WAREVALLEY

DBMS

SOLUTION

PARK

www.warevalley.com

WARE VALLEY

01

데이터베이스 내부통제는 어떻게 하고 있습니까?

CHAKRA MAX

DB·SYSTEM 접근제어 및 작업결재 솔루션

Chakra Max V3

Chakra Max는 고객의 데이터베이스를 책임집니다. Chakra Max는 기업의 중요 자산인 데이터베이스를 보호하는 데이터베이스 보안 솔루션입니다.
고객의 민감정보를 보호하고 기업의 중요한 자산을 보호하기 위해 Chakra Max를 사용해 보십시오.
데이터베이스와 서버의 접근제어와 계정관리, 권한통제까지 하나의 솔루션으로 보안구현이 가능합니다. On-Premise와 Cloud에 이르는 모든 민감 정보에 접근한 감사 이력 제공, 접근 권한 통제, 안전한 계정관리와 로그 관리로 귀사가 법규를 준수할 수 있도록 돕겠습니다.

Why Chakra Max

가트너(Gartner)가 인정한 정보보안 솔루션
세계적인 IT 리서치 기관인 가트너(Gartner)는 데이터 감사와 통제(DCAP), 리스크 관리, 데이터 마스킹 까지 다양한 시장 분석 보고서에서 Chakra Max를 언급하고 있습니다.
이러한 평가로 웨어밸리는 2012년부터 9년 연속 주요 정보보안 벤더로 선정되어 아시아뿐만 아니라 글로벌 데이터 보안 기업으로 인정받고 있습니다.

Chakra Max KEY FEATURES

접근제어

사용자의 세션 속성, 실행된 SQL과 응답 정보, 서버에서 수행된 명령과 결과 등 데이터베이스 혹은 서버의 작업 이력을 기록하고 부적절한 접근을 통제할 수 있습니다. 경보, 차단, SQL 제어, 마스킹, 작업결재, 어플리케이션 통제, 우회접속 감지와 변경 전/후 데이터 수집기능까지 현장에서 필요한 다양한 접근제어 기능을 제공합니다.

감사 및 로깅

데이터베이스와 서버에서 이뤄지는 다양한 작업 이력을 누락 없이 육하원칙에 맞게 감사로그로 제공합니다. 저장된 로그는 시스템의 자체 보안 기능으로 훼손되지 않아 무결성이 보장됩니다. 예상할 수 없는 손실을 막기 위해 로그 저장소의 이중화를 지원하며 자동화된 헬스체크를 통해 감사 기능에 필요한 리소스 이슈 파악이 가능합니다.

실용적인 데이터 마스킹

데이터베이스와 시스템의 입/출력 흐름을 분석하여 중요 정보가 노출되는 것을 실효적으로 차단합니다. 분석 과정에서 주민번호나 계좌번호와 같은 민감한 정보를 자동으로 인지하며 정책에 따라 마스킹을 수행할 수도 있습니다. 마스킹 룰을 회피하기 위해 사용자 함수나 문자열을 조합하는 쿼리 조작 시도는 지능화된 인지 기능으로 경보와 함께 자동 차단됩니다. 정책 적용 과정에서 생기는 실무 요건의 수렴을 위해 마스킹 해제 결재, 예외 사용자 지정, 지정된 건수의 제한적 해제 등 실용적 기능도 탑재하고 있습니다.

강력한 대용량 데이터 유출 통제

강력한 분석 기능으로 악의적인 정보 유출 목적의 대량 데이터 획득 시도를 감지할 수 있습니다.

- SQL 응답시간을 기반으로 감지
- 네트워크 패킷 전송량을 기반으로 감지
- 조회 건수가 임계치를 초과하는 경우 통제
- 일별 통계를 기초로 평상 시 조회 건수를 초과하는 경우 자동 감지

다양한 접근경로의 통제

중요 정보로의 접근 경로가 다양하다는 것은 보안 취약점으로 지적될 수 있습니다. 실효적 보안을 위해서는 각 경로의 특성을 파악하여 적합한 보안 구성과 기능을 지원해야 합니다. 서버 콘솔 또는 시리얼 통신을 이용한 작업은 서버 보안 에이전트로 통제합니다. 공통 계정을 이용하는 WAS 작업에 대해 "실제 사용자"를 에이전트로 확인할 수 있습니다. 보안 게이트웨이를 통하지 않은 우회접속을 서버 보안 에이전트로 감지하고 차단합니다. 데이터베이스 로컬 접속을 통한 작업의 감사와 통제를 위해 Software TAP과 DB Local Agent를 제공합니다.

