

Assured Controls



- 01 소개
- 02 거세지는 규제외 파고
- 03 압박에 놓인 업종들
- 04 5단계 계획
- 05 결론



O1

소개



협업은 현대 비즈니스의 원동력입니다. 팀, 지역, 조직 전반에서 데이터를 공유하면 혁신을 촉진하고, 팀 생산성을 높이며, 비즈니스 성장을 가속화할 수 있습니다. 그러나 이러한 개방성은 종종 데이터 보안 및 규정 준수 요구사항과 충돌하여 비즈니스에서 해결해야 할 복잡한 과제를 야기하기도 합니다.

이는 비즈니스에 큰 부담이 될 수 있습니다. 2024년 한 해 동안만 해도 유럽연합 내 개인 정보 보호법(GDPR) 위반 사례가 277건 발생해 총 11억 9천만 유로에 달하는 과징금¹이 부과되었습니다. 이 중에서 대표적인 사례로는 Meta가 EU 사용자의 데이터를 적절한 보호 조치 없이 미국으로 이전하여 12억 유로 과징금²을 처분을 받은 것으로, 규정 미준수가 기업에 초래할 수 있는 재정 및 평판 위험을 여실히 보여줍니다.

이러한 과제의 핵심에는 데이터 주권이 있습니다. 데이터 주권이란 데이터가 저장되는 위치, 데이터에 액세스하는 방법 및, 데이터를 처리할 권한이 있는 사용자를 제어할 수 있는 능력을 의미합니다. EU, 미국 등 전 세계 지역에서 규정이 진화함에 따라 주권 유지가 점점 더 중요해지고 있습니다. 조직은 나날이 복잡해지는 지역 법규를 준수하면서 무단 액세스로부터 데이터를 보호해야 하며, 이는 데이터 보호 이니셔티브에 대한 내부적 저항에 직면하는 경우가 많은 CIO, CISO, 규정 준수 책임자에게 중대한 과제입니다.

출처: 1. <https://www.enforcementtracker.com/?insights> 2. https://www.edpb.europa.eu/news/news/2023/12-billion-euro-fine-facebook-result-edpb-binding-decision_en

Google Workspace의 Assured Controls는 조직에 데이터를 리전별로 격리할 수 있는 옵션을 제공하여 조직이 엄격한 규정을 충족하기 위해 데이터가 처리되고 저장되는 위치(예: EU 또는 미국)를 선택할 수 있도록 합니다. 세분화된 관리 제어를 통해 데이터를 무단 액세스로부터 안전하게 보호하는 동시에 안전하고 원활한 협업을 지원합니다.

이 가이드에서는 데이터를 보호하고 규정 준수 문제를 정면으로 해결하기 위한 실용적인 로드맵을 제공합니다. 현재 환경 평가부터 고급 제어 구현에 이르기까지 데이터 주권의 복잡성을 탐색하는 데 필요한 인사이트와 도구를 얻을 수 있습니다.



협업이 이루어지는 환경에서 데이터 주권을 확보하려면 조직은 다음을 수행해야 합니다.

01

데이터가 저장되고 처리되는 위치를 제어할 수 있습니다.

02

승인된 당사자만 액세스할 수 있도록 합니다.



02

거세지는 규제의 파고



전 세계 정부는 개인 정보를 보호하고 민감한 정보에 대한 현지 통제를 보장하기 위해 더 엄격한 데이터 보호법을 도입하고 있습니다. 이러한 프레임워크는 비즈니스가 정보를 관리하는 방식을 재편하고 있으며, 규정 준수 및 혁신을 위한 새로운 기회를 창출하는 동시에 규정 미준수에 수반되는 위험성을 높이고 있습니다.





유럽연합: GDPR 및 유럽연합 인공지능법

개인 정보 보호법(GDPR)은 데이터 개인 정보 보호에 대한 글로벌 기준을 제시합니다. 특히 유럽 경제 지역(EEA) 외부에서 개인 정보를 저장, 처리, 전송하는 방식에 대한 엄격한 통제를 의무화합니다. 조직은 규정 준수를 보장하기 위해 표준 계약 조항 또는 이에 상응하는 보호 조치와 같은 적절한 보호 장치를 구현해야 합니다. GDPR은 비즈니스의 소재지와 관계없이 EU 시민에게 상품이나 서비스를 제공하거나 EU 시민의 행동을 모니터링하는 비즈니스에 적용됩니다.



유럽연합 인공지능법(EU AI Act)은 AI에 관한 세계 최초의 법적 프레임워크로, 유럽에서 AI의 위험을 규제하고 신뢰할 수 있는 AI 사용을 촉진합니다. 이 법은 기업의 소재지와 관계없이 EU 시장 내에서 AI를 개발하거나 배포하는 모든 비즈니스에 적용됩니다. AI 시스템은 다음의 4가지 위험 수준으로 분류됩니다.

수용 불가 위험

안전과 권리를 위협하는 AI 애플리케이션 (예: 사회적 평점, 생체 인식 감시)을 금지했습니다.

위험도 높음

의료, 법 집행 기관 등 중요한 부문의 AI는 위험 평가 및 인간 감독을 포함한 엄격한 규정을 준수해야 합니다.

투명성 위험

챗봇 및 생성형 AI와 같은 AI 시스템은 AI 생성 생성 콘텐츠를 명확하게 알려야 합니다.

