1. DB 접근제어 / System 접근제어 (GS 인증, 국제 CC, 조달)
2. Gateway, Sniffing, Hybrid, Agent 운영 / 이중화 운영 / 클라우드/ NoSQL/ MAC
3. 작업결재 - 사전/사후/다단계/대리/제3자 실행 / 서버 접근 및 작업결재
4. Dynamic Data Masking / 사전사후 데이터 기록 / 콘솔로깅
5. 우회접속차단 / 로컬 접속 감시통제 / 사용자 파일저장 통제
6. 사용자 2-Fact 인증 / 가상 계정 통제 / 인증키 로그인
7. 통신구간 암호화 / 감사로그 암호화 / DB통신채널 (SSL/TLS) 암호화 연결

Chakra MAX V2 – DB & System 접근제어 솔루션

WAREVALLEY

DBMS, Database Management and Security

http://www.warevalley.com

Chakra Max
Database Security Assurance

1. 웨어밸리 – Innovative Data Solution

"데이터베이스 솔루션 기업"
㈜웨어밸리 – WAREVALLEY, Since 2001
http://www.warevalley.com
서울 마포구 상암동 누리꿈스퀘어 비지니스타워 22F
DBMS, DB보안(접근제어,암호화,취약점분석),
DB 운영관리 및 성능관리 솔루션 개발
전세계 3,500 고객사 / 400,000 사용자

Gartner

Hype Cycle for Application Security, 2016
13 July 2016 | ... Fortinet; HexaTier; IBM; Imperva; McAfee; Mentis; Oracle; Trustwave; **WareValley** Recommended Reading: Analysis By: Jonathan Care; Avivah Litan ...
Analyst(s): Ayal Tirosh

Hype Cycle for Data Security, 2016
13 July 2016 | ... Fortinet; HexaTier; IBM; Imperva; McAfee; Mentis; Oracle; Trustwave; **WareValley** Recommended Reading: Analysis By: John Girard Definition: Interoperable ...
Analyst(s): Brian Lowans

가트너 2012년 ~ 2019년 8년 연속 선정 ;
- **아시아 DB보안 선두 기업**
- **전세계 7개 주요 DB보안 벤더 중 하나**
- **DB보안 모든 Portfolio 제공**

Gartner 2012-2019
- Leader of Database Security
- One of Global Top 7 Vendors
- Owns full portfolio of Database security and management

Market Definition
Analysis
- Competitive Situation and Trends
  - Market Trends
- Market Players
- The Future of Competition
- Competitive Profiles
  - Application Security
  - BeyondTrust
  - IBM InfoSphere Guardium
  - Imperva
  - McAfee (A Division of Intel)
  - Oracle
  - WareValley
- References and Methodology

Gartner Recommended Reading

1. 웨어밸리 – Innovative Data Solution

DB 솔루션	제품명	설명
DB-System 접근통제	CHAKRA MAX	Enterprise급 규모의 DB 및 Server 접근 통제/감사
DB 암호화	GALEA	Column-Level (Plug-in, API) 방식의 DB 암호화
DB 작업결재	CHAKRA MAX	DB Tool, DB 종류에 상관없는 강력한 DB 작업결재
	Trusted ORANGE	Orange 사용자 기반의 강력한 DB 작업결재
개인정보스캔 DB 취약점 분석	CYCLONE	개인정보 모니터링, DBMS의 취약점 Scan (모의해킹 및 내부감사)
DB 관리 및 개발	ORANGE	DB 성능 모니터링 및 개발 지원 도구
DBMS	PetaSQL	빅데이터 분석/데이터웨어하우스/데이터 마트/실시간 로그 분석
통합 로그관리	LOG_CATCH	개인정보 접속이력 관리 및 이상징후 감지 및 소명 관리
DB 수집 및 활용	Peta INSIGHT	이기종 데이터베이스간 실시간 데이터 복제 및 활용

데이터보안인증(DQC-S)에 완벽대응

- 접근통제(Level 1) / 암호화(Level 2) / 작업결재(Level 3) / 취약점 분석(Level 4)
- 인증기관 : 한국 데이터베이스 진흥원

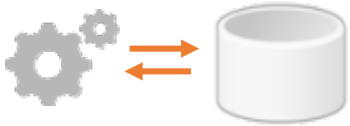
데이터보안 진단 컨설팅

- 한국데이터베이스진흥원의 데이터 품질관리 지침(Ver2.1)과 데이터 품질관리 성숙모형(Ver1.0)을 기준으로 하여 '데이터베이스 품질관리 인증서'를 받을 수 있도록 정확하고 신속하게 컨설팅 지원

2. 제품 구성 | 제품 구성

DB접근제어 서버

Chakra Max Server



Chakra Max Engine

Chakra Max Repository (PetaSQL)

Chakra Max™ Database Security Assurance

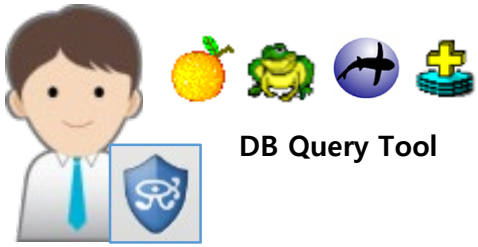
DB접근제어 관리자

Chakra Max Manager Program

접근제어 관리자

DB사용자 Client

Chakra Max Client Program

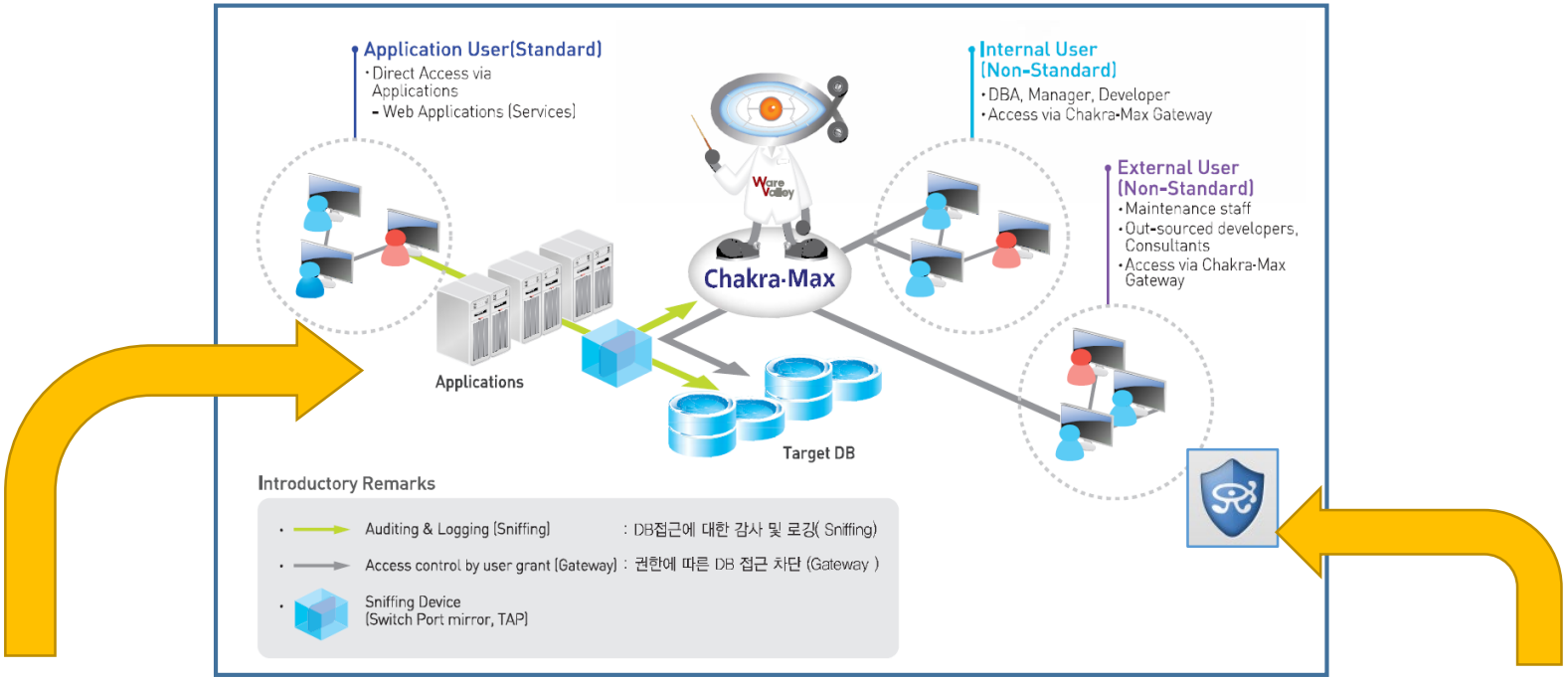


DB Query Tool

DB 사용자

보안 정책 관리 / 적용	DB / System / 사용자 /그룹 관리	DB / System 직접 접속 통제
DB & System 작업 감사 데이터 로깅	보안 정책 설정(결재/차단/경보)	기안 / 승인 / 진행 상태 조회 및 관리
보안 시스템 운영 현황 모니터링	실시간 모니터/보고서 생성	개인 정보 관리 / 파일저장통제

2. 제품 구성 | 시스템 구성



Sniffing mode

중요 DB 접근에 대한 실시간 모니터링 및 사후감사

- 사용자 별 DB에 연결된 Session에 대한 다양한 상태 정보를 실시간 모니터링
- DB 트렌잭션 로그 데이터에 대한 분석 및 감사보고서 생성
- DB 서버 부하율 0%의 처리방식

Gateway mode

사용자 별 DB 접근에 대한 권한관리 등 접근통제

- 불법적인 개인정보 조회, 유출방지
- 사용자 정의 보안정책에 따라 경보 및 차단 기능

Hybrid : Gateway, Sniffing, Agent 구성의 혼합형태

- 정형 접근에 대한 가용성 보장 및 감사기능 제공
- 비정형 접근에 대한 강력한 권한제어 및 접근통제

3. 주요기능 | 요약

System 접근통제 (6종)

Windows
HP-UX
AIX
Solaris
Linux
Mainframe

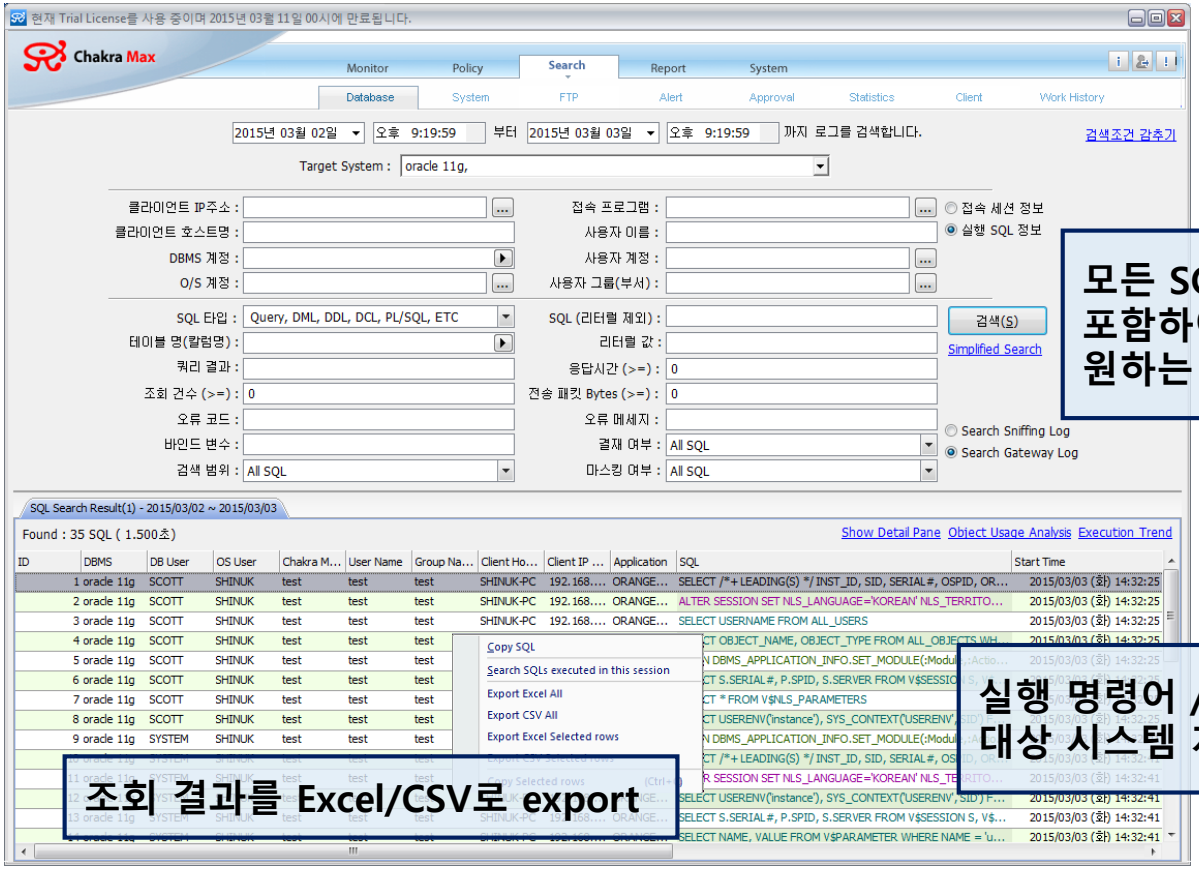
Database 접근통제 (30종)

Oracle / Time-Stan /Exadata
Microsoft SQL Server
IBM DB2 (Mainframe, UDB)
SAP Sybase IQ/ASE
SAP HANA
Mysql / MariaDB
IBM Netezza
TeraData
PostgreSQL / Greenplum
Altibase / Tibero / Cubrid / Kairos / SunDB
Amazon RedShift / Aurora
Dameng DM7
Fujitsu Symfoware
PetaSQL
Firebird / Couch / Influx / MongoDB

- **DB 및 System 접근 및 작업결재**
- **HA(이중화) 구성**
- **데이터 마스킹 (지정/패턴방식)**
- **3 Tier User Tracking**
- **우회접속 통제**
- **사용자 파일저장 통제**
- **불법 로그 위.변조 방지**
- **개인정보/민감정보 탐색**
- **사전-사후 데이터 기록**
- **사용자 2-Factor 인증**
- **DB/서버 가상 계정 통제**
- **Cloud 지원(AWS, MS, KT 등등)**
- **Client Mac OS 지원**

3. 주요기능 | DB 접근통제 및 기록

DB에 접근하는 모든 사용자(및 시스템)을 식별하고,
접근이력/수행SQL/변수/결과값을 기록하고 통제합니다. (실시간 모니터링 및 로그 조회)

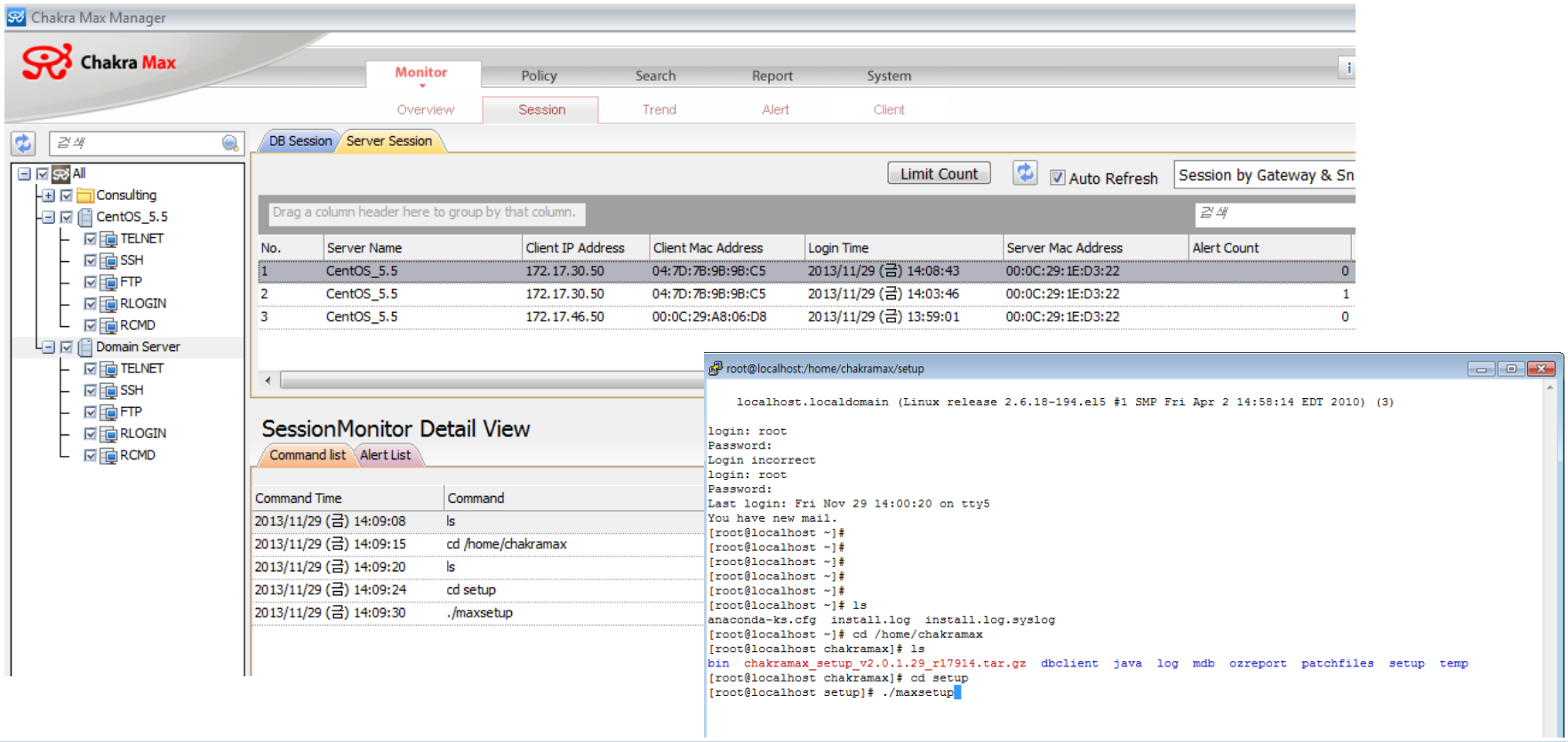


**모든 SQL커맨드에 대하여 전문을 포함하여 약 40여 가지의 정보를 축적!
원하는 조건에 맞는 검색이 가능**

**실행 명령어 / 접속 시각 / 종료 시각 /
대상 시스템 계정 / 클라이언트 IP 정보 확인**

3. 주요기능 | System 접근통제 및 기록

System (Linux, Unix, Windows, Mainframe)에 접근하는 모든 사용자(및 시스템)을 식별하고, Telnet, (s)FTP, SSH, R-Login, R-Command, Windows Terminal, Mainframe 등 다양한 시스템 접근이력 및 명령어 수행을 기록하고 통제합니다. (실시간 모니터링 및 로그 조회)
(시스템에서 입력된 커맨드를 포함하여 vi 편집기에서 작업된 내역도 확인 가능)

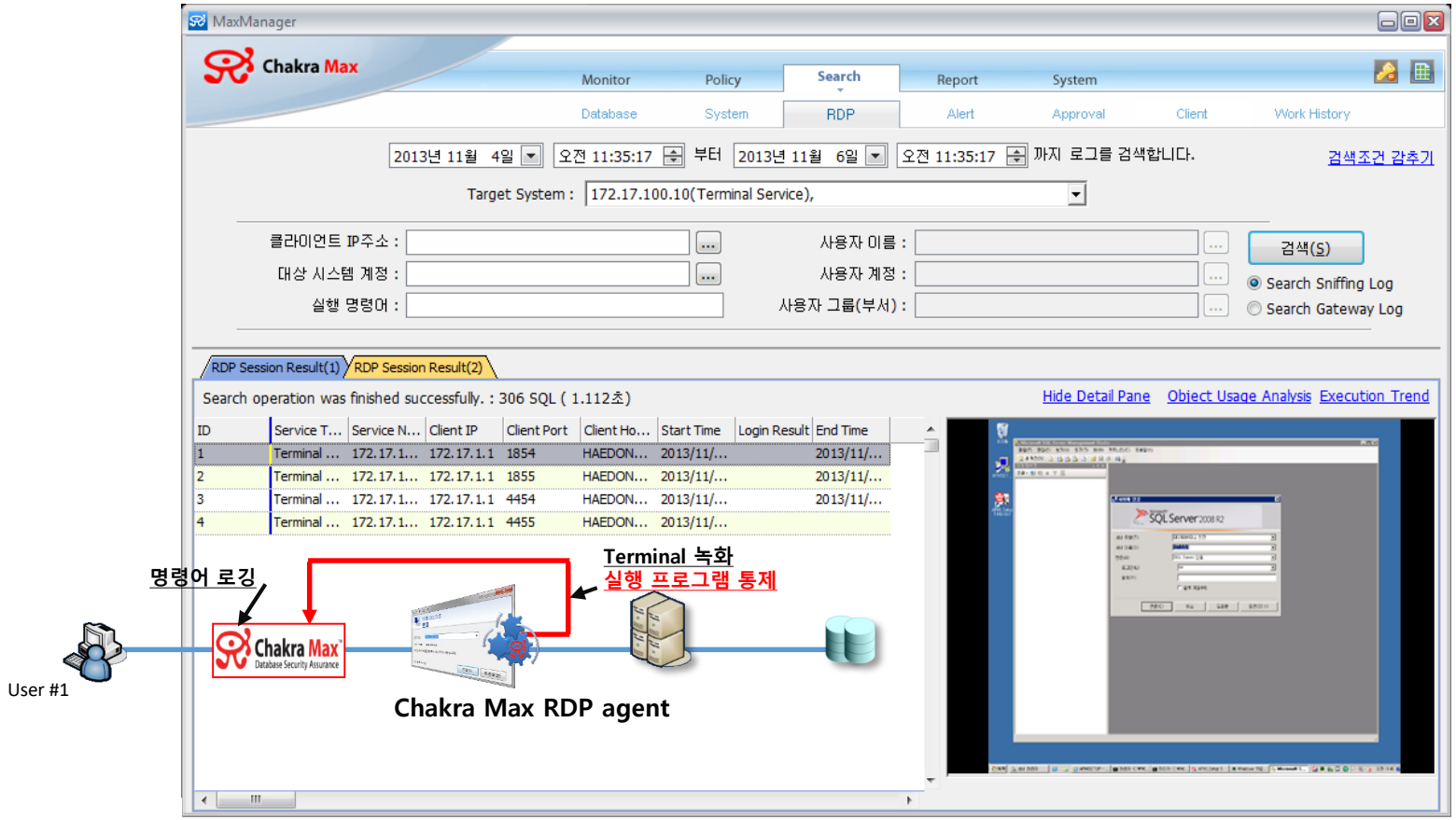


3. 주요기능 | System 접근통제 – Windows Terminal

Windows Remote Desktop (Windows Terminal) 연결 시 수행 내역 동영상으로 녹화, Shell에서 실행 된 명령어 감사 기록으로 저장

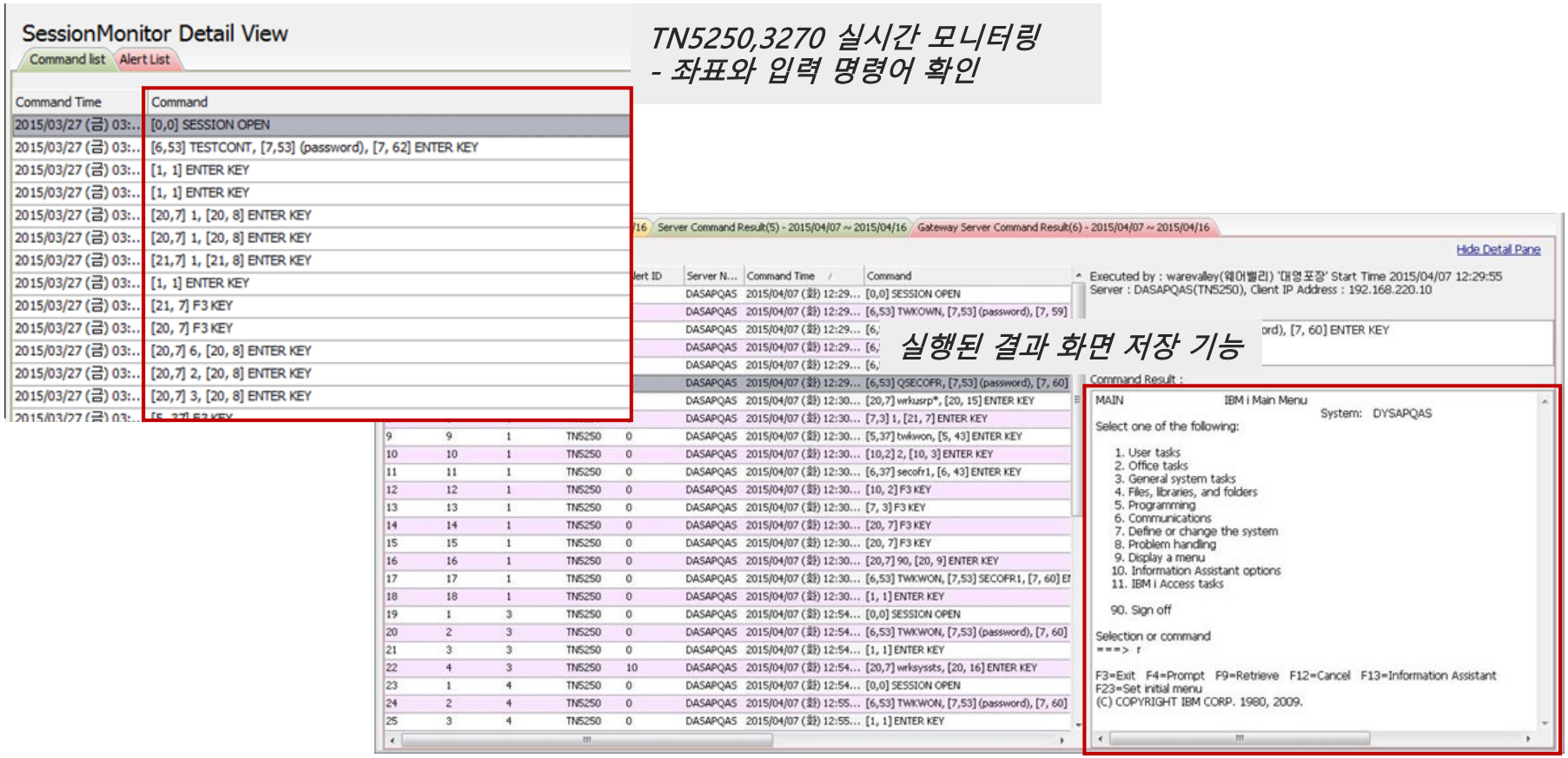
원격 사용자 통제 및 실행하는 프로그램 통제

관리자 화면에서 감사로그 명령어 조회 및 녹화 동영상 재생 기능

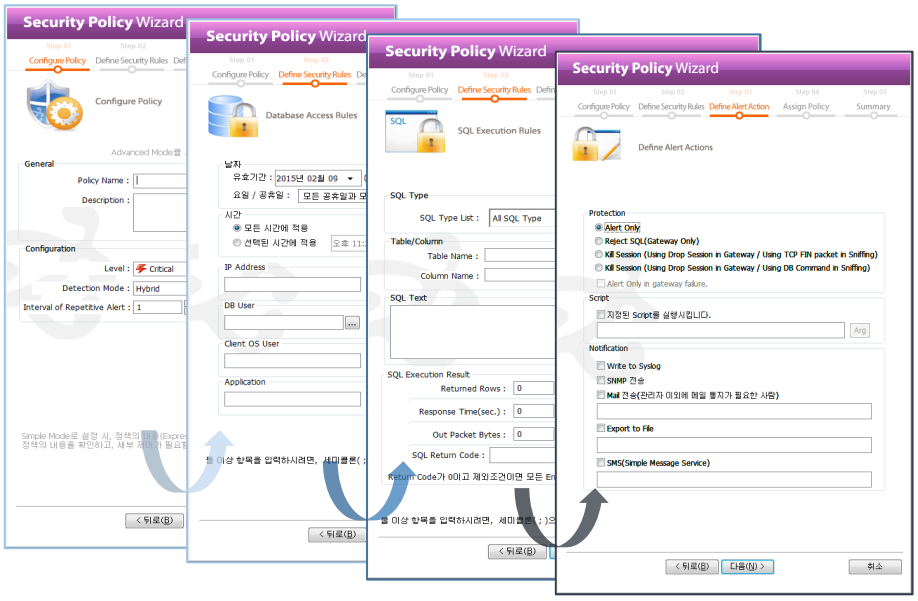


3. 주요기능 | System 접근통제 – Mainframe (TN5250, 3270)

As/400과 같은 IBM Mainframe서버에 접근하는 TN3270,5250 터미널의 사용자 식별 및 작업이력을 기록하고 통제합니다.



DB, System에 접근하는 모든 사용자(및 시스템)을 접근 및 작업 통제를 위하여,
위저드(Wizard) 방식의 손쉬운 보안정책을 구성할 수 있습니다.



데이터베이스/시스템 접근 및 실행제어 정책

Database Access Control Policy
데이터베이스 접근 통제 정책을 정의합니다.

SQL Execution Control Policy
SQL 실행 통제 정책을 정의합니다.

System Access Control Policy
시스템 접근 통제 정책을 정의합니다.

System Command Execution Control Policy
시스템 명령어 실행 통제 정책을 정의합니다.

결재정책 / 파일저장 통제 정책

Database / System Access Approval Policy
접근 권한을 획득하기 위한 결재 정책을 정의합니다.

CMD/SQL Execution Approval Policy
CMD/SQL 실행 권한 제어를 위한 결재 정책을 정의합니다.

SQL Result Save Approval Policy
SQL 실행 결과 저장을 통제하기 위한 결재 정책을 정의합니다.

Approval Policy For Masking Exception
승인 받은 쿼리의 결과는 마스킹 되지 않는 정책을 정의합니다.

변경 전/후 데이터 저장 정책

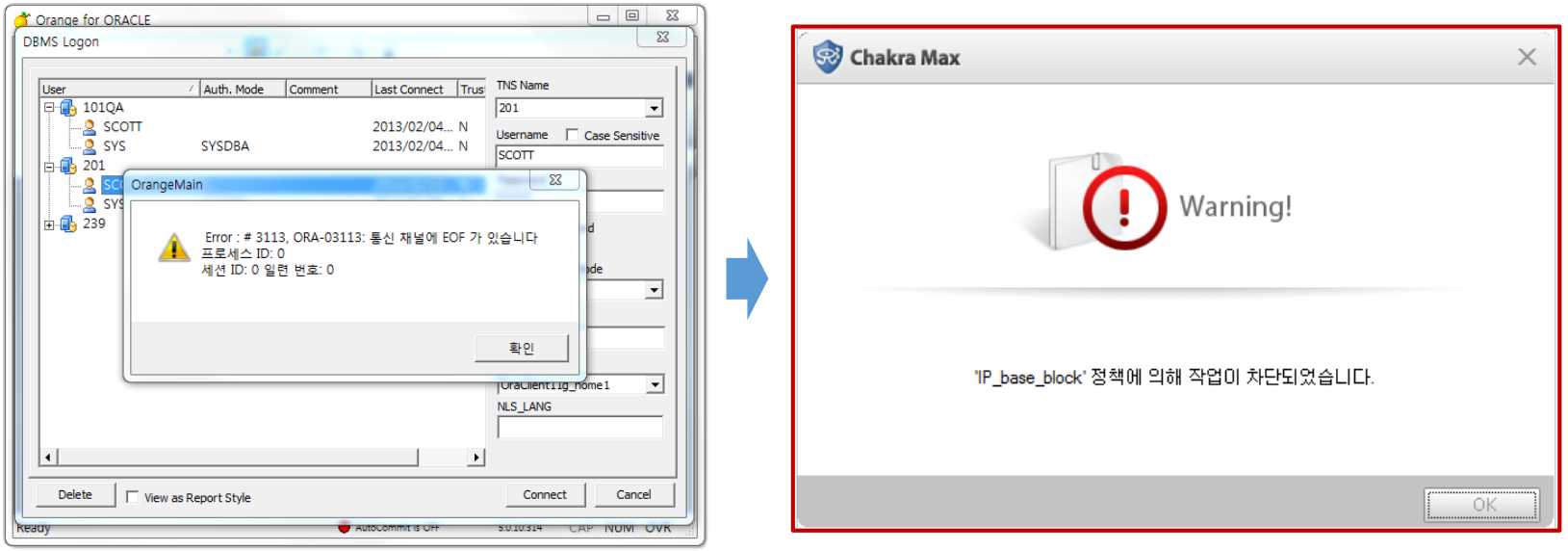
Modified Data Policy
데이터베이스 변경 전/후 데이터 로깅 정책을 정의합니다.

마스킹 정책

SQL Result Masking Policy
쿼리 결과 중 보안이 필요한 항목에 대해 Masking정책을 정의합니다.

