

# Chakra Trusted Orange

데이터베이스 보안 솔루션



# 0%부하, 100% 로깅 실시간 감시 보안

## DB 보안 솔루션 구성 방안

### Chakra + Trusted Orange \_ 시스템 부하 없는 사전 통제 및 실시간 보안

DB Tool 표준화를 통한 강력한 논리적 접근 통제 (허용범위,금지범위,결재제약 등)

표준 Tool 이외 불법 접근 차단

데이터베이스 사전 보안과 실시간 보안 시스템을 완벽히 구축

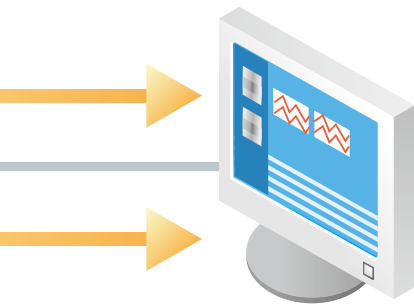
0% Impact, 100% Logging, High Level Protection

### Chakra + DAR \_ 비정형 접근 통제를 위한 하이브리드 구성

다양한 DB Tool 사용 고객사에 효율적 적용

IP Forwarding Mode 를 통한 비정형 접근 제어

DAR을 통한 사용자 인증 및 접속 환경 자동 변경



Web환경  
통합Viewer

TRUSTED

Orange



for ORACLE

사전 접근 통제 및 제어

사전 보안 효과  
대외 이미지 개선  
체계적 보안 업무 수행  
DB관련 작업 표준화  
DB작업의 정당성 입증  
데이터 암호화

도입효과

Chakra

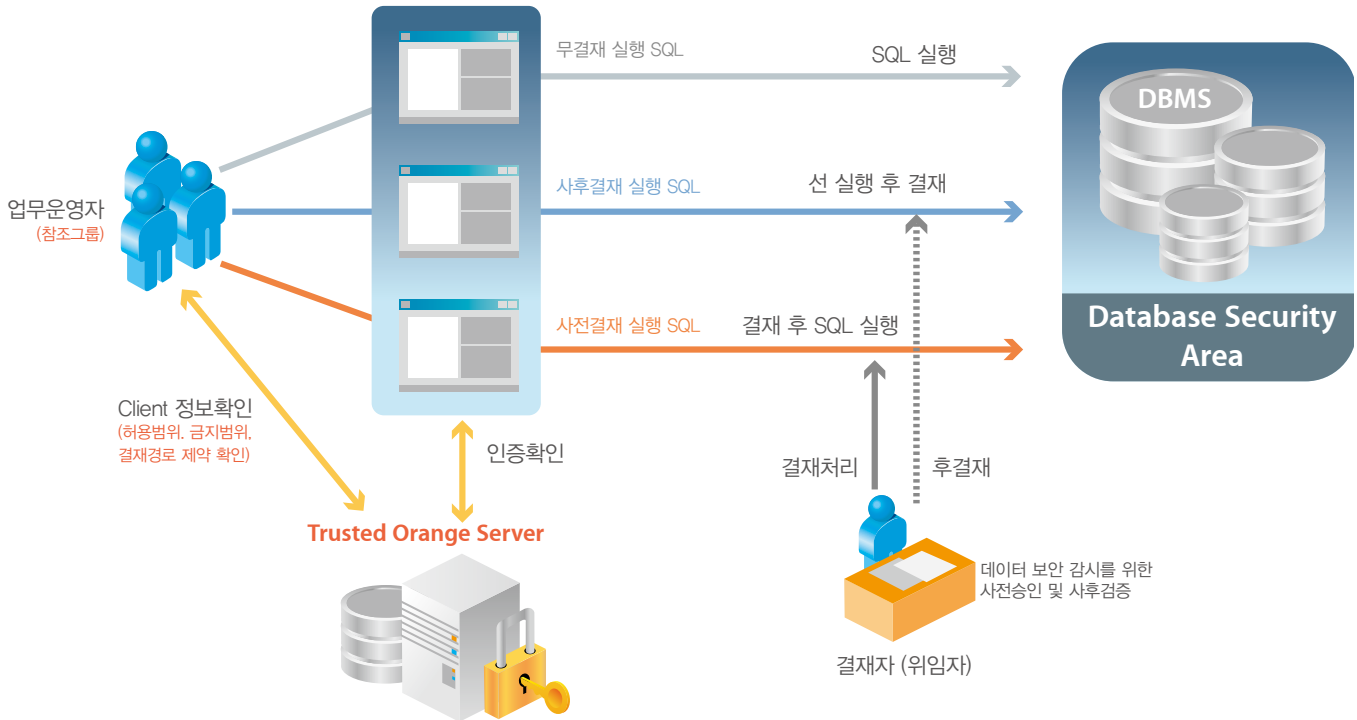


DB 접근 감시 및 차단

부하없는 DB 접근 Logging  
선별적 감시 및 조치  
실시간 감시 및 분석  
실시간 모니터링을 통한 DB 성능 개선  
시스템, App부하 0%  
다양한 로그 분석  
IT compliance 준용 Report

# Trusted Orange

DB 사용자가 고의적인 DB 유출을 목적으로 DB에 접근하거나 또는 DB 작업시 실수로 인하여 문제가 발생하는 것을 사전에 차단하기 위하여 사전에 정의된 보안 정책에 따른 내부 결재를 거친 SQL만 실행 하도록 하는 사전 보안 감시 솔루션 (강력한 논리적 사전 접근 통제)입니다.



- 개인별, 그룹별 권한(허용범위, 금지범위, 결재경로, 결재제약)관리를 통한 강력한 접근 통제
- 개인별 사용자 정보 및 Client 정보 관리를 통한 개인 정보 도용 방지 (다른 PC에서 ID 도용을 통한 작업 사전 제거)
- Orange 기반의 SQL 작성 Tool과 결재 신청 프로세스의 자동 연계를 통해 사전 통제의 효율성, 일관성 제공