위험이 거의 없거나 전혀 없음

위험도가 낮은 AI(예: 스팸 필터, AI 기반 게임)에는 제한이 적용되지 않습니다.



미국: HIPAA, CCPA, CDPA

미국에는 연방 차원의 일원화된 데이터 개인 정보 보호법이 없지만 부문별 및 주 차원의 규정이 다음과 같은 중대한 의무를 부과합니다.

HIPAA

의료 서비스 제공업체, 보험사 및 유관 비즈니스에 적용되며 엄격한 개인 정보 보호 및 보안 조치를 통해 환자 정보를 보호합니다.

CCPA(캘리포니아)

소비자에게 개인 정보에 대한 액세스, 삭제, 판매 거부 권한을 비롯한 다양한 권리를 부여합니다. 특정 수익 또는 데이터 기준점을 충족하는 비즈니스에 적용됩니다.

CDPA(버지니아)

CCPA와 유사하게 이 법은 소비자 개인 정보 보호를 목표로 하지만 데이터 수집 최소화과 투명성을 강조합니다.

아시아 태평양: APPI 및 PIPA

- 01 일본의 개인 정보 보호법(APPI): 일본 시민의 데이터를 처리할 때 동의 또는 그에 상응하는 보호 조치를 요구하는 국경 간 데이터 전송에 중점을 둡니다.
- 02 대한민국 개인 정보 보호법(PIPA): 데이터의 국경 간 이전을 제한하며 위반 시 엄격하게 처벌하는 등 강력한 요구사항을 시행합니다.

남미: 브라질의 LGPD

브라질의 Lei Geral de Proteção de Dados(LGPD)는 GDPR을 준용하며 데이터 처리에 대한 엄격한 동의를 요구하고 위반 시 무거운 처벌을 내립니다. 브라질 시민과 관련된 데이터를 처리하는 비즈니스에 적용됩니다.



초국가적 복잡성

데이터를 국제적으로 이전하려면 여러 프레임워크를 준수해야 합니다.

진화하는 요구사항

GDPR, LGPD와 같은 법률이 계속 발전함에 따라 조직은 규정 준수를 위해 이에 적응해야 합니다.

부문별 특성

규정은 종종 중복되지만 업종별 위험과 필요에 따라 니즈에 따라 달리 적용됩니다.

프레임워크 전반의 공통 과제

지역적 차이는 있지만, 기업들은 보편적인 과제에 직면합니다.

이러한 프레임워크는 데이터 주권의 법적 근간을 마련해 주지만, 민감한 정보를 처리하는 업종에 매우 큰 영향을 미치기도 합니다. 금융, 의료, 기술 등의 분야에서 이러한 고유한 과제를 어떻게 해결하고 있는지 자세히 알아보세요.



3

압박에 놓인
업종들

데이터 주권 문제는 모든 업종에 동일한 방식으로 영향을 미치지 않습니다. 민감한 데이터를 다루는 특정 업종의 경우 그 특성상 모든 움직임이 강력하게 규제되므로 더 큰 영향을 받게 됩니다.

금융, 의료, 정부, 기술과 같은 부문에서 주권 확보는 단순히 규정 준수 요건을 충족하는 것 이상의 의미를 지닙니다. 이는 중요한 애셋을 보호하고, 이해관계자와의 신뢰를 구축하며, 점점 더 복잡해지는 환경에서 운영이 원활하고 안전하게 유지되도록 보장하는 것입니다.

 공유

금융: 경쟁 환경 속 신뢰 보호

금융 기관은 고객 데이터의 민감한 특성과 글로벌 경제에서 차지하는 역할로 인해 항상 엄격한 규제 환경에 놓여 있습니다. GDPR과 같은 규정은 데이터 저장 및 액세스에 대한 철저한 제어를 요구하며, 오픈뱅킹 이니셔티브는 혁신을 촉진하기 위해 고객 데이터를 서드 파티 제공업체와 안전하게 공유할 것을 요구합니다.



셜리 프랭클린

주요 고려사항:

초국가적 과제

여러 관할권에 걸쳐 금융 데이터를 관리하는 것은 위험을 초래하며, 특히 서로 다른 규제 요건을 가진 지역 간에 데이터가 이동할 때 더욱 그러합니다.

기존 시스템

많은 은행이 고급 암호화 또는 역할 기반 액세스와 같은 최신 규정 준수 조치를 구현하기 어렵게 만드는 오래된 인프라에 의존하고 있습니다.

평판 위험

신뢰가 모든 것을 좌우하는 업종에서는 단 한 번의 보안 침해나 규정 준수 실패만으로도 심각한 재정 및 평판적 손실을 볼 수 있습니다.

세분화된 액세스 제어 및 현지화된 데이터 처리와 같은 솔루션을 구현하면 금융 조직은 고객의 신뢰를 보호하면서도 자신 있게 규정 준수 표준을 충족할 수 있습니다.



헬스케어: 개인 정보 보호와 발전 사이의 균형

의료 분야에서 환자 개인 정보 보호는 법적 의무이자 윤리적 약속입니다. 의료 업종은 민감한 의료 기록을 보호하면서도 생명을 구할 수 있는 연구 협업을 지원하기 위해 섬세한 균형을 유지해야 합니다.

주요 고려사항:

규제 중복

의료 서비스 제공업체는 미국의 HIPAA부터 EU의 GDPR에 이르기까지 데이터 저장, 암호화 및 액세스에 대한 각기 다른 기준으로 인해 초래된 '거미줄 규제'를 헤쳐나가야 합니다.

