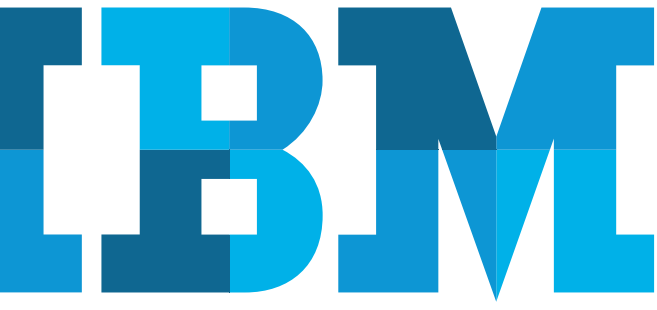
IBM InfoSphere Guardium

전체 데이터베이스 보안 및 준수 라이프사이클 관리

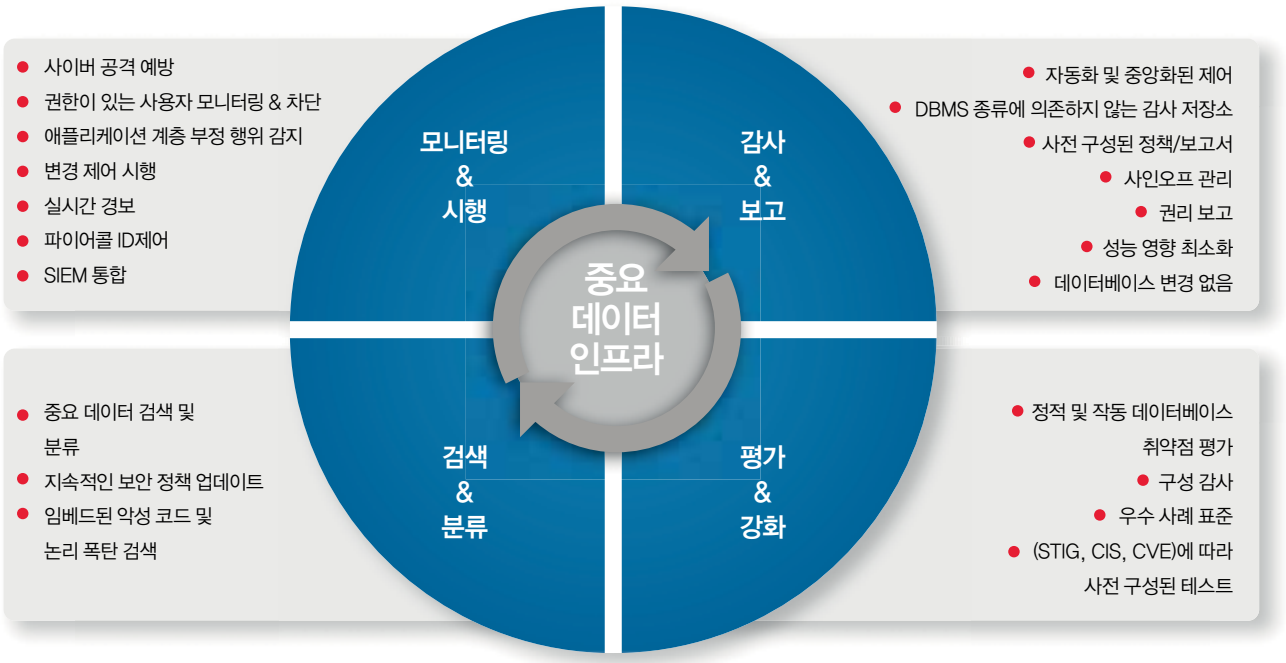
전 세계적으로 1,000개 이상의 조직에서 중요한 엔터프라이즈 데이터를 보호하는 데 있어 다른 어떤 기술 제공자보다도 IBM을 신뢰하고 있습니다. 실제로 IBM은 재무 및 ERP 정보, 고객 및 카드 소유자 데이터, 엔터프라이즈 시스템에 저장된 지적 재산을 보호하는 데 필요한 가장 간단하고 강력한 솔루션을 제공합니다.

IBM의 엔터프라이즈 보안 플랫폼은 권한이 있는 내부자 및 잠재적인 해커의 권한 없는 활동이나 의심스러운 활동을 예방합니다. 또한 Oracle E-Business Suite, PeopleSoft, SAP 및 내부 시스템 같은 엔터프라이즈 애플리케이션의 일반 사용자에 의한 잠재적 부정 행위도 모니터링 합니다.