데이터 작업의 결재

데이터베이스에서 수행되는 중요 정보의 변경이나 조회 작업에 대해 전문화된 결재 시스템을 제공합니다. 이는 작업의 신청과 승인 그리고 이어지는 권한 부여와 실행, 그리고 감사 이력 확보에 이르는 일련의 프로세스를 의미 합니다. 데이터 작업 결재라고 불리는 이 기능은 가장 상위 레벨의 권한제어 기능으로 고도의 보안을 요구하는 고객에게 선택되는 기능입니다. 다양한 결재 라인 관리가 가능하고, 사전 및 사후 결재, 위임결재, 기간별 자동 경로 변경과 메일 결재 등 업계 최고의 편의 기능들이 제공됩니다. 데이터 베이스 작업뿐만 아니라 서버 작업까지 지원 범위가 확장되어 OS 명령 실행까지 결재 통제가 가능합니다. 데이터베이스와 서버의 접근 및 명령어 실행에 대해 기안자와 결재자를 분리한 제3자 실행 결재기능을 지원합니다.

실용적인 빌트인 보안 정책

다년간 구축 경험을 토대로 얻은 현업의 보안 요구사항을 40여개 빌트인 정책으로 제공합니다. 현장의 운영 데이터를 토대로 통계를 자동 생성하고 이를 기반으로 이상징후를 탐지할 수 있습니다. 대표적인 정책들로, 평소 보다 잦은 접속 또는 정보 감지, 갑자기 증가된 SQL 오류 또는 조회 건수 폭증을 감지합니다. 이 밖에도 Where 조건이 없이 실행되는 쿼리를 인지하고 통제할 수 있으며 DB 접속 프로 그램의 무결성을 검사하여 변조를 통제할 수 있습니다. 평균적인 네트워크 트래픽을 감안한 변경 추이도 정책화가 가능합니다.

EYES ON YOUR DB

사용자 계정과 패스워드 관리

보다 견고한 정보보안을 위해서는 데이터 접근에 필요한 사용자 계정의 철저한 관리가 필수적입니다. Chakra Max는 계정의 권한, 유효기간, 패스워드 자동변경 등 일련의 계정관리 기능을 함께 제공 합니다. 운영체제와 더불어 데이터베이스의 계정과 권한까지 단일 인터페이스로 관리가 가능하고 접근제어 정책과 연계를 지원합니다.

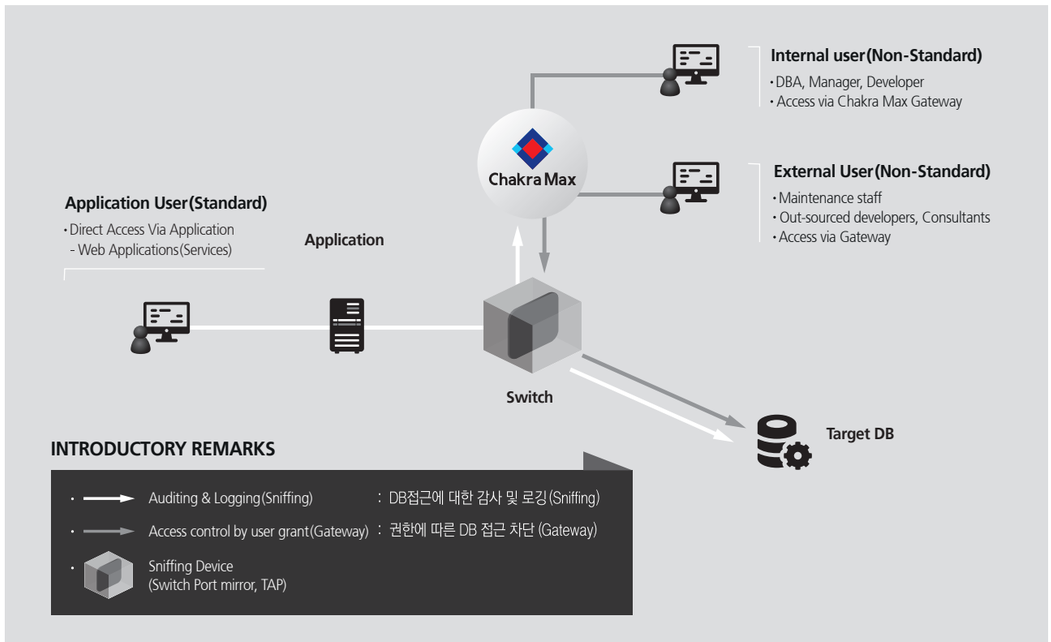
강력해진 서버 접근제어

서버 접근제어 기능이 크게 향상되었습니다. 네트워크를 경유하지 않는 로컬 작업을 포함하여 역할 기반의 통제 와 강력한 명령어 통제 기능을 제공합니다. 특히 실행파일의 악성코드 감염 또는 악의적인 변조를 차단하고 경보와 사용자가 정의한 사후조치를 지원합니다. 원격 데스크톱을 통한 원격 작업에 대한 접근 및 프로그램 통제, 작업을 동영상으로 녹화하여 감사로그로 저장합니다. 서버 접근제어와 DB 접근제어를 이원화시켜 병행 운영 해야 했던 현재의 관리 체계가 Chakra Max로 일원화될 수 있습니다.