국경을 초월한 협업

종종 국제 데이터 공유가 필요한 연구 기관에 있어 규정 준수는 더 복잡한 문제입니다. 예를 들어 글로벌 임상 시험을 위해 익명 처리된 환자 데이터를 공유하려면 현지 데이터 주권법을 준수해야 합니다.

운영상의 차질

오래된 시스템과 사일로화된 데이터는 규정 준수 감사 중에 비효율성과 위험 증가로 이어지는 경우가 많습니다.

엔드 투 엔드 암호화, 실시간 감독 도구와 같은 강력한 데이터 보호 조치를 통해 의료 조직은 규정 준수를 충족하는 동시에 혁신과 협업을 촉진할 수 있습니다.

정부 기관: 시민 신뢰 및 국가 안보 확보

정부 기관은 세금 기록부터 국가 안보 정보에 이르기까지 방대한 양의 민감한 시민 데이터를 관리합니다. 이러한 데이터를 보호하는 것은 규정상의 의무를 준수하는 것일 뿐만 아니라 대중의 신뢰와 국가 안보에 관한 문제이기도 하므로 그 중요성이 매우 큼니다.



주요 고려사항:

지정학적 위험

각국의 정부 기관은 사이버 위협과 외국 행위자의 압력 등 고유한 과제에 직면해 있으며, 이로 인해 데이터 상주 구현과 주권 확보가 필수적입니다.

투명성 vs 보안

개방성과 엄격한 데이터 제어의 필요성 사이에서 균형을 맞추는 것은 대중의 신뢰를 유지하는 데 매우 중요합니다.

지역별 법률

정부 기관은 유럽의 GDPR 또는 데이터 현지화를 요구하는 현지 규정과 같이 중복되는 규정을 준수해야 합니다.

엔드 투 엔드 암호화, 엄격한 액세스 제어와 같은 데이터 주권 도구를 사용하면 공공 부문 조직은 투명성이나 운영 효율성을 저해하지 않으면서 데이터를 보호할 수 있습니다.

기술: 엄격한 감시 속에서 혁신

기술 기업은 글로벌 확장성과 지역별 규정 준수 사이에서 국경을 넘어 방대한 양의 사용자 데이터를 처리합니다. 이러한 조직의 경우 데이터 상주는 규정 준수 문제일 뿐만 아니라 지식 재산을 보호하고 고객 신뢰를 유지하는 데도 매우 중요합니다.

“데이터가 지역별로 구분되어 있지 않거나 다른 기술 제공업체에 의해 처리되면 유럽과 국가는 물론, Airbus에도 위험이 발생합니다. 그러한 위험은 당사가 감당할 수 없을 것입니다.”

세바스티앙 오비노, Airbus

주요 고려사항:

글로벌 도달범위, 현지 규칙

Airbus와 같은 기업은 민감한 정보를 보호하고 주권 규정을 준수하기 위해 리전화된 데이터 처리의 중요성을 강조합니다.

확장 가능한 솔루션

기술 조직은 규정 준수를 저해하지 않으면서 전 세계로 확장할 수 있는 시스템을 구현해야 합니다.

새로운 위험

급격한 혁신은 서드 파티 애플리케이션 통합부터 충분히 제어되지 않은 액세스에 이르기까지 예상치 못한 취약점으로 이어지는 경우가 많습니다.

세분화된 관리 제어와 고급 보안 조치를 통해 기술 기업은 혁신이나 성장을 저해하지 않고도 이러한 과제를 해결할 수 있습니다.



04

5단계 계획

데이터 주권 확보를 위해서는 고유한 니즈, 업종, 위치에 맞춘 체계적인 접근방식이 필요합니다. 이 가이드에서는 데이터 환경을 제어하고, 규정을 준수하며, 조직의 규정 준수 전략에 대한 신뢰를 구축하는 데 도움이 되는 5가지 실행 가능한 단계를 설명합니다.

01

환경 평가

데이터가 저장된 위치, 액세스 권한이 있는 사용자, 적용되는 규정을 파악하는 것부터 시작하여 격차를 식별합니다.

02

데이터 리전 선택

데이터 저장 및 처리를 현지화하여 규제 요건에 부응하는 동시에 운영 유연성을 유지합니다.

03

액세스 제어 개선

권한을 조정하여 적절한 사람만 적절한 데이터에 액세스할 수 있도록 하여 데이터 노출을 최소화합니다.

04

데이터 보호 강화

보안 조치를 강화하고 민감한 정보를 보호하여 진화하는 사이버 위협에 한발 앞서 대응합니다.

05

보고 및 감독

지속적인 모니터링과 보고를 통해 끊임없이 변화하는 규제 환경에서 선제적으로 대응하고 규정 준수를 유지합니다.



01

환경 평가

모든 여정은 현재 위치와 목표를 파악하는 것에서 시작됩니다.

데이터 주권을 탐색하려면 먼저 조직이 속한 업종을 규제하는 외부 규정과 조직 내부 데이터 환경의 현실을 이해해야 합니다. 데이터가 저장되는 위치, 액세스 방식, 규정 준수를 위해 필요한 사항을 파악하고 현재 조직 환경의 격차를 식별하기 위한 것입니다.



