ALTIUM 365

Approche et pratiques de sécurité

CONTENT

Introduction

Altium 365 est la plateforme de développement électronique qui unifie la conception, les design data et la collaboration dans un environnement cloud unique et sécurisé. Conçue pour prendre en charge l'ensemble du cycle de vie du développement électronique, elle fournit l'infrastructure moderne dont les équipes d'ingénierie ont besoin pour travailler plus rapidement, plus efficacement et à grande échelle. Incluse avec Altium Agile et Altium Develop, la plateforme rationalise les processus, améliore la productivité et accélère la livraison des produits.

Chez Altium, nous estimons que la véritable valeur d'une plateforme cloud se mesure non seulement à ce qu'elle permet, mais aussi à la sécurité avec laquelle elle protège le travail qui lui est confié. La sécurité est intégrée au cœur de l'architecture d'Altium 365, guidant la manière dont nous concevons, développons et exploitons la plateforme. Cet engagement nous pousse à respecter les normes modernes de cybersécurité et à constamment les dépasser.

Ce livre blanc offre une vue d'ensemble claire et transparente des nombreuses mesures de sécurité qui protègent Altium 365. Notre objectif est simple : vous montrer comment vos données sont protégées, comment nos mesures de protection sont conçues et comment notre stratégie de sécurité évolue pour anticiper les nouvelles menaces.

Au fil de ces pages, vous découvrirez les principes de planification, les processus et les mécanismes de protection qui définissent notre approche, depuis les pratiques de développement sécurisées jusqu'aux contrôles à plusieurs niveaux intégrés à l'ensemble de la plateforme. Vous découvrirez comment la rigueur de nos pratiques d'ingénierie, notre discipline opérationnelle et notre architecture cloud native conjuguent leurs efforts pour protéger vos données à chaque étape.

En définitive, notre objectif est de vous apporter la tranquillité d'esprit que procure le fait de savoir que votre travail collaboratif sur Altium 365 est protégé par un cadre de sécurité robuste, en constante évolution. Nous voulons que vous puissiez vous concentrer sur la création et l'innovation, tandis que nous nous chargeons de la sécurité qui protège vos projets.

Ce document décrit l'approche et les pratiques de sécurité d'Altium 365 au niveau de la plateforme ; les fonctionnalités spécifiques peuvent varier selon l'abonnement, l'environnement de déploiement (p. ex., GovCloud) et la configuration client.

Mesures de sécurité d'Altium 365

La sécurité est le fondement de la confiance, et nos clients s'appuient sur Altium 365 pour protéger leurs actifs les plus précieux : leurs données, leurs conceptions et leur propriété intellectuelle. La sécurité est intégrée à chaque couche de la plateforme, depuis les premières étapes de l'architecture et du développement jusqu'au déploiement et aux opérations continues. Notre approche est méticuleuse, proactive et en constante évolution, créant un environnement sécurisé et résilient pour le développement collaboratif de produits électroniques.

Développement axé sur la sécurité

Nous avons développé la plateforme Altium 365, ses fonctionnalités et ses fonctions en tenant compte de la sécurité des utilisateurs. À chaque étape du développement, nous vérifions rigoureusement les mesures de sécurité en place. Cela comprend des examens approfondis de l'architecture, des analyses de dépendances, des examens de code et des tests dynamiques de sécurité des applications. Notre objectif est d'identifier, de traiter et de prévenir de manière proactive toute vulnérabilité de sécurité potentielle dès le départ. Nous faisons également appel à des tests indépendants effectués par des tiers afin de garantir la robustesse de notre cadre de sécurité.

Protection fiable des données

Amazon Web Services (AWS) constitue le fondement de la sécurité physique et de la fiabilité d'Altium 365. Nous stockons les données client exclusivement sur des ressources AWS et utilisons Relational Database Service (RDS) spécifiquement pour nos besoins en matière de base de données. Pour le stockage de données binaires standard, nous utilisons AWS S3, tandis que FSx est employé pour les scénarios nécessitant un stockage binaire haute performance. Des clusters Elasticsearch dédiés sont utilisés pour offrir des capacités de recherche haute performance.

