

Chakra Max V4.0

목차

I. DB 접근 통제

- 1.1 도입 기대 효과
- 1.2 제품구성
- 1.3 주요 기능
- 1.4 관리기능

II. 시스템 접근 통제

- 2.1 주요 기능
- 2.2 기본 구성 플로우
- 2.3 서버 보안
- 2.3 접근 행위 기록

III. 계정관리

- 3.1 도입 기대 효과
- 3.2 주요 기능
- 3.3 기능 소개

IV. 통합관리

- 4.1 통합 관리 솔루션
- 4.2 통합 구성 플로우

V. 레퍼런스

CHAKRAMAX FOR DAC
DB접근통제

01

01 도입 기대 효과



컴플라이언스 준수 및 내부회계감사 대응에 따른 고객정보의 안전성 및 보안성 강화

컴플라이언스 준수 및 내부회계감사 대응에 따른 고객정보의 안전성 및 보안성 강화

컴플라이언스 준수를 위한
안정적인 솔루션 구축



내부 정보 불법 유출 차단을 위한
검증된 솔루션 구축

개인정보보호법 강화 및 정보통신망법,
여신전문 금융업법 등 **컴플라이언스 준수**

- 16년 09월 개인정보보호법령 강화에 따른 이슈 발생
- 여신전문 금융업법 등 법적 기준 준수 필요
- ISMS 등 감사 관련 항목 보완 필요
- **컴플라이언스 미준수**

2016년 09월 강화된 개인정보 보호법
시행에 따른 추가 기능 필요

- 중요 작업 수행 시 책임자 승인
- 개인정보를 마스킹하여 표시 제한
- 2 Factor 인증을 통한 안전한 인증수단

강화된 개인
정보보호법 시행
(16. 09)

규제의 강화

DB접근제어
구축 필요

솔루션
구축으로
안전성 확보

DB접근제어 시스템의 구축을 통한
내부정보 유출 차단 및 고객정보 보안 강화

- DB보안사고 대응체계 마련
- 기업의 자산인 고객정보의 안전성 및 보안성 강화
- **내부정보의 불법 유출 차단 필요**

DB접근제어 시스템의 구축 필요성

- 내부정보 유출 차단 및 고객 정보 보안 강화
- **감독 기관의 컴플라이언스**

02 제품 구성 (1/2)

DB접근제어 서버

Chakra Max Server



보안 정책 관리 / 적용

DB & System 작업 감사 데이터 로깅

보안 시스템 운영 현황 모니터링

DB접근제어 관리자

Chakra Max Manager Program



접근제어 관리자

DB / System / 사용자/그룹 관리

보안 정책 설정(결재/차단/경보)

실시간 모니터/보고서 생성

DB사용자 Client

Chakra Max Client Program



DB 사용자

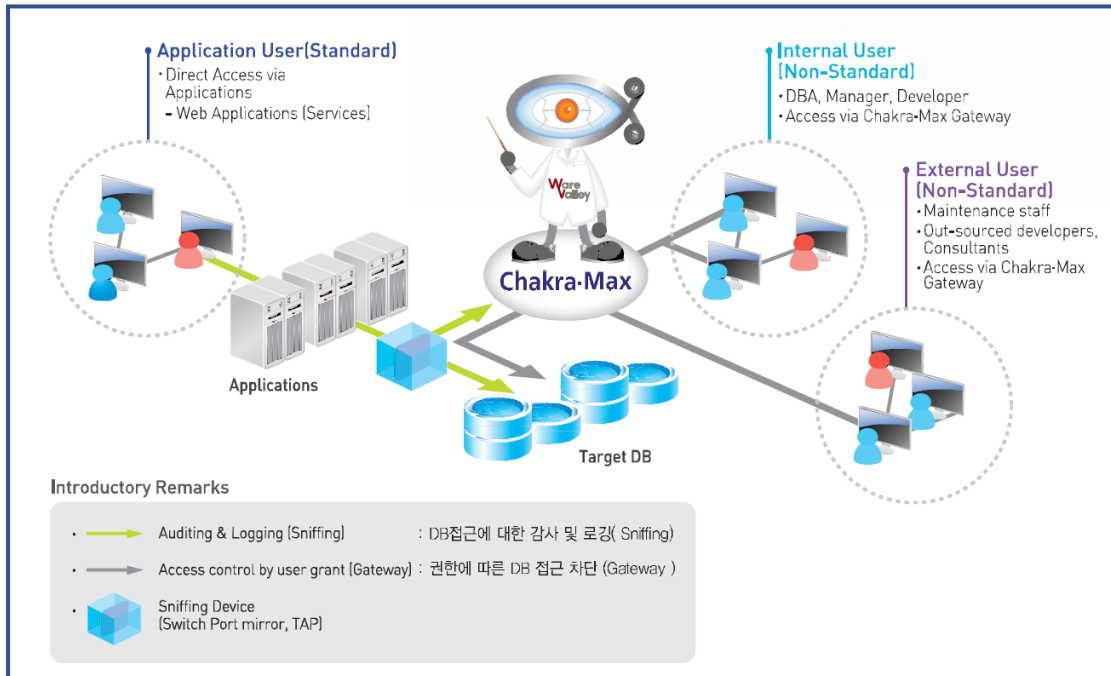
DB / System 직접 접속 통제

기안 / 승인 / 진행 상태 조회 및 관리

개인 정보 관리 / 파일저장통제

02 제품 구성 (2/2) | 구성도

고객사 환경 및 구성 방식에 따라 고객사 DB환경 변화 없이 맞춤형 구성 지원



• Gateway mode

사용자 별 DB 접근에 대한 권한관리 등 접근통제

- Max Client를 통해 Chakra Max 서버를 경유하여 DB 접속
- 결재, 마스킹 등의 보안정책 적용 및 차단
- 불법적인 개인정보 조회, 유출방지
- 사용자 정의 보안정책에 따라 경보 및 차단 기능

• Sniffing mode

중요 DB 접근에 대한 실시간 모니터링 및 사후감사

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

• Hybrid

Gateway, Sniffing 구성의 혼합형태

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

03 주요 기능 (1/9) | 작업이력 감사



DB 및 시스템에 접근하는 모든 사용자를 식별하고 작업시간, 접근이력, 수행 SQL 등을 기록 조건 별로 상세 검색할 수 있으며, Excel / CSV 형태의 결과값 추출 지원

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

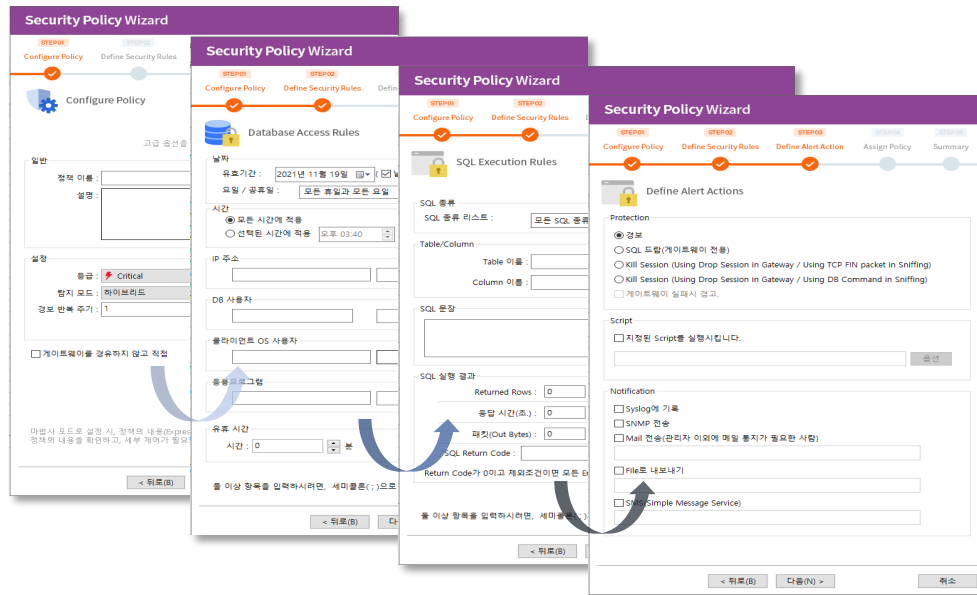
실행 명령어 / 접속 시각 / 종료 시각 / 대상 시스템 계정 / 클라이언트 IP 정보 확인

ID	데이...	DB 사용...	클라이언...	클라이언...	OS 사용자	응용프로...	사용...	사용...	그룹 이름	시작 시간	종료 시간	SQL ...	SQL	Retur...	응답 ...	서버...	Error ...	Error ...
1	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT /*+ LEADING(S) */ INS...	0	0.010	0.010	942	ORA-...
2	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT USERENV('instance'), S...	1	0.013	0.013	0	
3	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT S.SERIAL#, P.SPID, S.S...	1	0.005	0.005	0	
4	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT NAME, VALUE FROM ...	1	0.003	0.003	0	
5	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT SYS_CONTEXT('USERE...	1	0.012	0.012	0	
6	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT * FROM V\$NLS_PARA...	19	0.055	0.006	0	
7	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	DCL	ALTER SESSION SET NLS_LAN...	0	0.011	0.011	0	
8	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT * FROM DUAL	1	0.012	0.012	0	
9	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT * FROM DUAL	1	0.020	0.020	942	ORA-...
10	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT * FROM DUAL	1	0.011	0.005	0	
11	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT * FROM DUAL	1	0.032	0.022	0	
12	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT * FROM DUAL	1	0.023	0.012	0	
13	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT * FROM DUAL	1	0.020	0.011	0	
14	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT * FROM DUAL	1	0.024	0.013	0	
15	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT * FROM DUAL	1	0.010	0.005	0	
16	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT * FROM DUAL	1	0.010	0.005	0	
17	Orac...	SYS	DESKTOP...	192.168.1...	TOS	ORANGE...	test1	test1	TG	2021/11/19 (금) 2...	2021/11/19 (금) 2...	Query	SELECT * FROM DUAL	1	0.047	0.032	0	

조회 결과를 Excel/CSV로 export

03 주요 기능 (2/9) | 보안정책 구성

DB 및 시스템의 접근 및 작업 통제를 위하여
위저드(Wizard) 방식의 손쉬운 보안정책 구성 지원



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 마스킹 정책을 정의합니다.

