elegancegroup

ATLASSIAN

Atlassian Cloud security shared responsibilities

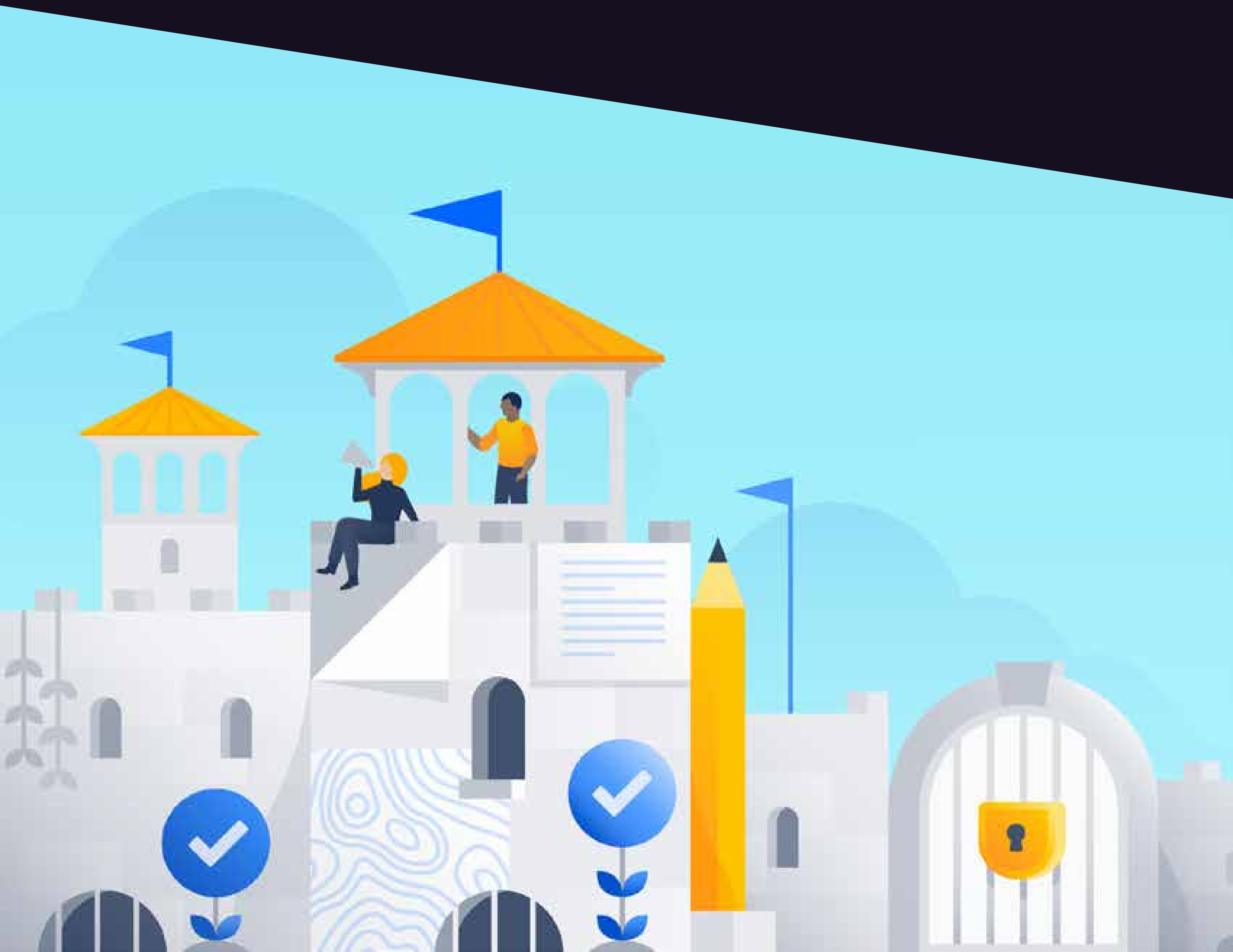

Table of contents

The shared responsibilities model

In Cloud, Atlassian focuses on the security of the applications, the systems they run on, and the environment those systems are hosted within. They ensure your systems and environments are compliant with relevant standards, including ISO27001, ISO27018, SOC2, GDPR, and many others that live with the Trust Center.

