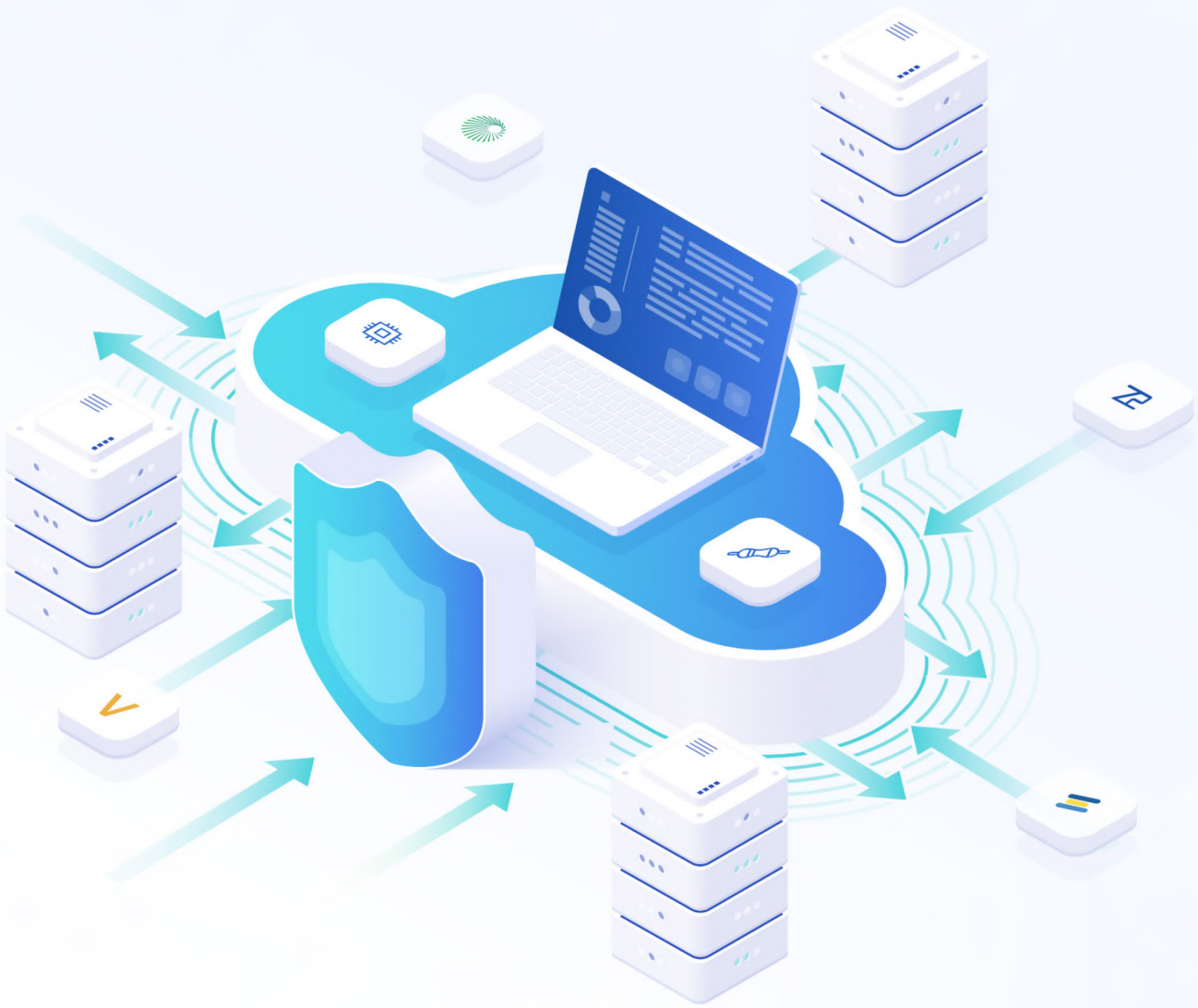
ALTIUM 365

Altium 365 Security Approach & Practices



CONTENT

Introduction

Altium 365 is the electronics development platform that unifies design, data, and collaboration into a single, secure cloud environment. Built to support the full lifecycle of electronics development, it provides the modern infrastructure engineering teams need to work faster, more efficiently, and at scale. Included with Altium Agile and Altium Develop, the platform streamlines workflows, enhances productivity, and accelerates product delivery.