이와 동시에 전체 애플리케이션 및 데이터베이스 인프라에서 준수 제어를 자동화하고 중앙화하는 확장 가능한 다중 계층 아키텍처를 사용하여 운영 효율을 최적화합니다. 무엇보다도 놀라운 것은 IBM 솔루션으로 인해 많은 뛰어난 성과를 얻을 수 있는 만큼 IBM 솔루션으로 인해 많은 일이 불필요해진다는 점입니다. IBM 솔루션은 사실상 성능에 전혀 영향을 주지 않으며 데이터베이스 변경을 필요로 하지도 않고 원시 데이터베이스 로그 또는 감사 유틸리티에 의존하지 않습니다.



실시간 데이터베이스 보안 및 모니터링



통합 솔루션: 단일 통합 콘솔 및 백엔드 데이터 저장소를 기반으로 빌드되었습니다. InfoSphere Guardium은 전체 데이터베이스 보안 및 준수 라이프사이클을 관리하는 데 사용되는 통합 모듈 제품군을 제공합니다.

InfoSphere Guardium은 통합 웹 콘솔, 백엔드 데이터 저장소 및 워크플로우 자동화 시스템을 사용하여 전체 데이터베이스 보안 및 준수 라이프사이클을 관리하는 유일한 솔루션입니다. 이 솔루션의 장점은 다음과 같습니다.

- 기업 데이터베이스에서 중요한 정보를 검색하고 분류합니다.
- 데이터베이스 취약점 및 구성 결함을 평가합니다.
- 권장 변경사항이 구현된 후 구성이 잠겼는지 확인합니다.
- 임무 구분이 지원되는 안전한 부정 조작 방지 감사 레코드를 통해 모든 플랫폼 및 프로토콜에서 발생하는 모든 데이터베이스 트랜잭션에 대해 100% 가시성 및 세분성을 제공합니다.
- Microsoft SharePoint 같은 주요 파일 공유 플랫폼에서의 활동을 추적합니다.
- 중요 데이터 액세스, 권한이 있는 사용자 조치, 변경 제어, 애플리케이션 사용자 활동 및 로그인 실패 같은 보안 예외에 대한 정책을 모니터링하고 시행합니다.
- SOX, PCI DSS 및 개인 정보 보호에 맞게 사전 구성된 보고서를 사용하여 관리 팀으로의 보고서 분배, 사인오프, 에스컬레이션을 비롯한 전체 준수 감사 프로세스를 자동화합니다.
- 엔터프라이즈 전체 준수 보고, 성능 최적화, 조사 및 증거 자료를 위해 사용할 중앙화된 단일 감사 저장소를 작성합니다.
- 단일 데이터베이스 보호에서 전 세계에 분산된 데이터 센터의 수많은 데이터베이스 보호에 이르기까지 쉽게 확장이 가능합니다.

검색 & 분류

자동으로 중요한 정보 검색, 분류 및 보안

조직에서 작성하고 관리하는 디지털 정보의 양이 점점 증가함에 따라 중요한 정보를 검색하고 분류하는 일이 점점 어려워지고 있습니다.

인수 합병 경험이 있거나 레거시 시스템이 원래 개발자보다 더 오래된 환경을 보유한 조직의 경우 더욱 그렇습니다. 가장 양호한 상황인 경우에도, 새로운 비즈니스 요구사항을 지원하는 데 필요한 애플리케이션 및 데이터베이스 구조의 지속적인 변화로 인해 쉽게 정적 보안 정책이 무효화되고 중요 데이터가 인식 및 보호되지 않는 상태가 될 수 있습니다.

조직에서 특히 어려움을 겪고 있는 부분은 다음과 같습니다.

- 중요 정보가 들어 있는 모든 데이터베이스 서버에 대한 계획을 세밀하게 수립하고 비즈니스 라인 애플리케이션, 일괄 처리 프로세스, 임시 쿼리, 애플리케이션 개발자, 관리자 등 모든 소스의 액세스 방법을 이해하기가 어렵습니다.
- 저장된 정보의 중요도가 알려지지 않은 경우 정보를 보안하고 리스크를 관리하기가 어렵습니다.
- 정보가 특정 규정 조항의 적용을 받는지 분명하지 않은 경우 준수를 보장하기가 어렵습니다.

