



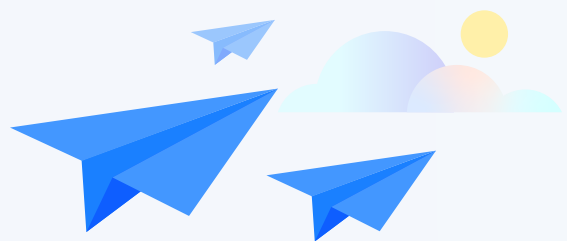
Atlassian Cloud Data Protection



 **ATLASSIAN**

Table of contents

3	Introduction
8	Section 1: Atlassian cloud infrastructure layer
12	Section 2: Data Protection, management, and controls
14	Data recovery
16	Data security
20	Protect sensitive data by limiting access
20	Meet data residency regulatory requirements
22	Privacy and compliance
25	Identity and access management
28	Section 3: Centralized admin
30	Monitoring and reporting
33	Product and org lifecycle management
35	Section 4: Atlassian Marketplace
36	Marketplace data security
41	Security-related issue resolution
44	Marketplace privacy
46	Apps and data management
48	Compliance and marketplace apps
51	Transparency & control
55	Conclusion



Introduction

Data is the most critical asset to your organization, yet, it's becoming increasingly more challenging to protect and secure. If data isn't protected correctly, the cost of a data breach is costly. In 2022, **IBM reported** that the average cost of a data breach was 4.35 million dollars. *What are the challenges?*

Managing complex and interconnected IT systems

Managing your IT infrastructure is a lot of work. The number of products and apps that teams use continues to grow. On average, enterprises use between **100 - 200 applications**, with many of them managed by lines of business outside your IT department.

Regardless of ownership, these apps and products are used in concert so data can flow between them to enable collaboration between cross-functional teams. Complex, multi-app environments increase the attack surface and introduce risk due to varying levels of security across different apps.

Ensuring that only the right people can access data

As your organization grows, more people, devices, and applications access your data – increasing the risk of unauthorized access. Striking a balance between keeping people productive and narrowing access points only becomes more difficult.

Adapting to regulatory requirements

Industries and geographies have requirements that specify what controls must be in place to meet regulatory obligations and keep personal data safe. But the landscape is constantly evolving, and the requirements are a moving target that takes time to keep track of. Plus, these governing bodies are putting more onus on organizations like yours to prove compliance with these requirements.

Keeping sensitive data secure

Your company's data is important, but some can be more sensitive, such as legal information or employee records. Correctly classifying data and applying appropriate safeguards is critical to protecting sensitive data like PII, credit cards, etc.

Recovering from outages	<p>An outage's impact on an organization only increases at scale. On average, one minute of downtime can cost an enterprise \$9,000. Multiplied by the total amount of downtime, an outage can cost hundreds of thousands of dollars.</p> <p>But outages don't just impact your revenue. They can also cause business disruptions, internal productivity loss, financial penalties, and litigation.</p>
Detecting and responding to threats	<p>You can't control threats you can't see. Your organization must have built-in threat detection, monitoring, and reporting features. Many products don't offer out-of-the-box solutions, which requires organizations to manage additional products that add to their already exhaustive list of applications.</p>
Evaluating Marketplace app security and privacy	<p>Marketplace apps provide flexibility to customize and extend your complete solution. However, many apps are built and managed by third parties.</p> <p>Installing an app requires a separate relationship with the company that offers the app. It's important to vet the apps on your instance, as they may handle data differently than the product they're extending.</p>

Compounding these challenges are good and bad actors – people.

Good actors: You may have a dedicated security team responsible for protecting your data, but most people in your org aren't experts. They aren't considering how their actions can contribute to a data breach. For example, many people reuse their passwords. If these credentials are compromised, hackers can access your organization's data.

Bad actors: Unfortunately, some people are actively looking to gain unauthorized access to your data and harm your business. In some cases, this can be disgruntled employees, but hackers often look to exploit vulnerabilities in your environments.

“ The human element continues to drive breaches. Whether it is the use of stolen credentials, phishing, or simply an error, people continue to play a large part in incidents and breaches alike.

VERIZON, DATA BREACH INVESTIGATION REPORT (DBIR) 2022

Overcoming these challenges isn't impossible, but you need the right tools. That's why we've specifically built Atlassian cloud products and solutions with the features and capabilities that you need to protect your data.

Secure collaboration through a connected platform and shared responsibility

Unlike self-managed environments, cloud operates under a shared responsibility model, which means that protecting your data becomes a partnership between you and Atlassian.

- **Atlassian:** Ensure the infrastructure that supports our cloud products is secure.
- **You:** Manage the information within your account and the users and user accounts accessing your data in line with your compliance obligations.



When you install a Marketplace app, you introduce a third party into this equation. App installation requires a relationship with a Marketplace Partner separate from your relationship with Atlassian.

In this context, Atlassian and Marketplace Partners both play an important role in a new shared responsibility model:



Marketplace Partners	Marketplace Partners are responsible for their own infrastructure. They are responsible for: <ul style="list-style-type: none">• Designing apps and operational processes according to their legal obligations, Atlassian’s developer guidelines, and general industry best practices for building and maintaining reliable, compliant, and secure apps.• Providing support and information to help customers make informed decisions.
-----------------------------	---

Atlassian	Atlassian is responsible for the security of our own infrastructure and for supporting partners and customers: <ul style="list-style-type: none">• We provide documentation, security standards, and capabilities to help partners build trustworthy apps in line with accepted industry practices.• We are also working to provide centralized information and controls across a number of trust factors so that you can assess and manage cloud apps against your requirements.
------------------	--

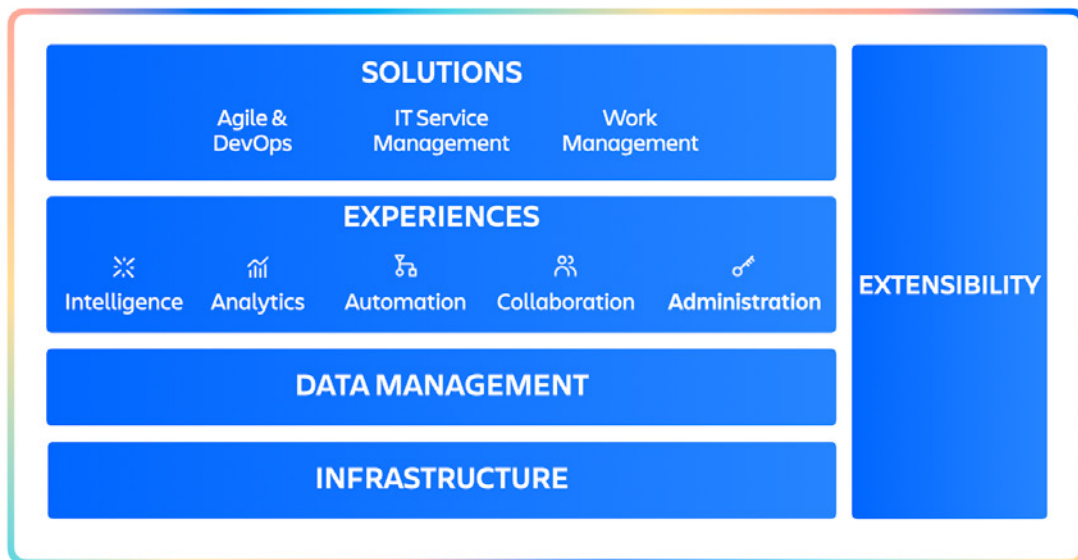
You	You do your part to use the information provided by Atlassian and Marketplace Partners to assess whether apps fit within your organization’s guidelines.
------------	--

You use available controls to manage your installed apps.

For more information on the shared responsibility model, [read our executive summary](#).

We've applied this model to the Atlassian Platform:

- Built on an enterprise-grade infrastructure that's reliable and secure at scale
- Enhanced data protection controls allow you to secure and manage your data
- Centralized administrative experience
- Extensible, with thousands of apps and integrations



In this whitepaper, you'll learn how we protect data across the three layers of the platform, the capabilities you can use to meet your organization's needs, and how to evaluate your Marketplace apps.



01

**Atlassian cloud
infrastructure layer**

For your teams to do their best work, they need access to their products and their data – downtime isn't an option. However, outages do happen, and you must be able to recover your systems as quickly as possible without experiencing any data loss.

Outages can be caused by infrastructure going down for an extended period. Whether you're administering your infrastructure or using cloud products, your organization depends on you and your IT team to restore service as quickly as possible. Unfortunately, how long it will take to recover is not always clear.

We've built Atlassian cloud on enterprise-grade infrastructure that delivers reliable experiences, so you don't have to worry about your teams losing productivity or lost revenue to your business.

What Atlassian does: Keep data safe and minimize data loss

Hosted on Amazon Web Services (AWS) infrastructure as a service (IaaS), Atlassian cloud products are hosted in multiple regions worldwide, including regions in the United States, Australia, and the European Union. Each of these regions has multiple availability zones (AZs) that are isolated from each other. Because data is replicated to other AZs in a region, if there is an AZ failure, your data remains accessible – ensuring high availability and failover.

Note: We offer data residency if you require data hosted in a specific region. When enabled, data residency pins **in-scope data to a specific region**.

High availability and failover provide the first line of defense to recover services in the event of an infrastructure-level outage. We also operate a backup program that offers another way to recover data.

Internal systems and critical services, such as our products, are backed up using Amazon's relational database service (RDS) snapshot feature. This enables us to create daily backups of each RDS instance. These snapshots are retained for 30 days and are encrypted with AES-256. Combined with database transaction logs, the snapshots enable point-in-time recovery, reducing the data loss risk.

