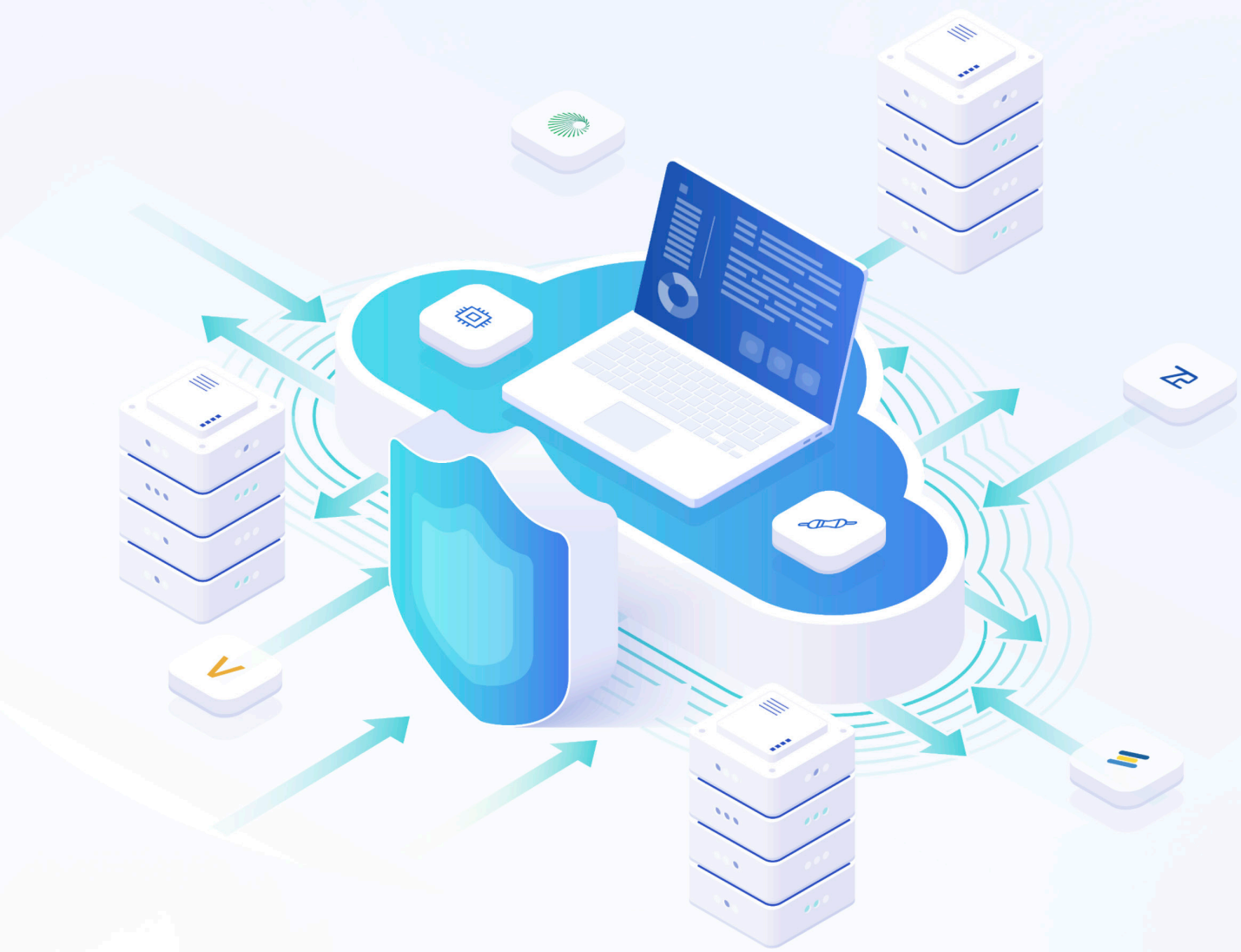
ALTIUM 365

Sicherheitsansatz und -praktiken



CONTENT

Einführung

Altium 365 ist die Plattform für Elektronikentwicklung, die Design, Daten und Zusammenarbeit in einer einzigen sicheren Cloud-Umgebung vereint. Die Plattform wurde zur Unterstützung des gesamten Lebenszyklus der Elektronikentwicklung entwickelt und bietet die moderne Infrastruktur, die Engineering-Teams benötigen, um schneller, effizienter und skalierbar zu arbeiten. Die Plattform ist in Altium Agile und Altium Develop enthalten und optimiert Arbeitsabläufe, steigert die Produktivität und beschleunigt die Produktlieferung.

