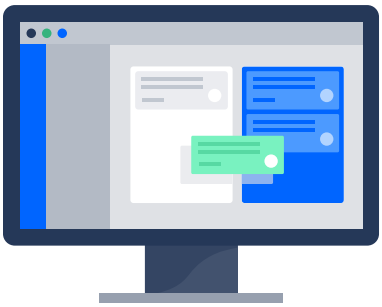
ATLASSIAN

Jira Align and Atlassian Trust

A brief overview of some of the ways we approach Trust at Atlassian

Table of contents



ATLASSIAN & JIRA ALIGN

Today more than 125,000 customers use our cloud products, accounting for over 10 million monthly active users. We have over 10 years of experience building our products in the cloud for our customers. Our investments give us the competitive advantage needed in the market that helps make your business successful. Atlassian provides enterprises with the capabilities to manage large-scale digital programs and portfolios while embracing agile ways of working with unparalleled flexibility, visibility, and effectiveness.

Jira Align helps you deliver the value your customers demand by keeping your digital evolution on track. With Jira Align you will realize true business agility, gain improved visibility, enhance strategic alignment, and scale agile practices up and out. Additionally, you can adapt our solution to your favorite scaled agile framework, such as SAFe, DA, LeSS, Scrum@Scale, or a hybrid collection of practices. Our solution centralizes your team level data giving you the insights needed to make the right strategic decisions.

TRUST - THE ATLASSIAN WAY

Atlassian empowers modern organizations to accelerate and scale their teams' productivity to their full potential. Our cloud-based tools and services are developed, from the ground up, with a security-centric approach that provides you with the maximum flexibility to meet your organization's objectives without compromising reliability or security.

The following is a brief overview of some of the ways we approach Trust at Atlassian as a whole, not necessarily specific to any one product.

We believe all teams have potential to do amazing things. Our mission is to unleash the potential of every team of every size and industry, and in turn, help advance humanity through the power of software.

We know that your mission is as important to you as our mission is to us, and information is at the heart of all our businesses and lives. This is why customer trust is at the center of what we do and why security is our top priority. We're transparent with our security program so you can feel informed and safe using our products and services.

Atlassian Trust Management System

The Atlassian Trust Management System (ATMS) takes each of our customers' security requirements into consideration and arrives at a set of requirements and initiatives unique to us and our environment. Details of our initiatives are provided on the Atlassian Trust site.

Building security into the way we work

We don't look at security as a destination to reach – it's an ongoing journey. We continually strive to improve our software development and internal operational processes with the aim of increasing the security of our software and services. Security should not be difficult and that's why security is built into the fabric of our products and infrastructure. Here are a few ways we build security in as part of the way we work, day-to-day.

Security incident management

The Security team at Atlassian aggregates logs from various sources in the hosting infrastructure and makes use of a Security Information and Event Management (SIEM) platform to monitor and flag any suspicious activity. Our internal processes ensure these alerts are triaged, investigated further, and escalated appropriately. Our customers and the wider community are encouraged to report suspected security incidents through Atlassian Support.

In the event of a serious security incident, Atlassian has access to the expertise internally – and through external subject matter experts – to investigate incidents and drive them until closure. The database of our security incidents is cataloged against the VERIS Framework.

Policy Management Program

The basis of the Trust Management System is our Policy Management Program (PMP). We have structured our policies to cover the domains included in both the ISO27001 standard as well as the Cloud Security Alliance (CSA) Cloud Controls Matrix (CCM). We have developed a couple of foundational principles to our Policy Management Program:

- Posted and available
- Supported by the security team to make it easy for you to comply
- Outlines our security objectives
- Shows commitment to meet our regulatory obligations
- Focuses on continual iteration and improvement
- Provides for an exception process
- Reviewed annually
- Risk management program

In order to continuously evaluate risks to our environments and our products, we perform ongoing risk assessments. In many cases, especially in the case of our products, these are performed as technical risk assessments or code reviews. However, we also evaluate each of our entire product stack or a portion of our organization to uncover higher-level business risks. Generally, we have adopted the ISO27005 or ISO31010 Risk Management methodology and apply that methodology to a particular scope.

