Database Risk Management

기밀성, 무결성, 가용성을 위한
데이터베이스 보안 및 감사

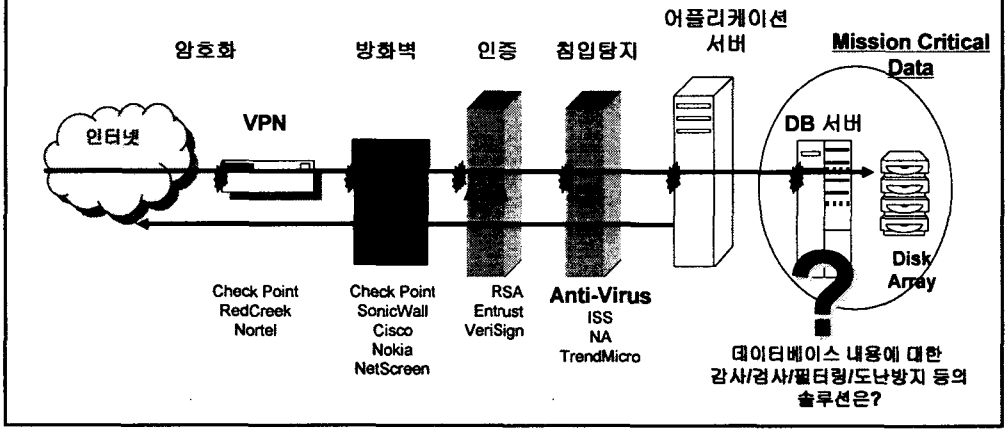
㈜잇츠커널

목차

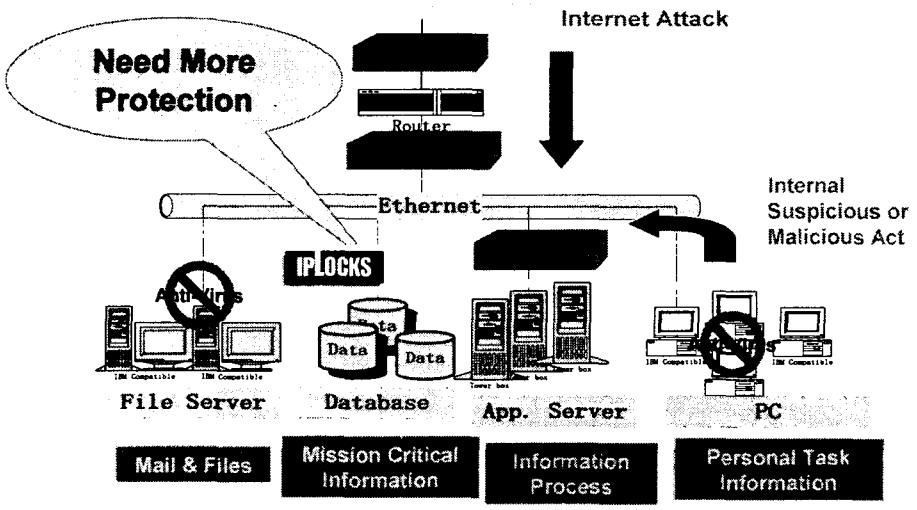
- ❑ DB 보안의 필요성
- ❑ DB 보안 솔루션
- ❑ DB 보안 시장
- ❑ 기대 효과

