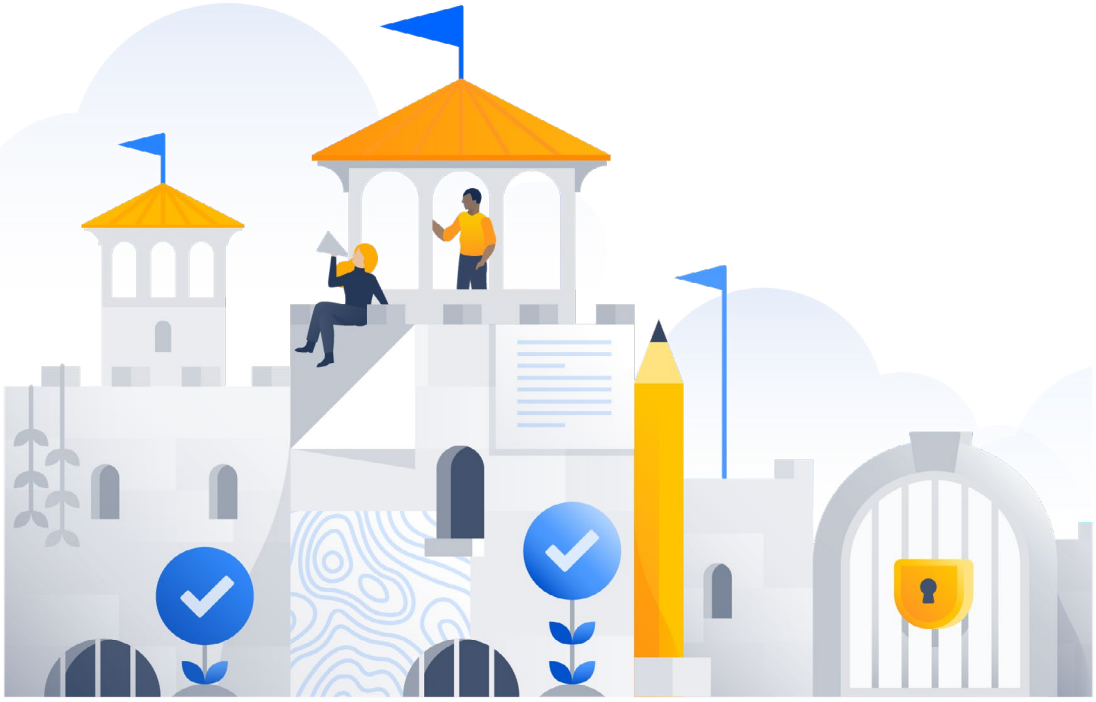
ATLASSIAN



Security @ Atlassian

An in-depth view of Atlassian's approach to Security

Table of contents

Most challenges – large and small – are solved not by individuals, but by teams. It's been our mission to unleash the full potential of every team, across organizations of all sorts throughout the world. In recent years, we've witnessed the growth of one of the most significant tools for team collaboration ever developed: the Cloud. And we've embraced it wholeheartedly. Our cloud products enable teams to collaborate and innovate more effectively, scale quickly, and focus more time and energy on their core mission.

The cornerstone of our cloud applications and services is ***security*** – our mission depends on it. So we're committed to ensuring the unfaltering safety and security of your company's data and to providing you with the information you need to understand and evaluate our security practices and policies for yourself.

This white paper outlines how the Atlassian security team keeps our cloud systems secure, the many steps we take to build security into our products, and the role your organization plays in keeping your work environment secure. We're transparent with our security program so you can feel informed and safe using our products and services. Our aim is to help your team take full advantage of all that Atlassian cloud services have to offer with the confidence that your organization's security is ensured.

It starts with trust

In cloud services, trust begins with security–but it doesn't end there. It also includes reliability, privacy, and compliance with industry standards and legal regulations. So, to fully earn your trust, our team is committed to these four principles:

Security

We follow extensive administrative, operational, and configuration practices to track and protect your information through a comprehensive set of security controls and practices. Our dedicated security team continuously improves our development, security operations, and threat-mitigation practices to detect and prevent new security threats, so you can rest assured that your data is safeguarded.