Privacy program

You own your data, and we're committed to protecting the privacy of that data. Our Privacy Policy explains what information we collect about you and your users, why we collect that data, what we do with that information, how we share it, and how we handle the content you use with 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.

Shared responsibility

In the cloud, the security of your data on our systems is a joint responsibility.

At a high level, Atlassian manages security of the applications themselves, the systems they run on, and the environments those systems are hosted in. You – our customers – manage the information within your accounts, manage the users accessing your accounts and related credentials, and control which apps you install and trust. You must ensure your business is meeting its compliance obligations in using our systems.

STANDARDS-BASED APPROACH TO SECURITY IS CRITICAL

At Atlassian we have placed trust and data security at the core of our business model. Our products integrate security considerations as well as regulatory and legal requirements by design to empower technical teams with the highest level of security assurance.

To maintain and constantly improve our security maturity, we make full use of centralized security functions. We have over 80 cybersecurity professionals across the globe working around the clock to continuously deploy improvements to our security practices, and the team continues to grow rapidly. This constant effort ensures that vulnerabilities and risks have been fully addressed, no matter the size, industry or location of our customers. All customers benefit from this ongoing investment.

Over the years, we have allocated significant financial and human capital to develop and optimize our unified security control framework. Using a shared framework enables us to optimize each individual control, which translates in a higher level of security assurance across our product suite.

We have also established a dedicated team for the sole purpose of building sophisticated tools across our platform. Our centralized logging and vulnerability management pipelines illustrate how this approach provides material value to our customers.

While all our customers can leverage the investments made in our platform by adopting our common controls framework, customizations and unique controls naturally diverge from these investments. Meeting unique security control requirements for a subset of customers also results in a significant increase in the complexity of our security controls, processes, resources and infrastructure. This complexity increases the risk that processes are not followed consistently across multiple heterogenous security control environments, and rather than increasing security it instead introduces challenges in maintaining a consistent level of assurance across these environments. We believe that contractual variations to our information security terms leads to poorer outcomes for the customer.

We encourage any customers with concerns about our security clauses to speak to our team so we can provide further assurance on our information security capabilities, compliance and regulatory frameworks, or discuss any specific areas of concern.

JIRA ALIGN'S TRUST ARCHITECTURE

In early 2019 we welcomed AgileCraft into the Atlassian family, rebranded as Jira Align. We have been working diligently to bring Jira Align into the Atlassian Trust way of working. To stay up to date on our progress, please follow our Trust Roadmap.

Security through Continuous Delivery

The Jira Align Team is a continuous-delivery software engineering organization with automated unit and API testing. We provide bi-weekly updates to all our SaaS customers during pre-arranged maintenance windows, keeping your organization up to date with the latest features and benefits of Jira Align.

Platform architecture

Jira Align utilizes common data architecture patterns of multi-tenant SaaS database applications that run in a cloud environment. Tenants can access the application service and have full ownership of their data stored as part of the application, while completely safe and isolated from other tenants' data. We also provide a REST-based API to enable robust and secure integration with our business logic and data.

Platform-wide availability and redundancy

We operate multiple geographically diverse data centers. Jira Align, along with several of our other cloud products, is hosted with the industry-leading cloud hosting provider Amazon Web Services (AWS), resulting in optimal performance with redundancy and failover options globally. Their data centers have been designed and optimized to host applications, have multiple levels of redundancy built in, and run on a separate front-end hardware node on which application data is stored.