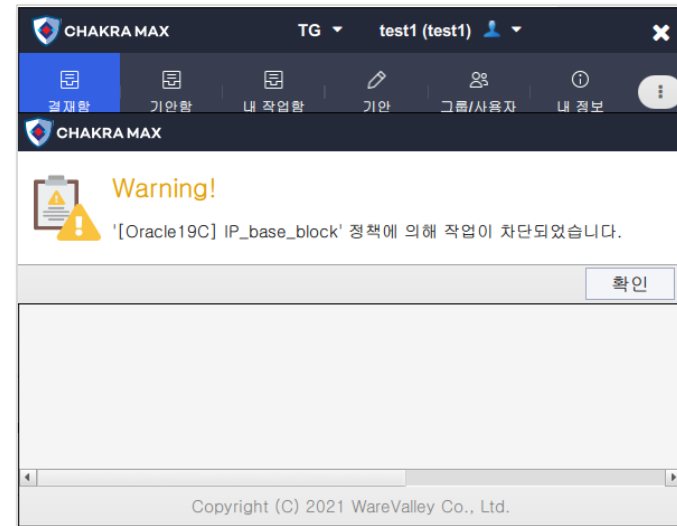
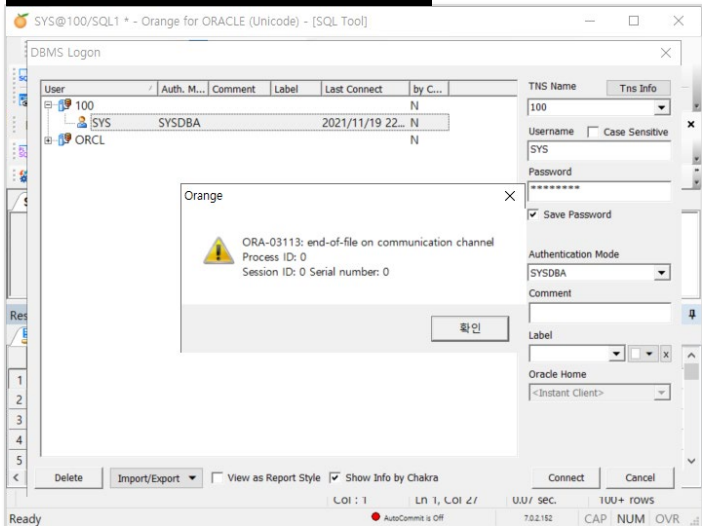
03 주요 기능 (3/9) | 보안정책에 따른 접근통제

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

다양한 조합으로 DB 및 시스템 접근 제어

- ✓ 사용자 식별 유저 정보: IP주소, DB 계정, OS 로그인 유저, 접속 어플리케이션, 접속시간 등
- ✓ 작업 내용: Table, Column, SQL Type(DDL/DML/DCL), Command 등
- ✓ 기타: 프로토콜, 시간대, 네트워크 사용량, Return Row 등

IP 통제에 의한 차단 예시화면



03 주요 기능 (4/9) | 경보 모니터

보안정책에 위배된 DB 및 시스템 접근이나 SQL, System 명령어 작업에 대해 실시간으로 관리자와 사용자에게 정책 위반 내용 및 경보 메시지 전달

The screenshot displays the Chakra Max Manager interface. The main window is titled "Session Monitor" and shows "Server / DataBase Session Monitoring". A table lists active sessions with columns for ID, user, host, session ID, user name, OS, status, and duration. A red lightning bolt icon in the first row indicates a warning.

ID	유저	호스트	세션 ID	유저명	OS	상태	시작 시간
1	Ds	DDB	621 31594	SYS test1...	TOS	192... 00:0...	DESKT... DESKT... ORANG... 5
2	Ds	DDB	745 46486	SYS test1...	TOS	192... 00:0...	DESKT... DESKT... ORANG... 2
3	Ds	DDB	868 42063	SYS test1...	TOS	192... 00:0...	DESKT... DESKT... ORANG... 0
4	Ds	DDB	11 9670	SYS test1...	TOS	192... 00:0...	DESKT... DESKT... ORANG... 0
5	Ds	DDB	137 60139	SYS test1...	TOS	192... 00:0...	DESKT... DESKT... ORANG... 0

Two warning messages are shown in the foreground:

- Warning!** '[DDB] SQL (select with insert) control' 정책에 의해 작업이 차단되었습니다.
- Warning!** '[DDB] scott dept block to sys' 정책에 의해 작업이 차단되었습니다.

A black box at the bottom of the screenshot contains the text: "사용자 Client 정책 위반 경보 팝업" (User Client Policy Violation Warning Pop-up).

03 주요 기능 (5/9) | 데이터 마스킹

민감정보에 대한 마스킹 적용으로 정보를 은닉하며,
Packet 분석을 통한 마스킹 처리로 DB성능 저하 없이 지원

- ✓ 지정된 Table/Column에 대한 민감정보 마스킹
- ✓ 개인정보를 가진 임의의 SQL 결과에 대한 패턴 마스킹

Define Masking Rules

오브젝트

Table, Column을 지정 민감정보 패턴을 지정

Table	Column	종류	Format
user_info	jumin	부분 마스킹	000000*

테이블/컬럼 또는 패턴 지정을 선택

컬럼 : 여러 컬럼을 동시 적용하려면 '*'을 구분자로 사용하십시오.
 Type : 컬럼 데이터 전체 은닉을 원하시면 'Full Masking'을 설정 형식에 따라 일부 은닉을 원하시면 'Partial Masking'을 선택하십시오.

Format : 'Partial Masking' 형식을 설정합니다.
 아래 예제와 같이 '*과 '0'을 이용하여 형식을 정의 하십시오.
 (예제) 원본 데이터 : 770101-1111111
 설정 방법 : 000000*
 Masking 결과 : 770101-*****

오브젝트 제외

Table	Column
마스킹 예외 테이블/컬럼 지정	



Orange for ORACLE (Unicode) - [SQL Tool:SCOTT@oracle 11g_scott/SQL1 *]

DB접근제어 솔루션 Chakra Max

10 - SCOTT@oracle 11g_scott

SQL1 *
 1
 2 ▶ `select * from user_info;`

Result

NO	NAME	JUMIN	CARD_NO	TEL
1	홍길동	777777*****	4677-3281-4596-6410	803-483-8155
2	54322	000000*****	4063-5304-5745-5067	647-7480-1940
3	고민서	647545*****	3349-3060-7605-4518	262-8849-5759
4	우라온	147184*****	7330-6564-6359-7687	628-5827-5088
5	이승해	459065*****	2145-7852-5670-9069	694-500-5667
6	최예선	986085*****	9730-6489-3367-1882	964-1496-1509
7	chakra	116355*****	2413-8032-3334-3245	311-1966-4070
8	박지혜	393117*****	5450-4772-1033-5238	880-2272-8379
9	배승호	717417*****	6580-2902-8075-1071	951-151-3404
10	서민술	018181*****	6667-9190-7227-1378	761-2725-0027
11	이지후	169012*****	3537-9029-6668-9865	369-2632-5979

Ln 2, Col 1 0.02 sec. 100+ rows

Ready AutoCommit is Off 6.0.125 CAP NUM OVR

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

03 주요 기능 (6/9) | 결재

관리자의 확인이 필요한 작업에 대해 결재 프로세스를 이용한 작업 확인, 승인(결재) 기능을 제공하며, 다양한 방식의 결재 정책을 통해 업무 연속성과 컴플라이언스 준수 지원

- ✓ 사전 결재
- ✓ 사후 결재
- ✓ 대리 결재
- ✓ 변경 전/후 데이터 수집 결재
- ✓ 긴급 결재
- ✓ 제3자 실행 결재
- ✓ DB 접근 권한 결재
- ✓ SQL 실행 권한 결재
- ✓ 마스킹 예외 결재
- ✓ Server 접근 권한 결재
- ✓ Server Command 실행 권한 결재
- ✓ 시스템 계정 관리 결재
- ✓ 이메일 결재
- ✓ 실행 권한 반환

Approval Procedure Wizard

STEP01
Configure
Approval Procedure
STEP02
Set Approval Steps
STEP03
Set Options

Set Approval Steps

결재 절차: 03 단계 절차

01번째 결재 절차- 사전 결재	기인	01번째 결재자의 결재 후 실행 가능
02번째 결재 절차- 사후 결재	기인	모든 결재자의 결재 후 실행 가능
03번째 결재 절차- 사후 결재	특정 사용자를 결재자로 지정	01번째 결재자의 결재 후 실행 가능

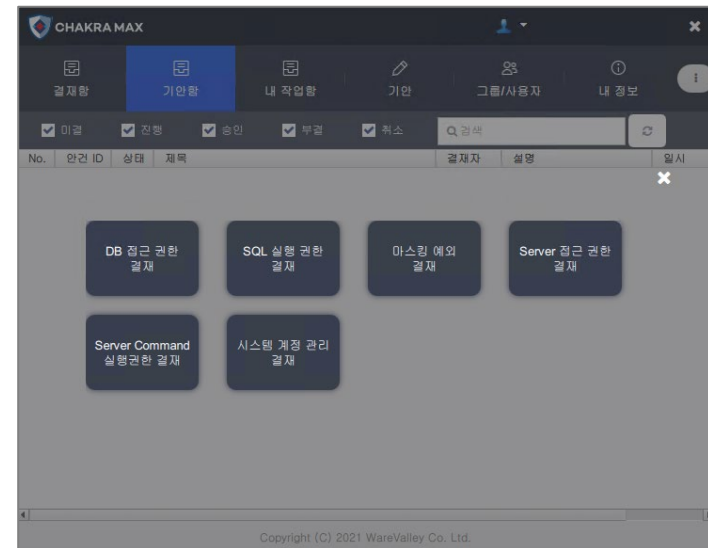
결재자 종류: 기인자의 상위 그룹 리더

결재자 종류: 특정 사용자를 결재자로 지정

결재자

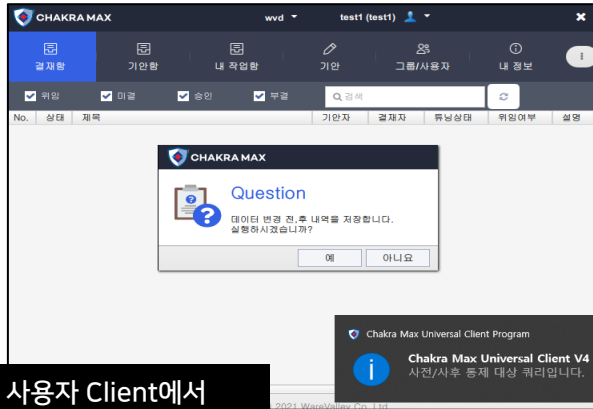
```

=====그룹장=====
기안자의 소속 그룹 리더
기안자의 상위 그룹 리더
기안자의 2번째 상위그룹 리더
특정 그룹의 리더
=====특정소속원=====
기안자가 본인 그룹 소속원 중 한명을 결재자로 지정
기안자가 상위 그룹 소속원 중 한명을 결재자로 지정
기안자가 2번째 상위 그룹 소속원 중 한명을 결재자로 지정
기안자가 특정 그룹 소속원 중 한명을 결재자로 지정
특정 사용자를 결재자로 지정
=====특정조건=====
기안자와 동일한 그룹 소속원 중 한 명이 결재함
기안자의 상위 그룹 소속원 중 한 명이 결재함
기안자의 2번째 상위 그룹 소속원 중 한 명이 결재함
특정 그룹 소속원 중 한 명이 결재함
                    
```