규칙 파악

GDPR, ISO, SOC와 같은 글로벌 프레임워크는 규정 준수를 위한 기반을 마련합니다. 하지만 이러한 규정은 독립적으로 존재하는 것이 아니라 조직의 특정 운영을 이에 맞춰 조정할 것을 요구합니다.

GDPR(유럽)

표준 계약 조항과 같은 적절한 보호 장치가 마련되어 있지 않은 경우 유럽 경제 지역(EEA) 내에서 엄격한 상주를 요구합니다. 유럽 고객을 보유한 조직의 경우 개인 정보가 정확히 어디에 저장되고 전송되는지 파악하는 것이 중요합니다.

유럽연합 인공지능법 (유럽 연합)

EU 인공지능법은 EU 내에서 AI에 대한 공통 규제 프레임워크를 수립하기 위한 유럽연합 규정입니다. AI 시스템과 모델을 여러 범주로 분류하고 각 범주에 서로 다른 요구사항을 적용하는 이 규정은 2024년 8월 2일부터 법적 효력을 발휘하기 시작했습니다.

DORA(유럽 연합)

디지털 운영 복원력 법(DORA)은 금융 기관의 IT 보안을 강화하기 위한 기술 표준을 제시합니다. 유럽 감독 당국(ESA)이 제정하고 유럽 위원회가 채택한 이 규정은 금융 부문과 ICT 서드 파티 제공업체의 운영 복원력에 관한 규칙을 통합합니다.

SOC 규정 준수(미국)

서비스 조직 제어(SOC) 보고서는 보안, 가용성, 기밀성과 같은 신뢰 원칙에 중점을 둡니다. 미국공인회계사협회(AICPA)에서 제정한 이러한 표준을 충족하려면, 특히 미국에 기반을 둔 조직이나 미국 법인과 거래하는 조직의 경우 엄격한 내부 감사와 운영 투명성이 필요합니다.

ISO 표준(전 세계)

국제표준화기구(ISO)에서 관리하고 전 세계적으로 인정받는 정보 보안 관리 프레임워크를 제공합니다. 이러한 표준은 EU, 미국, 아시아 태평양과 같은 지역에서 운영되는 다국적 조직이 일관된 보안 정책을 수립하는 데 필수적입니다.



조직 데이터 감사

다음 단계는 내부적으로 데이터 환경을 매핑하는 것입니다. 데이터가 저장된 위치, 액세스 권한이 있는 사용자, 현재 조직 시스템의 격차를 파악하는 것은 규정 준수 전략 수립의 기초가 됩니다.

이는 예를 들면 다음과 같습니다.

- 의료 서비스 제공업체는 민감한 환자 데이터가 여러 클라우드 서비스에 다양한 수준의 암호화로 저장되어 있음을 발견할 수 있습니다. 연구를 위한 국경 간 데이터 공유는 GDPR(유럽) 및 HIPAA(미국) 규정 준수를 더욱 복잡하게 만듭니다.
- 이 경우 데이터 감사를 통해 규제 요구사항을 충족하기 위해 반드시 해결해야 하는 암호화되지 않은 기록이나 불분명한 액세스 권한과 같은 위험을 파악할 수 있습니다.

이러한 인사이트를 외부 규정과 일치시킴으로써 조직은 규정 준수 의무와 운영 현실 사이의 격차를 해소할 수 있습니다.





팀 구성

데이터 주권은 단순히 기술적인 과제가 아닌 협업이 필요한 과제입니다. 따라서 적절한 교차 기능팀을 구성하는 것이 중요합니다.

- **IT 리더**는 기술 인프라를 매핑하고 암호화 또는 스토리지 격차를 해결할 수 있습니다.
- **법무팀**은 지역별 규제 요구사항을 해석하고 계약에 규정 준수 요구사항이 반영되도록 할 수 있습니다.
- **각 사업부**는 액세스 권한 및 워크플로 중단과 같은 사항이 일상적인 운영에 미치는 실질적인 영향을 파악하는 데 도움이 될 수 있습니다.

이 팀은 협력하여 각 지역의 GDPR, SOC 또는 ISO와 같은 프레임워크의 요구사항에 맞게 내부 프로세스를 조정해야 합니다.

선제적 계획 수립

규정이 나날이 진화하는 것처럼, 비즈니스 니즈 또한 그렇습니다. 지금 이 5가지 단계를 수행하면 조직은 수동적인 규정 준수에서 벗어나 미래 성장을 지원하는 프레임워크를 구축할 수 있습니다.

예를 들어 **Google Workspace의 Assured Controls**와 같은 솔루션을 도입하면 데이터 상주 및 액세스 요구사항을 충족하기 위한 기반을 마련하여 유연성을 유지하면서 규정 준수를 보장할 수 있습니다.



데이터 상주 및 액세스 제어

02

데이터 상주는 단순히 데이터가 저장되는 위치를 의미하는 것이 아니라 성능, 확장성, 규정 준수 사이의 균형을 유지하면서 데이터가 저장, 액세스, 처리되는 방식을 제어할 수 있도록 보장하는 것을 말합니다.

대량의 민감한 정보를 처리하는 조직의 경우 Google Workspace의 Assured Controls와 같은 도구를 사용하면 운영 중단 없이 규정 준수를 간소화할 수 있습니다.

“비용이 많이 들고 복잡한 서드 파티 통합 없이도 원활하게 광범위한 리전 내 데이터 처리를 분석할 수 있었습니다. 심지어 이를 어떠한 오작동이나 지연 문제없이 일상적인 업무처럼 수행할 수 있었죠.”