- 결재, 개인작업, 그룹공유, 참조, 튜닝 등의 Tree 구조 체계의 User Interface를 제공함으로써 작성 및 결재된 SQL 정보 활용의 효율성 제공
- 타 그룹에서 작성된 SQL 정보, 공유 Tool 정보를 논리적 접근 통제 체계를 통해 제공함으로써 업무 효율성 극대화
- 검증 되지 않은 SQL에 대해 튜닝 요청 프로세스를 통한 최적화 작업으로 업무 생산성 및 DBMS 효율성 극대화
- 결재 프로세스 단계별 통계 정보 및 결과 정보를 다양한 조건으로 검색, 보고서 생성, 출력기능을 제공함으로써 사용자의 업무 처리 지원
- 데이터 암호화 기능 지원으로 DB 보안 강화

# Chakra

접근 제어를 통한 DB 실시간 감시 및 차단, 접근 이력 100% 기록, 기록된 자료의 재분석을 통해 기존 시스템에 부하없이 DB 유출에 대한 모든 위협 요소로부터 중요 정보를 보호합니다.

## 접근 제어 (Protection)

### 1. Alert Policy (Alerting, Denial of Service)

- 기업의 보안 전략 및 업무 수행 절차에 따라 DB에 악영향을 줄 수 있는 접근에 대해 경고 발생, 강제 차단 등의 보안 정책을 설정
- Client Connection, DB/OS Account, Instance, Session, SQL, SQL Result, Action 등 다양한 조건의 경고 발생 및 차단 기능 설정

### 2. Alert Monitor

- 보안 담당자가 설정한 경고 조건에 의해 발생한 Alert 및 상세 내역 확인
- 보안 정책에 의해 차단 기능이 설정된 경고 발생시 자동으로 세션 차단
- 경고 발생시 사전 설정된 관리자 메일이나 SMS로 자동 통보

## 로깅 및 감사 (Audit)

### 1. 데이터베이스(SQL) 로깅 및 감시 정책 관리

- 다양한 보안 정책 수립을 위한 편리한 정책 설정
- Client IP, DB/OS Account, App, SQL Type, 각 시간 조건과 함께 세부 작업 내역 구분 조건 설정

### 2. 서버(Telnet/FTP/RCmd) 로깅 및 감시 정책 관리

- 감시 대상 서버에 대한 Telnet, FTP, RCmd 접근 및 작업 내역 감시를 위한 로깅 및 감시 정책 설정
- Server Name, IP, Port, Output Logging, 로그 자료 백업/압축 등의 환경 설정
- 360° 전방위 감시 및 로깅(SSh, Telnet 작업 내역 기록)