3. 주요기능 | 보안정책에 따른 DB 접근통제

Client IP, DB user, Table, Column, SQL Command 등의 다양한 조건의 통제 정책 적용

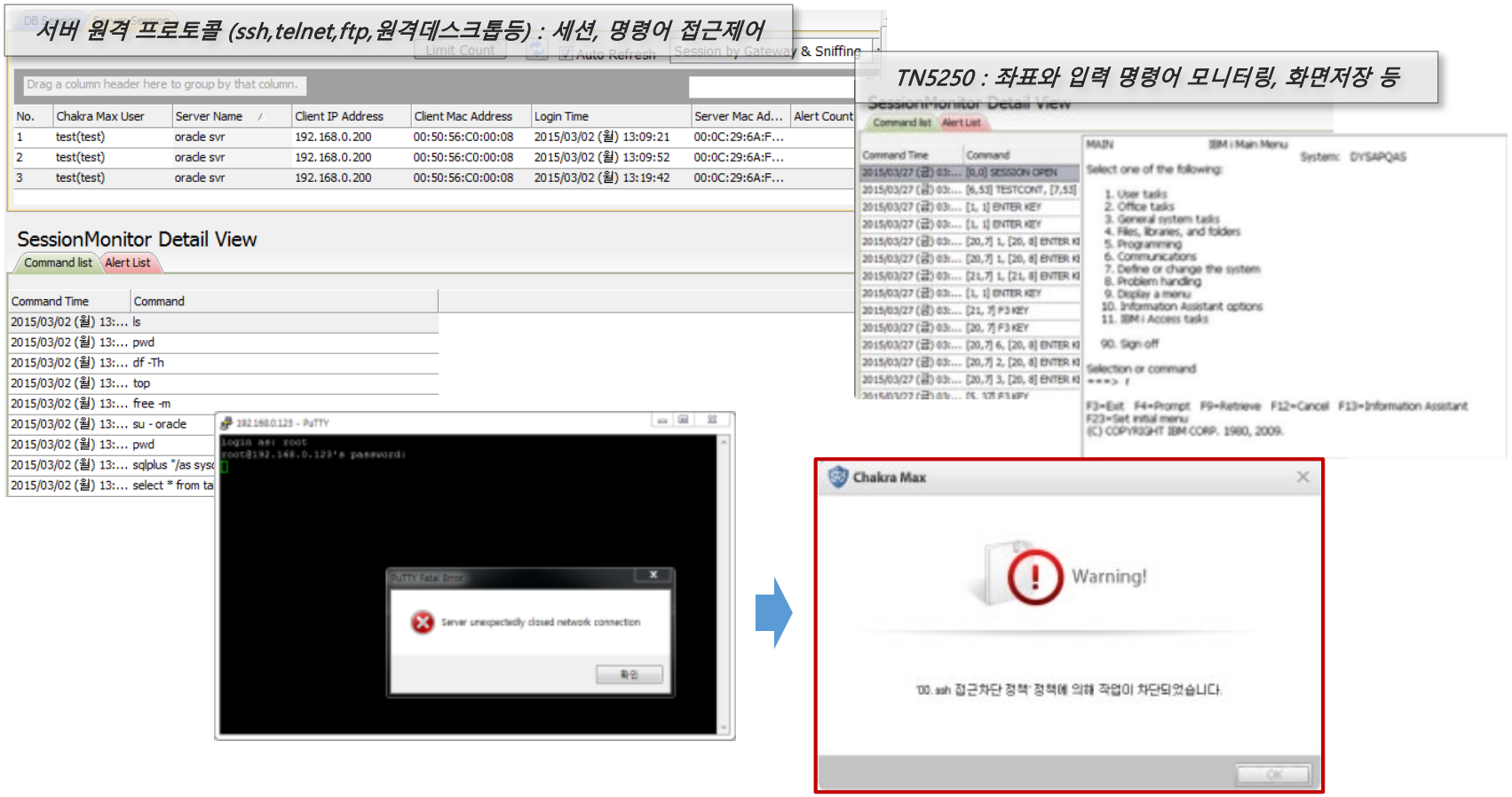


다양한 조합으로 DB 접근을 제어

- **사용자 식별 유저 정보** : IP 주소, DB 계정, OS 로그인 유저, 접속 어플리케이션, 접속시간 등
- **DB작업내용** : 테이블, 컬럼, SQL 타입(DDL/DML/DCL), 입력 커맨드 등
- **기타** : 프로토콜, 시간대, 네트워크 사용량, SQL 결과 리턴 로우

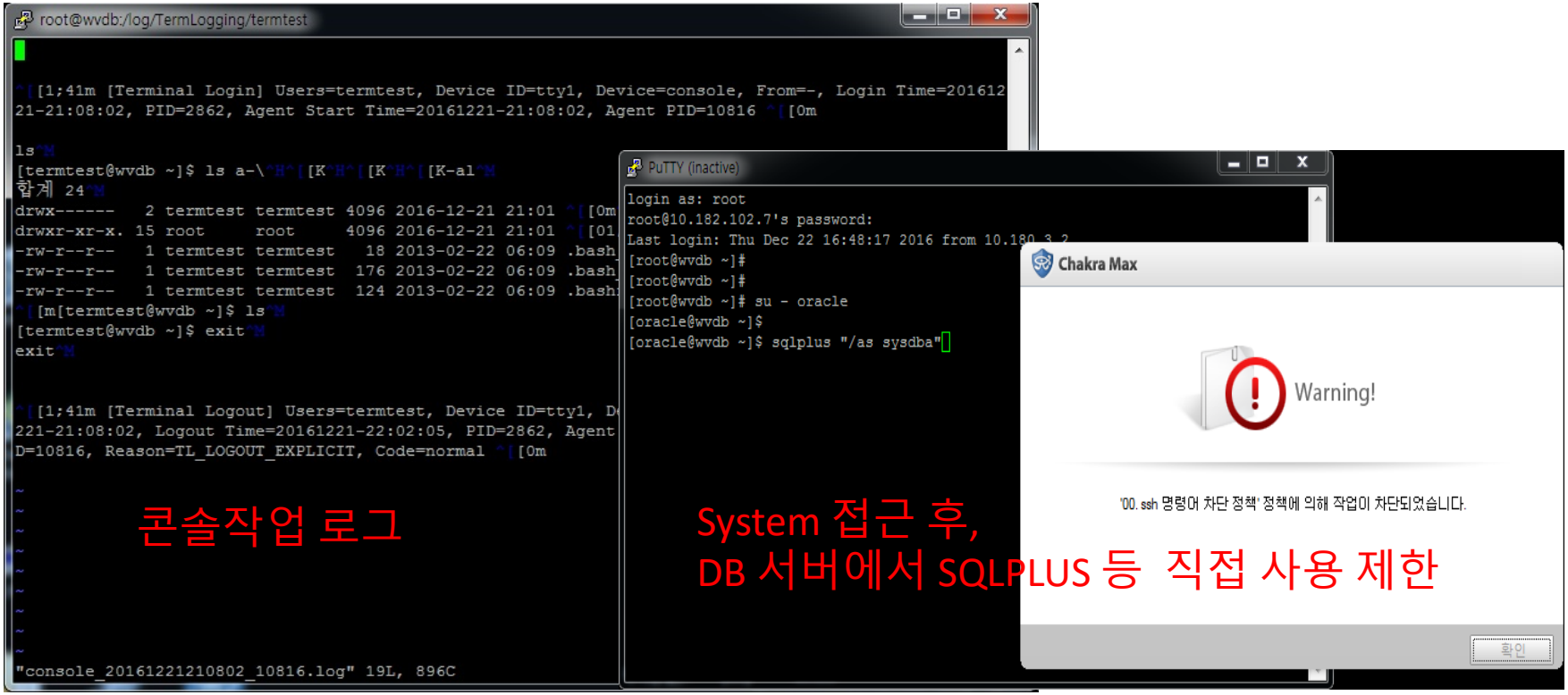
3. 주요기능 | 보안정책에 따른 System 접근통제

SSH, Telnet, FTP, Windows Terminal, TN5250 등의 시스템 접속에 대한 실시간 감시 및 통제, 접근 이력의 재분석이 가능



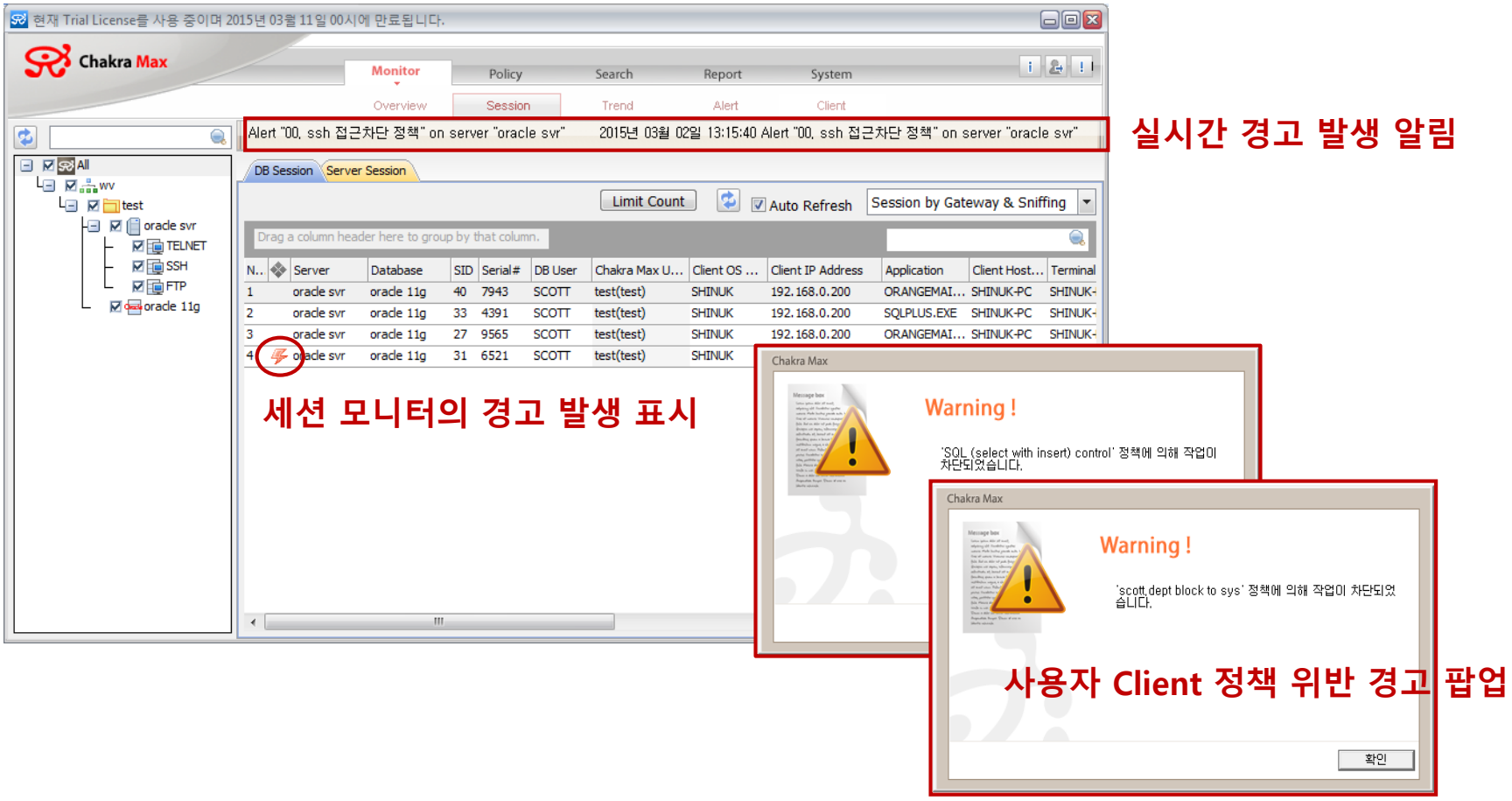
3. 주요기능 | 보안정책에 따른 System 접근통제

DB 서버 내의 콘솔접근인 경우, 콘솔 접속 세션 별로, 시스템 작업 내역들이 별도의 파일로 기록 되며, 또한, 원격 시스템 작업 (SSH, Telnet, FTP, RDP 등) 에 대한 통제는 세션 차단이나, 명령어 통제가 수행



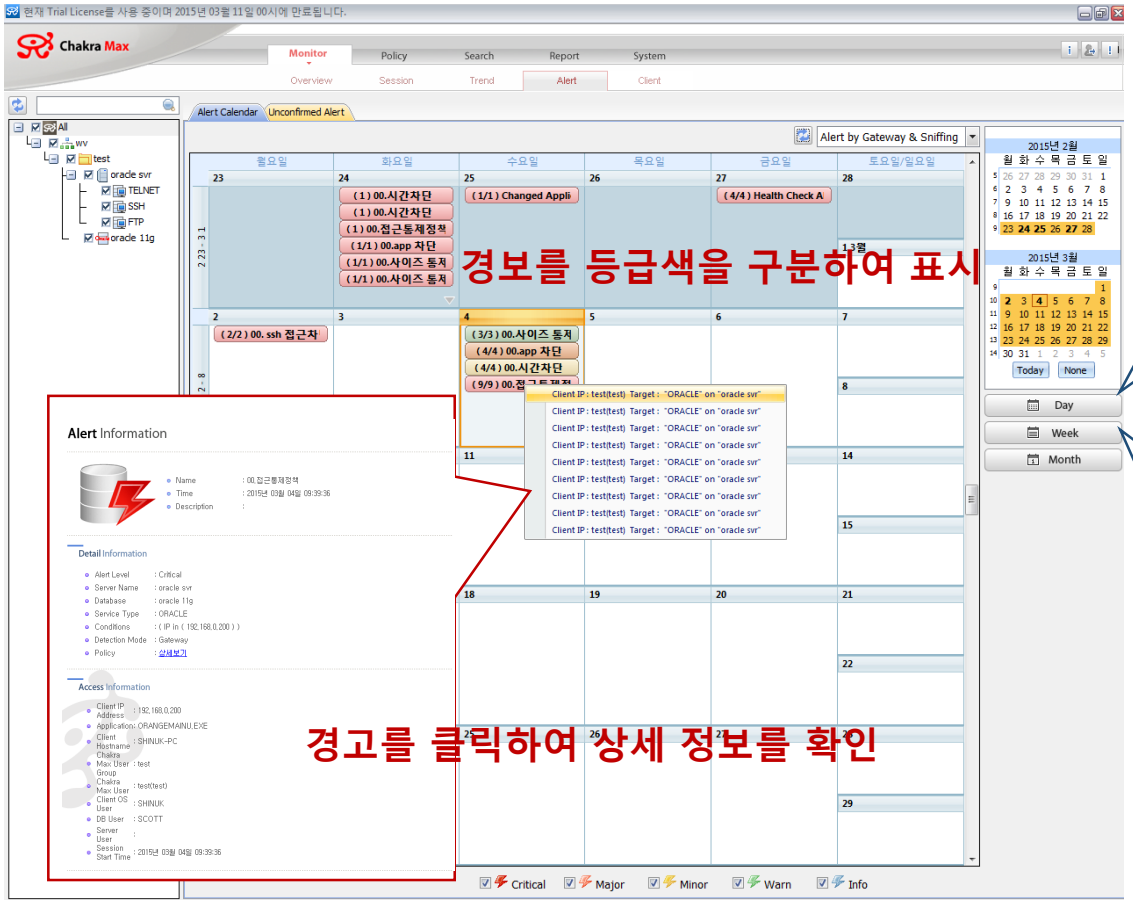
3. 주요기능 | 경고 모니터

보안정책에 위배된 DB접근이나 System 접근 혹은 SQL, System 명령어 작업에 대해,
실시간으로 관리자, 사용자에게 정책 위반 및 경고 메시지를 쉽게 확인이 가능



3. 주요기능 | 경보 캘린더

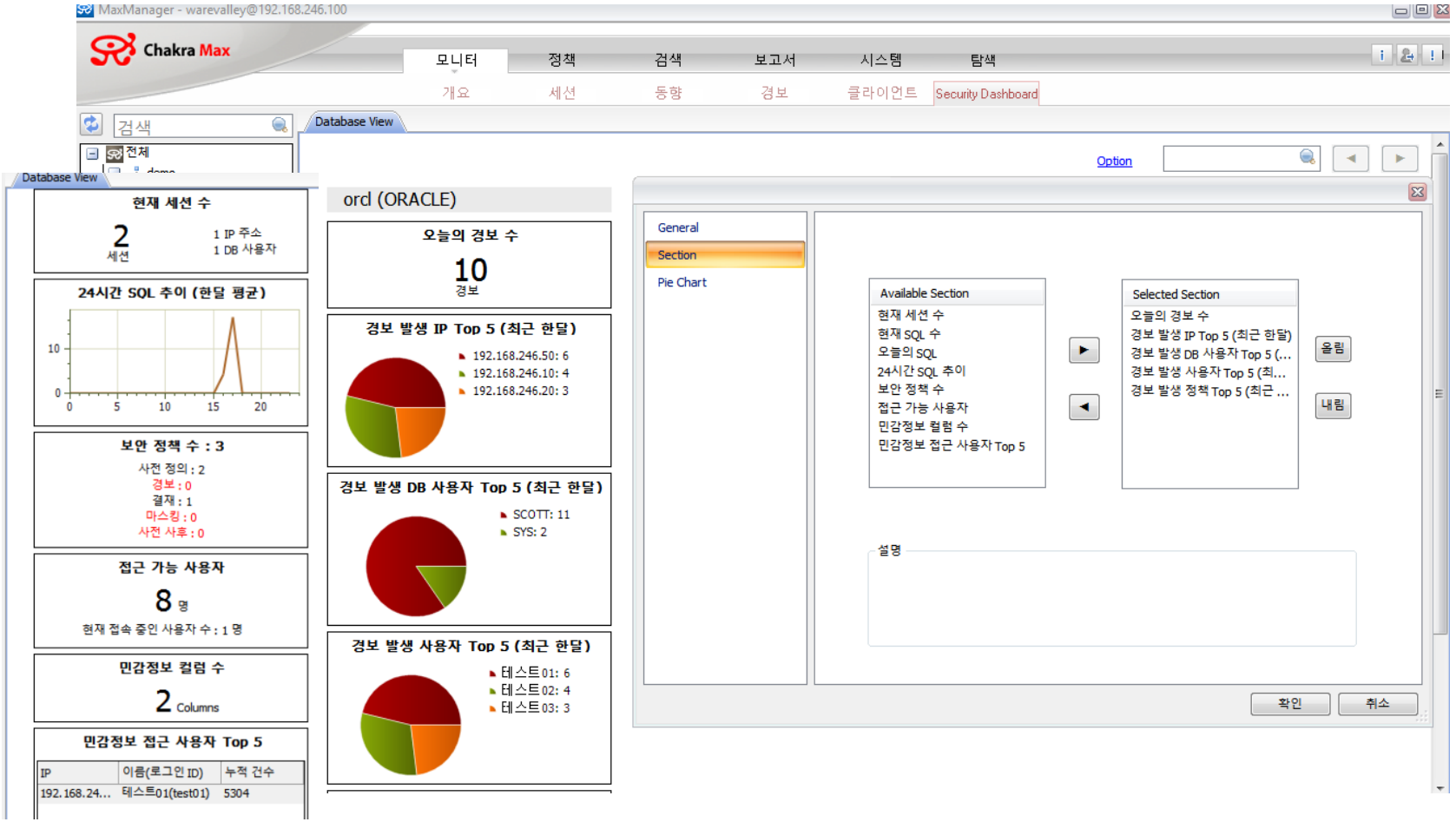
발생된 경보가 월/주/일별의 달력형태로 표현하여 확인 및 추이 파악이 용이



월/주/일별 경보 현황 확인

3. 주요기능 | Security Dashboard

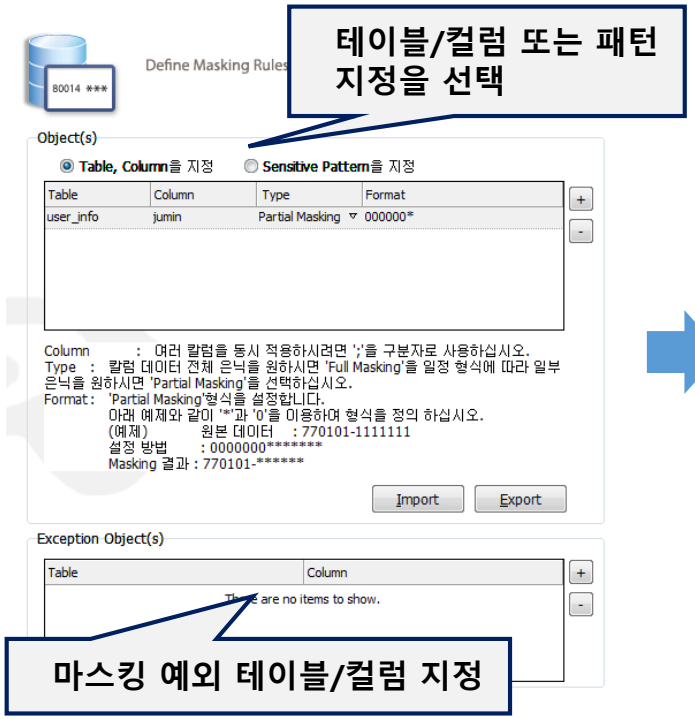
현재 접속현황 / 민감정보 접근자 / 경보발생IP top5 등, 경보에 관련된 정보 표시

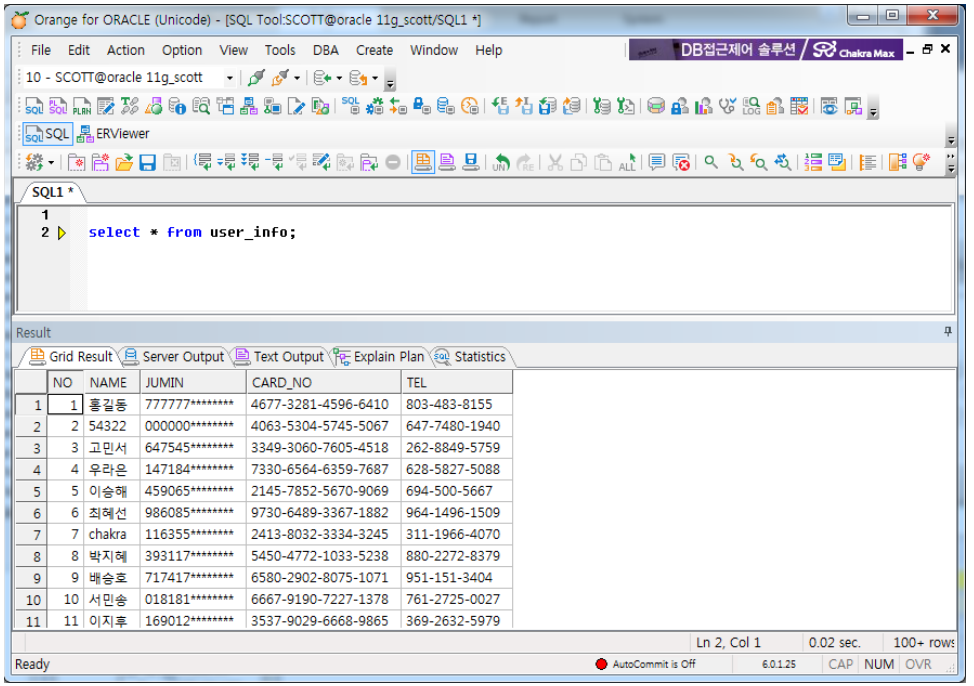


3. 주요기능 | 데이터 마스킹(Masking)

DB내의 민감 정보에 대한 Masking을 통한 정보를 은닉하며, DB성능 저하가 없이 Packet 분석을 통해 Masking 처리를 지원

1) 지정된 Table/Column에 대한 민감 정보 Masking
2) 개인정보를 가진 임의의 SQL 결과에 의한 패턴 Masking

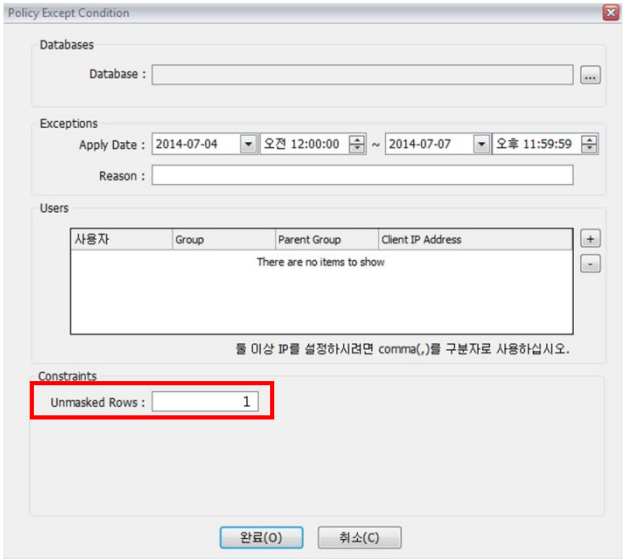




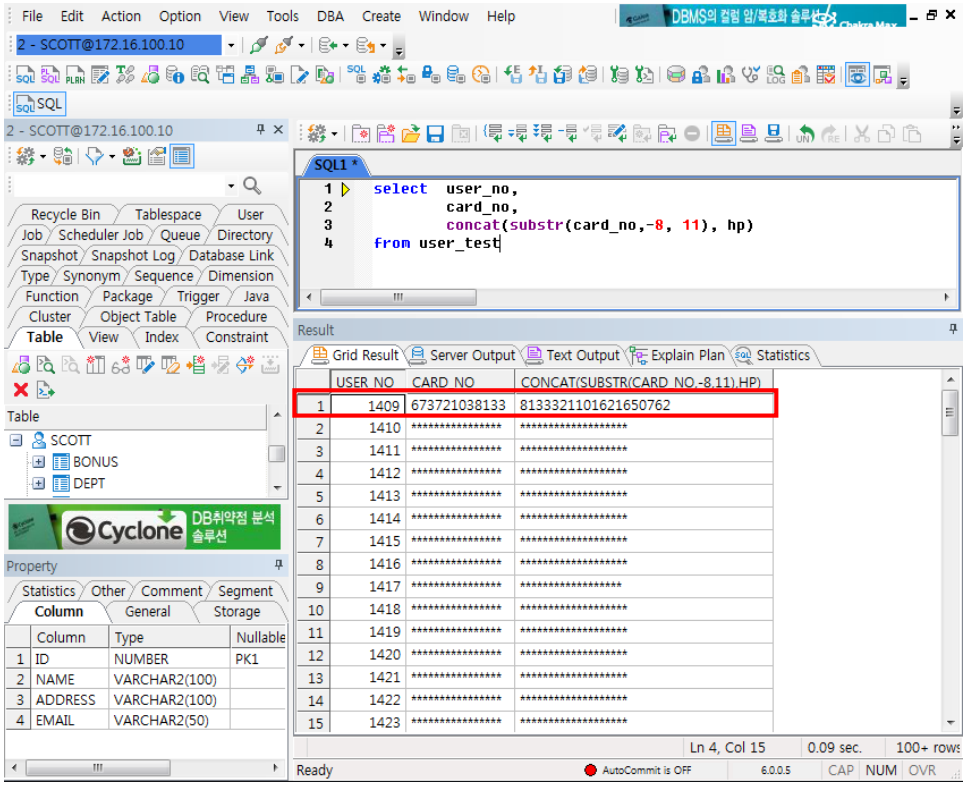
- Chakra MAX의 경우 마스킹을 위해 고객의 DB에 View를 설치하거나 SQL 변조를 일으키는 행위를 하지 않습니다.

3. 주요기능 | 고객 업무편의를 위한 선택적 마스킹 해제

고객의 업무 편의를 위해 마스킹 처리된 오브젝트에서 일부 선택적 마스킹 해제를 지원



- **마스킹이 적용된 오브젝트에서 마스킹 해제되는 레코드 건수를 설정**



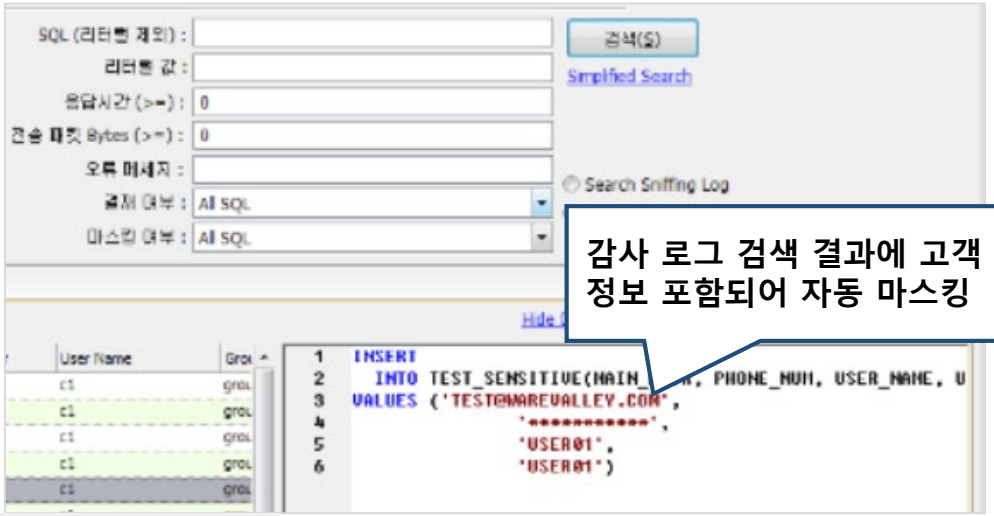
- **설정 된 행수를 제외한 부분은 마스킹 처리**

3. 주요기능 | 감사로그 내의 민감정보보호를 위한 마스킹

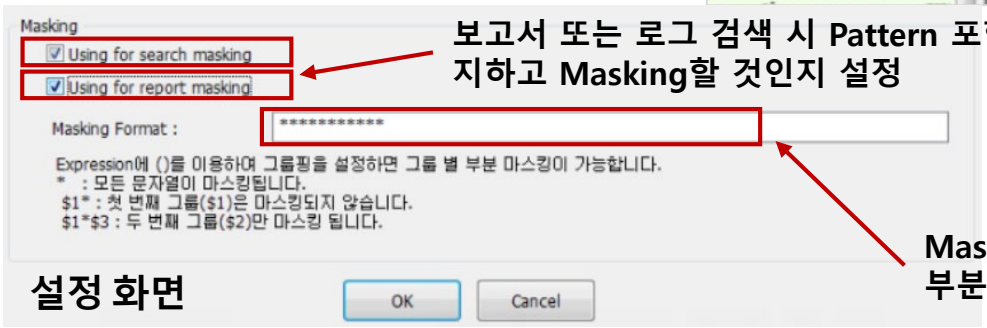
Chakra MAX에 수집된 감사로그에 고객의 민감정보를 보호하기 위해,
로그조회나 리포트 출력에서 마스킹을 통해 고객의 정보를 보호합니다.

```
INSERT
  INTO TEST_SENSITIVE(MAIN_ADDR, PHONE_NUM, USER_NAME,
VALUES ('TEST@WAREVALLEY.COM',
                '01012345678',
                'USER01',
                'USER01')
```

실제 실행된 SQL



감사 로그 검색 결과에 고객 정보 포함되어 자동 마스킹



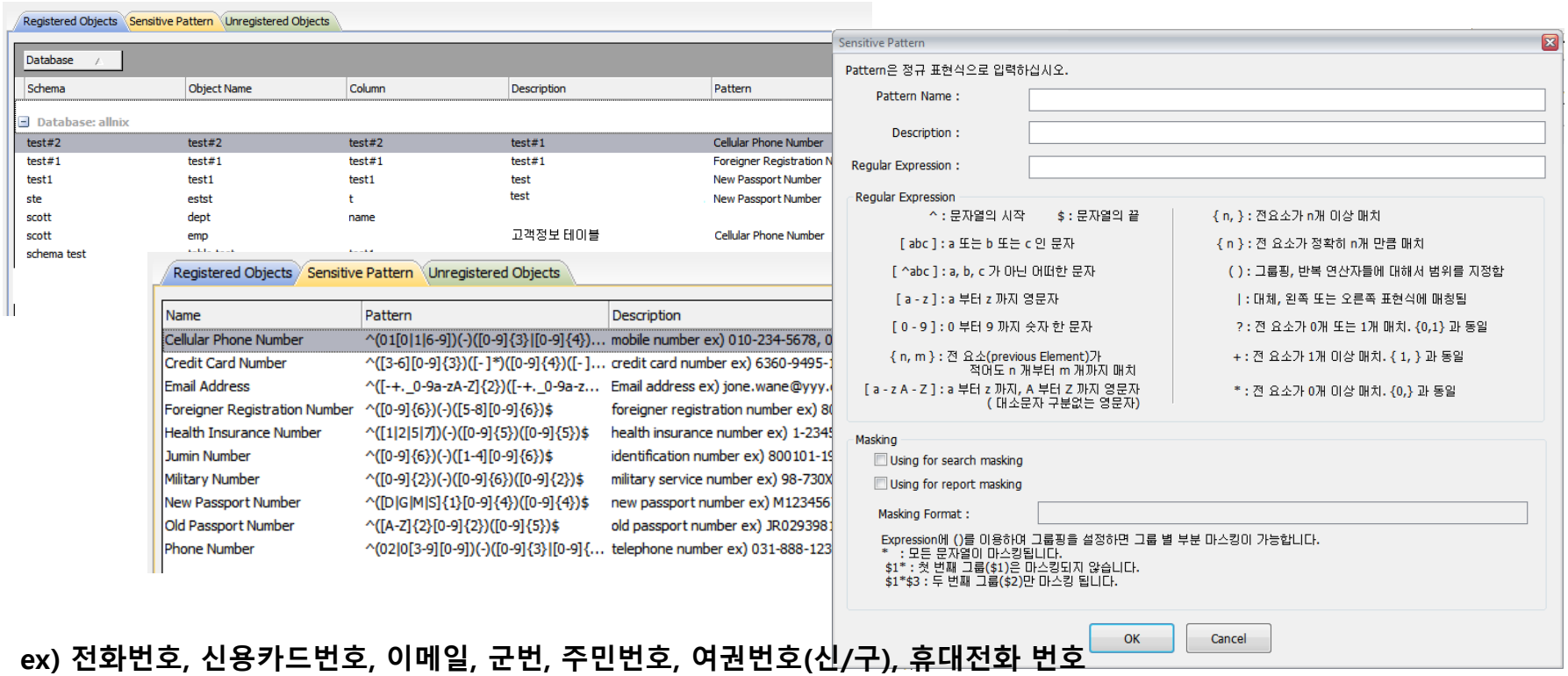
보고서 또는 로그 검색 시 Pattern 포함을 감지하고 Masking할 것인지 설정