Reliability

Organizations run mission-critical projects and operations on Atlassian products – that's why we are committed to delivering products, applications, and networks that are stable and secure at scale. Our products are built on best-in-class core technologies and our business continuity, disaster recovery, and data backup programs ensure the impact on our customers is minimized in the event of a disruption to our operations.

Privacy

Your data is our responsibility, and we're committed to protecting it from unauthorized access and supporting your organization in meeting data privacy obligations around the world. We provide information and governance controls to help you make the right decisions for your organization. Additionally, we've invested heavily in GDPR, Privacy Shield, and stringent privacy safeguards to keep your data private and in your control.

Compliance

We encourage you to inspect and verify our security and privacy practices and operations. Our products regularly undergo independent third-party audits and certifications against global standards such as SOC2, ISO 27001, ISO 27018, and PCI DSS. Additionally, our service providers undergo regular SOC1, SOC2 and/or ISO/IEC 27001 audits to verify their practices.

Below you'll find our approach and practices regarding each of these four essential principles of trust.

Our approach to security

In this paper, we discuss Atlassian's approach to security. It covers the key steps we take and controls we implement across a number of security domains, both in securing our own environments (including our cloud-based platforms), and the processes we have in place to ensure we create products that are secure as possible for our customers and users.

Our security philosophy

Our approach to security is based around a couple of core themes:

- We want to lead our peers in cloud and product security
- Meet all customer requirements for cloud security and exceed requirements for industry security standards and certifications
- Being open and transparent about our programs, processes, and metrics. This includes sharing our journey and encouraging other cloud providers to do the same, and setting new standards for customers
- Identifying present and future security threats to Atlassian and its customers, and limiting the impact and duration of security incidents

In this section we highlight the range of measures and initiatives we have in place to fulfill this philosophy as covered by these key themes.

We're also proud of the fact that many of our flagship products underpin and form a critical part of our internal day-to-day processes and workflows at Atlassian. For example, our Jira and Confluence applications form key pillars of our approach to incident management and vulnerability management programs. That means we're invested in securing our products not only because one of our **key values** is we "don't #@!% our customers", but because we use those same products ourselves.

Our team

We know most companies would say this, but we're genuinely proud of our security team. We believe we have recruited and grown a team that consists of some of the best and brightest in the industry who have helped create unique initiatives and programs which underpin our security program. Our Security Team is headed up by our San Francisco based CISO and includes over 130 people based across our Sydney, Amsterdam, Bengaluru, Austin, Mountain View, San Francisco and New York offices (with some remote team members). The team is continually growing in recognition of the priority Atlassian places on security. We have multiple sub-teams, including:

- **Product security** – responsible for the security of our products and platforms
- **Ecosystem security** – responsible for the security of our Marketplace and add-ons
- **Security intelligence** – responsible for detecting and responding to security incidents
- **Red team** - responsible for adversary emulation and exercising Security Intelligence
- **Security architecture** – responsible for defining the security requirements of our products and platforms
- **Corporate security** – responsible for our internal security with respect to our corporate network and applications
- **Trust** - responsible for tracking and responding to customer expectations and provide transparency into our processes and practices

- **Development and SRE** – responsible for building and running tooling for the security team
- **Awareness and training** - responsible for ensuring our employees and partners know how to work securely

While our security team continues to expand, everyone at Atlassian is part of our vision; We want to lead our peers in cloud security, meet all customer requirements for cloud security, exceed requirements for all industry security standards and certifications and be proud to publish details about how we protect customer data. Our goals and vision are made clear to all of our staff throughout their time here at Atlassian.

While our security team continues to expand, everyone at Atlassian is part of our mission to achieve better security and this is made clear to all of our staff throughout their time with us.