DB 보안의 필요성 - 현재의 보안 체계

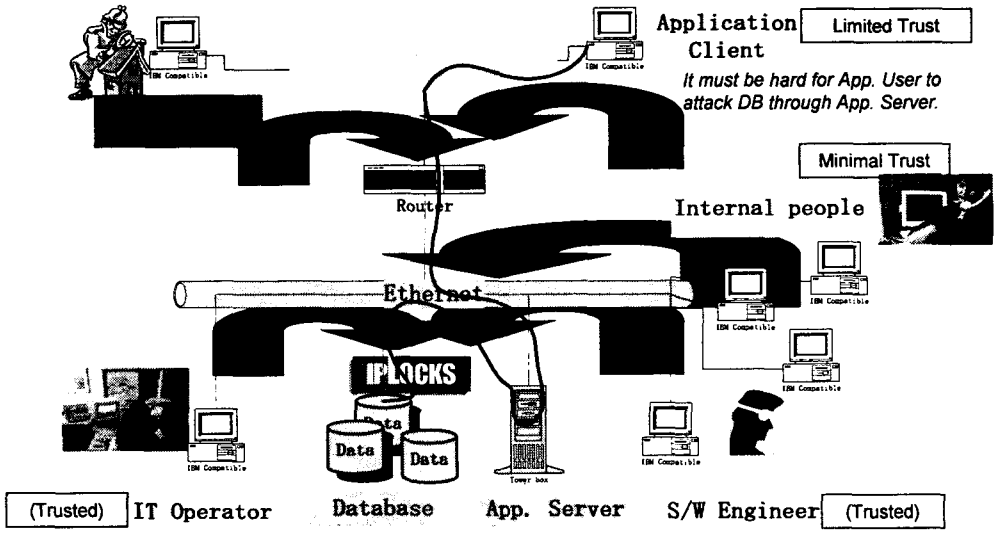
❑ 대부분의 조직이 외부위협에는 비교적 잘 대응하고 있으나,
정보 보호의 궁극적 대상인 데이터에 대한 방어는 미약한 편임



DB 보안의 필요성 – Who's Viewing Your Data?



DB 보안의 필요성 – DB 위험



DB 보안의 필요성

해커 Malware

- ❑ 알려지지 않은 취약성 또는 패치되지 않은 시스템
- ❑ 트로이 목마 프로그램을 통한 루트 권한 획득
- ❑ 발견되지 않은 바이러스에 의한 레코드 삭제 및 오염

HW / SW 시스템 중단

- ❑ 타 시스템으로부터 잘못된 데이터 유입 또는 파일 임포트
- ❑ 하드웨어 또는 소프트웨어의 버그 또는 결함
- ❑ 분산 **DB**에서의 ***spidering corruption(cascading updates or deletes)***
- ❑ 서로 다른 어플리케이션 모듈에서 사용되는 일관성 없는 데이터
- ❑ 비즈니스 협력 파트너 파일에 의해 오염된 데이터

내부 오용, 사기 / 절도

- ❑ 불만있는 직원의 중요 데이터 삭제
- ❑ 악의있는 내부인의 자금 또는 기밀 데이터 절취
- ❑ 보안정책 또는 타 업무 규칙 위반
- ❑ **Mal-administration(DBA** 문제**)**
- ❑ 부정 트랜잭션 또는 가상 트랜잭션 입력

사용자 오류

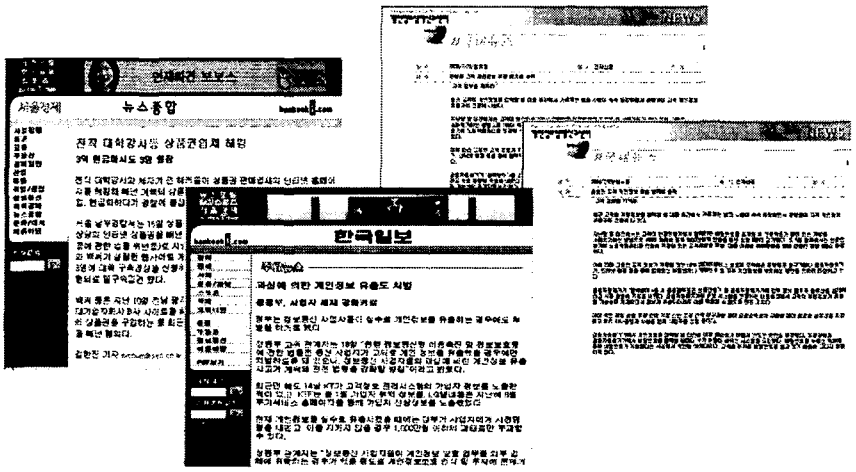
- ❑ 잘못 입력한 값
- ❑ 관리 또는 운영 오류

외부위협 30%

내부위협 70%

DB 보안의 필요성 – DB 보안의 현주소

- 해킹의 목적은 데이터
- 금융권, 의료계, e-Business의 주요 고객 데이터 유출의 심각성 대두
- 외부위협보다 내부 위협이 상대적으로 더 심각