InfoSphere Guardium에서는 데이터베이스 자동 검색 및 정보 분류 기능을 사용하여 기밀 데이터 저장 위치를 식별한 다음, 개별 맞춤화가 가능한 분류 레이블을 사용하여 해당하는 중요 오브젝트 클래스에 적용되는 보안 정책의 시행을 자동화합니다. 이러한 정책은 권한이 있는 사용자만 중요 정보를 보거나 중요 정보를 보고 변경할 수 있도록 합니다.

중요 데이터 검색이 정기적으로 실행되도록 예약하여 로우그(rogue) 서버 개입을 예방하고 중요 정보가 "망각" 되지 않도록 할 수도 있습니다.

평가 & 강화

취약점, 구성 및 작동 평가

InfoSphere Guardium의 데이터베이스 보안 평가에서는 전체 데이터베이스 인프라를 스캔하여 취약점이 있는지 확인하고 실시간 데이터 및 과거 데이터를 모두 사용하여 데이터베이스 보안 상태에 대한 지속적인 평가를 제공합니다.

업계 우수 사례(CVE, CIS, STIG) 및 플랫폼별 취약점에 따라 사전 구성된 테스트에 대한 포괄적 라이브러리가 제공되며 InfoSphere Guardium의 Knowledge Base 서비스를 통해 정기적으로 업데이트됩니다. 특정 요구사항을 충족시키도록 맞춤형 테스트를 정의할 수도 있습니다. 평가 모듈에서는 SOX 및 PCI DSS 준수 전용 Oracle EBS 및 SAP 테이블에 대한 권한 없는 액세스 같은 준수 관련 취약점에도 플래그를 지정합니다.

평가는 크게 다음 두 개의 범주로 구분됩니다.

- 취약점 및 구성 테스트 – 누락 패치, 잘못 구성된 권한 및 기본 계정 같은 취약점을 점검합니다.
- 작동 테스트 – 데이터베이스 액세스 및 조작 방식에 따라 모든 데이터베이스 트래픽을 실시간으로 모니터링하여 초과 로그인 실패 횟수, 관리 명령 실행 고객, 시간 외 로그인 같은 취약점을 식별합니다.

평가 모듈에서는 드릴다운 기능이 있는 자세한 보고서는 물론, 가중치 평가(우수 사례 기준), 산업 표준 참조 번호, 데이터베이스 보안을 강화하기 위해 권장되는 구체적인 활동 계획이 포함된 보안 상태 보고서 카드도 생성합니다.

구성 잠금 및 변경 추적

취약점 평가에서 생성된 권장 조치를 구현한 후에는 보안 구성 기준을 설정할수 있습니다. InfoSphere Guardium의 CAS(Configuration Audit System)의 사용은 이러한 기준에 대한 모든 변경을 모니터링하고 공인된 변경 제어 정책 및 프로세스를 제외한 어떠한 변경도 이루어지지 않도록 할 수 있습니다.

모니터링 & 시행

데이터베이스 보안 및 변경 제어 정책 모니터링 및 시행

InfoSphere Guardium은 로우그(rogue) 사용자 또는 외부자의 공격은 물론, 권한이 있는 데이터베이스 계정의 권한 없는 활동이나 의심스러운 활동을 예방하기 위해 세분화된 실시간 정책을 제공합니다. Oracle EBS와 PeopleSoft, Siebel, SAP, Cognos 그리고 IBM WebSphere, Oracle WebLogic, Oracle AS 같은 애플리케이션 서버를 기반으로 빌드된 맞춤형 시스템처럼, 공통 서비스 계정으로 데이터베이스에 액세스하는 다중 계층 애플리케이션을 통해 데이터베이스에 권한 없는 변경을 수행하는 애플리케이션 사용자를 식별할 수도 있습니다.

이 솔루션은 데이터베이스 관리자(DBA)가 개입할 필요 없이 정보 보안 담당자가 관리할 수 있습니다. 또한 OS 로그인, IP 또는 MAC 주소, 소스 애플리케이션, 시간, 네트워크 프로토콜, SQL 명령 유형 등을 기준으로 특정 테이블에 대한 액세스를 제한하는 세분화된 액세스 정책을 정의할 수도 있습니다.