Additional programs we use to support security

While we focus on doing the fundamentals of security , we also have a range of programs in place to ensure our approach to security remains wide-reaching, community-driven and proactive. These include:

Security Champions Program
We have security leads within all of our product and service teams who assume responsibility for delivering on key security initiatives among their peers on an ongoing basis and keeping communication flows with our central security team as open as possible. In this way, we keep security front and center of mind across our organization.

Security Detections Program
Our security detections program compliments Atlassian's incident response processes. Embedded within our standard incident management process, we have put in place a **separate program** to proactively create searches and alerts for not only the incident types we face today, but those we will face in the threat landscape of the future.

Bug Bounty Program
Our **Bug Bounty Program** has consistently been recognised as one of the best in the industry, and enables us to leverage a trusted community of tens of thousands of researchers to test our products constantly and report back any vulnerabilities they find.

Continually improving our security program

We are intent on ensuring our security program remains cutting edge and being leading peers in the industry. We know to do that, we need to continually evaluate our current approach to security (including in comparison to our industry peers) and identify opportunities for improvement.

To this end, we have undertaken (and will continue to undertake) numerous maturity assessments of our security program, using independent reputable security consulting companies. In 2020, we also performed a peer assessment of our overall Trust and Security Program. We take the outputs from these processes, including key recommendations, and use them to address any gaps in that have been identified and opportunities for improvement.

We have also defined a series of programs across our various security capabilities – such as Product Security and Security Intelligence – to guide our internal improvement processes. We have defined metrics to support each of these programs which we review through our Security Management Team. We use these metrics to identify and target areas for improvement across each of our core capabilities.

More information

While this paper will provide a broad overview of our approach to security, more detail regarding our security program is available on our Atlassian Trust Center. There's also a range of dedicated whitepapers on different areas of our security program available, including:

- **Our Security Practices**
- **How Atlassian Manages Customer Data**
- **Our Approach to External Security Testing**
- **Our Approach to Managing Security Incidents**
- **Our Approach to Vulnerability Management**
- **Cloud Security Shared Responsibilities**
- **Our Atlassian Trust Management System**
- **Our Atlassian Security & Technology Policies**

You can also view details of the Atlassian Controls Framework we have developed to bring together the security requirements of seven international standards, which underpins our approach to security and compliance.

Securing our internal environment

An effective approach to security starts with getting our own house in order – specifically by keeping our own internal environments secure. There are a number of steps we take to achieve this.

Building security into our network architecture

Atlassian practices a layered approach to security for our networks. We implement controls at each layer of our cloud environments, dividing our infrastructure by zones, environments, and services. We have zone restrictions in place that include limiting office/staff, customer data, CI/CD and DMZ network traffic. We also have environment separation to limit connectivity between production and non-production environments, and production data is not replicated outside of production environments. Access into production networks and services is only possible from within those same networks – e.g. only a production service can access another production service.

Services must be explicitly authorized to communicate with other services through an authentication allowlist. We control access to our sensitive networks through the use of virtual private cloud (VPC) routing, firewall rules, and software defined networking, with all connections into those networks encrypted. We've also implemented intrusion detection in both our office and production networks to detect potential compromises.