DB 보안의 필요성 – 현실적 배경

- 시스템 중지로 인한 영향
  - 재무 손실
  - 기업 명성
  - 기업 생산성
  - 법적 규제

운영 중단으로 인한 재무적 영향의 업종별 평균(미국)

Retail Brokerage	$6.45 M/h
Credit Card Sales Authorization	$2.6 M/h
Infomercial/800# promotion	$199,500/h
Catalog Sales Centers	$90,000/h
Airline Reservations	$89,500/h
ATM Service Fee	$14,500/h

"CSI study는 외부 위협에 의한 피해액 $57K는 내부 위협 피해액 $2.7M이 훨씬 많다고 발표했다."

2001년 8월 유나이티드 에어라인사는 시카고발 볼베이행 왕복티켓을 $140에 발매(원래는 2000)했다. 결과적으로 $223,200의 매출 감소를 초래했다. 부정확한 요금이 요율DB에 리스팅된 것이 원인이었으며 8개월 동안 3번이나 이런 On-line상의 오류가 발생하였다.

IDG보고에 의하면 27%의 은행 및 금융기관에 종사하는 데이터베이스 소프트웨어 개발자들은 2001년에 Virus, Human error 그리고 비인가된 무단침입에 의해 그들의 데이터베이스가 손상되거나 삭제된 경험이 있다고 함.

DB 보안의 필요성 – 컴퓨터 범죄의 비용

ITS KERNEL

IPLOCKS

모니터링/탐지 활동
- 주요 정보 절취/유출
- 데이터 손상, 악의적 변경
- 정보보호 규칙 위반
- 정보보호 취약점

48개월 동안 컴퓨터 범죄 및 정보보호 규칙 위반으로 발생한 비용 총계

2003년 응답자의 75%가 재무적인 손실을 경험한 것으로 조사되었고 47%만 정량화 가능한 것임

	Lowest Reported				Highestest Reported				Average Losses				Total Annual Losses			
	2000	2001	2002	2003	2000	2001	2002	2003	2000	2001	2002	2003	2000	2001	2002	2003
Theft of proprietary info.	$1K	$100	$1K	$2K	$25	$50M	$50M	$35M	$3,032,818	$4,447,900	$6,571,000	$2,699,842	$66,708,000	$151,230,100	$170,827,000	$70,195,900
Sabotage of data of networks	1K	100	1K	500	15M	3M	10M	2M	969,577	199,350	541,000	214,521	27,148,000	5,183,100	15,134,000	5,148,500
Telecom eavesdropping	200	1K	5K	1K	500K	500K	5M	50K	66,080	55,375	1,205,000	15,200	991,200	886,000	346,000	76,000
System penetration by outsider	1K	100	1K	100	5M	10M	5M	1M	244,965	453,967	226,000	56,212	7,104,000	19,066,600	13,055,000	2,754,400
Insider abuse of net access	240	100	1K	100	15M	10M	10M	6M	307,524	357,160	536,000	135,255	27,984,740	35,001,650	50,099,000	11,767,200
Financial fraud	500	500	1K	1K	21M	40M	50M	4M	1,646,941	4,420,738	4,632,000	328,594	55,996,000	92,935,500	115,753,000	10,186,400
Denial of service	1K	100	1K	500	5M	2M	50M	60M	108,717	122,389	297,000	1,427,028	8,247,500	4,283,600	18,370,500	65,643,300
Virus	100	100	1K	40	10M	20M	9M	6M	180,092	243,835	283,000	199,871	29,171,700	45,288,150	49,979,000	27,382,340
Unauthorized insider access	1K	1K	2K	100	20M	5M	1.5M	100K	1,124,725	275,636	30,000	31,254	22,554,500	6,064,000	4,503,000	406,300
Telecom fraud	1K	500	1K	100	3M	6M	100K	250K	212,000	502,278	22,000	50,107	4,028,000	9,041,000	6,015,000	701,500
Active wiretapping	1M	0	0	5K	5M	0	0	700K	5M	0	0	352,500	5,000,000	0	0	705,000
Laptop theft	500	1K	1K	2400	1.2M	2M	1M	2M	58,794	61,881	89,000	47,107	10,404,300	8,849,000	11,766,500	6,830,500
CSI/FBI 2003 Computer Crime and Security Survey											Total Annual Losses		265,337,990	377,828,700	455,848,000	201,797,340