Implementation

Jira Align is designed to operate with a range of cloud vendors to provide maximum flexibility for our customers, based on their existing relationships or business requirements:

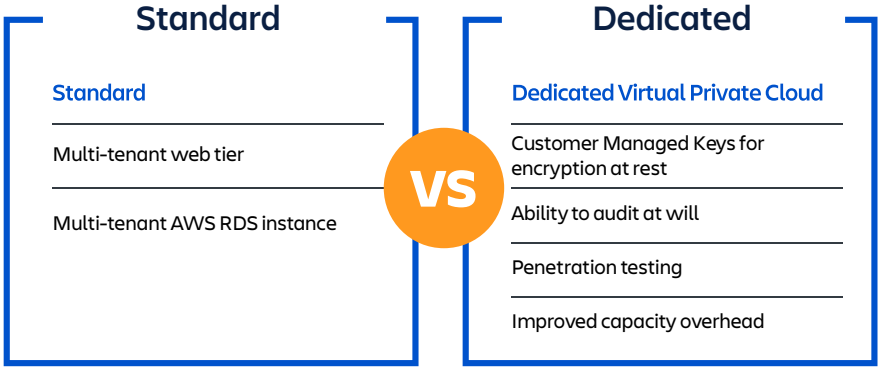
aws

Amazon Web Services (AWS) provides a geographically distributed solution to host VMs that leverage the latest fault tolerances, performance enhancements and security.

We care about high availability of your data and services. We focus on product resiliency through standards and practices that allow us to minimize downtime.

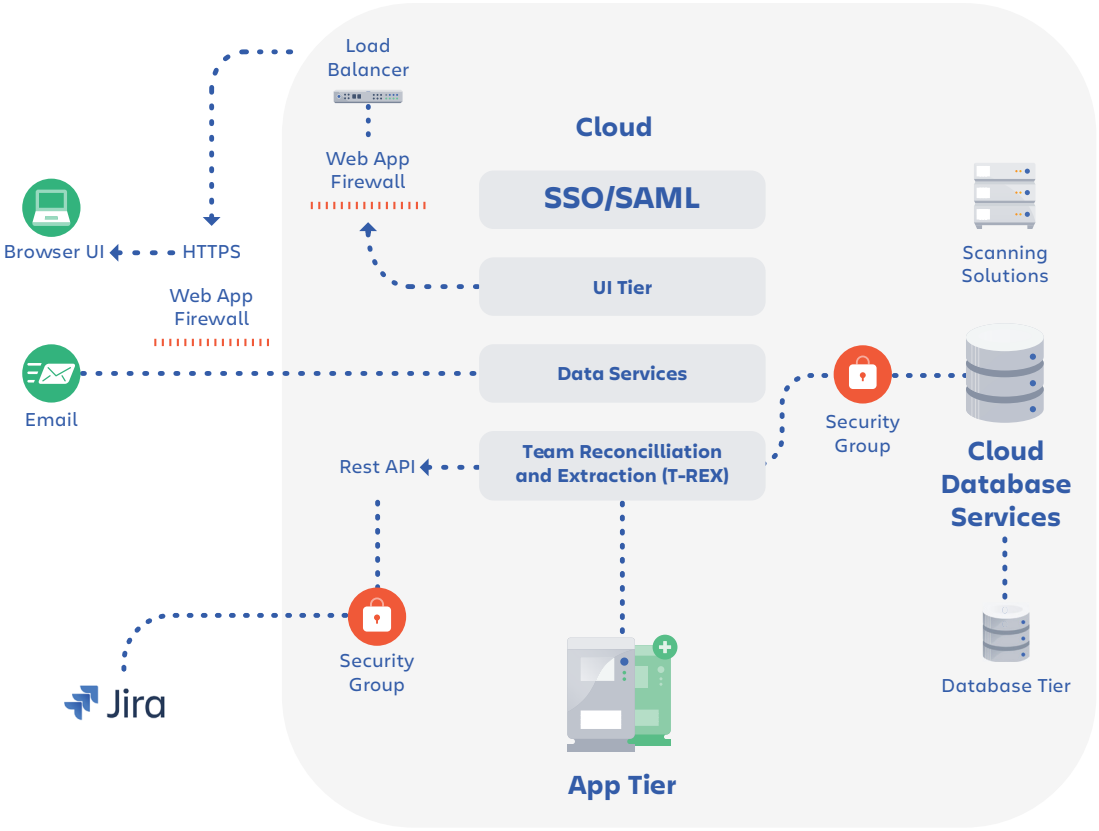
Jira Align supports both multi-tenant and a dedicated virtual private cloud.