Masking 방식을 정의
부분 Masking이 필요하면 Rule을 정의

설정 화면

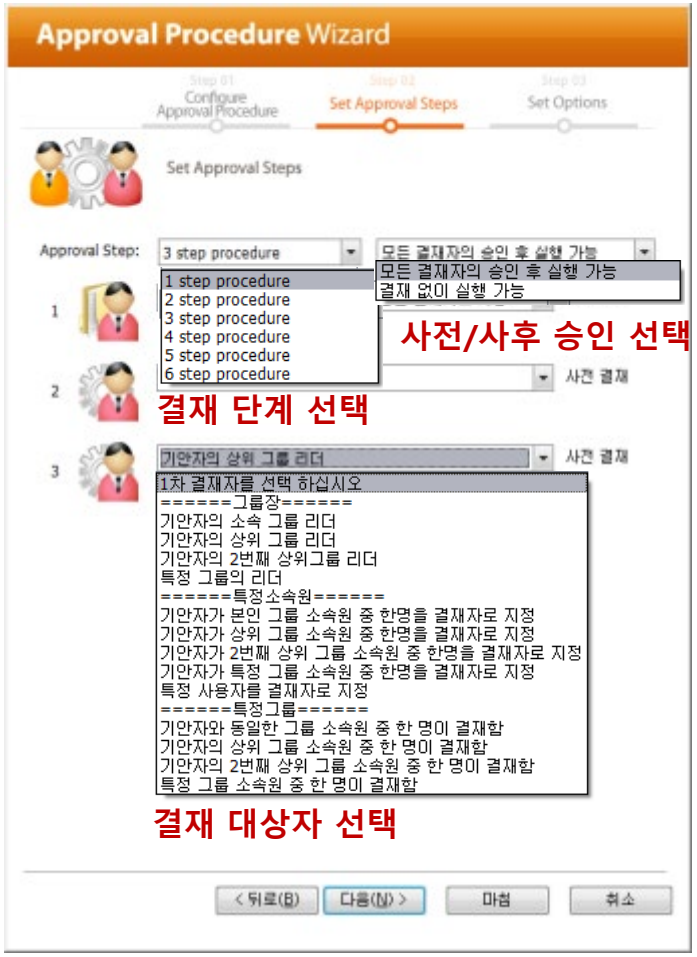
3. 주요기능 | 민감정보 관리

고객 정보와 같은 민감한 정보를 “Sensitive Object”로 관리
미리 정의된 정보 패턴(Sensitive Pattern) 를 제공 및 사용자 정의 가능

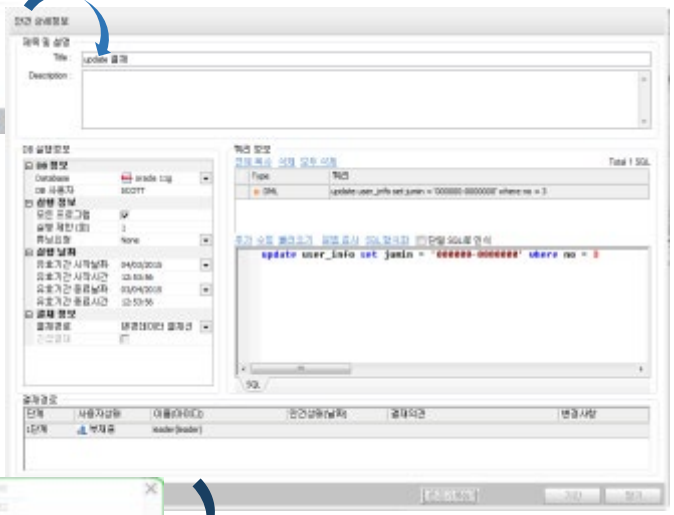


ex) 전화번호, 신용카드번호, 이메일, 군번, 주민번호, 여권번호(신/구), 휴대전화 번호
필요 시 민감정보 패턴을 직접 작성/수정 가능

다양한 방식의 결재 정책 및 다단계 결재 정책 지원



결재정책 차단 후 기안

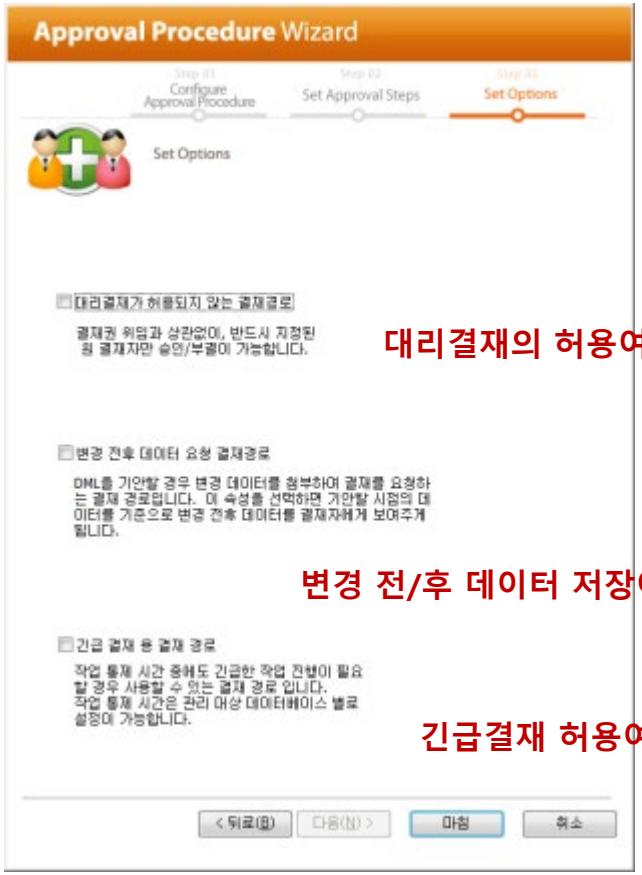


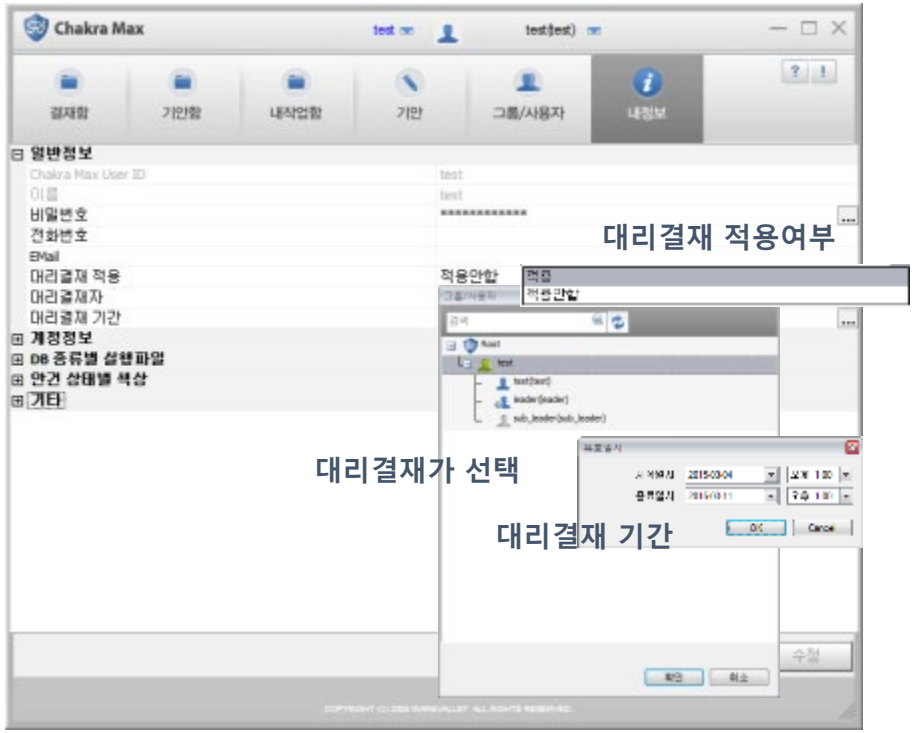
기안 완료 후 결재 대상자의 승인 후 SQL 실행

사후 결재시
기안 후 결재전 실행가능, 실행이력 감사로그로 저장 및 결재자에 이메일 통보

3. 주요기능 | 대리결재/긴급결재

관리자의 확인이 필요한 작업에 대해 결재 프로세스를 이용한 작업 확인, 승인(결재) 기능을 제공하며, 사전/사후 결재 및 대리/긴급결재를 제공하여 업무 연속성을 보장

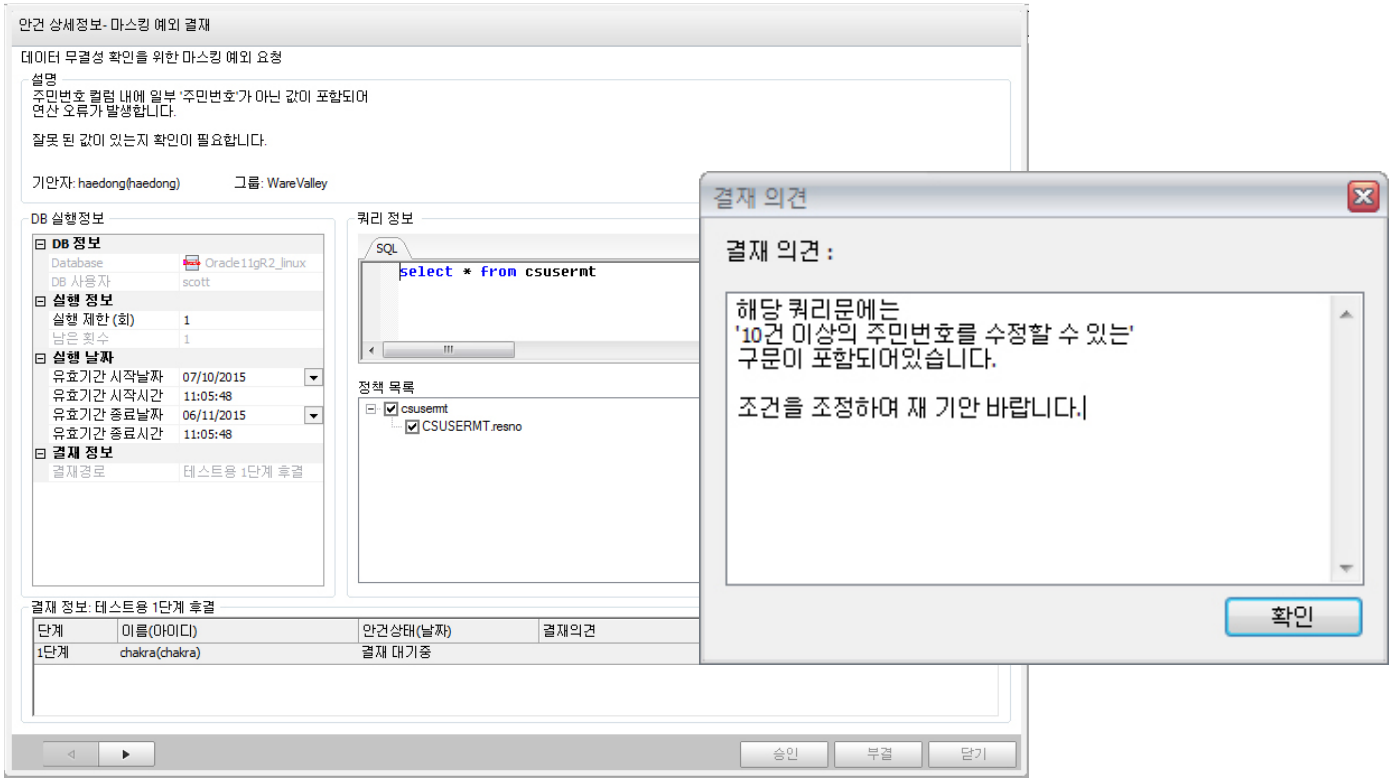




대리결재 적용 및 대리결재자/기간은 사용자가 지정

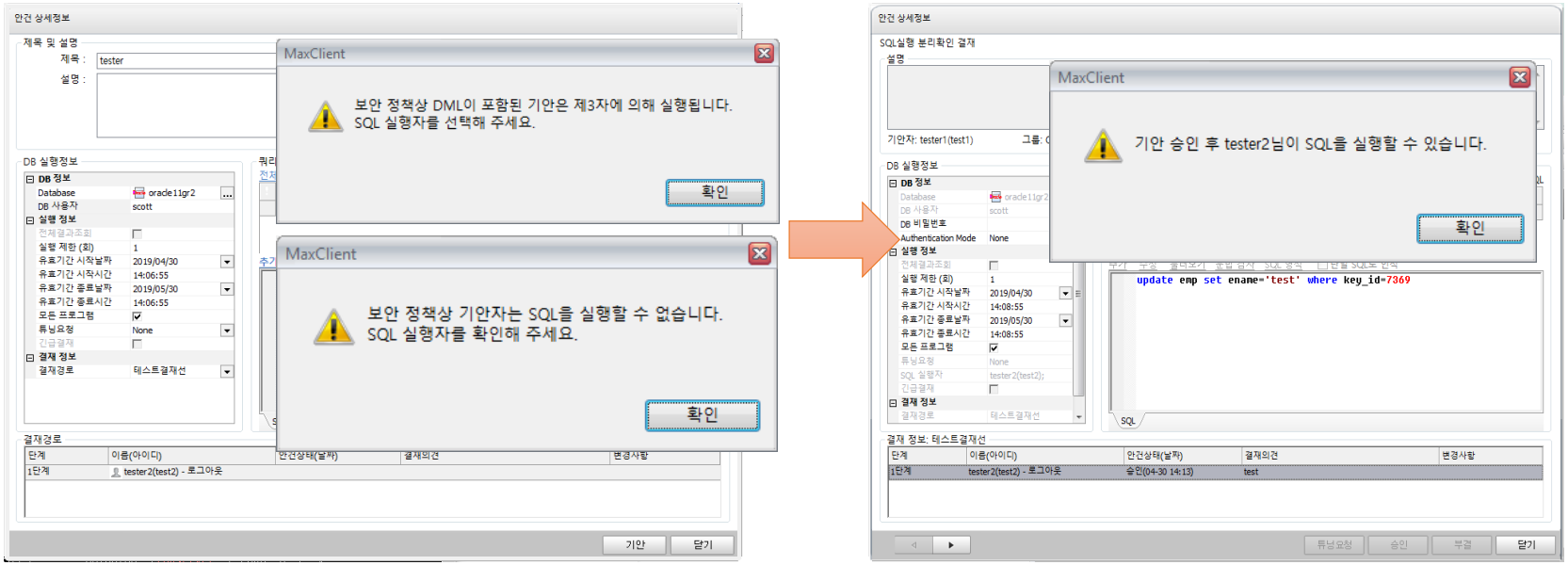
결재자의 결재 / 부결 처리 시 결재권자의 결재/부결 의견 기입

(결재자의 결재 처리 시 결재 의견 삽입을 통해 결재 / 부결 등에 대한 명확한 의견 전달)



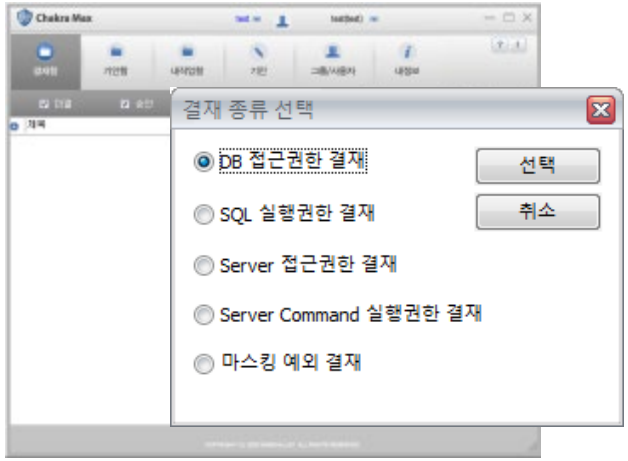
기안자와 실행자의 권한 분리 기능

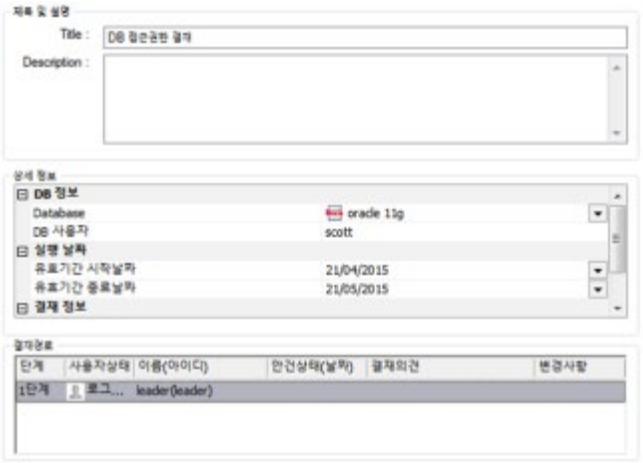
결재를 요청하는 기안자와 SQL의 실행자를 분리하는 기능으로, 기안자는 기안작성 후 결재요청시 sql 실행자를 선택하여 결재를 올리고, 결재완료시 실행자가 SQL을 실행할 권한을 가진다.



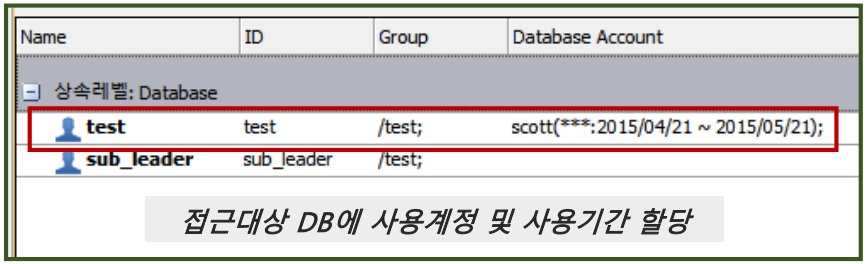
3. 주요기능 | DB 접근권한 결재

접근 권한이 없는 데이터베이스에 DB 접근권한 결재 기능을 이용하여 사용자가 직접 기안 후 결재자의 승인을 통해 접속하는 기능을 제공



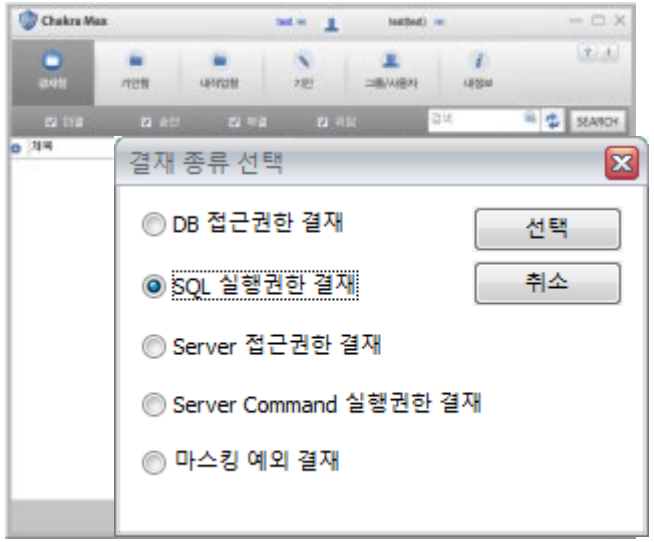


사용자가 DB 접근권한 기안, 결재자의 승인 완료 후 접속 권한 부여



3. 주요기능 | SQL 실행권한 결재

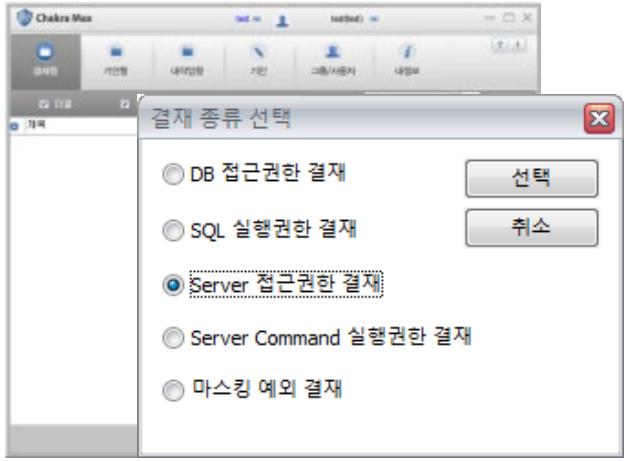
SQL 실행 결재 정책이 적용된 SQL 실행시, SQL 실행권한 결재를 통해 사용자가 직접 기안하고 결재자의 승인 후 SQL 실행 및 이력을 감사기록으로 저장

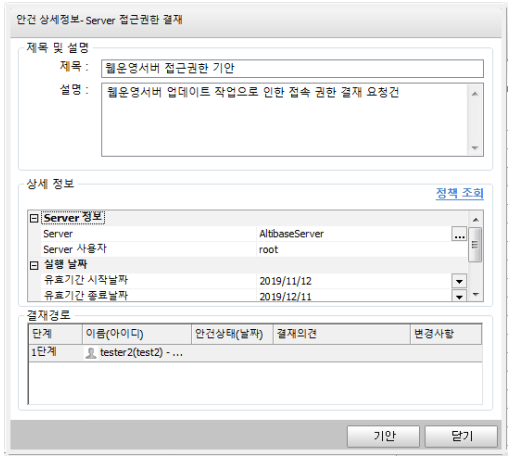


사용자가 SQL 실행권한 기안 요청, 결재자의 승인 완료 후 SQL 실행 가능

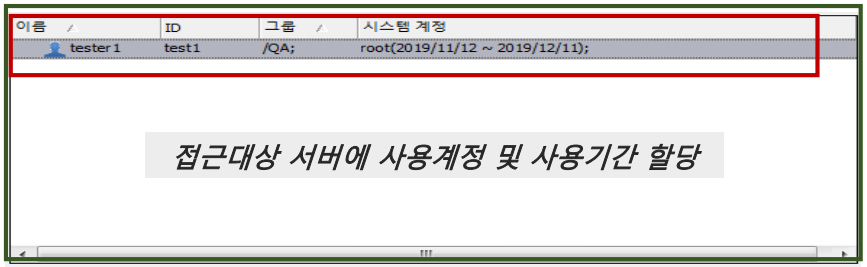
3. 주요기능 | 서버 접근권한 결재

접근 권한이 없는 SERVER에 server 접근권한 결재 기능을 이용하여 사용자가 직접 기안 후 결재자의 승인을 통해 접속하는 기능을 제공



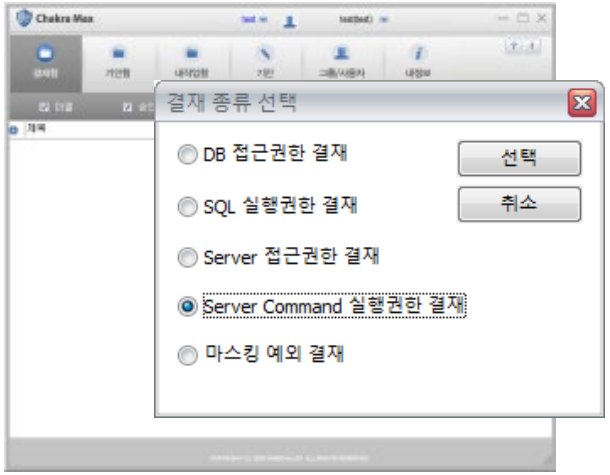


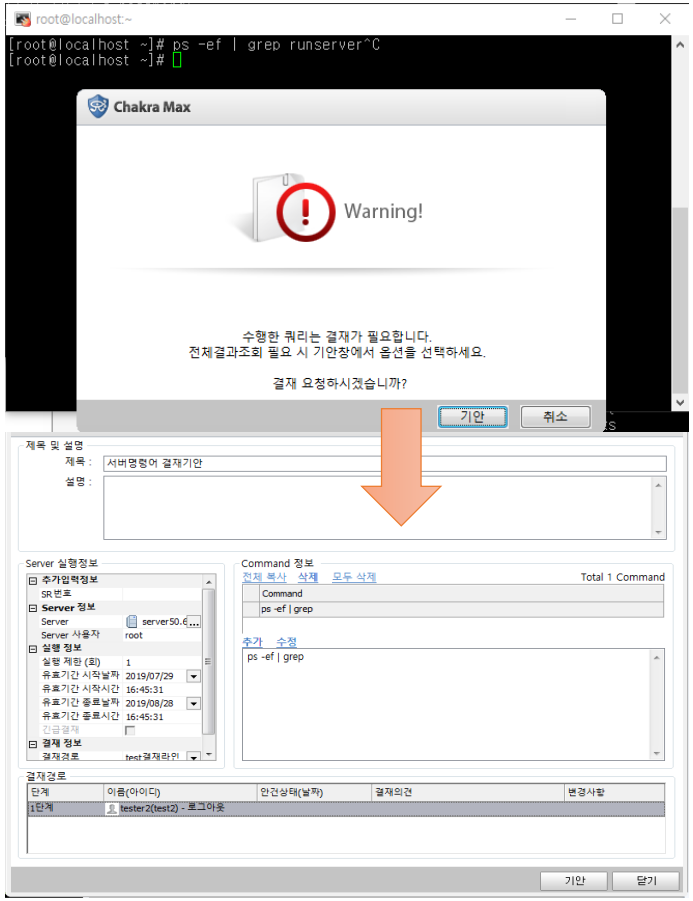
사용자가 DB 접근권한 기안, 결재자의 승인 완료 후 접속 권한 부여

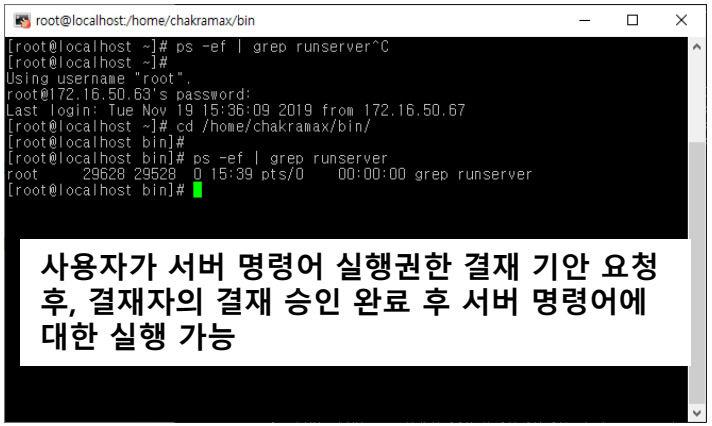


3. 주요기능 | 서버 명령어 실행권한 결재

서버 명령어 결재 정책이 적용된 command 실행시, 서버 명령어 결재를 프로세스를 통해 사용자가 기안 후 결재자의 승인을 통해 서버 명령어를 실행권한을 취득하고, 명령어 실행시 이력을 감사기록으로 저장

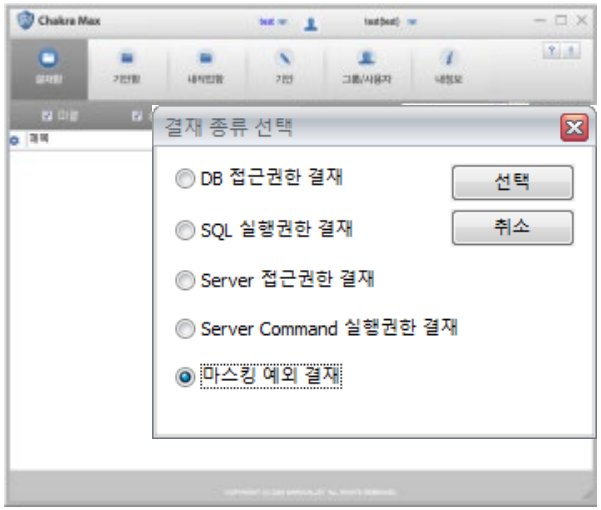


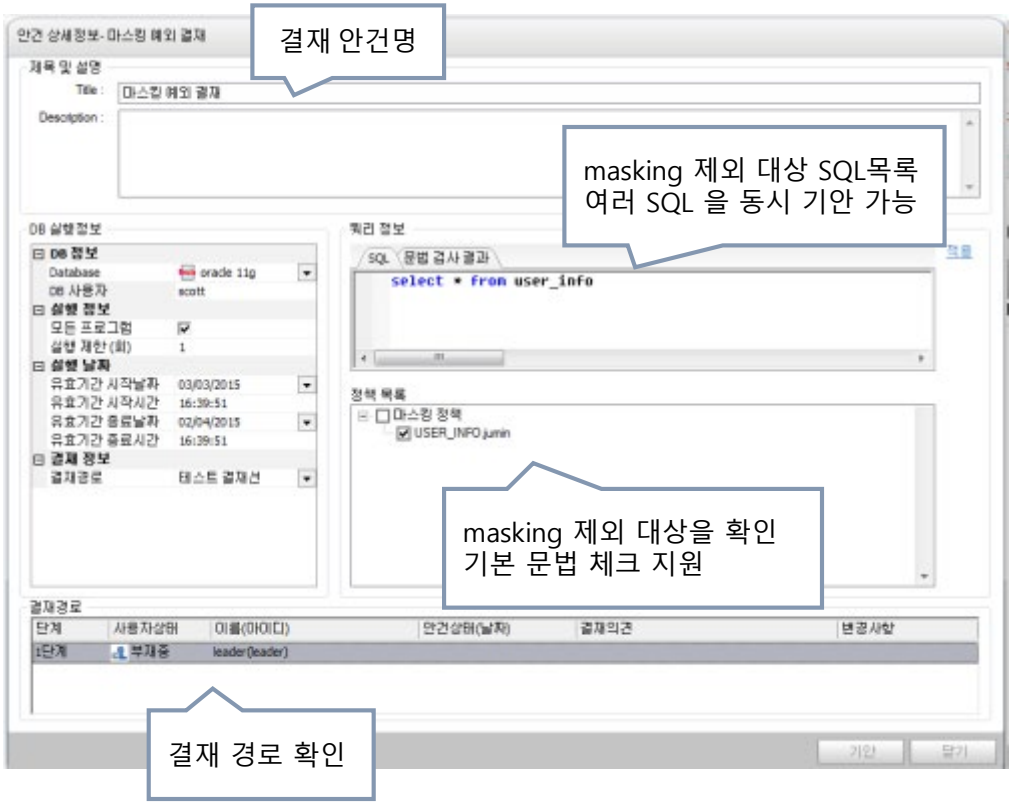




3. 주요기능 | 마스킹 예외 결재

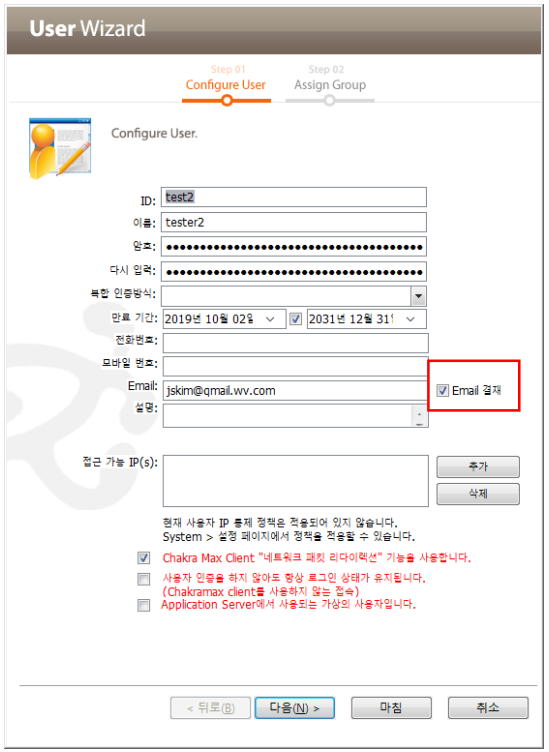
마스킹 지정 테이블/칼럼을 결재를 통하여 실행하는 SQL이 일정기간, 지정된 횟수에 한하여 마스킹 정책에서 예외 할 수 있는 기능 제공