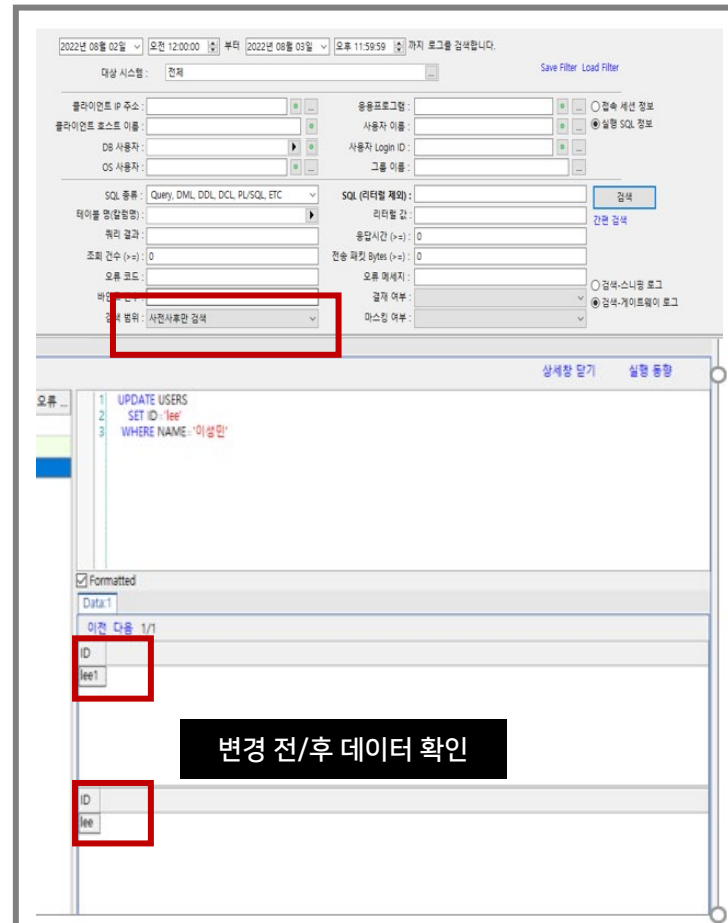
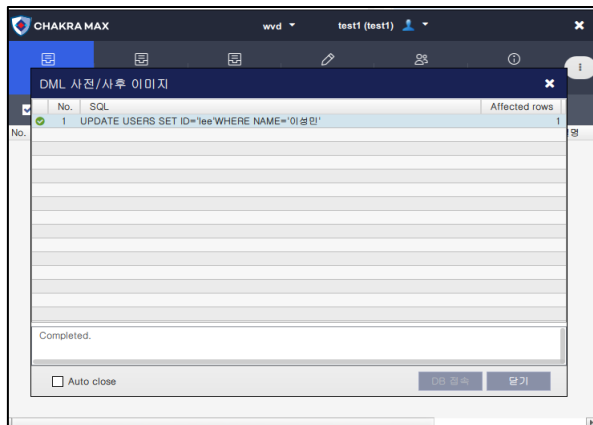


03 주요 기능 (7/9) | 변경 전/후 데이터

중요 정보의 변경이 발생하였을 때, 변경 전/후 데이터를 기록하는 기능을 사용 틀에 관계 없이 지원



사용자 Client에서
변경 전/후 저장 팝업



변경 전/후 데이터 확인

03 주요 기능 (8/9) | 보안계정 관리정책

ChakraMax Manager/Client 계정의 접속 및 패스워드 보안정책 지원

사용자 규칙 | 관리자 규칙 | 암호 규칙 | 계정 관리 프로필

User Profile Setting

Client User Profile Setting

30 일 주기로 비밀번호를 변경합니다.

3 번 비밀번호 입력 오류 시 10 분 동안 로그인할 수 없습니다.

100 일 동안 로그인하지 않으면 계정이 잠깁니다.

30 분 동안 사용하지 않으면 비밀번호를 다시 입력받습니다.

예외 사용자:

재인증시 설정된 추가인증을 사용합니다.

사용자 생성시 적용되는 기본 설정

를 기본 복합 인증방식으로 사용합니다.

로 비밀번호를 초기화합니다.

OTP (One Time Password)
Google T-OTP (Time-based
Google H-OTP (HMAC-Base
SMS (Short Message Service

- ✓ 패스워드 사용기간 설정 기능
- ✓ 비밀번호 오류 시 계정 잠김 기능
- ✓ 계정 미 사용에 따른 계정 잠김 기능
- ✓ 미 사용지 비밀번호 재입력 기능
- ✓ 프로그램 사용 시 초기 비밀번호 설정 기능

사용자 규칙 | 관리자 규칙 | 암호 규칙 | 계정 관리 프로필

Password Rule Setting

User Password Rule Setting

비밀번호의 길이를 최소 9 자 이상 16 자 이하로 지정합니다.

첫 글자는 문자만 허용합니다.

대문자를 반드시 포함 합니다.

소문자를 반드시 포함 합니다.

숫자 또는 특수문자 를 반드시 포함 합니다.

동일한 문자의 3 자 이상 연속 사용을 금지 합니다.

연속된 문자의 3 자 이상 연속 사용을 금지 합니다.

계정의 전화번호 사용을 금지합니다.

계정의 E - mail 주소 사용을 금지합니다.

과거 1 회 까지 사용한 비밀번호는 재사용이 불가능합니다.

다음 문자열은 비밀번호에 포함될 수 없습니다.

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

03 주요 기능 (9/9) | 2 Factor 인증

ChakraMax Manager/Client 계정 접속 시 다양한 추가 인증 적용

User Wizard

STEP01
Configure User
STEP02
Assign Group

Configure User

ID:

이름:

암호:

다시 입력:

복합 인증방식:

만료 기간: OTP (One Time Password)

SMS (Short Message Service)

전화번호: Google T-OTP (Time-based One Time Passw...

모바일 번호: Google H-OTP (HMAC-Based One Time Pas...

Email:

설명:

접근 가능 IP(s): 추가 삭제

현재 사용자 IP 통제 정책은 적용되어 있지 않습니다.
System > 설정 페이지에서 정책을 적용할 수 있습니다.

복합 인증방식 선택



- ✓ OTP
- ✓ SMS
- ✓ Google OTP
- ✓ 인증서(PKI)
- ✓ Biometric(지문)

Database Security Assurance
Securing Your Databases Against Threats
Database Activity Monitoring & Access Control
Database Vulnerability Assessment
Trusted Database operation obtaining Approval

Chakra Max Universal Client V4

Additional Auth.

인증

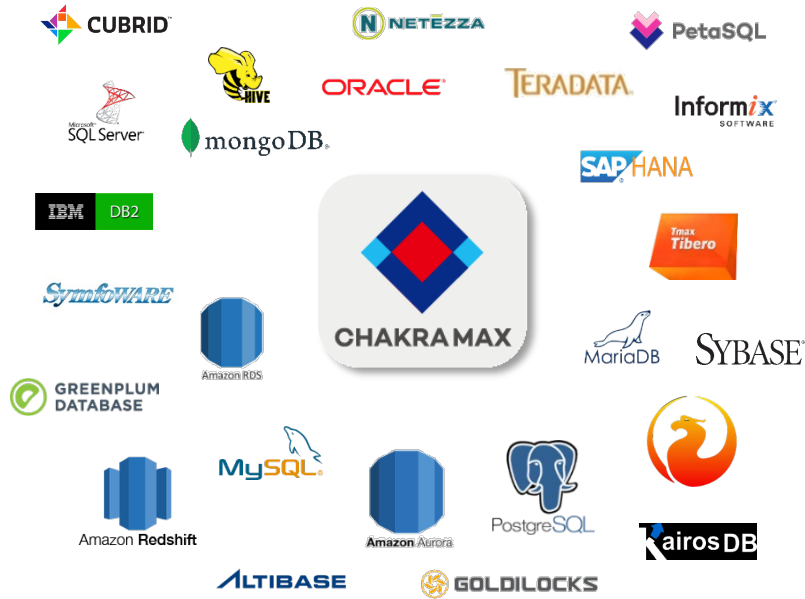
[OTP Key 재발급](#)

04 관리기능 (1/8) | DBMS 지원범위 확대

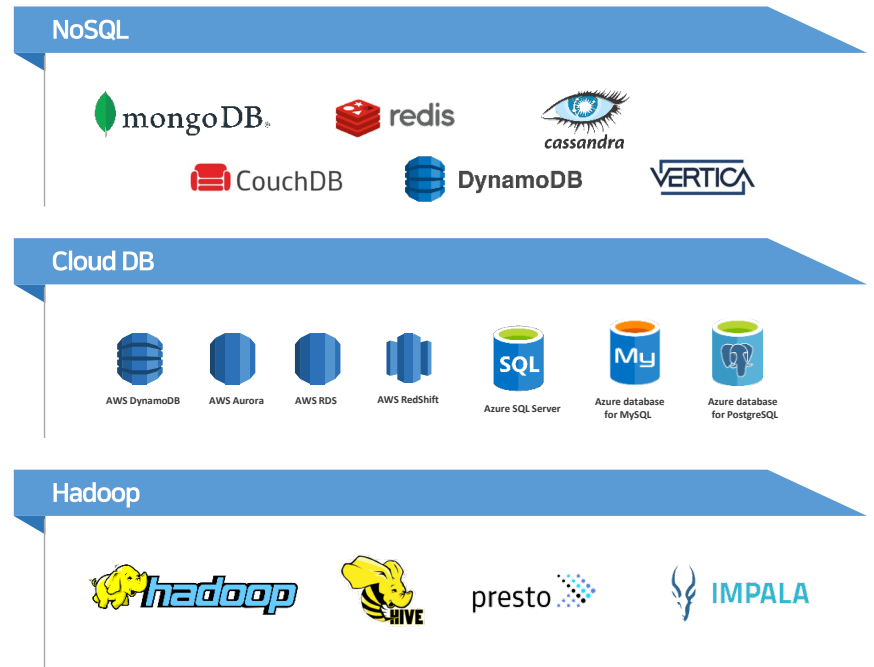


최신 개발 트렌드에 맞춰 NoSQL 및 다양한 Cloud DBMS에 대한 보안기능 지원을 확대하고 지속적인 업데이트를 제공

✓ 국내 최다 DBMS 지원



✓ 지원 범위 확대



04 관리기능 (2/8) | 최신 OS 지원 및 보안기능 강화

주요 보안 이슈와 취약점에 대한 신속한 대응으로 보안 요구사항을 충족하며, 최신의 보안 환경으로 솔루션의 안정적인 기술지원 및 운영 환경 구성을 지원

최신 OpenSSL

OpenSSL 1.0의 EOS(2023.09.11) 대응
및 최근 발견된 CVE 취약점 제거를 위해
OpenSSL 3.0을 채택하여 향후
안정적인 운영 지원

Rocky Linux 9.0

RHEL 7.0의 EOL(2024.06.30) 확정으로 지원이
종료됨에 따라 향후 안정적인 운영을 위해
RHEL과의 호환성,이식성이 높은 Rocky Linux 9을
공식 OS로 지정

최신 CC인증 EAL4

국가정보원(NIS)에서 발표된 최신 "국가용
보안 요구사항 V3.0" 규격을 기준으로
CC인증 취득하여 최신 보안 트렌드 요건 충족

인증 고도화

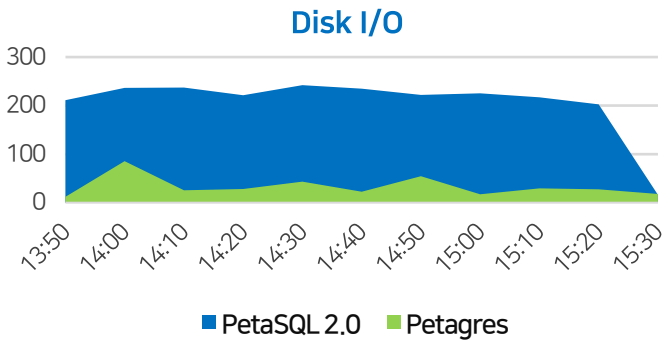
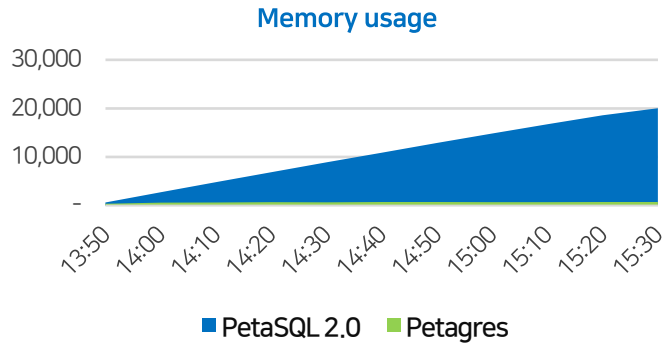
FIDO(홍채, 지문 등 생체인증) 및
인증 연동(SSO, Octa, OneLogin 등)
고도화로 사용자 인증 보안성/편의성 강화