These backups are also secure and immutable. Backups for product SQL data stores are stored and locked in a write-once-read-many (WORM) vault. This process protects backups against potential deletion by bad actors and rogue software, protecting us from complete data loss.

Note: We don't use our backups to revert customer-initiated changes, such as deleted issues or projects. To mitigate data loss, you need to take regular backups of your data. To learn more about these capabilities, see the [Data Management section](#).

What Atlassian does: Identify and mitigate vulnerabilities

One of the most [common reasons that systems go down](#) is because vulnerabilities have been exploited. To minimize this risk, we do:

- **External Penetration Testing:** Security consulting firms complete penetration tests, such as white box, code assisted, and threat-based, on high-risk products. Validation and results are provided through letters of assessment and published multiple times a year.
- **Atlassian Red Team:** Team that mimics real-world cyber scenarios to identify vulnerabilities in our systems and services.
- **Bug Bounty Program:** Opt-in program designed to identify vulnerabilities in our products by having end-users test our products. The results of the reports are published regularly.

What Atlassian does: Meet your business requirements

Our approach to reliability and availability isn't just focused on having the right technologies in place. We've implemented programs and policies that enable us to support your business requirements and operate in line with industry standards.

- **Business Continuity (BC):** The strategic and tactical capability of Atlassian to plan for and respond to business disruptions to continue business operations at an acceptable and predefined level.

- **Disaster Recovery (DR) program:** Processes, policies, and technologies that ensure critical IT systems and services are quickly restored during an outage. In the event of an outage, our RTOs and RPOs define the maximum amount of time we strive to restore services to normal operations.
- **Service Level Agreements (SLAs):** Financially backed guaranteed monthly uptime percentages across key experiences of Jira Software, Confluence, and Jira Service Management with Premium and Enterprise cloud plans.
- **Simulated infrastructure-failure outage tests:** Tests ensure we can recover from AZ failure with minimal downtime.



KEY TAKEAWAYS

What Atlassian does:

- Atlassian cloud platform, products, and solutions are hosted on AWS regions worldwide with multiple AZs that provide failover and high availability so they can withstand infrastructure-level failures.
- We run a program that provides another mechanism for backing up internal systems and services.
- We have an established disaster recovery program that enables us to restore systems and services in the event of an outage. Our business continuity program is designed to respond to unplanned events and deliver reliable products that users can trust.
- External penetration testing, the Bug Bounty Program, and the Atlassian Red Team help validate our resilience against dynamic threats.



02

Data Protection, Management, and Controls

Protecting your data at scale is challenging. Period. As you scale your organization, you face more risks – often keeping you and your security teams in reactionary mode. Even if you can continue growing your team, it’s easy to become overwhelmed.

The benefit of using cloud is that you now have another enterprise – Atlassian – in your corner, ensuring that our systems remain secure and building features that can transition you from reactionary to proactive. To do this effectively, we’ve focused on building solutions that address the following directly into the data protection, management, and controls layer of our platform:

- **Recovery:** Enable us to recover quickly in the event of an outage, prevent accidental deletion, and mitigate data loss so that teams can resume work efficiently and effectively
- **Security:** Platform controls that enforce strict authentication and authorization, encryption, and support of multiple regions with the flexibility for organizations to add and enforce additional controls over their data
- **Privacy and compliance:** Protect personal data and have the necessary controls to adhere to regulatory obligations
- **Identity and access management:** Reduce the risk of unauthorized access to data through architectural controls alongside customer features



Data recovery

As we mentioned in our previous section, our infrastructure helps to ensure that we can recover from infrastructure-level failures. Still, other types of outages can occur and significantly impact your business - both in revenue and lost team productivity.

According to the [Uptime Institute's annual report](#), human error played a role in about 60 - 80% of all outages, which could be caused by understaffed resources or a lack of training. You must have a solution in place to help to minimize this risk.

What Atlassian does: Prevent accidental deletion

We've built guardrails into the cloud architecture that help prevent someone from accidentally deleting a product and the corresponding data. Product delayed deletion acts as a safety net, so instead of the entire product being deleted, it's put into a suspended state where you have limited or no access to your product for a period of time. This enables us to quickly restore service to your products to minimize the impact on your teams. In the future, we'll provide soft deletion capabilities, which will prohibit certain types of deletion and provide multiple layers of protection to avoid errors.

What you do: Enable your organization to reduce data loss

It's imperative that you regularly take your own backups to ensure:

1. **Business continuity:** Your IT team needs to be able to restore data if it's accidentally deleted, such as Jira projects or Confluence spaces, or revert changes.
2. **Compliance with regulations:** Your organization's policies or the regulatory requirements that you need to abide by may require that you take your own data backups to be in compliance.
3. **Collect historical evidence during disputes:** Backups can be used to show what's changed in your environments, which you can use during litigation.

We offer an out-of-the-box solution called the backup manager to enable you to take these backups. It allows you to take an XML backup (export) that you can use to recover your data (import) in your environment.

In addition to the backup manager, we've developed a platform that will enable customers with extremely large data sets to export data more quickly and reliably. On top of this, we're developing new functionality that will live in Atlassian Administration (admin.atlassian.com) that will allow you to easily backup and restore all of your data whenever needed. As part of that work, we recently launched a command-line interface (CLI) that allows you to back up and **restore** data more accurately and reliably than ever!

KEY TAKEAWAYS

What Atlassian does:

- Safeguards are built into the Atlassian Platform to mitigate the risk of a product being accidentally deleted.

What you do:

- Use the backup manager or backup CLI to ensure you can reliably recover your data whenever you need to.

Data security

The National Institute of Standards and Technology (NIST) **defines data security** as:

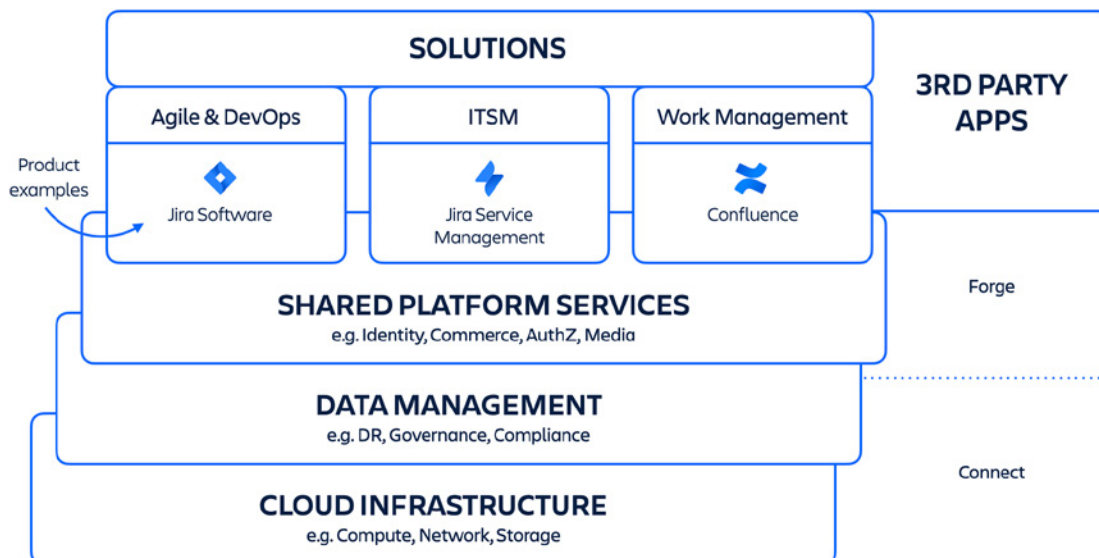


The process of maintaining the confidentiality, integrity, and availability of an organization's data in a manner consistent with the organization's risk strategy. Before an incident happens, companies must have a security architecture and response plan in place.

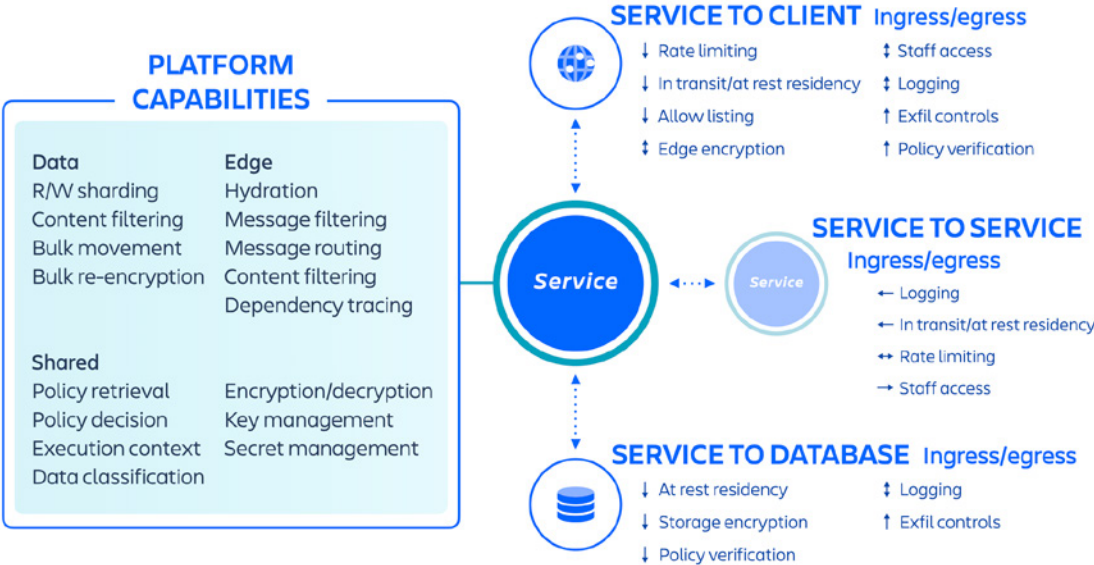
What Atlassian does: Securely manage a multi-tenant environment

We use the AWS architecture to host several platform and product services that are used across our solutions. This includes platform capabilities that are shared and consumed across multiple Atlassian products, such as Media, Identity, and Commerce, experiences such as our Editor, and product-specific capabilities, like Jira Issue service and Confluence Analytics.

