한 SHA2. 이제 기본으로 제공됩니다! (caching_sha2_password)

- 강력한 성능(저장 시)과 빠른 속도(연결 시)
  - 강력한 SHA-256 암호 해싱
  - 빠른 캐싱: 대기 시간 대폭 단축

원활한 RSA 암호 교환 기능

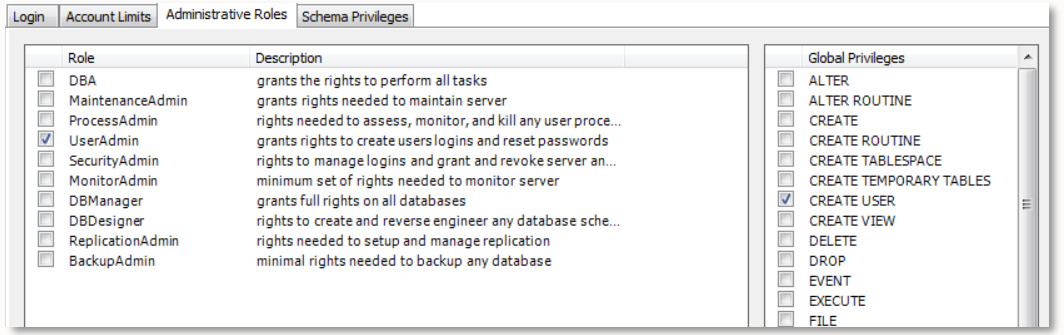
이중 암호 지원

MySQL 권한 부여

관리 권한
데이터베이스 권한
세션 제한 및 객체 권한
사용자 권한을 세부적으로 제어

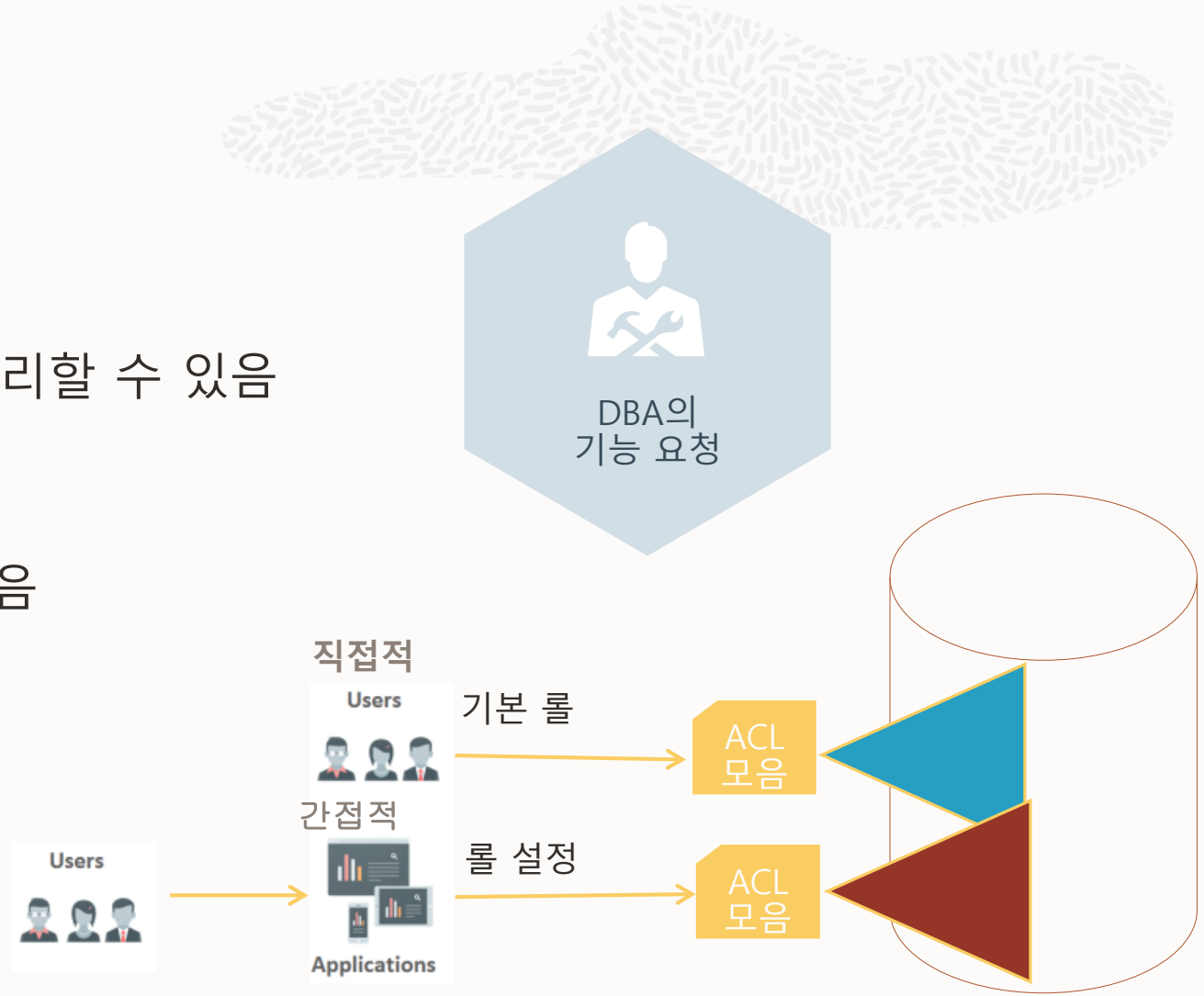
- 데이터베이스 생성, 변경, 삭제
- 테이블 생성, 변경, 삭제
- INSERT, SELECT, UPDATE, DELETE Query 실행
- 필요한 권한으로 내장 프로시저 생성, 실행 또는 삭제
- 인덱스 생성 또는 삭제

