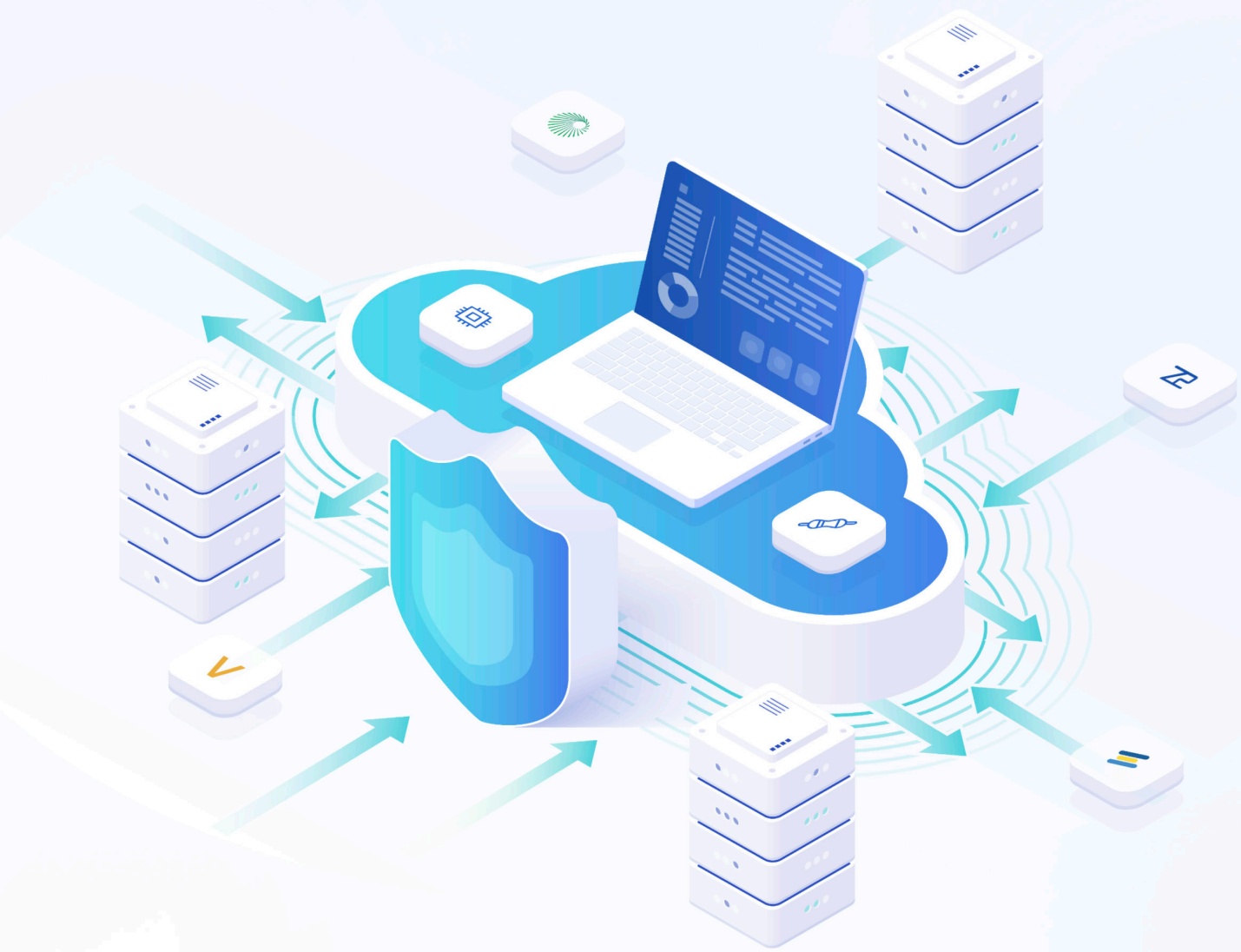
ALTIUM 365

보안 접근 방식 및 사례



CONTENT

소개

Altium 365는 설계, 데이터, 협업을 단일 보안 클라우드 환경으로 통합하는 전자 개발 플랫폼입니다. 전자 개발의 전체 라이프사이클을 지원하도록 구축되었으며, 엔지니어링 팀이 더 빠르고 효율적으로 대규모 작업을 수행하는 데 필요한 최신 인프라를 제공합니다. Altium Agile 및 Altium Develop에 포함된 이 플랫폼은 워크플로를 간소화하고 생산성을 향상시키며 제품 출시를 가속화합니다.