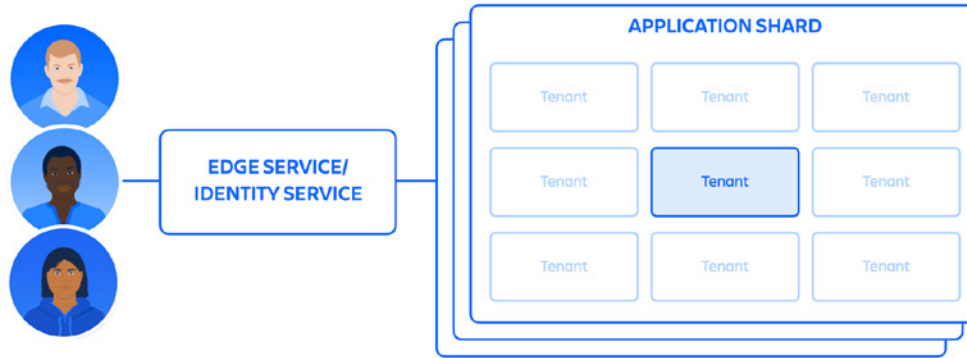
Atlassian developers provision these services through an internally developed platform-as-a-service (PaaS), called Micros, which automatically orchestrates the deployment of shared services, infrastructure, data stores, and their management capabilities, including security and compliance control requirements.



Atlassian products consist of multiple containerized services deployed on AWS using Micros. Atlassian products use core platform capabilities, which include networking, data storage, observability, and analytics. These micro-services are built using approved technical stacks standardized at the platform level.



On top of this infrastructure, we've built a multi-tenant micro-service architecture along with a shared platform that supports our products. In a multi-tenant architecture, a single service serves multiple customers. Each shard (essentially a container) contains the data for multiple tenants, but each tenant's data is isolated and inaccessible to other tenants.



What Atlassian does: Scale services while maintaining logical separation of data

While our customers share a common cloud-based infrastructure when using our cloud products, we have measures in place to ensure they are logically separated so that the actions of one customer can't compromise the data or services of another customer.

Atlassian's approach to achieving this varies across our applications. In the case of Jira and Confluence Cloud, we use a concept we refer to as the "tenant context" to achieve logical isolation of our customers. This is implemented both in the application code and managed by something we have built called the tenant context service (TCS). This concept ensures that:

- Each customer's data is kept logically segregated from other tenants when at rest.
- Any requests processed by Jira or Confluence have a tenant-specific view so other tenants are not affected.

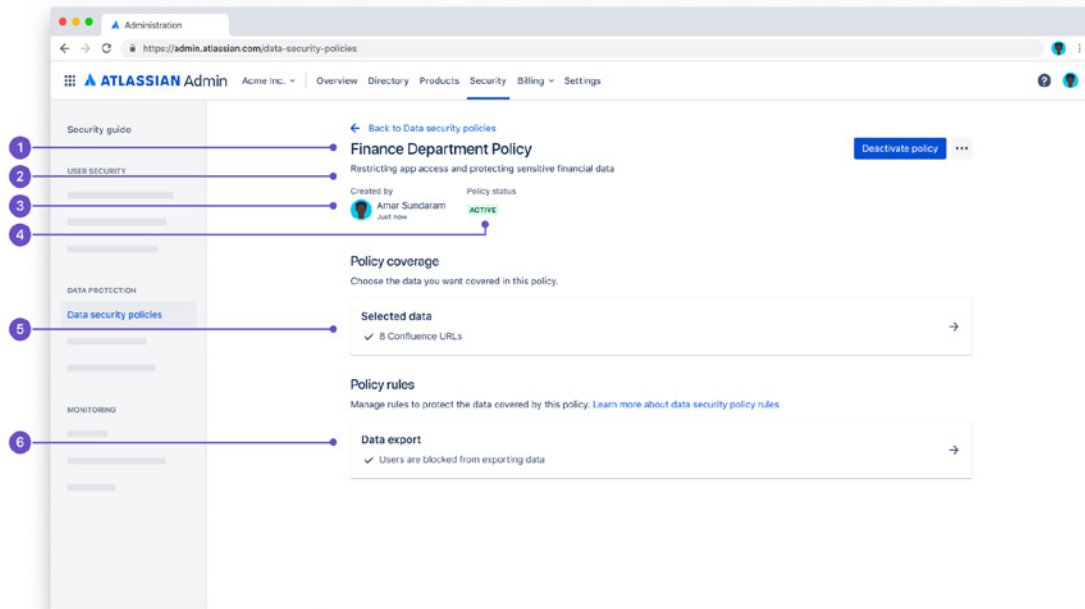
In broad terms, the TCS stores a context for individual customer tenants. The context for each tenant is associated with a unique ID stored centrally by the TCS and includes a range of metadata associated with that tenant, such as which databases the tenant is in, what licenses the tenant has, what features they can access, and a range of other configuration information. When a customer accesses Jira or Confluence cloud, the TCS uses the tenant ID to collate that metadata, which is then linked with any operations the tenant undertakes in the application throughout their session.

This protects against cross-tenant data leakage or any issues, such as incorrect database connections - effectively adding an additional safeguard.

What you do: Implement content governance

We ensure that only authorized people have access to your data, but it doesn't help govern how users, applications, and even people outside of your organization interact with your content.

Soon, we'll offer data security policies, enabling you to apply additional protection around your data.



Instead of being restricted to granting or removing user permissions, you can limit their actions. For example, you can create a policy against one of your sites that doesn't allow your teams to export Confluence pages – thus reducing the risk of data exfiltration or other data loss.

You can define the policy coverage – aka the scope of the products that the policy applies to if you have more than one product – and the rules – security controls that are configured as part of the policy.

 For more information, [read our documentation](#).

Protect sensitive data by limiting access

Data encryption continues to be one of the primary mechanisms for keeping sensitive data protected. Data encryption works by applying a ciphertext around your data so that no one can read it unless they have a key to the cipher.

What Atlassian does: Encrypt data in transit and at rest

With our cloud products, Atlassian primarily handles this under the shared responsibility model. We encrypt your data in transit using TLS 1.2+ with perfect forward secrecy (PFS) and at rest using AES-256. We use the AWS Key Management Service (KMS) to manage our cipher keys, so only people with authorized AWS roles and permissions can access these keys and decrypt your data.

What you do: Manage who can decrypt your data

Your organization may want additional encryption capabilities beyond what we provide out-of-the-box in the Atlassian Platform. Coming soon – we'll offer bring your own encryption (BYOK), which will enable you to generate and host keys in your AWS account via the [AWS Key Management Service \(KMS\)](#). To stay up-to-date, subscribe to the [cloud roadmap](#).

Meet data residency regulatory requirements

Organizations often work across multiple geographies that require data to be stored in specific locations to mitigate risk and protect against unauthorized personal data usage. By design, AWS has regions worldwide, allowing us to expand the number of locations where our product data can be hosted.

What you do: Specify where your data needs to reside

By default, all products are hosted in the Global location, which includes all of our AWS regions, but we offer [data residency](#), which enables you to pin in-scope data to a specific location. Today, we offer data residency in the United States, Asia Pacific (APAC), the European Union (EU), Germany, and Singapore. To better support you, [we continue to expand these regions](#).

As mentioned in the infrastructure section, each region has multiple availability zones (AZs). If there is an AZ failure in the region that you pinned your data to, you will failover to another AZ in that same region so you can continue to meet your regulatory obligations in the event of an outage. We don't provide cross-regional failover.

In some cases, you may have some requirements that limit you from having all of your data in cloud, but you still want to allow teams without those constraints to begin using Atlassian cloud. [Application tunnels](#) provide a secure gateway between our self-managed and cloud products. This will enable you to integrate your Atlassian products and securely exchange data and functionalities between them without exposing your network or allow listing any incoming connections or IPs.



KEY TAKEAWAYS

What Atlassian does:

- We use the AWS architecture to host several platform and product services used across our solutions. These services are provisioned using a PaaS called Micros, which orchestrates deploying these services. Security and compliance controls are provisioned as part of it.
- The Atlassian platform, products, and solutions use a multi-tenanted microservice architecture with strict tenant isolation to keep data inaccessible through the tenant context service (TCS). Each tenant has a unique ID and metadata to protect against cross-tenant leaks.
- We encrypt data in transit and at rest to protect your data.
- Expand the number of AWS regions that we support so that you can meet your regulatory requirements.

What you do:

- Use BYOK to generate your own AWS keys to reduce the number of people who can decrypt your data.
- Use data security policies to apply content governance over your data for additional protection.
- Turn on data residency to host your data in specific regions to meet your regulatory requirements.

Privacy and compliance

Privacy and compliance are two terms that are often used interchangeably.

- **Privacy:** Data privacy is focused on ensuring that personally identifiable information belongs to the individual, and they have the right to determine what, how, when, and who has access to their information. The onus is on businesses to meet the appropriate requirements to meet these needs.
- **Compliance:** Compliance refers to a set of policies, regulatory requirements, or laws that outline the conditions that need to be met to be considered secure, reliable, and private.

In short, privacy focuses on protecting personal data, and compliance provides a blueprint for how that needs to be done, in addition to providing other security conditions.