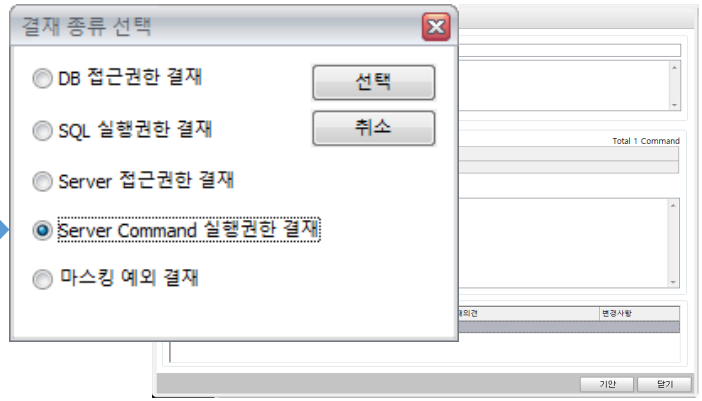


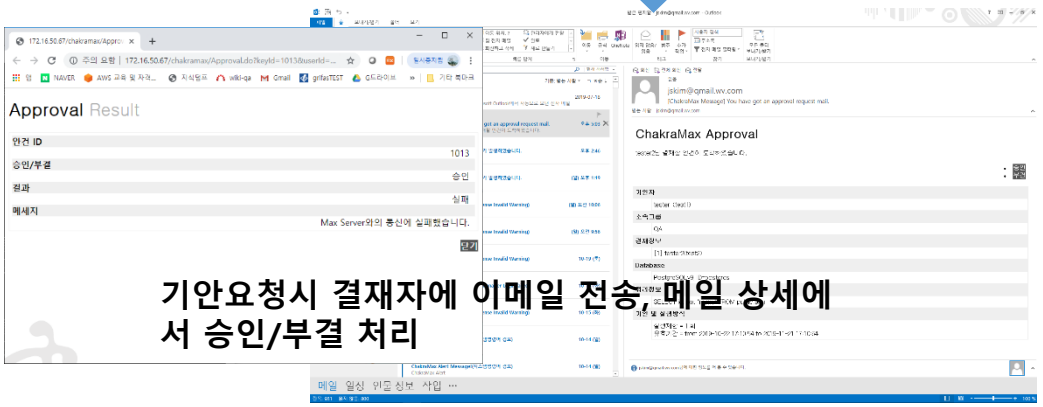


3. 주요기능 | 이메일 결재

이메일 결재 옵션이 설정된 경우, 기안자가 기안 작성 후 결재 요청시 결재자에 이메일로 안건이 전송되고, 결재자가 이메일에서 승인/부결 처리함



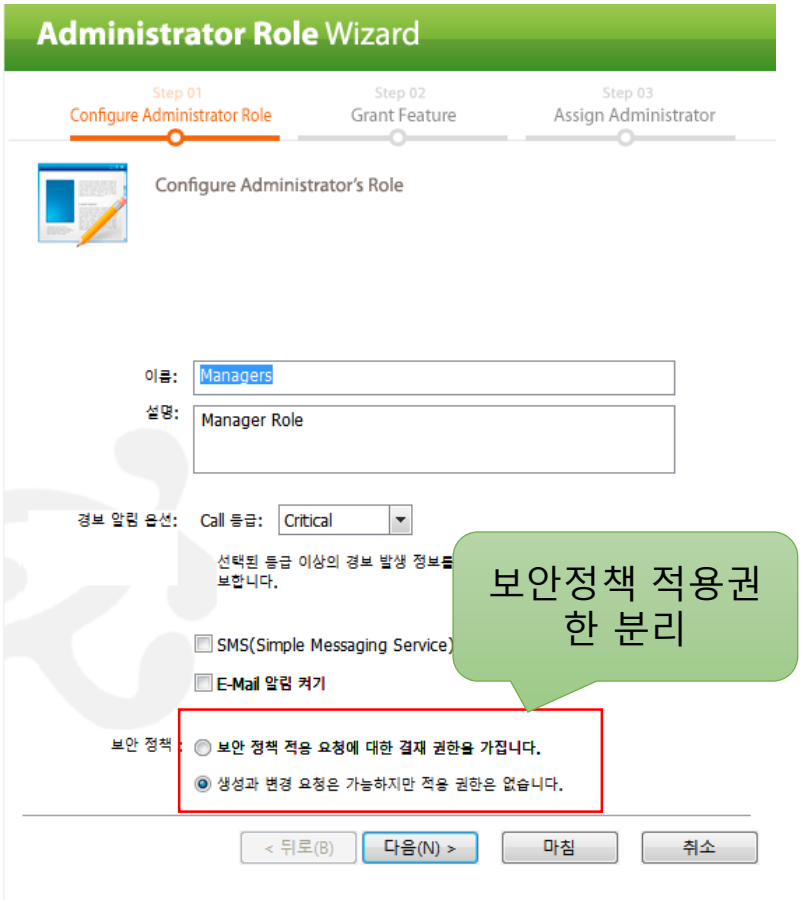


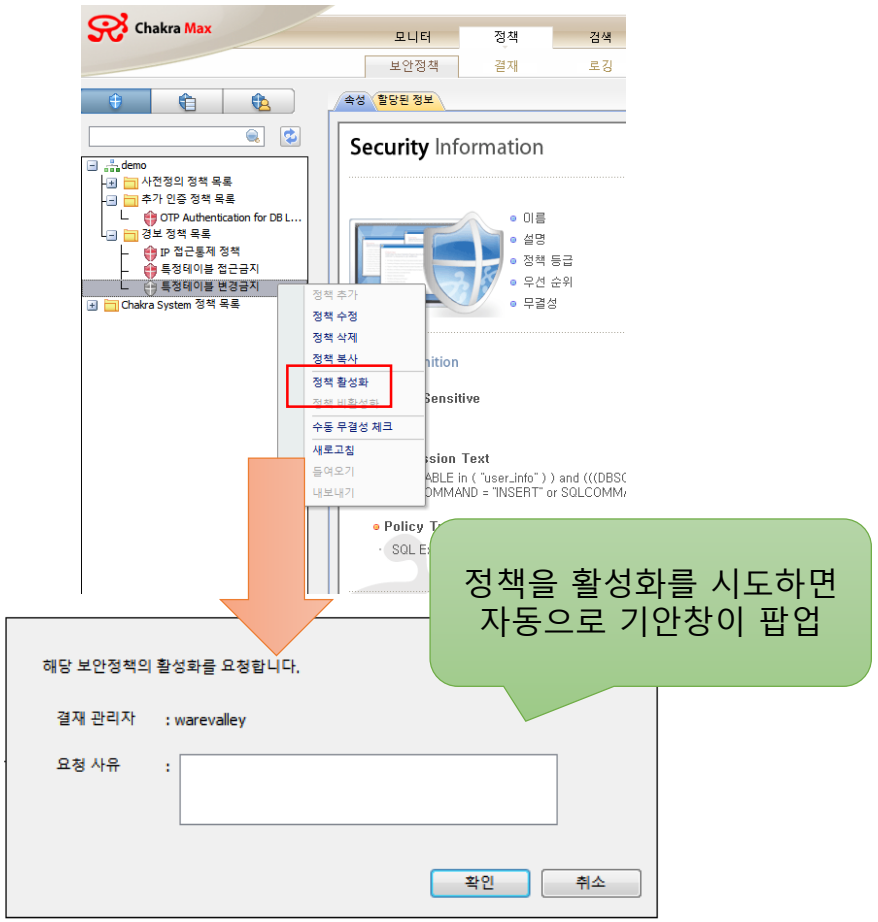


기안요청시 결재자에 이메일 전송, 메일 상세에서 승인/부결 처리

3. 주요기능 | 정책 적용 권한 분리

보안정책의 등록과 적용권한을 분리하여, 적용시점에 기안-승인의 절차를 적용



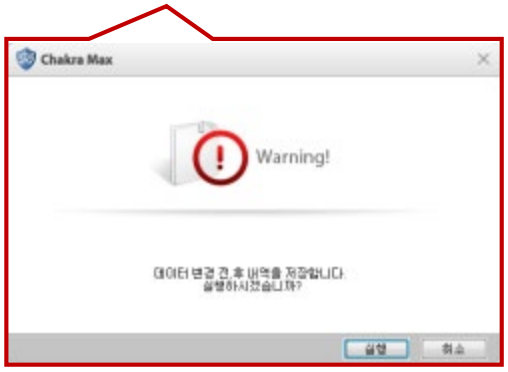


3. 주요기능 | 변경 전/후 데이터 저장

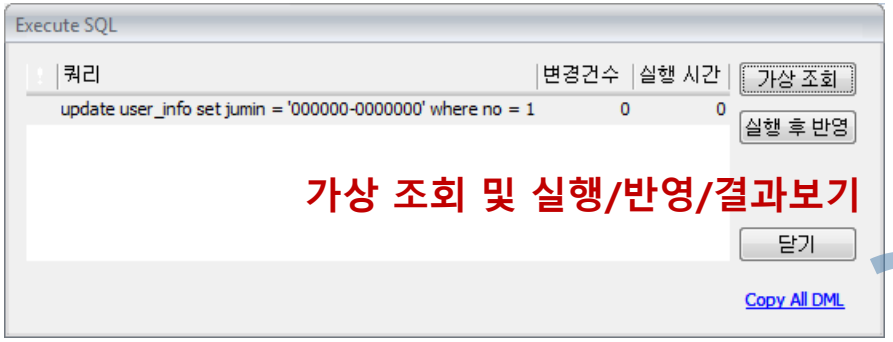
중요 정보의 수정 시 수정 전 대상 데이터 기록, 수정 후 데이터 기록
사용 툴에 관계없이 지원 (결재 & 비 결재)

```
update user_info set jumin = '000000-0000000' where no = 1;
```

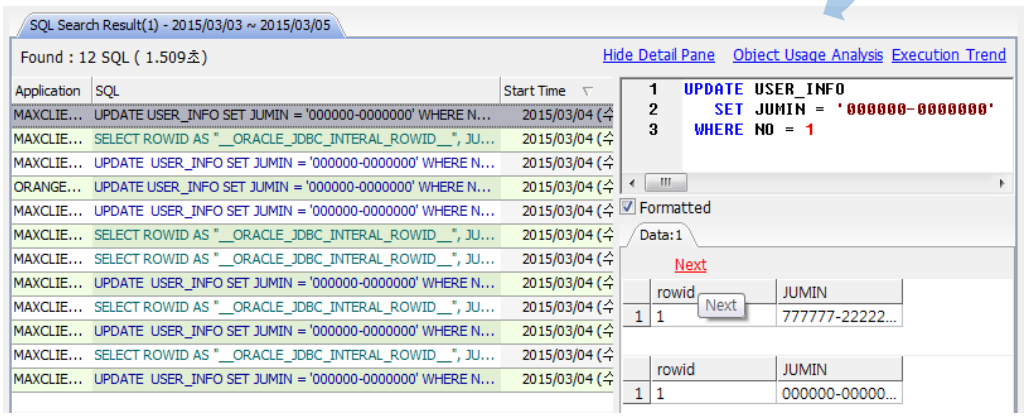
update SQL 실행



정책 차단 팝업



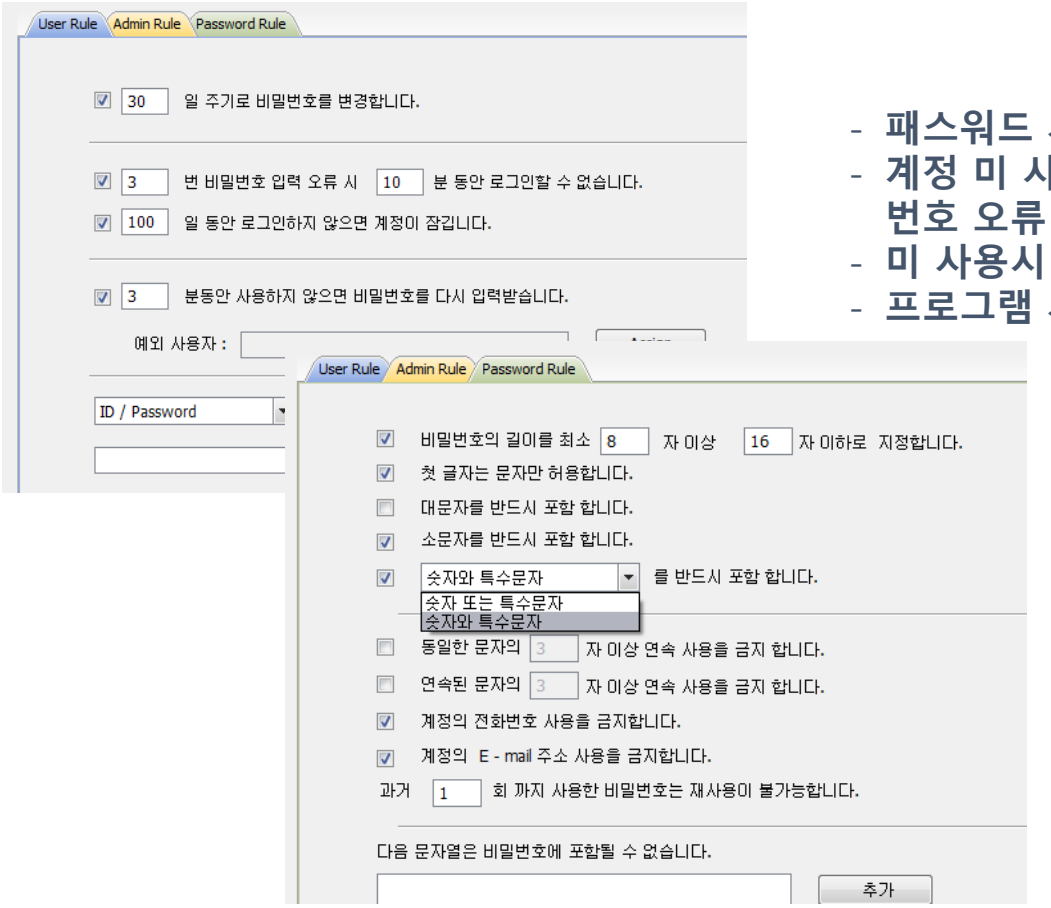
가상 조회 및 실행/반영/결과보기



변경 전/후 데이터 확인

3. 주요기능 | 보안계정 관리정책

보안계정에 대해 접속 및 패스워드 대한 다양한 정책을 제공

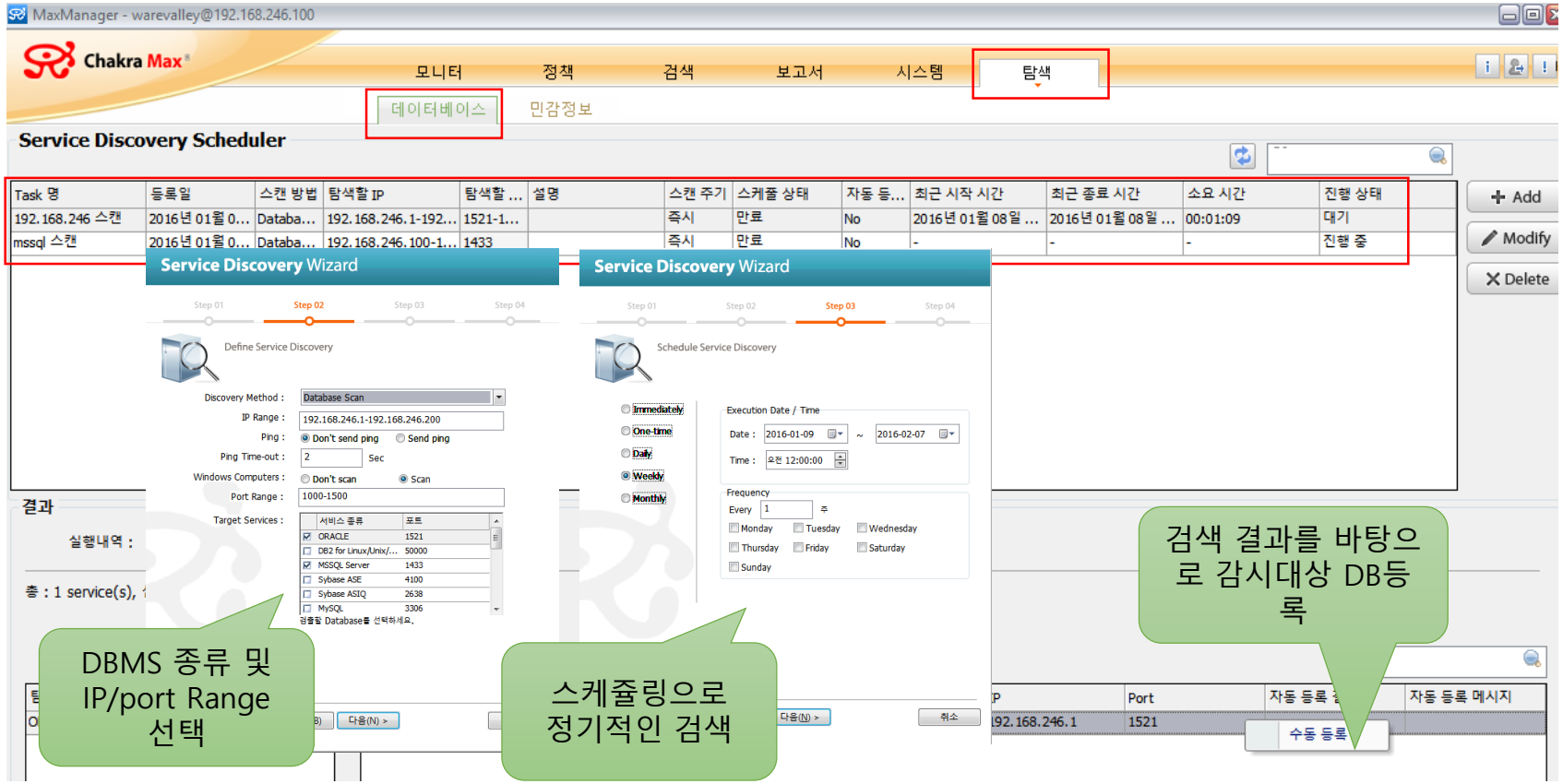


- 패스워드 사용기간 설정 기능
- 계정 미 사용에 따른 계정 잠김 기능 및 비밀번호 오류 시 계정 잠김
- 미 사용시 비밀번호 재 입력 기능
- 프로그램 사용 시 초기 비밀번호 설정 기능

- 패스워드 길이의 관리
- 숫자 및 특수문자를 포함한 구성
- 패스워드에 개인정보 포함 제한
- 과거 사용 비밀번호 제한
- 특정 문자열 패스워드 포함 제한

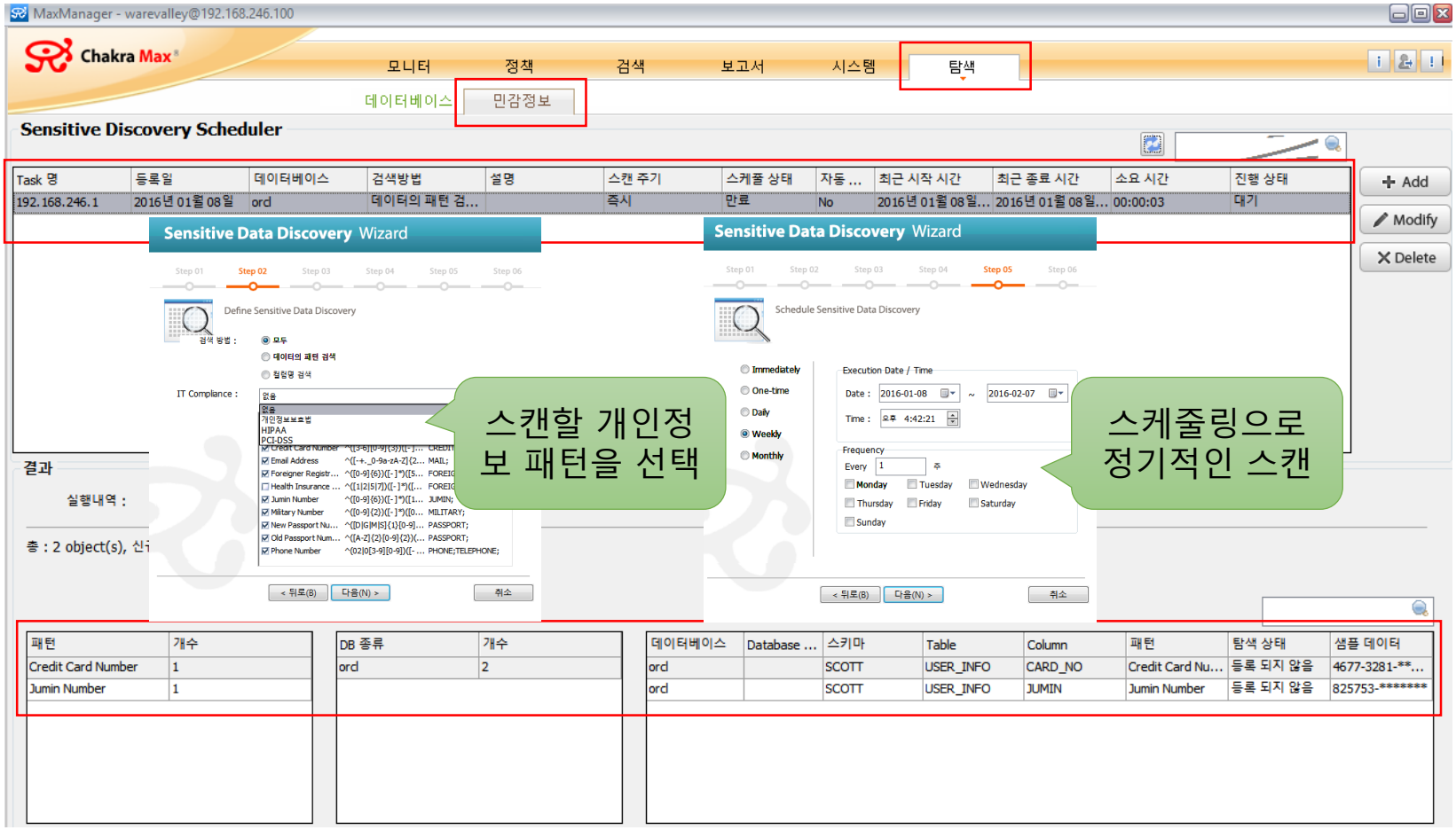
3. 주요기능 | Auto Discovery – 데이터베이스 서비스 탐색

네트워크상의 추가된 데이터베이스를 자동 검색하여 감시대상 DB로 등록
스케줄링으로 정기적인 검색을 제공



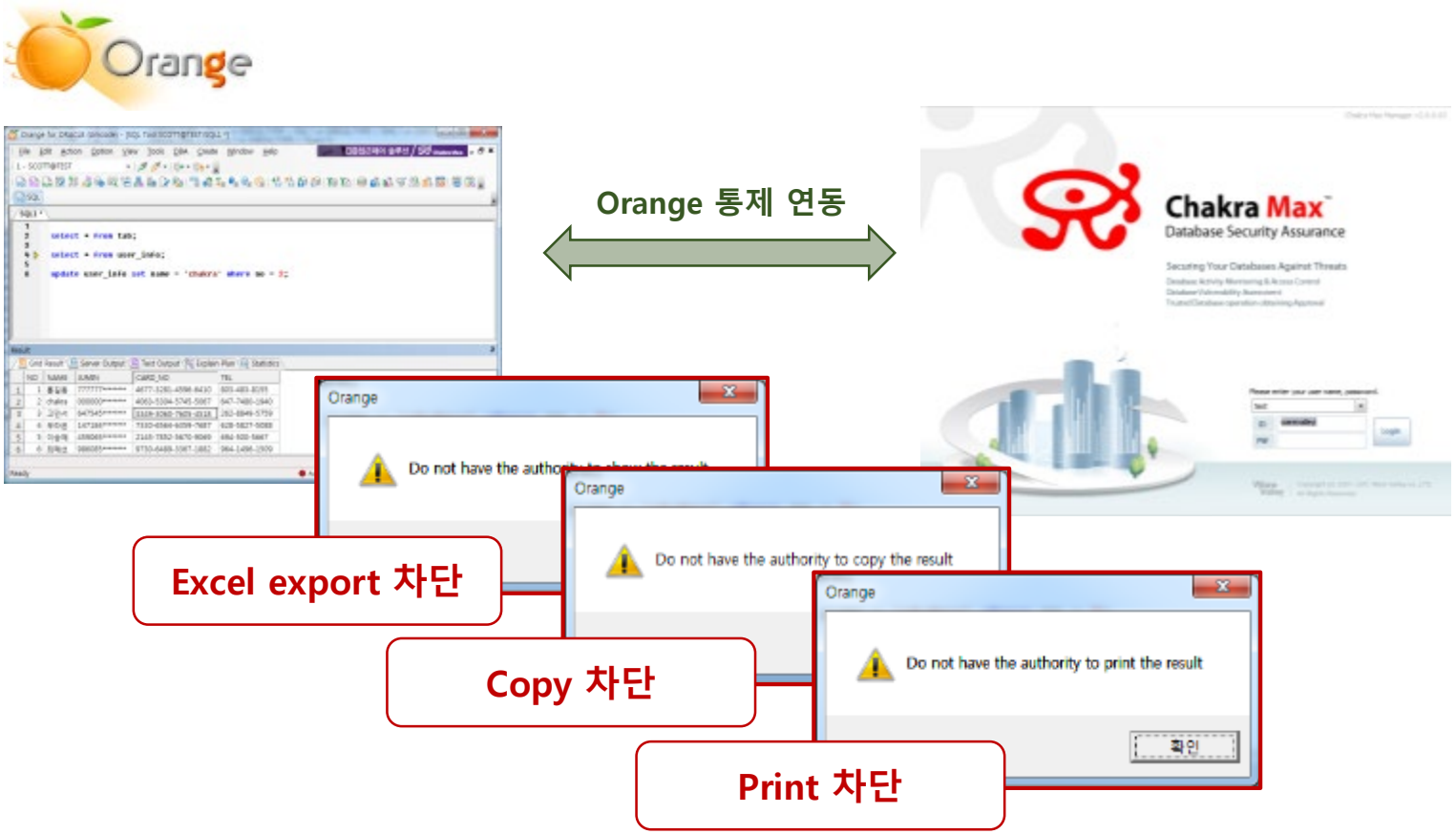
3. 주요기능 | Auto Discovery – DB 내의 민감정보 탐색

데이터베이스 테이블 및 컬럼을 패턴스캔 하여 민감정보 유무를 감지,
감지된 데이터의 샘플데이터로 민감정보 대상으로 지정하여 접근이력을 조회 / 리포팅



3. 주요기능 | 메뉴통제(오렌지연동)

파일저장, 복사, 프린트 기능을 차단하여 중요정보의 유출을 방지하고 보안을 강화

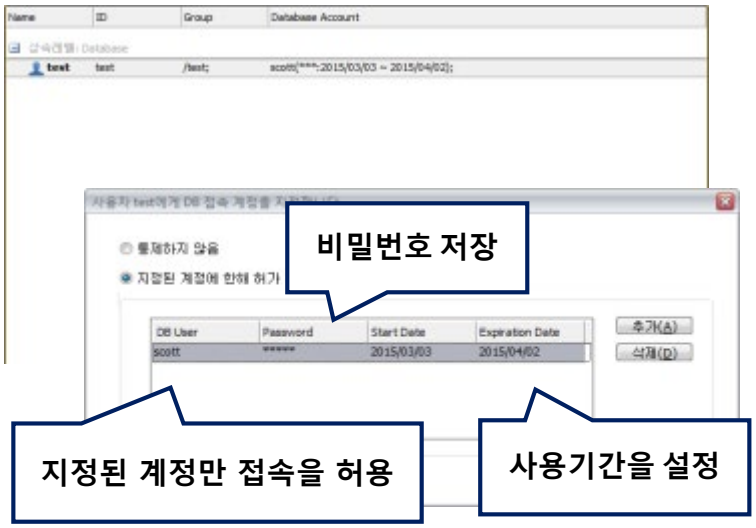


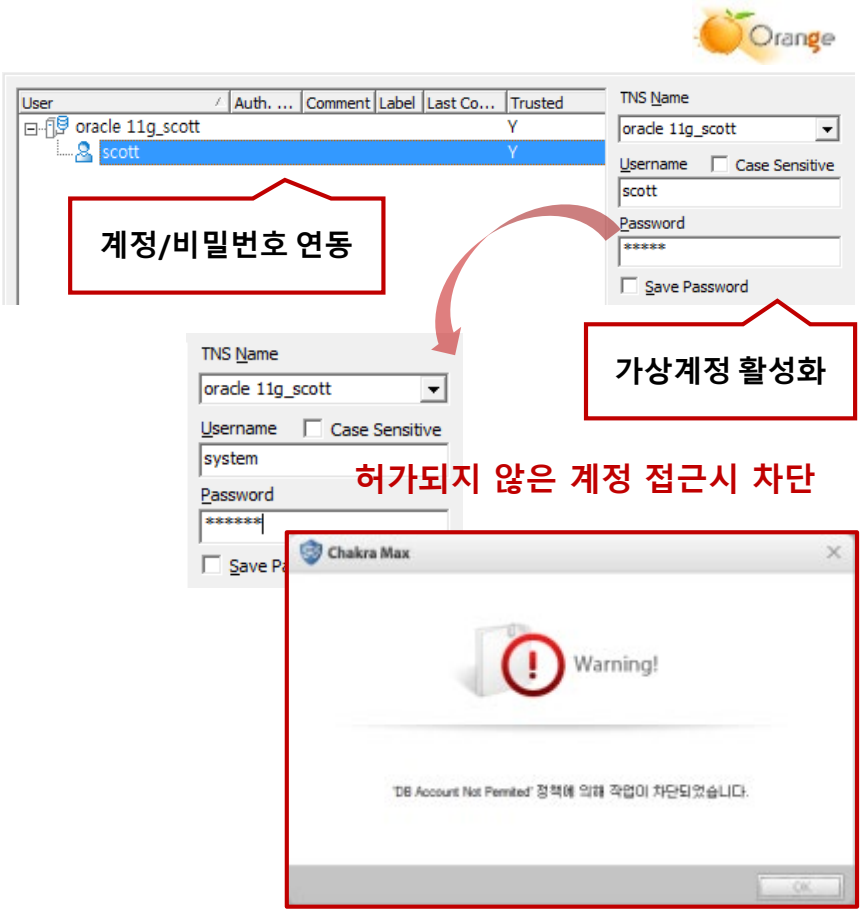
본 기능은 WareValley Orange와 연동 시 제공되는 기능입니다.

3. 주요기능 | DB 계정은닉(오렌지연동)

가상계정 기능을 연동하여 DB 계정의 통제 및 비밀번호 은닉

Chakra Max 가상계정 설정

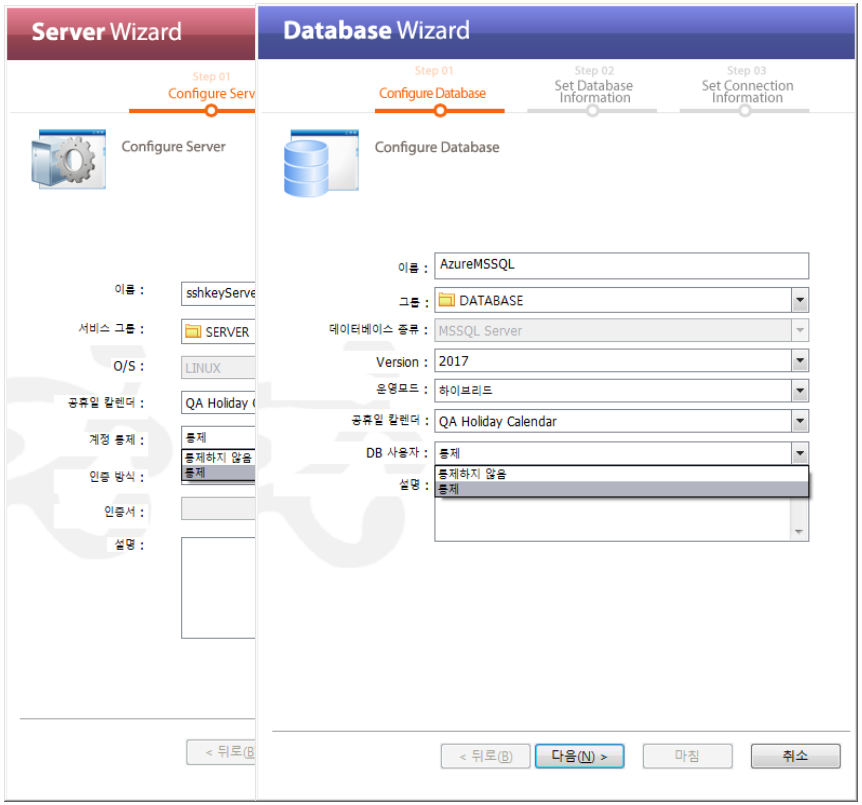




본 기능은 WareValley Orange와 연동 시 제공되는 기능입니다.