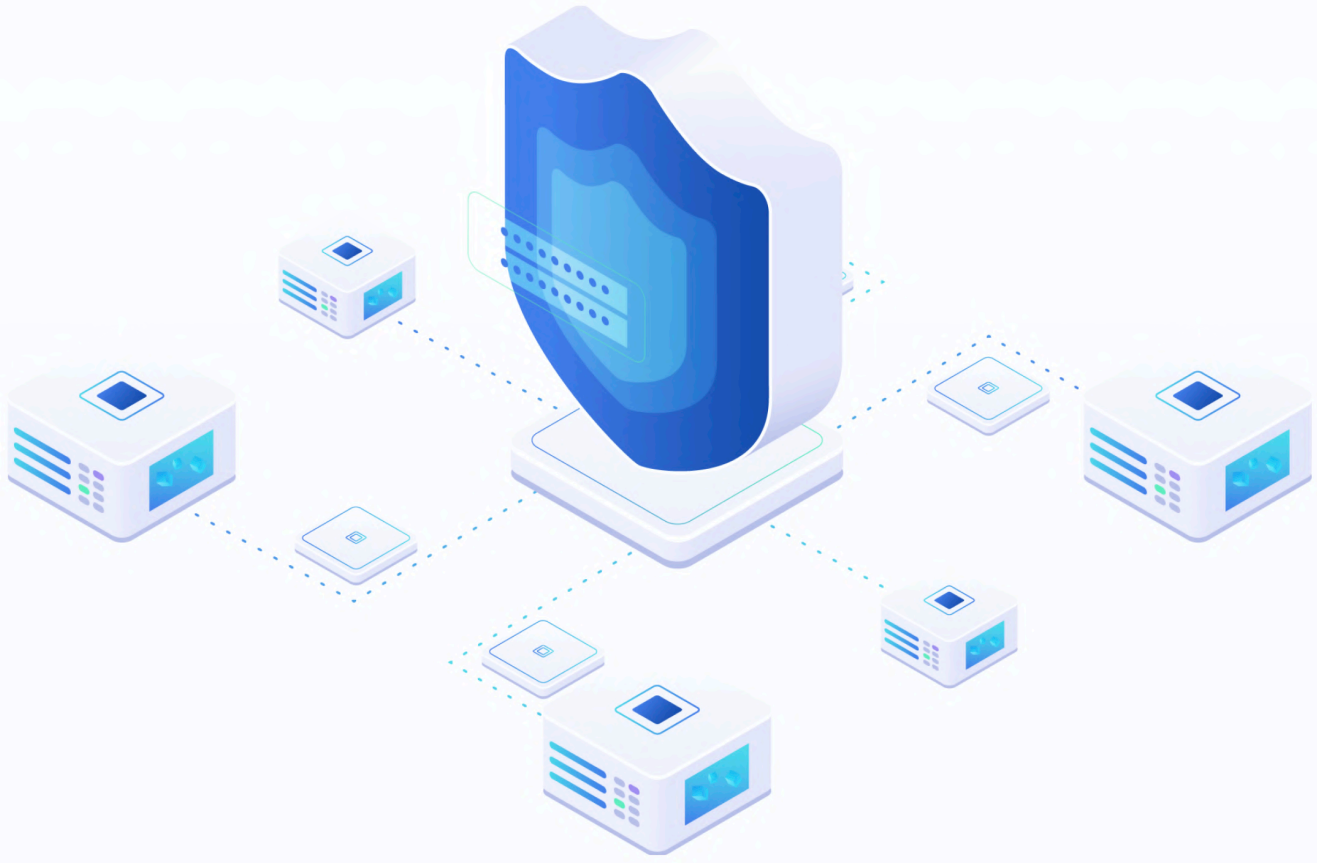
Altium은 클라우드 플랫폼의 진정한 가치가 무엇을 가능하게 하는지뿐만 아니라, 맡겨진 작업을 얼마나 안전하게 보호하는지에 의해 측정된다고 믿습니다. 보안은 Altium 365 아키텍처의 핵심에 내재되어 있으며, 플랫폼을 설계, 구축 및 운영하는 방식을 안내합니다. 이러한 노력은 현대의 사이버 보안 표준을 충족하고 지속적으로 능가하도록 이끕니다.