What Atlassian does: Build compliance and regulatory controls into our products

To get a compliance certification or attestation, we have to prove that we've implemented the numerous controls outlined in those specific frameworks. The types of controls and the complexity of implementing them depend on the industry they support.

Today, we support the following **frameworks, laws, and certifications**:



Each of our compliance certifications receives independent third-party validation to ensure that we meet all relevant requirements.

And the benefit to organizations that may not be in heavily regulated industries is that you use the same infrastructure with those advanced controls.

What Atlassian does: Ensure that your data remains private

Keeping your data private is of the utmost importance, and it requires more than just having the technical controls in place. We've also focused on building policies and programs, which include:

- [Privacy policy](#)
- [Data management policies](#)
- [Restricted data access policies](#)
- [Data processing addendum](#)

What you do: Operate your products in a compliant way

Part of meeting your regulatory obligations is that you operate your products in a compliant way. We empower you with features like data residency and documentation to make that happen. For example, if you need to be HIPAA compliant, we've created an [implementation guide](#) that instructs you how to operate eligible Atlassian products in order to operate them in a HIPAA compliant way.

KEY TAKEAWAYS

What Atlassian does:

- We build controls into our infrastructure, products, and solutions that enable us to achieve compliance across different frameworks, and we undergo independent third-party validation annually to ensure that we're operating in compliance.
- We operate our privacy program in line with industry standards.

What you do:

- Operate your data in a compliant way so you're able to meet your regulatory obligations.

Identity and access management

Gartner defines identity and Access Management (IAM) as:



A security and business discipline that includes multiple technologies and business processes to help the right people or machines to access the right assets at the right time for the right reasons, while keeping unauthorized access and fraud at bay.

In short, it's all about protecting your data by ensuring that only the right people, devices, and applications can access it. Unfortunately, compromised credentials continue to be one of the leading causes of data breaches. That's why we've taken a shared approach to IAM.

What Atlassian does: Enforce service authentication and authorization

Our platform uses a least privilege model for accessing data. This means all data is restricted to only the service responsible for saving, processing, or retrieving it. For example, the media services, which allow you to have a consistent file upload and download experience across our cloud products, have dedicated storage that no other Atlassian services can access. Any service that requires media content access must interact with the media services API. As a result, strong authentication and authorization at the service layer also enforce a strong separation of duties and least privileged access to data.

We use JSON web tokens (JWTs) to ensure signing authority outside the application, so our identity systems and tenant context are the source of truth. Tokens can't be used for anything other than what they are authorized for. When you or someone on your team makes a call to a microservice or shard, the tokens are passed to your identity system and validated against it. This process ensures the token is current and signed before sharing the appropriate data. When combined with the authorization and authentication required to access these microservices, it's limited in scope if a service is compromised.

However, we know that sometimes identity systems can be compromised. To mitigate this risk, we use two mechanisms:

1 First, TCS and the identity proxies are highly replicated. We have a TCS sidecar for almost every microservice and we use proxy sidecars that offshoot to the identified authority, so thousands of these services are running at all times. If there is anomalous behavior in one or more, we can quickly resolve that and remediate the issue.

2 In addition, we don't wait for someone to find a vulnerability in our products or platform. We're actively identifying these scenarios so there is minimal impact on you, and we run a number of security programs to identify, detect, and respond to security threats.

We ensure that requests to any microservices contain metadata about the customer – or tenant – requesting access. This is called the tenant context service. It's populated directly from our provisioning systems. When a request is started, the context is read and internalized in the running service code, which is used to authorize the user. All service access, and thus data access, in Jira and Confluence, require this tenant context, or the request will be rejected.

Service authentication and authorization are applied through Atlassian service authentication protocol (ASAP). An explicit allowlist determines which services may communicate, and authorization details specify which commands and paths are available. This limits the potential lateral movement of a compromised service.

Service authentication, authorization, and egress are controlled by a set of dedicated proxies. This removes the ability for application code vulnerabilities to impact these controls. Remote code execution would require compromising the underlying host and bypassing the Docker container boundaries – not just the ability to modify application logic. Instead, our host-level intrusion detection flags discrepancies.

These proxies constrain egress behavior based on the service's intended behavior. Services that don't need to emit webhooks or communicate with other microservices are prohibited from doing so.

What you do: Enforce user and device authentication and authorization

Atlassian Access enables admins with IAM features and capabilities that allow you to apply security and governance over your users and devices from within the Atlassian Administration – enabling you to implement a zero-trust approach.

USERS

Continuous identity verification lies at the heart of a zero-trust security strategy. To ensure employees have access to the right resources, you'll need to have a robust user management system and set up strong processes.

Enforced SAML SSO

Verify users' identity using SSO by syncing your external identity provider – or identity providers – to Atlassian Access.

Multi-factor authentication

Require your users to authenticate in two distinct ways before they gain access to any corporate systems.

Automated user provisioning

Integrate an external user directory with your Atlassian organization to automatically update the users and groups in your Atlassian organization when you make updates in your identity provider.

IP allowlisting

Specify which IP addresses users must use to access content for Jira Software, Jira Service Management, and Confluence.

External user security

Require external users who collaborate with people inside your organization to use two-factor verification or apply verification frequency – coming soon.

DEVICES

Devices accessing corporate data should be uniquely identified in a database. By having employees register any bring-your-own-device (BYOD) and corporate devices in an MDM program, you'll know exactly which devices are accessing your system and ensure that they meet your enterprise's security needs (by having up-to-date operating systems or requiring a passcode).

Mobile device management (MDM)

Configure security controls for your users' iOS and Android devices, whether provided by your users or your organization. This allows you to enhance security by:

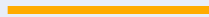
- Updating software and device settings
- Monitoring compliance with organizational policies
- Remote wiping or locking devices

Mobile application management (MAM)

Create a policy that specifies how your users' devices need to meet your security requirements before they can access the mobile apps connected to your organization. Unlike MDM, you don't need additional software; users don't need to download additional device management software or enroll their devices.



03

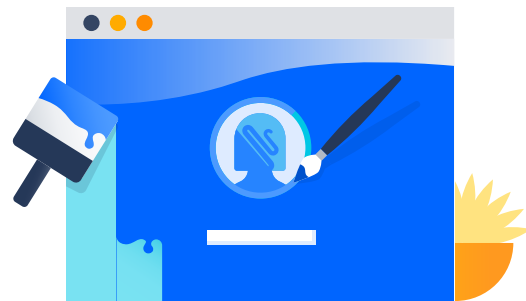


Centralized admin

As an admin, you must have a line of sight across all your Atlassian products. In self-managed environments, that's not easy to accomplish. By design, self-managed products are isolated from each other to keep data inaccessible from other instances. However, you then lack the mechanisms to see what's happening across your footprint. In cloud, you can still keep your data isolated – if you need to – but you get a centralized administrative experience to help you govern your Atlassian products and get increased visibility to keep your data safe.

This centralized administrative experience – Atlassian Administration – is built on the Atlassian Platform and has been optimized with:

- **Monitoring and reporting:** Maintain your security posture and compliance position with threat detection and auditing capabilities
- **Product and org lifecycle management:** Manage your products and org to meet your requirements effectively



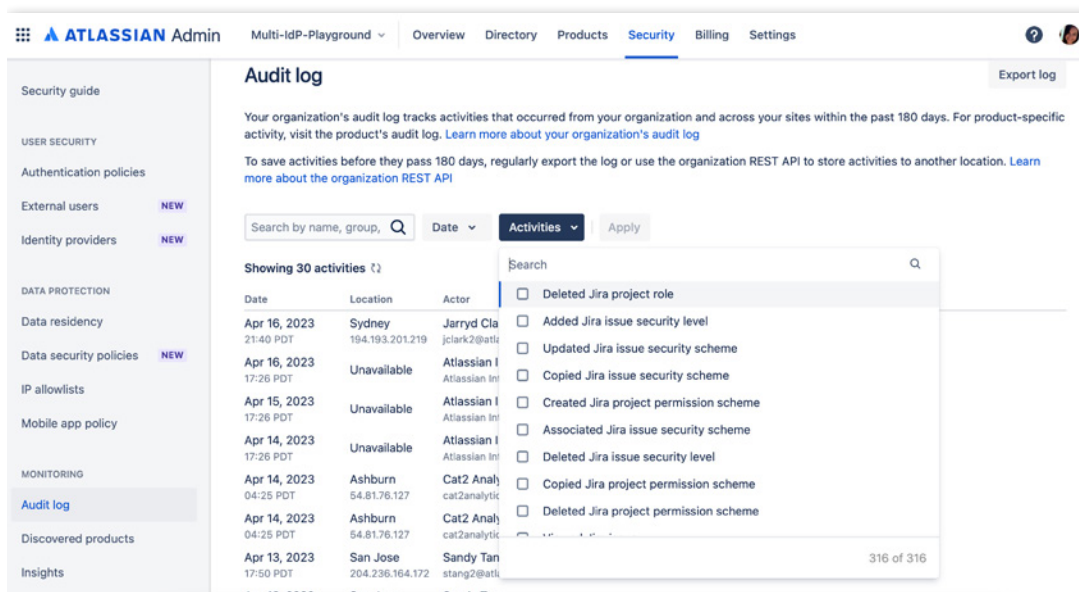
Monitoring and reporting

Getting visibility into your instance can provide numerous benefits to organizations at scale, but regardless of size, every organization can benefit from using threat detection tools.

Threat detection tools monitor your network to identify malicious activity so your security team can quickly address the risk. Threat detection also enables you to prioritize risk and get real-time information to respond to suspicious behavior before they become a risky, widespread incident.

What you do: Track events that occur in your instance

Standard and Premium Cloud products contain audit logs that allow you to track key in-product events. Still, they don't provide full visibility into the security of your data across all of your Atlassian products in one location. With Atlassian Access, you can view organization audit logs, which track events such as changes to someone's access to your products or shifts in administrative access. Unlike product audit logs that are dependent on the amount of storage your plan has, organization audit logs are retained for 180 days to provide you additional assurance.



