Informatica

백서

마스터 데이터 관리의 프라이버시 위험 완화하기

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 기업이 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.

목차

총괄 요약 4

개요 5

민감한 데이터 프라이버시 위험을 완화하기 위한 4가지 요소 전략 5

- 검색 및 분류 6
- 규정 준수 6
- 보호 7
- 감사 준비 및 반응 7

결론 7

권장 사항 8

총괄 요약

고객, 제품, 서비스, 운영 및 기타 비즈니스에 중요한 엔터프라이즈 정보의 신뢰할 수 있는 확실한 뷰를 구현하기 위해서는 MDM(마스터 데이터 관리) 이니셔티브에 투자합니다. MDM은 기업 전반의 필수 데이터의 요소를 통합된 레코드에 결합하여 신뢰할 수 있는 데이터를 만듦으로써 필요한 사람들 및 애플리케이션과 그러한 요소를 공유할 수 있게 해줍니다. 고객 중심적인 제공 사항을 구축하고, 고객 서비스 및 충성도 프로그램을 개선하고, 제품 관리 및 솔루션에서 효율성을 창출하고, 클라우드로 안전하게 마이그레이션하려는 비즈니스에 막대한 가치를 제공합니다.

신뢰할 수 있는 데이터는 조직의 고객 및 제품 이니셔티브의 핵심이 되며 경쟁 우위를 제공합니다. 하지만 민감한 데이터의 통합은 외부 공격의 탐나는 표적이 되어 데이터 보안 위반이 발생하고 잠재적인 내부 오남용을 증가시키며, 이에 따라 GDPR(일반 데이터 보호 규정) 및 CCPA(California Consumer Privacy Act) 등의 프라이버시 규정이 적용됩니다.

이러한 환경에서 데이터 보호 및 규정 준수와 관련해 다음과 같은 궁금증이 드는 것은 당연합니다.

- 모든 데이터는 어디에 있으며 어떻게 확산되는가?
- 무엇이 리포지토리에 피드를 제공하며 누가 어떤 애플리케이션을 사용하여 데이터에 액세스하는가?
- 현재의 액세스 및 사용이 규정 및 승인된 데이터 사용 정책을 준수하는가?
- 데이터 보호가 적절하며 데이터 위험이 적정 수준으로 관리되는가? 아니면 현재 상태가 해결이 필요한 더 큰 부적절한 위험을 초래하는가?

민감한 고객 데이터를 검색하고 분류한 결과는 마스터 데이터의 위험, 보호 및 프라이버시 규정 준수에 관한 의사 결정을 뒷받침할 기반이 됩니다.

이 백서는 데이터 중심의 솔루션에 동반되는 위험을 완화하기 위한 다음과 같은 전략 및 고려 사항의 프레임워크를 제공합니다.

- 분석, 메타데이터 기반 인텔리전스, 자동화 및 AI를 적용하여 민감한 마스터 데이터를 식별하고 보호
- 계속 진화하는 데이터 거버넌스 및 프라이버시 규정 준수
- 제어 기능이 준비되어 있음을 증명하기 위한 감사에 대해 준비 및
- 이상한 사용자 행동이 발생하면 이해 관계자에게 알리고 조사 요구

개요

연구 조사 기업인 IDC는 전 세계 데이터 양이 2018년에는 33제타바이트였지만 2025년에는 175제타바이트에 달하는 데이터가 생성될 것으로 전망했습니다.[1] 모든 산업 분야의 조직들은 수익을 창출하고, 고객에게 서비스를 제공하며, 생산성을 늘리고, 운영을 최적화하고, 기타 미션 크리티컬한 비즈니스 프로세스를 수행하기 위해 데이터의 정확성, 가용성, 보호에 의존하고 있습니다.

또한 데이터의 양과 사용량이 지속적이고 급격하게 증가하면서 여러 사일로, 온 프레미스 및 클라우드에서 다양한 데이터 형식으로 민감한 마스터 데이터도 늘어날 것입니다. 이러한 상황 때문에 기존 데이터 보안 방법이 쓸모없게 되어[2] 조직 전체에서 마스터 데이터 보안에 대한 새로운 접근 방식이 요구되고 있습니다.