 Chakra Max

04 관리기능 (3/8) | 고속데이터 분석용 DBMS 탑재



고속데이터 분석용 Petagres의 탑재로 저장공간 효율 확대 · 검색속도 향상 · 리소스 효율 증가 등 최적화된 운영 환경을 제공



경량화
1/10

Chakra Max Repository 사용시 로그 저장 사이즈

- 기존 PetaSQL 2.0 대비 약 1/10의 로그 **저장** 효율 증가

고속화
400%

Chakra Max Repository 사용시 로그 검색 시간

- 기존 PetaSQL 2.0 대비 약 400% 로그 **검색** 효율 증가

데이터 건수	제품	저장 성능	검색 성능	메모리 사용량
117,527,198	PetaSQL v2.0	6,764 MB	192분 45초	6,995 MB
	Petagres	524 MB	47분 6초	1,096 MB

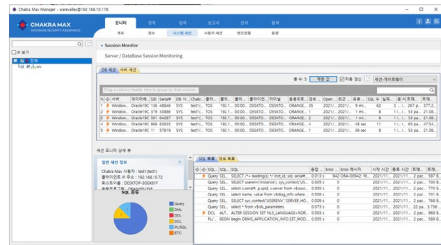
04 관리기능 (4/8) | 데이터 위변조 방지 및 암호화

로그 위변조 방지를 위해 ChakraMax 엔진 외에 쓰기 및 변경 제한 로그데이터를 암호화하여 저장함으로써 데이터 보안 기능 강화

```
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'
```

사용자가 Repository DB에 접근하여 로그 테이블에 update, delete 등을 시도하였을 때, 테이블이 보호되어 실행할 수 없음

감사 로그 테이블의 컬럼을 암호화하여, 복호화 키 없는 불법적인 데이터 열람 시 식별 불가



Name	ID num
홍길동	730603-2468246
김둘러	821110-1357913
김철수	961208-1346793
...	...
가나다	430303-2371121
고사을	690815-1965852
김영희	561219-1654812
이순자	880312-2674984
Varchar(20)	Char(14)

복호화된 데이터 (Plain Text)

보안관리자의 매니저 프로그램을 통한 감사로그 조회

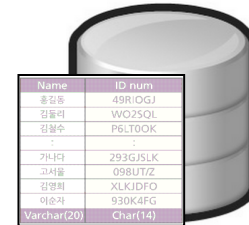


CHAKRAMAX

복호화 키 AES / RC4 / SEED / DES3 지원



복호화



감사로그 (Encrypted Text)

04 관리기능 (5/8) | 통신구간 암호화



사용자 <-> ChakraMax <-> DB 서버 모든 구간의 암호화 통신 지원

구간 암호화 옵션 활성화
DB서버 ssh 계정/비밀번호 입력

Set Database Information

구성환경: Stand alone RAC (Real Application Clusters)

SID:

서비스 이름:

데이터베이스가 설치/운영 중인 서버를 선택하십시오.

서버:

네트워크	IP 주소	서비스 포트	게이트웨이 포트	Listening f
	192.168.10.171	1521	10103	SID and S

사용되는 네트워크 환경을 모두 선택하고, 서비스 포트와 사크라 게이트웨이 서버에서 사용할 포트를 확인/변경 하십시오.

포트 리다이렉션

Connection through Jump Server

Jump Server:

Secure Connection Port:

User Name:

Password:

사용자 - Chakra Max 구간 암호화

```

00000: 0000 2997 4a36 1802 0520 0141 0000 4508  ...J.....E.
00010: 0029 11e0 0000 0000 4400 0000 0000 0000  ...D.....
00020: 0012 c038 0377 0312 0300 1372 030c 5010  ...f.....P.
00030: 100a 3e77 0000 0000 0000 0000  ...u.....
18-21-44.30264 IP 132.168.10.72.52287: Flags [L], ack 1, win 165, options (nop,nop,ack 1 (0:11), length 0
00000: 1802 0520 0141 0000 2997 4a36 0000 4508  ...A...J...E.
00010: 0029 11e0 0000 0000 4400 0000 0000 0000  ...D.....
00020: 0012 c038 0377 0312 0300 1372 030c 5010  ...f.....P.
00030: 0005 5671 0000 0101 050a 0c74 0300 0312  ...q.....l..I.
00040: 0300  ...
18-21-44.412731 IP 132.168.10.72.52286 > dbase:1815: Flags [L], seq 3636809478-3636809479, ack 919396159, win 4106, length 1
00000: 0000 2997 4a36 1802 0520 0141 0000 4508  ...J.....E.
00010: 0029 11e0 0000 0000 4400 0000 0000 0000  ...D.....
00020: 0012 c038 0377 0312 0300 1372 030c 5010  ...f.....P.
00030: 100a 595a 0000 0000 0000 0000  ...Z.....
...
18-21-44.412759 IP 132.168.10.72.52286: Flags [L], ack 1, win 168, options (nop,nop,ack 1 (0:11), length 0
00000: 0000 2997 4a36 1802 0520 0141 0000 4508  ...A...J...E.
00010: 0029 11e0 0000 0000 4400 0000 0000 0000  ...D.....
00020: 0012 c038 0377 0312 0300 1372 030c 5010  ...f.....P.
00030: 0005 5671 0000 0101 050a 0c74 0416 0c74  ...q.....l..f..t
00040:  ...
18-21-44.439455 IP 132.168.10.72.52280 > dbase:1815: Flags [L], seq 1740706614-1740706615, ack 1156608081, win 4105, length 1
00000: 0000 2997 4a36 1802 0520 0141 0000 4508  ...J.....E.
00010: 0029 11e0 0000 0000 4400 0000 0000 0000  ...D.....
00020: 0012 c038 0377 0312 0300 1372 030c 5010  ...f.....P.
00030: 1009 1f64 0000 0000 0000 0000  ...
00040:  ...
18-21-44.439455 IP 132.168.10.72.52280 > dbase:1815: Flags [L], seq 1740706614-1740706615, ack 1156608081, win 4105, length 1
00000: 0000 2997 4a36 1802 0520 0141 0000 4508  ...J.....E.
00010: 0029 11e0 0000 0000 4400 0000 0000 0000  ...D.....
00020: 0012 c038 0377 0312 0300 1372 030c 5010  ...f.....P.
00030: 1009 1f64 0000 0000 0000 0000  ...
00040:  ...
18-21-44.440094 IP 132.168.10.72.52145 > db
00000: 0000 2997 4a36 1802 0520 0141 0000 4508  ...J.....E.
00010: 0029 11e0 0000 0000 4400 0000 0000 0000  ...D.....
00020: 0012 c038 0377 0312 0300 1372 030c 5010  ...f.....P.
00030: 1005 5377 0000 0000 0000 0000  ...
00040:  ...
18-21-44.440094 IP 132.168.10.72.52145 > db
00000: 0000 2997 4a36 1802 0520 0141 0000 4508  ...J.....E.
00010: 0029 11e0 0000 0000 4400 0000 0000 0000  ...D.....
00020: 0012 c038 0377 0312 0300 1372 030c 5010  ...f.....P.
00030: 1005 5377 0000 0000 0000 0000  ...
00040:  ...
17-05-31.119254 IP 172.17.6.111.39576 > 172.16.100.11.ssh: Flags [L], seq 5182992, length 0
00000: 4500 0034 9101 4000 4006 d077 ac11 0661  E..4..0..v...e
00010: ac10 0406 3a30 0016 8c61 5311 770c e03e  ..d..h...of..*..
00020: 8010 01c2 0142 0000 0101 080a 3451 65e6  ...8.....4%.
00030: 7aeb 8e10
00040:  ...
17-05-31.119254 IP 172.17.6.111.39576 > 172.16.100.11.ssh: Flags [L], ack 105182992, length 0
00000: 4500 0034 9101 4000 4006 d077 ac11 0661  E..4..0..v...e
00010: ac10 0406 3a30 0016 8c61 5311 770c e03e  ..d..h...of..*..
00020: 8010 01c2 2415 0000 0101 080a 7aeb a275  ...$......u..
00030: 7aeb 8e10
00040: 3451 65e6
17-05-31.119254 IP 172.16.100.11.ssh > 172.17.6.111.39576: Flags [L], seq 576842051, length 0
00000: 4500 0034 a07e 4000 3406 d2aa ac10 640e  E..4..h...d..
00010: ac11 0661 0016 3a30 770c e03e 8c61 5400  ...$......of..t.
00020: 8010 01c2 2415 0000 0101 080a 7aeb a275  ...$......u..
00030: 3451 65e6

```

04 관리기능 (6/8) | 감사로그 백업



일일 로그데이터의 자동 백업 및 복구 기능 제공

- ✓ 감사로그 백업 및 복구
- ✓ 설정 데이터 백업 및 복구
- ✓ 보안 정책 백업 및 복구
- ✓ 성공 및 실패 여부 확인
- ✓ 저장위치, 시간, 용량 등 정보제공
- ✓ 일일 백업 스케줄 설정

The screenshot displays the Chakra Max Manager interface with the following components:

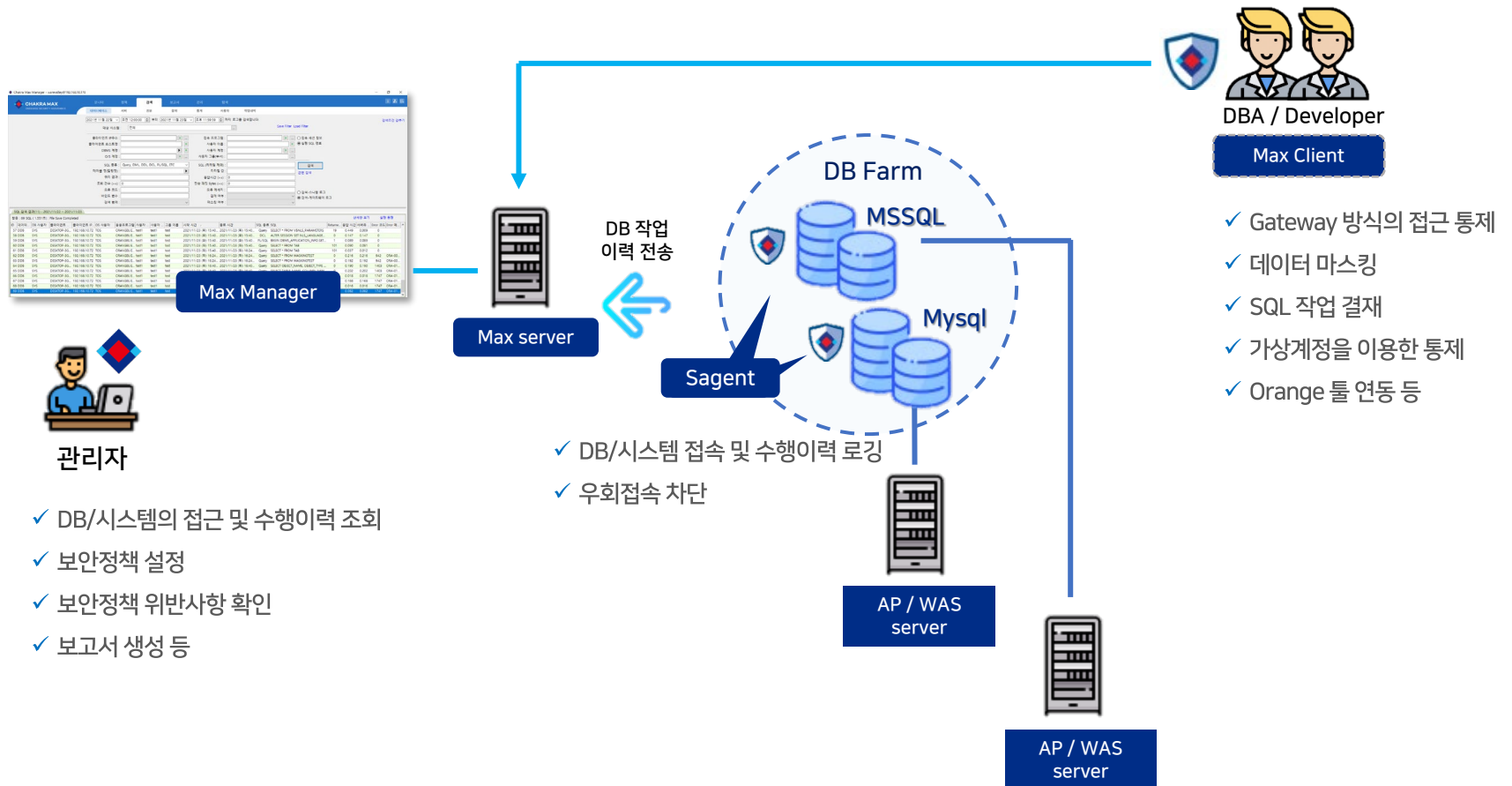
- Navigation Bar:** Includes tabs for '관리' (Management) and '탐색' (Search), and sub-tabs for '시스템', '사용자', '권리자', '백업', 'S-TAP 에이전트', and '환경설정'.
- Backup Schedule Table:** A grid showing backup status for months from July to November 2021. Legend: Green (successful), Orange (failed), Red (restored), Bold (recovery).
- Backup History Table:**

백업 상태	ChakramaxDB...로그 날짜	종류	파일 경로	백업 파일 사...	여유 공간	시작 시간	종료
완료	2021년 11월 22일	자동	/home/chakramax/log_backup/2021-11-22/MAX_SQL...	0.3 Mbytes	27.98 Gbytes	2021년 11월 23일 01:01:07	2021년 11월 23일 01:01:06
완료	2021년 11월 21일	자동	/home/chakramax/log_backup/2021-11-21/MAX_SQL...	0.1 Mbytes	28.31 Gbytes	2021년 11월 22일 01:01:06	2021년 11월 22일 01:01:06
- Backup Settings Dialog:**
 - 스케줄 옵션:** Radio buttons for '백업 안함', '일일 백업', and '오전 1:00'.
 - Email 알림 옵션:** Radio buttons for '통보 없음', '오류시 통보', and '항상 통보'.
 - 디스크 남은 용량 점진:** Slider set to 10%.
 - 파일 분리:** Radio buttons for '분리하지 않음' and '파일 분리'.
 - 백업 암호:** Password field with dots.
 - 암호 확인:** Confirmation password field with dots.
 - 백업 파일 위치:** Fields for 'Chakra Max DB' and '/home/chakramax/log_backup'.
 - Audit Log Retention Period Table:**

종류	유지 기간	설명
Database 접속 이력 로그	365 Database	접속 정보를 저장합니다.
SQL 실행 로그	365 SQL 실행	실행 정보를 저장합니다.
Alert	365 보안 경고 발생	이력을 저장합니다.
- Visualizations:**
 - 파일 공간:** Pie chart showing '백업' (Backup) and '여유' (Free) space.
 - 데이터 스페이스:** Horizontal bar chart showing usage for db_sess, apprv_schedule, max_machine_status, sql_log, max_engine_status, and etc.
 - 메모리 사용량:** Vertical bar chart showing memory usage.
- Footer Note:** "총 2가 백업 파일이 있으며 평균 크기는 0.186 Mbytes 입니다. 최대 허용치가 50년을 넘으므로 날짜를 제한할 수 없습니다. 이 주이에는 환경 로그의 데이터가 반영되어 있지 않습니다."

04 관리기능 (7/8) | 클라우드(가상화) 환경 지원

AWS / Azure / NCP / GCP / KT / NHN / HCI 등 다양한 클라우드(가상화) 환경에서 Gateway 및 Sniffing 구성 지원



04 관리기능 (8/8) | 보고서 기능

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

- ✓ 스케줄러를 이용한 보고서 자동 생성과 메일 전송 지원
- ✓ Excel, PDF, DOC, HWP 등 다양한 문서 포맷 제공
- ✓ 약 50종에 달하는 다양한 형식의 보고서 포맷 제공

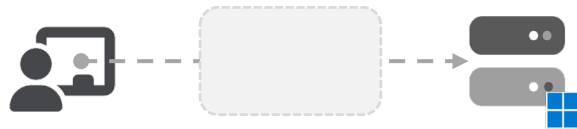
The screenshot displays the Chakra Max Manager v4.0 interface. On the left, a tree view lists various report categories such as '카테고리', '정보 보고서', '로그 보고서', 'DB 세션 보고서', '인증이력 보고서', '기간장부 접속기록 보고서', '간접장부 보고서', '서버 세션 보고서', 'SQL 보고서', '통계 보고서', '보고서 파일', '스케줄러', and '예외 리스트'. The main window shows a '사용량 보고서' (Usage Report) with a list of reports and a preview of a 'DB 세션 요약 보고서' (DB Session Summary Report).

The report preview includes a bar chart showing session counts for different DB instances and a table with the following data:

DB	클라이언트 IP	DB 계정	시작시간	종료시간	세션수	SQL수	결과행수
ASMS.0	192.168.0.10	AOS	2023-06-01 00:00:00	2023-07-03 00:00:00	387	59,430	73,687
ASMS.0	192.168.0.10	root	2023-05-27 0:00	2023-07-03 11:28	190,093	24,965,721	30,417,512
mssql_2019	192.168.0.42	jyjun	2023-06-12 11:34	2023-06-13 14:26	36	289	2,688
mssql_2019	192.168.0.23	sa	2023-06-11 19:48	2023-06-11 19:50	4	19	22
mssql_2019	192.168.0.23	sa	2023-06-12 14:02	2023-06-12 14:03	3	47	46
mssql_8	192.168.0.23	jyjun	2023-06-11 19:48	2023-06-11 19:50	1	16	1,214
mssql_2019	192.168.0.23	jyjun	2023-06-12 11:38	2023-07-03 11:28	143	777	7,921
mssql_2019	192.168.0.23	sa	2023-06-12 14:03	2023-06-12 14:06	1	43	44
mssql_2019	192.168.0.23	sa	2023-06-12 11:56	2023-06-12 12:08	4	12	0
mssql_8	192.168.0.42	jyjun	2023-06-28 14:52	2023-06-28 14:54	5	0	0
oracle	192.168.0.42	SYSTEM	2023-06-28 14:12	2023-06-28 14:54	27	138	402

CHAKRAMAX FOR SAC

시스템 접근 통제



- RDP (Remote Desktop Protocol)
- FTP (File Transfer Protocol)
- SFTP (SSH File Transfer Protocol)