And if your organization requires even more granularity, with Enterprise Cloud, you can choose to include user-created activities in your audit logs. This allows you to track product actions for both unmanaged and managed in a central location. For more information, [check out our audit log Community post](#).

What you do: Monitor potential threats

Applying controls will help you protect your data, and users will reduce the risk of a data breach. Still, one of the most important tools you need in your arsenal is the ability to monitor your environment to stop threats before they ever happen.

Threat detection adds additional oversight to your instance so that you can track day-to-day events quickly to identify any malicious activities.

One of the many advantages of SaaS solutions is that it's easy for teams to get started. Unfortunately, that also makes it easier for teams to download new versions of products outside your IT department's governance, which presents another avenue for potentially malicious data access. With Automatic Product Discovery, you can seamlessly access this information from the Atlassian Administration and take immediate action.

Automatic Product Discovery runs a daily analysis to see if instances are created by anyone with an email address attached to your organization's domain. It sends you a daily email with this data. Through the Atlassian Administration, you'll see who created the instance and how many users are using it, so you can decide if you want your IT team to begin managing it or work with the instance owner to get them on your company-managed instance.

Soon, you'll be able to take a content-based approach to governing how your data in Atlassian products can be used. This differs from a user-based approach that relies on giving or revoking specific permissions that allow users or apps to perform certain actions.

 For more information, [read our documentation](#).

But you also need to be aware of where data is being stored. Especially at large enterprises, it can become more challenging for teams to know what products your IT team supports. So it's not uncommon for people to spin up new product instances to help them get work done. Unfortunately, these new instances can inadvertently open you up to a data breach. Coming soon, you can stop your managed users from provisioning new products without your approval with [product requests](#). Not only will you have more control, but you'll also get more visibility into your users.

It's also important to know what activities people are doing within your Atlassian products. While you or someone on your team may be a security expert, most people are not, and they may unintentionally expose you to additional risk.

- **Org and admin insights:** Track active users who have viewed a page, view active vs. inactive users, and see how many managed users have two-step verification applies relative to users who have access to your products who are unmanaged
- **CASB integration:** Connect to the CASB software McAfee MVISION Cloud to get automatic security monitoring and behavioral analytics through your McAfee MVISION Cloud dashboard

In addition, we've launched Beacon, which provides even more threat detection capabilities. With Beacon – currently in beta – you can:

- **Detect:** Get automated alerts when there is unusual activity across your Atlassian products that will help you detect threats.
- **Investigate:** Gather detailed information that will help you determine the credibility of the threat.
- **Respond:** Bring threats under control with alert details, status tracking, and SIEM forwarding for seamless alert handling.

For more information, [contact us](#).



KEY TAKEAWAYS

- Audit logs provide detailed records of events within your instance. If your organization records more advanced recording, Cloud Enterprise also tracks user-generated activities. These audit logs can be used to maintain the security of your instance and prove compliance.
- Use automatic product discovery to stay informed when someone in your organization creates a new instance to maintain your security posture.
- Soon, you can restrict users from creating a new instance with product requests.
- Beacon is intelligent threat detection for your Atlassian products.

Product and org lifecycle management

Atlassian cloud products are associated with an Atlassian Organization. This allows you to keep track of the instances that belong to your organization. Especially as you scale your organization, you need the flexibility to meet your security requirements.

What you do: Structure your data based on data requirements

When you scale your business, you're ultimately faced with a decision. You need to determine if how you've structured your Atlassian products will give you the flexibility to grow your business and maintain the right level of oversight. Unlimited instances give enterprises this flexibility.

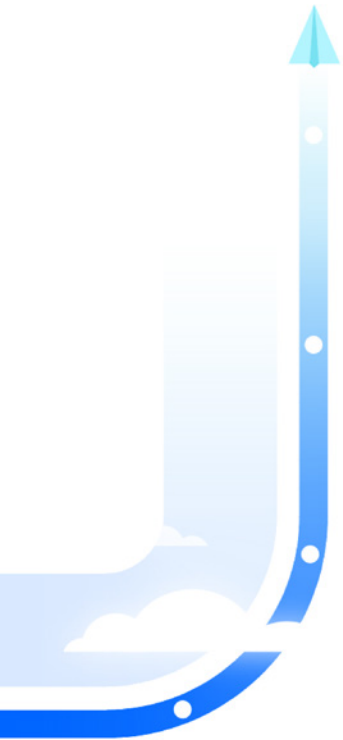
Here are some common examples of how organizations like you have setup multi-instance environments:

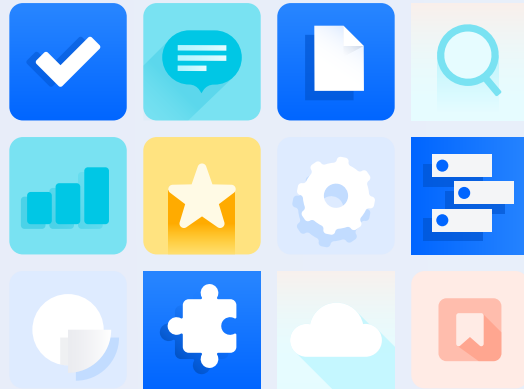
Separate departments and governance	Grant teams autonomy by creating sites for each of your business units (BUs). This allows teams to customize their sites. For example, teams can apply customized workflows and apps without impacting other teams.
Growth through acquisition and collaboration with external stakeholders	New teams may join your organization through mergers or acquisitions, and you may want to continue administering those teams separately. You can give those teams their own site and still administer them in a central location.
Highly sensitive intellectual property	Some of your teams have access to sensitive or proprietary data. You can create separate sites for those teams and limit access to maintain the right level of security.
Data Isolation for geo-dispersed teams	<p>Many organizations have globally distributed teams so that you can create different sites for specific geos. For example, maybe you want to create a separate site to support your EMEA teams with strict regulatory requirements.</p> <p>Create separate sites to maintain your data privacy requirements. For example, if you have certain data that must stay within a specific region, you can create a separate site and pin your in-scope data to that specified location.</p>

Read our [ebook](#) to learn more about unlimited instances.

 **KEY TAKEAWAYS**

- Unlimited instances enable organizations to meet complex use cases, such as protecting highly sensitive data.
- Each instance can be fully customized through the Atlassian Administration to meet your specifications without impacting other instances associated with your organization. For example, you can pin your instance data to different regions based on your regulatory obligations.





04

Atlassian Marketplace

The Atlassian Marketplace has over 5300 apps and integrations, more than half of which extend and customize Atlassian cloud products. While Atlassian offers a few Marketplace apps, the majority of apps are built and run by third-party Marketplace Partners.

Marketplace data security

Atlassian is working to support Marketplace partners in building secure, reliable cloud apps that support your compliance needs. One method we employ is security requirements and programs.

What Atlassian does: security requirements & enforcement

As Marketplace apps are built and operated by third party partners, Atlassian's approach to Marketplace security is focused on defining security requirements and taking enforcement actions as further explained in the next section. Specifically, our approach involves:

- Clearly defined (and regularly updated) security requirements for cloud apps
- Ongoing scans and reporting of missing security requirements or vulnerabilities
- **Planned actions** to protect customers when necessary



Atlassian's cloud app security requirements

While server and Data Center apps are given [guidelines](#) to improve their security posture, every Marketplace Partner must commit to meeting [Atlassian-defined security requirements](#) when they list a cloud app on the Marketplace. These requirements fall into the following categories:

Authentication & Authorization	Apps must authenticate and authorize every request on all endpoints exposed.
Data Protection	<p>Any time an app stores End User Data* outside of Atlassian, they must take steps to protect that data, including:</p> <ul style="list-style-type: none">• Ensuring full disk encryption at rest• Using TLS version 1.2 (or higher) to encrypt all traffic and enabling HSTS with a minimum age of one year• Securely store and manage secrets (OAuth tokens, sharedSecret, API keys, etc.) <p>* End User Data = any data, content, or information of an end user that is accessed, collected or otherwise processed by you or your app in connection with use of the Atlassian Marketplace.</p>
Application Security	<p>Partners must take steps to protect customer data from security threats. They must:</p> <ul style="list-style-type: none">• Maintain and securely configure domains where the app is hosted• Validate and sanitize all untrusted data and treat all user input as unsafe to mitigate injection-related vulnerabilities• Not use versions of third-party libraries and dependencies with known critical or high vulnerabilities
Privacy	Apps must not collect or store credentials belonging to Atlassian user accounts such as user passwords or user API tokens.
Vulnerability Management	Partners must provide security contact information and participate in Atlassian's vulnerability management program. If Atlassian or a security researcher finds a security issue with an app, Atlassian's security team needs to be able to reach the partner.

These requirements are mandatory for all cloud apps per Atlassian's [Marketplace Partner Agreement](#).

Scans, testing, and outreach

The work doesn't end when apps are built and listed on the Marketplace. In order to promote continued security across all cloud apps, Atlassian has several strategies in place to identify and manage security-related issues and vulnerabilities.

Ecoscanner

The Ecoscanner platform runs daily scans to check all Marketplace cloud apps for key security requirements and vulnerabilities.

As part of the Ecoscanner Platform, Atlassian has eight key requirement scanners available, six of which are available as open source tools that partners can use to scan their own apps. That way, partners can test their own apps to ensure new releases meet these important requirements before Atlassian begins scanning for them.

 You can read the [Ecoscanner developer documentation here](#) for more details on the specific requirements covered.