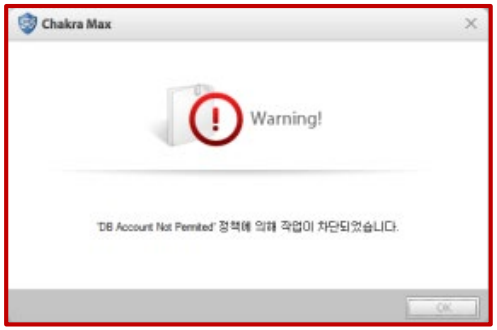
3. 주요기능 | DB / 서버 가상 계정 통제

가상계정 기능을 연동하여 사용자별로 할당된 계정에 대해서만 접속 권한을 허용하고 이외의 계정에 대해서는 통제



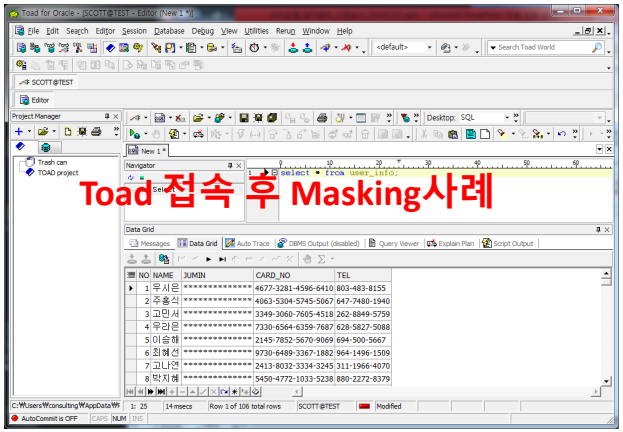
Chakra Max 가상계정 설정

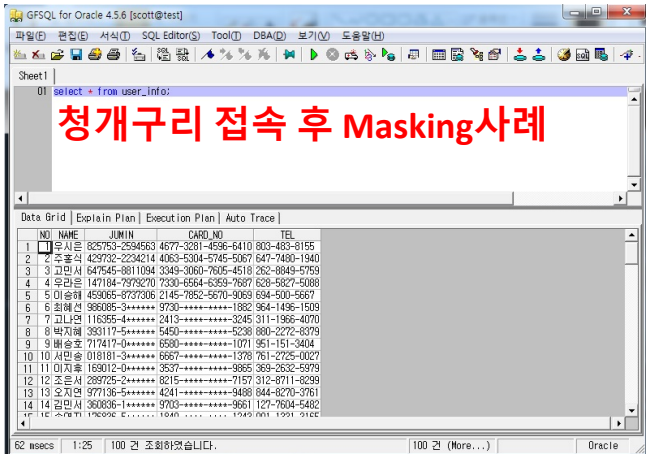
허가되지 않은 계정 접근시 차단



3. 주요기능 | 비인가 어플리케이션 접근통제

DB에 접속하는 Application의 Signature를 확인, 위변조 Application도 탐지 및 차단





어플리케이션 시그니쳐 기능을 이용한 위변조 탐지 기능 제공

3. 주요기능 | 사용자 2-Factor 인증

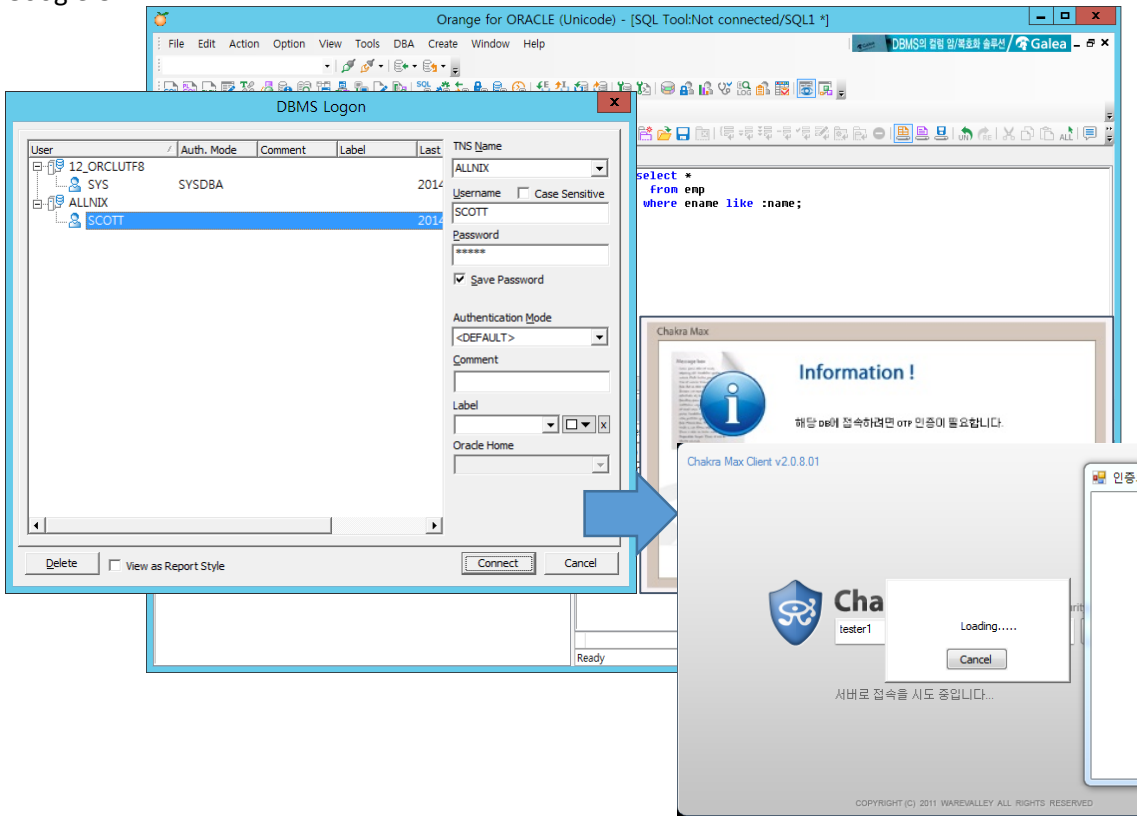
- **DB접근제어 계정 및 DB접속 계정에 대한 다양한 인증 적용**
- **유저 등록 화면에서 복합인증 등을 지정하여 유저 생성하여 로그인 정책 관리**

- 사례

OTP 인증: 외환은행, 대우증권, KEB 하나은행, 수출입은행

인증서(PKI), Biometric(지문) : KB은행

Google OTP



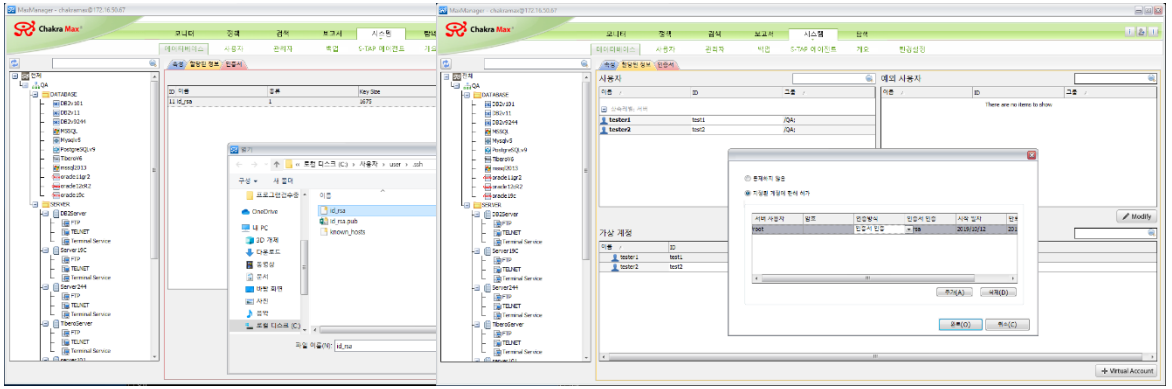
폐쇄 망에서도 가능한 Mobile OTP

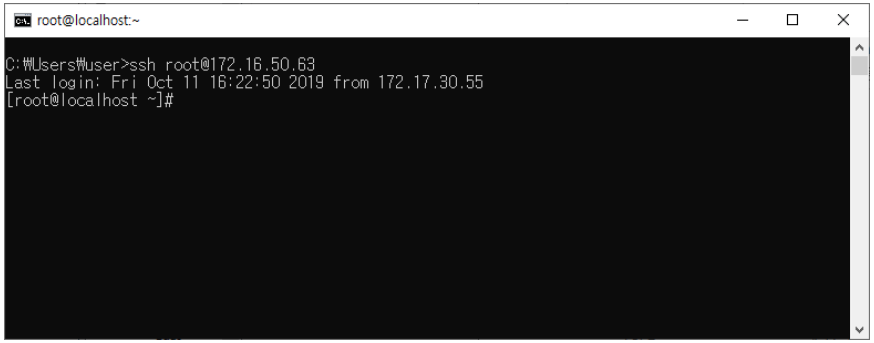
3. 주요기능 | 사용자 인증서 로그인 인증

인증서 로그인 방식은 서버 접속시 비밀번호 대신 SSH key를 제출하는 방식으로, 비밀번호 보다 높은 수준의 보안을 필요로 하거나, 비밀번호 입력 없이 자동으로 서버에 접속할 때 사용

Chakra max manager 프로그램을 통해 SSH Key의 비공개 키를 사전 등록하고 사용자의 가상계정에 할당하면, 사용자는 패스워드나 인증서 없이 권한을 할당 받은 서버에 chakra 의 인증을 거쳐 자동 로그인 할 수 있다.

지원 프로토콜 : SSH, SFTP 암호화키 지원 : RSA/DSA





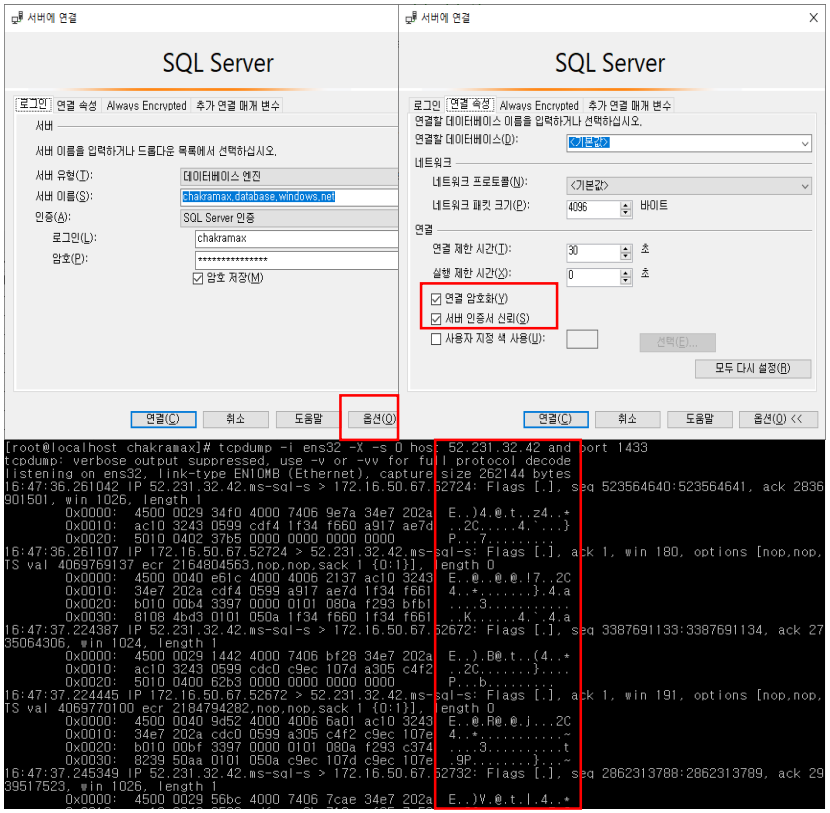
할당 받은 서버에 접속시 패스워드 입력 없이 자동 로그인 처리

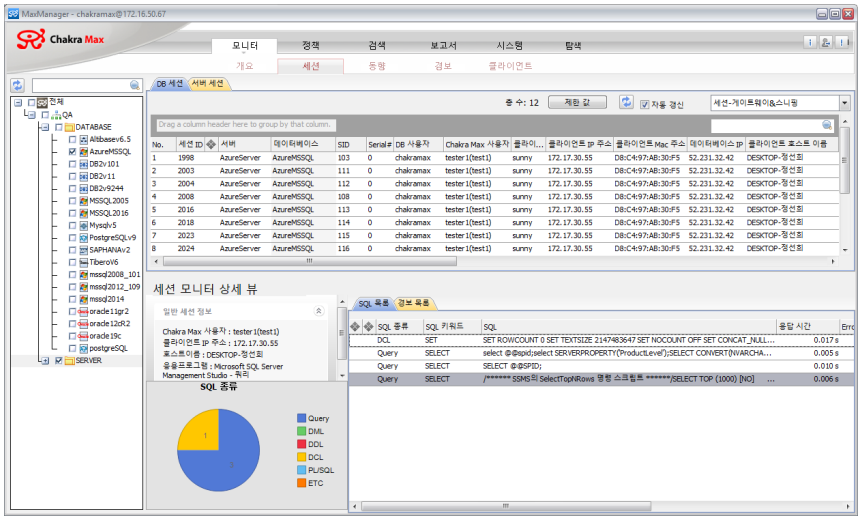
3. 주요기능 | SSL/TSL 를 사용하여 암호화 연결하는 데이터베이스 지원

DB 접속시 TLS 암호화 통신을 하는 데이터베이스의 통신을 지원(SSL Proxy)

애플리케이션에서 SSL(Secure Socket Layer) 또는 TLS(전송 계층 보안)를 사용하여 암호화 연결하는 데이터베이스를 지원

- 지원 데이터베이스 : **MSSQL, Mysql, Maria, PostgreSQL**



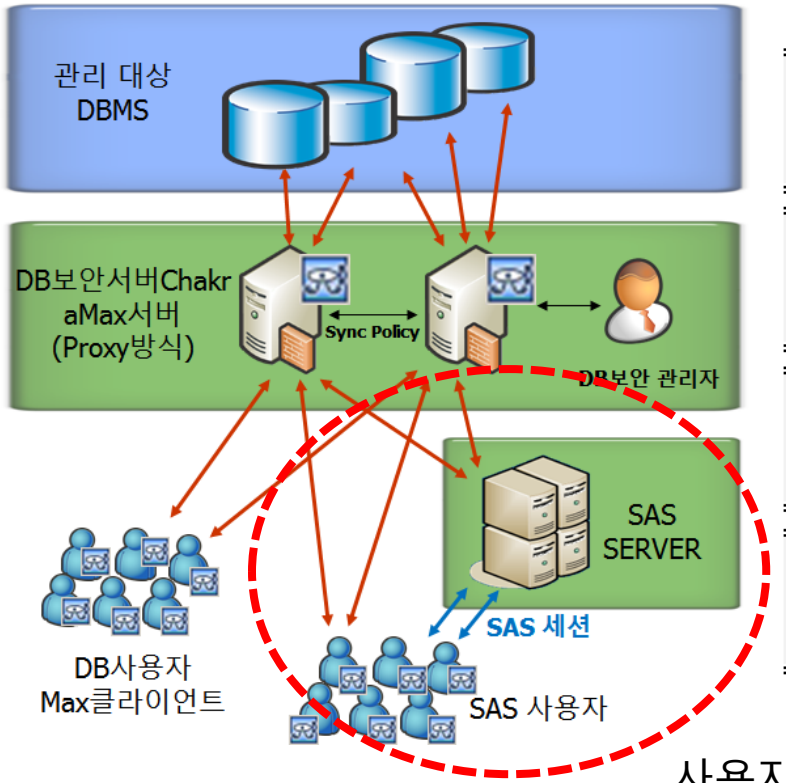


DB에 접속시 “연결 암호화” 옵션에 따라, 전송 데이터가 암호화되어 통신됨.

샤크라는 proxy 암호화 연결을 중계하여, 통제 및 감사로그를 수집

3. 주요기능 | SAS, OLAP, BO 등 3 Tier 사용자의 비정형 쿼리 통제

여러 DB의 주요정보에 접근 가능한 시스템을 Chakra Max와 연동하여 식별 및 통제



Proxy방식으로 운영되는
ChakraMax는 SQL 실행을 통제

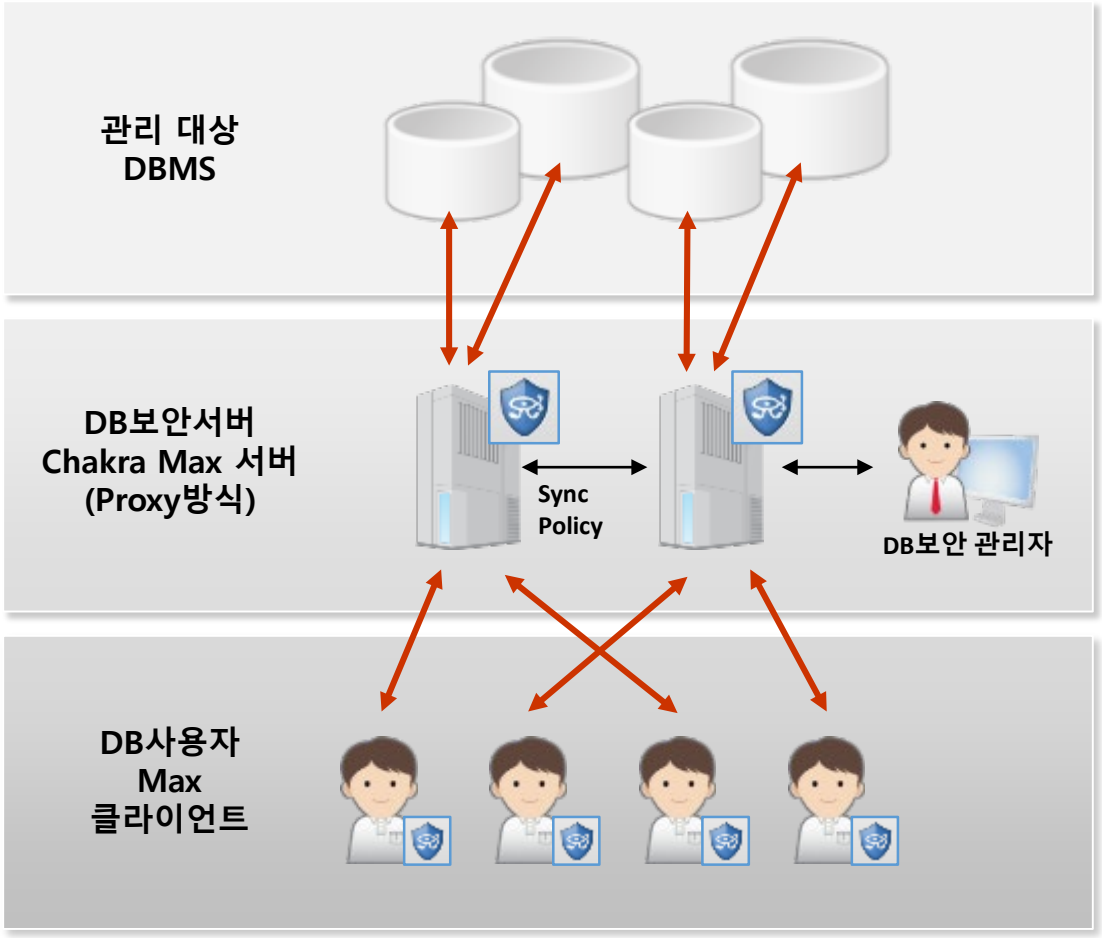
사용자는 DB직접 접속이 통제되며
보안 서버를 경유한 접속만 허가됨

보안 관리자는 ChakraMax서버에
접속하여 접근제어 정책을 설정

SAS 서버의 DB 접속 정보를
ChakraMax 서비스로 설정

사용자 별 고유 DB 계정(행번 등)
사용으로 사용자 식별

Chakra Max는 고객의 DB환경 변화 없이 기존 구성 그대로 적용 가능



Proxy방식으로 운영되는
Chakra Max는 SQL 실행을 통제

사용자는 DB직접 접속이
통제되며 보안 서버를 경유한
접속만 허가됨

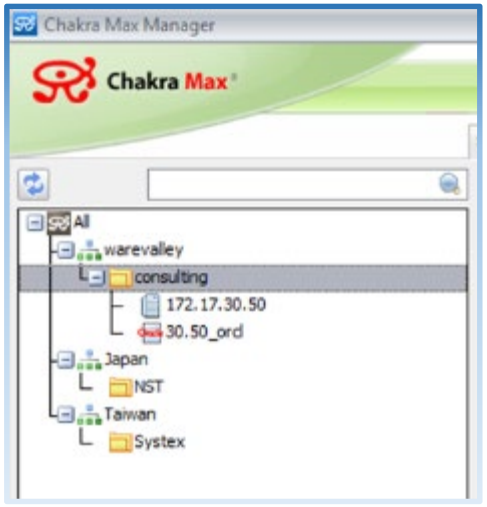
보안 관리자는 Chakra Max 서버에
접속하여 접근제어 정책을 설정

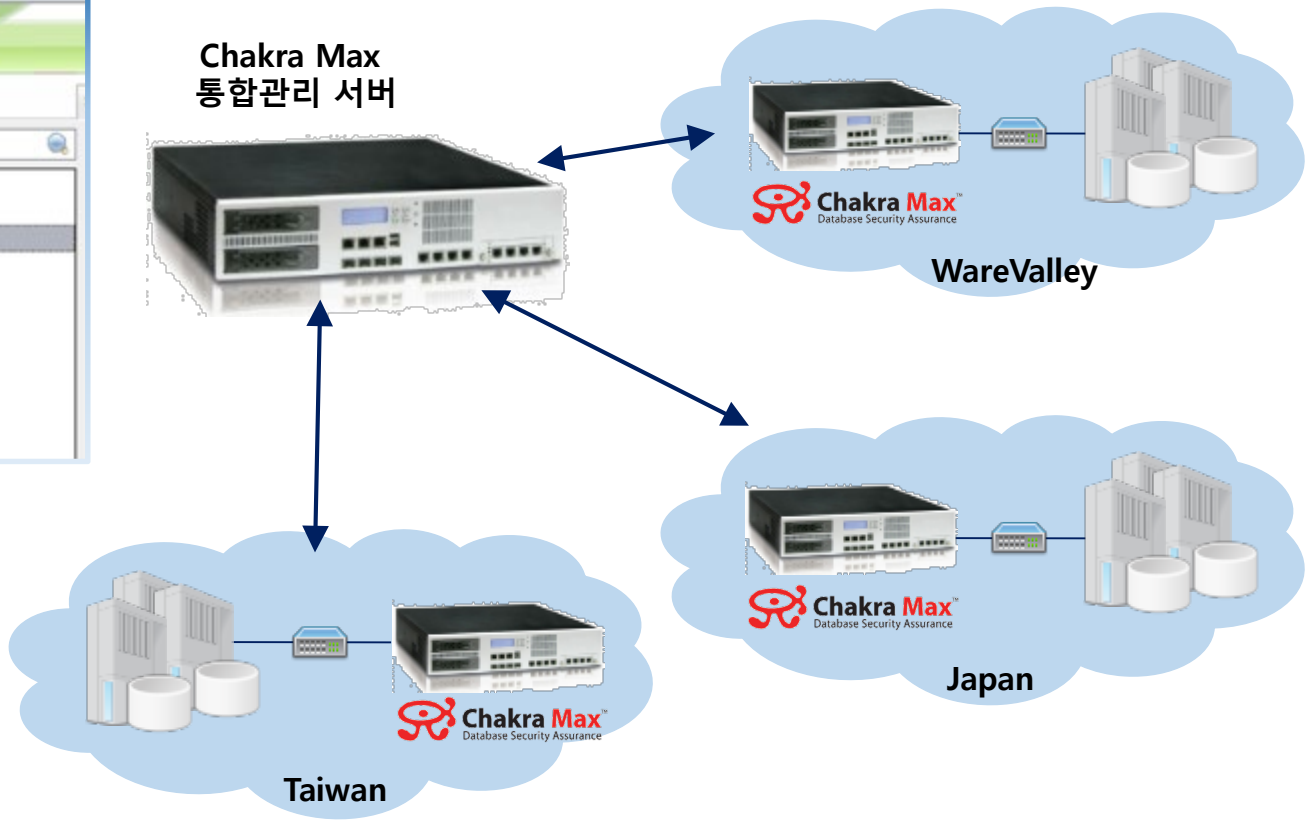
Chakra Max서버 이중화 구성을
통해 업무 연속성을 확보

PC의 셋팅 변경 없이
Agent 설치 만으로 사용자 인증 및
DB 접근 경로 변경 구성

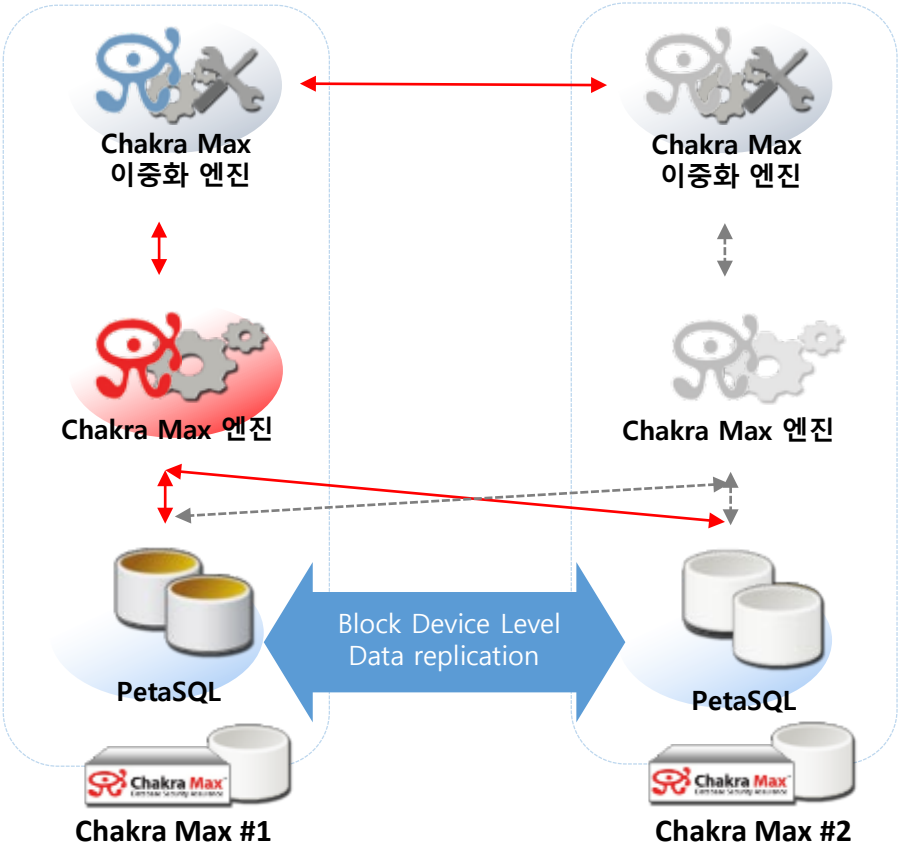
Central Management(CM)기능을 통한 중앙 모니터링

(통합 Alert 모니터링 / 보안정책 관리 / 로그 검색 / 보고서 생성이 가능)





Chakra Max 엔진 및 로그데이터 이중화 기능



Partition-Level Replication 적용으로
"감사 로그 유실 방지"

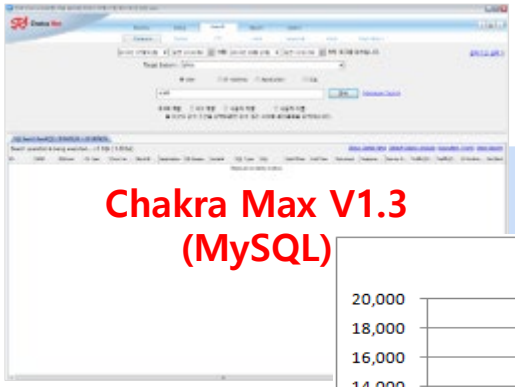
엔진 이중화 및 PetaSQL 이중화를 통한
"업무 연속성 보장"

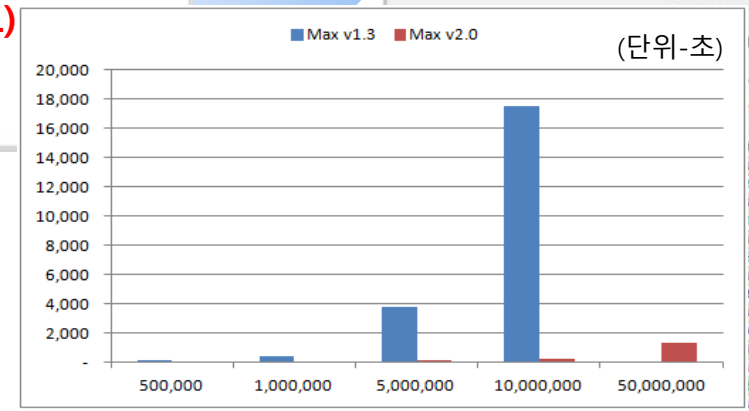
- 장애 대비를 위한 Active-Standby 구성 지원
- Load balancing을 위한 Active-Active 구성 지원

DB 접근제어서버의 엔진 이중화 및 로그용 DBMS의 이중화로 서비스의 연속성 확보 및 로그데이터 유실 방지 강화

Column Stored DBMS (PetaSQL) 탑재로 더욱 빨라진 로그검색

Fast-Loading / Real-time Analysis 데이터 베이스
Column based database로 OLAP에 특화
기존 Chakra Max V1.3 대비 약 1600%이상의 검색 효율 증가



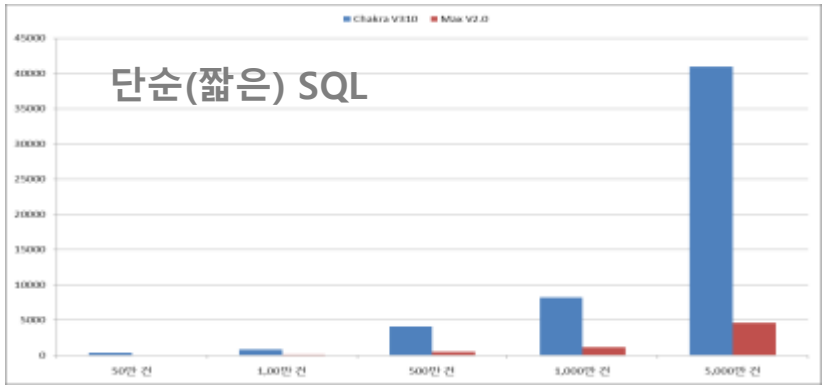


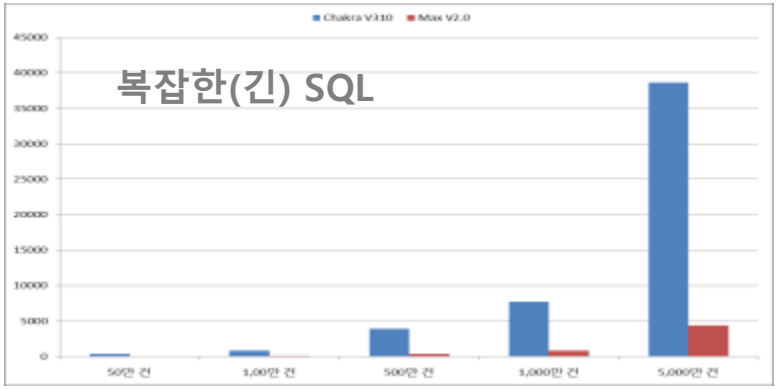
	500,000건	1,000,000건	5,000,000건	10,000,000건	50,000,000건
Max v1.3	192	472	3,794	17,580	N/A
Max v2.0	13	28	128	240	1,302

Column Stored DBMS (PetaSQL) 탑재로 로그기록용 디스크의 효율적 운영

Dictionary 기반 중복데이터 제거를 통한 데이터 감소
기본 압축 기능 강화를 통한 디스크 사용량 감소

SQL 로그 데이터 저장 시 MySQL 대비 약 1/10 수준의 저장 공간 사용



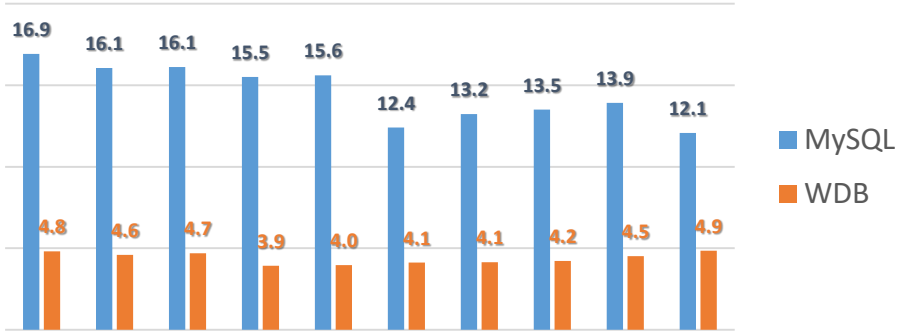


	50만 건	1,00만 건	500만 건	1,000만 건	5,000만 건	비고
Chakra V3.1	402	804	4,096	8,192	40,960	select * from dual_NUMBER where dummy_NUMBER_ = _NUMBER_
Max V2.0	54	104	491	1,135	4,616	
Chakra V310	385	797	3,890	7,716	38,619	Select * from dual where dummy = _NUMBER_
Max V2.0	52	74	388	844	4,338	