Standard vs. Dedicated



The diagram below highlights a typical Jira Align implementation:

Jira Align Scaled Agile Management Platform Architecture



- User authentication via SSO/SAML is self-managed via our set of open APIs.
- Connectivity to team tools is managed via a set of pre-built configuration options within Jira Align. There is no need to build or customize an integration to any third-party tools.

Learn more at
atlassian.com/jira-align

The following measures highlight our security program:

DATA SECURITY

Jira Align provides data encryption at rest using AES 256

DENIAL OF SERVICE

We leverage a leading Web application firewall and content-delivery network service.

PHYSICAL SECURITY

The data centers we leverage are fully SOC 2 certified for physical security and infrastructure fault tolerance.

INTERNAL NETWORK

All traffic is sent via encrypted communication, and is firewall port blocked between devices.

SINGLE SIGN ON

SAML protocol streamlines user authentication/ authorization; we support Active Directory Federation Services, CA SiteMinder, and more.

BACKUP AND FAILOVER

Jira Align automatically maintains encrypted offsite storage of data backups, validated monthly.

SCANNING

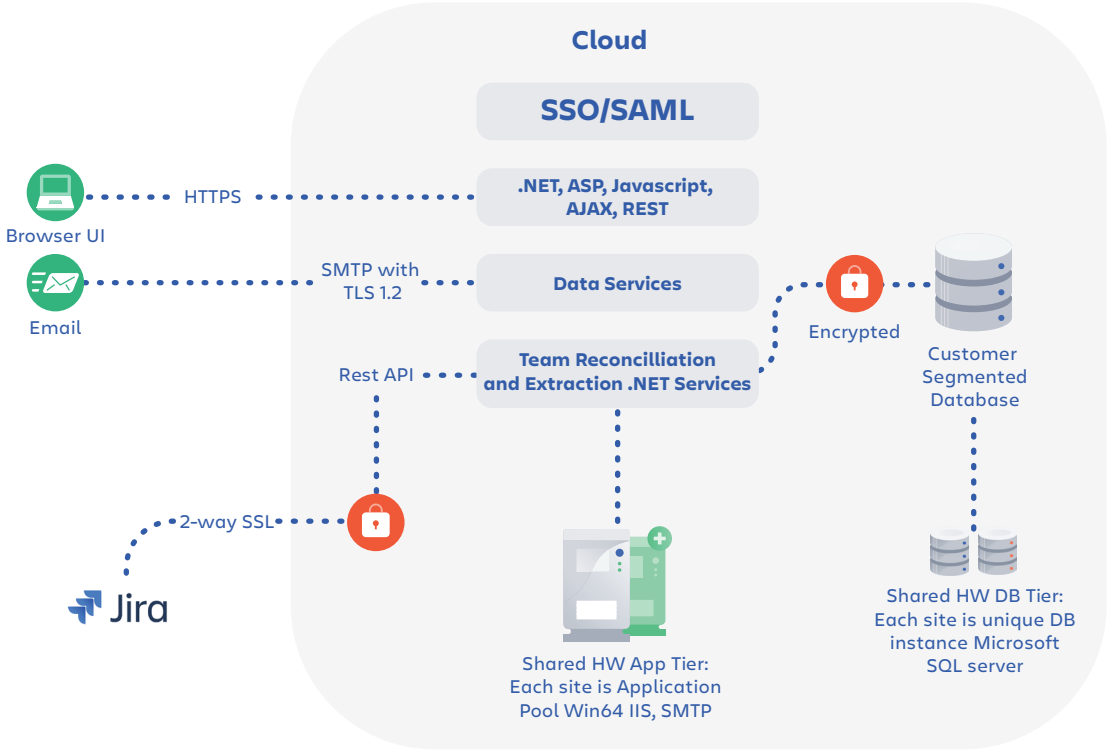
Our security policy includes daily port scans, system and application log analysis, virus and malware scans, and automated application and OS updates.