MySQL Workbench의 보안 권한 관리



MySQL 롤

MySQL 액세스 제어 향상
8.0 버전에서 도입됨
사용자 및 애플리케이션 권한을 더 쉽게 관리할 수 있음
최대한 표준 준수
여러 개의 기본 롤
롤 그래프를 GraphML로 익스포트할 수 있음



MySQL 암호화

SSL/TLS 암호화

- MySQL 클라이언트와 서버 사이
- 복제: 마스터와 복제본 사이
- 데이터 암호화
- AES 암호화/암호 해독(Decrypt)

MySQL Enterprise TDE

- 투명한 데이터 암호화
- 키 관리(KMIP)

MySQL Enterprise Encryption

- 대칭적 암호화/암호 해독
- 공개키 및 개인키 생성
- 세션 키 불러오기
- 디지털 서명

MySQL Enterprise Backup

- AES 암호화/암호 해독(Decrypt)

MySQL Enterprise Security

MySQL Enterprise 및 MySQL Cluster CGE 에디션을 위한 향상된 보안 기능

MySQL Enterprise Security

MySQL Enterprise TDE
- 미사용 데이터 암호화
- 키 관리/보안

MySQL Enterprise Authentication
- 외부 인증 모듈 : Microsoft AD, Linux PAM, LDAP

MySQL Enterprise Encryption
- 공용/전용 키 암호화
- 비대칭 암호화
- 디지털 서명, 데이터 검증
- 사용자 활동 감사(Audit), 규제 준수