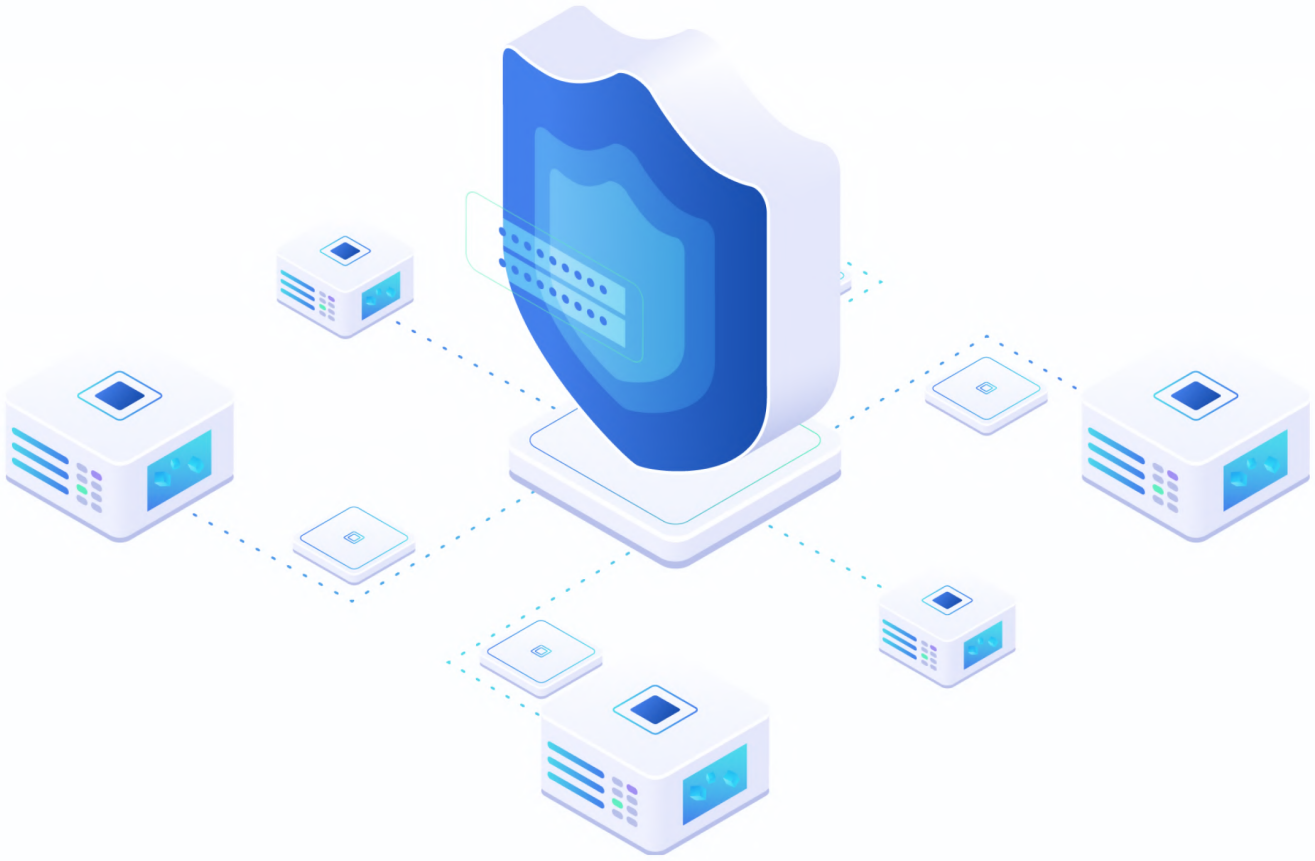
At Altium, we believe a cloud platform's true value is measured not only by what it enables, but by how securely it protects the work entrusted to it. Security is embedded into the core of Altium 365's architecture, guiding how we design, build, and operate the platform. This commitment drives us to meet—and continually exceed—modern cybersecurity standards.

This whitepaper provides a clear, transparent view of the extensive security measures that underpin Altium 365. Our goal is simple: to show you how your data is protected, how our safeguards are engineered, and how our security posture evolves to stay ahead of emerging threats.

