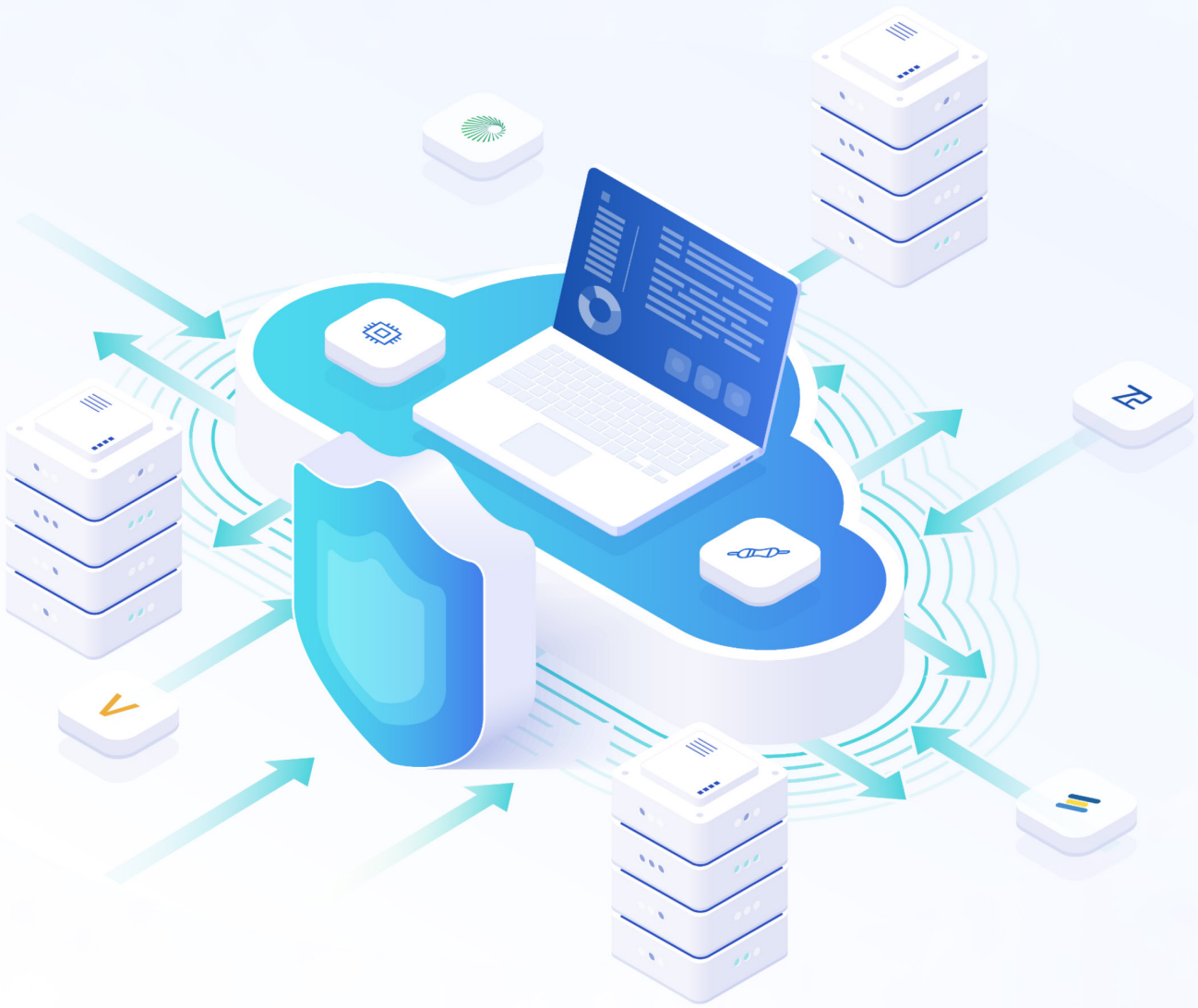
ALTIUM 365

Altium 365 Security Approach & Practices



CONTENT

Introduction

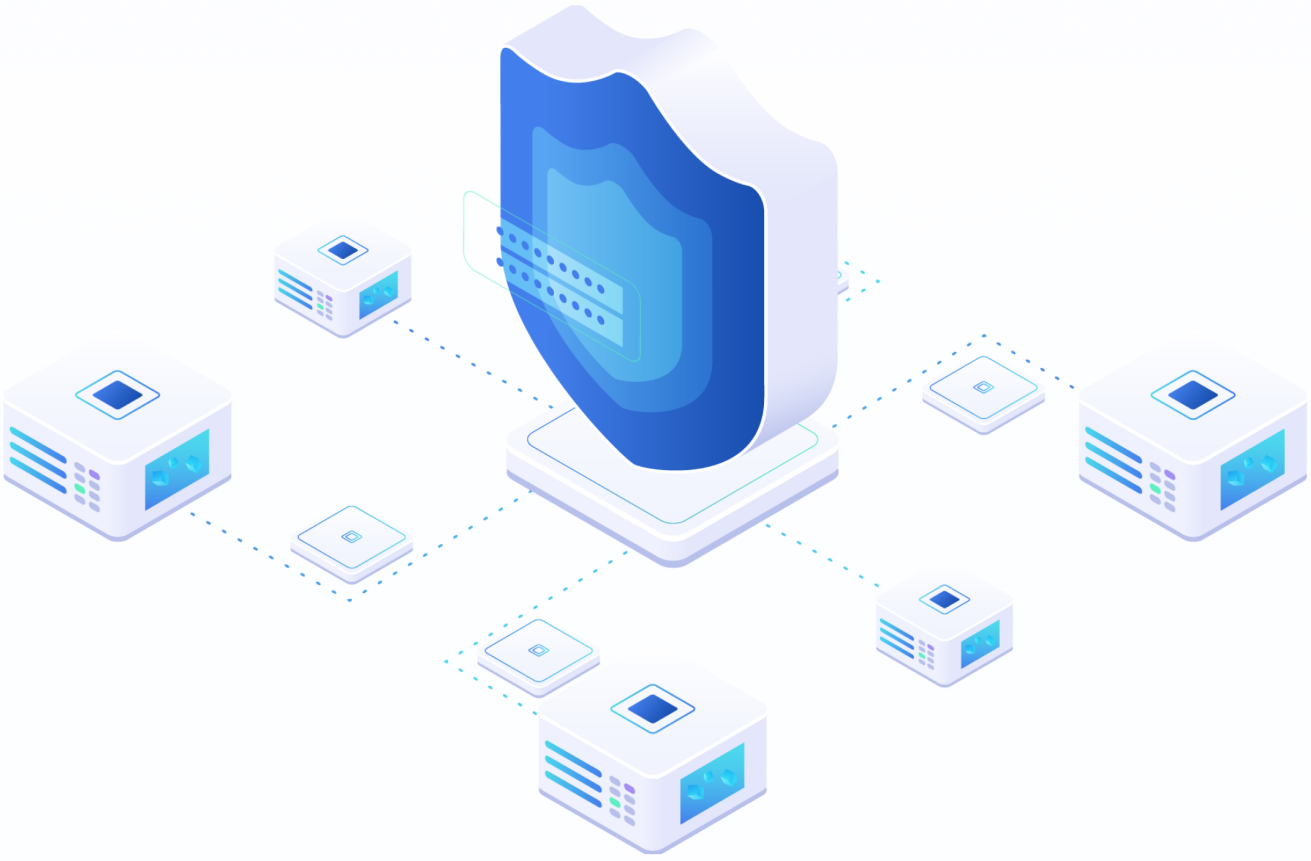
Altium 365 is the electronics development platform that brings together all aspects of electronics development, helping organizations deliver better products faster than ever before. The platform streamlines the development process, fosters collaboration, and enhances productivity.

At Altium, we understand that a cloud platform's true value lies not only in its features but also in how securely it handles your data. This belief is at the heart of everything we do, pushing us to meet and exceed the standards in cyber security.

This whitepaper is crafted to help you understand the extensive security measures that underpin Altium 365. We're committed to keeping your data safe, and we want to show you exactly how we do it.

As you turn these pages, you'll get an inside look at the careful planning and innovative strategies behind our security approach, from the development process to our comprehensive data protection tactics.

