ALTIUM 365

Approccio e pratiche di sicurezza

CONTENT

Introduzione

Altium 365 è la piattaforma di sviluppo per l'elettronica che unifica progettazione, dati e collaborazione in un unico ambiente cloud sicuro. Progettata per supportare l'intero ciclo di vita dello sviluppo elettronico, offre la moderna infrastruttura di cui i team di ingegneria hanno bisogno per lavorare più rapidamente, in modo più efficiente e su larga scala. Inclusa in Altium Agile e Altium Develop, la piattaforma semplifica i flussi di lavoro, migliora la produttività e accelera la consegna dei prodotti.

In Altium, crediamo che il vero valore di una piattaforma cloud si misuri non solo da ciò che consente di fare, ma anche da quanto protegge in modo sicuro il lavoro che le viene affidato. La sicurezza è integrata al centro dell'architettura di Altium 365 e guida il modo in cui progettiamo, sviluppiamo e gestiamo la piattaforma. Questo impegno ci spinge a soddisfare e superare costantemente i moderni standard di sicurezza informatica.

Questo white paper fornisce una visione chiara e trasparente delle ampie misure di sicurezza alla base di Altium 365. Il nostro obiettivo è semplice: mostrarti come vengono protetti i tuoi dati, come sono progettate le nostre misure di protezione e come si evolve la nostra strategia di sicurezza per rimanere al passo con le minacce emergenti.

Scorrendo queste pagine, otterrai informazioni sulla pianificazione, sui processi e sui meccanismi di protezione che definiscono il nostro approccio, dalle pratiche di sviluppo sicuro ai controlli stratificati integrati in tutta la piattaforma. Scoprirai come il nostro rigore ingegneristico, la disciplina operativa e l'architettura nativa del cloud lavorano insieme per proteggere i tuoi dati in ogni fase.

In definitiva, il nostro obiettivo è darti la tranquillità che deriva dal sapere che il tuo lavoro collaborativo su Altium 365 è protetto da un solido framework di sicurezza in continua evoluzione. Vogliamo che tu sia concentrato su creazione e innovazione, mentre noi ci occupiamo della sicurezza che lo protegge.

Questo documento descrive l'approccio e le pratiche di sicurezza di Altium 365 a livello di piattaforma; le funzionalità specifiche possono variare in base all'abbonamento, all'ambiente di distribuzione (ad es., GovCloud) e alla configurazione del cliente.

Misure di sicurezza di Altium 365

La sicurezza è alla base della fiducia e i nostri clienti si affidano ad Altium 365 per proteggere le loro risorse più preziose: i dati, i progetti e la proprietà intellettuale. La sicurezza è integrata in ogni livello della piattaforma, dall'architettura e dallo sviluppo iniziali fino alla distribuzione e alle operazioni continue. Il nostro approccio è meticoloso, proattivo e in continua evoluzione, e crea un ambiente sicuro e resiliente per lo sviluppo collaborativo di prodotti elettronici.

Sviluppo orientato alla sicurezza

Abbiamo sviluppato la piattaforma Altium 365, le sue caratteristiche e funzionalità tenendo conto della sicurezza dell'utente. In ogni fase dello sviluppo, verifichiamo rigorosamente le misure di sicurezza in atto, includendo revisioni approfondite dell'architettura, scansione delle dipendenze, revisioni del codice e test dinamici di sicurezza delle applicazioni. Il nostro obiettivo è identificare, affrontare e prevenire in modo proattivo qualsiasi potenziale vulnerabilità di sicurezza fin dall'inizio. Inoltre, utilizziamo test indipendenti di terze parti per garantire la solidità del nostro framework di sicurezza.

Protezione affidabile dei dati

Amazon Web Services (AWS) costituisce la base della sicurezza fisica e dell'affidabilità di Altium 365. Archiviamo i dati dei clienti esclusivamente su risorse AWS e, nello specifico, utilizziamo il Relational Database Service (RDS) per le nostre esigenze di database. Per l'archiviazione dei dati binari standard, utilizziamo AWS S3, mentre FSx viene impiegato per gli scenari che richiedono un'archiviazione binaria ad alte prestazioni. Vengono utilizzati cluster Elasticsearch dedicati per fornire capacità di ricerca ad alte prestazioni.