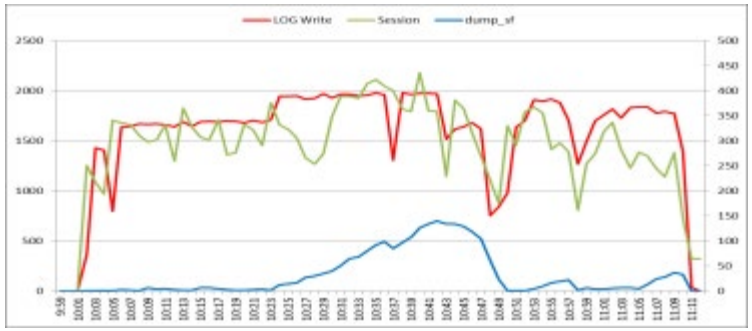
동일한 DB에 대하여 Chakra V3.1(MySQL)과 Chakra Max V2.0(PetaSQL) 를 이용하여 감사 시도 한 후 로깅 된 데이터 용량

Column Stored DBMS (PetaSQL) 탑재로 로그기록 시간 단축 및 I/O 병목 해결

Chakra Max Repository 사용시 로그 Log write 시간
- 기존 MySQL 대비 약 200% 로그 기록 효율 증가



단위 : 초



180byte 20만 row insert 20회 시도 후 최저, 최고 값 제외 후 10회에 대한 평균 값 산출

4. 관리기능 | 데이터 위변조 – 테이블 보호 기능

로그 데이터의 위변조 방지를 위하여 PetaSQL의 로그 저장 테이블에 Chakra Max 엔진만 쓰기 및 변경이 가능하며 사용자 접근 시 읽기로 제한

로그 위변조 방지를 위한 임의의 로그테이블 쓰기 방지 기능 (Chakra Max 엔진만 가능)

	inst_name	client_ip	db_user	date	sql_text
1	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT DBMS_TRANSACTION.LOCAL_TRANSACTION_ID FROM DUAL
2	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT DBMS_TRANSACTION.LOCAL_TRANSACTION_ID FROM DUAL
3	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT DBMS_TRANSACTION.LOCAL_TRANSACTION_ID FROM DUAL
4	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT DBMS_TRANSACTION.LOCAL_TRANSACTION_ID FROM DUAL
5	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT /*+ LEADING(S) */ INST_ID, SID, SERIAL#, OSPID, ORANGE.ORANGE_FN_HOST_NAME,
6	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT USERENV('□'), SYS_CONTEXT('□','□') FROM DUAL
7	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT S.SERIAL#, P.SPID, S.SERVER FROM V$SESSION S, V$PROCESS P WHERE S.SID = □ AND
8	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT * FROM V$NLS_PARAMETERS
9	oracle	192.168.0.200	SCOTT	2015-03-04	ALTER SESSION SET NLS_LANGUAGE='□' NLS_TERRITORY='□' NLS_CURRENCY='□'
10	oracle	192.168.0.200	SCOTT	2015-03-04	BEGIN DBMS_APPLICATION_INFO.SET_MODULE(:Module,:Action); END;
11	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT USERNAME FROM ALL_USERS
12	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT OBJECT_NAME, OBJECT_TYPE FROM ALL_OBJECTS WHERE UPPER(OWNER) = UPPER(:owner)
13	oracle	192.168.0.200	SCOTT	2015-03-04	SELECT /*+ LEADING(S) */ INST_ID, SID, SERIAL#, OSPID, ORANGE.ORANGE_FN_HOST_NAME,

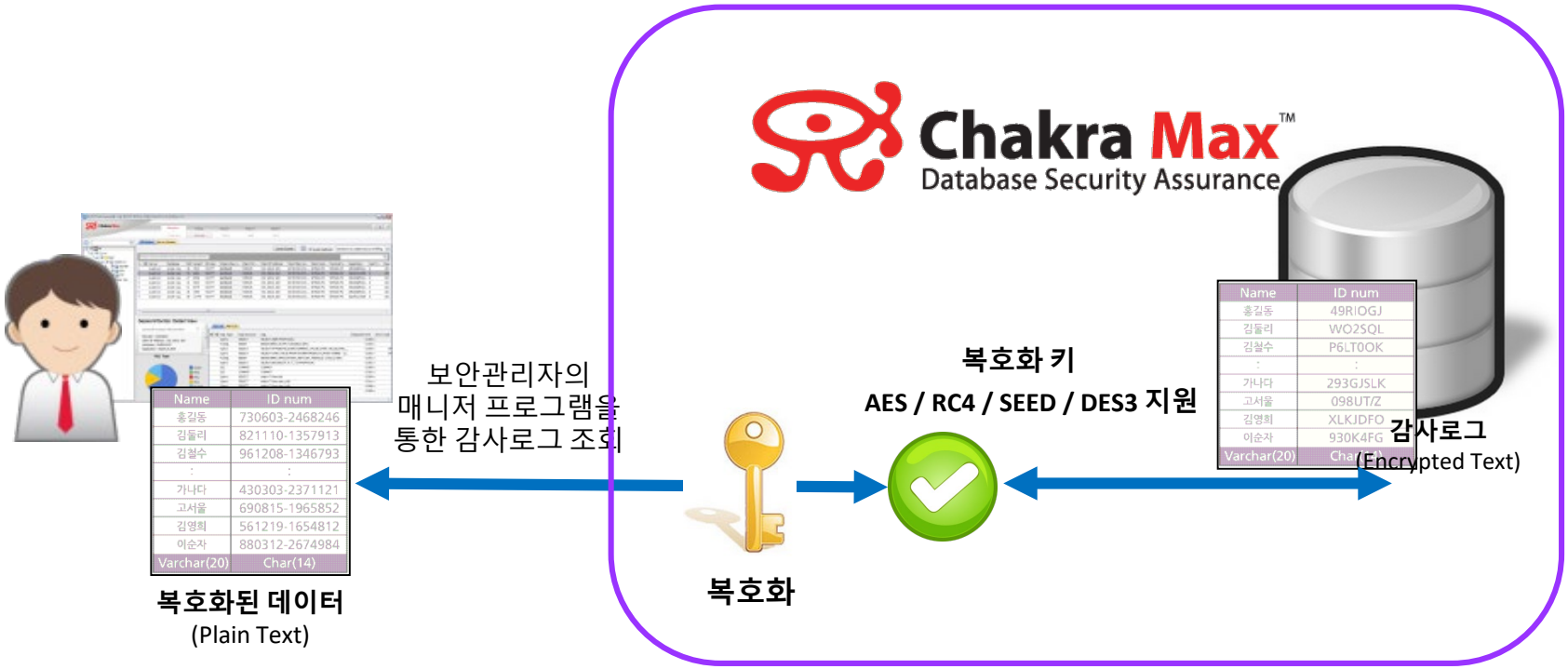
엔진에서 저장된 로그데이터

사용자가 Repository DB에 접근하여 로그 테이블에 update, delete 등을 시도하였을 테이블이 보호되어 실행을 할 수 없음

```
wdb sql> update sql_log_20150304 set sql_text = 'select * from tab;';
UPDATE: cannot update protected table 'sql_log_20150304'
wdb sql>
wdb sql> delete from sql_log_20150304;
DELETE FROM: cannot delete protected table 'sql_log_20150304'
```

4. 관리기능 | 데이터 위변조– 감사로그 암호화 지원

엔진이 감사 테이블을 생성시 암호화된 테이블로 생성하고, 로그데이터를 암호화하여 저장함으로써 실제 데이터를 식별할 수 없도록 감사로그 데이터의 보안 기능을 강화
관리자가 매니저 프로그램을 통해 로그 조회시에 복호화 키를 이용하여 복호화된 로그를 표시

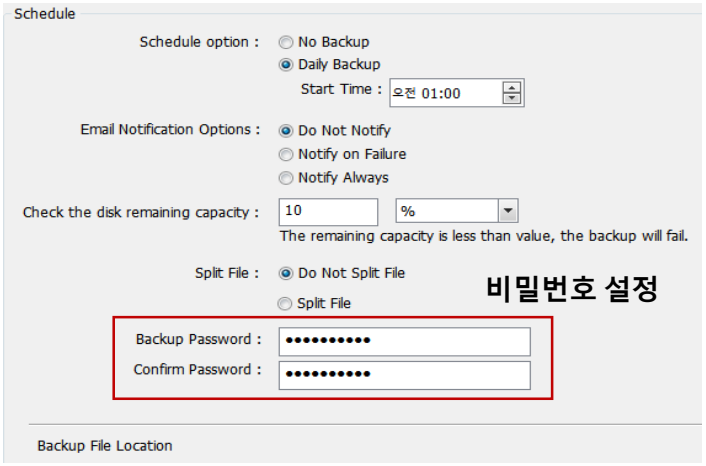


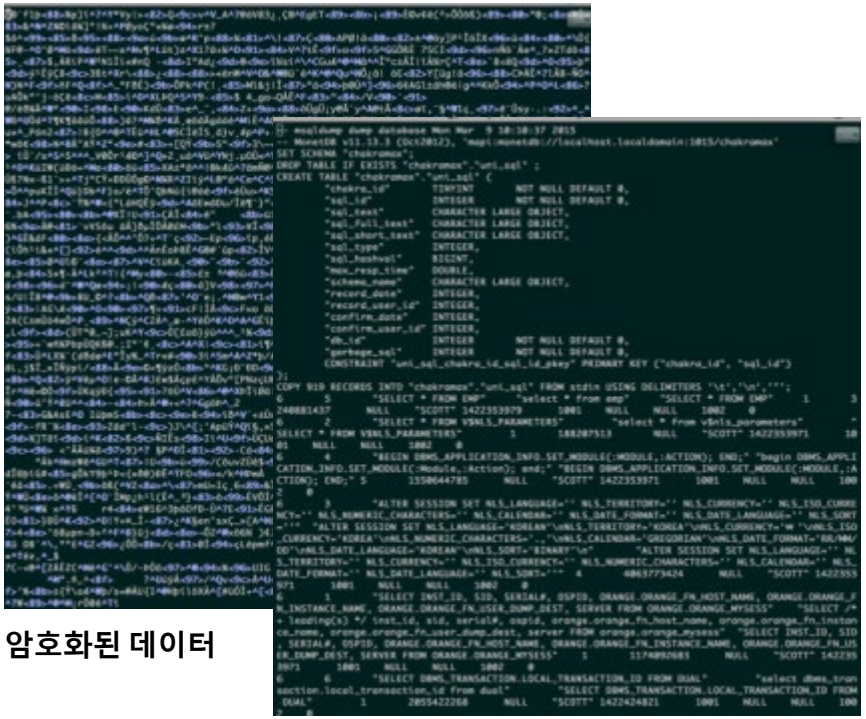
** 감사 로그 테이블의 컬럼을 암호화하여, 복호화키 없는 불법적인 데이터 열람시 식별 불가

4. 관리기능 | 데이터 위변조 – 백업 암호화

일일 백업 파일을 암호화 알고리즘을 적용하여 백업 로그의 열람 및 수정을 방지

암호화된 백업 데이터는 Chakra Max에서만 복호화하여 백업 복구에 사용 가능



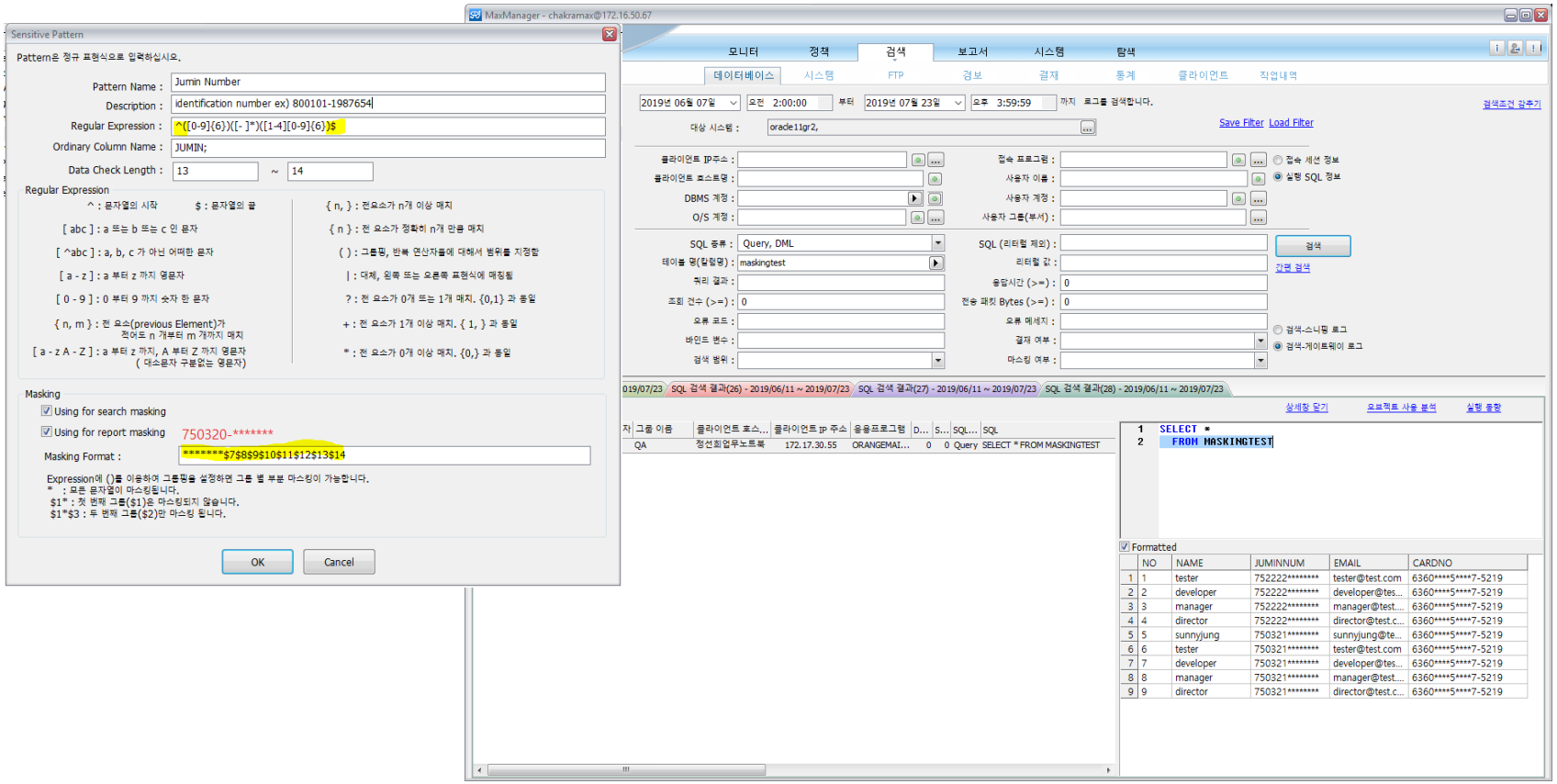


암호화된 데이터

일반 데이터

4. 관리기능 | 개인정보 보호– 감사데이터 마스킹 처리

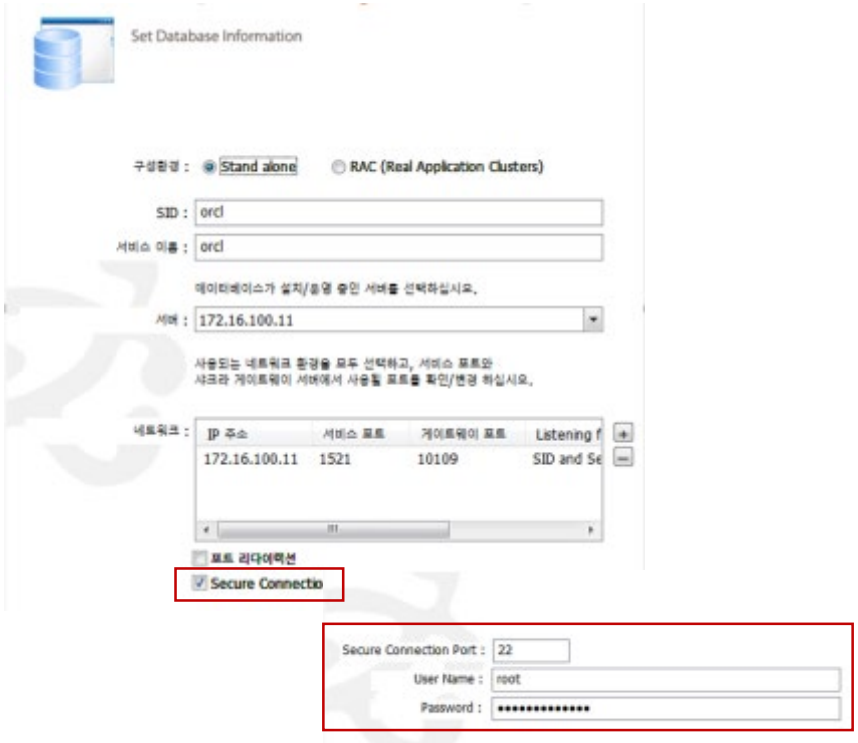
샤크라가 수집하여 저장하는 감사로그내의 개인정보를 보호하기 위한 기능으로,
민감정보로 등록된 데이터를 자동 인식하여, 수집 저장하는 감사로그(SQL, 리턴로우)에
포함된 개인정보를 마스킹 처리



4. 관리기능 | 통신구간 암호화

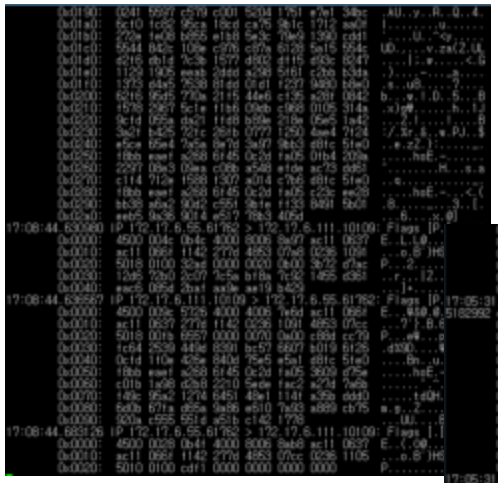
Chakra Max는 사용자와 데이터베이스 서버의 구간 DB 세션 암호화를 기능을 지원하여 통신 구간의 보안성을 강화

사용자 <–> Chakra Max <–> DB 서버 : 모든 구간의 암호화 통신

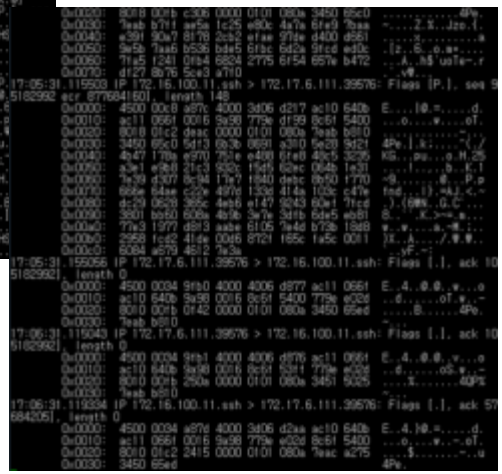


구간 암호화 옵션 활성화, DB서버 ssh 계정/비밀번호 입력

사용자 – Chakra Max 구간 암호화

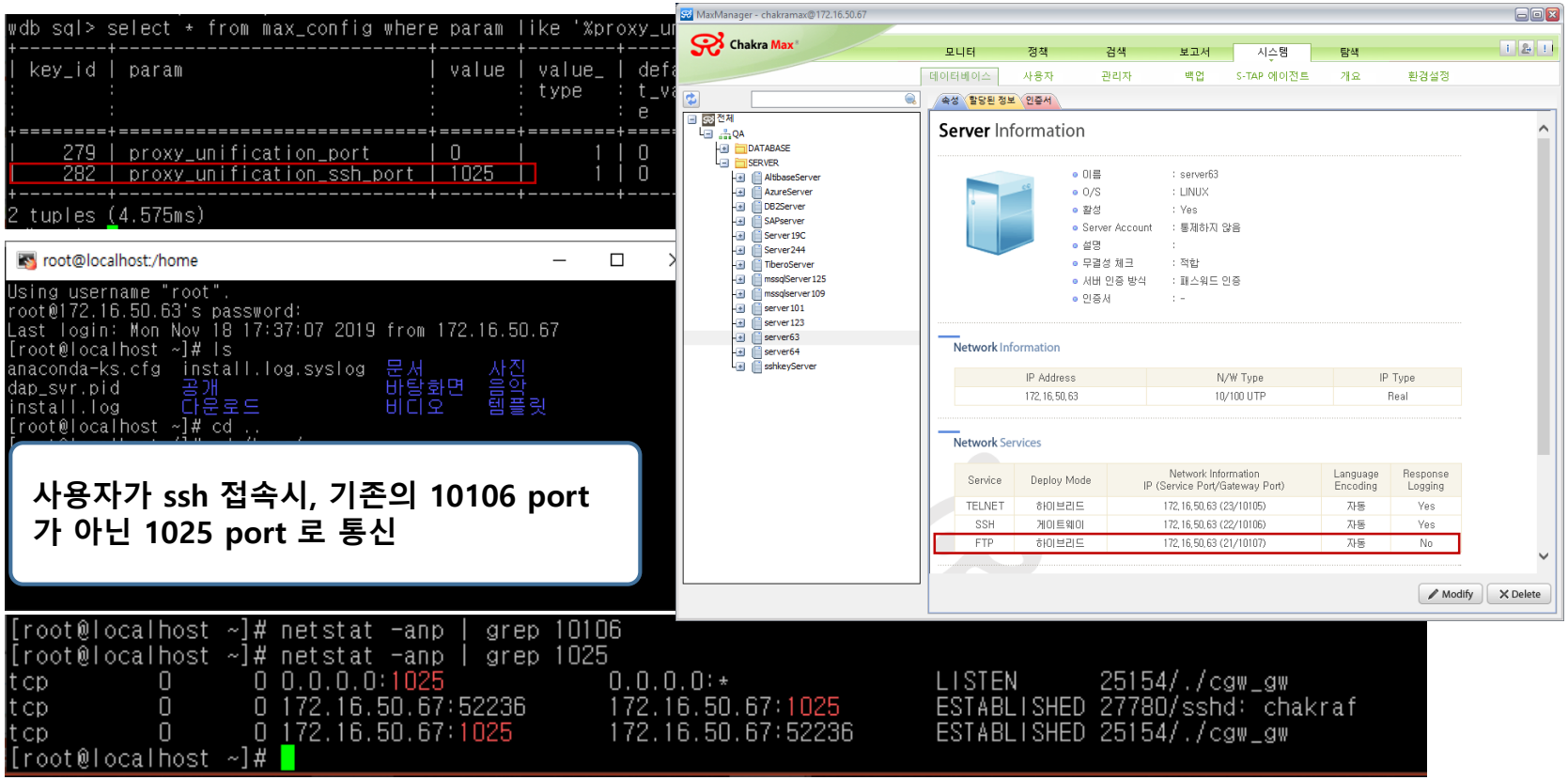


Chakra Max - DB 서버 구간 암호화



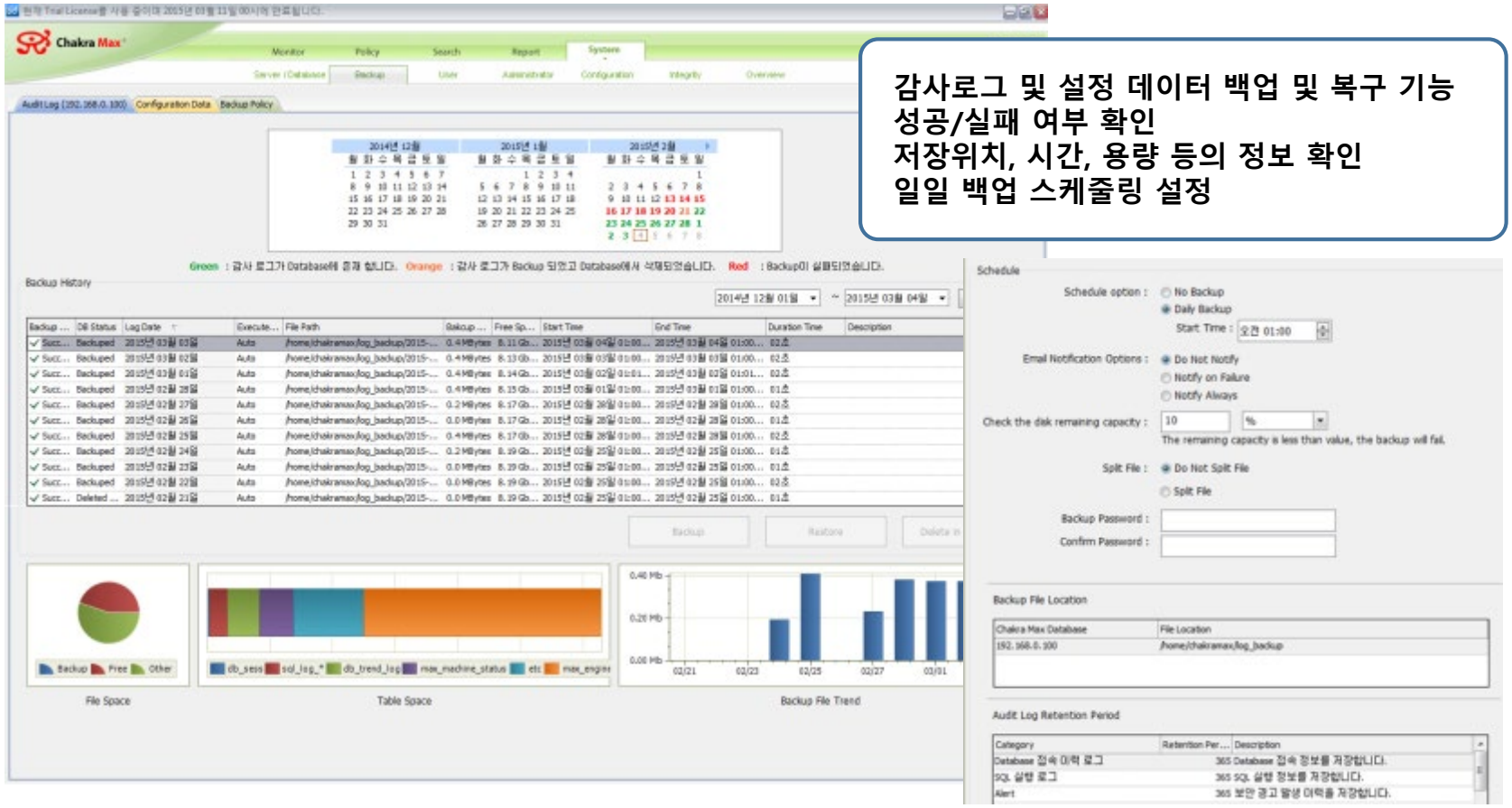
4. 관리기능 | 통신보안 강화를 위한 GW Port 단일화

시스템 운영측면의 보안 강화기능으로 DB접근제어 시스템의 gw 운영시 서버나 데이터베이스 별로 포트를 open 오픈하여 운영하던 방식을 변경하여, 하나의 port 로 통신할 수 있도록 지원