EXTERNAL NETWORK TRAFFIC

Users must access the platform via TLS 1.2 and an authenticated user account; we integrate with third-party tools via mutual TLS certificate-managed communication, and all email traffic is TLS encrypted. Jira Align maintains a Qualsys SSL labs rating of A+.

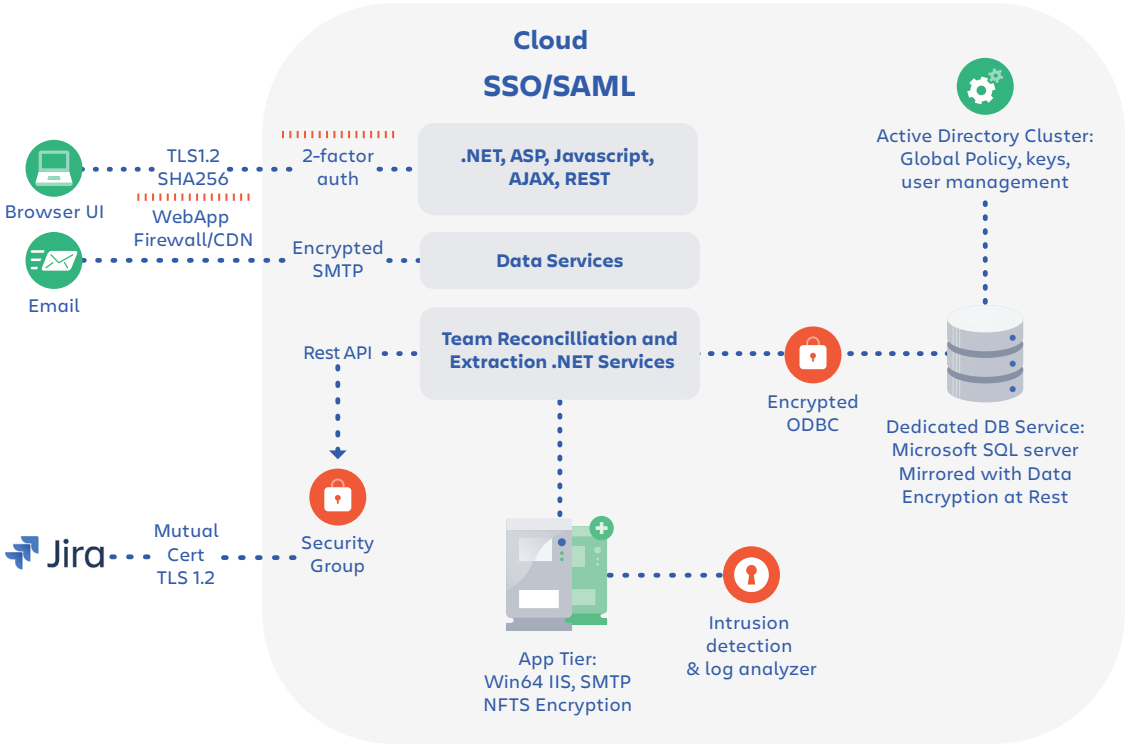
Below is a diagram of Jira Align architecture with a spotlight on security protocols:

Jira Align Scaled Jira Management Platform Architecture



Learn more at
atlassian.com/jira-align

Jira Align Scaled Jira Management Platform Architecture:
Dedicated Hardware and Maximum Security



Learn more at
atlassian.com/jira-align

Application trust

Atlassian has a secure application development approach based on elements of a range of industry standards, and incorporated into our agile workflow. Our team of security engineers continually do a rolling review of all source code in our products as part of our development cycle. Both automated and manual techniques are employed. We also utilize a mandatory dual peer review process, where multiple senior or lead developers review all commits to master. Agile workflows let us identify and fix any vulnerabilities quickly, especially for our cloud services. We train our developers on the OWASP Best Practices for development security.