Les données au repos au sein d'Altium 365 sont chiffrées à l'aide de clés AWS Key Management Service (KMS). Ces clés utilisent des modules de sécurité matériels validés selon la norme FIPS 140-2, une norme de sécurité informatique du gouvernement américain utilisée pour approuver les modules cryptographiques. L'utilisation de ces clés de chiffrement est journalisée et surveillée. Les journaux sont ensuite envoyés à notre système de gestion des informations et des événements de sécurité (SIEM), ce qui nous permet de savoir quand les clés de chiffrement sont utilisées.

L'accès à l'infrastructure Altium 365 qui héberge les données client est limité au personnel autorisé, conformément au principe du moindre privilège. Tous les accès sont enregistrés, vérifiables et surveillés en continu par l'équipe de sécurité dédiée d'Altium.

Communication sécurisée

La communication entre les clients Altium 365, comme un navigateur Web, Altium Designer ou une application mobile, et la plateforme cloud Altium 365 est uniquement autorisée par l'intermédiaire de connexions sécurisées et fiables utilisant le protocole HTTPS, une méthode standard pour sécuriser les communications Internet sur les ports standard.

Authentification et gestion des identités

Pour accéder aux services Altium 365 qui gèrent des données client sensibles, les utilisateurs doivent suivre un processus d'authentification pour chaque demande. Cette authentification ne se limite pas aux saisies traditionnelles de nom d'utilisateur et de mot de passe ; elle s'intègre également aux systèmes d'authentification unique (SSO) ou aux fournisseurs d'identité (IdPs) tels que Google et Facebook. Ces systèmes peuvent utiliser divers identifiants, notamment des clés matérielles, des cartes à puce ou des données biométriques telles que des empreintes digitales, que nous ne contrôlons pas directement. Quelle que soit la méthode, toutes les sessions sont limitées dans le temps pour des raisons de sécurité, et toute information de connexion sensible est chiffrée de manière sécurisée pendant la transmission.

Altium 365 prend en charge l'authentification unique (SSO) à l'aide du protocole SAML 2.0. Cette fonctionnalité s'intègre à la plupart des fournisseurs d'identité (IdP) modernes, notamment OneLogin, Okta, Microsoft Azure AD et Google Identity. La prise en charge étendue du protocole SCIM permet de centraliser le provisionnement et le déprovisionnement des utilisateurs et des groupes. Selon l'IdP, vous pouvez opter pour une protection renforcée grâce à l'authentification multifactorielle (MFA).

Distribution et contrôle

Altium 365 utilise des protections périmétriques multicouches pour contrôler et inspecter le trafic entrant, notamment un pare-feu d'application Web et un équilibrage de charge géré. Ces contrôles contribuent à protéger les points de terminaison exposés à Internet et à assurer la disponibilité en répartissant le trafic entre les services applicatifs. L'accès administratif aux systèmes de production est réservé au personnel autorisé selon le principe du moindre privilège, et il est journalisé et surveillé.

Architecture mono-tenant et multi-tenant

Altium 365 repose sur une architecture multi-tenant dans laquelle chaque tenant, actuellement associé au concept d'espace de travail, dispose de son propre schéma de base de données isolé. Ce modèle assure une forte séparation des données tout en tirant parti d'une infrastructure cloud partagée pour garantir efficacité et évolutivité. Pour les organisations nécessitant une isolation, une personnalisation et un contrôle opérationnel accrus, Altium propose un environnement mono-tenant unique (STE) : une instance dédiée de l'application et de son infrastructure de prise en charge. STE assure une isolation élevée des données, des performances prévisibles et des options de configuration propres au tenant, combinant la commodité d'un service hébergé avec le contrôle traditionnellement associé aux déploiements sur site.

Analyse des vulnérabilités

Les déploiements en production pour Altium 365 sont soumis à une analyse des vulnérabilités dans le cadre du processus de publication. Les conclusions font l'objet d'un suivi jusqu'à leur correction ou à l'acceptation documentée du risque, conformément à la politique de gestion des vulnérabilités d'Altium et aux délais de correction définis.

Tests effectués par des tiers

Nous collaborons chaque année avec des tiers externes dans le cadre de tests d'intrusion afin de garantir le plus haut niveau de sécurité face à des menaces en constante évolution. L'équipe de développement examine tous les retours des tests de pénétration et met en œuvre les mises à jour nécessaires de nos services d'application et de notre infrastructure. Nous sommes disposés à partager avec les parties intéressées le dernier résumé exécutif de notre rapport de test de pénétration, à condition qu'un accord de confidentialité mutuel (MNDA) soit en place.