I dati inattivi all'interno di Altium 365 vengono crittografati utilizzando le chiavi AWS Key Management Service (KMS). Queste chiavi utilizzano moduli di sicurezza hardware convalidati secondo gli standard FIPS 140-2, uno standard di sicurezza informatica del governo degli Stati Uniti utilizzato per approvare i moduli crittografici. L'utilizzo di queste chiavi di crittografia viene registrato e monitorato. I log vengono quindi inviati al nostro sistema di gestione delle informazioni di sicurezza e degli eventi (SIEM), permettendoci di tenere traccia di quando vengono utilizzate le chiavi di crittografia.

L'accesso all'infrastruttura Altium 365 che ospita i dati dei clienti è limitato al personale autorizzato secondo il principio del privilegio minimo. Tutti gli accessi vengono registrati, sono sottoposti ad audit e monitorati continuamente dal team di sicurezza dedicato di Altium®.

Comunicazione sicura

La comunicazione tra i client Altium 365, come un browser Web, Altium Designer o un'applicazione mobile, e la piattaforma cloud Altium 365 è consentita solo tramite connessioni sicure e affidabili che utilizzano il protocollo HTTPS, un approccio standard per proteggere le comunicazioni Internet tramite porte standard.

Autenticazione e gestione delle identità

Per accedere ai servizi Altium 365 che gestiscono dati sensibili dei clienti, gli utenti devono sottoporsi a un processo di autenticazione per ogni richiesta. Questa autenticazione non si limita ai tradizionali inserimenti di nome utente e password; si integra anche con sistemi di Single Sign-On (SSO) o Identity Providers (IdPs) come Google e Facebook. Questi sistemi possono utilizzare varie credenziali, tra cui chiavi hardware, smart card o dati biometrici come le impronte digitali, che non controlliamo direttamente. Indipendentemente dal metodo, tutte le sessioni sono a tempo limitato per motivi di sicurezza e tutte le informazioni di accesso sensibili vengono crittografate in modo sicuro durante la trasmissione.

Altium 365 supporta l'Autenticazione Unica (SSO) utilizzando il protocollo SAML 2.0. Questa funzionalità si integra con i più moderni IdP, inclusi OneLogin, Okta, Microsoft Azure AD e Google Identity. Il supporto esteso del protocollo SCIM consente di organizzare il provisioning e il de-provisioning centralizzati di utenti e gruppi. A seconda dell'IdP, è possibile optare per una protezione avanzata con autenticazione a più fattori (MFA).

Distribuzione e controllo

Altium 365 utilizza protezioni perimetrali a più livelli per controllare e ispezionare il traffico in entrata, tra cui il firewall per applicazioni Web e il bilanciamento del carico gestito. Questi controlli aiutano a proteggere gli endpoint esposti a Internet e supportano la disponibilità distribuendo il traffico tra i servizi applicativi. L'accesso amministrativo ai sistemi di produzione è limitato al personale autorizzato secondo il principio del privilegio minimo e viene registrato e monitorato.

Struttura Single-Tenancy e Multi-Tenancy

Altium 365 opera su un'architettura multi-tenant in cui ciascun tenant, attualmente allineato al concetto di spazio di lavoro, dispone del proprio schema di database isolato. Questo modello offre una solida separazione dei dati, utilizzando un'infrastruttura cloud condivisa per garantire efficienza e scalabilità. Per le organizzazioni che richiedono un maggiore isolamento, personalizzazione e controllo operativo, Altium offre un ambiente single-tenant (STE): un'istanza dedicata dell'applicazione e della relativa infrastruttura di supporto. STE offre un elevato isolamento dei dati, prestazioni prevedibili e opzioni di configurazione specifiche per il tenant, combinando la comodità di un servizio in hosting con il controllo tradizionalmente associato alle distribuzioni on-premise.

Scansione vulnerabilità

Le distribuzioni in produzione per Altium 365 sono soggette a scansioni delle vulnerabilità nell'ambito del processo di rilascio. I risultati vengono monitorati fino alla correzione o all'accettazione documentata del rischio, in conformità con la politica di gestione delle vulnerabilità di Altium e le tempistiche di correzione definite.

Verifiche di terze parti

Collaboriamo annualmente con terze parti esterne per eseguire test di penetrazione, al fine di garantire il mantenimento del massimo livello di sicurezza rispetto alle minacce in continua evoluzione. Il team di sviluppo esamina tutti i feedback dei test di penetrazione e implementa gli aggiornamenti necessari ai nostri servizi applicativi e alla nostra infrastruttura. Siamo disponibili a condividere con le parti interessate l'ultima sintesi esecutiva del nostro rapporto sui test di penetrazione, a condizione che sia in vigore un accordo reciproco di non divulgazione (MNDA).