Third-party software vulnerability scanners

We also leverage scanners to identify vulnerabilities that arise from third-party software. Open source is powerful, and almost all developers in the world rely on open-source libraries for their applications. But these libraries do occasionally have vulnerabilities that impact a wide segment of tech companies, including apps.

We continuously scan apps built on Atlassian's Forge platform for critical or high-severity vulnerabilities in 3rd party libraries.

In the event of a zero-day vulnerability with a significant impact (for example, the recent vulnerabilities found in log4j or OpenSSL), Atlassian investigates whether this is something it can detect in all Marketplace cloud apps, including those not built on our Forge platform. If we can, we use scanners to discover the vulnerability in Marketplace apps, and work with partners to make sure the vulnerability is patched in a timely manner. If vulnerabilities are not patched in a timely manner, we take action to protect customers.

Example - Apache Log4j To share an example - Our programs, scanning capabilities, and reporting mechanisms were put to the test in December 2021 when the remote code execution vulnerabilities in Apache Log4j were publicly disclosed. Atlassian quickly responded by mitigating the vulnerability for all Atlassian cloud products.

Additionally, Atlassian's app security team was able to scan our entire ecosystem and identify which apps were vulnerable, report those vulnerabilities, and get them closed in partnership with app developers as soon as possible. Within about a week, we were able to confirm that all cloud apps were free from the Log4j vulnerability, and all Data Center and Server apps were either patched or removed from our marketplace.

FRIDAY	SUNDAY	MONDAY	FRIDAY	TODAY
Software companies all over the world discover a vulnerability in a popular Java library	Atlassian finishes scanning all apps for this vulnerability	All vulnerable cloud apps are notified and given a deadline to address the issue	All vulnerable cloud apps have been patched or paused (only one app needed to be paused!)	No active cloud apps are vulnerable

External security bug reporting

In addition to our security requirements and vulnerability discovery strategies, Marketplace Partners, customers, or any person outside of Atlassian can also report security issues related to 3rd-party apps via the Atlassian Marketplace Security (AMS) Jira Project (for partners) or through Atlassian support (for customers).

Vulnerabilities from any source, including bug bounty, scanners, security reviews, and external reports are funneled into AMS and then tracked by Atlassian's security team for remediation.


Opt-In Program: [Marketplace Bug Bounty](#)

Partners can opt into Atlassian’s Marketplace Bug Bounty Program, which will get them access to a trusted community of cyber security researchers who are constantly testing their apps and reporting back any vulnerabilities they find.

Tip

You can identify apps that are in the Bug Bounty Program by the following Marketplace badges:

- The “Cloud Security Participant” badge, which signifies participation in the Bug Bounty Program.
- The “Cloud Fortified” badge, which signifies that an app participates in the Bug Bounty Program and has also taken other actions to improve security and reliability. Cloud Fortified apps also offer at least 24-hour/ five-days-a-week support for customers.

 By prioritizing security and actively participating in initiatives like Atlassian’s Bug Bounty & Cloud Fortified Programs, we are not only protecting our users’ valuable data but also building trust and credibility with our customers. Our commitment to security is unwavering, and we will continue to work diligently to provide our users with the most secure and reliable apps possible.

JOHN WHITTAKER, VICE PRESIDENT AT SMARTBEAR, AN ATlassian PLATINUM MARKETPLACE PARTNER

Security-related issue resolution

The strategies covered so far are in place to help Atlassian identify and track potential security risks on the Marketplace. But of course, vulnerability discovery is only the first part of the strategy to protect customers with apps.

If a vulnerability is discovered, all apps are subject to the [Security Bug Fix Policy for Marketplace apps](#), which outlines remediation due dates for security-related bugs discovered in Marketplace apps. When we discover that an app is not meeting a security requirement, we notify Marketplace Partners and give them a deadline to fix the issue. If apps fail to meet these deadlines, Atlassian will take action.

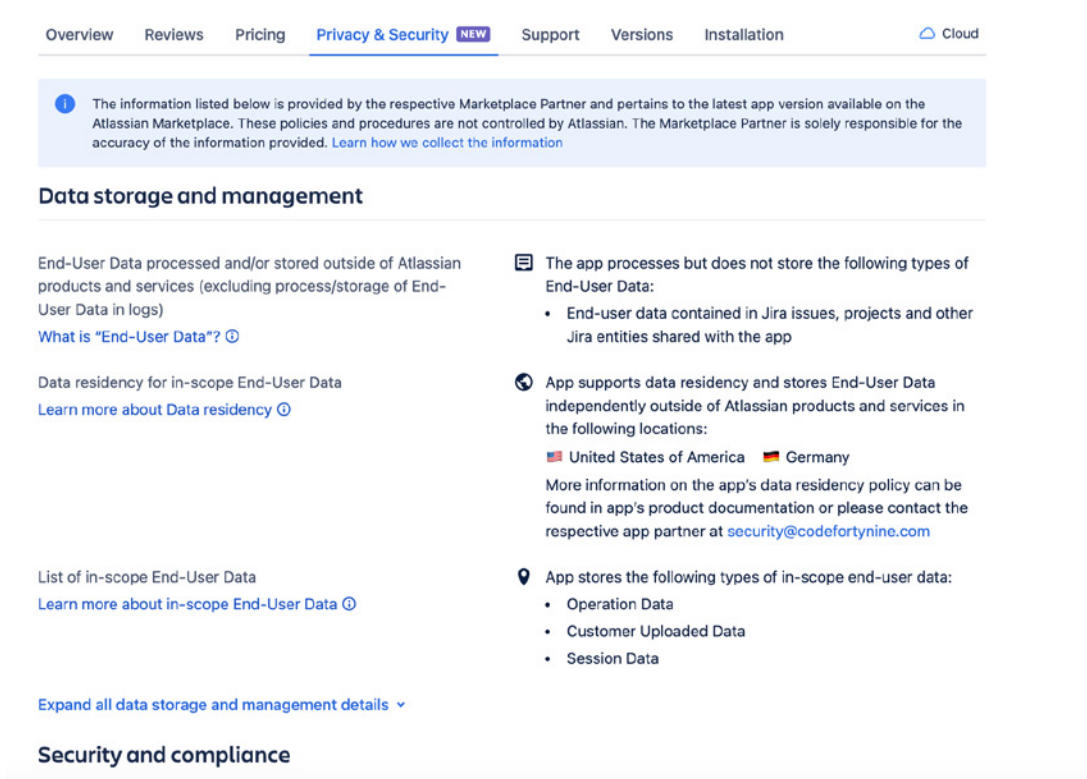
For critical issues or issues that go unaddressed for too long, Atlassian will take actions like removing security badges and hiding the app from the Marketplace. Apps in violation of our Security Bug Fix Policy for Marketplace Apps are listed publicly on our [App Security Transparency page](#). In severe cases, Atlassian may even pause an app to protect customer data.

In short, our message to Marketplace Partners is clear: maintaining the security of your app is critical. If an app is not meeting our security requirements, we will find out and take action.



What you do: Be aware and report things you see

While Atlassian has processes in place to support partners, you also have a role to play. Familiarize yourself with an app's privacy and security details before installing, which you can find on the app's Privacy & Security tab on Atlassian Marketplace.



The screenshot shows the 'Privacy & Security' page for an app on Atlassian Marketplace. The navigation bar includes 'Overview', 'Reviews', 'Pricing', 'Privacy & Security' (highlighted with a 'NEW' badge), 'Support', 'Versions', and 'Installation'. A 'Cloud' icon is visible in the top right. A blue information box at the top states: 'The information listed below is provided by the respective Marketplace Partner and pertains to the latest app version available on the Atlassian Marketplace. These policies and procedures are not controlled by Atlassian. The Marketplace Partner is solely responsible for the accuracy of the information provided. [Learn how we collect the information](#)'.

Data storage and management

End-User Data processed and/or stored outside of Atlassian products and services (excluding process/storage of End-User Data in logs)
[What is "End-User Data"? ①](#)

Data residency for in-scope End-User Data
[Learn more about Data residency ①](#)

List of in-scope End-User Data
[Learn more about in-scope End-User Data ①](#)

[Expand all data storage and management details ▾](#)

- ☰ The app processes but does not store the following types of End-User Data:
 - End-user data contained in Jira issues, projects and other Jira entities shared with the app
- 🌐 App supports data residency and stores End-User Data independently outside of Atlassian products and services in the following locations:
 - 🇺🇸 United States of America 🇩🇪 GermanyMore information on the app's data residency policy can be found in app's product documentation or please contact the respective app partner at security@codefortynine.com
- 📍 App stores the following types of in-scope end-user data:
 - Operation Data
 - Customer Uploaded Data
 - Session Data

Security and compliance

Also, be aware that apps in violation of Atlassian's Security Bug Fix Policy for Marketplace Apps will be listed on the [App Security Transparency page](#). If you see one of your apps on this page, reach out to the Marketplace Partner directly to better understand the nature of the violation.

Finally, remember that you can also leverage Atlassian's systems for reporting vulnerabilities. If you find something in an app, you can raise a ticket to our [support team](#).

KEY TAKEAWAYS

- Marketplace Partners agree to **security** requirements when they list an app on the Atlassian Marketplace.
- Atlassian performs daily custom security scans to help verify all cloud apps meet the security requirements. If apps fail to comply in a timely manner, enforcement measures will be taken as per the **Security Bugfix Policy for Marketplace Apps**.
- In addition to these programs, partners can opt-into more in-depth security programs like the **Marketplace Bug Bounty program** for security, or the **Cloud Fortified program** for security, reliability, and support.
- Customers can report app security vulnerabilities to Atlassian, and should be aware of the **App Security Transparency page**, where Atlassian lists apps that are in violation of the **Security Bugfix Policy for Marketplace Apps**.