클라우드 환경 지원

IT 인프라의 클라우드 마이그레이션이라는 세계적인 추세에 맞춰 KT, AWS, Azure, NTT CloudN을 비롯한 다양한 퍼블릭 클라우드 환경을 지원하며 많은 레퍼런스를 갖고 있습니다.
간편하고 빠른 구축으로 데이터베이스와 애플리케이션의 배치 확장을 대응할 수 있습니다.

Chakra Max FLOW



Chakra Max 국내·외 컴플라이언스 준수

Chakra Max는 기업의 정보보호 활동에서 발생할 수 있는 여러 법률적 문제 식별과 리스크 최소화를 위한 다양한 규정의 준수를 가능하게 합니다.

국내	개인정보보호법, 정보통신망법, 개인정보영향평가(PIA), 개인정보보호 관리체계 인증(PIMS), 정보보호관리체계 인증(ISMS), 데이터보안인증(DQC-S), 클라우드서비스 보안인증제(CSAP), IT회계감사
해외	General Data Protection Regulation(GDPR), PCI DSS, Sarbanes-Oxley Act(SOX), ISO/IEC 27001, Health Insurance Portability and Accountability Act(HIPAA), Basel II, Federal Information Security Modernization Act(FISMA)

Chakra Max SUPPORT SPEC

Chakra Max는 다양한 정보 저장소에 대한 감사와 접근제어를 지원합니다.
Windows, LINUX, UNIX 운영시스템부터 IBM AS/400과 메인프레임까지 지원하며 관계형 데이터베이스뿐만 아니라 빅데이터 처리를 지원하는 NoSQL 데이터베이스까지 총 30 종류의 이기종 데이터베이스를 동시에 보호할 수 있습니다.

SYSTEM	SSH, (S)FTP, Mainframe TN3270, AS/400 TN5250, Telnet, rcmd, rlogin, Windows 원격 데스크톱
DATABASE	Oracle, Microsoft SQL Server, IBM DB2, Sybase ASE/IQ, MySQL, MariaDB, Informix, Teradata, PostgreSQL, Netezza, Greenplum, SAP HANA Database, Tibero, Altibase, Cubrid, Symfoware, KAIROS, PetaSQL, Dameng DM7, SunDB, mongoDB, FireBird, Influx, Vertica, Greenplum, Amazon Aurora, Amazon, Redshift, CouchDB

Chakra Max CONFIGURE & SPEC

구성 방식

다양한 경로의 접근 패턴을 빈틈없이 통제하기 위해 여러 가지 구성방식과 옵션을 제공합니다.

Sniffing mode	데이터베이스와 서버에 부하를 주지 않고 접근이력을 수집합니다.
Gateway mode	Chakra Max 게이트웨이 서버를 통해 강력한 접근제어를 수행하는 방식입니다. 사용자 인증과 이벤트 통지 및 결재 기능 활용을 위해 PC Agent 프로그램 연동을 선택할 수 있습니다.
Hybrid mode	정형화된 접근에 대하여 운영 성능을 고려한 Sniffing 방식을 적용하고, 적극적인 통제가 필요한 내부자에 대해서는 Gateway 방식을 병행하는 동시 운영 구성입니다.
HA mode	누락 없는 감사 로그 확보와 접근 통제의 연속성을 고려한 이중화 구성입니다. Active-Standby, Active-Active 뿐만 아니라 감사로그와 보안 정책의 이중화까지 지원합니다.

WAS Agent	WAS를 통한 데이터 접근에 대하여 실제 사용자(End-User)의 신원을 식별하고 접근 통제 기능을 제공합니다.
Server Agent	서버 보안 에이전트를 통해 다음 기능을 지원합니다. · 콘솔 또는 시리얼 통신을 이용한 서버작업 통제 · Windows 원격 데스크톱을 이용한 서버작업 감시, 통제 · 보안 Gateway를 경유하지 않는 우회접속 통제 · 우회된 경로(Path) 추적 기능 제공
WAC Agent	RDP를 통한 서버 접속 작업에 대해 동영상 녹화를 통한 보안감사 기능, 실행프로그램 및 명령어 수집, 실행 통제 기능을 제공합니다.