## 로그 모니터링 (Monitoring & Report)

### 1. Session Monitoring

- 감시 대상 DB에 연결되어 있는 세션들에 대한 다양한 상태 정보를 일괄적으로 모니터링
- 각 세션에 대한 Client IP, Connect Time, DB User, App, SQL Count 등의 정보 제공
- 수행된 SQL의 Type, Text, 응답시간, Return Row, Transaction Usage 등의 정보 제공

### 2. SQL Monitoring

- 현재 실행 중인 SQL에 대한 실시간 목록 및 상세 내역 제공  
(SQL 내용, 성능 정보, 세션 정보, Client 정보 등)
- Orange Tool과 연계하여 SQL에 대한 상세한 Tracing 가능

### 3. Report Builder

- Report Builder를 통해 DB별, Host별 보안 관점 별로 다양한 검색 조건에 의한 보고서 생성
- 검색 조건에 의해 생성된 Report는 HTML, PDF 등 다양한 포맷으로 변환 제공

### 4. Telnet/FTP/Rcmd Log Monitoring

- 감시 대상 서버로 접속한 모든 작업자의 Telnet, FTP, RCmd 로그를 다양한 검색 조건으로 감시
- Client IP, 사용 명령어, 사용 시간, 결과 정보 등의 상세 정보 제공

## 접근 분석 (Analysis & Reaction)

### 1.Trend Analyzer (추세 분석 및 예측)

- 감시 대상 DBMS의 Server Time, Session Count, Transaction Usage, Return Row 등의 추이분석 그래프 제공
- 패턴에 대한 임계치 설정을 통한 경고 발생 및 추이 분석을 통한 사전 예보 서비스

### 2.Log Analyzer (Alert, SQL, Server Log 분석)

- 감시 대상 DB에 대한 로그 분석기로 문제 발생 시점의 추이 분석 및 추적
- 다양한 조건의 검색 기능을 제공하며, 해당 SQL에 대한 튜닝을 위해 Plan Tool 연계(Rich Client시) 기능지원

## 사용자 인증 관리

### 1. 사용자 정보 관리

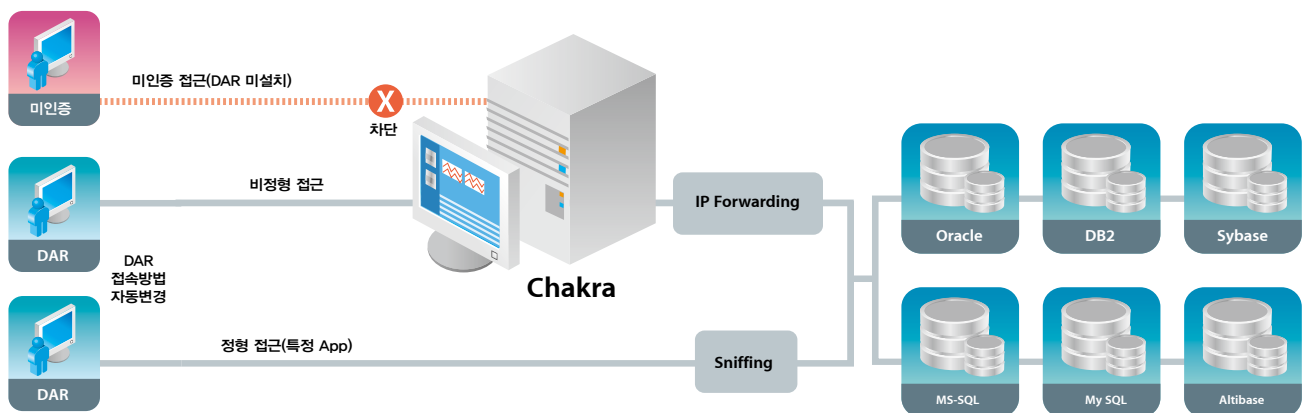
- 사용자 기본 정보 (ID, Password, IP, 유효기간 등) 및 접속 가능 DBMS 정보 등록 관리
- Client의 DAR과 연동하여 사용자 인증(암호, IP, 유효기간) 후 권한 있는 DBMS에 대해 접속 허용

### 2.DAR 정책 관리

- 정형, 비정형 접속 Tool을 등록 관리하여 Application별 접속 허용, 차단 정책 관리
- 감시 대상 DBMS별 Routing 정책 관리 및 Chakra 서버 장애에 따른 Fail-Over 정책 관리