Our aim is simple: to give you the peace of mind that comes from knowing your collaborative work on Altium 365 is protected by a robust security framework. We want you to focus on your passion–creating and innovating–while we handle the security side of things.



Altium 365 Security Measures

Security is the very foundation upon which the trust of users is built. At Altium 365, we understand that our customers entrust us with their most valuable assets–their data and designs. Check the comprehensive security measures that are ingrained in every aspect of our platform. From the initial stages of development to the final deployment and ongoing maintenance, our approach to security is meticulous, proactive, and always evolving.

Security-Driven Development

We've developed the Altium 365 platform, its features, and functionalities with user security in mind. At every stage of development, we rigorously verify the security measures in place. This includes extensive architectural reviews, dependency scanning, code reviews, and dynamic application security testing. Our objective is to proactively identify, address, and prevent any potential security vulnerabilities right from the start. Additionally, we employ independent third-party testing to ensure that our security framework is robust.

Reliable Data Protection

Amazon Web Services (AWS) forms the backbone of physical security and reliability for Altium 365. We store customer data across AWS resources exclusively and use Relational Database Service (RDS) specifically for our database needs. For standard binary data storage, we use AWS S3, while FSx is employed for scenarios requiring high-performance binary storage. Dedicated Elasticsearch clusters are used to provide high-performance search capabilities.

All data at rest within Altium 365 is encrypted using AWS Key Management Service (KMS) keys. These keys use hardware security modules validated under FIPS 140-2 standards, a U.S. government computer security standard used to approve cryptographic modules. The usage of these encryption keys is logged and monitored. The logs are then sent to our Security Information and Event Management (SIEM) system, allowing us to track when the encryption keys are used.

Access to Altium 365 infrastructure that stores customer data is tightly restricted, controlled and monitored by a dedicated security team within Altium.

Secure Communication

Communication between Altium 365 clients, such as a web browser, Altium Designer, or a mobile application, and the Altium 365 cloud platform is only permitted through secure, trusted connections using the HTTPS protocol–a standard approach to secure internet communications over standard ports.

Authentication and Identity Management

To access Altium 365 services that manage sensitive customer data, users must undergo an authentication process for every request. This authentication isn't limited to traditional username and password inputs; it also integrates with Single Sign-On (SSO) systems or Identity Providers (IdPs) like Google and Facebook. These systems may use various credentials, including hardware keys, smart cards, or biometric data like fingerprints, which we do not directly control. Regardless of the method, all sessions are time-limited for security, and any sensitive login information is securely encrypted during transmission.

Altium 365 supports SSO using the SAML 2.0 protocol. This feature integrates with most modern IdPs, including OneLogin, Okta, Microsoft Azure AD, and Google Identity. Extended support of SCIM protocol allows organizing centralized user and group provisioning and de-provisioning. Depending on the IdP, you can opt for enhanced protection with multi-factor authentication (MFA).

Distribution and Control

All regions of Altium 365 are protected from the wider internet by a Web Application Firewall (WAF) and an Application Load Balancer (ALB), both integral components of AWS. This serves two primary purposes: first, to distribute incoming client (a web browser or Altium Designer) requests across the collection of Elastic Compute Cloud (EC2) instances or Kubernetes cluster evenly; second, to act as a digital barrier between the wider internet and Altium 365 internal network. Access to critical operations like server administration is strictly limited to authorized internal staff.

Multi-Tenancy Architecture

Altium 365 implements a multi-tenancy architecture that operates at the database level. That is, each individual “tenant” (currently synonymous with the concept of a “workspace”) has its own standalone, isolated schema. This helps to ensure customer data isolation.

Vulnerability Scanning

All instances related to Altium 365 must pass a vulnerability scan before going into production. Vulnerabilities found during this process are tracked and fixed at the source.

Third-Party Testing

We periodically collaborate with external third parties for penetration testing to ensure we maintain the highest level of security against ever-evolving threats. The development team reviews all feedback from penetration testing and implements necessary updates to our application services and infrastructure. We’re open to sharing the latest executive summary of our penetration test report with interested parties, provided a Mutual Non-Disclosure Agreement (MNDA) is in place.