Source: Computer Security Institute

DB 보안의 필요성 - DB 보안의 허점 및 해결방안

ITS KERNEL

DB 보안의 허점

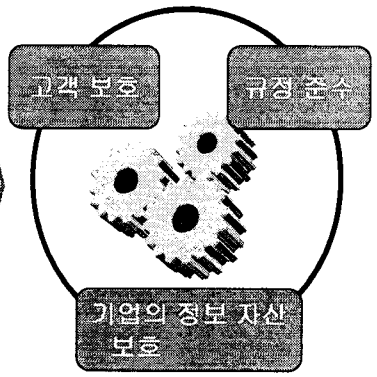
- 운영 시간 경과에 따라 DB의 무결성 문제 발생 가능
- 어플리케이션 변경으로 인한 보안 누수 발생

DB 보안 원칙

기초적인 보안 항목
- 관리와 운영 직무 분리
- 접근 권한 상세화 및 최소화
- 사용자 계정 보안 관리
- 효과적인 감사

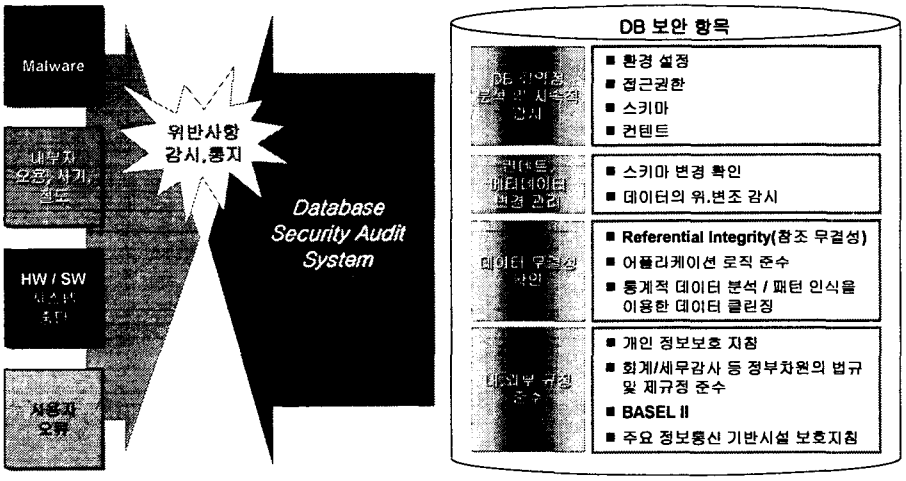
효과적인 모니터링/대응
- 감사 자동화
- 감시활동 유형별 감사 (접근권한/스키마/컨텐트 무결성/데이터 사용 패턴)
- 위반사항 자동 통지 및 대응

효과적인 법규/규제 준수
- 개인정보보호
- 주요 정보통신 기반시설 보호
- **BASEL II**



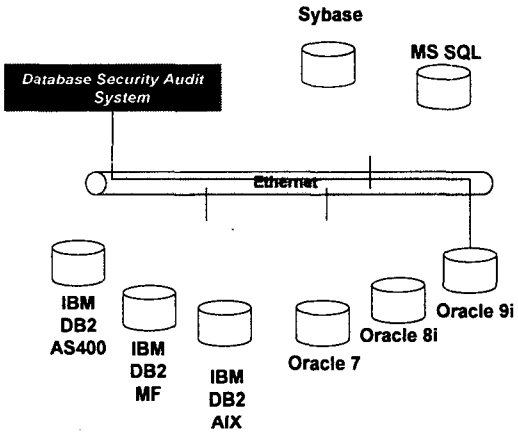
DB 보안 솔루션 역할

- 고의적 혹은 실수에 의한 데이터 및 시스템의 불법적인 공개(노출), 변조, 파괴, 지체로부터 자산이나 정보를 보호하는 것
- 궁극적으로 정보 및 통신시스템에서 저장 및 유통되는 정보의 기밀성(Confidentiality) 과 무결성(Integrity) 을 보장하여 시스템의 가용성(Availability)을 향상