Monitoraggio della sicurezza e gestione degli incidenti

Abbiamo implementato una pratica completa di registrazione e monitoraggio per consentire il rilevamento precoce e una risposta efficace agli incidenti di sicurezza. Utilizzando il framework di cybersecurity del NIST come base, la registrazione e il monitoraggio sono componenti chiave delle funzioni "Rileva" e “Rispondi”. Queste funzioni sono essenziali per identificare e comprendere gli eventi di sicurezza e le vulnerabilità, migliorando l'accuratezza e la precisione di Altium 365. L'identificazione degli incidenti è fondamentale nel nostro processo di risposta, in cui i team di sicurezza, i sistemi e gli strumenti collaborano per riconoscere e confermare potenziali incidenti di sicurezza. Una volta identificato un incidente di sicurezza, attiviamo il nostro Piano di risposta agli incidenti per garantire una risposta rapida ed efficace, allineata agli obiettivi di sicurezza e aziendali dell'organizzazione.

Consapevolezza e formazione sulla sicurezza

Altium® garantisce che tutti i nuovi assunti ricevano una formazione sulla consapevolezza della sicurezza durante l'onboarding, con aggiornamenti annuali per tutto il personale. Il team delle Risorse umane contatta i dipendenti che non hanno completato la formazione per garantire la conformità. Inoltre, inviamo regolarmente notifiche sulla consapevolezza della sicurezza al personale, informandolo sui nuovi protocolli e sulle potenziali minacce. Il nostro team di Ricerca e sviluppo segue una formazione specializzata sulle pratiche di codifica sicura. Il materiale formativo viene periodicamente rivisto e aggiornato per riflettere le pratiche di codifica o i linguaggi di programmazione.

Privacy dei dati

Le Condizioni generali di servizio di Altium e l' Informativa sulla privacy delineano le misure che adottiamo per garantire la privacy e la sicurezza dei dati dei Clienti. Questi documenti e le procedure interne di supporto aderiscono alle normative globali sulla protezione dei dati, tra cui il GDPR e il California Consumer Privacy Act (CCPA). Tale adesione garantisce la riservatezza, l'integrità e la disponibilità di tutti i dati gestiti da Altium, comprese le informazioni affidateci dai nostri Clienti e partner commerciali. Nell'odierno ambiente competitivo del business globale, è fondamentale mantenere la privacy dei dati per prevenire le minacce, tra cui errori, perdite, frodi e spionaggio. Il nostro approccio è progettato per prevenire qualsiasi violazione della sicurezza dei dati che gestiamo.

Informativa sui cookie

L'utente può gestire le preferenze sui cookie tramite le impostazioni del suo browser. Alcuni browser consentono di inserire in una lista sicura i siti dai quali l'utente accetta i cookie. Per maggiori dettagli sulla gestione delle preferenze sui cookie, consulta la nostra Informativa sui cookie.

Politica di conservazione dei dati

Se l'utente smette di usare Altium 365, i suoi dati saranno conservati secondo i periodi di tempo specificati nella nostra Informativa sulla retention dei dati. Alla scadenza di questo periodo, i suoi dati saranno cancellati dai nostri sistemi.

Backup e disaster recovery

Altium 365 utilizza un sistema di backup automatico per garantire che tutti i tuoi dati archiviati in Altium 365 vengano copiati nelle nostre regioni di backup, eliminando la necessità di un intervento manuale. Disponiamo di un piano completo di disaster recovery per supportare la continuità aziendale dei servizi e delle piattaforme di produzione. In caso di interruzione del sistema, puntiamo a un Recovery Point Objective (RPO) e a un Recovery Time Objective (RTO) di 24 ore ciascuno. Questo piano viene revisionato e testato ogni 120 giorni per verificarne l'efficacia e include politiche e procedure dettagliate per ripristinare i servizi in caso di disastro.

Per ulteriori informazioni, visita il Trust Center Altium 365 ed esplora le risposte alle domande frequenti.

Altium 365 GovCloud

Altium 365 GovCloud è una regione dedicata della piattaforma cloud Altium 365 situata all'interno degli Stati Uniti, gestita esclusivamente da persone statunitensi nella regione AWS GovCloud. Scegliere un'area di lavoro Altium 365 nella regione GovCloud può aiutare le organizzazioni a conformarsi alle normative del governo statunitense, come ITAR ed EAR.