로만 스파트가르, Randstad 글로벌 협업 부문
제품 책임자

현지 데이터 상주 vs 유연성

많은 조직이 엄격한 데이터 상주 요구사항과 운영의 민첩성 사이에서 적절한 균형을 맞추기 위해 노력하고 있습니다. 일례로 글로벌 조직은 현지 규제와 성능 요구사항을 동시에 충족시켜야 하는 경우가 많습니다.

이는 규정을 준수하면서도 협업을 방해하는 사일로화된 시스템 구축을 피할 방법을 찾아야 하는 문제를 발생시킵니다. Google Workspace의 Assured Controls는 클라우드 확장성을 유지하면서 데이터가 저장되고 처리되는 위치를 정의할 수 있는 세분화된 유연성을 제공하여 이 문제를 해결합니다. 다국적 기업의 경우 성능 저하 없이 개별 팀, 부서 또는 리전에 대한 데이터 상주 정책을 설정할 수 있습니다.

데이터 처리: 스토리지 그 이상

많은 조직이 데이터가 저장되는 위치에만 집중하고 데이터가 처리되는 위치는 간과합니다. 데이터가 처리되는 위치는 GDPR과 같은 프레임워크에서 중요한 규정 준수 요소입니다. 데이터 처리란 데이터가 사용, 분석 또는 공유되는 방식을 의미하며, 단순한 스토리지보다 더 많은 감독이 필요한 경우가 많습니다. Assured Controls는 스토리지 그 이상의 기능을 제공합니다. 스토리지와 처리 현지화를 모두 지원하므로 조직은 엔드 투 엔드 주권 요구사항을 충족할 수 있습니다.





미국 의료 규정 준수 방법 탐색

HIPAA와 같은 연방법에서 환자 데이터 보호에 대한 전국적인 표준을 제시하지만, 주마다 다른 법률이 추가적인 복잡성을 가져옵니다. 캘리포니아의 CCPA 및 버지니아의 CDPA와 같은 규정은 데이터 개인 정보 보호, 소비자 권리, 보관 기간에 대한 더 엄격한 요구사항을 적용합니다. 현지화된 데이터 처리는 의료 서비스 제공업체가 이러한 중복되는 의무를 자신 있게 헤쳐나가는 데 도움이 됩니다.

규제 변화에 대비

데이터 주권은 끊임없이 움직이는 표적과 같습니다. 정부는 기존 규정을 계속해서 개선하고 새로운 규정을 도입하여 기업에 불확실성을 야기합니다. 따라서 오늘의 규칙만을 충족하도록 설계된 경직된 시스템은 내일의 변화에 적응하기 어려울 수 있습니다. Google Workspace의 Assured Controls는 규정 변화에 따라 데이터 상주 정책을 조정할 수 있는 유연성을 제공합니다. 지역 간 데이터 마이그레이션이든 액세스 제어 개선이든 목표는 주권 상태가 변화에 맞춰 유지되도록 하는 것입니다.