MySQL 데이터 마스킹

MySQL Enterprise Firewall
- SQL 주입 공격 차단
- 침입 감지

MySQL Enterprise Audit
- 사용자 활동 감사(Audit), 규제 준수

MySQL Enterprise Monitor
- 데이터베이스 구성, 유저 권한, 데이터베이스 스키마, 암호 관련 변경사항

MySQL Enterprise Backup
- 백업 보안, AES 256 암호화

MySQL Enterprise 스레드 풀
- 공격에 대한 보안 강화

MySQL Enterprise Authentication

중앙 집중식 인증 시스템과 통합

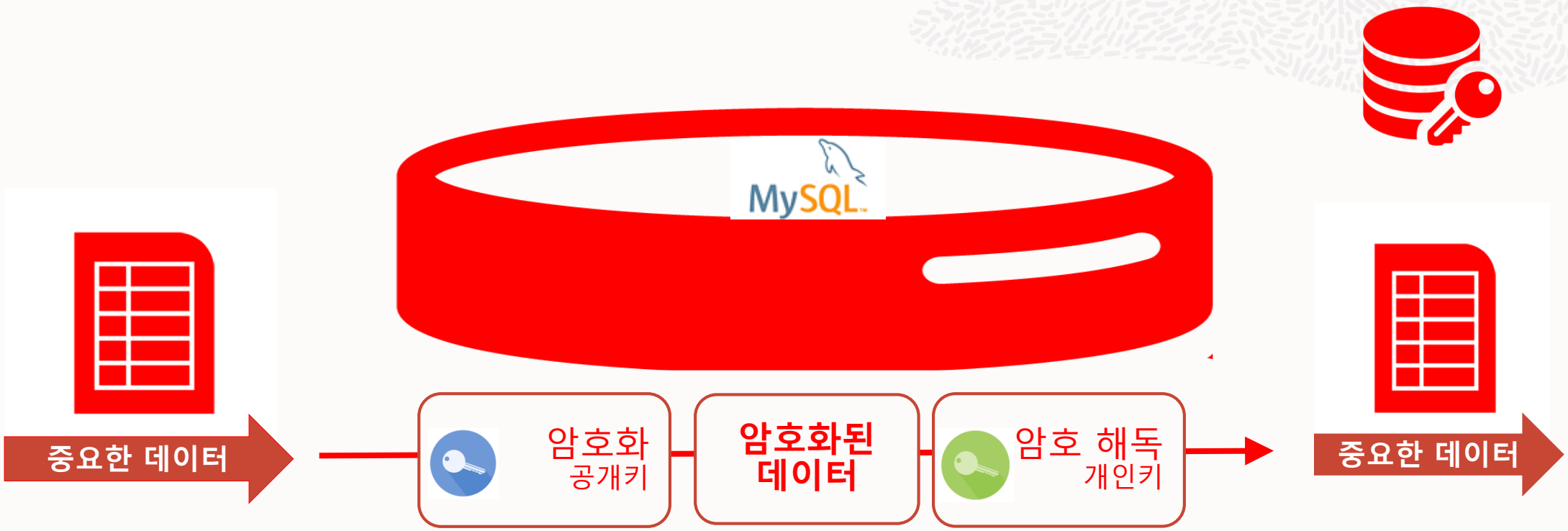
- 중앙 집중식 계정 관리
- 암호 정책 관리
- 그룹 및 롤

지원

- Windows Active Directory(Windows MySQL Server용)
- Linux PAM(Pluggable Authentication Modules)
- Native LDAP
  - 엄청나게 빠른 속도 및 유연성
  - Windows AD에서 작동(Windows MySQL Server가 아닌 경우에도 가능)

MySQL을 기존 보안 인프라와 통합

MySQL Enterprise Encryption
MySQL 암호화/복호화(Encryption/Decryption)



전용/공용 키 쌍

- MySQL Enterprise Encryption 기능으로 생성
- 외부에서 생성된 키 사용(예: OpenSSL)

MySQL Enterprise TDE(Transparent Data Encryption)

- 미사용 데이터 암호화
- 애플리케이션 및 사용자에 대한 투명성
- DBA에 대한 투명성
- 키 관리 필요

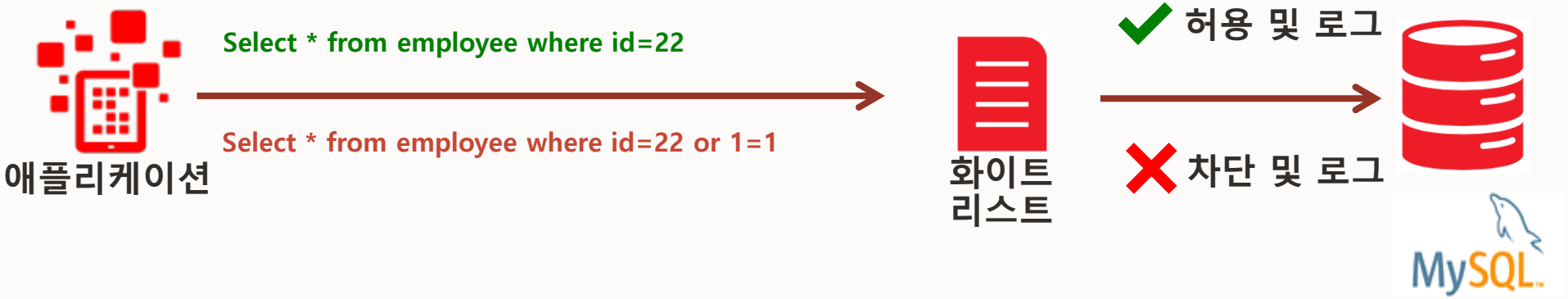
MySQL Enterprise Audit

- 연결, 로그인, 쿼리에 대한 바로 사용 가능한 로깅 기능
- 로그 회전 및 필터링을 위한 사용자 정의 정책
- 동적으로 활성화/비활성화: 서버 재시작 없음
- Oracle Audit Vault 사양에 따른 XML 기반의 감사(Audit) 스트림
- 5.7.21 및 8.0의 기능
  - JSON
  - 압축
  - 암호화