이 백서는 Altium 365를 뒷받침하는 광범위한 보안 조치에 대해 명확하고 투명한 정보를 제공합니다. 당사의 목표는 간단합니다. 데이터가 어떻게 보호되는지, 보안 장치가 어떻게 설계되었는지, 그리고 새로운 위협에 앞서 나가기 위해 보안 태세가 어떻게 발전하고 있는지 보여드리는 것입니다.

이 페이지를 살펴보면서 안전한 개발 관행부터 플랫폼 전반에 내장된 계층적 제어에 이르기까지, 당사의 접근 방식을 형성하는 계획, 프로세스 및 보호 메커니즘에 대한 통찰력을 얻게 될 것입니다. 당사의 엔지니어링 엄격성, 운영 규율 및 클라우드 네이티브 아키텍처가 어떻게 협력하여 모든 단계에서 데이터를 보호하는지 확인하실 수 있습니다.

궁극적으로 저희의 목표는 Altium 365에서의 협업 작업이 강력하고 지속적으로 진화하는 보안 프레임워크에 의해 보호받고 있다는 사실에서 오는 마음의 평화를 드리는 것입니다. 저희는 귀하가 창작과 혁신에 집중하실 수 있도록, 그 결과물을 보호하는 보안은 저희가 책임지겠습니다.

이 문서는 플랫폼 수준에서의 Altium 365 보안 접근 방식 및 사례를 설명하며, 특정 기능은 구독, 배포 환경(예: GovCloud) 및 고객 구성에 따라 다를 수 있습니다.



Altium 365 보안 조치

보안은 신뢰의 기반이며, 당사 고객들은 Altium 365를 사용하여 데이터, 설계, 지적 재산과 같은 가장 소중한 자산을 보호합니다. 보안은 초기 아키텍처 및 개발부터 배포와 지속적인 운영에 이르기까지 플랫폼의 모든 계층에 내장되어 있습니다. 당사의 접근 방식은 꼼꼼하고 선제적이며 지속적으로 발전하고 있어, 협업 전자 설계 개발을 위한 안전하고 탄력적인 환경을 조성합니다.

보안 주도 개발

당사는 사용자 보안을 염두에 두고 Altium 365 플랫폼과 그 기능 및 기능을 개발했습니다. 개발의 모든 단계에서 당사는 적용된 보안 조치를 엄격하게 검증합니다. 여기에는 광범위한 아키텍처 검토, 종속성 스캐닝, 코드 검토 및 동적 애플리케이션 보안 테스트가 포함됩니다. 당사의 목표는 처음부터 잠재적인 보안 취약점을 선제적으로 식별, 해결 및 방지하는 것입니다. 또한 당사는 독립적인 제3자 테스트를 활용하여 보안 프레임워크의 견고함을 보장합니다.

신뢰할 수 있는 데이터 보호

Amazon Web Services(AWS)는 Altium 365의 물리적 보안 및 안정성의 중추를 형성합니다. 당사는 고객 데이터를 AWS 리소스에만 저장하며, 데이터베이스 요구 사항을 위해 특별히 Relational Database Service(RDS)를 사용합니다. 표준 바이너리 데이터 저장을 위해 AWS S3를 사용하며, 고성능 바이너리 스토리지가 필요한 시나리오에는 FSx를 사용합니다. 고성능 검색 기능을 제공하기 위해 전용 Elasticsearch 클러스터가 사용됩니다.

Altium 365 내의 미사용 데이터는 AWS Key Management Service(KMS) 키를 사용하여 암호화됩니다. 이 키는 암호화 모듈을 승인하는 데 사용되는 미국 정부 컴퓨터 보안 표준인 FIPS 140-2 표준에 따라 검증된 하드웨어 보안 모듈을 사용합니다. 이러한 암호화 키의 사용은 기록되고 모니터링됩니다. 그런 다음 로그는 보안 정보 및 이벤트 관리(SIEM) 시스템으로 전송되어 암호화 키가 사용된 시기를 추적할 수 있습니다.

고객 데이터를 호스팅하는 Altium 365 인프라에 대한 접근은 최소 권한 원칙에 따라 승인된 인원에게만 제한됩니다. 모든 접근은 Altium의 전담 보안 팀에 의해 기록되고, 감사 가능하며, 지속적으로 모니터링됩니다.