모든 데이터베이스 트래픽에 대한 지속적인 컨텍스트 분석

InfoSphere Guardium은 실시간으로 모든 데이터베이스 조작에 대한 지속적인 모니터링을 수행하며 특허 출원 중인 언어 분석 기능을 사용하여 각 SQL 트랜잭션에 대해 "누가, 무엇을, 어디서, 언제, 어떻게" 수행했는지와 같은 자세한 컨텍스트 정보를 바탕으로 권한 없는 조치가 수행되는지 감지합니다. 이러한 고유의 접근 방식은 사전 정의된 패턴이나 서명만 검색하는 기존 방식과 달리 긍정적 판단 및 부정적 판단의 오류를 최소화하는 동시에 전례 없는 높은수준의 제어를 제공합니다.

예외적인 작동을 감지하고 정책 정의를 자동화하는 기준 설정

IBM 시스템은 기준을 설정하고 정상적인 비즈니스 프로세스 및 예외적으로 나타나는 활동을 모두 식별하여 SQL 인젝션 같은 공격을 예방하는 데 사용할 수 있는 정책을 자동으로 제안합니다. 편리한 드롭다운 메뉴를 통해 맞춤형 정책도 쉽게 추가할 수 있습니다.

사전 예방적인 실시간 보안

InfoSphere Guardium은 권한이 없거나 예외적인 작동에 미리 대처하는 데 필요한, 다양한 실시간 제어를 제공합니다. 정책 기반 조치로는 실시간 보안 경보(SMTP, SNMP, Syslog), 소프트웨어 차단, 전체 로깅 사용, 검역 사용자, VPN 포트 시스템 종료 및 경계 IDS/IPS 시스템에 따른 조정과 같은 맞춤형 조치 등이 있습니다.

보안 인시던트 추적 및 해결

준수 규정에 따르면 조직은 모든 인시던트가 시기 적절하게 기록, 분석 및 해결되고 관리 레벨에 보고됨을 증명해야 합니다. InfoSphere Guardium은 보안 인시던트를 해결하는 데 필요한 비즈니스 사용자 인터페이스 및 워크플로우 자동화와 주요 평가 기준을 추적하는 데 필요한 대시보드를 함께 제공합니다. 주요 평가 기준으로는 열린 인시던트 수, 심각도 레벨, 인시던트가 열린 기간 등이 있습니다.

감사 & 보고

세분화된 감사 레코드 캡처

InfoSphere Guardium은 모든 데이터베이스 활동에 대해 지속적이며 세분화된 레코드를 작성합니다. 이러한 레코드는 실시간으로 컨텍스트에 따라 분석되고 필터링되어 사전 예방적 제어를 구현하고 감사 담당자에게 필요한 구체적 정보를 생성합니다.

결과 보고서는 로그인 실패, 권한 에스컬레이션, 스키마 변경, 시간 외 액세스 또는 권한 없는 애플리케이션을 통한 액세스, 중요 테이블에 대한 액세스 등 모든 데이터베이스 활동에 대한 높은 가시성을 제공하여 준수를 증명합니다. 다음은 시스템에서 모니터링하는 활동의 예입니다.

- SQL 오류 및 로그인 실패 같은 모든 보안 예외
- 데이터베이스 구조를 변경하는 테이블 작성/삭제/변경 같은 모든 DDL 명령(SOX 같은 데이터 거버넌스 규정에 특히 중요)
- PCI DSS 같은 개인 정보 보호 규정에 중요한 모든 SELECT 쿼리
- 바인드 변수를 포함한 모든 DML 명령 (삽입, 업데이트, 삭제)
- 계정, 역할 및 권한을 제어하는 모든 DCL 명령 (GRANT, REVOKE)
- PL/SQL(Oracle) 및 SQL/PL(IBM) 같은, 개별 DBMS 플랫폼에서 지원되는 모든 프로시저 언어
- 데이터베이스에서 실행되는 모든 XML
- SharePoint 오브젝트에 대한 모든 변경