MySQL 애플리케이션에 규제 준수 추가
(HIPAA, Sarbanes-Oxley, PCI 등)

MySQL Enterprise Firewall

- 양성(Positive) 보안 모델로 SQL 주입 방어



- 정책에 맞지 않는 데이터베이스 트랜잭션을 감지하여 차단
- 로깅 및 분석

MySQL Enterprise Masking and De-Identification

중요한 데이터의 익명화 및 비식별화

- 실제 값을 대체 값으로 교체하여 중요한 정보를 은폐

마스킹 및 식별 정보 제거는 규제 준수의 핵심

- 프로덕션 데이터를 sanitize하여 IT 비용 절감
- 데이터 침해의 위험을 크게 낮춤
- 기밀 정보 보호

직원 테이블

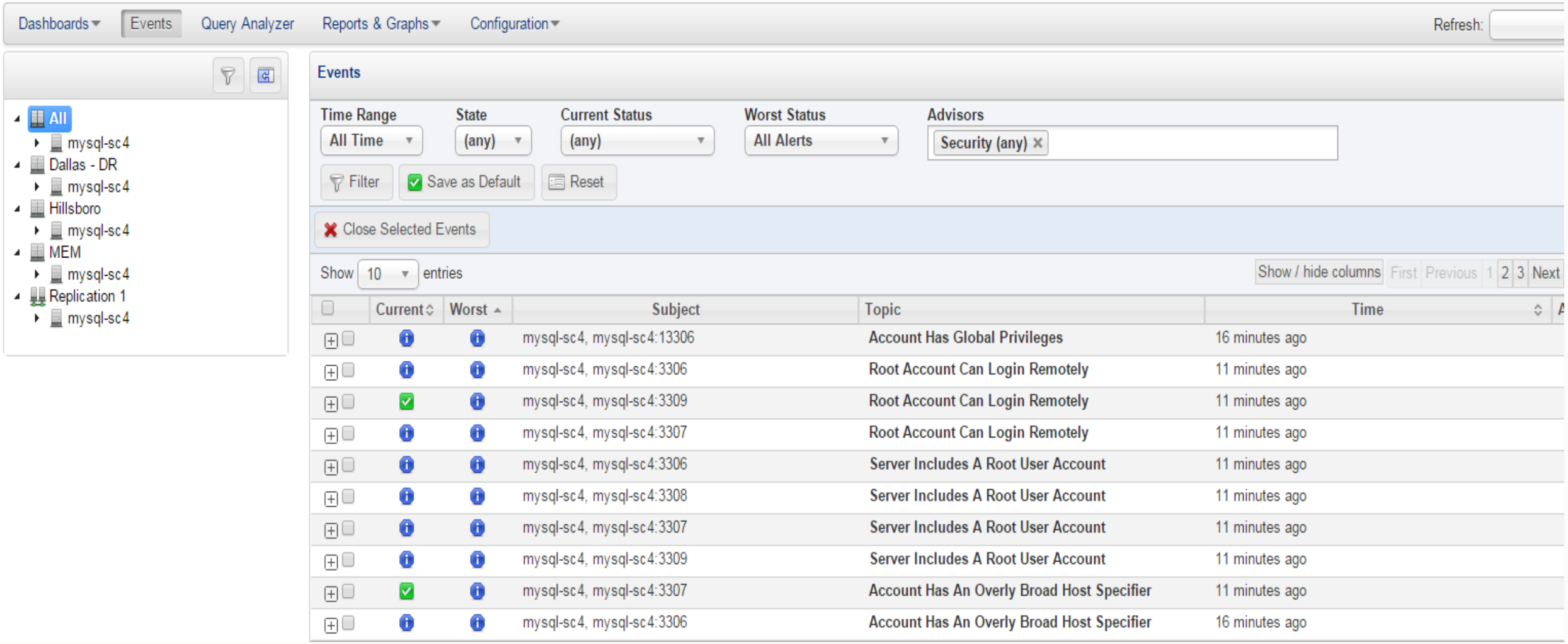
ID	성	이름	SSN
1111	Smith	John	555-12-5555
1112	Templeton	Richard	444-12-4444

