

Informatica Secure@Source

핵심 이점

- 개인 데이터와 민감한 데이터를 보호하고 모니터링하여 데이터 중심 디지털 변혁을 추진하고 개인 정보 보호 및 규정 준수 노력을 지원
- 모든 데이터 플랫폼과 유형에 대한 가시성을 확보하여 오늘날의 복잡한 하이브리드 환경에 필요한 지원을 제공
- 개인 데이터와 민감한 데이터에서 지속적으로 위험을 분석하여 기능, 지역, 사업부 부 전반에 걸쳐 리소스 및 투자 우선 순위 지정
- 비정상적인 고위험 데이터 사용을 알아내기 위한 AI 기반 검색
- 민감한 데이터 인텔리전스를 활용한 자동화된 오케스트레이션 및 보호로 개인 정보 보호 및 보안 위험 해결

개인 데이터 및 민감한 데이터 검색, 분류, 해결 및 모니터링

Informatica® Secure@Source®는 조직 전체에서 개인 및 민감한 데이터 위험을 검색하고 해결하는 데 도움이 됩니다. AI(인공 지능) 및 기계 학습을 활용하여 실행 가능한 데이터 검색 및 분류, 위험 점수, 행동 분석, 자동화된 보호 기능을 하나의 솔루션으로 제공합니다. 클라우드, 온 프레미스, 빅 데이터 저장소와 모든 관계형 및 메인프레임 시스템에서 정형 데이터와 비정형 데이터를 모두 지원합니다.

Secure@Source는 다음과 같은 방법으로 데이터 보호 및 개인 정보 보호에서 투자, 정책, 프로그램의 우선 순위를 정하는 데 도움을 줍니다.

- **정형 및 비정형 민감한 데이터에 대해 알고 있는 부분 확인:** 관리자와 실무자 모두 기업 전반에서 데이터 분류, 검색, 확산 분석, 사용자 액세스, 활동 상관 관계를 통해 개인 데이터와 민감한 데이터에 대한 전체 가시성을 얻습니다.
- **지속적으로 위험 모니터링:** 조직의 요구에 맞게 맞춤화할 수 있는 여러 요소를 기반으로 데이터 위험과 해결책을 추적하고, 요구 사항에 따라 가장 위험한 영역을 파악합니다.
- **예상치 못한 액세스 탐지:** 분석을 활용하여 의심스럽거나 승인되지 않은 데이터 액세스를 감지합니다. 이는 민감한 데이터를 위협하는 고위험 상태와 잠재적으로 비정상적인 행동에 대해 지속적으로 상관 관계를 만들고, 기준을 정하고, 분석하고, 알리는 방식으로 수행됩니다.
- **위험 해결:** 데이터 보안 제어의 오케스트레이션을 자동화하여 보관 중이거나 사용 중인 데이터를 보호하고, 무단 액세스를 방지하며, 민감한 데이터를 식별 불가능하게 하고 익명화합니다. 위험 시뮬레이터를 통해 구현하기 전에 데이터 제어의 영향을 파악할 수 있습니다.

주요 기능

민감한 데이터 찾기 및 분류

- 기업 전반에서 민감한 데이터와 개인 데이터의 위험을 찾고, 분류하고, 분석합니다. 기존 관계 데이터베이스(예: 메인프레임) 전체의 정형 데이터, HDFS 및 Amazon S3의 반정형 데이터(CSV, XML, JSON), CIFS NFS의 비정형 데이터, 그리고 SharePoint의 기존 정형 데이터 저장소에서 이를 수행할 수 있습니다.
- 대시보드 및 드릴다운으로 민감한 데이터에 대한 완벽한 가시성을 확보하여 부서, 애플리케이션, 사용자, 데이터 스토리지 유형 같은 직무 및 조직 정보를 식별합니다.
- 확산 추적 및 대화식 시각화를 통해 기업 내부와 외부, 그리고 파트너와 클라이언트 조직 간에 이루어지는 데이터 이동을 완전히 파악합니다.

Informatica 정보

디지털 변혁은 우리의 기대치를 바꿔 놓았습니다. 이제 더 적은 비용으로 더 나은 서비스를 더 빠르게 제공할 수 있어야 합니다. 이러한 상황에 부응하기 위해서는 기업은 변화해야 하며, 데이터가 이에 대한 해답을 쥐고 있습니다.

엔터프라이즈 클라우드 데이터 관리 분야의 세계적인 선도 기업인 Informatica는 모든 부문, 카테고리, 틈새시장에서 지능적인 방식으로 고객을 지원할 준비가 되어 있습니다. Informatica는 더욱 민첩하게 운영하고, 새로운 성장 기회를 발견하거나 새로운 혁신을 이룰 수 있는 통찰력을 기업에 제공합니다. 또한 모든 종류의 데이터에 100% 집중하여 성공에 필요한 다양한 서비스를 제공하고 있습니다.

Informatica가 제공하는 모든 서비스에 관해 알아보고 데이터의 힘을 활용하여 미래의 지능형 혁신을 실현하시기 바랍니다.



그림 1. Secure@Source는 대시보드(왼쪽)와 위험 해결 시뮬레이션(오른쪽)을 통해 민감한 데이터에 대한 360도 가시성을 제공합니다.

규정 준수 보장

- 데이터 민감도, 양, 보호, 확산, 위치, 사용자 활동 등 맞춤화 가능한 요소를 기반으로 하는 위험 점수를 사용하여 규제되는 개인 정보 보호 데이터 규정 준수를 추적하고 지속적으로 측정합니다.
- 데이터 도메인 조합을 적용하여 정책, 법, 규정과 관련된 GDPR, PII, PHI, PCI 위험을 정의합니다.
- 자동화된 해결책과 사용자 및 데이터 모니터링으로 규정 준수를 적용합니다.

민감한 데이터 보호

- 중요한 데이터 보호 우선 순위를 파악합니다.
- 통합된 Informatica Dynamic Data Masking, Persistent Data Masking, 타사 보호 방법(예: Hortonworks Ranger, Cloudera Sentry)과 암호화를 활용하는 자동화된 해결책으로 민감한 데이터를 보호합니다.
- 맞춤 스크립트, 이메일 알림, 시스템 로그 메시지 또는 ServiceNow 티켓과 통합됩니다. 보안 정책 위반으로 트리거될 때 이러한 작업이 실행되도록 구성하거나 잠재적 위험이 감지될 때 작업을 수동으로 실행할 수 있습니다.
- 사용자 행동, 데이터 액세스, 이동을 모니터링하고 알립니다.

자세한 내용은 [Secure@Source 제품 페이지](#)를 참조하십시오.



한국인포매티카 06611 서울시 서초구 서초동 강남대로 465 교보타워 B동 13층, 대표 전화: +82 2 6293 5001
미국 내 수신자 부담 번호: 1.800.653.3871 informatica.com/kr [linkedin.com/company/informatica](https://www.linkedin.com/company/informatica) twitter.com/InformaticaKR

IN06_0818_02878

© Copyright Informatica LLC 2018. Informatica, Informatica 로고, CLAIRE 및 PowerCenter는 미국 및 기타 국가에서 Informatica LLC의 상표 또는 등록 상표입니다. Informatica 상표의 최신 목록은 <https://www.informatica.com/trademarks.html>에 있는 웹에서 확인할 수 있습니다. 기타 회사 및 제품 이름은 해당 소유주의 상품명 또는 등록 상표일 수 있습니다. 이 문서의 정보는 예고 없이 변경될 수 있으며 일체의 명시적 또는 묵시적인 보증 없이 '있는 그대로' 제공됩니다.