Surveillance de la sécurité et gestion des incidents

Nous avons mis en œuvre une pratique complète de journalisation et de surveillance afin de permettre la détection précoce et une réponse efficace aux incidents de sécurité. S'appuyant sur le cadre de cybersécurité du NIST, la journalisation et la surveillance constituent des éléments clés des fonctions « Détecter » et « Répondre ». Ces fonctions sont essentielles pour identifier et comprendre les événements et les vulnérabilités de sécurité, améliorant ainsi l'exactitude et la précision d'Altium 365. L'identification des incidents est fondamentale dans notre processus de réponse aux incidents, où les équipes de sécurité, les systèmes et les outils collaborent pour reconnaître et confirmer les incidents de sécurité potentiels. Une fois qu'un incident de sécurité est identifié, nous activons notre plan de réponse aux incidents afin de garantir une réponse rapide et efficace, alignée sur les objectifs de sécurité et commerciaux de l'organisation.

Sensibilisation et formation à la sécurité

Altium veille à ce que tous les nouveaux employés reçoivent une formation de sensibilisation à la sécurité lors de leur intégration, ainsi que des mises à jour annuelles pour l'ensemble du personnel. L'équipe des ressources humaines assure le suivi auprès des employés qui n'ont pas terminé leur formation afin de garantir la conformité. En outre, nous envoyons régulièrement au personnel des notifications de sensibilisation à la sécurité, l'informant des nouveaux protocoles et des menaces potentielles. Notre équipe de recherche et développement suit une formation spécialisée sur les pratiques de codage sécurisé. Le matériel de formation est régulièrement révisé et mis à jour afin de refléter les pratiques de codage ou les langages de programmation.

Confidentialité des données

Les Conditions générales d'utilisation d'Altium et la Politique de Confidentialité décrivent les mesures que nous prenons pour garantir la confidentialité et la sécurité des données client. Ces documents et nos procédures internes de soutien respectent les réglementations mondiales en matière de protection des données, notamment le RGPD et la loi californienne sur la protection de la vie privée des consommateurs (CCPA). Ce respect garantit la confidentialité, l'intégrité et la disponibilité de toutes les données gérées par Altium, y compris les informations qui nous sont confiées par nos clients et partenaires commerciaux. Dans l'environnement commercial mondial concurrentiel d'aujourd'hui, il est essentiel de préserver la confidentialité des données afin de prévenir les menaces, notamment les erreurs, les pertes, les fraudes et l'espionnage. Notre approche est conçue pour prévenir toute faille de sécurité dans les données que nous traitons.

Politique de cookies

Vous pouvez gérer vos préférences en matière de cookies dans les paramètres de votre navigateur. Certains navigateurs vous permettent d'ajouter à une liste blanche les sites dont vous acceptez les cookies. Pour plus d'informations sur la gestion de vos préférences en matière de cookies, consultez notre Politique en matière de cookies.

Politique de conservation des données

Si vous cessez d'utiliser Altium 365, vos données seront conservées conformément aux délais précisés dans notre Politique de conservation des données. Après l'expiration de cette période, vos données seront effacées de nos systèmes.

Sauvegardes et reprise après sinistre

Altium 365 utilise un système de sauvegarde automatisé afin de garantir que toutes vos données stockées dans Altium 365 soient copiées dans nos régions de sauvegarde, éliminant ainsi toute intervention manuelle. Nous disposons d'un plan complet de reprise après sinistre pour assurer la continuité des activités des services et plateformes de production. En cas de perturbation du système, nous visons un objectif de point de récupération (RPO) et un objectif de temps de récupération (RTO) de 24 heures chacun. Ce plan est examiné et testé tous les 120 jours afin de confirmer son efficacité et comprend des politiques et procédures détaillées pour rétablir les services en cas de catastrophe.

> Pour plus d'informations, veuillez consulter Centre de confiance Altium 365 et découvrir les réponses aux questions fréquemment posées.

Altium 365 GovCloud

Altium 365 GovCloud est une région dédiée de la plateforme Altium 365 cloud située aux États-Unis, exploitée exclusivement par des citoyens américains dans la région AWS GovCloud. Choisir un espace de travail Altium 365 dans la région GovCloud peut aider les organisations à se conformer aux réglementations du gouvernement américain telles que l'ITAR et l'EAR.