02

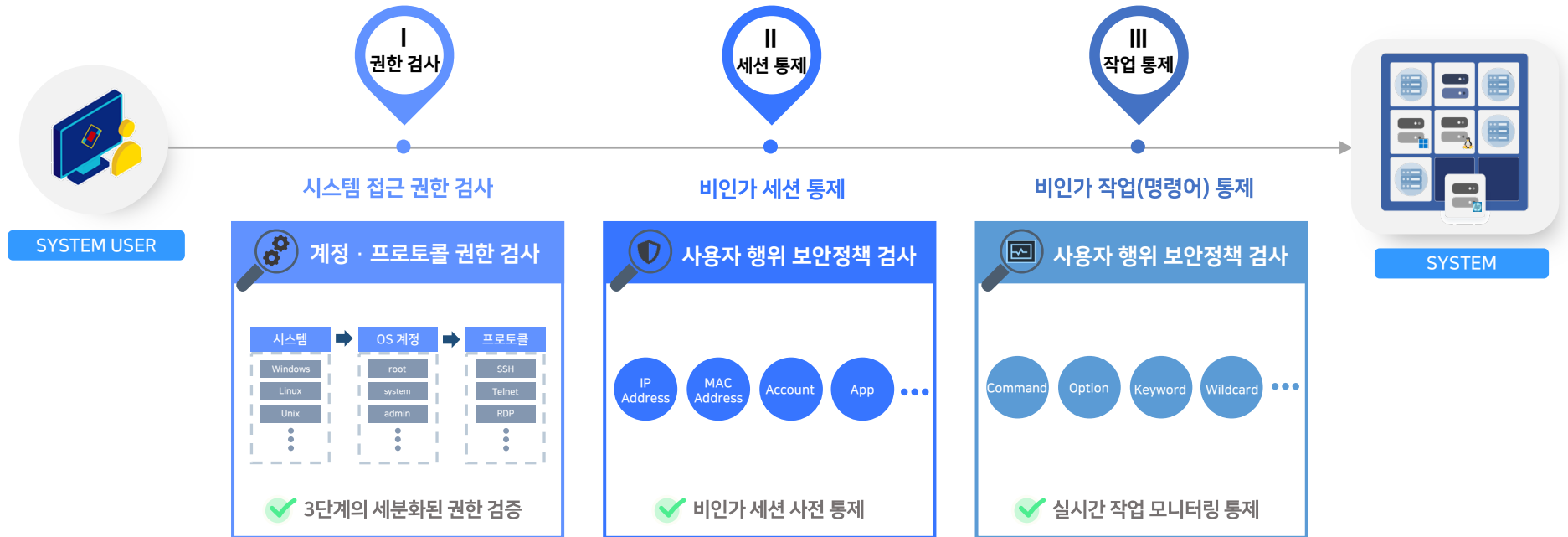
01 주요 기능 | 시스템 접근통제



02 기본 구성 플로우 | 시스템 접근통제



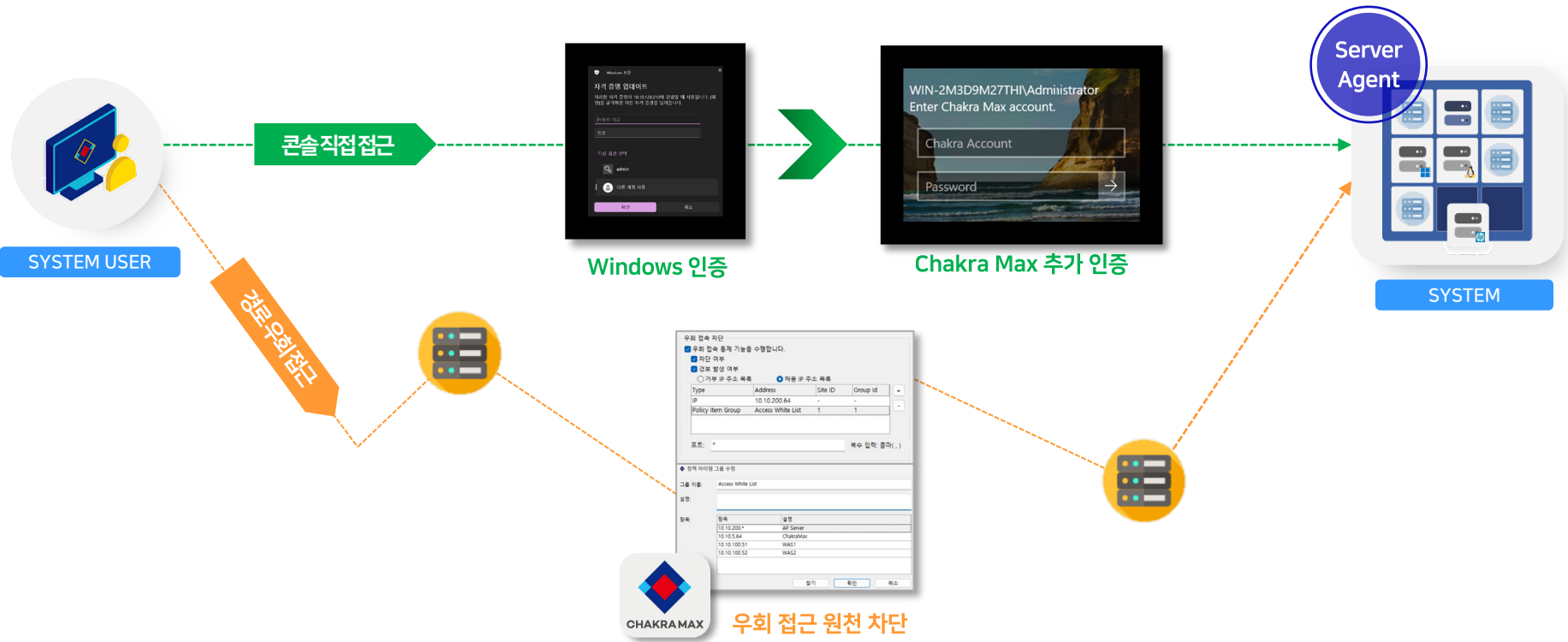
사용자 계정 · 프로토콜 등 세션 검사를 통한 비인가 접근의 세부적인 정책 설정을 지원하며, 불법적인 접근 및 금지 명령어를 사전에 통제하여 보안 사고를 예방



03 서버 보안 | 시스템 접근통제



인가되지 않은 외부 접근이나, 타 시스템을 경유한 우회 접근에 대한 통제 정책을 관리
또한, 콘솔 · 시리얼 접근과 같이 시스템 로컬 접속에 대하여 2차 추가 인증 기능을 지원하며 모든 작업 행위를 기록



04 접근 행위 기록 | 시스템 접근통제



모든 시스템 접근에 대한 세션 · 명령어 정보 기록하고, 다양한 감사 보고서를 제공합니다.
또한 별도의 Agent 설치 없이 Windows Server에 대한 작업 화면 녹화 · 재생 · 다운로드 기능을 지원합니다.

로그 기록 및 감사보고서

23가지 세션 정보 기록

20가지 명령어 정보 기록

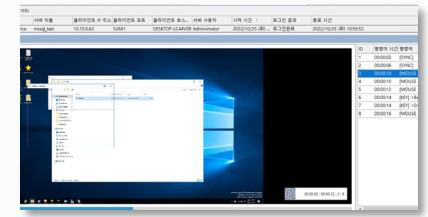
OZ Report 탑재 · 감사보고서 제공

종류	OS	프로세스명	로그인 시간	로그아웃 시간	종료시간(부수)	프로세스명	종료시간(카운트)
관리자	Windows	cmd	2023.06.15 15:09:38	2023.06.15 15:09:38	10.10.200.1	cmd	1
관리자	Windows	cmd	2023.06.15 15:10:28	2023.06.15 15:10:28	10.10.200.1	cmd	2
관리자	Windows	cmd	2023.06.15 15:11:27	2023.06.15 15:15:48	10.10.200.1	cmd	22
관리자	Windows	cmd	2023.06.15 15:15:56	2023.06.15 15:15:56	10.10.200.1	cmd	23
관리자	Windows	cmd	2023.06.15 15:14:58	2023.06.15 15:17:29	10.10.200.1	cmd	1
관리자	Windows	cmd	2023.06.15 15:18:32	2023.06.15 15:18:32	10.10.200.1	cmd	24
관리자	Windows	cmd	2023.06.22 17:22:09	2023.06.22 17:22:22	10.10.200.1	cmd	25
관리자	Windows	cmd	2023.06.22 17:28:11	2023.06.22 18:02:06	10.10.200.1	cmd	26