You, Atlassian customers, manage the data within your accounts, the users and user accounts accessing your data, and control which Marketplace Apps (formerly called "add-ons") you install and trust. When using Atlassian applications, you are responsible for ensuring your organization is using Atlassian Cloud products in a compliant way.

As Atlassian evolves their cloud offerings, they will continue to keep security and compliance a top priority. This paper will discuss the actions Atlassian takes to protect your data, and how your local Solution Partner can help guide you as we all embark on the journey together.

Responsibilities

Atlassian	Shared
• System	• Policy and compliance
• Hosting	• Users
• Application	• Information
	• Marketplace apps

The four pillars of trust at Atlassian

Atlassian believes all teams have the potential to accomplish incredible things. Their mission is to unleash that potential in every team of every size and industry, and in turn, create a more connected world through the power of software.

Customer trust is at the center of everything Atlassian does and why security is their top priority. Atlassian is transparent with their security program so you can feel informed and safe using Atlassian products and services.

Security

Atlassian Cloud products, infrastructure, and processes are designed with security in mind. Atlassian takes the responsibility of protecting your organization's data seriously, and Atlassian's approach to security is based around their responsibility to be an industry-leader in Cloud and product security.

The security section of the Trust Center outlines Atlassian's detailed approach and proactive security protocols.

Reliability

Atlassian Cloud is built to support organizations by providing a reliable platform that can dynamically scale as you grow. Atlassian approaches this by focusing product development on resiliency, the ability to help you scale, and Atlassian's product performance.

Atlassian keeps internal teams accountable by instituting SLAs, publishing the service availability status, and sharing their approach to improved QA process and performance. You can review Atlassian's in-depth approach at Reliability at Atlassian.

Privacy

You own your data, and Atlassian is committed to protecting the privacy of your data. Atlassian's Privacy Policy explains what information is collected about you and why, what Atlassian does with that information, how it's shared, and how the content you place in Atlassian products is handled and services. Atlassian Guidelines for Law Enforcement Requests outlines the process for how Atlassian receives, scrutinizes, and responds to government requests for customer information.

This information, and more, is always available within the privacy section of the Trust Center.

Compliance

A critical aspect of Cloud migrations is validating compliance and entrusting the right Cloud partner for your organization. At Atlassian, compliance certification across geographies are actively growing and industries in order to meet your needs. Atlassian strives to adhere to widely accepted compliance standards and actively monitor evolving regulations with a proactive approach. Atlassian tests out their operations, environment and controls using independent, third-party advisors.

Atlassian's compliance section within the Trust Center provides comprehensive information about the Compliance Program and Atlassian's growing list of certifications.

Decisions, decisions

Your key decisions

The decisions you make about how you set up Atlassian products significantly influence the way security is implemented.

Key decisions include:

- **Domain verification & centralized management.** You can verify one or multiple domains to prove that you or your organization own those domains. Domain verification and user claim allows your organization to centrally manage all its employees' Atlassian accounts and apply authentication policies (including password requirements, multi-factor authentication, and SAML). After verifying your domain, you claim all users with existing Atlassian accounts under that domain. Anyone signing up for a new Atlassian account with that domain will see that they are getting a managed account.
- **Granting access to your data.** Atlassian products are designed to enable collaboration, which requires access. But you do need to be careful about granting permissions to access your data to other users, and to Marketplace Apps. Once you grant such permissions, Atlassian will not be able to prevent those users from taking the actions allowed under those permissions, even if you don't approve of those actions. In some products you have the ability to grant public anonymous access to your data. If you permit such access, you may not be able to prevent that information being copied or further distributed.
- **Centralized user access management:** Atlassian customers are strongly encouraged to use Atlassian Access for centralized administration and enhanced security across all Atlassian products they use (including use of enforced 2FA and single sign-on).