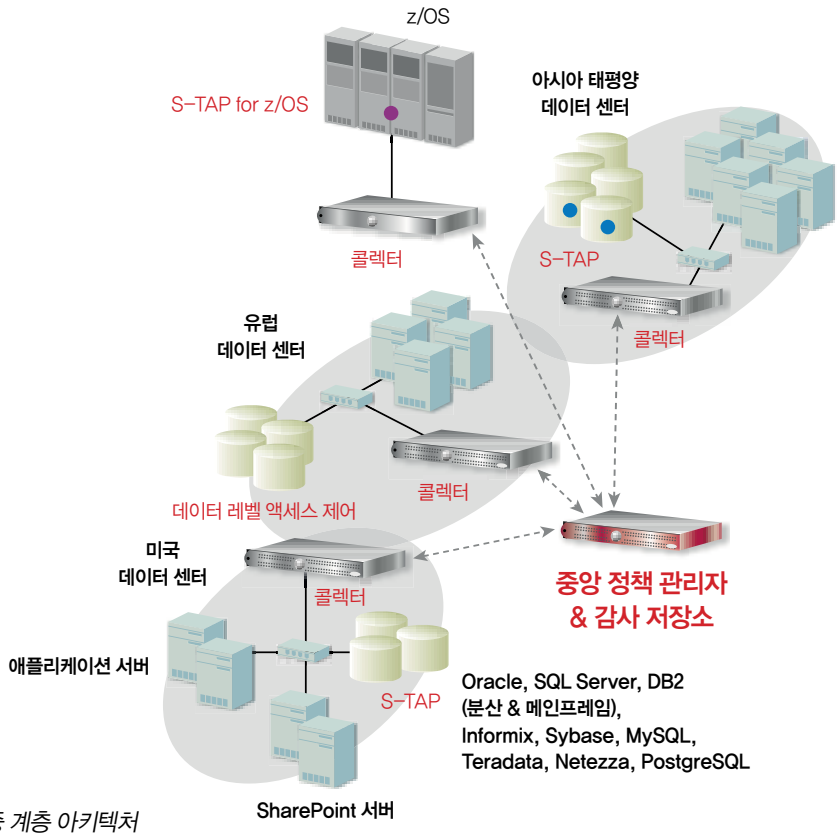
동종 최고의 보고 기능

InfoSphere Guardium 솔루션에는 1,000개의 글로벌 기업 그리고 세계 4대 감사 및 평가 업체와 함께 일한 경험과 우수 사례를 기반으로 한 150개 이상의 사전 구성된 정책 및 보고서가 있습니다. 이러한 보고서는 SOX, PCI DSS 및 개인 정보 보호법 같은 규정 요구사항을 충족시키고 데이터 거버넌스와 개인 정보 보호 이니셔티브를 효율적으로 추진하는 데 도움이 됩니다.

사전 패키지된 보고서 템플리트 외에도, InfoSphere Guardium은 그래픽으로 된 끌어 놓기 인터페이스를 제공하므로 쉽게 새 보고서를 빌드하거나 기존 보고서를 수정할 수 있습니다. 보고서는 이메일을 통해 PDF 형식(첨부 파일)이나 HTML 페이지 링크로 사용자에게 자동 전송될 수 있습니다. 또한 웹 콘솔 인터페이스를 통해 온라인으로 보거나 SIEM 및 기타 시스템에 표준 형식으로 내보낼 수도 있습니다.

기업 성장을 보장하는 확장성

- **비침투적:** 권한이 있는 사용자의 로컬 액세스를 포함한 모든 데이터베이스 트랜잭션에 대해 100% 가시성을 제공 하면서도 성능에 미치는 영향은 최소화되어 있으며 데이터베이스나 애플리케이션 변경을 필요로 하지 않습니다.
- **DBMS 독립적:** 원시 로깅 또는 감사에 의존하지 않는 플랫폼에 의존하지 않는 솔루션입니다.
- **어플라이언스 기반:** "블랙 박스" 어플라이언스(자체 포함된 스토리지, 사전 설치된 애플리케이션, 내장된 관리)를 통한 빠른 배치를 위해, 강화된 Linux 커널을 기반으로 빌드된 모듈형 소프트웨어 제품입니다. 하드웨어 통합 전략을 지원하는 가상 어플라이언스로도 사용할 수 있습니다.
- **유연한 모니터링:** 경량 호스트 기반 프로브, SPAN 포트, 네트워크 TAP 또는 이들의 조합을 사용합니다.
- **준비된 인프라:** SNMP, SMTP, Syslog, LDAP, Kerberos, RSA SecurID®, BMC Remedy 같은 변경 디켓팅 시스템, CEF 및 모든 주요 SIEM 플랫폼과의 통합을 지원합니다.
- **다중 계층:** InfoSphere Guardium은 업계에서 유일하게 자동으로 여러 데이터베이스 플랫폼 및 위치의 감사 정보를 중앙화된 단일 감사 저장소로 집계하게 표준화합니다.
- **중앙화된 관리:** 웹 콘솔을 통해 엔터프라이즈 전체에서 DBMS 종류에 종속적이지 않게 보안 정책을 관리합니다.
- **확장 가능:** 모니터 대상 서버의 수 또는 트래픽 크기가 증가하면 간단히 어플라이언스를 추가하여 증가된 로드를 처리합니다. 특허를 받은 인텔리전트 스토리지 알고리즘이 기존의 플랫 파일 기반 접근 방식에 비해 100배 향상된 스토리지 효율을 제공합니다.
- **부정 조작 방지 감사 저장소:** 루트 액세스가 없는 강력한 인증 및 암호화된 아카이브를 갖추고 있습니다.
- **역할 기반:** 조직 역할에 따라 모듈 및 데이터에 대한 액세스가 제어됩니다.