# DAR (Dynamic Access Router)

데이터베이스에 대한 정형 접속과 비정형 접속을 구분하여 접속 환경을 자동으로 변경합니다. DB 사용자 pc에 설치된 DAR 에이전트를 통한 사용자 인증 작업 후 정형 접속은 DBMS로 직접 라우팅하고 비정형 접속은 샤크라 서버를 통한 IP Forwarding 방식으로 DB에 접근하도록 접속 환경을 자동으로 변경하여 스니핑 방식과 Gateway 방식을 동시에 구성합니다.



- ① **사용자 정보 등록** : Chakra 사용자 관리 화면을 통해 ID, Password, 사용자 정보를 등록 (변경사항 및 이력 관리)
- ② **인증된 사용자만 DB 접속** : Chakra 관리 화면에서 설정된 DAR 정책은 암호화 되어 Client에 자동 배포  
DAR 미 설치 접근은 Chakra에 의해 접근 차단 됨
- ③ **접속 환경 자동 변경** : 사전 정의된 Application에 의한 정형 접속은 DB로 직접 연결 하며, 비 정형 접속은 Chakra 서버를 통한 IP Forwarding 방식으로 DB에 접근 할 수 있도록 접속 환경을 자동으로 변경 함

- 사용자의 환경 변화 없이 DB접근을 자동으로 Gateway 방식으로 전환
- DAR 인증을 통한 사용자관리와 Logging 자료의 신뢰도 향상
- 감시 대상 DB에 대한 사전 접근 통제 (사용자 툴, IP대역, 프로토콜 등의 조건으로)
- 기업 IT 요구사항에 맞는 다양한 아키텍처 구성 가능 (이중화 또는 Load Balancing 기능 제공)

### 국내 최대 고객사 도입, 운영 및 해외 수출 (한국·일본 시장 점유 1위, 영국·독일·호주 등 10 여개 국 수출)

#### IT Compliance 준용을 위한 최적의 보안 솔루션

(정형/비정형, GW/스니핑 통합관리 및 Result data를 포함한 사용자 접근 정보 로깅)

- 국내: 개인정보보호법, 금융감독원지침, 증권거래법, 회계감사법, 전자금융 거래법, 정보통신망 이용 촉진 등에 관한 법률(정보통신부) 등
- 해외: SOx, HIPPA, GLBA, PCI, 신 바젤 협약, EU 지침 등

#### 국내 최초 대용량 Hybrid 방식 실 적용 솔루션

- 표준 Tool을 통한 정형 접근은 Sniffing 방식으로 감시 및 로깅 : 무 부하 안정성 보장
- 비표준화 Tool에 의한 비정형 접근은 Gateway 방식으로 실시간 감시, 차단 및 로깅

#### 국내 대다수의 상용 DB (Oracle, DB2, Sybase, MS-SQL, MySQL, Altibase등 ) 적용 및 실 납품

#### 이종 DBMS 통합 관리 및 모니터링 솔루션 (N:M:1)

#### 전 방위 100% 로깅 구현으로 DB 보안 감시 영역 확대

- 인가된 직원이 서버Side (콘솔 or Telnet)에서 직접 작업한 내용과 그 실행 내역 감시 로깅

#### SQL 로깅 무결성 및 제품 안정화 실현 (대형 고객사 4년 이상 실 적용 운영 중)

#### 품질평가 및 공인인증

- CC인증 평가 계약, 신기술인증(과학기술부), Good Software(정보통신부), 조달청 우수제품
- 신소프트웨어대상(정보통신부), 다산기술상(한국경제신문) 하이서울브랜드(서울산업통상진흥원)

#### 특허 (제0481130호)

"데이터베이스 시스템에 접속하지 않고 데이터베이스 시스템을 모니터링 하는 방법"

대상 DBMS : Oracle, DB2, MS-SQL, Sybase, MySQL, Altibase 등  
 OS : Windows, Unix, Linux  
 H/W : 3.0Ghz Xeon CPU \* 2 EA 이상  
 4GB Main Memory 이상  
 SQL Capture : 1~10,000/sec  
 Disc Capacities : 수십 KB ~ 20GB/Day (운영시스템의 TPS나 로깅 정책에 따라 달라질 수 있음)