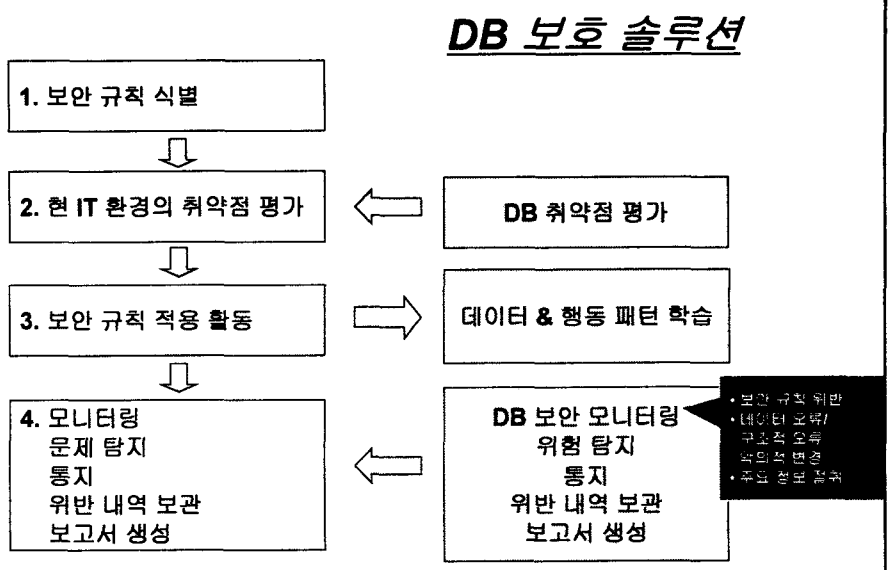


DB 보안 솔루션 - 데이터베이스 위협 파악 및 감시 솔루션

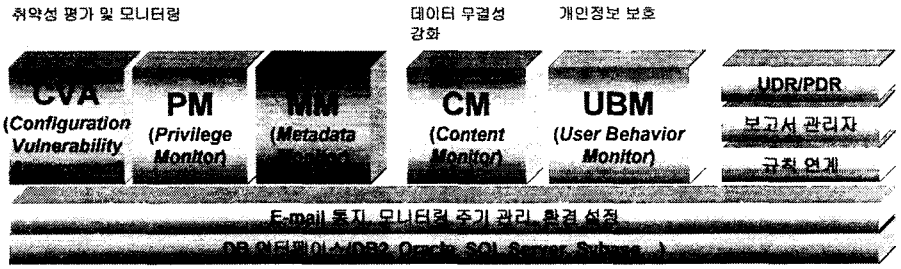
- 취약성 평가 및 지속적인 모니터링
  - DB 환경 설정 및 변경
  - 모범사례 적용 및 개발
  - 접근 권한 및 메타데이터 변경 모니터링
- 데이터 무결성 강화
  - 통계 알고리듬 적용
  - 데이터 변질/손상 탐지
  - 데이터 변경 로그 기록
  - 업무규칙 준수 검증
- 개인정보보호
  - 데이터 사용 패턴 분석
  - 의심스러운 접근 파악
    - ✓ 오사용 탐지
- 집중화된 DB 모니터링
  - 공유 데이터와 네트워크 상의 DB 구조로 인한 연쇄적 손상 발생 이전에 변칙 데이터 탐지
  - 집중화된 모니터링으로 ROI 증대
- **External and Non-intrusive**
  - DB 서버의 변경이나 추가 모듈 설치가 필요 없음.
  - 설치가 용이하고 위험이 없음.