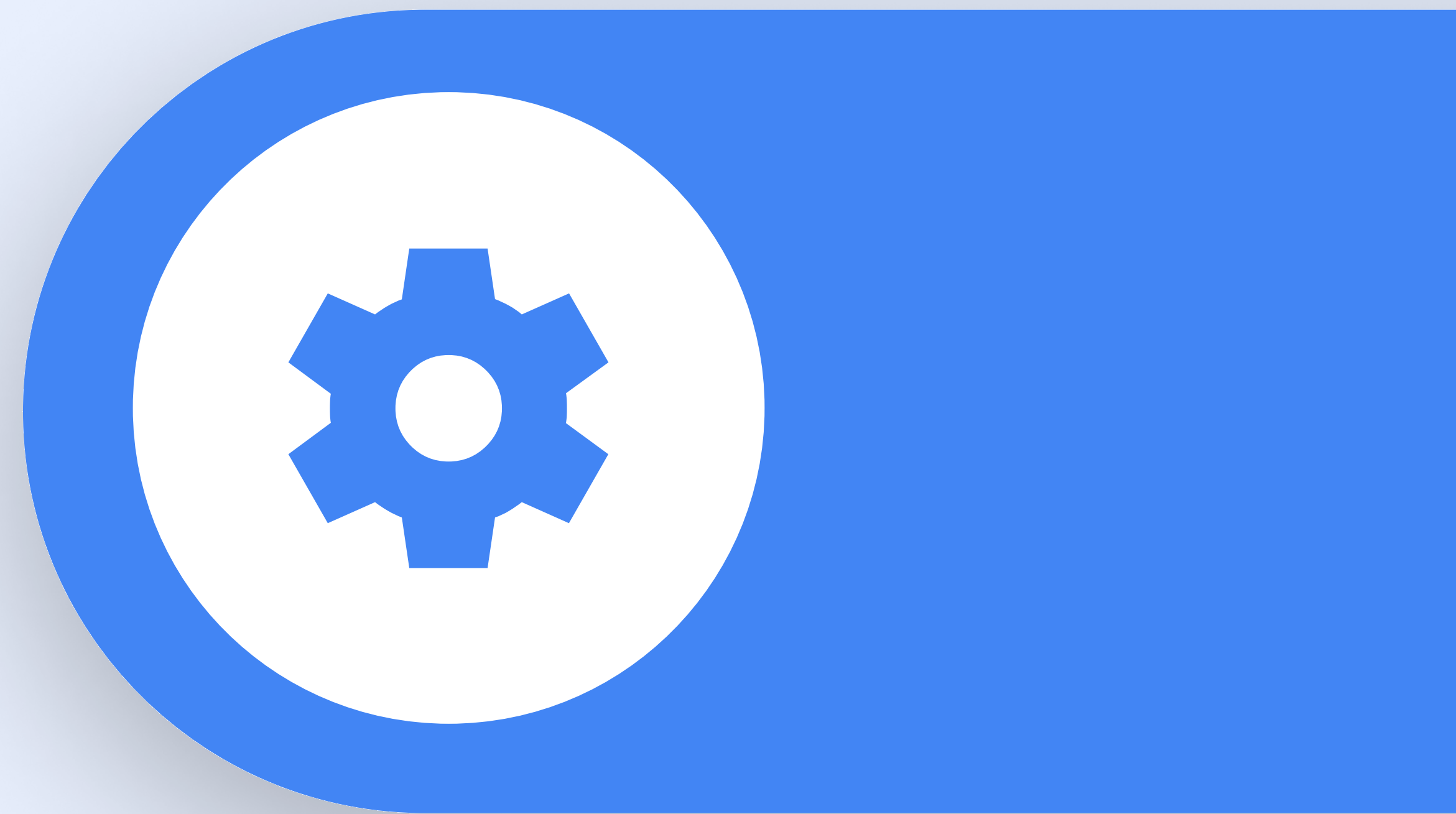
03

액세스 제어 개선

안전한 데이터 저장을 구현했다면, 다음 단계는 액세스를 동등한 수준으로 보호하는 것입니다. 최소 권한의 원칙을 적용하면 조직은 민감한 정보에 실제로 필요한 사람만 액세스할 수 있도록 보장할 수 있습니다. 조직은 누가 무엇을 볼 수 있는지 엄격하게 관리하여 실수로 인한 유출, 내부 오용, 서드 파티 취약점의 위험을 줄일 수 있습니다.

액세스 제어가 중요한 이유

무분별한 액세스는 오늘날의 환경에서 점점 더 큰 위험이 되고 있습니다. 과도한 내부 권한 부여는 유출 및 오류 위험을 증가시키고, 서드 파티 액세스는 규정 준수의 복잡성을 더하며, GDPR, HIPAA 및 기타 프레임워크와 같은 규정은 민감한 정보에 액세스할 수 있는 사용자에게 대한 더 엄격한 감독을 요구합니다.



액세스 권한을 조정하는 방법

조직은 적절한 도구를 통해 더 스마트하고 안전한 액세스 정책을 시행할 수 있습니다.



제로 트러스트 프레임워크

'아무도 신뢰하지 말고 모든 것을 검증하라'는 원칙에 따라 내부 사용자를 포함한 모든 사용자, 기기, 연결을 인증하고 승인합니다.

액세스 투명성 및 승인

서드 파티 액세스에 명시적인 승인이 필요한 워크플로를 구현합니다. Google Workspace의 액세스 승인과 같은 도구를 사용하면 지원팀이 완전한 가시성과 제어 기능을 갖춘 상태에서 꼭 필요한 경우에만 데이터에 액세스할 수 있습니다.

역할 기반 액세스 제어 (RBAC)

권한을 특정 역할에 맞게 조정하면 불필요한 노출을 최소화할 수 있습니다. 예를 들면 다음과 같습니다.

- 재무팀은 결제 시스템에 액세스할 수 있지만 인사 기록에는 액세스할 수 없습니다.
- 의료 서비스 제공자는 환자 진료 데이터는 볼 수 있지만 병원 행정 자료는 볼 수 없습니다.
- 지원팀은 명시적인 승인을 받은 후 제한된 기간 동안만 데이터에 액세스할 수 있습니다.

클라이언트 측 암호화

보안 계층을 추가하면 비즈니스에서 자체 암호화 키를 관리하여 클라우드 제공업체조차도 민감한 정보에 액세스하지 못하도록 할 수 있습니다.

조직은 세분화된 액세스 제어로 보안 및 규정 준수와 협업을 위한 최신 업무 환경 사이에서 균형을 맞출 수 있습니다. 다음 단계에서는 보안 조치를 강화하여 위험을 더욱 줄이고 조직이 진화하는 사이버 위협에 앞서 나갈 수 있도록 하는 방법을 살펴보겠습니다.

 공유

액세스 제한은 보안뿐만 아니라 더 스마트한 운영을 위한 것입니다.

성능:

최종 사용자와 가까운 곳에 데이터를 저장하면 지연 시간이 줄어들고 생산성이 향상되며 팀이 어디에 있든 원활하게 작업할 수 있습니다.

규정 준수:

데이터를 지역 내에 보관하면 법적 위험을 피하고 GDPR, HIPAA 및 기타 진화하는 규정과 같은 프레임워크를 준수할 수 있습니다.



보안 및 데이터 손실 방지(DLP)

04

데이터를 안전하게 저장하고 액세스 제어를 개선했다면 다음으로 중요한 단계는 진화하는 위협으로부터 조직을 보호하는 것입니다. Google Workspace의 Assured Controls는 고급 클라이언트 측 암호화, 세분화된 액세스 제어, 강력한 DLP(데이터 손실 방지) 도구를 제공하여 데이터가 저장, 전송, 사용에 이르는 모든 단계에서 안전하게 보호되도록 합니다.





