Informatica

백서

하이브리드 환경을 위한 데이터 중심 보안

클라우드 및 온 프레미스 환경의 GDPR 규정 준수

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.

Informatica는 엔터프라이즈 클라우드 데이터 관리의 선두 주자로서 고객이 지능적으로 업계를 선도할 수 있도록 도와드릴 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

오늘날 대부분의 조직은 민감한 고객, 제품 및 기타 필수 데이터를 전 세계에 걸쳐 점점 늘어나는 다양한 플랫폼과 물리적 위치에 저장합니다. 비즈니스에 중요한 이러한 데이터는 대개 퍼블릭 클라우드, 온 프레미스, 그리고 SaaS(Software as a Service) 애플리케이션에 있습니다. Informatica를 예로 들면, Informatica Intelligent Cloud Services™를 통해 운영 체제, 데이터베이스 및 애플리케이션 수준에서 장애 조치 데이터 센터, 사용자 인증 및 액세스 제어, 네트워크 보안 프로토콜, 암호화, 보안 계층의 형태로 인프라 보안을 제공할 수 있습니다.[1]

하이브리드 환경은 데이터 규정 준수와 보안 팀에 새로운 과제를 제공합니다. 데이터, 사용자, 애플리케이션의 동적인 특성 때문에 조직의 중요한 데이터를 항상 추적하고, 이해하고, 보호할 수 있는 추가적인 수단이 필요합니다. 주요 클라우드 및 온 프레미스의 위반 사례와 새로운 규정(예: 일반 데이터 보호 규정(GDPR))에 따른 벌금에서 보듯이 이러한 위험은 실질적입니다.

이러한 동적 하이브리드 환경에서는 지속적인 데이터 보호 및 규정 준수를 보장할 인텔리전스와 자동화 솔루션이 필요하며, 조직은 다음과 같은 질문에 답할 수 있어야 합니다.

- 보호해야 할 데이터가 모두 어디에 있는가?
- 누가 어떤 애플리케이션에서 데이터에 액세스하는가?
- 현재의 액세스 및 사용이 규정 및 데이터 사용 정책을 준수하는가?
- 데이터 보호가 적절하며, 데이터 위험이 적정 수준으로 관리되는가, 아니면 이러한 상태가 우리가 해결할 수준보다 큰 위험을 초래할 수 있는가?

민감한 데이터를 검색하고 분류한 결과는 하이브리드 데이터 에코시스템에서 데이터 위험, 보안, 규정 준수에 관한 의사 결정을 뒷받침할 기반이 됩니다. 이 문서는 다음을 가능하게 하는 데이터 중심 접근 방식과 함께 하이브리드 환경의 보안 고려 사항과 전략의 틀을 제공합니다.

- 분석, 자동화 및 AI(인공 지능)를 적용하여 하이브리드 환경의 모든 소스에서 민감한 데이터를 식별하고 보호(대시보드 및 보고용 단일 인터페이스 사용)
- 계속 진화하는 데이터 거버넌스 및 보안 규정 준수
- 감사에 대해 준비
- 이상한 사용자 행동이 발생하면 핵심 이해 관계자에게 알림

Informatica Data Masking 및 Informatica Secure@Source®는 이러한 기능을 수행하는 데 뛰어난 기능을 제공하여 하이브리드 에코시스템의 모든 민감한 데이터 소스에 통합된 데이터 중심 보안 계층을 추가합니다.

[1] Monahan, David, 'Informatica Cloud Security Architecture Overview(Informatica Cloud 보안 아키텍처 개요', EMA(Enterprise Management Associates), 2016년 3월.

하이브리드 환경을 위한 데이터 보안

연구 조사 기업인 IDC는 2015년 10제타바이트에 불과하던 데이터가 증가하여 2025년에는 세계에서 180제타바이트의 데이터가 생성될 것으로 전망했습니다.[2] 모든 산업 분야의 조직들이 데이터의 정확성, 가용성, 보안에 의존하여 수익을 창출하고, 고객에게 서비스를 제공하며, 생산성을 늘리고, 기타 미션 크리티컬한 비즈니스 프로세스를 지원하고 있습니다.