Soggetti statunitensi

Il funzionamento della regione GovCloud sul lato Altium è limitato ai soli ci ttadinistatunitensi. I Clienti Altium determinano e controllano chi aggiungono alla loro area di lavoro e a chi concedono l'accesso ai dati archiviati nell'area stessa.

Protezione dati

Controllo del traffico in uscita

Per proteggere dall'esportazione non autorizzata di dati, utilizziamo un proxy in uscita che controlla e impedisce al traffico in uscita non autorizzato di lasciare l'ambiente.

Funzionalità limitate

Abbiamo disattivato per impostazione predefinita le funzionalità che potrebbero potenzialmente comportare un'uscita involontaria di dati dagli Stati Uniti, mitigando così i rischi associati a errori dell'utente.

- **Condivisione al di fuori dell'area di lavoro.** Per impostazione predefinita, la condivisione di progetti, release, librerie e pacchetti di produzione (funzione “Invia al produttore”) con persone che non appartengono all'area di lavoro Altium 365 GovCloud dell'utente è disabilitata. Questa impostazione può essere modificata dagli amministratori, se necessario.
- **Spazio Altium 365 Personal.** Gli utenti aggiunti a un'Area di lavoro Altium 365 GovCloud non possono archiviare alcun dato nei rispettivi spazi Altium 365 Personal.
- **Integrazione PLM.** L'amministratore controlla la connessione ai sistemi PLM di terze parti e fornisce le impostazioni necessarie.
- **Sistemi client.** La responsabilità di Altium non si estende alla configurazione, alla sicurezza o alla manutenzione dei sistemi lato client, come browser o strumenti CAD, che si connettono ad Altium 365 GovCloud. Il cliente deve mantenere aggiornati questi sistemi e installare tutti gli aggiornamenti e le patch necessari.

Suolo degli Stati Uniti

Le regioni AWS GovCloud US-East e US-West sono gestite da dipendenti cittadini statunitensi che si trovano sul territorio degli Stati Uniti.

Controlli di accesso

Accesso all'Area di lavoro da paesi al di fuori degli Stati Uniti

L'accesso all'area di lavoro dall'esterno degli Stati Uniti è esplicitamente bloccato, incluso l'accesso da parte di persone statunitensi che cercano di accedere allo spazio di lavoro da un altro Paese. Per ulteriori informazioni sull'accesso VPN, fare clic qui.

Per ulteriori informazioni, visita Altium 365 GovCloud.

Conformità: Certificazioni e normative

La conformità non è solo una formalità da spuntare; è un impegno verso l'eccellenza e una promessa di affidabilità. In Altium 365, prendiamo sul serio questa responsabilità, assicurandoci che la nostra piattaforma soddisfi i più elevati standard di conformità e certificazione.

CSA STAR Level 1: Autovalutazione

Il programma Security, Trust, Assurance, and Risk (STAR) è un'iniziativa della Cloud Security Alliance (CSA) concepita per offrire un solido quadro di garanzia per il cloud computing. Altium 365 ha ottenuto lo STAR Level 1 della CSA, che consiste in un'attestazione autonoma di conformità ai controlli della Cloud Control Matrix (CCM), comunemente nota come Consensus Assessment Initiative Questionnaire (CAIQ). Altium 365 è quindi elencato nello STAR Registry.

Attestazione SOC 2 Type 2

Altium 365 ha ottenuto l'attestazione Service Organization Control (SOC) 2 Type 2, a conferma del fatto che rispettiamo i più elevati standard di sicurezza dei dati e dei sistemi previsti dal principio di sicurezza. Questo framework di conformità alla cybersecurity è stato sviluppato dall'American Institute of Certified Public Accountants (AICPA) e richiede alle aziende di sottoporsi a un audit condotto da un revisore esterno accreditato dall'AICPA. Altium 365 conduce audit SOC 2 Type 2 con cadenza annuale.

GDPR

Riconosciamo l'importanza della privacy dei dati e ci impegniamo a rispettare i severi requisiti stabiliti dal Regolamento generale sulla protezione dei dati (GDPR), garantendo che i tuoi dati siano gestiti con la massima cura e rispetto.

Conformità ITAR

Altium 365 GovCloud può aiutare i nostri clienti a raggiungere la conformità all'International Traffic in Arms Regulations (ITAR). Questa regione specializzata soddisfa le esigenze specifiche dei nostri utenti che operano in settori altamente regolamentati.