Windows Server 터미널 녹화 및 재생 기능

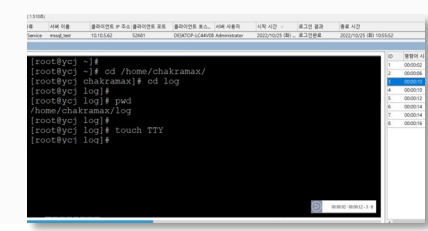
Agent 설치 없이 Windows 작업 화면 녹화



- ✓ Event 녹화
- ✓ 자체 재생 기능
- ✓ 영상 다운로드

LINUX / UNIX Server 터미널 녹화 및 재생 기능

Agent 설치 없이 Linux/Unix 작업 화면 녹화



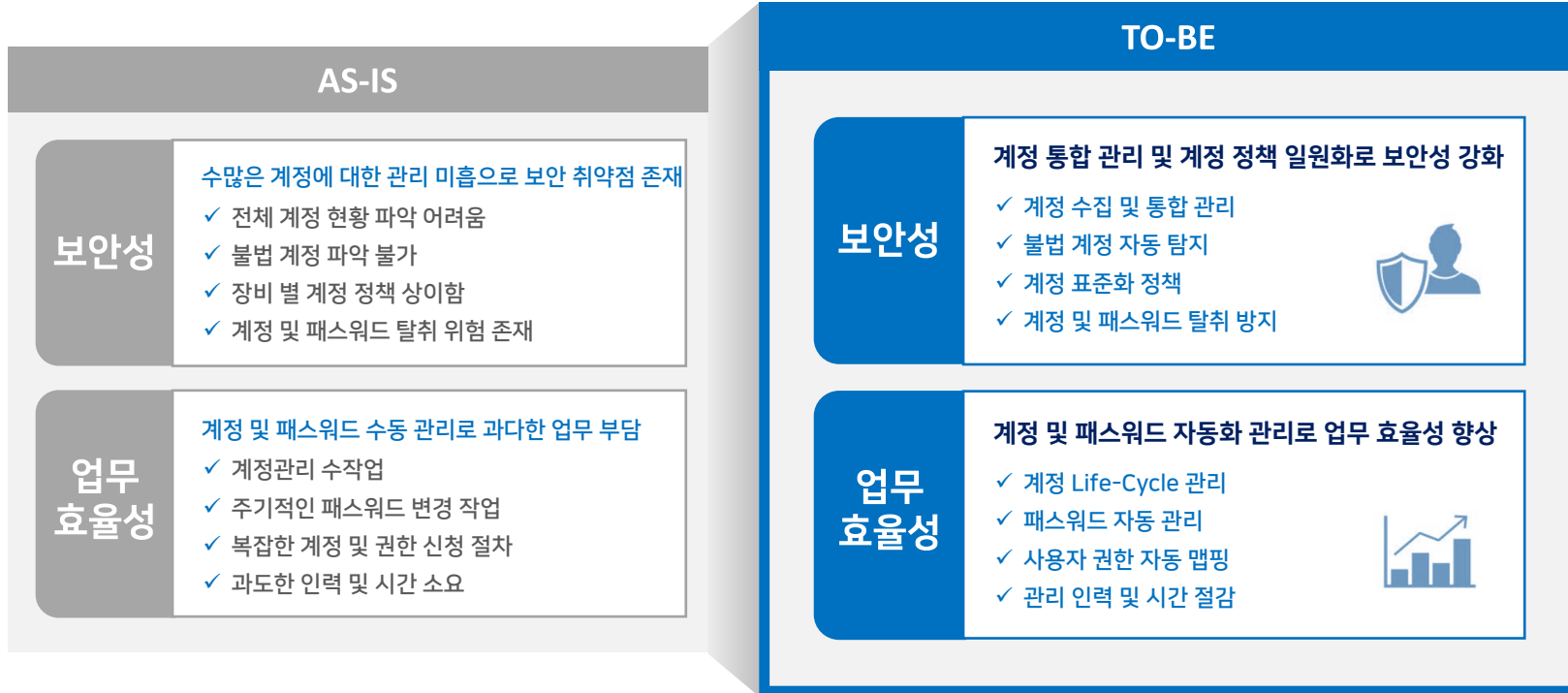
CHAKRAMAX IAM
계정 관리

03

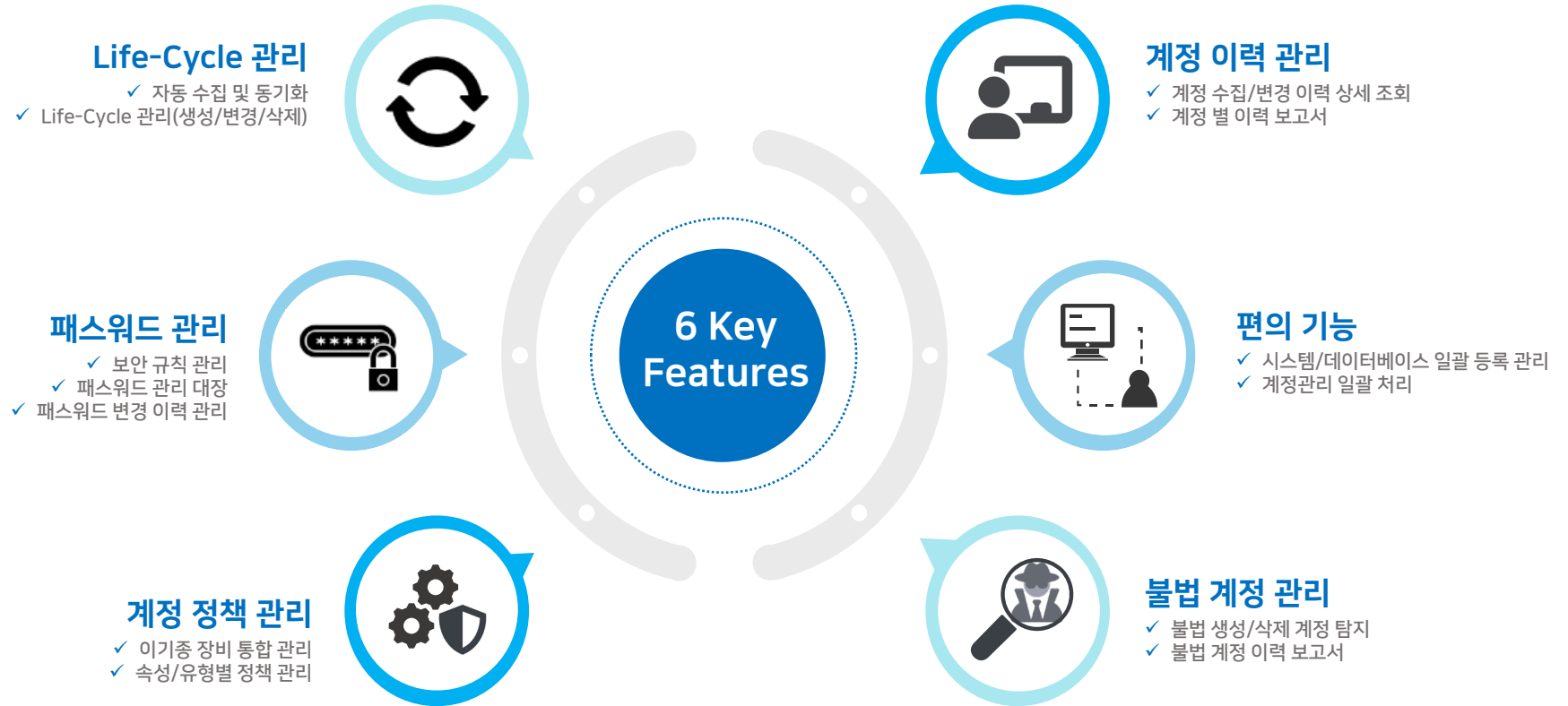
01 도입 기대 효과 | 계정 관리

계정 통합 관리 및 계정 정책 일원화로 보안성을 강화하고, 계정 및 패스워드 관리 자동화로 업무 효율성 향상

100 SYSTEM * 100 ACCOUNT = 10000 ACCOUNT !

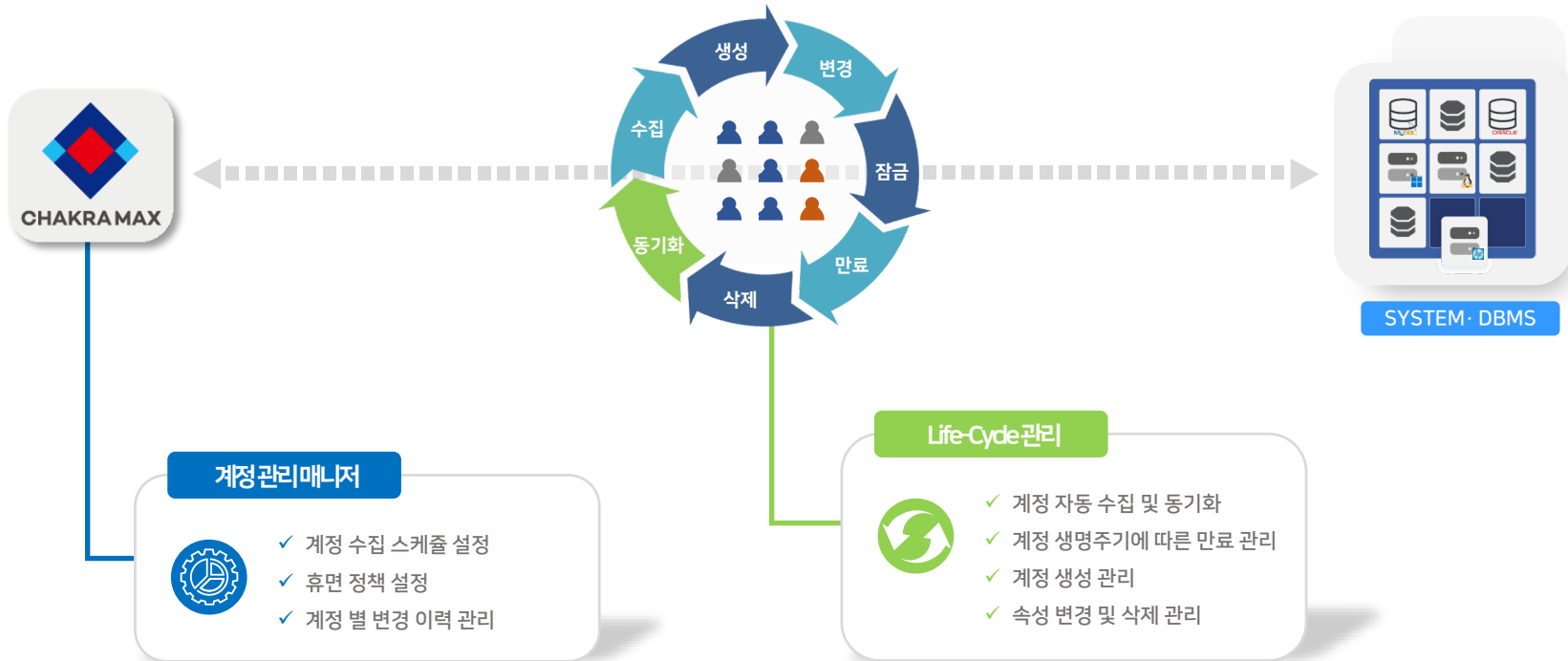


02 주요 기능 | 계정 관리



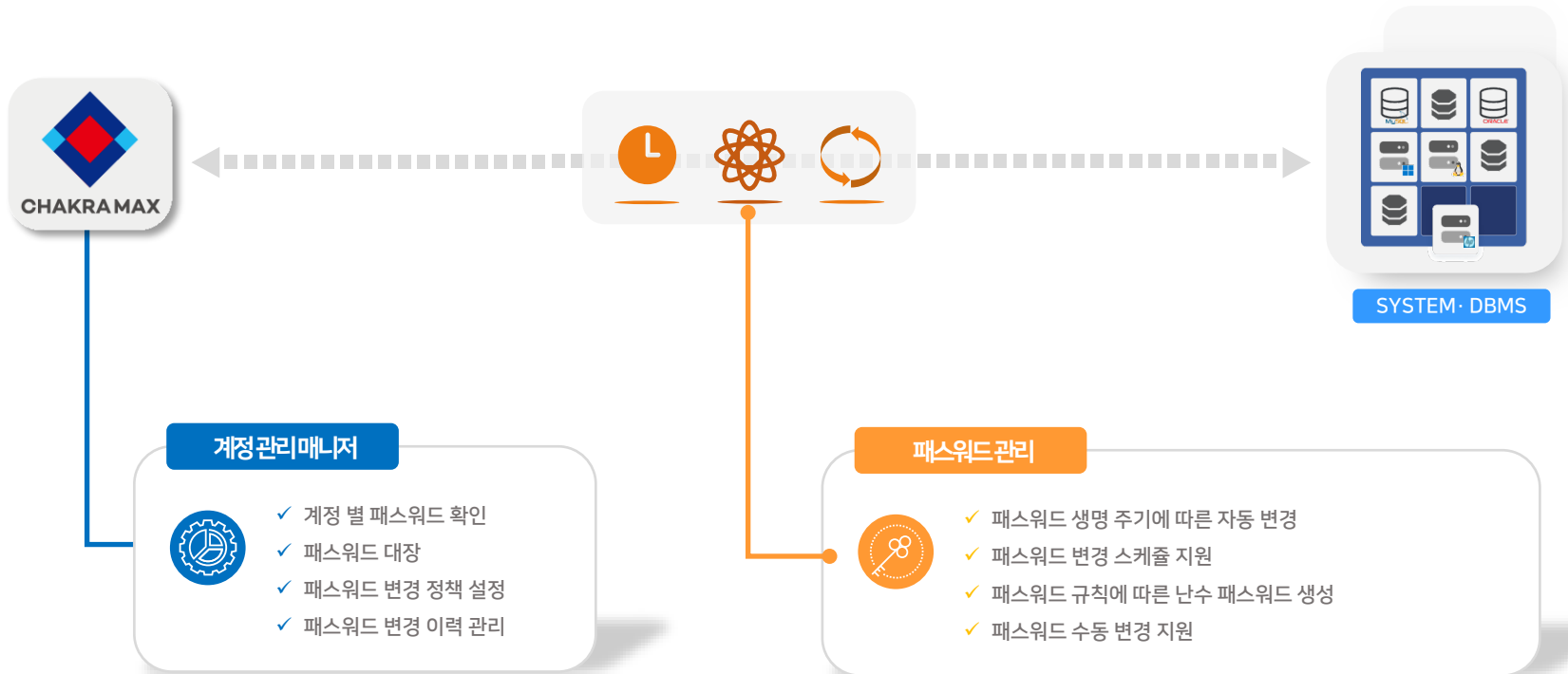
03 기능 소개 (1/5) | Life-Cycle 관리

별도의 Agent 설치 없이 데이터베이스 · 시스템의 모든 계정 정보를 자동으로 수집하고, 수집된 계정에 대한 생성/변경/삭제 등의 프로비저닝 기능 지원



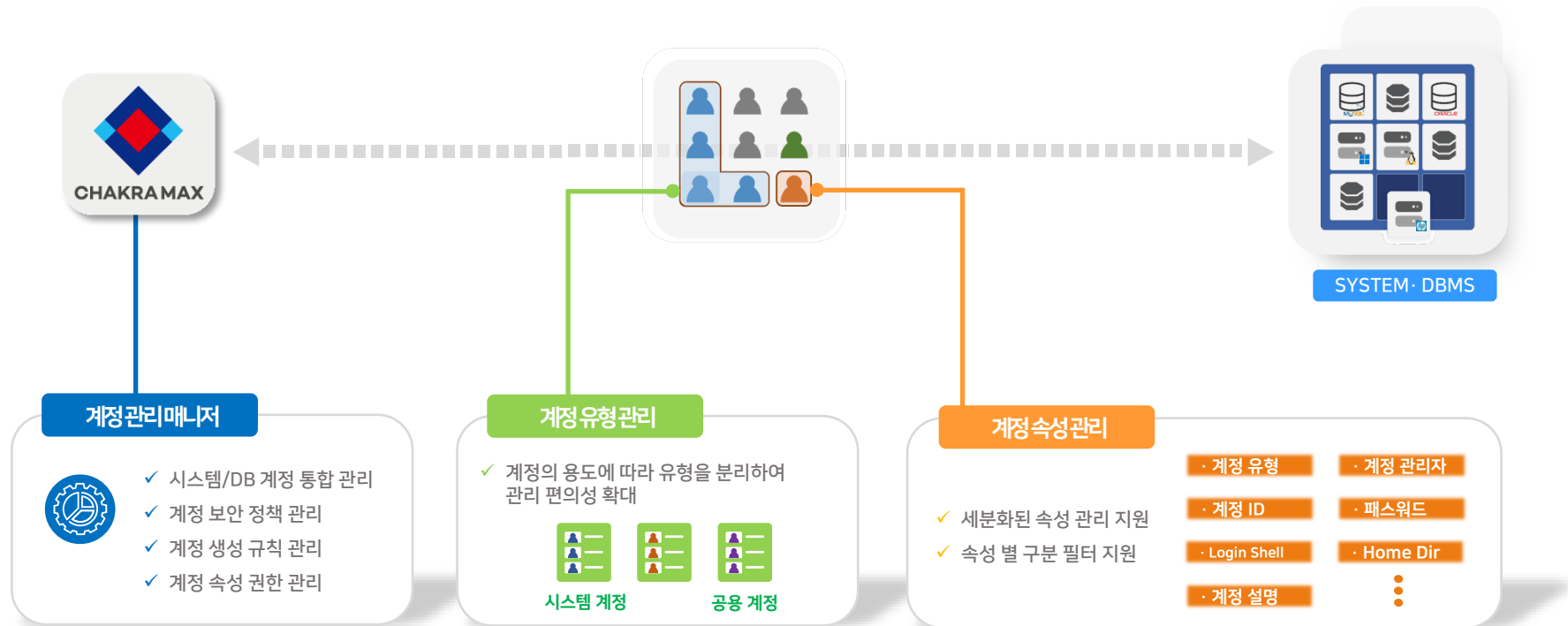
03 기능 소개 (2/5) | 패스워드 관리

영문+숫자 혼합 · 특수문자 등 다양한 생성 규칙을 적용하여 일원화된 패스워드 관리 정책을 제공하고, 패스워드 생명 주기에 따라 자동 변경 및 패스워드 이력 관리 기능 지원