Marketplace Privacy

What Atlassian & partners do: create and agree to privacy obligations

In addition to meeting security requirements, apps are also required to provide a privacy policy that notifies end-users about:

- How a partner accesses, collects, and processes End User Data
- With whom an app or partner shares End User Data, and
- In which country or countries the End User Data will be stored

In addition to a privacy policy, Atlassian requires partners to obtain all necessary rights, permissions, and consents from end users for any:

- access
 - collection
 - storage
 - transmission
 - treatment
 - use
 - disclosure
 - sharing, and
 - other processing
- of any End User Data.



What you do: Review app privacy information

Review the privacy policy to learn more about how the app handles data.

You can find an app's privacy policy on the app's listing on marketplace.atlassian.com. Scroll down to the "More Details" section, where you'll see "Privacy and Security" on the right side. The app's privacy policy should be linked there under "Privacy Policy." You can also find this in the app's Privacy & Security tab at the top of the app listing, next to Support.

Based on this information, you may determine that an app requires a data processing agreement, which you'll need to enter into with the partner directly. We provide a space in the Privacy section of the Privacy & Security tab for partners to provide their standard **data processing agreement**, but if that agreement does not meet your requirements (or if the partner did not provide one) you may need to reach out to the partner directly.

Privacy and security

Privacy policy

Atlassian's privacy policy is not applicable to the use of this app. Please refer to the privacy policy provided by this app's partner.

[Partner privacy policy](#)

Security

✔ This app is part of the Marketplace Bug Bounty Program. [Learn more](#)

✔ This partner has completed the Security Self-Assessment Program. [Learn more](#)



KEY TAKEAWAYS

- Marketplace Partners agree to share privacy information publicly when they list an app on the Atlassian Marketplace.
- You should familiarize yourself with an app's privacy policy before installing the app.

Apps and data management

Marketplace Partners are ultimately responsible for running their own businesses, and they will make strategic investments based on the demand they see from customers. Beyond Atlassian's requirements as set out in our [developer documentation](#), [Developer Terms](#), and [Marketplace Partner Agreement](#), partners make their own business decisions about how apps are built and what features they support.

Atlassian constantly works to provide new tooling and guidance so Marketplace Partners can prioritize and build the most secure, high-quality apps possible.

What partners do: Secure-by-design apps

Via documentation, resources, live trainings, and tools, Atlassian encourages partners to employ secure-by-design principles when building their apps:

1

Least privileged access

Minimize data access to only what your app needs.

2

Least data egress

Minimize the need for data to leave the parent product whenever possible.

3

Use Atlassian's infrastructure

Use Atlassian's infrastructure for data storage and processing whenever possible.

Least privileged access

The data an app needs to access will vary based on its function, but in general, we encourage partners to limit access to only the information needed to operate. You can see the data an app requires by looking at the Integration Details section of the app listing, or reviewing the app's Privacy & Security tab.

In addition to sharing this principle with partners, we are working on bringing admins more control over the spaces or projects an app has access to so you can limit app access to data yourself. (You can follow this work in the Apps & Extensibility section of Atlassian's [cloud roadmap](#)).

Least data egress & using Atlassian's infrastructure

Apps with more complex use cases may need to store or process some data externally.

However, apps with more straightforward use cases can often limit the amount of stored data they are responsible for securing, and place more responsibility on Atlassian to meet customer security and compliance needs.

To limit the amount of customer data that leaves Atlassian's environment, partners can use Atlassian-built storage options for their apps:

- **Storing End-User Data exclusively in Jira or Confluence:** Apps that don't have major storage needs can sometimes store End-User Data in Jira or Confluence, reducing the amount of effort required to independently secure data.
- **Using Atlassian-run storage and compute on Forge:** Partners can also choose to build apps on Forge, where they have the option to exclusively store and process data in Atlassian's environment.

You can learn more about where an app stores End-User Data and what End-User Data it stores by going to the app's listing on Atlassian Marketplace, where you can find an app's privacy policy, documentation, and other partner-provided information.

What Atlassian and partners do: App data recovery

While Atlassian hosts a backup of any data stored in Jira, Confluence, or on Forge, Marketplace Partners are responsible for their own data backup and recovery procedures for any data stored outside of Atlassian's infrastructure.

We **encourage all Marketplace Partners** to have a plan in place. Reach out to a partner directly if you have questions about a specific app.



KEY TAKEAWAYS

- In addition to security requirements and privacy obligations, Atlassian is constantly working to provide tools and guidance so that partners can implement best practices for protecting customer data.
- Be sure to check an app's Privacy & Security tab and Privacy Policy to learn more about how the app handles data.

Compliance and Marketplace apps

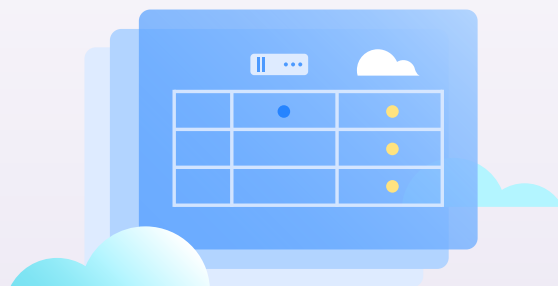
If your company is subject to legal obligations or internal compliance requirements regarding data protection, it's important that your installed apps also support those obligations. To this end, we provide partners with education to inform and tooling to support their investments in areas we know are important.

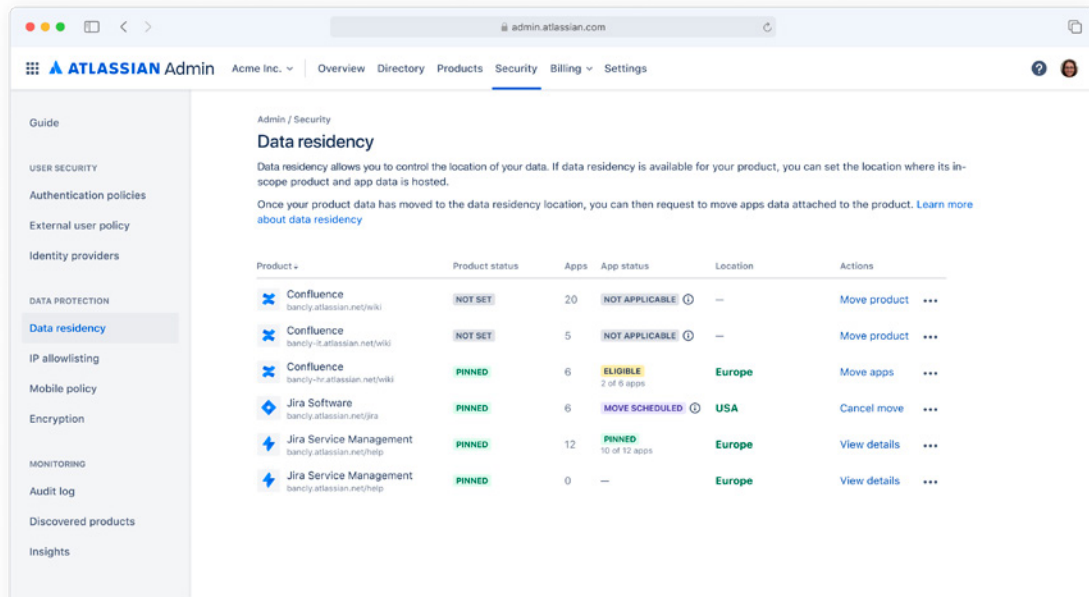
What Atlassian and partners do: Data residency

One goal in sharing the principles of secure by design is to minimize the number of apps that need to independently support data residency. Some apps store data exclusively within the Atlassian products and services. As these apps don't have any externally-stored data, your **in-scope** app data is pinned to and follows any regional moves of the product where it is installed.

However, apps that do need to externally store data are responsible for independently supporting data residency. Marketplace Partners with apps that store data outside of Atlassian can, in most cases, invest in pinning data to select regions so customers can meet data protection requirements related to data localization or transport.

While we provide our own definition of in-scope data as an example, Partners will determine what data is in scope for data residency managed outside of Atlassian's environment, so it's best to check the app's documentation, Privacy & Security tab on the app listing, or reach out to the partner directly to learn more. Organization and Site admins for Jira and Confluence will also be able to view and manage data residency for installed apps soon on Atlassian Administration (admin.atlassian.com) via a new beta experience.





View app data residency eligibility and schedule app data moves on admin.atlassian.com.

What partners do: Legal compliance

According to their agreement with Atlassian, partners are required to meet legal obligations in the regions where they operate. In addition, our Privacy team publishes high-level resources to help partners better understand their legal obligations in certain geographies, including under the GDPR.

What partners do: Compliance standards and certifications

Most Marketplace Partners understand the benefits of achieving compliance with data protection standards, and many partners have invested or are investing in certification.

“ The way we see it, protecting customer data is good business – plain and simple. We say that safety drives our decisions and certifying our compliance with industry-leading standards allows us to prove that we mean what we say.

JULIA WESTER, CEO & CO-FOUNDER AT 55 DEGREES, AN ATlassian PLATINUM MARKETPLACE PARTNER

To help partners prioritize, Atlassian provides suggestions and support with compliant infrastructure whenever possible.

Partners who choose to use Atlassian-hosted storage via Atlassian's Forge platform benefit from Atlassian's investments in compliance standards. While compliance standards require work beyond infrastructure, Atlassian's Forge platform is SOC2 compliant, which means partners have a head start in getting SOC2 certification when they build on Forge.

What you do: Let partners know what you're looking for

Partners will make strategic investments based on the demand they see from customers like you. If you are interested in or are using an app that stores data externally and you'd like the app to support data residency, let the app's owner know. You can find contact information on the Marketplace listing for most Marketplace apps.