그러나 대부분의 회사는 민감한 마스터 데이터가 모두 어디에 있는지, 어디에서 액세스되는지 정확하게 파악하지 못합니다. 특히 이러한 데이터가 구조화되지 않은 형식인 경우에는 더욱 그렇습니다. 가시성이 떨어지면 조직의 위험은 증가하며, 따라서 데이터 보안 위반은 가장 가능성이 높은 IT 보안 위험으로 남아 있습니다.[3]

부적절하게 사용되는 민감한 마스터 데이터의 확산과 더불어 데이터 보안 위반이 화두로 떠오름에 따라, 조직은 데이터 중심 프라이버시 솔루션을 고려한 다음과 같은 핵심 기능을 갖춘 위험 완화 전략을 개발해야 합니다.

- 조직 전체에 있는 민감한 마스터 데이터를 찾고 분류할 수 있는 모든 데이터 소스에 대한 가시성
- 데이터 보안 위반을 줄이기 위해 민감한 마스터 데이터에 대한 보호 메커니즘을 구현하는 기능
- 메타데이터 기반 인텔리전스, 자동화 및 AI를 사용하여 거의 실시간으로 사용자 행동을 모니터링하고 이상 행동을 보고하는 기능이 포함된 최신 프라이버시 규정 준수 기능
- 위험 평가 및 민감한 데이터 관리를 위한 다양한 분석 시각화 툴
- 감사 준비로 제어 기능이 준비되어 있음을 입증하기 위한 투명하고 포괄적인 보고 기능

Gartner는 이질적이고 서로 고립된 데이터 보안 툴 대신 통합된 보호 제품을 사용하는 대기업의 비율이 5% 미만에서 40%까지 증가할 것이라고 전망했습니다.[4] 데이터 중심 보호 솔루션은 위험 상태의 데이터에 대해 중앙 집중식 뷰를 제공하므로, 글로벌 조직의 모든 핵심 이해 관계자가 거버넌스 정책 및 규정의 요구사항에 따라 민감한 데이터의 이동을 추적하고 보호 메커니즘을 적용할 수 있습니다.

민감한 데이터 프라이버시 위험을 완화하기 위한 4가지 요소 전략

민감한 데이터 프라이버시 위험은 민감한 데이터가 부적절하게 노출되는 것의 영향이며, 가장 일반적인 원인은 데이터 규정 위반 또는 내부자의 오남용입니다. 그저 민감한 마스터 데이터를 찾는 것만으로도 위험을 충분히 해결할 수 있다는 생각은 잘못된 인식입니다. 이러한 데이터를 찾아 분류하는 것은 포괄적인 위험 해결 전략의 첫 단계에 불과합니다.

[1] IDC 백서, '디지털화되는 세상 – 엣지에서 코어까지' (2018년 11월).
[2] Gartner, '데이터 중심 감사 및 보호를 위한 시장 가이드', 2017년 3월 21일.
[3] Ponemon Institute LLC, '데이터 규정 위반 및 민감한 데이터의 위험', 2016년 2월.
[4] Gartner, '데이터 중심 감사 및 보호를 위한 시장 가이드', 2017년 3월 21일.

다음 단계는 데이터를 찾고 분류 분석을 거친 결과에 따라 조직의 해결해야 할 위험 우선순위를 평가하는 것입니다. IT 조직뿐 아니라 모든 핵심 이해 관계자가 참여하여 데이터 거버넌스 정책이 적용되는 자동화된 제어 기능과 함께 가장 큰 위험을 줄일 수 있는 전략을 결정해야 합니다. 전략에는 위험 가시성 대시보드 및 규정 준수 제어에 대한 감사 보고를 위한 민감한 데이터의 다양한 분석 시각화 기능과 조직 전체의 모든 민감한 마스터 데이터 유형의 보호 기능을 포함하여 규정 준수 기능을 제공하는 신뢰할 만한 데이터 중심 및 프라이버시 보호 솔루션을 구현하는 것이 포함되어야 합니다.