또한 데이터의 양과 사용량이 지속적이고 급격하게 증가하면서 여러 사일로, 온 프레미스 및 클라우드에서 다양한 데이터 형식으로 민감한 데이터도 늘어날 것입니다. 이러한 상황 때문에 기존 데이터 보안 방법이 쓸모 없게 되어 조직 전체에서 데이터 보안에 대한 새로운 접근 방식이 요구되고 있습니다.[3]

여기에 조직에서 사용하는 대부분의 데이터가 외부 소스에서 오고 있다는 분명한 동향도 확인됩니다. 따라서 데이터가 조직에 유입되는 시점에, 즉 여러 시스템 및 분석용으로 확산되기 전에 이 데이터의 민감성을 파악하는 것이 중요합니다. 그러나 대부분의 회사는 모든 민감한 데이터가 어디에 있는지 정확하게 파악할 수 없습니다. 특히 이러한 데이터가 비정형 형식이거나 다양한 온 프레미스 및 클라우드 애플리케이션, 관계 데이터베이스, 데이터 웨어하우스 어플라이언스, 빅 데이터 소스에 퍼져 있는 경우에는 더욱 그렇습니다. 이처럼 소재가 파악되지 않으면 조직의 위험이 증가합니다. 이러한 이유로 데이터 위반은 현재 최고의 IT 보안 위험이 되었습니다.[4]

민감한 데이터의 확산과 더불어 데이터 위반이 증가하면서, 조직은 다음과 같은 핵심 기능이 있는 데이터 중심 보안 제품이 포함된 위험 완화 전략을 개발해야 합니다.

- 조직 전체에서 민감한 데이터를 찾고 분류할 수 있는 모든 데이터 소스에 대한 가시성
- 위반을 줄이기 위해 민감한 데이터에 대한 보호 메커니즘을 구현하는 기능
- 자동화 및 AI를 사용하여 거의 실시간으로 사용자 행동을 모니터링하고 이상 행동을 보고하는 기능이 포함된 최신 데이터 보안 및 개인 정보 보호 규정 준수 기능
- 민감한 데이터 관리를 위한 다양한 분석 시각화 툴.
- 감사 준비를 위한 투명하고 강력한 보고 기능

Gartner는 2020년까지 데이터 중심 감사 및 보호 제품이 40%의 대기업에서 이질적이고 서로 고립된 데이터 보안 툴을 대체할 것이며, 이에 따라 현재의 5% 미만에 불과한 비율이 증가할 것으로 전망했습니다.[5] Informatica Data Masking 및 Informatica Secure@Source를 비롯한 이러한 데이터 중심 보호 솔루션은 위험 상태의 데이터에 대해 중앙 집중식 뷰를 제공하므로, 조직의 모든 핵심 이해 관계자가 거버넌스 정책 및 규정의 요구사항에 따라 민감한 데이터의 이동을 추적하고 보호 메커니즘을 적용할 수 있습니다.

[2] '2016 IoT Midyear Review – 모두가 볼 수 있는 지금까지의 성적표', IDC, 2016년 8월 4일.
[3] '데이터 중심 감사 및 보호를 위한 시장 가이드', Gartner, 2017년 3월 21일.
[4] '데이터 규정 위반 및 민감한 데이터의 위험', Ponemon Institute, 2016년 2월.
[5] '데이터 중심 감사 및 보호를 위한 시장 가이드', Gartner, 2017년 3월 21일.

민감한 데이터를 보호하기 위한 4가지 요소 전략

'민감한 데이터 위험'은 민감한 데이터의 손실로 인한 결과이며, 이러한 손실의 가장 큰 원인은 데이터 위반입니다. 일반적으로 잘못 알려진 점은 그저 민감한 데이터를 찾는 것만으로 위험을 충분히 해결할 수 있다는 것입니다. 그러나 이러한 데이터를 찾아 분류하는 것은 포괄적인 위험 해결 전략의 첫 단계에 불과합니다.