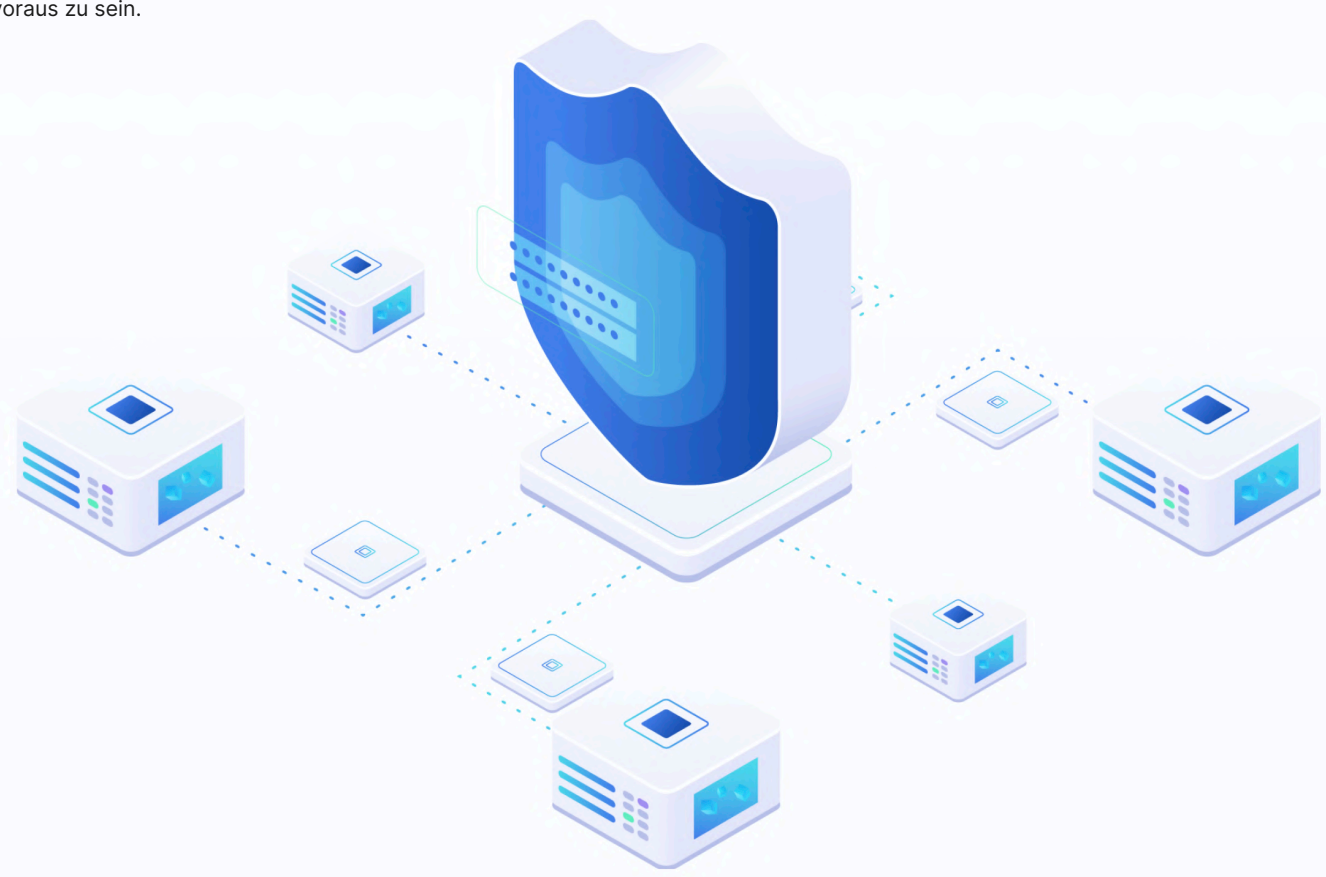
Bei Altium glauben wir, dass sich der wahre Wert einer Cloud-Plattform nicht nur daran bemisst, was sie ermöglicht, sondern auch daran, wie sicher sie die ihr anvertraute Arbeit schützt. Sicherheit ist fest in den Kern der Architektur von Altium 365 eingebettet und bestimmt, wie wir die Plattform entwerfen, entwickeln und betreiben. Dieses Engagement treibt uns an, moderne Cybersicherheitsstandards zu erfüllen – und kontinuierlich zu übertreffen.

Dieses Whitepaper bietet einen klaren, transparenten Einblick in die umfassenden Sicherheitsmaßnahmen, die Altium 365 zugrundeliegen. Unser Ziel ist einfach: Ihnen zu zeigen, wie Ihre Daten geschützt werden, wie unsere Schutzmaßnahmen entwickelt werden und wie sich unsere Sicherheitslage weiterentwickelt, um neuen Bedrohungen immer einen Schritt voraus zu sein.