1. 검색 및 분류

일반적인 임시의 검색 방식은 기존 소스를 검토하고 질문을 전송하는 것입니다. 하지만 사용자 행동 및 데이터 흐름을 실제로 실시간으로 모니터링하지 않고 자체 보고에 의존하는 수동적인 이 방식은 귀중한 시간과 리소스를 많이 사용하며 가끔 부정확하고 빠른 속도로 뒤떨어지기 때문에 적절하지 않습니다.

조직은 스스로에게 다음과 같은 질문을 해야 합니다.

- 어떤 데이터를 저장하고, 누가 이 데이터에 액세스하며, 어떤 목적으로 액세스하는가?
- 사용자 권한을 어떻게 관리하고 데이터 권한을 어떻게 프로비저닝하는가?
- 민감한 마스터 데이터를 어떻게 보호할 것이며, 적절한 제어 기능이 준비되어 있는가?

검색 및 분류 규정 준수를 위한 기타 고려 사항은 다음과 같습니다.

- 데이터베이스 및 비정형 데이터를 포함한 데이터 환경 정의 및 이해
- 어떤 시스템이 민감한 마스터 데이터를 포함하고 있는지 매핑 및 데이터를 ID에 매핑
- 에코시스템에서 이 데이터의 이동을 매핑할 수 있는 솔루션을 조달하면서, 분석 및 보고 툴로 거의 실시간 뷰를 유지

2. 규정 준수

조직은 데이터 위험을 식별하고, 모니터링하고, 해결하여 데이터 프라이버시 규정을 준수합니다. 조직은 이를 넘어 규정 준수를 위험에 빠뜨릴 수 있는 데이터 액세스나 이동을 모니터링하고, 분석하고, 알려야 합니다.

2018년 5월 25일부터 시행된 GDPR은 EU의 모든 개인을 위해 데이터 보호를 강화하고 통일하려는 목적으로 도입되었습니다. 이에 따라 국제적인 기업의 규제 환경이 단순화되었습니다. 이와 비슷하게, 2020년 1월 1일부터 시행된 CCPA는 기준을 높여 개인 정보 보호가 가족 구성원 데이터를 포함하도록 범위를 넓혔습니다.

하지만 많은 기업이 이 두 가지 규정에 완전히 대비하지 못해 충분하게 규정을 준수하지 못하고 있으며, 규정을 준수하지 않을 경우 큰 벌금이 부과되고 평판에 해가 될 수 있습니다. 반대로, 규정 준수는 고객 충성도를 향상하기 위한 마스터 데이터 프라이버시 차별화 요소로 경쟁 우위의 기회를 제공할 수 있고, 디지털 변환 성과를 촉진할 수도 있습니다. 또한, 데이터를 보호함으로써 노력을 보여주는 회사는 고객의 개인 정보를 책임감 있게 처리할 것이라고 믿음을 얻어 5배 더 많은 개인 정보에 액세스할 수 있게 됩니다.[5]

[5] Boston Consulting Group, "개인 데이터에서 신뢰의 간극을 메우다"에서 발췌

조직은 GDPR, CCPA 및 이와 비슷한 개인정보 보호 요건과 관련된 '데이터 도메인'이 포함된 데이터 저장소를 식별하는 지능형 정책을 개발해야 합니다. 이러한 정책은 여러 요소를 고려하고, 어떤 조합이 프라이버시 노출 위협을 제기할지 결정하는 데이터 인텔리전스 로직이 포함되어 있어야 합니다.

3. 보호

2019년 3분기에 5,000건이 넘는 데이터 규정 위반이 발생했으며, 거의 80억 건의 레코드가 노출되었습니다.[6] 보안에 대한 대규모 투자에도 불구하고 중요한 데이터가 취약한 상태로 남아 있는 것은 분명합니다. 조직은 지속적으로 고위험 데이터를 보호하고, 의심스러운 행동과 무단 사용 또는 이동을 파악하는 동시에 해결책을 자동화하고 오케스트레이션해야 합니다.

조직은 기존의 서버 액세스 제어, 방화벽 및 이와 비슷한 시스템 중심의 사이버 보안 툴에만 의존하는 대신, 가장 중요한 데이터 위험의 우선순위를 지정하고 데이터 중심 제어를 통해 이러한 위험을 해결해야 합니다. 예를 들어, 데이터 중심 제어에는 마스킹, ID 기반 제어 및 암호화가 포함됩니다.