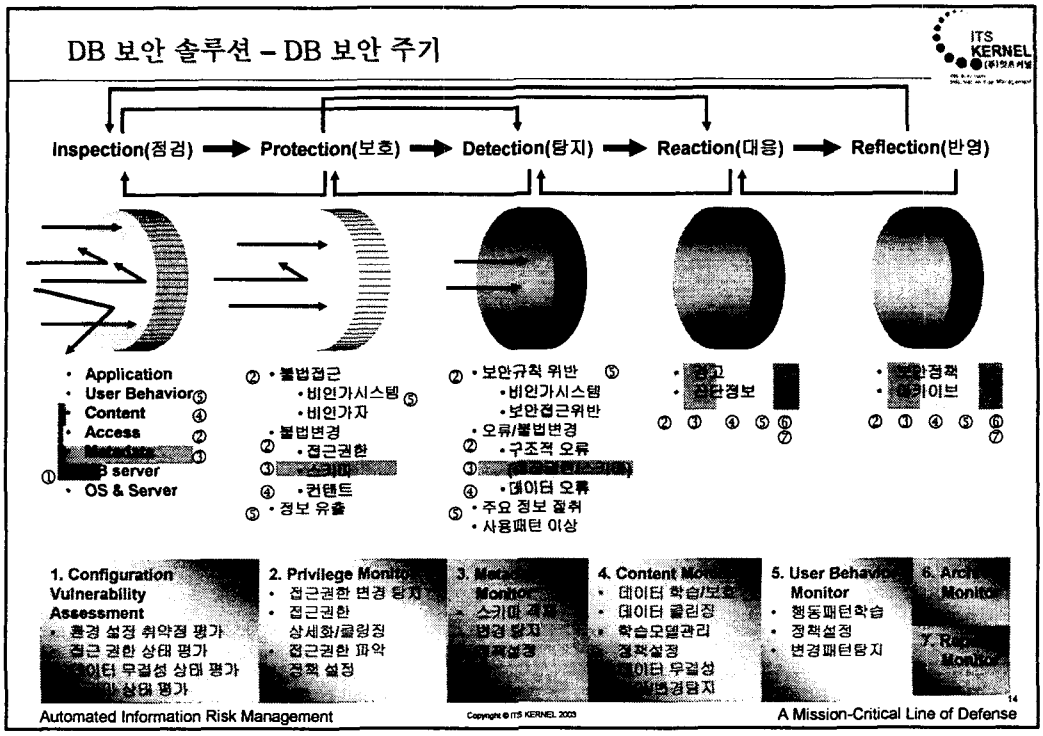
DB 보안 솔루션 – 보안 절차

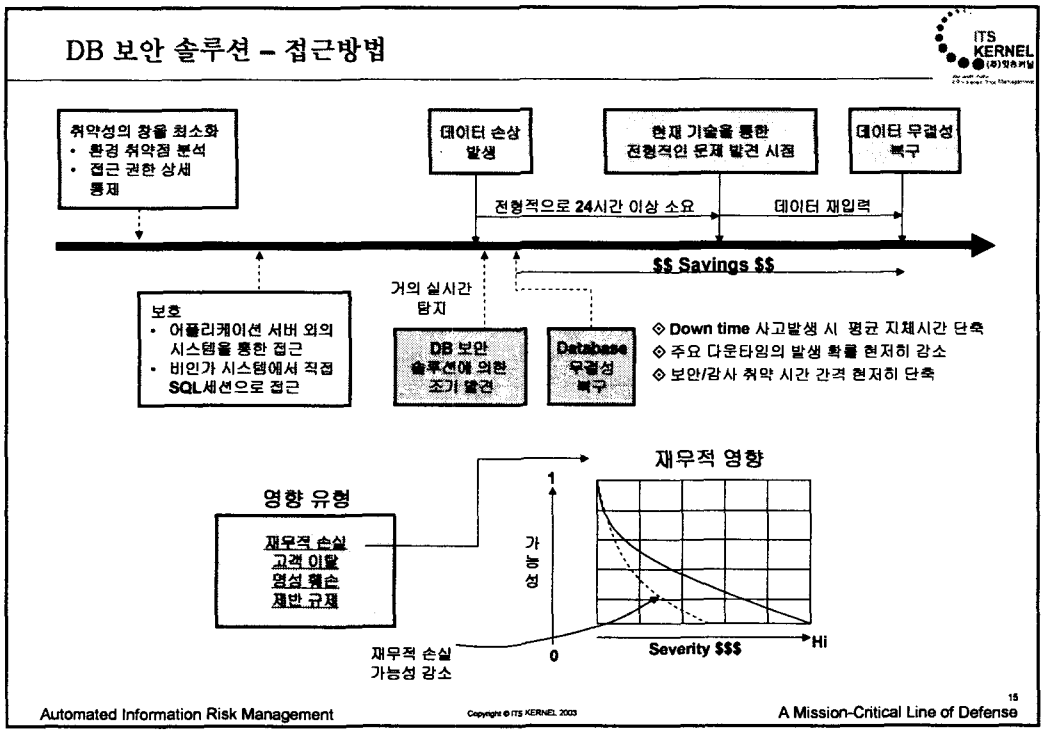


DB 보안 솔루션 –아키텍처



Configuration Vulnerability Assessment	취약성이 존재하는 환경 설정 파악
Privilege Monitor	접근 권한 및 역할의 변경 모니터링 및 통지
Metadata Monitor	스키마/테이블/컴포넌트의 변경 통지
Content Monitor	데이터 가용성/무결성/보안상의 문제를 자동 탐지
User Behavior Monitor	의심스러운 데이터 접근과 시스템 자원 패턴 탐지
규칙 연계	모듈 간의 정책 연관성을 정의하여 기존 정책의 위반사항 탐지 후 자동으로 연계 정책 수행
보고서 관리자	경고 메시지를 유연하게 보고서로 생성
사용자 정의 규칙(UDR)	업무에 맞는 정보보호 규칙을 추가
사전 정의 규칙(PDR)	업무 규칙에 맞는 모범 사례의 적용 및 모니터링


DB 보안 솔루션 – DB 보안 주기
ITS KERNEL
Inspection(점검)
Protection(보호)
Detection(탐지)
Reaction(대응)
Reflection(반영)
• Application
• User Behavior
• Content
• Access
• OS & Server
② • 불법접근
• 비인가시스템
• 비인가자
• 불법변경
② • 접근권한
④ • 컨텐트
⑤ • 정보 유출
② • 보안규칙 위반
• 비인가시스템
• 보안접근위반
• 오류/불법변경
② • 구조적 오류
④ • 데이터 오류
