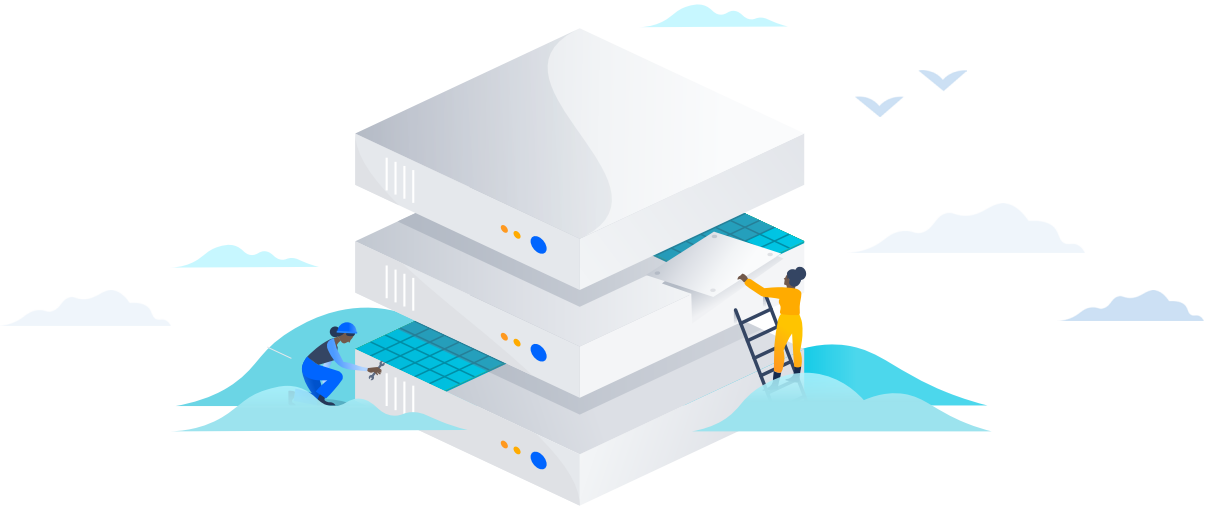
ATLASSIAN



Atlassian Cloud Security Shared Responsibilities

We're on the same team

We understandably receive a lot of questions from our customers as to how Atlassian is taking appropriate action for the protection and confidentiality of our customer's data as a cloud service provider.

The responsibilities detailed in this paper are broadly applicable across our product suite, but are specifically written in the context of Confluence Cloud, Jira Cloud, Stride, and Bitbucket Cloud.

At a high level, Atlassian handles security of the applications themselves, the systems they run on, and the environments those systems are hosted within. We ensure your systems and environments are compliant with relevant standards, including PCI DSS and SOC2, as required.

You, our customers, manage the information 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 our applications, you are responsible for ensuring your business is meeting your own compliance obligations.

In the cloud, the security of your data on our systems is a joint responsibility. We developed this paper to explain what actions we take to protect your data, and what you can do to help us, help you best.

Trust @ Atlassian

Our goal is to build trust with every team. Across our five pillars of trust, we value complete transparency in what we do, and why we do it.

Security

Our customer-focused culture makes security a top priority. We are open and transparent with our security program, so you can feel safe using our products and services.

Availability

We understand that in order for a cloud service to be useful, it has to be available. This starts with ensuring services are built on top of a solid platform of core technologies. We are proactive about hunting down possible points of failure, and we stress-test relentlessly. We publish our service availability status in real-time, so you can access your data when you want.

Quality

Atlassian's QA team works with our development teams to ship features quickly and safely. At Atlassian, we've optimized the QA process by educating and empowering developers to test their own features to our quality standards.

Privacy

You own your data, and we're committed to protecting the privacy of your data. Our Privacy Policy explains what information we collect about you and why, what we do with that information, how we share it, and how we handle the content you place in our products and services. Our Guidelines for Law Enforcement Requests outlines our process for how we receive, scrutinize, and respond to government requests for customer information.