Atlassian doing their part

Atlassian's Trust Management Program takes the security requirements of Atlassian customers into consideration, along with industry standards and expectations, and arrives at a set of requirements unique for the company. Atlassian's trust strategy is built around the following themes:

- Continually enhancing security in Atlassian applications, platform, and the environment to provide a compelling standard in Atlassian products and services–commonly known as continuous improvement.
- Being open and transparent about Atlassian programs, processes, and metrics. This includes sharing the Atlassian journey and encouraging other cloud providers to do the same, and setting new standards for customers.
- Identifying present and future security threats to Atlassian and its customers, and limiting the impact and duration of security incidents.

Details of Atlassian's initiatives are provided on the Trust Center, where you can download or request Atlassian's certification reports for ISO 27001 and SOC2, and can follow a link to review Atlassian's Cloud Security Alliance (CSA) STAR questionnaire. You can also view details of the Atlassian Controls Framework developed by Atlassian to bring together the security requirements of seven international standards, which underpins their approach to security and compliance.

The CSA STAR entry includes answers to more than 300 questions included in the Consensus Assessments Initiative Questionnaire (CAIQ). As with this paper, Atlassian's CAIQ entry covers Jira, Confluence, Bitbucket, Halp, Jira Align, Opsgenie, Statuspage, and Trello, and they will add entries for other products as needed. Those controls are then verified via various audits associated with SOC2, ISO 27001, and PCI DSS.

Shared responsibility

In the security model shown on the first page, four areas are identified as a shared responsibility.

These are:

Policy and Compliance: The approach meets your business needs and is operated in accordance with industry, regulatory, and legislative compliance obligations

Users: The creation and management of user accounts

Information: The content you store within Cloud

Marketplace Apps: Third party services which you give access to your information and the ability to integrate with Atlassian products

This is how the responsibilities across these areas split out:

Policy and compliance

Atlassian's role	Your role
• Consider the risk profile of Atlassian customers when assessing the need for security controls • Have a comprehensive security risk management program in place and effectively implement the controls detailed in the CSA STAR response • Keep customers updated about compliance certifications and what Atlassian is doing to support • Make available the information you need to make decisions about Atlassian platforms • Ensure Atlassian's system has failover and redundancy built in • Receive and manage vulnerability reports related to Atlassian products • Adhere to the laws of the various jurisdictions Atlassian operates in	• Understand your risk profile and the sensitivity of your data • Assess the suitability of Atlassian Cloud-based platforms based on the information we provide • Ensure the platform is sufficient to meet your compliance needs • Meet the agreed upon data breach disclosure and notification requirements when relevant • Protect your endpoints through good security practices • Only host permitted data on Atlassian platforms • Operate within the law of the jurisdictions in which you operate

Users

Atlassian’s role	Your role
• Develop and roll out security controls that empower you to manage your users effectively • Monitor Atlassian platforms for bad or malicious use • Provide domain verification and user claim capabilities for a centralized view of users across your cloud organization • Provide the option for Atlassian Access for more efficiency and control by allowing you to connect your identity provider to (1) enforce SSO or 2FA/MFA and (2) automate SCIM user provisioning • Provide implementation and user support via Atlassian internal teams • Develop products and features that encourage organization-wide insights on usage and growth	• Verify your domain if you want to centrally manage your accounts • Approve user access to your data • Periodically review the list of users with access to your data and remove access from anyone who shouldn’t have it • Determine Authentication policies in Atlassian Access | Atlassian based on your users and organizational needs • If you have a verified domain: • Implement strong user access management controls such as federated identity management (SAML), two-step verification, and password policies as needed based on your risk • Monitor your organization’s user accounts for harmful or malicious use • Set a password policy appropriate for your business • Notify Atlassian of any unauthorized use of your organization’s accounts • If you don’t have a verified domain, or if you grant access to users outside your domain: • Communicate the importance of good password management to all users with access to your data • Notify Atlassian of any unauthorized use of your account • Be aware of the risks of social login (see ‘Credential re-use’ below)