KEY TAKEAWAYS

- In addition to defining security requirements and privacy obligations, Atlassian is constantly working to provide tools and guidance so that partners can support your compliance needs.
- Be sure to check an app's Privacy & Security tab and Privacy Policy to learn more about an app, and let partners know if you'd like an app to meet a specific requirement.

Transparency & control

Atlassian is working to make it easier for you to access information so you can make informed decisions about the apps you install in your cloud environment, and to give you more controls so you can manage the apps you have installed.

What you do: Ensure apps meet your requirements before you install

Check the app's privacy & security details

If you are responsible for ensuring apps meet your security requirements, you'll need information about how apps handle data. Many partners understand this, and are committed to providing information to help you evaluate their apps against your security requirements.

“ At Appfire we believe in trust, and trust is based on transparency and consistency. Our [trust center](#) significantly speeds up the ability of our customers to evaluate our apps, as a security review of one app can be applied to all Appfire apps. Our goal is to provide comfort and build trust so customers are comfortable making purchasing decisions.

DOUG KERSTEN, CHIEF INFORMATION SECURITY OFFICER AT APPFIRE, AN ATlassian PLATINUM MARKETPLACE PARTNER

While many partners are committed to transparency, they may have different approaches to providing information and offer it in different places online, which can make it difficult to find the details you need.

Start your security evaluation by going to the app's listing on the Atlassian Marketplace, where you'll find key partner-provided information in the app's Privacy & Security tab, the app's privacy policy, and other documentation. To help you find information faster, we're continuing to work on creating more consistent places for you to learn about an app's privacy and security details.

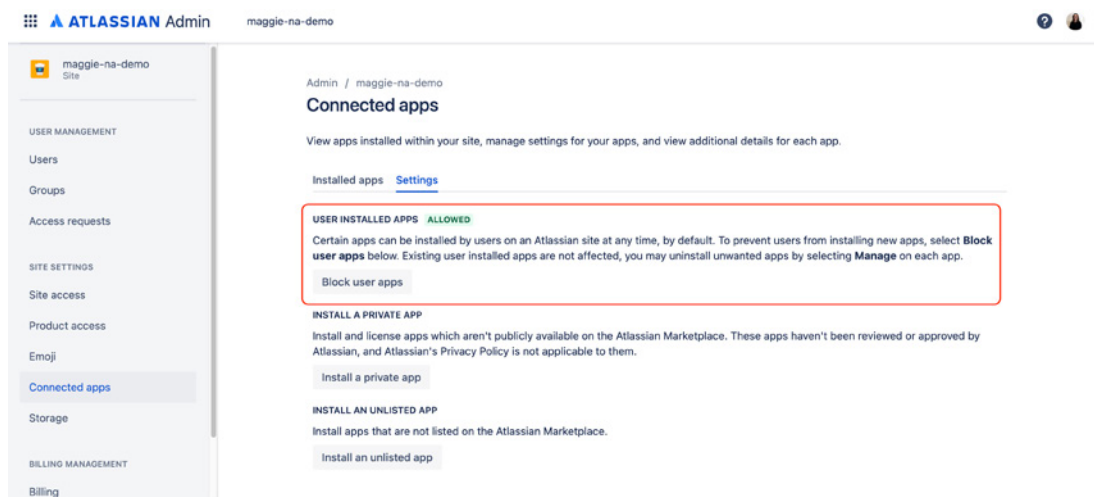
Review the app's permissions

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. We recommend reviewing the suitability of the app and the reasonableness of the requested permissions prior to installation.

What you do: Manage the apps on your instance

Limit install permissions

Installation for the vast majority of cloud apps is limited to admins. End-users must send a [request to their admin](#) if they'd like to install an app. However, by default, end-users can install and run OAuth 2.0 (3LO) apps.

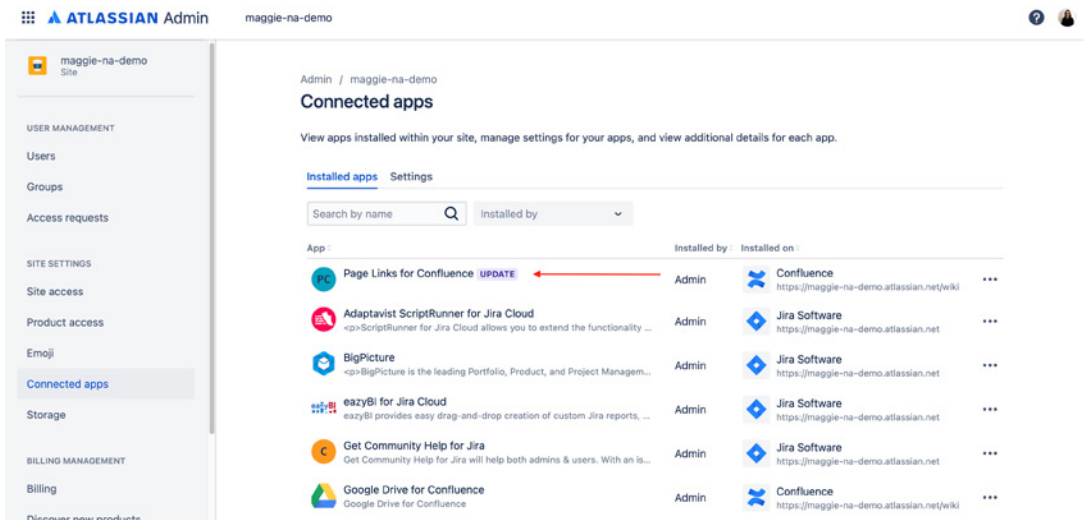


To gain more control over app installs, site admins can turn off (or back on) end-user installation capabilities for OAuth 2.0 (3LO) apps via a toggle in admin.atlassian.com.

Of course, there are many workflow benefits to allowing end users to install apps that help them work. If you want to leave this capability on but still keep an eye on end-user-installed apps, you can look for “Users” in the “installed by” column and remove any apps that pose a risk.

Stay up to date on changes and keep apps updated

With apps constantly checking for security requirements and evolving to increase security, it helps to stay up to date. You can sign up for email alerts on an app's Marketplace listing on marketplace.atlassian.com, or check your list of installed apps on admin.atlassian.com to see which apps have an update available.



See apps with updates available on admin.atlassian.com.



- AWS CodeCommit
- BitBucket
- Git on Linux/Windows
- Gerrit
- SSH
- HTTP/HTTPS
- git protocol

Add the free Git Integration for Jira app Extensions:

- [Team Insights for Jira](#) to see Git + Jira team activity at the project, epic, or sprint level.
- [CI/CD for Jira](#) to see build and deployment information.

Security

- ✓ This app is part of the Marketplace Bug Bounty Program. [Learn more](#)
- ✓ This partner has completed the Security Self-Assessment Program. [Learn more](#)

i We've introduced detailed information on privacy, security, data handling, and compliance practices followed by this app. [Learn more](#)

Resources

[Descriptor](#)

[Version history](#)

Watch this app and get email alerts for new version releases. You can stop watching this app at anytime

[Watch App \(704\)](#)

Sign up to "Watch App" on marketplace.atlassian.com to get email alerts when new versions are available.

KEY TAKEAWAYS

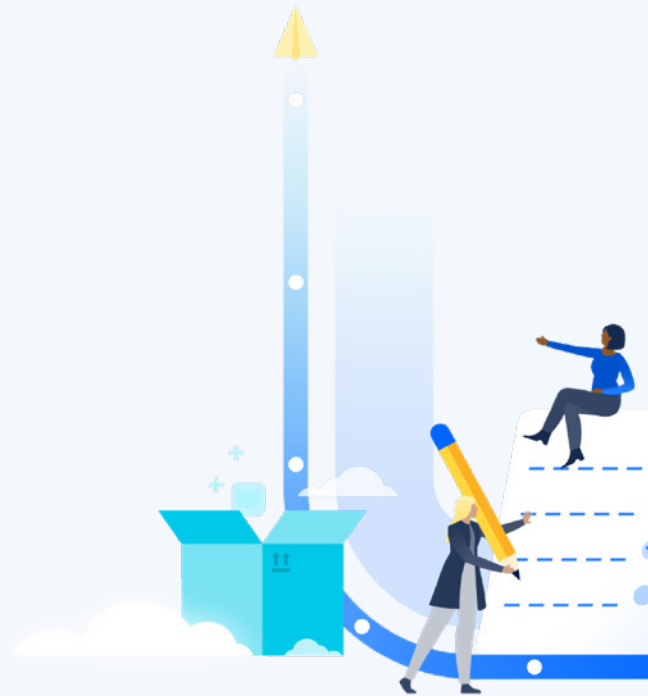
When it comes to protecting your data while using cloud apps, it's important to remember that Atlassian, partners, and customers all have a role to play. Atlassian will continue working to:

- **Increase the level of security and privacy across our cloud Marketplace** through requirements, education, and tooling for partners, and
- **Bring you more transparency and control** so you can make informed decisions when buying and managing apps.

Conclusion

Ensuring that your data remains secure is a shared partnership between you, Atlassian, and your Marketplace partners - with each of us taking some part of the responsibility. We believe this comes down to:

- Hosting our platform on a reliable and secure infrastructure that can quickly recover in the event of an outage
- Building data protection controls directly into the platform and enabling organizations with advanced features that allow them to meet their business requirements
- Providing admins with a centralized administrative experience that allows them increased visibility into their Atlassian products to protect them from possible security incidents
- Enabling our Marketplace partners and ecosystem with the right tools so they're able to build robust data security into their applications



To learn more about our approach to data protection, [contact us](#), or if you're evaluating a migration to Cloud, visit the [Atlassian Migration Program](#) to get guidance on how to assess Atlassian cloud.