Securing access to our networks through ZeroTrust

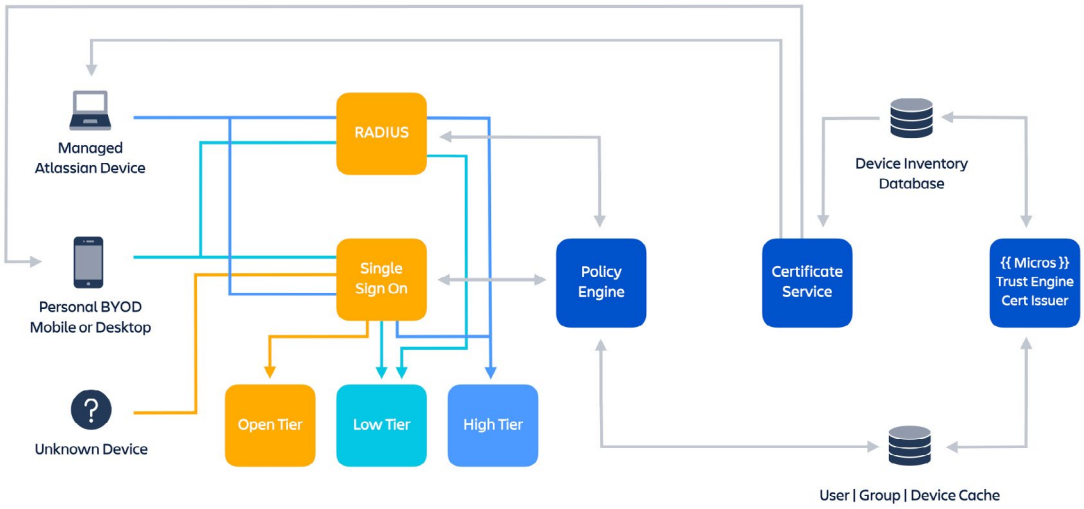
Atlassian secures access to its corporate network, internal applications and cloud environments through a concept called ZeroTrust. Simply stated, the core tenet of ZeroTrust is: "*never trust, always verify*."

ZeroTrust moves away from traditional approaches for network security that rely solely on authentication of a user to determine whether a user can access resources on our network. Such an approach introduces the risk of an untrusted and insecure device potentially compromising security. As a result, many organizations have begun moving to a model in which only trusted devices are able to access their network using approaches such as mobile device management technologies or restricting access at a network level to a list of known devices.

While useful, these approaches lack granularity. Atlassian's approach to ZeroTrust effectively ensures that whether users are able to access resources and services on our networks is a decision based on not only their authentication credentials, but also involves a dynamic policy decision that takes into account a range of factors to deny or allow access at a per-resource level based on the security posture of the user's device (regardless of their location).

In simple terms, we have created three tiers of resources (based on their relative criticality and sensitivity) on our network around which ZeroTrust works:

- **Open tier** – Any corporate user who successfully authenticates into our network can access these services
- **Low tier** – Access to these resources is available to an authenticated corporate user only if they are accessing our network from a trusted corporate device (devices that Atlassian owns and manages) or a managed BYOD (this is a personal device that has been enrolled into Atlassian's MDM program)
- **High tier** – These resources are only available when accessed by an authenticated corporate user from an Atlassian issued corporate device. Access into our production services from our corporate network is only possible via a high-tier device and SAML authentication



Atlassian's implementation of ZeroTrust works using a range of automated processes, services and components. At a high level:

- Authenticated users on corporate or managed BYOD devices are granted a certificate by our Trust Engine service. The certificate includes metadata that marks whether it is for a BYOD or corporate device. These are deployed onto devices using our endpoint management solutions and re-issued (or revoked) on a regular basis
- When a user authenticates, their certificate is requested and presented to our infrastructure. The information from the certificate is used to verify the user's account is valid and what type of device they have. Based on this information, the user is pushed either into our low tier network where their network and application access is restricted, or they are granted access to our high tier
- Devices connected to Atlassian's network are polled on an hourly basis and cross-referenced with our endpoint management solutions to determine ownership, device security and posture information. This includes ensuring devices meet minimum requirements including for anti-malware, encryption, OS versions etc
- A central database is updated with information regarding the compliance of user devices. This is used to determine whether users will be allowed or denied access to resources

on our network. Devices marked as non-compliant will have their connection to our network terminated.

Atlassian has written a separate paper describing our **philosophy and implementation of a ZeroTrust architecture**.

Managing access to our systems and services securely

Atlassian has a well-defined process for provisioning (assigning or revoking) user access for all systems and services. We have an established workflow (8-hour sync) linking our HR management system and our access provisioning system. We use role-based access control based on predefined user profiles to ensure staff only have access appropriate to their job role. All user accounts must be approved by management prior to having access to data, applications, infrastructure or network components.