Personnes Américaines

Le fonctionnement de la région GovCloud du côté d'Altium est limité aux ci toyens américains uniquement. Les clients d'Altium déterminent et contrôlent les personnes qu'ils ajoutent à leur espace de travail et les personnes à qui ils accordent l'accès aux données stockées dans l'espace de travail.

Protection des données

Contrôle du trafic sortant

Afin de protéger contre l'exportation non autorisée de données, nous utilisons un proxy sortant qui contrôle et empêche le trafic sortant non autorisé de quitter l'environnement.

Fonctionnalité restreinte

Nous avons désactivé par défaut les fonctionnalités susceptibles d'entraîner involontairement la sortie de données des États-Unis, atténuant ainsi les risques liés à une erreur de l'utilisateur.

- ✓ Partage en dehors de l'espace de travail. Par défaut, le partage de projets, de versions, de bibliothèques et de packages de fabrication (fonction « Envoyer au fabricant ») avec des personnes qui n'appartiennent pas à votre espace de travail Altium 365 GovCloud est désactivé. Ce paramètre peut être modifié par les administrateurs si nécessaire.
- ✓ Espace personnel Altium 365. Les utilisateurs ajoutés à un espace de travail Altium 365 GovCloud ne peuvent pas stocker de données dans leurs espaces personnels Altium 365.
- ✓ Intégration PLM. L'administrateur contrôle la connexion aux systèmes PLM tiers et fournit les paramètres requis.
- ✓ Systèmes clients. La responsabilité d'Altium ne s'étend pas à la configuration, à la sécurité ou à la maintenance des systèmes côté client, tels que les navigateurs ou les outils de CAO, qui se connectent à Altium 365 GovCloud. Le client doit maintenir ces systèmes à jour et installer toutes les mises à jour et tous les correctifs nécessaires.

Sol américain

Les régions AWS GovCloud US-Est et US-Ouest sont exploitées par des employés qui sont des citoyens américains situés sur le sol américain.

Contrôles d'accès

Accès à Workspace depuis l'extérieur des États-Unis

L'accès à l'espace de travail depuis l'extérieur des États-Unis est explicitement bloqué, y compris pour les personnes américaines qui essaient d'y accéder depuis un autre pays. Pour en savoir plus sur l'accès au VPN, cliquez ici.

Pour plus d'informations, consultez Altium 365 GovCloud.

Conformité : Certifications et réglementations

La conformité ne se résume pas à une case à cocher ; c'est un engagement envers l'excellence et une promesse de fiabilité. Chez Altium 365, nous prenons cette responsabilité au sérieux, en veillant à ce que notre plateforme respecte les normes les plus strictes en matière de conformité et de certification.

CSA STAR Level 1 : auto-évaluation

Le programme Security, Trust, Assurance, and Risk (STAR) est une initiative de la Cloud Security Alliance (CSA) conçue pour offrir un cadre d'assurance robuste pour l'informatique en nuage. Altium 365 a obtenu le STAR Level 1 de la CSA, qui est une auto-attestation de conformité aux contrôles de la Cloud Control Matrix (CCM), plus connue sous le nom de Consensus Assessment Initiative Questionnaire (CAIQ). Altium 365 figure ainsi dans le STAR Registry.

Attestation SOC 2 Type 2

Altium 365 fait l'objet d'une attestation SOC 2 de type 2 (Service Organization Control), qui confirme que nous respectons les normes les plus strictes en matière de sécurité des données et des systèmes, conformément au principe de sécurité. Ce cadre de conformité en matière de cybersécurité a été élaboré par l'American Institute of Certified Public Accountants (AICPA) et exige que les entreprises se soumettent à un audit réalisé par un auditeur externe accrédité par l'AICPA. Altium 365 réalise des audits SOC 2 Type 2 chaque année.

RGPD

Nous reconnaissons l'importance de la confidentialité des données et nous nous engageons à respecter les exigences strictes énoncées par le Règlement général sur la protection des données (RGPD), afin de garantir que vos données soient traitées avec le plus grand soin et respect.

Conformité ITAR

Altium 365 GovCloud peut aider nos clients à se conformer aux International Traffic in Arms Regulations (ITAR). Cette région spécialisée répond aux besoins spécifiques de nos utilisateurs opérant dans des secteurs hautement réglementés.