확장 가능한 다중 계층 아키텍처

InfoSphere Guardium의 확장 가능한 아키텍처는 웹 콘솔을 통해 엔터프라이즈 전체에서 중앙화된 감사 데이터 집계와 표준화, 중앙화된 보안 정책 관리를 사용하여 대규모 환경 및 소규모 환경을 모두 지원합니다. S-TAP는 권한이 있는 사용자의 로컬 액세스를 포함한 모든 데이터베이스 트래픽을 모니터링하는 경량의 호스트 기반 프로브로, 분석 및 보고를 위해 InfoSphere Guardium 콜렉터 어플라이언스로 정보를 릴레이합니다. 콜렉터 어플라이언스는 S-TAP에서 또는 네트워크 스위치의 SPAN 포트에 직접 연결하여 모니터링된 데이터를 수집합니다. 애그리게이터는 자동으로 여러 콜렉터 어플라이언스의 감사 데이터를 집계합니다. 확장성 및 유연성을 최대화하기 위해 다중 계층 애그리게이터를 구성할 수 있습니다. 또한, S-TAP 확장으로 구현되는 InfoSphere Guardium의 데이터 레벨 액세스 제어는 DBA가 새 데이터베이스 계정 작성 및 기존 계정 권한 승급 같은 보안 기능을 수행하지 않도록 차단하여 보안을 강화하고 임무 구분을 시행합니다.

준수 워크플로우 자동화

업계에서 유일한 InfoSphere Guardium의 준수 워크플로우 자동화 애플리케이션은 전체 준수 워크플로우 프로세스의 효율을 향상시켜 감사 보고서 생성, 주요 이해 관계자에게로의 분배, 전자 사인오프 및 에스컬레이션 프로세스를 자동화하는 데 도움이 됩니다. 워크플로우 프로세스는 상세한 레벨에서 완전하게 사용자 정의될 수 있으며 특정 감사 항목이 사인오프에 따라 개별적으로 라우트되고 추적되도록 할 수 있습니다.

이기종 환경을 위한 통합 솔루션

광범위한 플랫폼 지원

InfoSphere Guardium의 플랫폼에 구속받지 않고 솔루션은 모든 주요 운영체제(Windows, UNIX, Linux, z/OS)와 Microsoft SharePoint 및 FTP 환경에서 실행되는 모든 주요 DBMS 플랫폼 및 프로토콜을 지원합니다.

지원되는 플랫폼	지원되는 버전
Oracle Database	8i, 9i, 10g(r1, r2), 11g, 11gR2
Oracle Database (ASO, SSL)	9i, 10g(r1, r2), 11g
Microsoft SQL Server	2000, 2005, 2008
Microsoft SharePoint	2007, 2010
IBM DB2 (Linux, Unix, Linux for System z)	9.1, 9.5, 9.7
IBM DB2(Windows)	9.1, 9.2, 9.5, 9.7
IBM DB2 for z/OS	7, 8, 9
IBM DB2 for iSeries	V5R2, V5R3, V5R4, V6R1
IBM Informix	7, 9, 10, 11, 11.50
Sun MySQL 및 MySQL Cluster	4.1, 5.0, 5.1
Sybase IQ	12.6, 15
Netezza	4.5
PostgreSQL	8
Teradata	6.X, 12, 13
FTP	