임의 데이터 생성

마스킹된 뷰

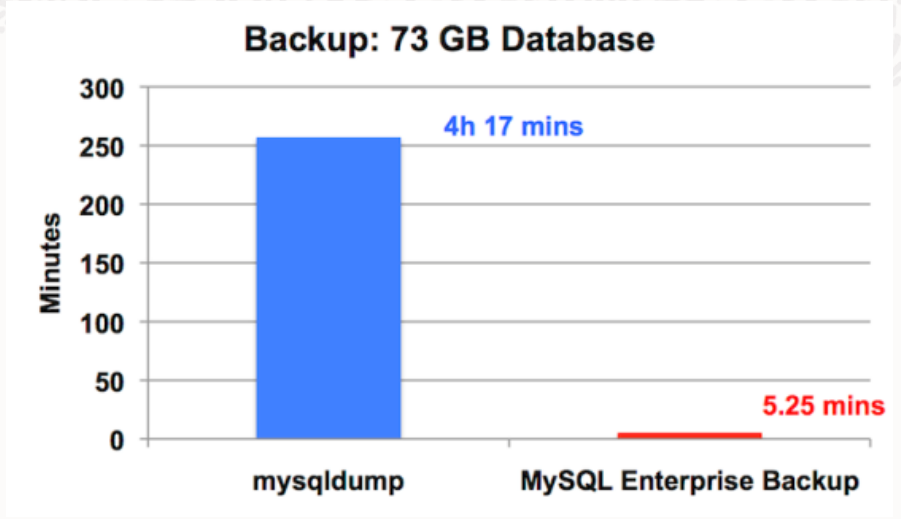
ID	성	이름	SSN
2874	Smith	John	XXX-XX-5555
3281	Templeton	Richard	XXX-XX-4444

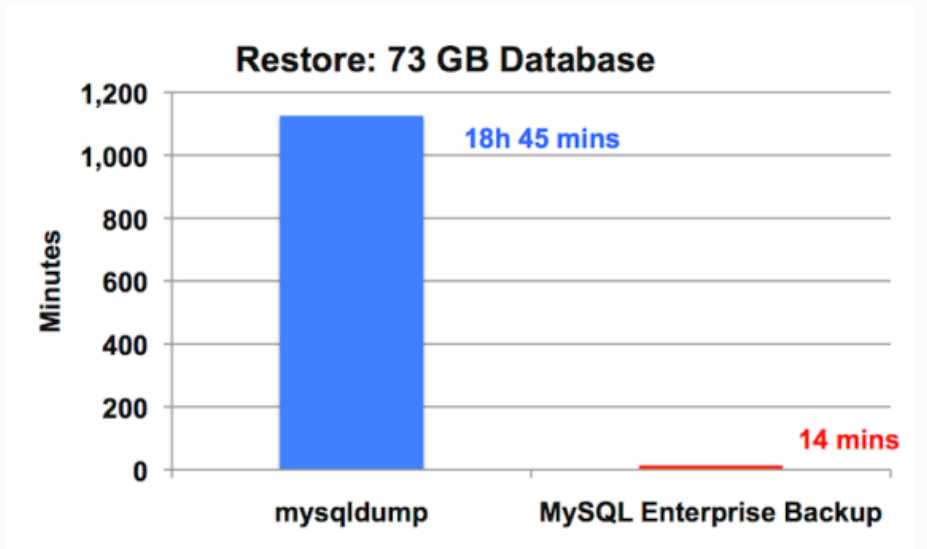
MySQL Enterprise Monitor 보안 모니터링 – 시스템 보안 확인



MySQL Enterprise Backup

- 백업은 업무상 필수
  - 공격 후 복원하는 데 사용
  - 서버 마이그레이션, 이동 또는 복제
  - Audit Trail의 일부
- 백업 정기 스케줄링
- 백업 모니터링
- 백업 암호화





MySQL 보안 제품군으로 데이터베이스 보안 유지

- **평가**
  위험과 취약점을 찾아내고, 필요한 보안 제어 수단이 마련되어 있는지 확인
- **예방**
  암호화, 사용자 제어, 액세스 제어 등 사용
- **감지**
  여전히 침해 가능성이 존재하므로 감사(Audit), 모니터링, 경고
- **복구**
  보안 사고로 인해 서비스가 중단되지 않도록 보장
  Primary Database가 중단되더라도 Recovery 가능
  사후 포렌식을 통해 취약점 수정

보안 리소스

- https://blogs.oracle.com/mysql
- https://www.mysql.com/why-mysql/#en-0-40
- https://www.mysql.com/why-mysql/presentations/#en-17-40
- https://www.mysql.com/news-and-events/on-demand-webinars/#en-20-40
- https://www.mysql.com/news-and-events/health-check/


ORACLE