4. 관리기능 | 감사로그 백업

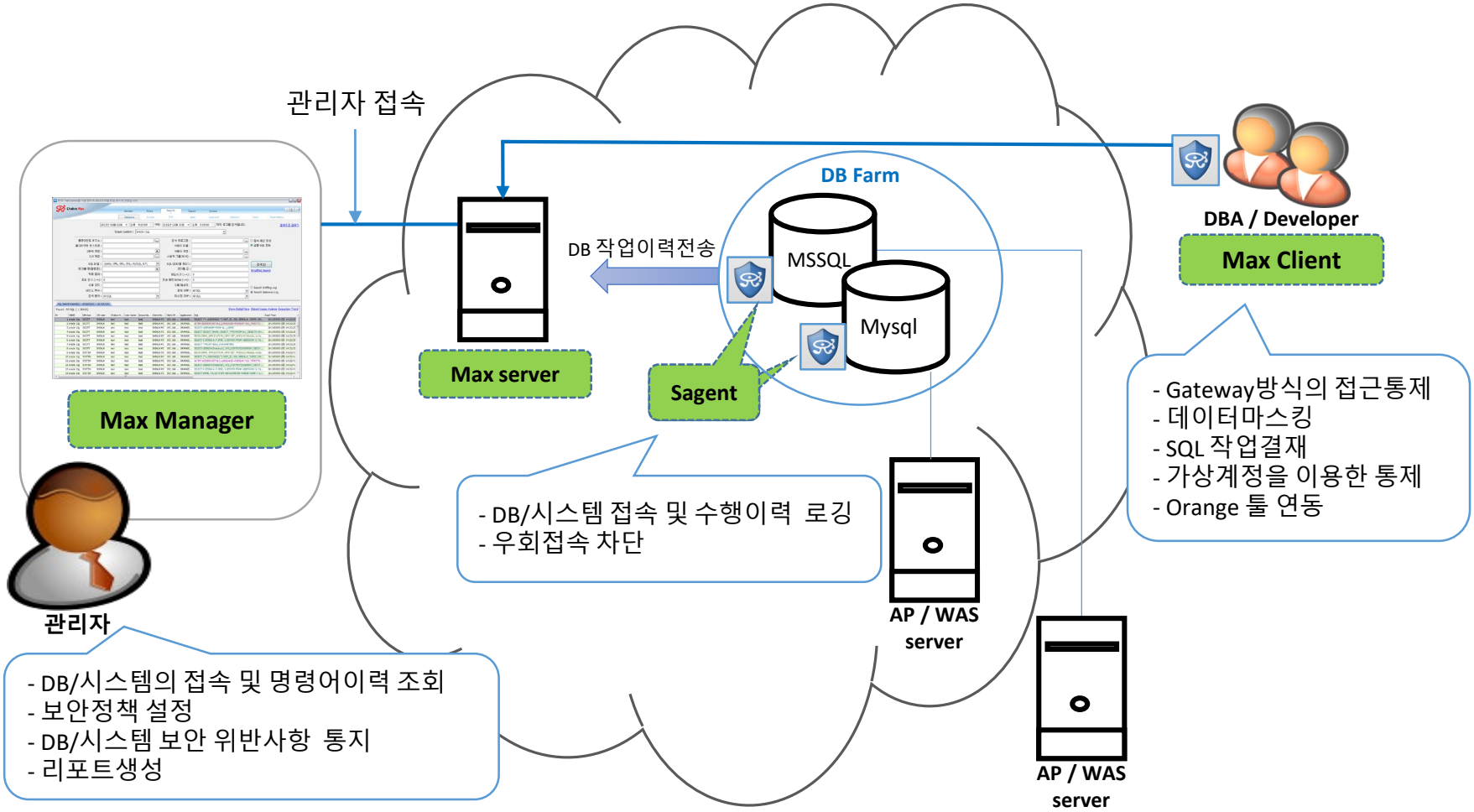
일일 로그데이터의 자동 백업 및 복구 복구 기능 제공



감사로그 및 설정 데이터 백업 및 복구 기능
성공/실패 여부 확인
저장위치, 시간, 용량 등의 정보 확인
일일 백업 스케줄링 설정

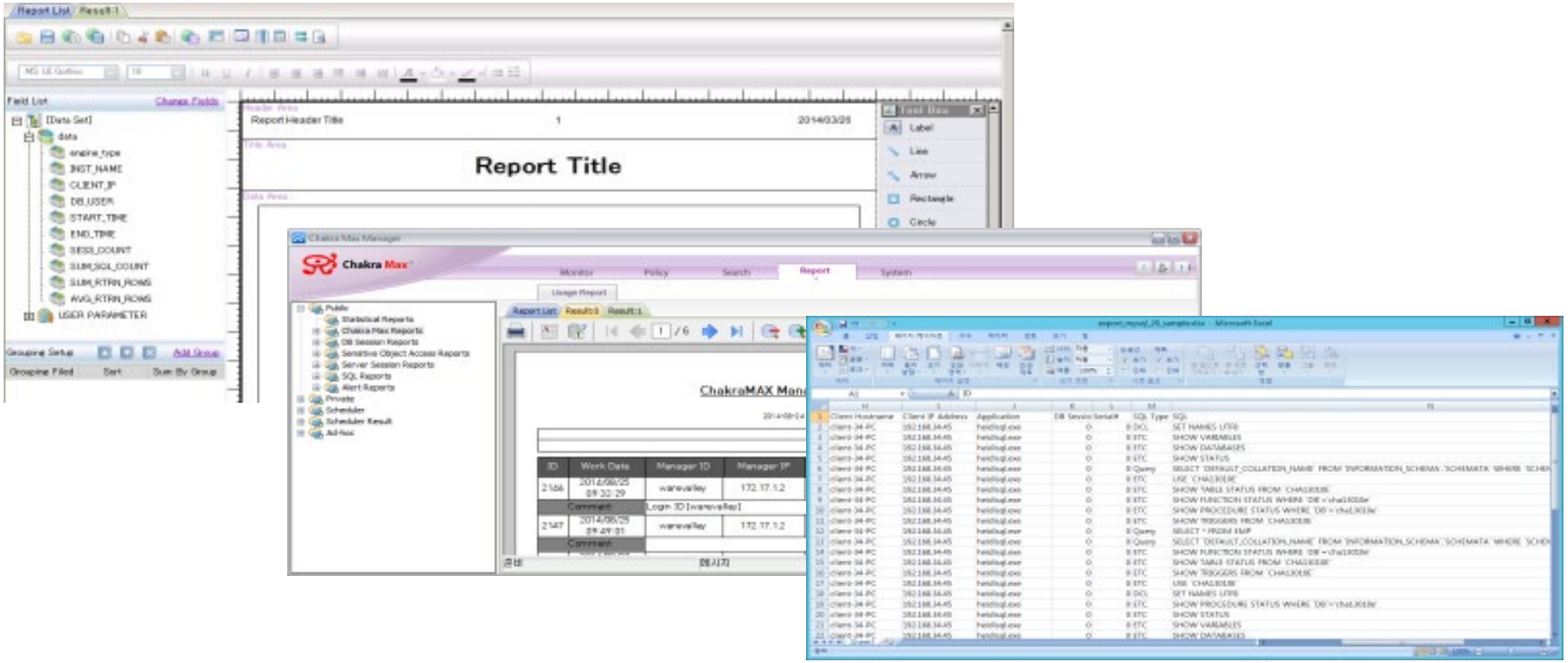
4. 관리기능 | Cloud 환경 지원

AWS, IBM, KT U cloud 등, 다양한 Cloud 환경에서 Gateway 및 Sniffing 모드 제공

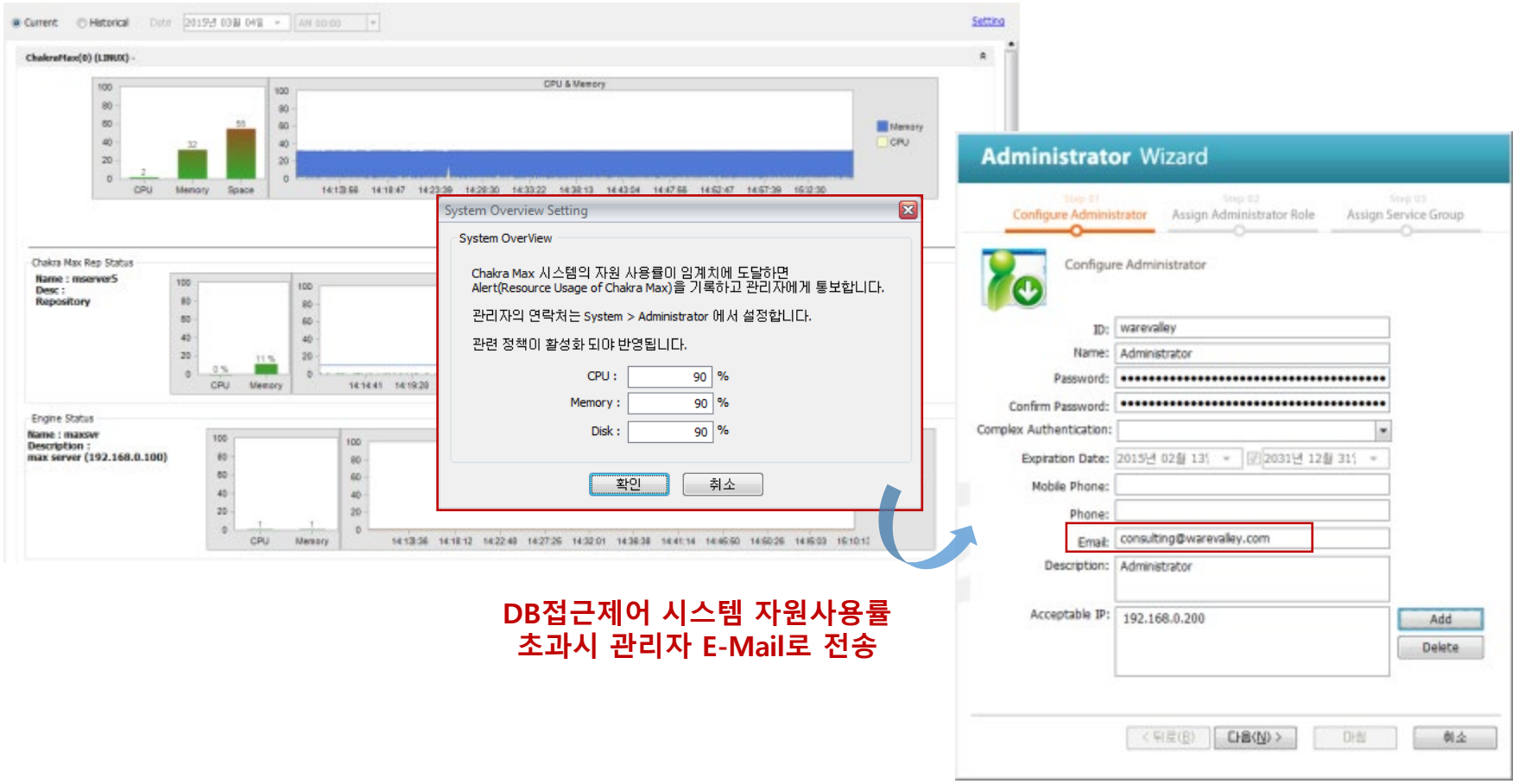


신규 보고서 엔진(Oz Report)을 탑재하여 더욱 편리한 보고서 기능

스케줄러를 이용한 보고서 **"자동 생성과 메일 전송"**
Excel, PDF, DOC, HWP 등 다양한 문서 포맷 제공
Ad-hoc 보고서 디자이너를 제공하여 필요한 보고서 디자인이 가능
약 50여 종에 달하는 다양한 형식의 보고서 포맷 제공



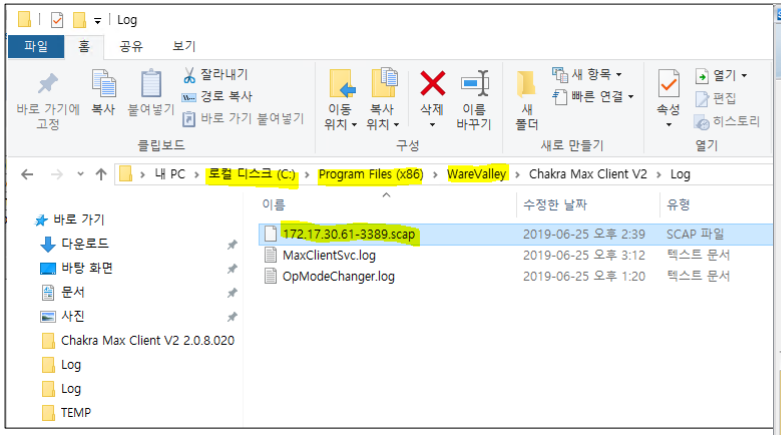
DB접근제어 시스템 성능 모니터링 및 임계치 초과 알림 기능

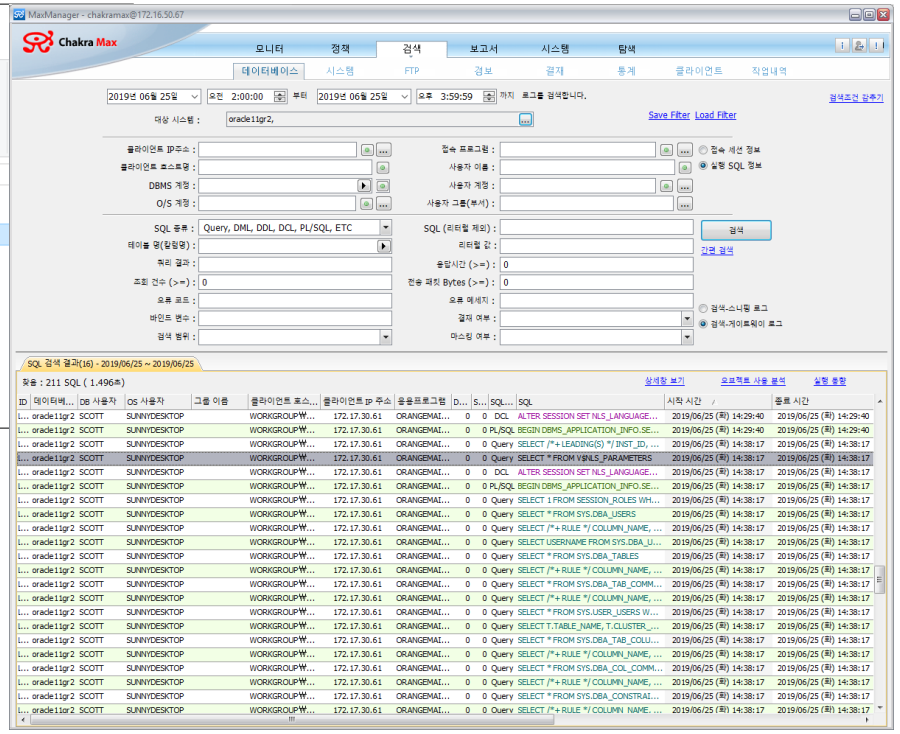


DB접근제어 시스템 자원사용률
초과시 관리자 E-Mail로 전송

4. 관리기능 | 장애 대처 기능 강화 – SQL 로그 유실 방지(fail logging)

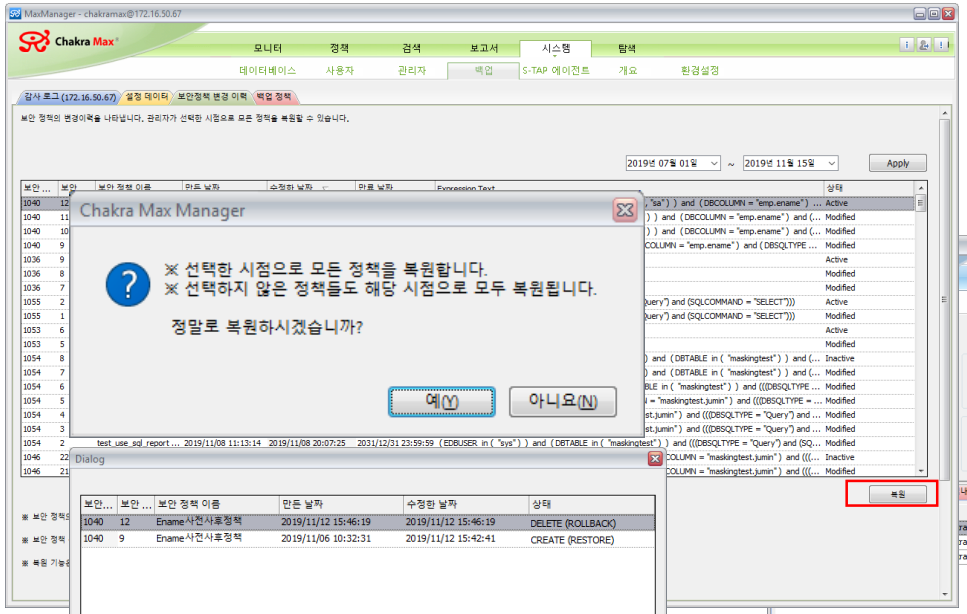
샤크라서버 시스템 장애시 사용자의 SQL 작업에 대한 감사로그 유실 방지를 위해, 사용자 SQL 작업 내용을 클라이언트 PC에 임시 저장 후 서비스 정상 복구된 후 샤크라서버로 전송하여 감사 로그를 저장

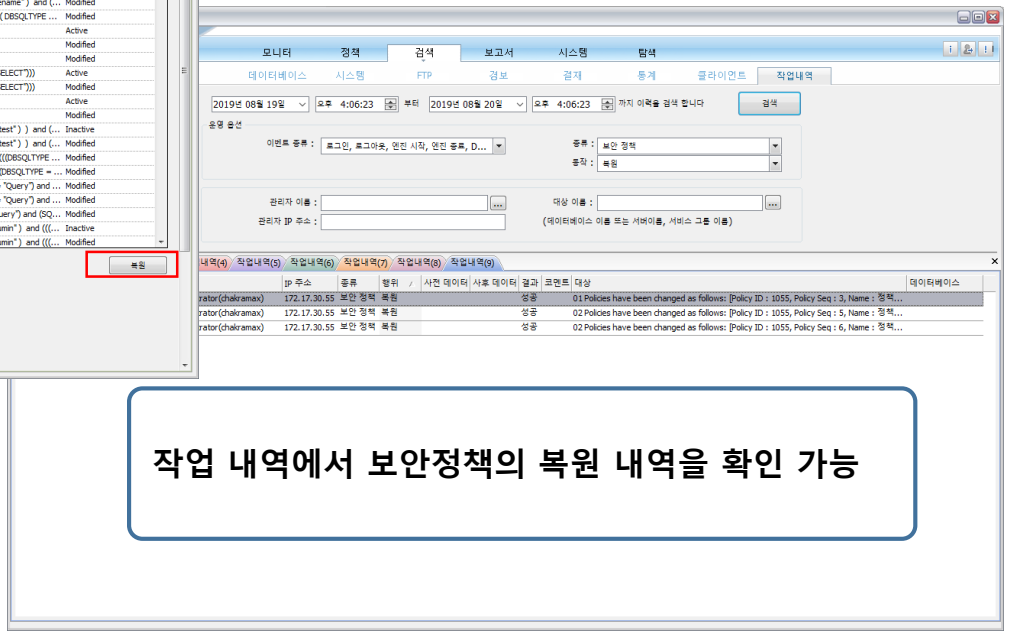




4. 관리기능 | 장애 대처 기능 강화 – 정책 복원 기능

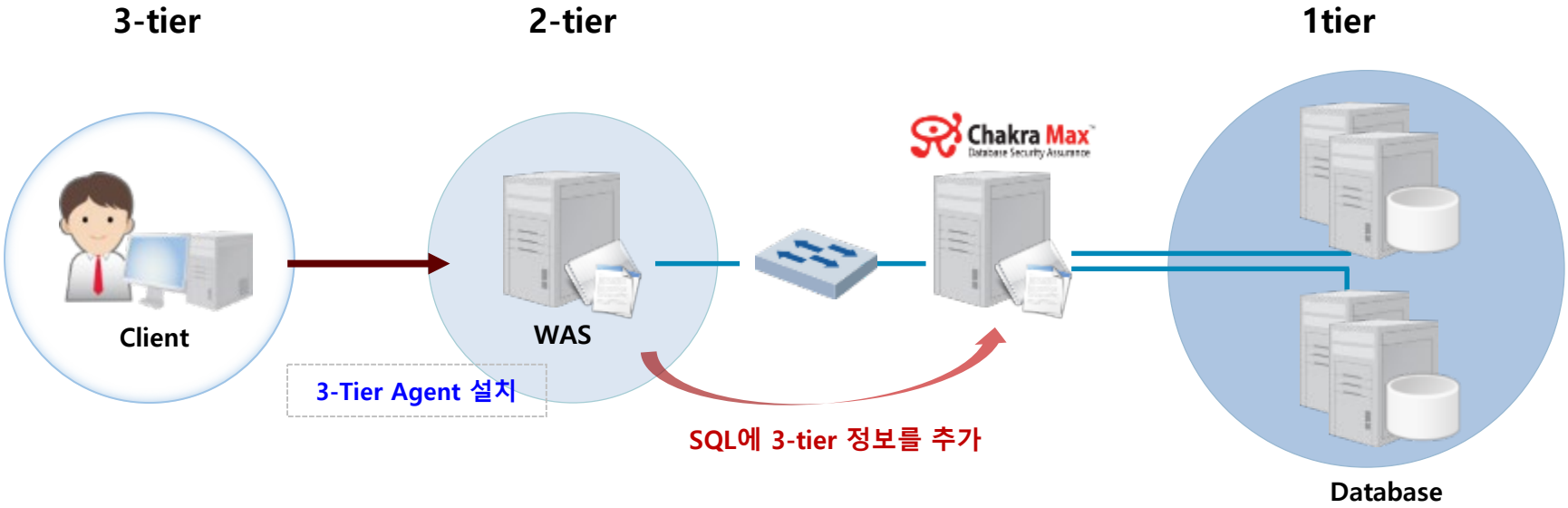
DB접근제어 시스템 운영중 장애 또는 정책 운영 변경으로 관리자가 등록한 보안 정책에 대해 특정 시점으로 roll back 하고자 할 때, 정책을 복원하는 기능
복원 결과는 검색의 작업내역에서 보안정책의 복원 동작 조건으로 검색 후 확인





작업 내역에서 보안정책의 복원 내역을 확인 가능

WAS, APP Server를 경유하여 데이터베이스에 접속한 사용자 **(3 Tier)의 IP / ID 추적**



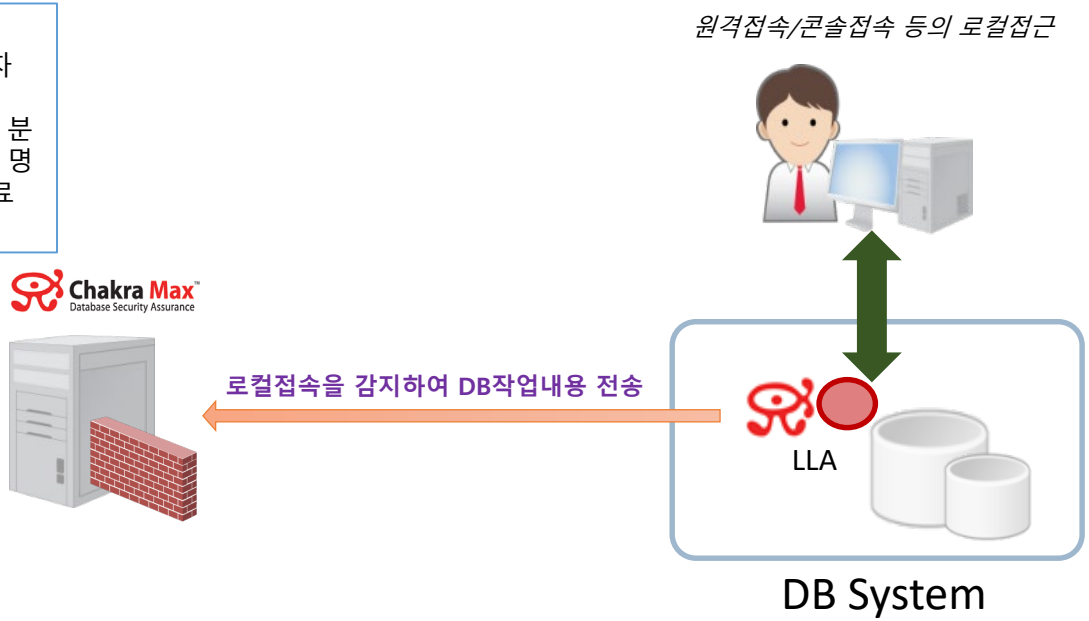
1. WAS를 경유한 End User를 추적하기 위해 "3-Tier Tracking Agent" 설치
2. 기존 WAS Application의 수정 불필요 (Standard Java Platform 운영 시)
3. Tomcat, Web Sphere, Web Logic, JEUS 등 WAS를 경유한 End User 추적

- **Agent 설치는 DBMS, OS, JAVA 환경에 따라 지원하지 않을 수 있으며 추가 비용이 발생할 수 있습니다**

LLA (Local Logging Agent)

서버내의 직접접속을 감시하기 위하여 설치되는 Agent 로, 원격 또는 콘솔 등을 통한 DB의 직접접속이 발생할 경우, 모든 작업내역을 저장
※DB Collect와 연계할 경우, DB 접속차단 정책적용 지원.

※DB collector 세션 차단
Chakra Max의 Dbcollector 가 세션을 차단 할 수 있는 관리자 권한(sys 등)으로, 항시 DB에 접속 해 있으면서 엔진 에서 분석된 차단 대상이 발견 될 경우DB 내부 명령어를 이용하여 DB 내에서 접속을 종료하도록 함



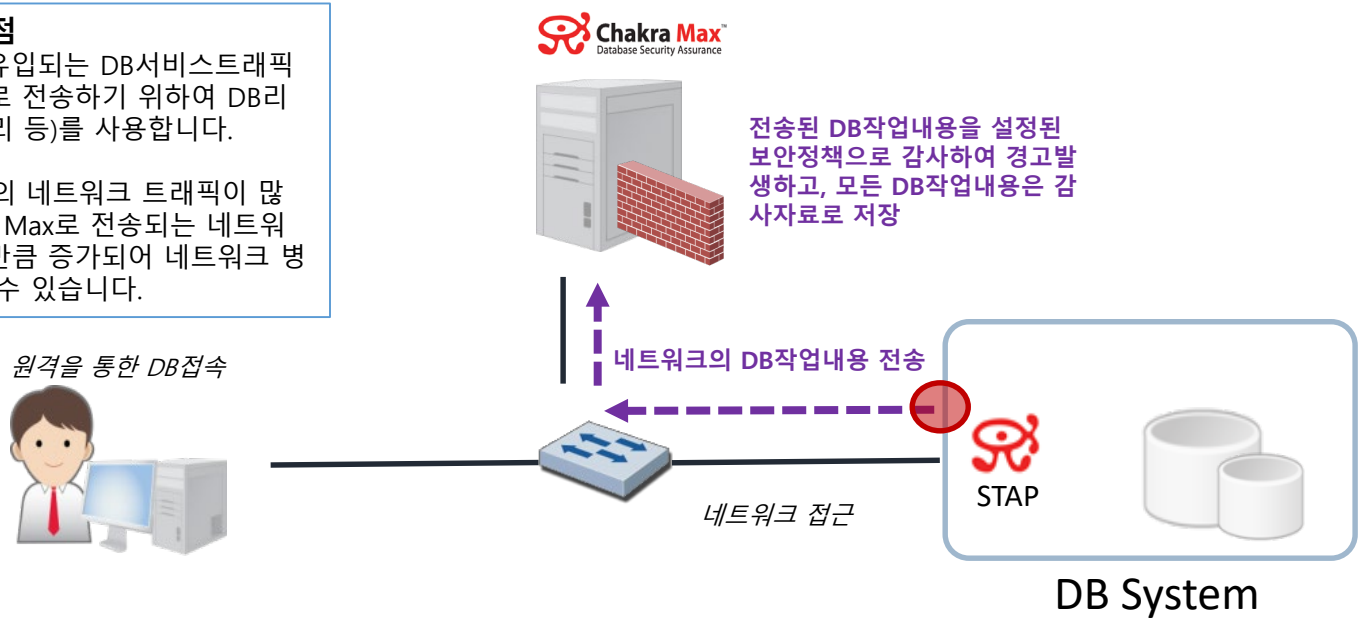
- **Agent 설치는 DBMS, OS, JAVA 환경에 따라 지원하지 않을 수 있으며 추가 비용이 발생할 수 있습니다**

STAP (Software Tap) - 로깅

DB작업내용 감사를 위하여 스위치의 Port Mirror 혹은 TAP장비를 사용하는데, 고객사의 상황으로 이와 같은 구성이 불가능할 경우 DB서버에 설치되는 Agent로, DB 서버의 네트워크인터페이스로 유입되는 DB서비스 트래픽을 Chakra Max 서버로 전송하여, DB작업내용을 저장

STAP 의 유의점
DB시스템으로 유입되는 DB서비스트래픽을 Chakra Max로 전송하기 위하여 DB리소스(CPU, 메모리 등)를 사용합니다.

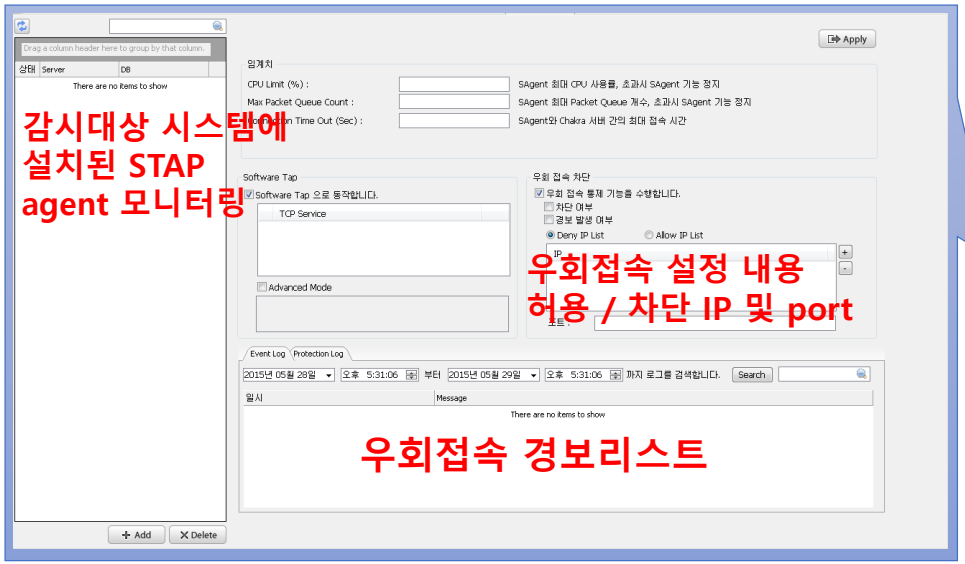
또한, DB서비스의 네트워크 트래픽이 많을 경우, Charka Max로 전송되는 네트워크 트래픽도 그만큼 증가되어 네트워크 병목의 원인이 될 수 있습니다.



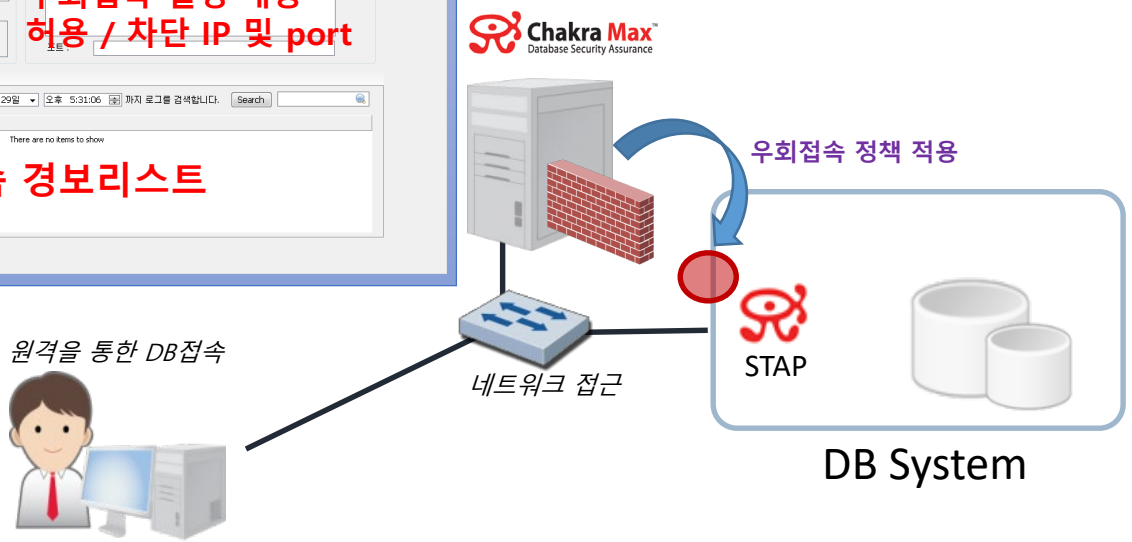
- **Agent 설치는 DBMS, OS, JAVA 환경에 따라 지원하지 않을 수 있으며 추가 비용이 발생할 수 있습니다**

STAP (Software Tap) - 우회접속차단

허용되지 않은 유저/시스템 으로부터 제한된 서비스포트로의 우회접속에 대하여 경보/차단 기능.



STAP 우회접속차단
DB 시스템에 설치된 STAP Agent로 접속하는 source IP및 서비스 port 를 제어하는 방식 Chakra Max에서 모든 STAP Agent 의 우회접속 허용/차단 정책을 일괄관리



5. 옵션기능 | Agentless Gateway

Chakra Max를 proxy 게이트웨이로 사용하여 DB에 접근하는 경우, Chakra Max Client Agent 의 설치 / 미설치 선택이 가능

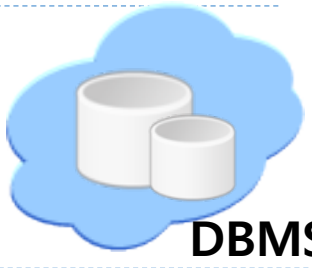
Chakra Max PC agent를 인스톨한 사용자는, 관리자가 설정한 ID/PASS 를 입력하고 Charka Max 서버에 로그인 한 후 관리대상 DB로 접속할 수 있습니다.

Agent ○

해당 유저의 DB접속 네트워크를 제어하도록 설정

가능한 기능:
쿼리에 대한 사전차단/마스킹 기능/실시간 얼럿UI /결재기능

비고: Windows 계열만 설치가능



Agent ×

Chakra Max PC agent를 인스톨하지 않은 사용자는 PC의 IP를 Chakra Max서버에 등록하여, 관리대상 DB로 접속할 수 있습니다.
이 경우, DB접근정보의 변경이 필요합니다.