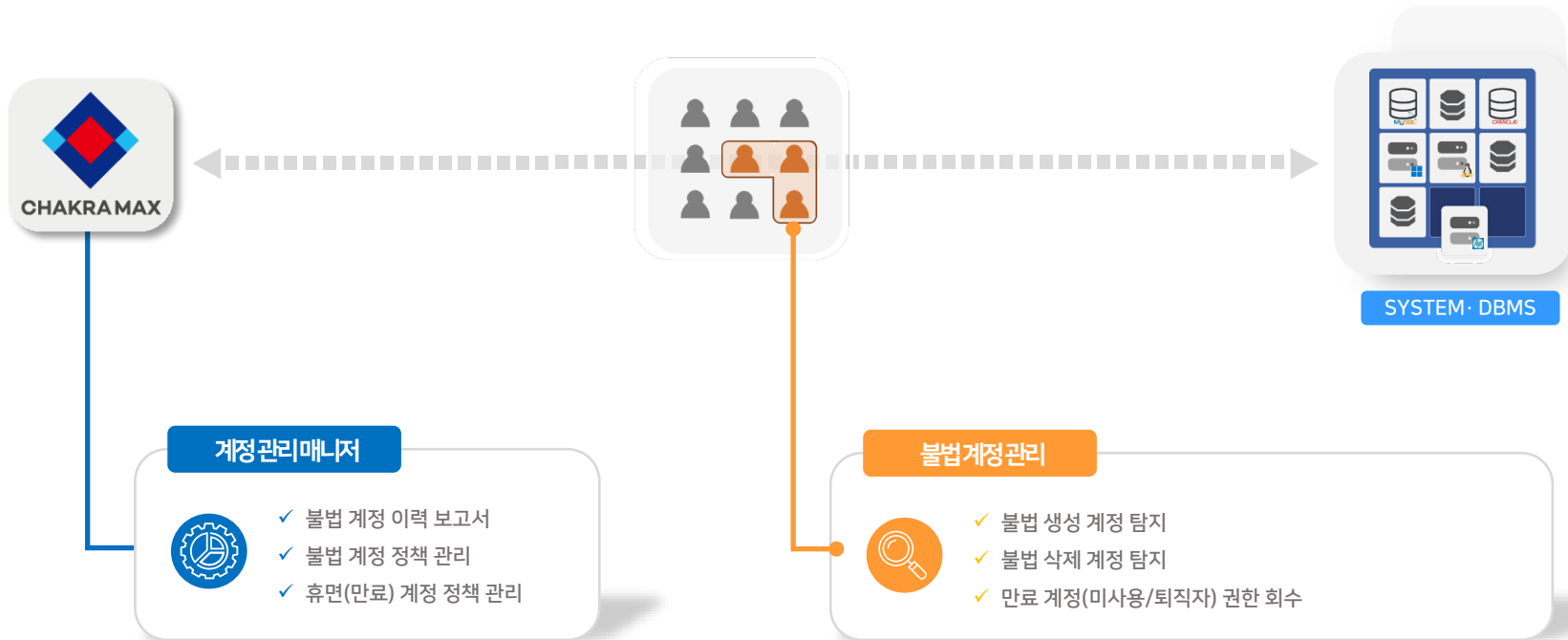
03 기능 소개 (3/5) | 계정 정책 관리

이기종 장비에 산재되어 있는 모든 계정을 수집 · 취합하여 통합 정책 관리 지원
계정의 유형별 · 속성별 관리 정책 수립으로 효율적인 관리 가능



03 기능 소개 (4/5) | 불법 계정 관리

사용자 계정의 유효성을 정기적으로 검사하여 위협이 될 수 있는 불법 생성 · 삭제된 계정을 자동으로 탐지
불법 계정에 대한 탐지 이력을 별도로 기록하여 감사 보고서를 제공



03 기능 소개 (5/5) | 편의 기능

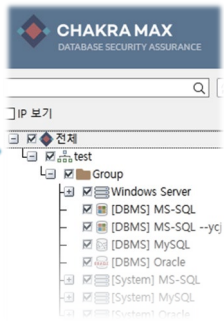


SYSTEM · 데이터베이스 일괄 등록 기능 및 프로비저닝 검증 플래그를 제공하여 다수의 SYSTEM을 안정적으로 관리 수집된 계정의 일괄 속성 관리 기능으로 업무 효율성 증대

SYSTEM · 데이터베이스 일괄 등록 및 계정 일괄 관리 기능 제공

NAME	계정 관리용 ID	IP Address	Protocol
기간계 시스템	Administrator	10.10.200.12	SSH
운영계 시스템	root	10.5.170.45	RDP FTP
인사 DB	System	10.5.100.98	SSH SFTP
그룹웨어 DB	Root	10.10.70.152	SSH
개발 TEST DB	sys	10.10.200.50	SSH TELNET
WAS 1	Admin	10.10.100.93	SSH SFTP

Import



다수의 SYSTEM 관리를 위한 검증 플래그 제공

No	SYSTEM	계정 관리 ID	검증 결과	...
1	기간계 시스템	Administrator	●	
2	운영계 시스템	root	●	
3	인사 DB	System	●	
4	그룹웨어 DB	Root	●	
5	개발 TEST DB	sys	●	
6	WAS 1	Admin	●	

Check	No	ID	속성 관리
<input checked="" type="checkbox"/>	1	Scott	Group 변경
<input checked="" type="checkbox"/>	2	System	PW 변경
<input checked="" type="checkbox"/>	3	Ycjeon	권한 제거
<input checked="" type="checkbox"/>	4	Root	PW 변경
<input checked="" type="checkbox"/>	5	Chakrafw	SSH TELNET
<input checked="" type="checkbox"/>	6	admin	SSH SFTP

일괄 설정



설정 반영



SYSTEM · DBMS

CHAKRAMAX V4.0
통합관리

04

01 통합 관리 솔루션

데이터베이스 · 시스템 접근통제 및 계정관리 기능을 하나의 시스템으로 통합하여 IT인프라 시스템의 보안을 강화하고, 동시에 관리 시간과 비용 소모를 줄여 보다 효율적인 업무 환경을 제공



통합 접근통제

- ✓ 데이터베이스 및 시스템 통합 접근 통제
- ✓ 보안정책을 통한 비인가 접근 및 작업 통제

통합 계정관리

- ✓ 데이터베이스 및 시스템 통합 계정 관리
- ✓ 계정 라이프사이클 관리
- ✓ 패스워드 관리

서버 보안

- ✓ Windows Server 동영상 녹화
- ✓ 콘솔 접근 통제
- ✓ 우회 접근 통제

작업 결재

- ✓ 접근 권한 및 실행 권한 결재
- ✓ 계정 관리 작업 결재

원장 관리

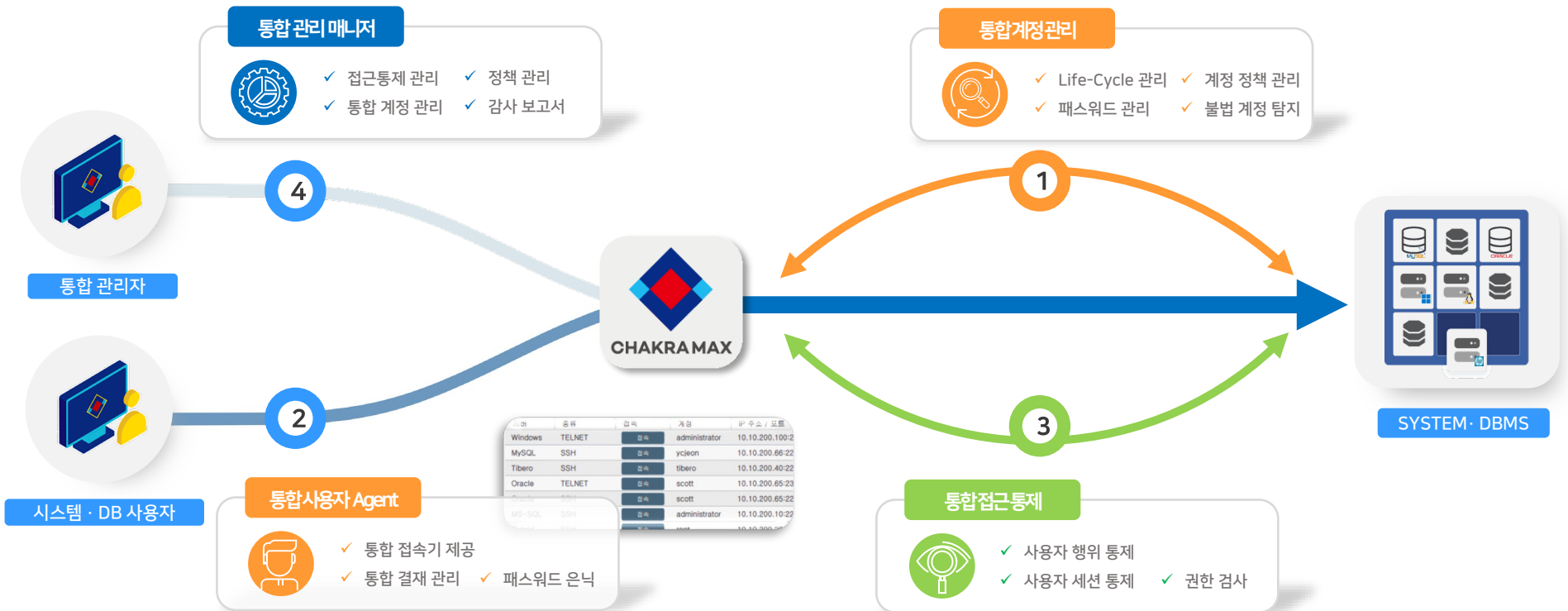
- ✓ 주요 정보의 변경 전/후 데이터 수집
- ✓ 데이터베이스 작업 톨 제한 없이 지원

민감 정보 관리

- ✓ 민감 정보 마스킹
- ✓ 과다 조회 등 이상 행위 감지
- ✓ 민감정보 접속기록 보고서 제공

02 통합 구성 플로우

데이터베이스 · 시스템 계정의 Life-Cycle을 관리하고, 접근통제 모듈과 연계하여 시스템 접속 자동화 기능 제공
또한, 통합 관리 매니저를 통해 하나의 화면에서 일원화된 정책 관리 지원



CHAKRAMAX V4.0
레퍼런스

05

주요 고객사 | 기업



주요 고객사 | 금융

주요 고객사 | 공공



THANK YOU!



Homepage :
<https://www.dsdata.co.kr/>

Address :
경기도 성남시 분당구 판교로255번길 9-22
우림 W-CITY 612-1호

Email :
sales@dsdata.co.kr

Phone :
031-698-2066