Während Sie sich durch diese Seiten bewegen, erhalten Sie Einblick in die Planung, die Prozesse und die Schutzmechanismen, die unseren Ansatz prägen – von sicheren Entwicklungspraktiken bis hin zu den mehrschichtigen Kontrollen, die in der gesamten Plattform eingebettet sind. Sie sehen, wie unsere technische Präzision, unsere operative Disziplin und unsere cloudnative Architektur zusammenwirken, um Ihre Daten in jeder Phase zu schützen.

Letztendlich ist es unser Ziel, Ihnen die Gewissheit zu geben, dass Ihre Zusammenarbeit in Altium 365 durch ein robustes, sich kontinuierlich weiterentwickelndes Sicherheitsframework geschützt ist. Wir möchten, dass Sie sich auf die Entwicklung und Innovation konzentrieren können – während wir uns um die Sicherheit kümmern, die dies schützt.

Dieses Dokument beschreibt den Sicherheitsansatz und die Sicherheitspraktiken von Altium 365 auf Plattformebene; spezifische Funktionen können je nach Abonnement, Bereitstellungsumgebung (z. B. GovCloud) und Kundenkonfiguration variieren.



Altium 365 Sicherheits-maßnahmen

Sicherheit ist die Grundlage für Vertrauen, und unsere Kunden verlassen sich darauf, dass Altium 365 ihre wertvollsten Ressourcen schützt – ihre Daten, Designs und ihr geistiges Eigentum. Sicherheit ist in jede Ebene der Plattform integriert – von der frühen Architektur und Entwicklung über die Bereitstellung bis hin zum laufenden Betrieb. Unser Ansatz ist sorgfältig, proaktiv und entwickelt sich kontinuierlich weiter, wodurch eine sichere und resiliente Umgebung für die gemeinsame Elektronikentwicklung entsteht.

Sicherheitsgerichtete Entwicklung

Wir haben die Altium 365-Plattform, ihre Funktionen und Funktionalitäten unter Berücksichtigung der Benutzersicherheit entwickelt. In jeder Phase der Entwicklung überprüfen wir die vorhandenen Sicherheitsmaßnahmen sorgfältig. Dazu gehören umfangreiche Architekturüberprüfungen, das Scannen von Abhängigkeiten, Codeüberprüfungen und dynamische Sicherheitstests von Anwendungen. Unser Ziel ist es, potenzielle Sicherheitslücken von Anfang an proaktiv zu identifizieren, zu beheben und zu verhindern. Darüber hinaus setzen wir unabhängige Tests durch Dritte ein, um sicherzustellen, dass unser Sicherheitsrahmen robust ist.

Zuverlässiger Datenschutz

Amazon Web Services (AWS) bildet das Rückgrat der physischen Sicherheit und Zuverlässigkeit für Altium 365. Wir speichern Kundendaten ausschließlich auf AWS-Ressourcen und verwenden speziell den Relational Database Service (RDS) für unsere Datenbankanforderungen. Für die standardmäßige Speicherung von Binärdaten verwenden wir AWS S3, während FSx für Szenarien eingesetzt wird, die eine leistungsstarke Binärspeicherung erfordern. Dedizierte Elasticsearch-Cluster werden verwendet, um leistungsstarke Suchfunktionen bereitzustellen.

Ruhende Daten innerhalb von Altium 365 werden mithilfe von AWS Key Management Service (KMS)-Schlüsseln verschlüsselt. Diese Schlüssel verwenden Hardware-Sicherheitsmodule, die nach den FIPS 140-2-Standards validiert wurden, einem US-amerikanischen Computersicherheitsstandard zur Genehmigung kryptografischer Module. Die Nutzung dieser Verschlüsselungsschlüssel wird protokolliert und überwacht. Die Protokolle werden dann an unser Security Information and Event Management (SIEM)-System gesendet, sodass wir nachverfolgen können, wann die Verschlüsselungsschlüssel verwendet werden.

Der Zugriff auf die Altium 365-Infrastruktur, auf der Kundendaten gehostet werden, ist nach dem Prinzip der geringsten Berechtigungen auf autorisiertes Personal beschränkt. Sämtliche Zugriffe werden protokolliert, sind auditierbar und werden kontinuierlich vom dedizierten Sicherheitsteam von Altium überwacht.

Sichere Kommunikation

Die Kommunikation zwischen Altium 365-Clients (wie z. B. einem Webbrowser, Altium Designer oder einer mobilen Anwendung) und der Altium 365 Cloud-Plattform ist nur über sichere, vertrauenswürdige Verbindungen unter Verwendung des HTTPS-Protokolls – einem Standardansatz für sichere Internetkommunikation über Standard-Ports – möglich.