Security Monitoring and Incident Management

We’ve implemented a comprehensive logging and monitoring practice to enable early detection and effective response to security incidents. Utilizing the NIST Cybersecurity framework as a base, logging and monitoring are key components of the "Detect" and “Respond” functions. These functions are essential for identifying and understanding security events and vulnerabilities, enhancing Altium 365 accuracy and precision. Incident identification is fundamental in our incident response process, where the security teams, systems, and tools work together to recognize and confirm potential security incidents. Once a security incident is identified we activate our Incident Response Plan to ensure a swift and effective response aligned with the organization’s security and business objectives.

Security Awareness and Training

We've implemented a comprehensive logging and monitoring Altium ensures all new hires receive security awareness training during onboarding, with annual refreshers for all staff. The Human Resources team follows up with employees who have not completed their training to ensure compliance. Additionally, we regularly send security awareness notifications to the staff, informing them of new protocols and potential threats. Our Research and Development Team undergoes specialized training in secure coding practices. The training material is periodically reviewed and updated to reflect coding practices or programming languages.

Data Privacy

The Altium General Terms of Service and Privacy Policy outline the steps we take to ensure customer data privacy and security. These documents and our supporting internal procedures adhere to global data protection regulations, including the GDPR and the California Consumer Privacy Act (CCPA). This adherence ensures the confidentiality, integrity, and availability of all data managed by Altium, including information entrusted to us by our customers and business partners. In today's competitive global business environment, it is critical to maintain data privacy to prevent threats, including error, loss, fraud, and espionage. Our approach is designed to prevent any security breaches in the data we handle.

Cookie Policy

You can manage your cookie preferences through your browser settings. Some browsers allow you to safelist sites from which you accept cookies. For more details on managing cookie preferences, see our Cookie Policy.

Data Retention Policy

If you stop using Altium 365, your data will be retained according to the timeframes specified in our Data Retention Policy. After this period expires, your data will be erased from our systems.

Backups and Disaster Recovery

Altium 365 employs an automated backup system to ensure all your data stored in Altium 365 is copied to our backup regions, eliminating manual intervention. We have a comprehensive Disaster Recovery plan to support business continuity for the production services and platforms. In the event of a system disruption, we aim for a Recovery Point Objective (RPO) and Recovery Time Objective (RTO) of 24 hours each. This plan is reviewed and tested every 120 days to confirm its effectiveness and includes detailed policies and procedures to restore services in case of a disaster.

For more information, please visit Altium 365 Trust Center and explore answers to frequently asked questions.

Altium 365 GovCloud

Altium 365 GovCloud is a dedicated region of the Altium 365 cloud platform situated within the US, operated exclusively by US Persons in the AWS GovCloud region. Choosing an Altium 365 workspace in the GovCloud region can help organizations comply with US government regulations such as ITAR and EAR.

US Persons

Operation of the GovCloud region on the Altium side is restricted to US Persons only. Altium customers determine and control who they add to their workspace and who they grant access to the data stored in the workspace.

Data Protection

Outbound Traffic Control

To safeguard against unauthorized data export, we employ an outbound proxy that controls and prevents unauthorized outbound traffic from leaving the environment.

Restricted Functionality

We have deactivated, by default, functionalities that could potentially lead to unintended data egress from the U.S., thereby mitigating risks associated with user error.

- **Sharing Outside of the Workspace**. By default, sharing projects, releases, libraries, and manufacturing packages ("Send to manufacturer" function) with persons not belonging to your Altium 365 GovCloud workspace is disabled. This setting can be modified by administrators if necessary.
- **Altium 365 Personal Space**. Users added to an Altium 365 GovCloud workspace cannot store any data in their Altium 365 Personal Spaces.
- **PLM Integration**. The administrator controls the connection to third-party PLM systems and provides the required settings.
- **Client Systems**. Altium's responsibility does not extend to the configuration, security, or maintenance of customer-side systems, such as browsers or CAD tools, that connect to Altium 365 GovCloud. The customer must keep these systems up-to-date and install all necessary updates and patches.

US Soil

AWS GovCloud US-East and US-West regions are operated by employees who are US citizens located on US soil.

Access Controls

Access to Workspace from Outside the US

Access to the workspace from outside the US is explicitly blocked, including access by US persons trying to access the workspace from another country. Learn more about VPN access here.