Supporting our ZeroTrust architecture, we control access to our corporate applications through a single-sign on platform. To access any of our applications, staff need to authenticate via this platform, including through the use of a second factor of authentication. Users need to authenticate either through U2F keys or via a mobile application authenticator provisioned to Atlassian employees – we have removed less secure authentication methods such as SMS and phone-based OTPs. Atlassian has adopted this approach to ensure our authentication process is highly resistant to phishing-based and man-in-the-middle attacks - any system that sends codes in a text message can be compromised by a skilled attacker.

Securing our endpoint devices

Atlassian uses a combination of endpoint management to deploy updates and patches to operating systems and key applications across our endpoint fleet. We have also implemented multiple endpoint protection solutions to protect against threats such as malware.

As part of our ZeroTrust approach, Atlassian staff who wish to access most of our services via their personal mobile devices need to enrol into our Mobile Device Management (MDM) Program. This enables us to make sure all mobile devices connecting to our network meet our minimum security requirements, covering aspects such as encryption, device locking, anti-malware software and OS versions.

All eligible staff who enrol in and maintain compliance with our MDM program receive a monthly allowance from Atlassian for their participation.

Any device identified as being not compliant will result in that staff member receiving an email notifying them of the non-compliance. Staff are given a 24-hour grace period to remediate the non-compliance before their access from that device is removed.

Security in our day-to-day operations

We strive hard to build security into all aspects of our day-to-day operational processes. We want security to be an inherent part of how we do things so that we minimise the need to 'retrofit' or 'bolt-on' security after-the-fact.

Keeping track of our information assets

Our production systems are located in infrastructure obtained through cloud service providers. These systems are not tracked at a hardware level due to the nature of the service. The underlying microservices that our products run on are tracked in a custom-built 'Service' database. This database is updated automatically when a service is deployed.

Our Workplace technology team maintains an asset inventory of all endpoints using our own Jira software for tracking purposes.

Managing changes in our environment

Our change management process is slightly different from a traditional one. Traditional change management processes rely on a pyramid-style change control hierarchy. That is, when someone wants to make a change, it has to be presented to a board that eventually approves or denies it.

We have embraced an open source style approach we call “Peer Review, Green Build” (PRGB). In contrast to a traditional change management process the PRGB approach requires that each change – be it a code change or an infrastructure change – is reviewed by one or more peers to identify any issues the change may potentially cause. We increase the number of reviewers based on the criticality of the change or the criticality of the systems that the change is going to impact, trusting our engineers to identify issues and then flag them before the change can go through. This process works well to provide a dynamic and adaptable way of managing changes in our environment. The green build portion of this control refers to a successful or clean build in our CI/CD with the new changes included. If the change introduces components that do not successfully pass any of the integration, function, unit or security tests, the build is rejected and returns to the original change request to address any issues.

Managing configurations in our systems

We have a limited set of engineers and architects who are allowed to install software in our production environment. In most cases, software installation is not possible. Configuration management tools are utilised in our production environments to manage configurations and changes to servers. Direct changes made to those systems are set to be overwritten by the approved configuration pushed through those configuration management tools ensuring consistency. We rely on standard Amazon Machine Images (AMIs), all changes to either our AMIs or operating systems must be made via our standard change management process, we track and report on exception configurations, and we have implemented resource isolation so issues with services don’t impact other services. We also rely on our Peer Review / Green Build (PRGB) process to ensure multiple reviewers approve configuration changes pushed through configuration management tools. All builds are cryptographically signed and only signed builds are allowed to run in our production environment.

Making use of logs

We use a SIEM platform to aggregate logs from various sources, apply monitoring rules to those aggregated logs, and then flag any suspicious activity. Our internal processes define how these alerts are triaged, investigated further, and escalated appropriately. Key system logs are forwarded from each system where logs are read-only. The Atlassian Security Team creates alerts on our security analytics platform and monitors for indicators of compromise. Our SRE teams use this platform to monitor for availability or performance issues. Logs are retained for 30 days in hot backup, and 365 days in cold backup.

Key system logs are combined into both an internal log analysis system and an Intrusion Detection System.

Logs are a key component of our overall incident detection and response strategy which is covered in detail in 'How we identify, protect against and respond to security threats' section.