Authentifizierung und Identitätsmanagement

Für den Zugriff auf Altium 365-Dienste, die sensible Kundendaten verwalten, müssen Benutzer für jede Anfrage einen Authentifizierungsprozess durchlaufen. Diese Authentifizierung ist nicht auf herkömmliche Eingaben von Benutzername und Passwort beschränkt; sie lässt sich auch in Single-Sign-on-Systeme (SSO) oder Identitätsanbieter (IdPs) wie Google und Facebook integrieren. Diese Systeme können verschiedene Anmeldeinformationen verwenden, darunter Hardwareschlüssel, Smartcards oder biometrische Daten wie Fingerabdrücke, die wir nicht direkt kontrollieren. Unabhängig von der Methode sind alle Sitzungen aus Sicherheitsgründen zeitlich begrenzt, und sämtliche sensiblen Anmeldeinformationen werden während der Übertragung sicher verschlüsselt.

Altium 365 unterstützt SSO unter Verwendung des SAML 2.0-Protokolls. Diese Funktion lässt sich in die meisten modernen IdPs integrieren, darunter OneLogin, Okta, Microsoft Azure AD und Google Identity. Die erweiterte Unterstützung des SCIM-Protokolls ermöglicht die Organisation einer zentralisierten Bereitstellung und Aufhebung der Bereitstellung von Benutzern und Gruppen. Je nach IdP können Sie sich für einen erweiterten Schutz mit Multi-Faktor-Authentifizierung (MFA) entscheiden.

Distribution und Kontrolle

Altium 365 setzt mehrschichtige Perimeterschutzmaßnahmen ein, um den eingehenden Datenverkehr zu steuern und zu überprüfen, einschließlich Web Application Firewalling und verwaltetem Load Balancing. Diese Kontrollmechanismen tragen zum Schutz der mit dem Internet verbundenen Endgeräte bei und sichern die Verfügbarkeit, indem sie den Datenverkehr auf verschiedene Anwendungsdienste verteilen. Der administrative Zugriff auf Produktionssysteme ist auf autorisiertes Personal beschränkt, wobei das Prinzip der geringsten Berechtigungen gilt; dieser Zugriff wird protokolliert und überwacht.

Single-Tenancy- und Multi-Tenancy-Architektur

Altium 365 basiert auf einer Multi-Tenancy-Architektur, bei der jeder Tenant – derzeit mit dem Konzept eines Arbeitsbereichs gleichgesetzt – ein eigenes isoliertes Datenbankschema erhält. Dieses Modell sorgt für eine starke Datentrennung und nutzt zugleich eine gemeinsame Cloud-Infrastruktur für Effizienz und Skalierbarkeit. Für Unternehmen/Organisationen, die eine stärkere Isolierung, individuelle Anpassung und operative Kontrolle benötigen, bietet Altium eine Single-Tenant-Umgebung (STE) an: eine dedizierte Instanz der Anwendung und der dazugehörigen Infrastruktur. STE bietet eine hohe Datenisolierung, vorhersehbare Leistung und mandantenspezifische Konfigurationsoptionen und vereint den Komfort eines gehosteten Dienstes mit der Kontrolle, die traditionell mit Vor-Ort-Bereitstellungen verbunden ist.

Scannen auf Sicherheitslücken

Produktivbereitstellungen für Altium 365 werden im Rahmen des Release-Prozesses einer Schwachstellenprüfung unterzogen. Die Ergebnisse werden im Rahmen der Behebung oder der dokumentierten Risikoakzeptanz gemäß der Altium-Richtlinie zum Sicherheitslückenmanagement und den festgelegten Zeitplänen für die Behebung nachverfolgt.

Prüfung durch Dritte

Wir arbeiten jedes Jahr mit externen Partnern zusammen, um Penetrationstests durchzuführen und so sicherzustellen, dass wir auch angesichts sich ständig weiterentwickelnder Bedrohungen ein Höchstmaß an Sicherheit gewährleisten. Das Entwicklungsteam wertet alle Rückmeldungen aus den Penetrationstests aus und nimmt die notwendigen Anpassungen an unseren Anwendungsdiensten und unserer Infrastruktur vor. Wir sind bereit, die aktuelle Zusammenfassung unseres Penetrationstest-Berichts an Interessierte weiterzugeben, sofern eine gegenseitige Geheimhaltungsvereinbarung (MNDA) vorliegt.