다음 단계는 데이터를 찾고 분류 분석을 거친 결과에 따라 조직의 위험을 평가하고, IT 조직뿐 아니라 모든 핵심 이해 관계자가 참여하여 위험을 줄일 수 있는 전략과 함께 데이터 거버넌스 정책을 적용하는 자동화된 제어 기능을 결정하는 것입니다. 전략에는 조직 전체에서 규정 준수, 대시보드 및 감사 보고를 위한 민감한 데이터의 다양한 분석 시각화, 모든 민감한 데이터 유형의 보호 기능을 제공하는 강력한 데이터 중심 보안 제품을 조달하고 구현하는 것도 포함되어야 합니다. 이렇게 선택한 데이터 중심 보안 제품은 하이브리드 환경(퍼블릭 클라우드, SaaS 애플리케이션, 온 프레미스 애플리케이션 및 데이터베이스, 비정형 데이터, 데이터 웨어하우스 어플라이언스)에서, 모든 소스에서 유입된 민감한 데이터도 보호해야 합니다.

1. 검색 및 분류

일반적인 검색 방식은 기존 소스를 검토하고 질문을 전송하는 것입니다. 하지만 매우 수동적인 이 방식은 사용자 행동을 실제로 모니터링하지 않고 자체 보고에 의존하므로, 귀중한 시간과 리소스를 많이 사용하고 가끔 부정확하고 오래된 결과를 가져오므로 적절하지 않습니다.

조직은 스스로에게 다음과 같은 질문을 해야 합니다.

- 우리는 어떤 데이터를 저장하고, 누가 이 데이터에 액세스하며, 어떤 목적으로 액세스하는가?
- 우리는 사용자 권한 및 데이터 권한을 어떻게 관리하는가?
- 우리는 민감한 데이터를 어떻게 보호할 것이며, 적절한 제어 기능이 준비되어 있는가?

검색 및 분류 규정 준수를 위한 기타 고려 사항은 다음과 같습니다.

- 데이터 환경(온 프레미스 데이터베이스와 클라우드 데이터베이스, 애플리케이션 및 비정형 데이터 포함)을 정의하고 이해합니다.
- 외부 소스의 데이터를 관리할 계획을 세웁니다.
- 어떤 시스템이 민감한 데이터를 포함할지 매핑합니다.
- 에코시스템에서 데이터의 이동을 매핑할 수 있는 솔루션을 조달하면서, 분석 및 보고 툴로 거의 실시간 뷰를 유지합니다.

2. 규정 준수

조직은 데이터 위험을 식별하고, 모니터링하고, 해결하여 데이터 개인 정보 보호 및 보안 규정을 준수합니다. 조직은 이를 넘어 규정 준수를 위험에 빠뜨릴 수 있는 데이터 액세스나 이동을 모니터링하고, 분석하고, 알려야 합니다.

2018년 5월 25일부터 시행된 GDPR은 유럽 연합의 모든 개인을 위해 데이터 보호를 강화하고 통일하려는 목적으로 도입되었습니다. 이에 따라 국제적인 기업의 규제 환경이 단순화되었습니다. 하지만 많은 기업이 아직 이 규정에 대비하지 못해 향후 충분하게 규정을 준수하지 못하게 됩니다. 그러나 규정을 준수하지 않을 경우 큰 벌금이 부과되고 평판에 해가 됩니다. 반대로, 규정 준수는 민감한 데이터 개인 정보 보호 및 보안 차별화 요소로 경쟁 우위의 기회를 제공할 수 있고, 데이터 중심 디지털 변혁 성과를 촉진할 수도 있습니다.

조직은 GDPR와 관련된 '데이터 도메인'이 포함된 데이터 저장소를 식별하는 지능형 정책을 개발해야 합니다. 이러한 정책은 여러 요소를 고려하고, 어떤 조합이 개인 정보 보호 위협을 제기할지 결정하는 로직이 포함되어 있어야 합니다.