⑤ • 주요 정보 접취
• 사용패턴 이상
1. Configuration Vulnerability Assessment
• 환경 설정 취약점 평가
접근 권한 상태 평가
2. Privilege Monitor
• 접근권한 변경 탐지
• 접근권한 상세화/클링징
• 접근권한 파악
정책 설정
4. Content Mon
• 데이터 학습/보호
• 데이터 클리징
• 학습모델관리
정책설정
5. User Behavior Monitor
• 행동패턴학습
• 정책설정
• 변경패턴탐지
Automated Information Risk Management
A Mission-Critical Line of Defense


DB 보안 솔루션 – 접근방법
ITS KERNEL
취약성의 창을 최소화
• 환경 취약점 분석
• 접근 권한 상세 통제
데이터 손상 발생
현재 기술을 통한 전형적인 문제 발견 시점
데이터 무결성 복구
전형적으로 24시간 이상 소요
데이터 재입력
$$ Savings $$
보호
• 어플리케이션 서버 외의 시스템을 통한 접근
• 비인가 시스템에서 직접 SQL세션으로 접근
거의 실시간 탐지
DB 보안 솔루션에 의한 조기 탐지
Database 무결성 복구
◇ Down time 사고발생 시 평균 지체시간 단축
◇ 주요 다운타임의 발생 확률 현저히 감소
◇ 보안/감사 취약 시간 간격 현저히 단축
영향 유형
재무적 손실
고객 이탈
명성 훼손
제반 규제
재무적 영향
가능성
1
0
Severity $$$
Hi
재무적 손실 가능성 감소
Automated Information Risk Management
A Mission-Critical Line of Defense