Sicherheitsüberwachung und Vorfallmanagement

Wir haben eine umfassende Protokollierungs- und Überwachungspraxis implementiert, um die frühzeitige Erkennung und wirksame Reaktion auf Sicherheitsvorfälle zu ermöglichen. Auf der Grundlage des NIST-Frameworks für Cybersicherheit sind Protokollierung und Überwachung zentrale Bestandteile der Funktionen „Erkennen“ und „Reagieren“. Diese Funktionen sind unverzichtbar, um Sicherheitsvorfälle und Schwachstellen zu erkennen und zu verstehen und so die Genauigkeit und Präzision von Altium 365 zu verbessern. Die Identifizierung von Vorfällen ist grundlegend für unseren Reaktionsprozess bei Vorfällen, bei dem die Sicherheitsteams, Systeme und Werkzeuge zusammenarbeiten, um potenzielle Sicherheitsvorfälle zu erkennen und zu bestätigen. Sobald ein Sicherheitsvorfall identifiziert wird, aktivieren wir unseren Incident-Response-Plan, um eine schnelle und wirksame Reaktion sicherzustellen, die mit den Sicherheits- und Geschäftszielen des Unternehmens bzw. der Organisation übereinstimmt.

Sicherheitsbewusstsein und -schulung

Altium stellt sicher, dass alle neuen Mitarbeiter während der Einarbeitungsphase eine Schulung zum Thema Sicherheitsbewusstsein erhalten und dass für alle Mitarbeiter jährliche Auffrischungskurse stattfinden. Das Personalteam fasst bei Mitarbeitern, die ihre Schulung nicht abgeschlossen haben, nach, um die Compliance sicherzustellen. Zusätzlich senden wir dem Personal regelmäßig Benachrichtigungen zum Sicherheitsbewusstsein, um es über neue Protokolle und potenzielle Bedrohungen zu informieren. Unser Forschungs- und Entwicklungsteam erhält eine spezielle Schulung zu sicheren Codierungspraktiken. Das Schulungsmaterial wird regelmäßig überprüft und aktualisiert, um Codierungspraktiken oder Programmiersprachen widerzuspiegeln.

Datenschutz

Die Allgemeinen Nutzungsbedingungen von Altium und seine Datenschutzerklärung beschreiben die Schritte, die wir unternehmen, um den Datenschutz und die Sicherheit der Kundendaten zu gewährleisten. Diese Dokumente und unsere dazugehörigen internen Verfahren entsprechen den weltweiten Datenschutzbestimmungen, darunter die DSGVO und der California Consumer Privacy Act (CCPA). Diese Einhaltung gewährleistet die Vertraulichkeit, Integrität und Verfügbarkeit aller von Altium verwalteten Daten, einschließlich der Informationen, die uns von unseren Kunden und Geschäftspartnern anvertraut werden. Im heutigen wettbewerbsintensiven globalen Geschäftsumfeld ist es entscheidend, den Datenschutz zu wahren, um Bedrohungen wie Fehler, Verlust, Betrug und Spionage vorzubeugen. Unser Ansatz zielt darauf ab, jegliche Sicherheitsverletzungen bei den von uns verarbeiteten Daten zu verhindern.

Cookie-Richtlinie

Sie können Ihre Cookie-Präferenzen über Ihre Browser-Einstellungen verwalten. Bei einigen Browsern können Sie Websites, von denen Sie Cookies akzeptieren, auf eine sichere Liste setzen. Weitere Einzelheiten zur Verwaltung von Cookie-Einstellungen finden Sie in unserer Cookie-Richtlinie.

Richtlinie zur Datenspeicherung

Wenn Sie Altium 365 nicht mehr nutzen, werden Ihre Daten gemäß den in unserer Richtlinie zur Datenspeicherung angegebenen Zeiträumen aufbewahrt. Nach Ablauf dieses Zeitraums werden Ihre Daten aus unseren Systemen gelöscht.

Datensicherung und Notfallwiederherstellung

Altium 365 verwendet ein automatisiertes Backup-System, um sicherzustellen, dass alle Ihre in Altium 365 gespeicherten Daten in unsere Sicherungsregionen kopiert werden, wodurch manuelle Eingriffe überflüssig werden. Wir verfügen über einen umfassenden Plan zur Wiederherstellung im Katastrophenfall, um die Geschäftskontinuität für die Produktionsdienste und -plattformen zu unterstützen. Im Falle einer Systemunterbrechung streben wir jeweils ein Recovery Point Objective (RPO) und ein Recovery Time Objective (RTO) von 24 Stunden an. Dieser Plan wird alle 120 Tage überprüft und getestet, um seine Wirksamkeit sicherzustellen, und enthält detaillierte Richtlinien und Verfahren zur Wiederherstellung der Dienste im Katastrophenfall.

Weitere Informationen finden Sie im Altium 365 Trust Center. Entdecken Sie außerdem Antworten auf häufig gestellte Fragen.