Infrastructure trust

The Atlassian Security Team performs ongoing network vulnerability scans of both internal and external infrastructure using an industry leading vulnerability scanner on an ongoing basis. We also maintain an internal Red Team that conducts on-going penetration test operations of all our infrastructure, cloud services, and people. You can always find more information on our Vulnerability Management program on our website.

At Atlassian, we have a very limited set of engineers and architects who are allowed to install software in our production cloud environment. In most cases, software installation is not possible. We also utilize configuration management tools for our production environments to manage configuration of all servers. Any direct changes made to those systems will be over-written by the approved configuration ensuring consistency. We also rely on our Peer Review / Green Build (PRGB) controls to ensure multiple reviewers approve any changes.

Atlassian restricts, logs, and monitors access to our information security management systems. These restrictions include Access Control Lists (ACLs) and multi-factor authentication requirements. We restrict, log, and monitor access to our Atlassian Account Identity Store. Logs are stored in a logically separate system and write-access to the logs is restricted to members of the Security Team. Alerts are sent to the Security team when specific actions or events are identified within the logs.

Data trust

All data are backed up via AWS Relational Database Services with automated and secure snapshot capability and stored for 35 days. With this facility, the Jira Align solution can be recovered for a specific customer in case of failure or data loss. Additional controls include:

- **Multiple region availability, monitored in real time.**
- **Automated region failover tests performed each week on pre-production environment.**
- **Automated configuration data restore tests performed daily on Production.**

Jira Align has high availability deployments in the AWS regions where the solution is deployed. The Amazon Elastic Block Store (EBS) spans the entire geographic region in these data centers, with a data resiliency guarantee. All data for our services is encrypted in transit using TLS to protect it from unauthorized disclosure or modification, whether over HTTPS or SMTPS. Atlassian's implementation of TLS enforce the use of strong ciphers.

Atlassian's Enterprise Risk Management (ERM) Program performs an annual risk assessment which incorporates likelihood and impact for all risk categories and is aligned with the COSO risk model. We also perform functional risk assessments as needed based on risk profile.

Visit Atlassian's trust center to view Atlassian's compliance programs.

JIRA ALIGN'S INTERACTION WITH YOUR DATA IN JIRA

Jira Align interacts with your Jira data in order to connect the work being done to the company's strategy. Data is mapped automatically between Jira Software and Jira Align during the synchronization process. Some of the data connections support a two-way synchronization, outlined in the following diagram.

COMPANIES AROUND THE WORLD TRUST THE ATLASSIAN CLOUD

Atlassian chose in 2007 to invest early in the cloud as a delivery platform for our products. We have over 10 years of experience building our products in the cloud for our customers. Our investments give us the competitive advantage needed in the market that helps make your business successful.

Today more than 125,000 customers use our cloud products, with more than 90% of our new customers purchasing one of our cloud products. This accounts for over 10 million monthly active users on our cloud products.

The cloud continues to be our focus and we will continue to invest in the cloud to expand the value we provide our customers.

Your trust in Atlassian is extremely important. Here are some additional resources to consider when making your decision to go with us.

- Atlassian Trust Center
- Jira Align Trust Page
- Atlassian Security Practices
- Atlassian Trust and Security Community
- Jira Align Cloud Security Alliance Submission
- Cloud Security Approach and Practices
- Why Security is a Shared Responsibility
- Atlassian Transparency Report
- Atlassian Privacy Policy

ATLASSIAN