중요한 이유

오늘날의 조직은 점점 더 복잡해지는 보안 문제에 직면해 있습니다.

- **외부 위협:** 피싱 공격, 멀웨어, 무단 액세스 시도가 점점 더 정교해지고 있습니다. 조직은 악의적인 행위자로부터 민감한 정보를 보호하기 위해 선제적으로 준비해야 합니다.
- **내부 위험:** 과도한 권한 부여, 실수로 인한 공유, 인적 오류는 여전히 주요 데이터 유출 원인입니다. 액세스를 강화하고 기술적 보호 장치를 내장하면 이러한 취약점을 완화하는 데 도움이 됩니다.

브라우저 확장 프로그램, 생산성 앱, 서드 파티 통합과 같이 직원이 매일 사용하는 도구는 의도치 않은 취약점이 될 수 있습니다. 검증되지 않은 앱에 민감한 정보를 공유하거나, 과도한 권한을 제공하거나, 악성 소프트웨어에 노출되는 등의 위험은 보안 태세에 보이지 않는 복잡성을 더하게 됩니다.

그렇다면 직원이 필요한 도구를 사용해 원활하게 작업할 수 있도록 하면서 중요한 데이터를 보호하려면 어떻게 해야 할까요?

Google Workspace의 Assured Controls를 사용하면 조직은 유연성과 보안 사이에서 균형을 유지할 수 있습니다.

- **세분화된 권한:** 서드 파티 도구의 액세스 범위를 제한하여 민감한 정보에 대한 액세스를 차단하고 불필요한 노출을 줄입니다.
- **클라이언트 측 암호화:** 직원이 클라우드 서비스 전반에서 공동작업을 수행하는 경우에도 처음부터 끝까지 데이터를 보호합니다. 암호화는 승인되지 않은 앱이나 서비스가 민감한 정보를 읽을 수 없도록 보장합니다.
- **가시성 및 승인:** 어떤 도구가 사용되고 있는지 지속적으로 감독하고, 잠재적인 위험을 조기에 식별하며, 외부 액세스는 정말로 필요한 경우에만 승인하도록 합니다.

이러한 제어 기능이 내장된 Assured Controls는 조직이 보안을 최우선으로 유지하면서 직원이 안전한 도구로 자유롭게 혁신할 수 있도록 지원합니다.

보호 계층 추가

Assured Controls는 제로 트러스트 프레임워크와도 원활하게 통합됩니다. '아무도 신뢰하지 말고 모든 것을 검증하라'는 철학을 바탕으로 모든 사용자, 기기, 연결이 민감한 정보에 액세스하기 전에 사용자 인증 정보를 증명하도록 요구합니다.

파일을 공유하기 전에 암호화하거나 서드 파티 액세스에 여러 단계의 승인을 요구하는 등 기술적 제어를 통해 보안이 항상 선제적으로 이루어지도록 보장합니다.



DLP가 중요한 이유

데이터 손실 방지(DLP) 정책은 보안을 강화하는 데 중요한 역할을 합니다. 그 효과는 다음과 같습니다.

- **데이터 이동 모니터링:** 시스템을 통해 이동하는 민감한 정보를 추적하여 유출 또는 무단 공유를 식별하고 해결합니다.
- **맞춤 정책 설정:** 규칙을 정의하여 규정 준수 의무를 위반하는 데이터 공유를 자동으로 차단, 알림 또는 신고합니다.
- **민감한 카테고리 보호:** 개인 식별 정보(PII), 금융 데이터, 지식 재산과 같은 특정 데이터 유형을 식별하고 보호합니다.



보안은 종종 협업의 장애물이나 추가적인 hurdles로 여겨집니다. 하지만 실제로는 비즈니스가 자신 있게 운영할 수 있도록 돕습니다. Assured Controls의 고급 암호화, 선제적인 DLP 정책, 승인 프로세스를 통해 조직은 민감한 정보 보호와 협업 지원 사이에서 적절한 균형을 유지할 수 있습니다.

다음 섹션에서는 끊임없이 변화하는 규제 환경에서 보고 및 감독이 어떻게 선제적으로 대응하고 규정을 준수하는 데 도움이 되는지 살펴보겠습니다.

보고 및 감독: 데이터 가시성을 통한 신뢰 구축

05

데이터 주권 구현의 여정은 제어 조치가 마련된 후에도 멈추지 않습니다. 제어가 작동한다는 것을 증명하는 것이 중요합니다. 보고 및 감독을 통해 조직은 데이터 전략을 모니터링, 감사, 조정할 수 있으며 암호화, 액세스, 스토리지 전반에서 지속적으로 가시성을 확보하여 규정 준수를 달성할 뿐만 아니라 유지할 수 있습니다. Randstad와 같은 조직의 경우 실시간 보고 도구를 사용하면 감사를 간소화하고 원활한 규정 준수를 보장할 수 있습니다.

“데이터 리전 구현은 EU 내 개인 정보 처리를 위한 전략상의 큰 변화였습니다. 차질없이 진행이 되었으며 그 어떤 운영상의 문제도 없었습니다.”

로만 스파트가르, Randstad 글로벌 협업 부문
제품 책임자



보고는 제어로 쌓은 피라미드와 같습니다. 즉, 각각의 계층에서 신뢰를 구축해 나가는 시스템입니다.