DB 보안 솔루션 – 데이터 보안의 이슈 해결

ITS KERNEL (주)잇츠커널

DB 취약성 평가 및 지속적 모니터링

- 데이터베이스 환경 취약성 평가 및 접근권한, 메타데이터 모니터를 통한 지속적 모니터링
  - 환경 설정 검증(DB 환경 설정 및 변수 확인)
  - 알려진 취약점(침입 테스트/보안 감사)
  - 기업 고유의 정보보호 규칙 준수 검증(사용자 정의 규칙(User Defined Rule))
  - 접근 권한 설정 모니터링
    - 사용자별로 할당된 역할
    - 사용자별로 접근 가능한 객체

기업 지적 자산 절취 및 유출

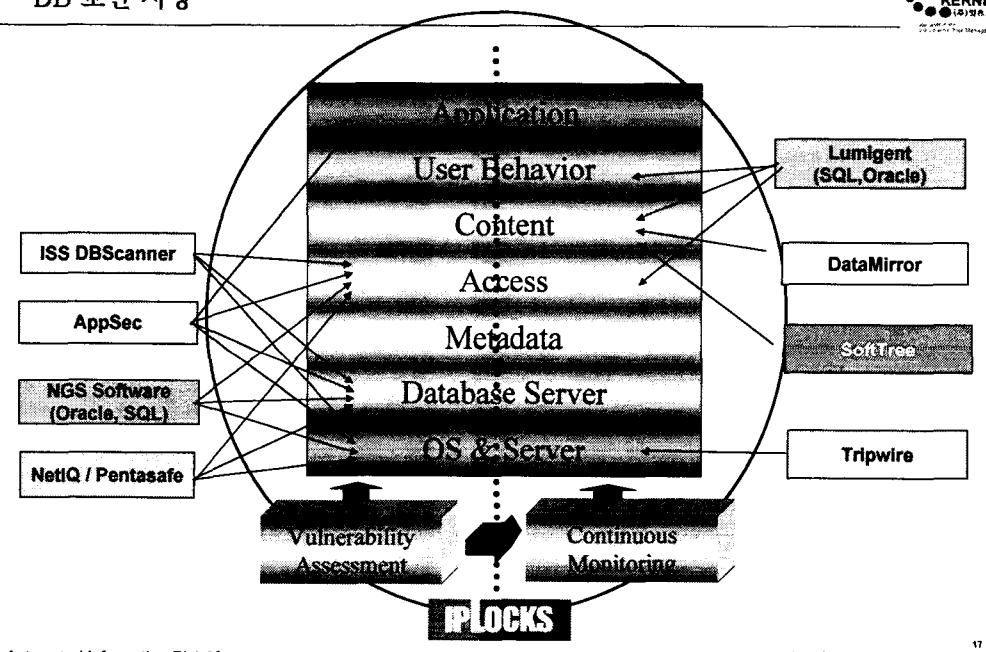
- 사용자 행동 패턴/데이터 사용 패턴 분석을 통해 다음 시나리오와 같은 의심스러운 접근을 탐지한 후 경고
  - 비인가자 접근 위반
  - 주요 데이터에 대한 접근 횟수/시스템 자원 사용이 갑자기 증가할 때
  - 인가된 경로(DB 사용자 / OS 사용자 / 터미널) 이외로 접근할 때
  - 업무 범위를 벗어난 비정상 접근 패턴

데이터의 무결성 강화

- **Content Monitor 및 User Behavior Monitor(사용자 행동 패턴 분석)의 병행 모니터링**
  - 사용자 정의 규칙 차이 정책에 모니터링 객체를 설정하면 데이터가 변경될 때 상세 변경 내역을 기록하고 경고 발령
    - 컬럼 단위로 변경 전의 값과 변경 후의 값
    - 추가/ 삭제된 데이터 등
  - 데이터를 기록.보관하여 차후의 근거 자료로 사용

DB 보안 시장

ITS KERNEL (주)잇츠커널



기대 효과

- 재무적, 영업적, 신뢰성에 대한 손실을 경감시키는 자동화된 정보자산 보호 시스템
- 데이터베이스관리에 대한 정보 보호/감사 규칙과 규정의 강화 및 운영상의 취약성 감소