For more information, visit Altium 365 GovCloud.

Compliance: Certifications & Regulations

Compliance isn't just a box to tick; it's a commitment to excellence and a promise of reliability. At Altium 365, we take this responsibility seriously, ensuring that our platform meets the highest compliance and certification standards.

CSA STAR Level 1: Self-Assessment

The Security, Trust, Assurance, and Risk (STAR) program is an initiative by the Cloud Security Alliance (CSA) designed to offer a robust assurance framework for cloud computing. Altium 365 has achieved CSA's STAR Level 1, which is a self-attestation of compliance with the Cloud Control Matrix (CCM) controls, commonly known as the Consensus Assessment Initiative Questionnaire (CAIQ). Altium 365 is thus listed in the STAR Registry.

SOC 2 Type 2 Attestation

Altium 365 is Service Organization Control (SOC) 2 Type 2 attested, which confirms we uphold the highest standards of data and systems security for the security principle. This cybersecurity compliance framework was developed by the American Institute of Certified Public Accountants (AICPA) and requires businesses to undergo an audit by an external AICPA-accredited auditor. Altium 365 performs SOC 2 Type 2 audits on a yearly basis.

GDPR

We recognize the significance of data privacy and are committed to upholding the stringent requirements set forth by the General Data Protection Regulation (GDPR), ensuring that your data is handled with the utmost care and respect.

ITAR Compliance and CMMC Level 1 Self-Attestation

The Altium 365 GovCloud can help our customers reach compliance with the International Traffic in Arms Regulations (ITAR) and boasts a CMMC Level 1 Self-Attestation. This specialized region meets the specific needs of our users who operate in highly regulated industries.

Compliance: Next Steps

Recognizing the critical importance of compliance standards, we are excited to share with you the next steps in our certifications. These milestones represent our ongoing dedication to safeguarding your data and ensuring the integrity of your work on Altium 365.

ISO 27001 Certification

We are actively working towards obtaining the ISO 27001 certification, a globally recognized standard for managing information security. This certification will support our international customers' enterprise risk programs, providing an added layer of confidence in our platform's security measures.

NIST 800-171 Self-Attestation and Third-Party Validation

Altium 365 is working toward adherence to NIST 800-171 Self-Attestation. We have obtained an Attestation Letter for our current System Security Plan (SSP) and Plan of Actions and Milestones (POA&M) from a certified third party to provide Altium 365 GovCloud customers with infrastructure that supports the security requirements for CUI data.

FedRAMP Certification

Altium 365 is currently working towards FedRAMP Moderate Impact Level Certification to better support our customers' demands. This step will enable US federal agencies, participating state and local (SLED) agencies, and third-party companies working with CUI to use Altium 365 for their electronic design and collaboration needs, ensuring compliance with the highest standards of security and compliance set by the U.S. government.

AWS Sovereign Cloud Region: Catering to EU Regulations

To better support regulated industries in the European Union, we are closely examining the potential of AWS's new region–Sovereign Cloud. This initiative aims to understand how Altium 365 can leverage this new region to meet the unique regulatory and data needs of the EU market.

Altium 365 Advanced Security Package

The Altium 365 Advanced Security Package is a step up in our security offerings, adding additional security capabilities. With advanced accessibility controls and a more transparent view of audit logs, you get a more secure and controlled experience on the Altium 365 platform. Discover what this advanced package can do for you!

Audit Logs

Audit logs in Altium 365 document each event, detailing when it happened, who was responsible, and what entity was affected. Recorded events include:

- User additions or deletions
- Changes in role memberships
- Modifications to access controls,
- Creation or deletion of objects

IP Whitelisting

By default, authorized users can access your organization's resources from any IP address, except in the case of Altium 365 GovCloud, which is restricted to US-based IP addresses only. However, you can enhance security by configuring a safelist of specific IP addresses, limiting access to your organization's private resources to these designated IPs.

Next Steps

We're further developing enhanced security control capabilities for Altium 365, focusing on Secure Sharing controls and Advanced Reporting Visibility.