Altium 365 GovCloud

Altium 365 GovCloud ist eine dedizierte Region der Altium 365-Cloud-Plattform, die innerhalb der USA liegt und ausschließlich von US-Personen in der AWS GovCloud-Region betrieben wird. Die Entscheidung für einen Altium 365-Arbeitsbereich in der GovCloud-Region kann Unternehmen dabei helfen, Vorschriften der US-Regierung wie ITAR und EAR einzuhalten.

Personen aus den USA

Der Betrieb der Region auf der Altium-Seite ist ausschließlich Personen aus den USA vorbehalten. Altium-Kunden bestimmen und kontrollieren, wen sie zu ihrem Arbeitsbereich hinzufügen und wem sie Zugriff auf die im Arbeitsbereich gespeicherten Daten gewähren.

Datenschutz

Steuerung des ausgehenden Datenverkehrs

Um vor unbefugtem Datenexport zu schützen, setzen wir einen Outbound-Proxy ein, der unbefugten ausgehenden Datenverkehr kontrolliert und verhindert, dass dieser die Umgebung verlässt.

Eingeschränkte Funktionalität

Wir haben standardmäßig Funktionen deaktiviert, die potenziell zu einem unbeabsichtigten Datenabfluss aus den USA führen könnten, und dadurch die mit Benutzerfehlern verbundenen Risiken abgeschwächt.

- ✓ Teilen außerhalb des Arbeitsbereichs. Standardmäßig ist die gemeinsame Nutzung von Projekten, Releases, Bibliotheken und Fertigungspaketen (Funktion „An Hersteller senden“) mit Personen, die nicht zu Ihrem Altium 365 GovCloud-Arbeitsbereich gehören, deaktiviert. Diese Einstellung kann bei Bedarf von Administratoren geändert werden.
- ✓ Altium 365 Personal Space. Benutzer, die zu einem Altium 365 GovCloud-Arbeitsbereich hinzugefügt wurden, können keine Daten in ihren Altium 365 Personal Spaces speichern.
- ✓ PLM-Integration. Der Administrator steuert die Verbindung zu PLM-Systemen von Drittanbietern und stellt die erforderlichen Einstellungen bereit.
- ✓ Client-Systeme. Altium ist nicht verantwortlich für die Konfiguration, Sicherheit oder Wartung kundenseitiger Systeme wie Browser oder CAD-Tools, die eine Verbindung zu Altium 365 GovCloud herstellen. Der Kunde muss diese Systeme auf dem neuesten Stand halten und alle erforderlichen Updates und Patches installieren.

US-Boden

Die AWS GovCloud-Regionen „USA-Ost“ und „USA-West“ werden von Mitarbeitern betrieben, die US-Bürger sind und sich auf US-amerikanischem Boden befinden.

Zugriffskontrollen

Zugriff auf den Arbeitsbereich von außerhalb der USA

Der Zugriff auf den Arbeitsbereich von außerhalb der USA ist ausdrücklich gesperrt, einschließlich des Zugriffs durch Personen aus den USA, die versuchen, von einem anderen Land aus auf den Arbeitsbereich zuzugreifen. Erfahren Sie mehr über den VPN-Zugang hier.

Weitere Informationen finden Sie unter Altium 365 GovCloud.

Compliance: Zertifizierungen & Vorschriften

Compliance ist nicht nur eine Formalität; sie ist ein Bekenntnis zu Exzellenz und ein Versprechen von Zuverlässigkeit. Bei Altium 365 nehmen wir diese Verantwortung ernst und stellen sicher, dass unsere Plattform die höchsten Compliance- und Zertifizierungsstandards erfüllt.

CSA STAR Level 1: Selbstbewertung

Das Programm für Sicherheit, Vertrauen, Gewährleistung und Risiko (STAR) ist eine Initiative der Cloud Security Alliance (CSA), die entwickelt wurde, um ein robustes Gewährleistungsframework für Cloud Computing bereitzustellen. Altium 365 hat CSA STAR Level 1 erreicht, eine Selbsterklärung über die Einhaltung der Kontrollen der Cloud Control Matrix (CCM), die allgemein als Consensus Assessment Initiative Questionnaire (CAIQ) bekannt ist. Altium 365 ist somit im STAR Registry aufgeführt.

SOC 2 Type 2-Bescheinigung

Altium 365 verfügt über eine SOC 2 Type 2-Bescheinigung, die bestätigt, dass wir für das Sicherheitsprinzip die höchsten Standards für Daten- und Systemsicherheit einhalten. Dieses Cybersicherheits-Compliance-Framework wurde vom American Institute of Certified Public Accountants (AICPA) entwickelt und verlangt von Unternehmen, sich einem Audit durch einen externen, von der AICPA akkreditierten Auditor zu unterziehen. Altium 365 führt jährlich SOC 2 Type 2-Audits durch.