보안 통신

Altium 365 클라이언트(웹 브라우저, Altium Designer 또는 모바일 애플리케이션)와 Altium 365 클라우드 플랫폼 간의 통신은 HTTPS 프로토콜을 사용하는 안전하고 신뢰할 수 있는 연결을 통해서만 허용됩니다. HTTPS 프로토콜은 표준 포트를 통한 안전한 인터넷 통신을 위한 표준 방식입니다.

인증 및 신원 관리

민감한 고객 데이터를 관리하는 Altium 365 서비스에 액세스하려면 사용자는 모든 요청 시 인증 과정을 거쳐야 합니다. 이 인증은 기존의 사용자 이름 및 비밀번호 입력에만 국한되지 않으며, 싱글 사인온(SSO) 시스템이나 Google 및 Facebook과 같은 ID 공급자(IdP)와도 통합됩니다. 이러한 시스템은 하드웨어 키, 스마트 카드 또는 지문과 같은 생체 인식 데이터를 포함한 다양한 자격 증명을 사용할 수 있으며, 당사는 이를 직접 제어하지 않습니다. 방법과 관계없이 모든 세션은 보안을 위해 시간 제한이 적용되며, 모든 민감한 로그인 정보는 전송 중에 안전하게 암호화됩니다.

Altium 365는 SAML 2.0 프로토콜을 사용하여 SSO를 지원합니다. 이 기능은 OneLogin, Okta, Microsoft Azure AD, Google Identity를 포함한 대부분의 최신 IdP와 통합됩니다. SCIM 프로토콜에 대한 확장된 지원을 통해 중앙 집중식 사용자 및 그룹 프로비저닝과 프로비저닝 해제를 구성할 수 있습니다. IdP에 따라 다중 요소 인증(MFA)을 사용하여 향상된 보호를 선택할 수 있습니다.

배포 및 제어

Altium 365는 웹 애플리케이션 방화벽 및 관리형 로드 밸런싱을 포함하여 인바운드 트래픽을 제어하고 검사하기 위해 계층화된 경계 보호 기능을 사용합니다. 이러한 제어 기능은 애플리케이션 서비스 전반에 트래픽을 분산하여 인터넷 연결 엔드포인트를 보호하고 가용성을 지원합니다. 프로덕션 시스템에 대한 관리자 액세스는 최소 권한 원칙에 따라 승인된 인원으로 제한되며, 기록 및 모니터링됩니다.

싱글 테넌시 및 멀티 테넌시 아키텍처

Altium 365는 각 테넌트(현재 워크스페이스 개념과 일치)가 자체적으로 격리된 데이터베이스 스키마를 제공받는 멀티 테넌시 아키텍처에서 작동합니다. 이 모델은 효율성과 확장성을 위해 공유 클라우드 인프라를 활용하면서 강력한 데이터 분리를 제공합니다. 더 깊은 수준의 격리, 사용자 지정 및 운영 제어가 필요한 조직을 위해 Altium은 애플리케이션과 해당 지원 인프라의 전용 인스턴스인 단일 테넌트 환경(STE)을 제공합니다. STE는 높은 데이터 격리, 예측 가능한 성능 및 테넌트별 구성 옵션을 제공하며, 호스팅 서비스의 편리함과 전통적으로 온프레미스 배포와 관련된 제어 기능을 결합합니다.

취약점 스캐닝

Altium 365의 프로덕션 배포는 릴리스 프로세스의 일부로 취약성 검사를 거쳐야 합니다. 결과물은 Altium의 취약성 관리 정책 및 정의된 수정 일정에 따라 수정 또는 문서화된 위험 수용을 통해 추적됩니다.

제3자 테스트

당사는 외부 제3자와 매년 협력하여 침투 테스트를 수행함으로써 진화하는 위협에 대비해 최고 수준의 보안을 유지합니다. 개발팀은 침투 테스트에서 얻은 모든 피드백을 검토하고 애플리케이션 서비스 및 인프라에 필요한 업데이트를 구현합니다. 상호 비밀 유지 계약(MNDA)이 체결된 경우, 관심 있는 당사자와 침투 테스트 보고서의 최신 요약본을 공유할 수 있습니다.