호스트 기반 모니터링

S-TAP는 업계에서 유일하게 데이터베이스 서버의 OS 레벨에서 네트워크 및 로컬 데이터베이스 프로토콜(공유 메모리, 이름 지정된 파이프 등)을 모두 모니터링하는 경량 소프트웨어 프로브입니다. S-TAP는 데이터베이스 자체에 의존하여 로그 데이터를 처리 및 저장하지 않고 실시간 분석과 보고를 위한 별도의 InfoSphere Guardium 어플라이언스로 모든 트래픽을 릴레이하여 서버 성능에 미치는 영향을 최소화합니다. S-TAP를 사용하는 경우 원격 위치 또는 데이터 센터의 사용 가능한 SPAN 포트에 전용 하드웨어 어플라이언스가 필요하지 않으므로 고객이 S-TAP를 선호하는 경우가 많습니다.

OS 유형	버전	32비트 및 64비트
AIX	5.2, 5.3	모두
	6.1	64비트
HP-UX	11.11, 11.23, 11.31	모두
Red Hat Enterprise Linux	3, 4, 5	모두
Red Hat Enterprise Linux for Systemk z	5.4	
SUSE Enterprise Linux	9, 10, 11	모두
SUSE Enterprise Linux fot System z	9, 10, 11	
Solaris – SPARC	8, 9, 10	모두
Solaris ? Intel/AMD	10	모두
Tru64	5.1A, 5.1B	64비트
Windows	2000, 2003, 2006	모두
iSerises	i5/OS*	

* Enterprise Integrator를 통해 네트워크 활동 모니터링 및 로컬 활동 지원

애플리케이션 모니터링

InfoSphere Guardium은 데이터베이스에 직접 액세스하지 않고 다중 계층 엔터프라이즈 애플리케이션을 통해 중요 테이블에 액세스하는 일반 사용자의 활동을 추적하여 잠재적 부정 행위를 식별합니다. 엔터프라이즈 애플리케이션은 일반적으로 "연결 풀 사용" 이라는 최적화 메커니즘을 사용하므로 이러한 모니터링은 필수입니다. 풀 사용 환경에서는 모든 사용자 트래픽이 일반 애플리케이션 계정 이름에 의해서만 식별되는 몇 개의 데이터베이스 연결 내에서 집계되어 일반 사용자 식별을 마스킹합니다. InfoSphere Guardium은 모든 주요 규격 엔터프라이즈 애플리케이션에 대해 애플리케이션 모니터링을 지원합니다. 내부 애플리케이션을 비롯한 다른 애플리케이션에 대한 지원은 애플리케이션 서버 레벨의 트랜잭션 모니터링을 통해 제공됩니다.

지원되는 엔터프라이즈 애플리케이션	• Oracle E-Business Suite • PeopleSoft • Siebel • SAP • Cognos • Business Objects Web Intelligence
지원되는 애플리케이션 서버 플랫폼	• IBM WebSphere • BEA WebLogic • Oracle Application Server(AS) • JBoss Enterprise Application Platform

IBM InfoSphere Guardium 정보

Guardium은 시스템에서 신뢰할 수 있는 정보를 정의, 통합, 보호 및 관리하는데 사용되는 통합 플랫폼, IBM InfoSphere의 일부입니다. InfoSphere 플랫폼은 공유 메타데이터 및 모델 코어에 모두 통합된, 데이터 통합, 데이터 웨어하우징, 마스터 데이터 관리, 정보 거버넌스 등을 포함한 신뢰할 수 있는 정보의 모든 기초 빌딩 블록을 제공합니다. 포트폴리오가 모듈형이므로 어디에서든 시작할 수 있으며 InfoSphere 소프트웨어 빌딩 블록을 다른 공급업체의 구성요소와 결합하고 맞추거나 여러 빌딩 블록을 함께 전개하여 진행 속도 및 가치를 향상시킬 수도 있습니다. InfoSphere 플랫폼은 정보 집약적 프로젝트를 위한 엔터프라이즈 클래스 기초를 제공하여 어려운 과제를 단순화하고 신뢰할 수 있는 정보를 회사에 보다 빠르게 제공하는 데 필요한 성능, 확장성, 안정성 및 빠른 속도를 제공합니다.

(135-270) 서울시 강남구 도곡동 467-12
군인공제회관빌딩

한국아이비엠주식회사
고객만족센터

TEL: (02)3781-7114
www.**ibm.com**/kr

2013년 6월

Please Recycle

InfoSphere
software

IMD14286-USEN-01