Information

Atlassian’s role	Your role
• Access your data only if there is a specific support need to do so • Notify you of any breach we become aware of that affects your data • Maintain system-level back-ups (which includes your information)	• Set up your Atlassian products to reflect the information accessibility that fits your needs • Create backups of your data

Marketplace Apps

Atlassian’s role	Your role
• Ensure all Cloud apps meet a baseline of security. They are continuously scanned and reviewed for vulnerabilities when listed on the marketplace • Verify the developers of Marketplace Apps • Require the developed to publish their privacy policies Data privacy guidelines for developers • Invite app vendors/partners can join the Cloud Security Participant or Cloud Fortified programs by investing in their own bug bounty program and increase support and reliability • Maintain Forge, a program in which Atlassian hosts the Cloud apps and enables app vendors to more easily leverage infrastructure investments to meet higher security and reliability standards	• Assess the suitability of any Marketplace Apps you want to use based on the information they provide • Notify Atlassian of any malicious behavior identified in a Marketplace App

Threat management

Preparation is key

Atlassian's security team is a big proponent of threat modeling, and spends a lot of time considering the scenarios to look out for, and the 'plays' Atlassian will run if and when those scenarios eventuate. Atlassian will help share some of the threats that you may need to consider when using their applications. Hopefully, these will help bring to life the joint responsibility outlined above.

Credential guessing

A malicious user may be able to guess a correct username and password combination and gain access to your account. Having strong passwords, and enabling multi-factor authentication, are the best controls to manage those risks. As noted in the guiding principles, if Atlassian see something affecting lots of users, they'll do their best to shut it down.

Credential re-use

If one or more of the accounts you have permitted to access your data uses the same email address and password combination elsewhere on the internet, a compromise of that site may expose your data to attackers. Similarly, approving access for users who use social login introduces a risk to your data in the event of a breach of that user's social account. Good security awareness across your user base (including third parties you have granted access), and two-step verification are strong controls.

Man-in-the-middle attacks

An attack that seeks to insert itself between your browser and Atlassian's server relies on you accepting the malicious system's certificate as valid. Atlassian will set up their systems to make this difficult for an attacker, but security awareness and certificate inspection are best practices.

Endpoint compromise

The compromise of one of your endpoints (whether your laptop, desktop, tablet, or smartphone) will render all other controls ineffective. The using of up-to-date security software and keeping your systems fully patched are the best controls.

Malicious Marketplace apps

Once you install and grant permissions to a Marketplace app, Atlassian will not be able to prevent that app from taking the actions allowed under those permissions, even if you don't approve of those actions. Reviewing the suitability of the app and the reasonableness of the requested permissions prior to installation is recommended.

Phishing or fake sites

As a cloud-based system, anyone can set up a website purporting to be Atlassian. Making sure that you're at the right site is important to ensure your data stays safe. Typing the URL into the browser directly, or using a bookmarked link is a good mitigation, and checking the certificate is worthwhile if in doubt.

Shared responsibility and shared success

When it comes to the security of your data in the Atlassian Cloud, we are all on the same team, and have important roles to play. Atlassian has a strong team of security professionals working day and night to ensure security is built in to their products, to monitor for potential risks and attacks, and to respond rapidly when they're identified. Your role is to help establish the effectiveness of your user access management, being conscious of the information you enter, making sure your endpoints are well managed, and verifying all Marketplace apps are appropriate and trustworthy. As your dedicated Solution Partner, our team is here to provide you with hands-on support and recommendations that work best for your business so that you can focus on