보안 모니터링 및 사고 관리

당사는 보안 사고를 조기에 탐지하고 효과적으로 대응할 수 있도록 포괄적인 로깅 및 모니터링 관행을 구현했습니다. NIST 사이버 보안 프레임워크를 기반으로, 로깅 및 모니터링은 "탐지(Detect)" 및 "대응(Respond)" 기능의 핵심 구성 요소입니다. 이러한 기능은 보안 이벤트와 취약점을 식별하고 이해하는 데 필수적이며, Altium 365의 정확성과 정밀도를 향상시킵니다. 사고 식별은 보안 팀, 시스템 및 도구가 협력하여 잠재적인 보안 사고를 인식하고 확인하는 당사의 사고 대응 프로세스에서 기본이 됩니다. 보안 사고가 식별되면 당사는 조직의 보안 및 비즈니스 목표에 부합하는 신속하고 효과적인 대응을 보장하기 위해 사고 대응 계획을 활성화합니다.

보안 인식 및 교육

Altium은 모든 신입 사원이 온보딩 중에 보안 인식 교육을 받고, 모든 직원이 매년 재교육을 받을 수 있도록 보장합니다. 인사팀은 규정 준수를 보장하기 위해 교육을 완료하지 않은 직원들을 대상으로 후속 조치를 취합니다. 또한 당사는 직원들에게 새로운 프로토콜과 잠재적인 위협을 알리는 보안 인식 알림을 정기적으로 발송합니다. 당사의 연구 개발 팀은 보안 코딩 관행에 대한 전문 교육을 받습니다. 교육 자료는 코딩 관행이나 프로그래밍 언어를 반영하기 위해 주기적으로 검토 및 업데이트됩니다.

데이터 개인정보 보호

Altium 일반 서비스 약관 및 개인정보 보호정책은 고객 데이터의 개인정보 보호 및 보안을 보장하기 위해 당사가 취하는 조치를 설명합니다. 이러한 문서와 이를 뒷받침하는 당사의 내부 절차는 일반 데이터 보호 규정(GDPR) 및 캘리포니아 소비자 개인정보 보호법(CCPA)을 비롯한 글로벌 데이터 보호 규정을 준수합니다. 이러한 준수를 통해 당사는 고객 및 비즈니스 파트너가 당사에 위탁한 정보를 포함하여 Altium이 관리하는 모든 데이터의 기밀성, 무결성 및 가용성을 보장합니다. 오늘날과 같이 경쟁이 치열한 글로벌 비즈니스 환경에서는 오류, 분실, 사기, 스파이 행위 등의 위협을 방지하기 위해 데이터 프라이버시를 유지하는 것이 매우 중요합니다. 당사의 접근 방식은 당사가 취급하는 데이터의 보안 침해를 방지하도록 설계되었습니다.

쿠키 정책

브라우저 설정을 통해 쿠키 환경 설정을 관리할 수 있습니다. 일부 브라우저에서는 쿠키를 허용할 사이트를 화이트리스트에 추가할 수 있습니다. 쿠키 환경 설정 관리에 대한 더 많은 정보를 보려면 쿠키 정책을 참조하세요.

데이터 보존 정책

Altium 365 사용을 중단하는 경우, 당사는 데이터 보존 정책에 명시된 기간에 따라 귀하의 데이터를 보관합니다. 이 기간이 만료되면 귀하의 데이터는 당사 시스템에서 삭제됩니다.

백업 및 재해 복구

Altium 365는 자동화된 백업 시스템을 사용하여 Altium 365에 저장된 모든 데이터가 백업 리전으로 복사되도록 보장하며, 수동 개입을 제거합니다. 당사는 프로덕션 서비스 및 플랫폼의 비즈니스 연속성을 지원하기 위한 포괄적인 재해 복구 계획을 보유하고 있습니다. 시스템 장애 발생 시, 당사는 각각 24시간의 복구 시점 목표(RPO) 및 복구 시간 목표(RTO)를 목표로 합니다. 이 계획은 유효성을 확인하기 위해 120일마다 검토 및 테스트되며, 재해 발생 시 서비스를 복구하기 위한 상세한 정책과 절차를 포함합니다.

자세한 내용은 Altium 365 보안 센터를 방문하여 자주 묻는 질문에 대한 답변을 확인해 보세요.

Altium 365 GovCloud

Altium 365 GovCloud는 미국에 위치한 Altium 365 클라우드 플랫폼의 전용 지역으로, AWS GovCloud 지역에서 미국인에 의해 독점적으로 운영됩니다. GovCloud 지역에서 Altium 365 워크스페이스를 선택하면 조직이 ITAR 및 EAR과 같은 미국 정부 규정을 준수하는 데 도움이 됩니다.