3. 보호

2017년에는 1,120건의 데이터 위반이 있었으며 거의 총 171백만 개의 레코드가 공개되었습니다.[6] 인프라 수준 보안에 대한 대규모 투자에도 불구하고 중요한 데이터가 취약한 상태로 남아 있는 적은 분명합니다. 조직은 지속적으로 고위험 데이터를 보호하고, 의심스러운 행동과 중요한 데이터 자산의 무단 사용이나 이동을 파악하며, 해결책을 자동화하고 오케스트레이션해야 합니다.

조직은 중요한 데이터 위험을 식별하고 기존 사이버보안 툴이 아닌 데이터 중심 제어를 통해 이러한 위험을 해결해야 합니다. 예를 들어, 이러한 제어에는 데이터 마스킹 및 암호화 솔루션이 포함됩니다. 뿐만 아니라, 조직은 사용자 액세스와 행동을 모니터링해야 합니다. 과도한 데이터 액세스나 비정상적인 행동은 사용자가 개인 정보 보호 정책을 준수하지 않고 있거나 이들의 자격 증명이 도난당했음을 의미합니다.

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.

[6] '2016년 데이터 위반 카테고리 요약', Identity Theft Resource Center, 2016년 12월 31일.

결론

사용자, 전 세계 데이터 센터 서버, 여러 클라우드 애플리케이션에 기밀 데이터를 전송하는 모든 하이브리드 환경을 보호하기 위해서는 최고의 인프라 보안 프로토콜이 필요합니다. 계속되는 데이터 위반 공격과 증가하는 규정 준수 요구사항은 조직이 민감한 데이터를 식별하고, 분석하고, 보호하는 적절한 프로세스와 툴을 구현해야 함을 보여주고 있습니다.

보안 위험이 커지고 정기적으로 데이터 위반이 발생하는 현재 환경에서 기업은 강력한 디지털 보안 전략을 개발하여 민감한 데이터에 대한 위험을 지속적으로 모니터링하고, 분석하여, 해결해야 합니다. 데이터를 거의 실시간으로 모니터링하여 잘못된 사용이나 위반, 과도한 액세스, 비정상적인 행동 또는 국경 간 전송의 징후가 있는지 파악해야 합니다. Informatica Data Masking 및 Informatica Secure@Source 같은 데이터 중심 보안 솔루션을 사용하면 조직에서 데이터 위험 형세를 개선하여 데이터 위반이나 내부의 잘못된 사용으로 인한 영향을 줄이고, 지역 및 업계 규정의 엄격한 요구사항을 충족하도록 할 수 있습니다.

권장 사항

1. 위험 평가를 수행하여 민감한 데이터가 어디에 있는지, 이러한 데이터가 데이터 에코시스템을 통해 어디까지 전파되는지, 그리고 어떤 민감한 데이터 세트가 가장 취약한지를 명확히 파악하십시오.
2. 평가 결과에 따라, 조직에서 가장 민감한 데이터의 상위 10가지 소스에 대해 우선 순위를 정한 후 해당 소스를 보호하기 위한 전략 및 제품을 결정하고 데이터 보안을 위한 전략을 구현하십시오.
3. 조직의 규정 준수 정책 및 GDPR 규정 준수의 책임이 있는 핵심 이해 관계자를 정의하고, 문서화한 후, 배포하십시오. 2018년 5월 이후의 상황을 고려하여 전략 계획을 구축하십시오.

추가 정보

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

- '감지 및 보호: 보안에 대한 데이터 중심 접근 방식', Informatica, 2017년 4월.
- '데이터 규정 위반 및 민감한 데이터의 위험', Ponemon Institute, 2016년 2월.

Informatica

한국 인포매티카, 한국인포매티카 06611 서울시 서초구 서초동 강남대로 465 교보타워 B동 13층, **대표 전화:** +82 2 6293 5001

IN09_0418_03429