DSGVO

Wir erkennen die Bedeutung des Datenschutzes an und verpflichten uns, die strengen Anforderungen der Datenschutz-Grundverordnung (DSGVO) einzuhalten, um sicherzustellen, dass Ihre Daten mit größter Sorgfalt und Respekt behandelt werden.

ITAR-Konformität

Altium 365 GovCloud kann unseren Kunden dabei helfen, die International Traffic in Arms Regulations (ITAR) einzuhalten. Diese spezialisierte Region erfüllt die spezifischen Anforderungen unserer Nutzer, die in stark regulierten Branchen tätig sind.

Sicherheits- und Governance-Funktionen in Altium 365

Altium bietet erweiterte Funktionen für Sicherheit, Identität und Governance, die Unternehmen dabei unterstützen, sensible Designdaten zu schützen, die Compliance einzuhalten und den Zugriff im großen Maßstab zu verwalten.

Zugriffskontrolle

- **Grundlegende Datenberechtigungen**
  Grundlegende Anzeige- und Bearbeitungsrechte, die festlegen, wie Benutzer auf der gesamten Plattform mit Dateien, Ordnern und Projekten interagieren.
- **Erweiterte Datenberechtigungen**
  Steuerungsmöglichkeiten, die über grundlegende Zugriffsrechte hinausgehen, darunter Freigaberegeln auf Organisationsebene, detaillierte Berechtigungseinstellungen und erweiterte Vererbungsoptionen, die festlegen, wie der Zugriff auf Daten teamübergreifend geregelt oder eingeschränkt wird.
- **Gruppenverwaltung**
  Standardisiert Berechtigungen, Lizenzen und die Sichtbarkeit von Arbeitsbereichen, indem der Zugriff auf der Grundlage definierter Rollen zugewiesen wird, und gewährleistet so eine einheitliche und skalierbare Kontrolle im gesamten Unternehmen.
- **Unterstützung für externe Gäste**
  Steuert, wie externe Mitarbeitende eingeladen, gruppiert und eingeschränkt werden, mit Sichtbarkeitsregeln und erzwungenen Arbeitsabläufen, die den Gastzugriff begrenzen und schützen.
- **Zugriffsfilter**
  Durchsuchen und prüfen Sie effektive Zugriffsrechte in allen Projekten, mit schnellen Anpassungen und der Entfernung von Gästen mit einem Klick.

Authentifizierung & Benutzerbereitstellung

- **Unternehmensverwaltung**
  Legt fest, wie Benutzer dem Unternehmen beitreten, wie Rollen zugewiesen werden und wie domainbasierte Regeln Identität und Zugriff auf interne Ressourcen steuern.
- **Single Sign-On (SSO) & SCIM**
  Lässt sich in Ihren bestehenden Identitätsanbieter integrieren, um die Authentifizierung zu zentralisieren und die Benutzerbereitstellung sowie -deprovisionierung über SCIM zu automatisieren.
- **Multi-Faktor-Authentifizierung (MFA)**
  Stärkt die Kontosicherheit, indem ein zusätzlicher Verifizierungsschritt erforderlich ist, wodurch das Risiko eines unbefugten Zugriffs selbst bei kompromittierten Anmeldedaten verringert wird.
- **Gruppenverwaltung**
  Unterstützt die Identitätsbereitstellung, indem Benutzer während des Onboardings und während ihres gesamten Lebenszyklus vordefinierten Rollen und Zugriffsprofilen zugeordnet werden.

Erweiterte Sicherheit

- **IP-Whitelisting**
  Beschränkt den Plattformzugriff auf genehmigte IP-Adressen oder -Bereiche und stellt sicher, dass nur vertrauenswürdige Netzwerke auf sensible Unternehmensdaten zugreifen können.
- **Ereignisprotokoll**
  Bietet Transparenz über Benutzer- und Systemaktionen im gesamten Arbeitsbereich und unterstützt Audits, Sicherheitsprüfungen und die Compliance-Berichterstattung durch übersichtliche, mit Zeitstempeln versehene Aktivitätsaufzeichnungen.
- **SIEM (API)**
  Verbindet Altium-Agile-Ereignisdaten mit Ihrem vorhandenen SIEM und ermöglicht so eine zentralisierte Analyse, Warnmeldungen und Compliance-Nachverfolgung in Ihrem gesamten Unternehmen.