Business continuity and disaster recovery management

We care deeply about the resiliency of our products, not least because we – internally, in Atlassian – rely on the very same products. We appreciate that disruptions can happen. So we are determined to build-in processes to plan for disruptions, and handle disruption with minimal impact to our customers when they do occur. Our business continuity (BC) and disaster recovery (DR) programs capture the various activities done to meet those objectives.

Leadership involvement in BC and DR planning activities ensures the oversight required to make sure accountability for resiliency reaches all teams. Our BC and DR planning activities strive to achieve the right balance between cost, benefits and risk through an analysis of 'recovery time objectives' (RTO) and 'recovery point objectives' (RPO) of services. This analysis has led to us establishing a simple 4-tier system to help group services based on their respective recovery requirements – details of this approach can be found on our page on **How Atlassian Manages Customer Data**.

Our BC and (DR) programs involve the following activities:

1. building-in redundancy measures to meet resiliency requirements
2. testing and verifying those redundancy measures
3. learning from tests to continuously keep improving BC and DR measures

We build our products to best utilise redundancy capabilities, such as availability zones and regions, offered by our cloud service providers.

We continuously monitor a wide range of metrics with the aim of detecting potential issues early. Based on those matrices, alerts are configured to notify site reliability engineers (SREs) or the relevant product engineering teams when thresholds are breached so that prompt action can be taken through our incident response process. SREs also play a key role in identifying gaps in the DR program, and work with our risk and compliance team to close those gaps. Each of our teams also include a DR champion to oversee and help manage disaster recovery aspects related to that team.

Our DR tests cover process and technology aspects, including relevant process documentation. The frequency of DR tests are done in line with the criticality tier of each service – for example, backup and recovery processes for key customer facing systems are tested quarterly. We conduct manual and ad-hoc failover tests on our systems. These tests range from less complicated table-top simulation exercises to more complicated availability zone or regional failover tests. Regardless of the complexity of the test, we are diligent in capturing and documenting test results, analysing and identifying possible improvements or gaps, and then driving them to closure with the help of Jira tickets to ensure continuous improvement of the overall process.

We conduct annual Business Impact Assessments (BIAs) to assess the risks associated with critical services. The output of these BIAs assist in driving the strategy for DR and BC efforts. As a result, critical services are able to develop effective DR and BC plans.

Service availability

In addition to the above measures, we also publish our **service availability status** in real-time for our customers using our own Statuspage product. If there are any issues with any of our products, our customers will know as soon as we do.

Backups

We operate a comprehensive backup program at Atlassian. This includes our internal systems, where our backup measures are designed in line with system recovery requirements. With respect to our Atlassian Cloud offerings, and specifically referring to customer and application data, we also have extensive backup measures in place. Atlassian utilises the snapshot feature of Amazon RDS (Relational database service) to create automated daily backups of each RDS instance.

Amazon RDS snapshots are retained for 30 days with support for point-in-time recovery and are encrypted using AES-256 encryption. Backup data is not stored offsite but is replicated to multiple data centers within a particular AWS region. We also perform quarterly testing of our backups.

Physical security

Physical security controls in our offices are guided by our physical and environmental security policy which ensures robust physical security is implemented across our environments on premises and in the cloud. This policy covers areas such as secure working areas, securing our IT equipment wherever it may be, restricting access to our buildings and offices to appropriate personnel, and monitoring physical ingress and egress points. Our physical security practices include reception attendance during work hours, requirements for visitors to register, badge access to all non-public areas, and we partner with our office building management for after hours access and video recording at ingress and egress points - both for main entrances as well as loading areas.

Our partner data centres are SOC-2 compliant, at a minimum. These certifications address a range of security controls including physical and environmental security and protection. Access to the data centres is limited to authorized personnel, and verified by biometric identity verification measures. Physical security measures include on-premises security guards, closed circuit video monitoring, man traps, and additional intrusion protection measures.

Keeping data secure

We have a number of measures to ensure that we keep customer data secure, available and that customers retain control over it to the fullest extent possible.