미국인

Altium 측 GovCloud 지역의 운영은 미국인으로만 제한됩니다. Altium 고객은 워크스페이스에 추가할 사람과 워크스페이스에 저장된 데이터에 대한 접근 권한을 부여할 사람을 결정하고 통제합니다.

데이터 보호

아웃바운드 트래픽 제어

무단 데이터 내보내기를 방지하기 위해 당사는 환경을 벗어나는 무단 아웃바운드 트래픽을 제어하고 차단하는 아웃바운드 프록시를 사용합니다.

제한된 기능

사용자 오류와 관련된 위험을 완화하기 위해 미국에서 의도치 않은 데이터 유출을 초래할 수 있는 기능을 기본적으로 비활성화했습니다.

- **워크스페이스 외부에서 공유.** 기본적으로 Altium 365 GovCloud 워크스페이스에 속하지 않은 사람과 프로젝트, 릴리스, 라이브러리 및 제조 패키지를 공유하는 기능("제조업체에 보내기" 기능)은 비활성화되어 있습니다. 이 설정은 필요한 경우 관리자가 수정할 수 있습니다.
- **Altium 365 개인 공간.** Altium 365 GovCloud 워크스페이스에 추가된 사용자는 Altium 365 개인 공간에 데이터를 저장할 수 없습니다.
- **PLM 통합.** 제3자 PLM 시스템과의 연결은 관리자가 제어하며 필요한 설정을 제공합니다.
- **클라이언트 시스템.** Altium은 Altium 365 GovCloud에 연결하는 브라우저나 CAD 도구 등 고객 측 시스템의 구성, 보안 또는 유지 관리에 대해 책임을 지지 않습니다. 고객은 이러한 시스템을 최신 상태로 유지하고 필요한 모든 업데이트와 패치를 설치해야 합니다.

미국 토양

AWS GovCloud 미국 동부 및 서부 지역은 미국 내에 거주하는 미국 시민권자 직원에 의해 운영됩니다.

접근 제어

미국 외부에서 워크스페이스에 접근

다른 국가에서 워크스페이스에 접근하려는 미국인의 접근을 포함하여 미국 외부에서 워크스페이스에 접근하는 것은 명시적으로 차단됩니다. VPN 접근에 대해 자세히 알아보려면 여기를 클릭하세요.

자세한 내용은 Altium 365 GovCloud에서 확인하세요.

규정 준수: 인증 및 규정

규정 준수는 단순히 확인란을 체크하는 것이 아니라, 우수성을 향한 헌신이자 신뢰성에 대한 약속입니다. Altium 365는 이러한 책임을 중요하게 생각하며, 당사 플랫폼이 최고 수준의 규정 준수 및 인증 표준을 충족하도록 보장합니다.

CSA STAR Level 1: 자가 평가

Security, Trust, Assurance, and Risk(STAR) 프로그램은 클라우드 컴퓨팅을 위한 강력한 보증 프레임워크를 제공하기 위해 Cloud Security Alliance(CSA)에서 시작한 이니셔티브입니다. Altium 365는 CSA의 STAR Level 1을 획득했으며, 이는 일반적으로 Consensus Assessment Initiative Questionnaire(CAIQ)로 알려진 Cloud Control Matrix(CCM) 통제 준수에 대한 자체 증명입니다. 따라서 Altium 365는 STAR Registry에 등재되어 있습니다.

SOC 2 Type 2 인증

Altium 365는 서비스 조직 제어(SOC) 2 Type 2 인증을 받았으며, 이는 당사가 보안 원칙에 대해 데이터 및 시스템 보안의 최고 표준을 준수함을 확인합니다. 이 사이버 보안 규정 준수 프레임워크는 미국공인회계사협회(AICPA)에서 개발했으며, 기업은 외부의 AICPA 공인 감사인으로부터 감사를 받아야 합니다. Altium 365는 매년 SOC 2 Type 2 감사를 수행합니다.

GDPR

당사는 데이터 개인정보 보호의 중요성을 인식하고 있으며, 일반 데이터 보호 규정(GDPR)에서 정한 엄격한 요구 사항을 준수하여 귀하의 데이터가 최대한 주의 깊고 존중하는 방식으로 처리되도록 최선을 다하고 있습니다.

ITAR 규정 준수

Altium 365 GovCloud는 고객이 국제 무기 거래 규정(ITAR)을 준수하도록 지원할 수 있습니다. 이 특수 영역은 규제가 엄격한 산업에서 운영되는 사용자의 특정 요구 사항을 충족합니다.