해당 유저의 DB접속 네트워크를 제어하지 않도록 설정
또한, 클라이언트의 고정 IP주소를 입력하여 해당 IP를 Chakra Max 유저를 식별

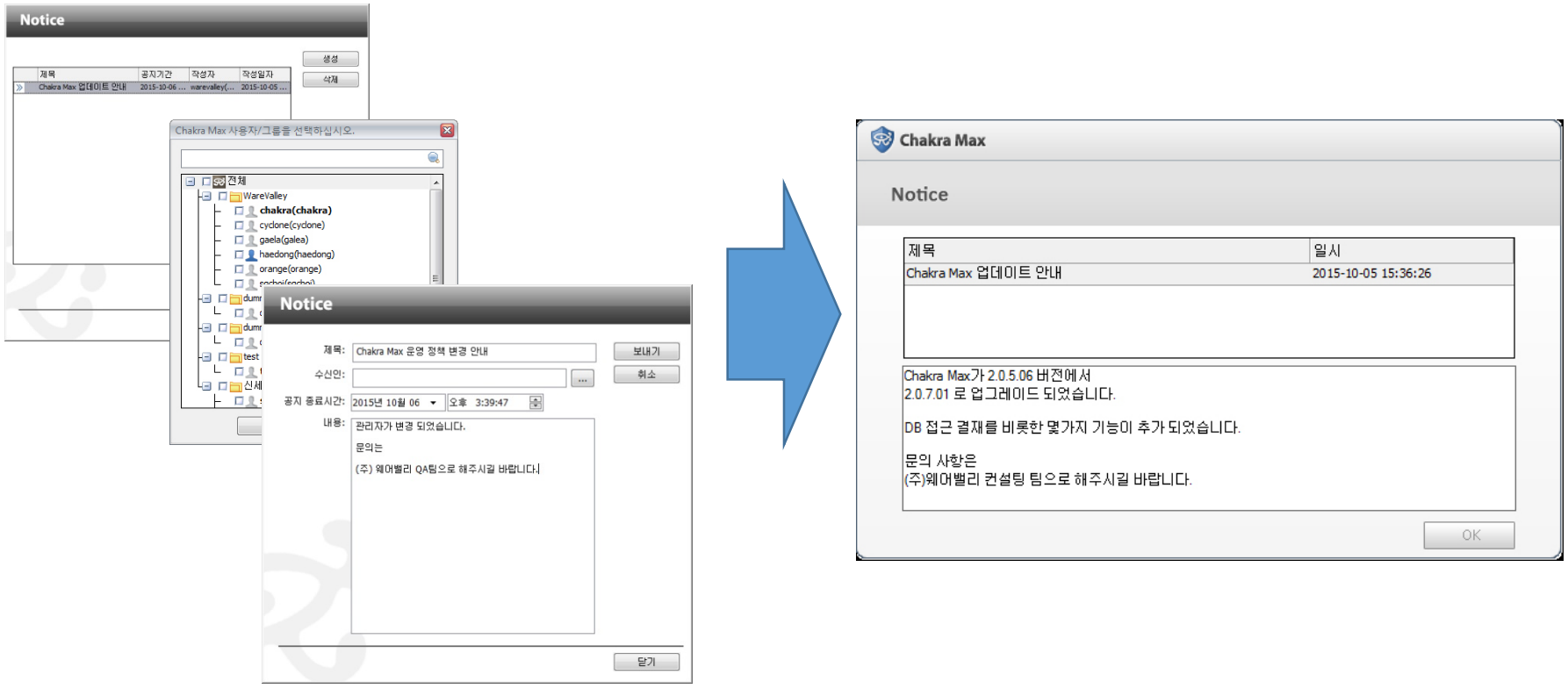
가능한 기능:
쿼리에 대한 사전차단 / 마스킹 기능

비고 : OS 무관

Appendix
Chakra MAX – Client 활용

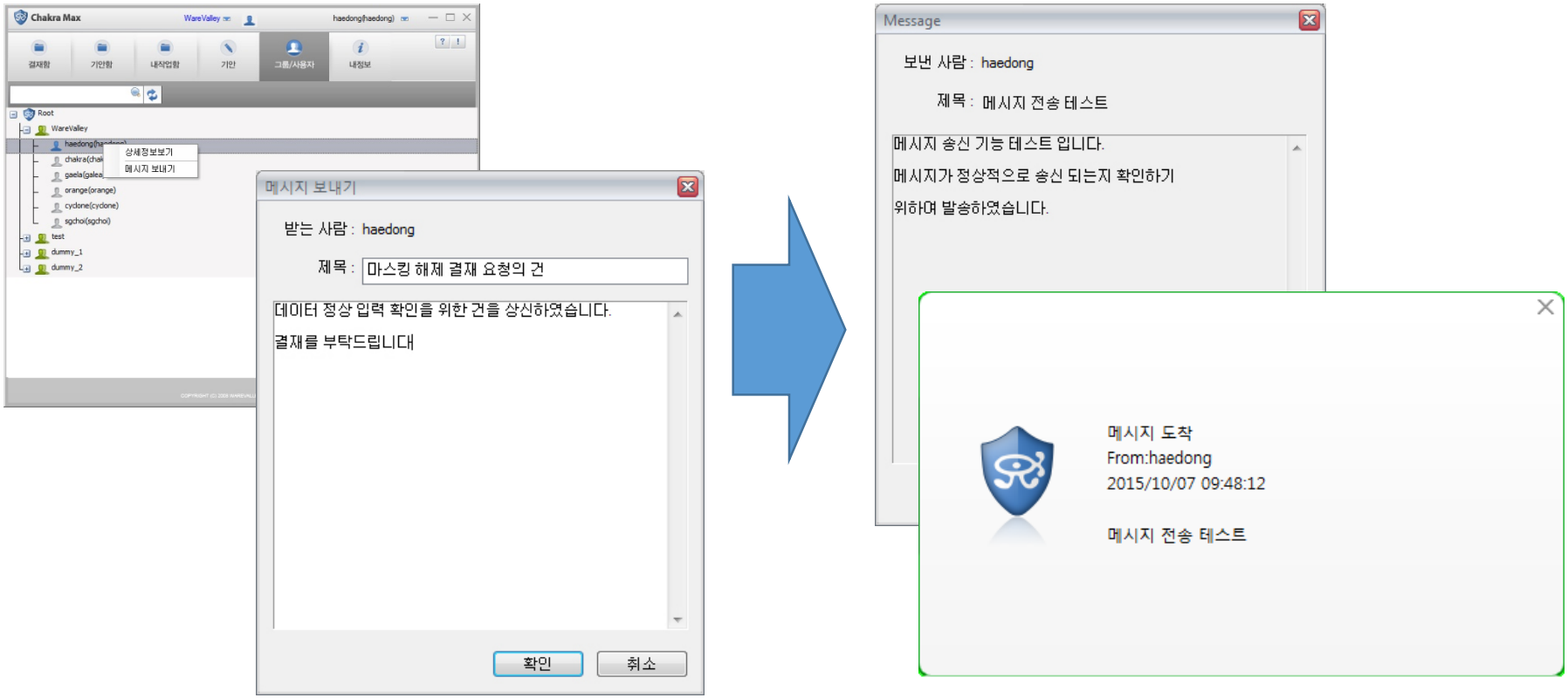
공지기능을 통한 클라이언트에 대한 알림 메시지 전송

Chakra Max 매니저를 통한 관리자의 공지 메시지 작성
공지 메시지를 수신 받을 사용자의 선별적 메시지 송신



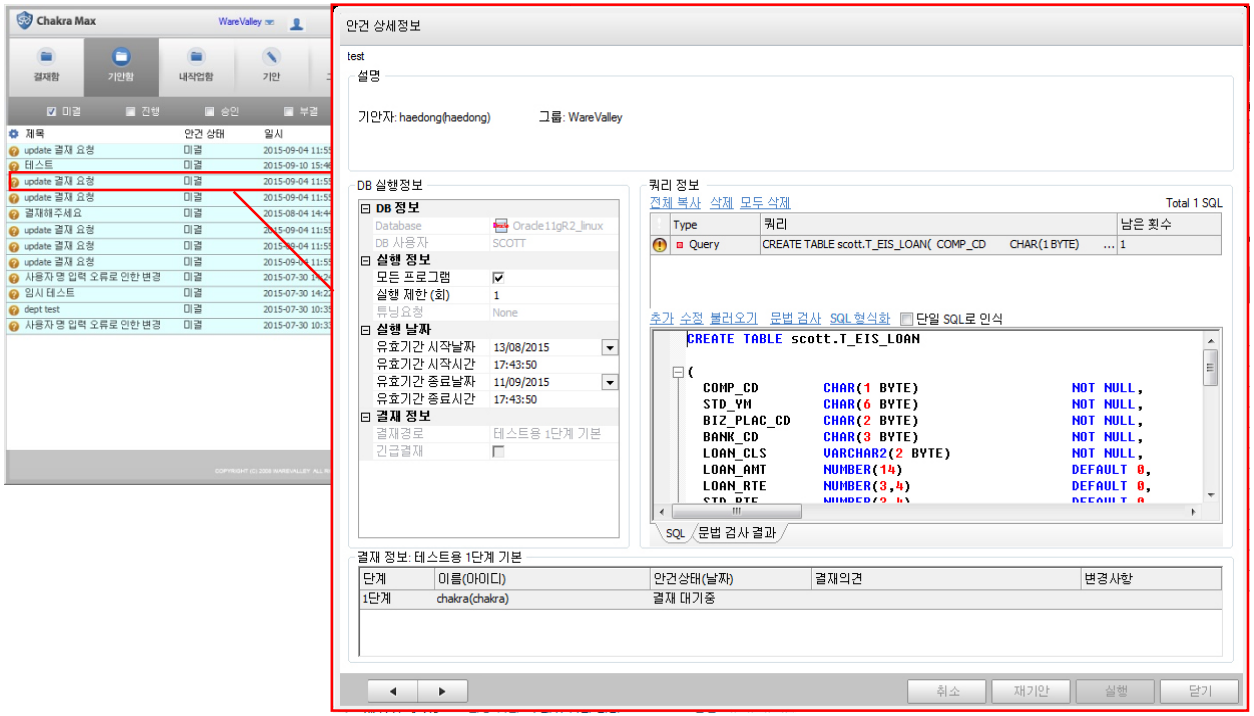
쪽지 보내기 기능을 통한 사용자 간의 메시지 전송

Chakra Max 클라이언트 사용자 간 메시지 전송
결재 / 기안 관련 건에 대한 긴급 처리 요청등의 메시지 송신



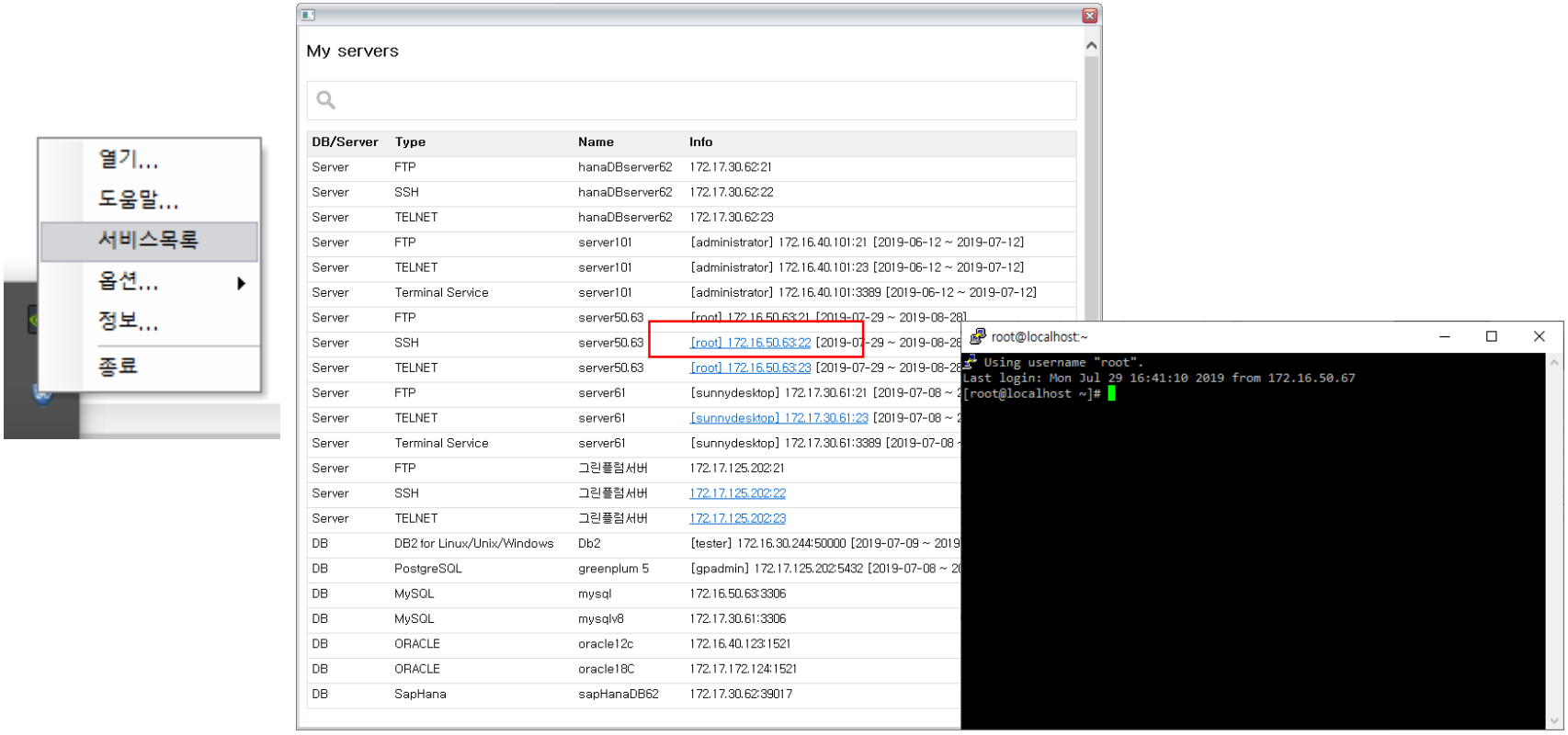
기안함의 기안문 저장 기능을 통한 과거 기안 내역 확인

자신이 작성한 기안문에 대한 기안함 제공을 통한 기안문의 상세 내역 및 결재/부결 여부 확인



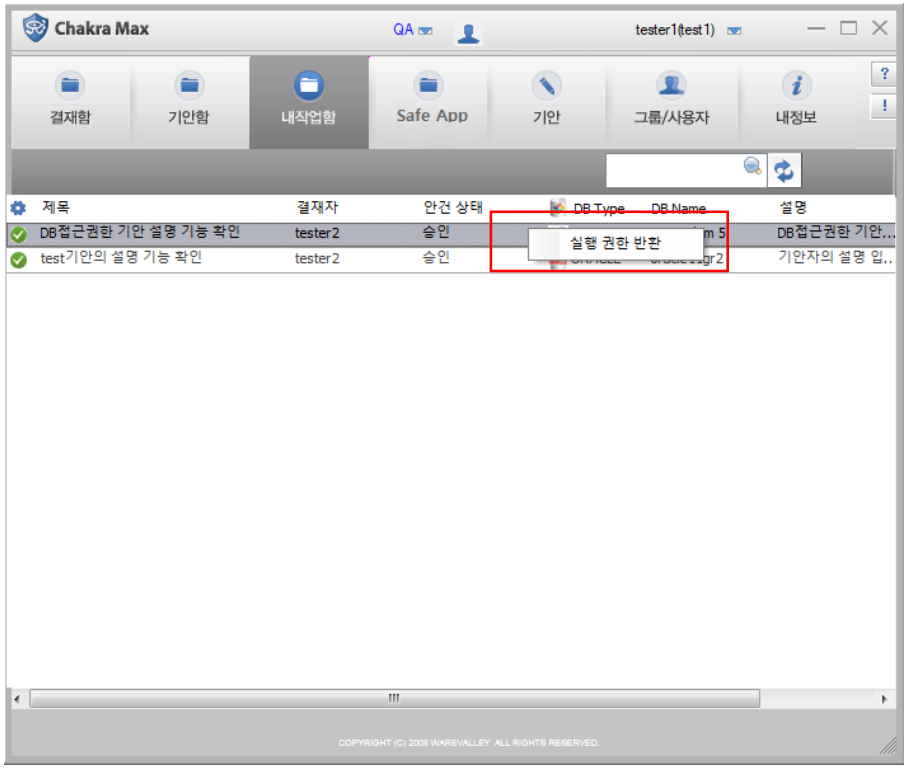
사용자가 접속 가능한 서버/데이터베이스 목록을 표시

사용자가 접속 가능한 서버/데이터베이스 목록을 표시하며, 할당된 서버 계정을 클릭하면 연결 프로그램으로 자동 접속 기능



결재받은 안건에 대한 실행권한 반환 기능

기안 후 결재 승인 받은 안건에 대해 잔여 실행 회수가 남은 안건에 대해 더 이상 진행이 필요 없는 안건에 대해 내 작업함에서 실행권한 반환 할 수 있는 기능



사용자 편의를 위한 다양한 클라이언트 프로그램 옵션 제공

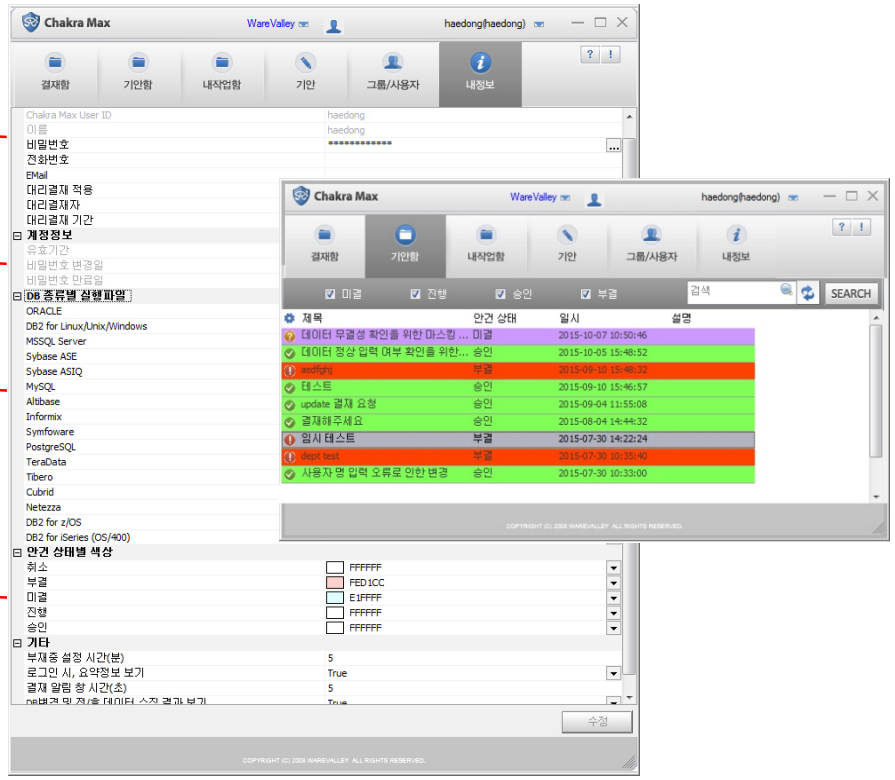
기안/결재함 진행 단계에 대한 컬러 표시
사용자 주 사용 DB관리 프로그램 선택

사용자 패스워드
/ 연락처 / E-mail 등의 개인정보 수정

계정 유효기간 / 패스워드 변경일
/ 만료일 등의 정보

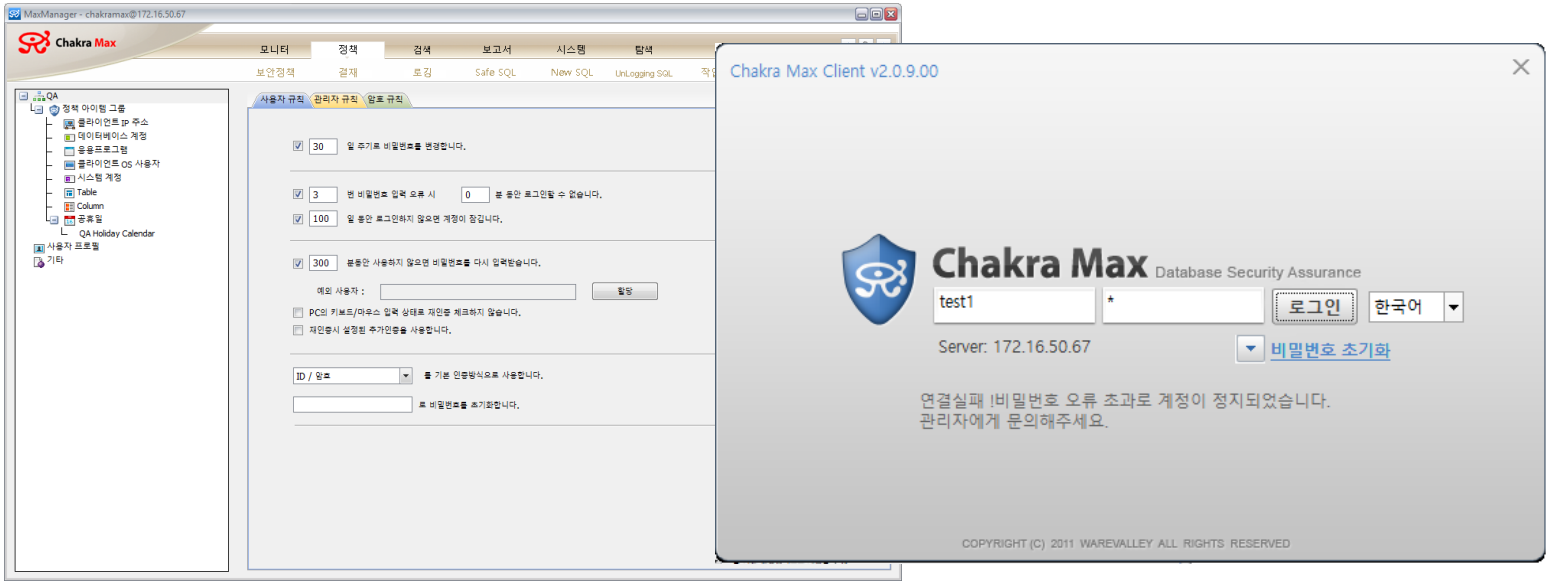
사용자의 주 사용 DB 관리 툴 지정

결재/기안함의 결재문 상태 표시 컬러



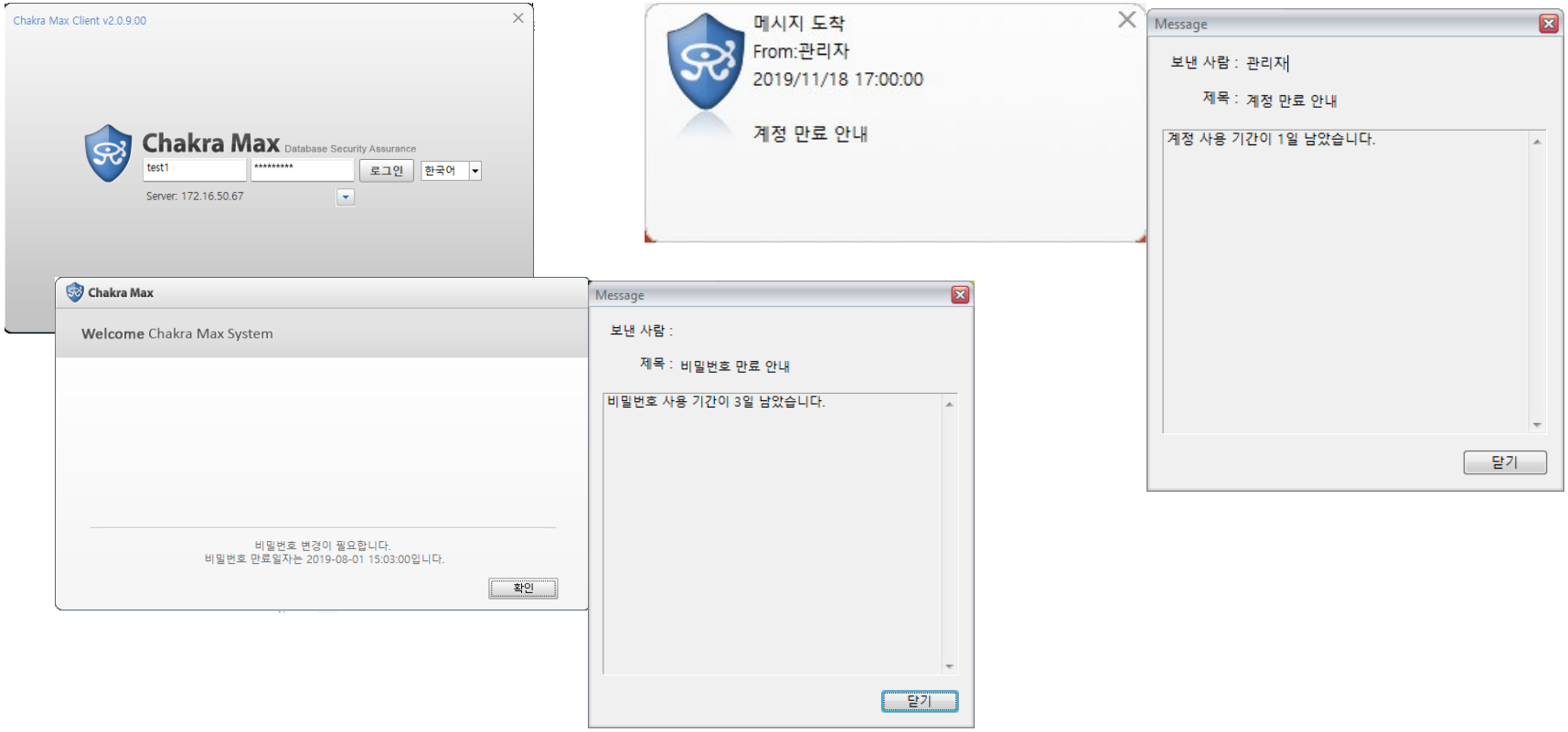
사용자 잠금 기능

사용자 로그인시 비밀번호 입력 오류 회수 초과시 설정에 따라 일정시간 로그인을 제한하는 기능에 사용자 계정을 잠금 처리하는 기능을 추가
해당 기능은 관리자가 잠금해제 처리전까지 해당 계정 사용이 불가하도록 보안 기능을 강화함.



사용자 계정만료 사전 알림 기능

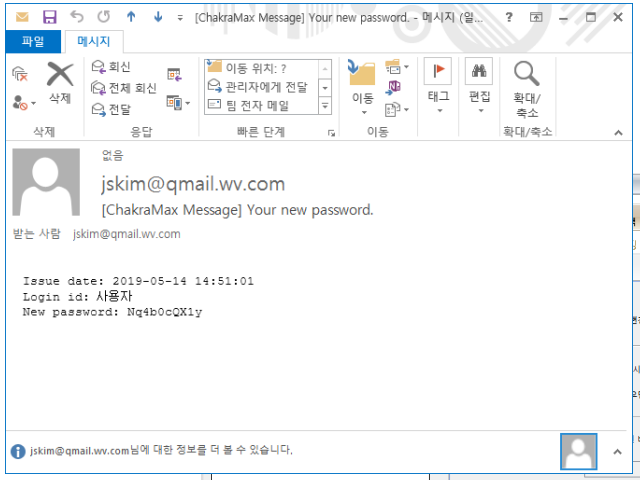
사용자 계정 및 비밀번호 만료기간이 임박함에 따라, 사용자 로그인시에 계정만료 및 패스워드 만료 안내 메시지를 출력하는 기능으로, 만료 7일전부터 알림이 표시되며 보안관리자의 설정에 따라 특정 시간에 메시지로 전송 가능

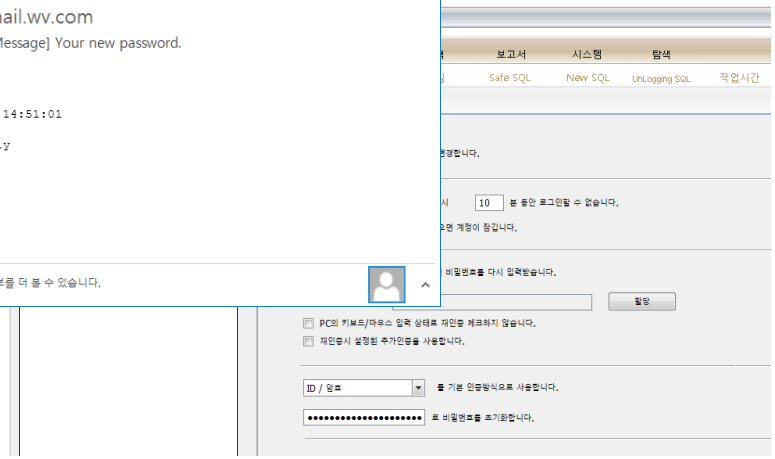


사용자 비밀번호 초기화

관리자 부재중에 사용자 계정이 잠기거나 장기 미사용 사용자에 대해 활성화가 필요한 상태에서 사용자의 비밀번호를 초기할 수 있는 기능 제공

- 샤크라가 생성한 임시 패스워드를 SMS, Email 로 전송하여 초기화 할 수 있도록 기능 제공
- 사용자가 비밀번호 초기화 요청시 관리자가 설정한 초기 패스워드를 사용자 임시 패스워드로 할당



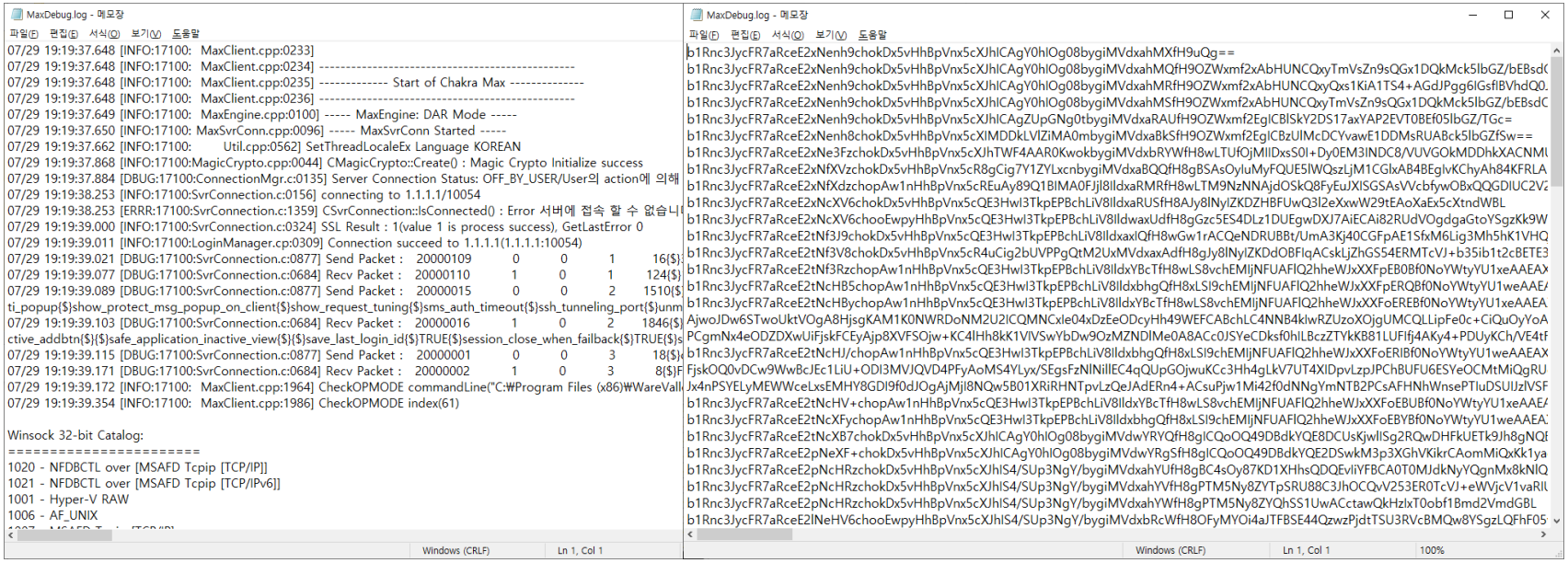


클라이언트 프로그램 생성 로그의 보안 기능 강화

클라이언트가 생성하는 MaxDebug.txt 로그 생성시 사용자의 IP 주소를 그대로 저장하지 않고, 1.1.1.1 로 마스킹 처리하여 저장

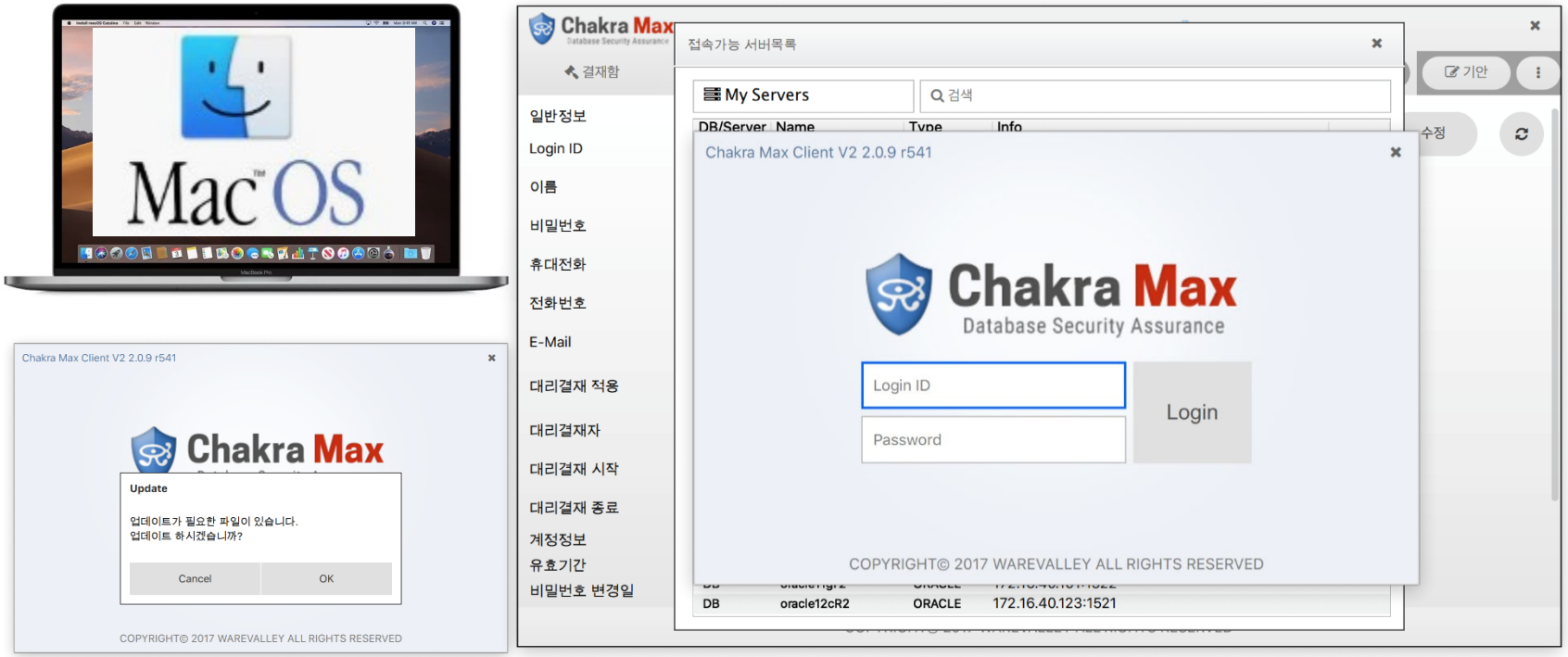
클라이언트가 생성하는 로그파일 암호화

클라이언트가 생성하는 MaxDebug.txt 로그 파일을 암호화하여 생성



클라이언트 프로그램의 MAC OS 호환성 지원

- Windows OS 와 동일한 보안 기능 지원
- 자동 업데이트



6. 주요 고객사 | 주요 고객사

Contact us.

Seoul Office :
22F, Nuritkum Square Biz Tower, 1605
Sangam-dong, Mapo-gu,
Seoul, Korea 121-795
Tel + 82.2.2132.5590

Japan Office :
Shinkasumigaseki Bldg 18F., 3-3-2,
Kasumigaseki, Chiyoda-ku, Tokyo 100-0013
Tel +81.3.5532.8801

Online Contact :
Sales@warevalley.com
http://www.warevalley.com

WareValley
http://www.warevalley.com

Database Audit and Protection [DB-System 접근통제]
Database Encryption [DB 암호화]
Database Vulnerability Assessment [개인정보 모니터링 / DB 취약점 분석]
Database SQL Query Approval [DB 작업결재]
Database Performance Monitoring and Management [DB 성능관리 및 개발]
BI / DW / OLAP DBMS [빅데이터 분석, 데이터웨어하우스]