Fonctionnalités de sécurité et de gouvernance d'Altium 365

Altium® fournit des fonctionnalités avancées de sécurité, de gestion des identités et de gouvernance qui aident les organisations à protéger les design data sensibles, à maintenir la conformité et à gérer les accès à grande échelle.

Contrôle d’accès

- **Autorisations de données de base**
  Droits fondamentaux de consultation et de modification qui définissent la manière dont les utilisateurs interagissent avec les fichiers, dossiers et projets sur l’ensemble de la plateforme.
- **Permissions avancées sur les données**
  Des contrôles qui vont au-delà des droits d’accès de base, y compris des règles de partage au niveau de l’organisation, des paramètres d’autorisation précis et des options d’héritage avancées qui déterminent la façon dont les données sont accessibles ou restreintes entre les équipes.
- **Gestion des groupes**
  Uniformise les autorisations, les licences et la visibilité des espaces de travail en attribuant l’accès en fonction de rôles définis, garantissant ainsi un contrôle cohérent et évolutif dans l’ensemble de l’organisation.
- **Prise en charge des invités externes**
  Contrôle la façon dont les collaborateurs externes sont invités, regroupés et limités, grâce à des règles de visibilité et à des processus appliqués qui garantissent un accès des invités restreint et sécurisé.
- **Filtre d’accès**
  Recherchez et auditez les accès effectifs dans l’ensemble des projets, avec des ajustements rapides et la suppression des invités en un clic.

Authentification et Approvisionnement des utilisateurs

- **Gestion des organisations**
  Définit la manière dont les utilisateurs rejoignent l’organisation, dont les rôles sont attribués et dont les règles basées sur le domaine régissent l’identité et l’accès aux ressources internes.
- **Authentification unique (SSO) et SCIM**
  S’intègre à votre fournisseur d’identité existant afin de centraliser l’authentification et d’automatiser l’approvisionnement et le déprovisionnement des utilisateurs via SCIM.
- **Authentification multifactorielle (MFA)**
  Renforce la sécurité des comptes en exigeant une étape de vérification supplémentaire, réduisant le risque d’accès non autorisé, même si les identifiants sont compromis.
- **Gestion des groupes**
  Prend en charge l’approvisionnement des identités en associant les utilisateurs à des rôles prédéfinis et à des profils d’accès lors de leur intégration et tout au long de leur cycle de vie.

Sécurité avancée

- **Liste blanche d’adresses IP**
  Restreint l’accès à la plateforme aux adresses IP ou plages approuvées, garantissant que seuls les réseaux fiables peuvent accéder aux données organisationnelles sensibles.
- **Journal des événements**
  Offre une visibilité sur les actions des utilisateurs et du système dans l’ensemble de l’espace de travail, facilitant les audits, les examens de sécurité et les rapports de conformité grâce à des enregistrements d’activité horodatés et clairs.
- **SIEM (API)**
  Connecte les données d’événements Altium Agile à votre SIEM existant, permettant une analyse centralisée, des alertes et un suivi de la conformité dans l’ensemble de votre organisation.

Restez informé de nos dernières mises à jour en matière de sécurité

Notre plateforme continue d'évoluer avec de nouvelles fonctionnalités qui renforcent la gouvernance, améliorent la visibilité, et répondent aux exigences de sécurité des organisations électroniques modernes. La sécurité reste fondamentale, et chaque mise à jour est conçue pour aider les équipes à avancer rapidement tout en gardant le contrôle des données sensibles et réglementées.

Alors que le paysage du développement de l'électronique et de la protection des données évolue, nous évoluons avec lui. Nous nous concentrons sur la fourniture d'améliorations pratiques et évolutives qui répondent aux besoins actuels tout en préparant votre organisation pour l'avenir.

Restez à l'écoute des améliorations continues à mesure que nous étendons les contrôles, approfondissons la surveillance et renforçons les protections, afin de garantir que sécurité et innovation restent alignées.

Pour plus de détails et de ressources connexes, rendez-vous sur altium.com

Vous voulez en savoir plus ? www.altium.com/platform/trust

Les informations fournies dans ce livre blanc sont exactes en date de février 2026. Veuillez noter qu'Altium 365 est une plateforme en constante évolution. Pour obtenir la dernière version de ce document, veuillez consulter cette page.