Compliance

We know you need to validate compliance to trust a cloud service provider. We work hard to attain certifications and strive to adhere to widely accepted standards and regulations to keep you at ease. We test our operations, environment, and controls using independent third-party advisors and publish their reports and opinions as they become available.

Our guiding principles

Atlassian is well known for our values, and those values genuinely influence everything we do—including our approach to shared security responsibilities in the cloud. In practice, our values have led us to the following guiding principles about shared responsibility:

If it's bad for the platform, it's our problem

We are running platforms which support numerous teams and users. When an issue affects the integrity or trustworthiness of the platform, it's a problem we need to solve.

Our first instinct is always to help your team

Our customers come first. Even if the answer is ultimately that we can't solve your problem, we'll do everything within our power to help.

We will be transparent about what we do

We know that honesty and integrity are key to any relationship. We will be as transparent as possible about the way we do things.

We believe in defense in depth

We implement layered controls and make sure all parties who are a part of the Atlassian ecosystem are rowing in the same direction. Atlassian, our suppliers, and our customers are one team when it comes to the security of our customers' information.

Your actions can trump our controls

We want our relationship to be built on mutual trust and responsibility. We can't tell who is sitting at a computer entering your email address and password. If you've given those credentials to someone else and they abuse your account, unfortunately there's not much we can do.

Your key decisions

The decisions you make about how you set up our products have a significant influence on the way security is implemented. Key decisions are:

- **Domain verification & central management.** You can verify one or multiple domains to prove that you or your organization own those domains. Domain verification allows your organization to centrally manage all its employees' Atlassian accounts and apply authentication policies (including password requirements and SAML). After verifying your domain, all users with existing Atlassian accounts under that domain will receive an email explaining that they are transitioning to a managed account. Anyone signing up to a new Atlassian account with that domain will see that they are getting a managed account.
- **Granting access**. Our 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, we 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.

Doing our part

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

- Continually enhancing security in "all the things" to provide a compelling standard in our products and services—commonly known as continuous improvement.
- Being open and transparent about our programs, processes, and metrics. This includes sharing our 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.

Detail of our initiatives is provided on the Trust @ Atlassian page, where you can download or request Atlassian's certification reports for ISO 27001 and SOC2, and can follow a link to review our CSA STAR questionnaire. You can also view details of the Atlassian Controls Framework we have developed to bring together the security requirements of seven International standards, which underpins our approach to security and compliance.

Atlassian control framework

The CSA STAR entry includes answers to more than 300 questions included in the Consensus Assessments Initiative Questionnaire (CAIQ). As with this paper, our Atlassian CAIQ entry covers our Jira and Confluence Cloud, Stride and Bitbucket Cloud offerings. 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:

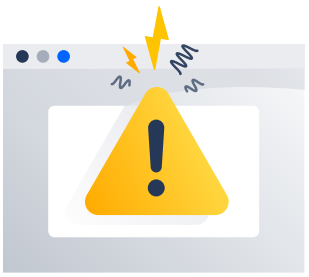
- **Policy and compliance:** Ensuring that the system meets your business needs and is operated in accordance with industry, regulatory and legislative compliance obligations
- **Users:** The creation and management of user accounts
- **Information:** The content you store within Confluence Cloud, Jira Cloud, Stride or Bitbucket 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 between us:

	What we do	What you need to do
Policy and compliance	Consider the risk profile of our customers when assessing the need for security controls Have a comprehensive security risk management program in place and effectively implement the controls detailed in our CSA STAR response Be clear about our compliance state and what we can't yet support (e.g., HIPAA) Make available the information you need to make your decisions about our platforms Help you to respond to cyber security incidents Ensure our system has failover and redundancy built in Receive and manage vulnerability reports related to our products Operate within the law of the various jurisdictions we operate in	Understand your risk profile and the sensitivity of your data Assess the suitability of our cloud-based platforms based on the information we provide Ensure the platform is sufficient to meet your compliance needs Meet your data breach disclosure and notification requirements when relevant Protect your endpoints through good security practices Only host permitted data on our platforms (e.g., Not HIPAA-related or personally identifiable information) Operate within the law of the jurisdictions in which you operate