Altium 365 보안 및 거버넌스 기능

Altium은 조직이 민감한 설계 데이터를 보호하고, 규정 준수를 유지하며, 대규모로 액세스를 관리할 수 있도록 돕는 고급 보안, ID 및 거버넌스 기능을 제공합니다.

접근 제어

- **기본 데이터 권한**
  사용자가 플랫폼 전반에서 파일, 폴더 및 프로젝트와 상호 작용하는 방식을 정의하는 기본적인 보기 및 편집 권한입니다.
- **고급 데이터 권한**
  기본 액세스 권한을 넘어 조직 수준의 공유 규칙, 세분화된 권한 설정, 팀 간 데이터 액세스 또는 제한 방식을 결정하는 고급 상속 옵션을 포함하는 제어 기능입니다.
- **그룹 관리**
  정의된 역할에 따라 액세스를 할당하여 권한, 라이선스 및 작업 공간 가시성을 표준화하고 조직 전체에서 일관되고 확장 가능한 제어를 보장합니다.
- **외부 게스트 지원**
  외부 협업자를 초대, 그룹화 및 제한하는 방법을 제어하며, 게스트 액세스를 제한하고 안전하게 유지하는 가시성 규칙과 강제 워크플로를 제공합니다.
- **액세스 필터**
  모든 프로젝트에 걸쳐 유효한 액세스를 검색 및 감사하고, 빠른 조정과 원 클릭 게스트 제거 기능을 제공합니다.

인증 및 사용자 프로비저닝

- **조직 관리**
  사용자가 조직에 가입하는 방법, 역할이 할당되는 방법, 도메인 기반 규칙이 내부 리소스에 대한 ID 및 액세스를 제어하는 방법을 정의합니다.
- **SSO(싱글 사인온) 및 SCIM**
  기존 ID 공급자와 통합하여 인증을 중앙 집중화하고 SCIM을 통해 사용자 프로비저닝 및 프로비저닝 해제를 자동화합니다.
- **다중 요소 인증(MFA)**
  추가 인증 단계를 요구하여 계정 보안을 강화하며, 자격 증명이 유출되더라도 무단 액세스 위험을 줄여줍니다.
- **그룹 관리**
  온보딩 및 전체 수명 주기 동안 사용자를 사전 정의된 역할 및 액세스 프로필에 맞춰 조정하여 ID 프로비저닝을 지원합니다.

고급 보안

- **IP 화이트리스트**
  승인된 IP 주소 또는 범위로 플랫폼 액세스를 제한하여 신뢰할 수 있는 네트워크만 민감한 조직 데이터에 접근할 수 있도록 합니다.
- **이벤트 로그**
  워크스페이스 전반의 사용자 및 시스템 작업에 대한 가시성을 제공하여 명확한 타임스탬프 활동 기록을 통해 감사, 보안 검토 및 규정 준수 보고를 지원합니다.
- **SIEM(API)**
  Altium Agile 이벤트 데이터를 기존 SIEM에 연결하여 조직 전반의 중앙 집중식 분석, 알림 및 규정 준수 추적을 지원합니다.

당사의 최신 보안 업데이트 소식을 확인하세요

당사 플랫폼은 거버넌스를 강화하고 가시성을 높이며 현대 전자 조직의 보안 요구 사항을 지원하는 새로운 기능으로 계속 발전하고 있습니다. 보안은 여전히 기본이며, 모든 업데이트는 팀이 민감한 데이터와 규제 대상 데이터에 대한 통제를 유지하면서 신속하게 작업할 수 있도록 설계되었습니다.

전자 개발과 데이터 보호 환경이 진화함에 따라, 당사도 그에 발맞춰 발전하고 있습니다. 당사는 오늘날의 요구 사항을 충족하는 동시에 조직이 앞으로 다가올 변화에 대비할 수 있도록 실용적이고 확장 가능한 개선 사항을 제공하는 데 중점을 두고 있습니다.

제어 기능을 확장하고 모니터링을 강화하며 보호 조치를 보강하여 보안과 혁신이 일관되게 유지되도록 지속적인 개선을 진행할 예정이니 많은 관심 바랍니다.

추가 정보 및 관련 리소스를 확인하려면 altium.com

더 자세히 알고 싶으신가요? www.altium.com/platform/trust