Informatica 빅 데이터 보안 솔루션

조직은 민감한 데이터의 위치, 보호, 볼륨, 확산, 사용 및 가치를 평가함으로써 위험 기반의 뷰를 생성하여 보안 투자의 우선 순위를 지정하고 데이터 보호 리소스 및 프로세스에 집중할 수 있습니다.

빅 데이터 분석 정보와 결정의 토대가 되는 지능형 데이터 보안

안전한가요? 소비자, 정부기관 및 상업 조직은 민감한 데이터의 안전과 규정 준수에 대해 항상 걱정합니다. 데이터 규정 위반 확산은 '만약(If)'이 아니라 '언제(When)'가 관건임을 잘 보여주고 있습니다. GDPR(일반 개인정보보호법)과 같은 새로운 기밀 유지 규정에는 데이터의 기밀 유지와 데이터 사용을 보장하는 특별 요건이 명시되어 있습니다. 경계 보안은 합리적인 보호를 제공하지만, 고도의 기술을 보유한 조직화된 공격자의 강력한 침투를 막지는 못합니다. 따라서 이제 데이터 보안을 위한 새로운 사전 대책을 마련해야 합니다.

빅 데이터의 장점을 활용하여 고객 및 운영에 대한 이해도가 높은 조직에게는 특별한 기회가 주어집니다. 데이터는 누구나 이용할 수 있다는 특성상 조직 전반의 여러 직무와 직원이 이용하도록 허용하면서도 데이터 오용 또는 데이터 유출 위험을 면밀히 관리할 수 있습니다. 처음부터 새로운 보안 경계를 추가하면 공격을 막고 데이터 중심의 기밀 유지 규정을 준수하며 규정 위반 복원력을 개선할 수 있습니다. 이 새로운 경계인 데이터 경계는 조직에서 가장 중요한 자산인 민감한 개인 데이터에 대한 보호와 리소스에 초점을 두고 있습니다. 하지만 새로운 경계로는 데이터를 보호하기에 충분하지 않습니다.

따라서 이제는 데이터 보안을 데이터 중심에서 살펴봐야 합니다. 조직은 민감한 데이터의 위치, 보호, 볼륨, 확산, 사용 및 가치를 평가함으로써 위험 기반의 뷰를 생성하여 보안과 규정 준수 투자의 우선 순위를 지정하고 데이터 보호 리소스와 프로세스에 집중할 수 있습니다. 또한, 실무자는 민감한 데이터의 위험을 감소시키기 위해 최상의 수정 방안에 대한 통찰력을 제공하는 지역, 애플리케이션 및 서버에 따른 자세한 데이터 분석을 사용할 수 있습니다.

데이터가 빅 데이터 환경으로 이동하기 전에 위험 분석 및 수정을 함으로써 조직은 데이터 기밀 유지 및 보안에 지장을 주지 않고 데이터 환경을 확대할 수 있습니다. 민감한 데이터를 지속적으로 분석하는 조직은 위험을 효과적으로 관리할 수 있습니다.

데이터 중심 보안은 데이터 분석 및 인텔리전스를 추가하여 민감한 데이터를 식별하고 데이터 자체에 대한 보호를 제공합니다. 또한, 조직은 인지된 위험에 따라 빅 데이터 구축에 기존의 보안 솔루션을 배포할 수 있습니다.

빅 데이터 보안 솔루션

빅 데이터를 위한 Informatica의 지능형 데이터 보안 솔루션에는 수상 경력에 빛나는 Informatica Secure@Source® 및 데이터 마스킹 솔루션이 포함되어 있습니다. Secure@Source는 민감한 데이터를 발견, 분석 및 시각화하는 프로세스를 자동화하므로 보안, 규정 준수 및 기밀 유지 팀은 민감한 데이터 위험을 신속하게 파악하고 데이터를 적절하게 제어하면서 올바른 정책을 적용할 수 있습니다. 이 솔루션은 위험에 대한 민감한 데이터를 정의, 검색 및 분석하는 정밀한 프로세스로 비용과 시간이 많이 드는 수동 데이터 감사를 대체합니다.

Informatica의 데이터 마스킹 솔루션을 통해 조직은 보고, 분석 및 미션 크리티컬 애플리케이션에 대한 데이터를 식별 방지 조치하고 민감도를 낮춰 기밀 유지 및 규정 문제에 대응할 수 있습니다. 데이터 마스킹은 암호화를 넘어 조직이 고객 및 운영 애플리케이션에 대해 사용하는 데이터를 보호합니다.

핵심 장점

규제 준수 가속화

규정에 있어 시스템, 부서, 역할 및 지역 전반의 데이터 보관, 확산, 보호 및 활용에 따른 위험을 정확히 이해하는 것이 필요합니다. 데이터가 있는 위치, 이에 대한 액세스 권한을 가진 사람 그리고 데이터 제어를 위해 마련한 수단을 파악해야 합니다. 조직이 빅 데이터의 기하급수적인 성장과 급증에 직면하면서 이는 점점 더 어려워지고 있습니다.

데이터 중심 보안은 규제 대상 데이터에 대한 위험 기반 분석을 제공하고
데이터가 이동하는 엔드포인트, 네트워크 및 애플리케이션뿐만이 아니라 데이터 자체도 보호하므로
언제든지 데이터를 찾고, 분류하고, 분석하고, 보호할 수 있습니다.

비즈니스의 속도로 민감한 데이터 보호

계속 증가하는 데이터 저장소를 잘 관리하는 동시에 비즈니스 요건에 방해가 되지 않도록 하려면 어려움이 따를 수 있습니다. 다이나믹 데이터 마스킹을 통해 데이터 식별을 불가능하게 하고 민감도를 저하시키면 유연성이 생기게 됩니다. 동적 데이터 마스킹은 미션 크리티컬 애플리케이션의 기밀을 유지해 주고 고속 엔진은 사용자 처리량에 영향을 주지 않습니다. 영구 데이터 마스킹은 컨텍스트와 참조 무결성을 유지하면서도 데이터를 익명화하므로 테스팅, 분석, 지원 환경에서 데이터를 사용할 수 있습니다.

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.

민감한 데이터의 위험을 찾아서 분석

다수의 복잡한 데이터 기밀 유지 관련 법과 산업 규정에서는 데이터 위험에 대한 정확한 이해는 물론, 특정 조건이 언제 충족되는지에 대한 알림도 필요합니다. 사용자 활동 및 권한을 분석하여 위험도가 높은 사용자를 식별하고, 데이터 계보(Lineage)를 시각적으로 추적하고, 비즈니스 우선 순위 및 거버넌스에 따라 민감한 데이터에 대한 위험에 액세스합니다.

Informatica Big Data Security를 통해 조직에서는 더 많은 소스와 데이터 플랫폼에서 위험을 높이지 않고도 더 많은 빅 데이터를 사용할 수 있습니다. Informatica의 고유한 메타데이터 기반 AI(인공 지능) 방식의 데이터 보안을 통해 완전 자동화된 체계적인 방식으로 빅 데이터를 완벽하게 보호할 수 있습니다.

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

IN08_0318_03022