Bleiben Sie über unsere neuesten Sicherheitsupdates auf dem Laufenden

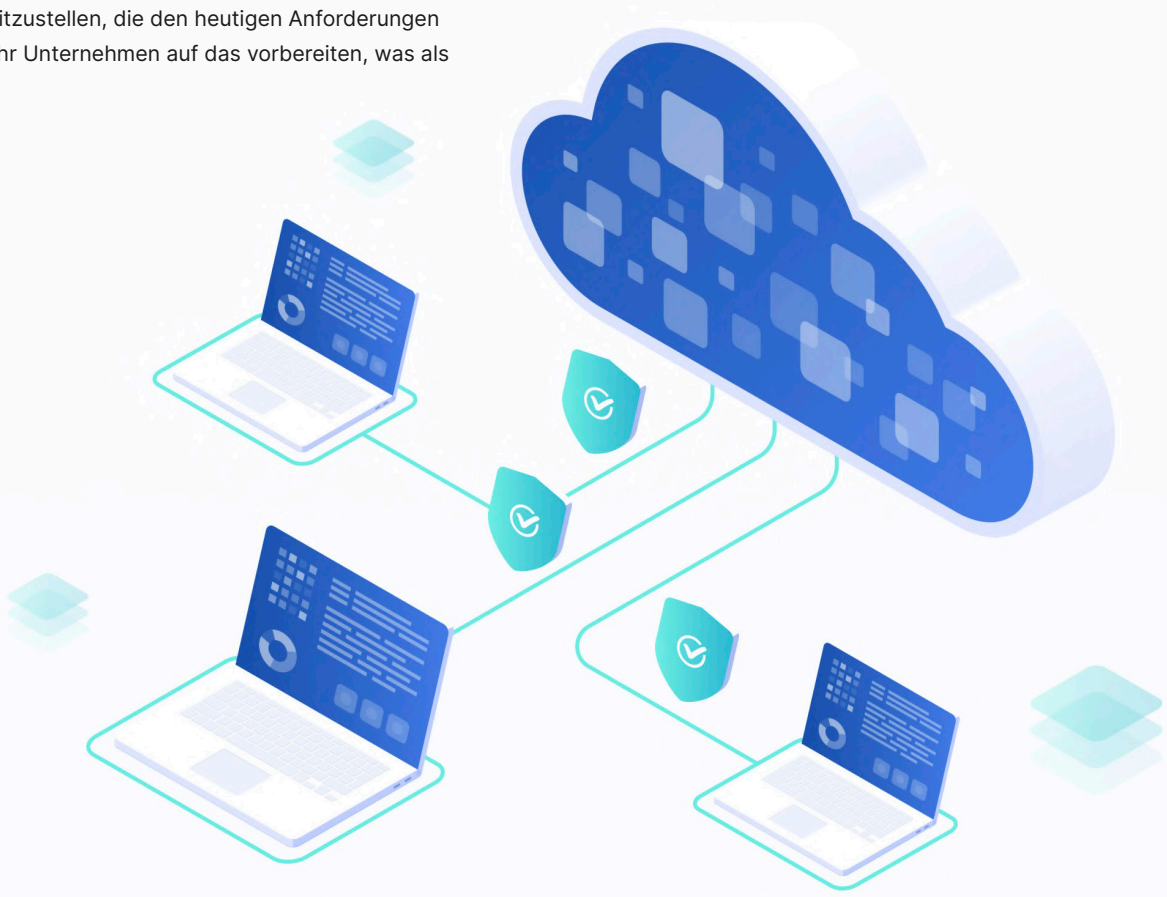
Unsere Plattform entwickelt sich kontinuierlich weiter – mit neuen Funktionen, die Governance stärken, die Transparenz verbessern und die Sicherheitsanforderungen moderner Elektronikunternehmen unterstützen. Sicherheit bleibt grundlegend, und jedes Update ist darauf ausgelegt, Teams dabei zu helfen, schnell voranzukommen und gleichzeitig die Kontrolle über sensible und regulierte Daten zu behalten.

Mit der Weiterentwicklung der Landschaft der Elektronikentwicklung und des Datenschutzes entwickeln auch wir uns weiter. Unser Fokus liegt darauf, praktische, skalierbare Verbesserungen bereitzustellen, die den heutigen Anforderungen gerecht werden und Ihr Unternehmen auf das vorbereiten, was als Nächstes kommt.

Bleiben Sie gespannt auf kontinuierliche Verbesserungen, während wir Kontrollen ausbauen, die Überwachung vertiefen und Schutzmaßnahmen verstärken – damit Sicherheit und Innovation weiterhin im Einklang bleiben.

Weitere Details und relevante Ressourcen finden Sie unter altium.com

Möchten Sie mehr erfahren? www.altium.com/platform/trust



Die in diesem Whitepaper bereitgestellten Informationen sind mit Stand von Februar 2026 korrekt. Bitte beachten Sie, dass Altium 365 eine sich weiterentwickelnde Plattform ist. Für die neueste Version dieses Dokuments besuchen Sie bitte diese Seite.