As you move through these pages, you'll gain insight into the planning, processes, and protection mechanisms that shape our approach—from secure development practices to the layered controls embedded throughout the platform. You'll see how our engineering rigor, operational discipline, and cloud-native architecture work together to safeguard your data at every stage.

Ultimately, our aim is to give you the peace of mind that comes from knowing your collaborative work on Altium 365 is protected by a robust, continuously evolving security framework. We want you focused on creating and innovating—while we take care of the security that protects it.

This document describes Altium 365 security approach and practices at the platform level; specific capabilities may vary by subscription, deployment environment (e.g., GovCloud), and customer configuration.



Altium 365 Security Measures

Security is the foundation of trust, and our customers rely on Altium 365 to protect their most valuable assets—their data, designs, and intellectual property. Security is built into every layer of the platform, from early architecture and development through deployment and ongoing operations. Our approach is meticulous, proactive, and continuously evolving, creating a secure and resilient environment for collaborative electronics development.

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.

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 hosts customer data is limited to authorized personnel based on the principle of least privilege. All access is logged, auditable, and continuously monitored by Altium's dedicated security team.

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

Altium 365 employs layered perimeter protections to control and inspect inbound traffic, including web application firewalling and managed load balancing. These controls help protect internet facing endpoints and support availability by distributing traffic across application services. Administrative access to production systems is restricted to authorized personnel on a least-privilege basis and is logged and monitored.

Single-Tenancy and Multi-Tenancy Architecture

Altium 365 operates on a multi-tenancy architecture in which each tenant—currently aligned with the concept of a workspace—receives its own isolated database schema. This model provides strong data separation while leveraging shared cloud infrastructure for efficiency and scale. For organizations requiring deeper isolation, customization, and operational control, Altium offers a Single Tenant Environment (STE): a dedicated instance of the application and its supporting infrastructure. STE delivers high data isolation, predictable performance, and tenant-specific configuration options, combining the convenience of a hosted service with the control traditionally associated with on-premises deployments.

Vulnerability Scanning

Production deployments for Altium 365 are subject to vulnerability scanning as part of the release process. Findings are tracked through remediation or documented risk acceptance in accordance with Altium's Vulnerability Management policy and defined remediation timelines.

Third-Party Testing

We annually 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

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

Altium 365 GovCloud can help our customers reach compliance with the International Traffic in Arms Regulations (ITAR). 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 watching 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. The latest update from AWS says Sovereign Cloud will be .

Altium 365 Security and Governance Capabilities

Altium provides advanced security, identity, and governance capabilities that help organizations protect sensitive design data, maintain compliance, and manage access at scale.

Access Control

- **Basic Data Permissions**
  Foundational view and edit rights that define how users interact with files, folders, and projects across the platform.
- **Advanced Data Permissions**
  Controls that extend beyond basic access rights, including organization-level sharing rules, granular permission settings, and advanced inheritance options that shape how data is accessed or restricted across teams.
- **Group Management**
  Standardizes permissions, licenses, and workspace visibility by assigning access based on defined roles, ensuring consistent and scalable control across the organization.
- **Support for External Guests**
  Controls how external collaborators are invited, grouped, and limited, with visibility rules and enforced workflows that keep guest access contained and secure.
- **Access Filter**
  Search and audit effective access across all projects, with quick adjustments and one-click guest removal.

Authentication & User Provisioning

- **Organization Management**
  Defines how users join the organization, how roles are assigned, and how domain-based rules govern identity and access to internal resources.
- **Single Sign-On (SSO) & SCIM**
  Integrates with your existing identity provider to centralize authentication and automate user provisioning and deprovisioning through SCIM.
- **Multi-Factor Authentication (MFA)**
  Strengthens account security by requiring an additional verification step, reducing the risk of unauthorized access even if credentials are compromised.
- **Group Management**
  Supports identity provisioning by aligning users with predefined roles and access profiles during onboarding and throughout their lifecycle.

Advanced Security

- **IP Whitelisting**
  Restricts platform access to approved IP addresses or ranges, ensuring that only trusted networks can reach sensitive organizational data.
- **Event Log**
  Provides visibility into user and system actions across the workspace, supporting auditing, security reviews, and compliance reporting with clear, timestamped activity records.
- **SIEM (API)**
  Connects Altium Agile event data to your existing SIEM, enabling centralized analysis, alerting, and compliance tracking across your organization.