데이터 프라이버시 제어 외에도, 조직은 ID 기반 데이터 액세스와 행동을 모니터링해야 합니다. 과도한 액세스나 비정상적인 행동은 사용자가 프라이버시 정책을 준수하지 않고 있거나 사용자 자격 증명이 손상당했음을 의미할 수 있습니다.

4. 감사 준비 및 반응

기업은 민감한 데이터에 대해 과거 어느 때보다 많은 감사와 평가를 받고 있으며, 중요한 데이터의 가시성과 보호 기능을 갖추고 있음을 감사자에게 증명하기 위해 노력하고 있습니다.

조직은 감사자에게 즉시 대응할 수 있어야 하고, 데이터가 어디에 있고, 데이터의 위험은 무엇이며, 데이터를 어떻게 보호하고, 데이터를 어떻게 사용하고 있는지 알고 있다는 증거를 제공할 수 있어야 합니다. 또한, 감사자가 부서 또는 사업장에 대해 요약되어 있고 특정 데이터 도메인에서 드릴다운하는 기능을 제공하는 보고서와 시각화를 요청하는 상황도 고려해야 합니다.

결론

MDM을 통해 조직은 운영과 서비스를 혁신할 수 있습니다. 이 데이터의 힘은 분명하지만 내부 또는 외부의 공격자가 악용할 수 있는 탐나는 표적이 되기도 합니다. 계속되는 데이터 규정 위반 공격과 증가하는 규정 준수 요구사항이 결합되어 조직이 민감한 데이터를 식별하고, 분석하고, 보호하는 프로세스와 툴을 재고해야 합니다.

프라이버시 위험이 커지고 일상적인 데이터 규정 위반이 발생하는 현재 환경에서 기업은 이제 강력한 디지털 전략을 개발하여 민감한 마스터 데이터에 대한 위험을 지속적으로 모니터링하고, 분석하여, 해결해야 합니다. 데이터를 거의 실시간으로 모니터링하여 잘못된 사용이나 데이터 보안 위반, 비정상적인 액세스 및 행동 또는 부적절한 국경 간 전송의 징후가 있는지 파악해야 합니다. 이러한 노력을 통해 조직은 MDM을 활용하고 데이터 위험 형세를 개선하여 데이터 규정 위반이나 내부의 잘못된 사용으로 인한 영향을 줄이고, 지역 및 업계 규정의 엄격한 요구사항을 충족할 수 있습니다.

[6] Risk Based Security의 2019년 3분기 데이터 규정 위반 QuickView 보고서

권장 사항

1. 데이터 프라이버시 위험 평가를 수행하여 민감한 마스터 데이터가 어디에 있는지, 이러한 데이터가 데이터 에코시스템을 통해 어디까지 확산되는지, 그리고 어떤 민감한 데이터 세트가 가장 취약한지를 명확히 파악하십시오.
2. 평가 결과에 따라, 조직에서 가장 민감한 마스터 데이터의 상위 소스에 대해 우선순위를 정한 후 해당 소스를 보호하기 위한 전략 및 일정을 결정하고 이 전략을 데이터 프라이버시 및 보호에 대한 접근 방식의 파일럿 솔루션으로 구현하십시오.
3. 조직의 프라이버시 규정 준수 정책 및 프라이버시 규정 준수의 책임이 있는 핵심 이해 관계자를 정의하고, 문서화한 후, 배포하십시오. 올해 및 그 이후의 상황을 고려하여 전략 계획을 구축하십시오.

더 알아보기

민감한 데이터 보안 위험 및 보호 고려 사항에 대한 자세한 내용은 다음 게시물과 동영상을 참조하십시오.

Informatica Data Privacy Management

Informatica Master Data Management–Customer 360

백서: 지능형 데이터 프라이버시

Bloor Research: 민감한 데이터 찾기

한국 인포매티카 06611 서울시 서초구 서초동 강남대로 465 교보타워 B동 13층 대표 전화: +82 2 6293 5019

IN09_0520_03409