Stay Informed on Our Latest Security Updates

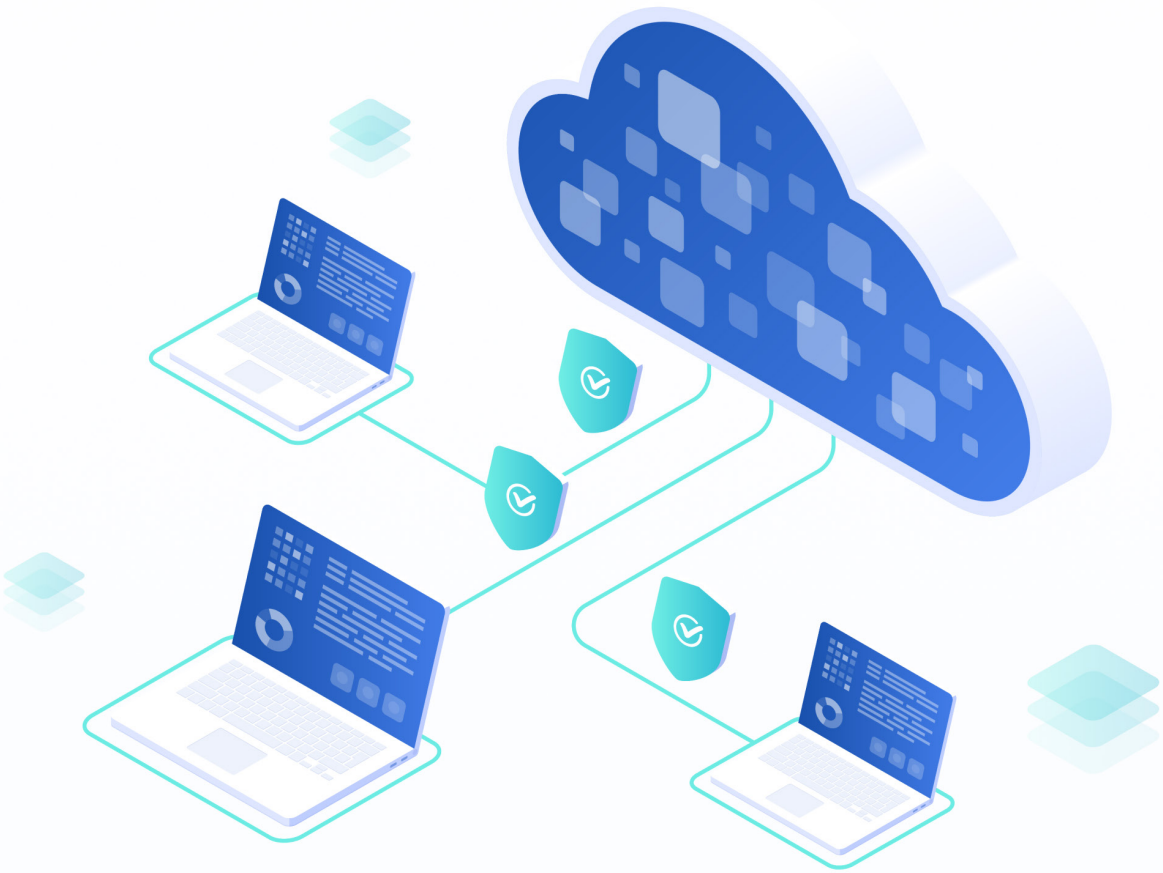
Altium 365 is the electronics development platform that brings together all aspects of electronics development, helping organizations deliver better products faster than ever before. This comprehensive ecosystem is designed to streamline the development process, foster collaboration, and enhance productivity. With its robust security measures, Altium 365 ensures that while your teams accelerate their pace of innovation, they do so with the confidence that their data and designs are protected by the highest standards of security.

The journey of Altium 365 is one of continuous improvement and adaptation to the ever-changing landscape of electronics design and data security. We are dedicated to providing you with a platform that not only meets your current needs but also anticipates and adapts to future challenges and opportunities.

Stay tuned for future updates and enhancements as we keep evolving Altium 365 to be your platform of choice, where security and innovation go hand in hand.

Schedule a personalized security consultation to see how Altium 365 can meet your specific security needs.

Book a meeting



The information provided in this whitepaper is accurate as of February 2024. Please note that Altium 365 is an evolving platform. For the latest version of this document, pleas visit this page