Funzionalità di sicurezza e governance di Altium 365

Altium offre funzionalità avanzate di sicurezza, gestione delle identità e governance che aiutano le organizzazioni a proteggere i dati sensibili di progettazione, mantenere la conformità e gestire gli accessi su larga scala.

Controllo degli accessi

- **Autorizzazioni dati di base**
  Diritti fondamentali di visualizzazione e modifica che definiscono il modo in cui gli utenti interagiscono con file, cartelle e progetti nell'intera piattaforma.
- **Autorizzazioni avanzate sui dati**
  Controlli che vanno oltre i diritti di accesso di base, tra cui regole di condivisione a livello di organizzazione, impostazioni granulari delle autorizzazioni e opzioni avanzate di ereditarietà che determinano il modo in cui l'accesso ai dati viene consentito o limitato tra i team.
- **Gestione dei gruppi**
  Standardizza autorizzazioni, licenze e visibilità dell'area di lavoro assegnando gli accessi in base a ruoli definiti, garantendo un controllo coerente e scalabile in tutta l'organizzazione.
- **Supporto per ospiti esterni**
  Controlla il modo in cui i collaboratori esterni vengono invitati, raggruppati e limitati, con regole di visibilità e flussi di lavoro applicati che mantengono l'accesso degli ospiti circoscritto e sicuro.
- **Filtro di accesso**
  Cerca e verifica gli accessi effettivi in tutti i progetti, con modifiche rapide e rimozione degli ospiti con un clic.

Autenticazione e provisioning degli utenti

- **Gestione dell'organizzazione**
  Definisce come gli utenti entrano a far parte dell'organizzazione, come vengono assegnati i ruoli e come le regole basate sul dominio disciplinano l'identità e l'accesso alle risorse interne.
- **Single Sign-On (SSO) e SCIM**
  Si integra con il provider di identità esistente per centralizzare l'autenticazione e automatizzare il provisioning e il deprovisioning degli utenti tramite SCIM.
- **Autenticazione a più fattori (MFA)**
  Rafforza la sicurezza dell'account richiedendo un ulteriore passaggio di verifica, riducendo il rischio di accesso non autorizzato anche se le credenziali sono compromesse.
- **Gestione dei gruppi**
  Supporta il provisioning delle identità allineando gli utenti a ruoli predefiniti e profili di accesso durante l'onboarding e per tutto il loro ciclo di vita.

Sicurezza avanzata

- **Whitelisting degli IP**
  Limita l'accesso alla piattaforma agli indirizzi IP o agli intervalli approvati, garantendo che solo le reti affidabili possano accedere ai dati organizzativi sensibili.
- **Registro eventi**
  Fornisce visibilità sulle azioni degli utenti e del sistema nell'intero spazio di lavoro, supportando audit, verifiche di sicurezza e report di conformità con registri delle attività chiari e contrassegnati da data e ora.
- **SIEM (API)**
  Collega i dati degli eventi di Altium Agile al SIEM esistente, consentendo analisi centralizzate, avvisi e monitoraggio della conformità in tutta l'organizzazione.

Rimani aggiornato sui nostri ultimi aggiornamenti di sicurezza

La nostra piattaforma continua a evolversi con nuove funzionalità che rafforzano la governance, migliorano la visibilità e supportano i requisiti di sicurezza delle moderne organizzazioni di elettronica. La sicurezza rimane fondamentale e ogni aggiornamento è progettato per aiutare i team a procedere rapidamente mantenendo il controllo sui dati sensibili e regolamentati.

Man mano che il panorama dello sviluppo elettronico e della protezione dei dati si evolve, noi evolviamo con esso. Il nostro obiettivo è offrire miglioramenti pratici e scalabili che soddisfino le esigenze attuali, preparando la tua organizzazione a ciò che verrà dopo.

Resta aggiornato sui continui miglioramenti mentre ampliamo i controlli, potenziamo il monitoraggio e rafforziamo le protezioni, garantendo che sicurezza e innovazione rimangano allineate.

Per ulteriori dettagli e risorse correlate, visitare altium.com

Vuoi saperne di più? www.altium.com/platform/trust

Le informazioni fornite in questo whitepaper sono aggiornate a febbraio 2026. Si prega di notare che Altium 365 è una piattaforma in continua evoluzione. Per la versione più recente di questo documento, ti invitiamo a visitare questa pagina.