클라이언트 측 암호화:

보안의 기본은 암호화입니다. 하지만 암호화는 일관되게 적용되어야만 효과가 있습니다. 보고 도구는 민감한 정보가 생성부터 저장까지 엔드 투 엔드로 암호화된 상태를 유지하는지 확인하며, 감사 추적은 암호화 키가 사용자의 제어하에 있는지 검증합니다.

컨텍스트 인식 액세스:

데이터 액세스는 제어뿐만 아니라 모니터링도 되어야 합니다. 실시간 보고는 비정상적인 액세스 위치, 로그인 시도 실패, 업무 시간 외 활동과 같은 이상 징후를 표시합니다. 이러한 데이터 가시성을 통해 위험이 실질적 문제로 발전하기 전에 해결할 수 있습니다.

세분화된 액세스 제어:

감독 도구를 사용하면 누가, 언제, 왜 무엇에 액세스할 수 있는지 확인할 수 있습니다. 명확한 액세스 로그와 보고서를 생성하여 과도한 권한이 부여된 역할을 파악하고, 임시 액세스(예: 지원팀용)를 모니터링하며, GDPR 및 HIPAA와 같은 프레임워크를 준수할 수 있습니다.

현지 데이터 스토리지:

엄격한 데이터 상주 요구사항이 적용되는 업종에서는 투명성이 무엇보다 중요합니다. 보고 도구는 데이터가 특정 주 또는 리전 등 있어야 할 곳에 저장되어 있는지 확인하여 IT팀과 규제 기관 모두에게 필요한 증거를 제공합니다.

데이터 리전:

보고 대시보드는 데이터가 저장, 처리 및 액세스되는 위치를 명확히 보여줌으로써 규제가 변화하거나 글로벌 운영 규모가 확대됨에 따라 기업이 정책을 조정할 수 있도록 지원합니다. 이러한 점은 새로운 시장으로 진출을 고려 중인 기업에게 특히 유용합니다.

제로 트러스트 아키텍처:

제로 트러스트는 추측을 배제하고 항상 검증하는 것을 의미합니다. 보고 도구는 모든 액세스 요청, 기기, 사용자 작업을 기록하여 데이터 정책을 준수하는 동시에 활동을 더 쉽게 모니터링하고 의심스러운 패턴을 감지할 수 있도록 합니다.

데이터 가시성이 중요한 이유

강력한 보고 시스템이 없다면 규정 준수는 추측에 의존할 수 밖에 없습니다. 조직은 규제 요구사항을 충족하는 동시에 새로운 위협에 대응할 수 있는 민첩성을 보유해야 합니다. Google Workspace의 Assured Controls는 조직이 자신 있게 데이터 전략을 모니터링하고 검증하며 조정하는 데 필요한 감독 도구를 제공합니다. 조직이 자신 있게 데이터 전략을 모니터링하고 검증하며 조정하는 데 필요한 감독 도구를 제공합니다.

- **감사 간소화:** GDPR, HIPAA, SOC 2와 같은 프레임워크 부합 여부를 확인하는 규정 준수 보고서를 생성합니다. Assured Controls는 IT팀과 규정 준수팀의 보고를 간소화하여 버튼 클릭 한 번으로 모든 데이터 활동에 대한 상세하고 감사 가능한 로그를 제공합니다.
- **빈틈없는 관리:** 조기 위험 파악을 위한 실시간 대시보드와 모든 활동, 승인 또는 변경을 추적하는 투명한 활동 로그를 제공합니다. 따라서 팀은 위험을 해결하고, 거버넌스를 입증하고, 신뢰를 유지하는 데 필요한 데이터 가시성을 확보할 수 있습니다.

Assured Controls는 실시간 인사이트, 감사에 최적화된 보고 시스템, 투명한 활동 로그를 제공합니다. 이는 단순한 규정 준수 지원을 넘어 조직이 규정 준수 요구사항에 선제적으로 대응할 수 있도록 지원합니다. 조직은 모니터링, 검증, 조정 도구를 활용하여 데이터에 대한 제어권을 확보할 수 있습니다. 동시에 간과하기 쉬운 부분이나 진화하는 위협으로 인한 위험을 줄일 수 있습니다.

강력한 보고 체계는 규정 준수를 단순한 형식적 절차에서 전략적 우위로 탈바꿈합니다. 활동을 모니터링하고, 제어를 검증하며, 선제적으로 대응할 수 있는 도구를 사용해 조직은 신뢰를 구축하는 동시에 진화하는 위험과 규제에 자신 있게 대응할 수 있습니다.





05

결론



Google Workspace의 Assured Controls

이 기능은 고급 규정 준수 도구와 클라우드의 유연성 및 확장성을 결합하여 조직이 최소한의 노력으로 데이터 주권 달성에 훨씬 더 가까이 다가갈 수 있도록 지원하며 데이터 저장, 처리, 액세스에 대한 세분화된 제어 기능을 제공하는 동시에 비즈니스가 진화하는 규정에 적응할 수 있도록 돕습니다. 항공우주 분야의 지식 재산 보호에서 금융 분야의 민감한 고객 데이터 관리에 이르기까지 Assured Controls를 사용하면 조직은 협업, 성장, 혁신에 더 집중할 수 있습니다.

[자세히 알아보기 →](#)