Stay Informed on Our Latest Security Updates

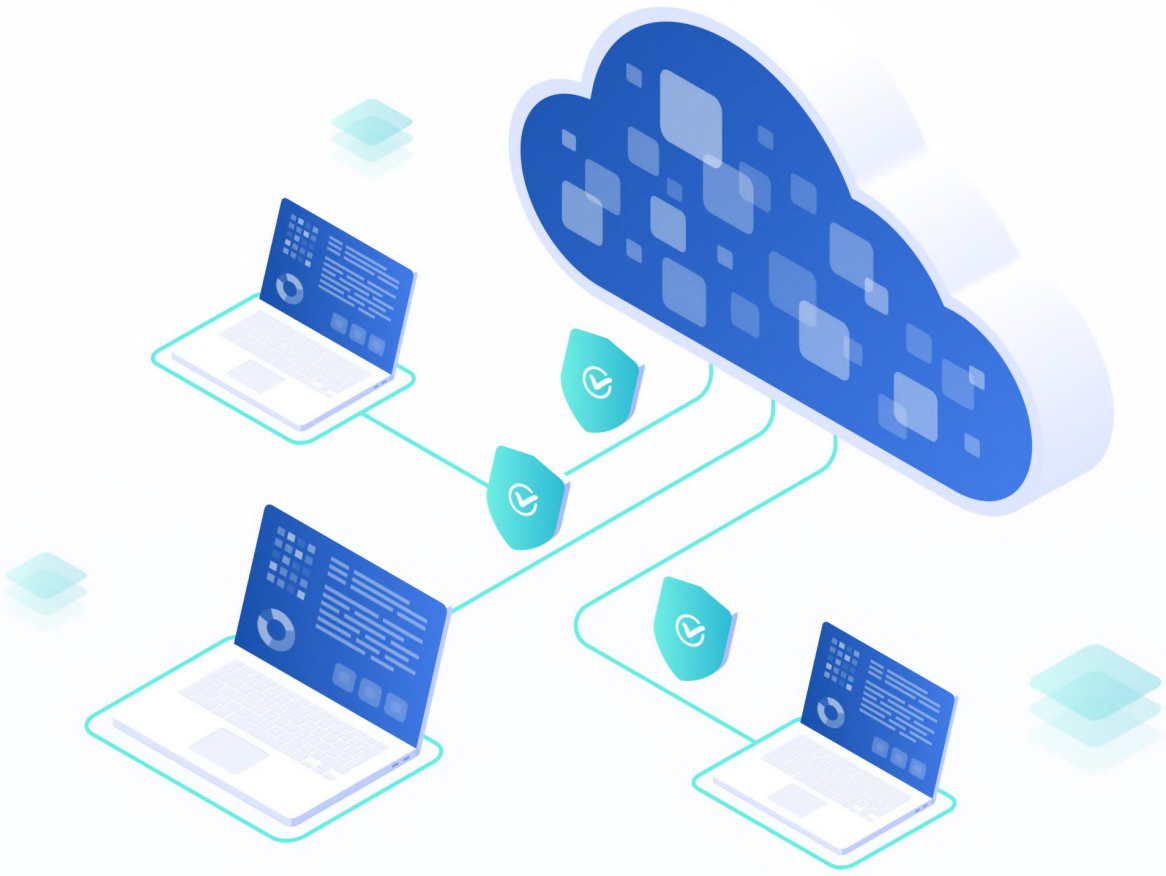
Our platform continues to advance with new capabilities that strengthen governance, enhance visibility, and support the security requirements of modern electronics organizations. Security remains foundational, and every update is designed to help teams move quickly while maintaining control of sensitive and regulated data.

As the landscape of electronics development and data protection evolves, we evolve with it. Our focus is on delivering practical, scalable improvements that m

Stay tuned for ongoing enhancements as we expand controls, deepen monitoring, and reinforce protections—ensuring that security and innovation remain aligned.

For additional details and related resources, visit altium.com

Want to find out more? www.altium.com/platform/trust



The information provided in this whitepaper is accurate as of February 2026. Please note that Altium 365 is an evolving platform. For the latest version of this document, please visit this page.