Continued on page 5

	What we do	What you need to do
Users	Develop and roll out security controls that empower you to manage your users effectively (e.g., https://www.atlassian.com/enterprise/cloud/identity-manager) Monitor our platforms for bad or malicious use	Verify your domain (https://confluence.atlassian.com/cloud/domain-verification-873871234.html) 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 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 (https://www.atlassian.com/enterprise/cloud/identity-manager) • Monitor your organization's user accounts for bad or malicious use • Force password changes when needed • 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	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 you want (e.g., anonymous access, public/private repositories) Create backups of your data
Marketplace Apps	Verify the developers of Marketplace Apps Receive and manage vulnerability reports related to Marketplace Apps	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



The threats you need to manage

Our security team is a big proponent of threat modeling, and spend a lot of time considering the scenarios we need to look out for, and the 'plays' we will run if and when we see those scenarios eventuate. We thought it might help to share with you some of the threats that you may need to consider when using our applications. Hopefully, these will help bring to life the joint responsibility we've discussed 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 two-step verification, are the best controls to manage those risks. As noted in our guiding principles, if we see something affecting lots of users, we'll do our 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 good controls.

Man-in-the-middle attacks

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

Endpoint compromise

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

Malicious Marketplace Apps

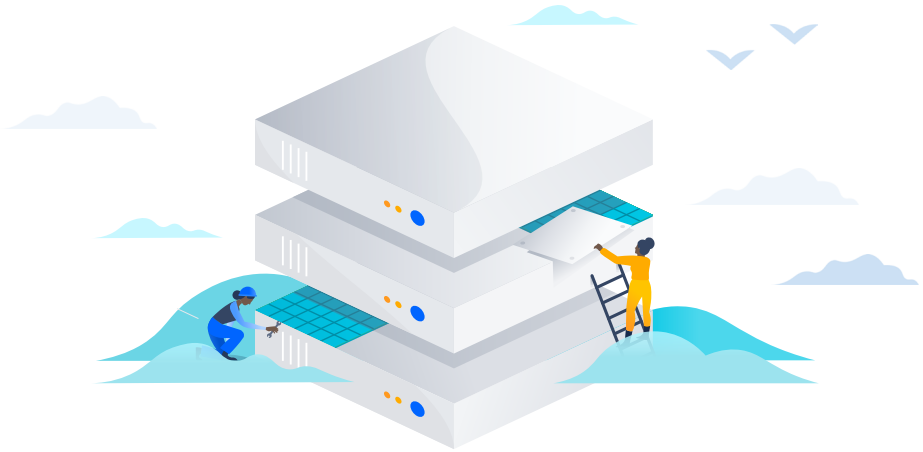
Once you install and grant permissions to a Marketplace app, we will not be able to prevent that app from taking the actions allowed under those permissions, even if you don't approve of those actions. Reviewing the suitability of the app and the reasonableness of the requested permissions prior to installation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

Phishing or fake sites

As a cloud-based system, anyone can set up a website purporting to be us. 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.

In summary

When it comes to the security of your data in the Atlassian Cloud, we are on the same team, and we both have important roles to play. We have a strong team of security professionals working day and night to ensure security is built in to our products, to monitor for potential risks and attacks, and to respond rapidly when they're identified. We need you to help by establishing 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.



Want to dig deeper?

We've referred to quite a few other documents and resources in this brief paper, and we encourage you to dig into them if you want to understand more about our approach to security and trust. Here are some good links to get you started:

Trust @ Atlassian

Atlassian's CSA STAR entry

The Atlassian Controls Framework

Our Customer Agreements

Atlassian Privacy Policy

Atlassian Security Incident Responsibilities

We're here to help

We've gathered the most popular questions and answers. Please don't hesitate to reach out to us with any questions or support needs.

FAQs

Contact us