Data centers

Atlassian products and data are hosted with the industry-leading cloud hosting provider Amazon Web Services (AWS). We make use of optimal performance with redundancy and failover options globally. We make use of multiple geographically diverse regions within AWS (US-East and US-West, European union and the Asia Pacific), and multiple availability zones within each of those regions to ensure that a failure in any single data center does not affect the availability of our products or customer data. For more information, see our separate paper on **How Atlassian Manages Customer Data** and our **Cloud Hosting Infrastructure** page.

Physical access to our data centers, where customer data is hosted, is limited to authorized personnel only, with access being verified using biometric measures. Physical security measures for our data centers include on-premise security guards, closed-circuit video monitoring, man traps, and additional intrusion protection measures.

Encryption of data

Any customer data in Atlassian cloud products is encrypted in transit over public networks using TLS 1.2+ with Perfect Forward Secrecy (PFS) to protect it from unauthorized disclosure or modification. Our implementation of TLS enforces the use of strong ciphers and key-lengths where supported by the browser.

Data drives on servers holding customer data and attachments in Jira Software Cloud, Jira Service Desk Cloud, Jira Core Cloud, Confluence Cloud, Statuspage, Opsgenie, and Trello use full disk, industry-standard AES-256 encryption at rest. Bitbucket does not offer encryption at rest for repositories at this time. Please refer to the **Atlassian Trust Roadmap** to keep up to date with our platform updates.

Key management

Atlassian uses the **AWS Key Management Service (KMS)** for key management. The encryption, decryption, and key management process is inspected and verified internally by AWS on a regular basis as part of their existing internal validation processes. An owner is assigned for each key and is responsible for ensuring the appropriate level of security controls is enforced on keys.

Tenant separation

While our customers share a common cloud-based IT infrastructure when using Atlassian's products, we have measures in place to ensure they are logically separated so that the actions of one customer cannot compromise the data or service of other customers.

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 that are processed by Jira or Confluence have a "tenant-specific" view so other tenants are not impacted

In broad terms, the TCS works by storing 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.

The context provided by the TCS effectively acts as a "lens" through which any interactions with customer data occur – and this lens is always confined to one specific tenant. This ensures that one customer tenant does not access data of another tenant – nor for one tenant to affect the service of another tenant through their own actions.

More information about our cloud architecture is available as part of our **cloud support resources**.

Sharing the responsibility for managing customer data

Atlassian assumes responsibility for security, availability and performance of the applications we provide, the systems they run on, and the environments within which those systems are hosted. However, security is a joint responsibility between Atlassian and our customers with respect to four areas in particular:

Policy and compliance
ensuring that the system meets customer business needs and is operated in accordance with industry, regulatory and legislative compliance obligations.

Users
the creation and management of user accounts.

Information
the content customers store within Confluence Cloud, Jira Cloud, Trello or Bitbucket Cloud.

Marketplace Apps
third party services which integrate with Atlassian products.

While Atlassian takes all necessary steps to protect and secure customer data, the reality is that the decisions our customers make about how they set up our products also have a significant influence on the way security is implemented. Important issues they need to be aware of when using our products include:

- **Domain verification and central management of user accounts** – administrators from our customer organizations can verify one or multiple domains to prove they own them. Verification of domains allows an administrator to centrally manage all of their employees' Atlassian accounts and apply authentication policies (including password requirements and SAML). This is an important step we strongly encourage all of our customers to take in helping to secure access to their accounts, and the data available through them
- **Access permissions** – While our products are by nature designed to enable collaboration, customers do need to exercise caution in the permissions they grant to users within their organization regarding access to data. In some cases they can also grant public access to data – Atlassian has no control over this and cannot in these cases prevent such data being copied or further distributed
- **Centralized access** – Our customers are strongly encouraged to use **Atlassian Access** for centralized administration and enhanced security across all Atlassian products they use (including use of enforced 2FA and single sign-on)

For more information, see our paper on **Cloud Security Shared Responsibilities**.

Controlling access to customer data

We treat all customer data as equally sensitive and have implemented stringent controls governing this data. Awareness training is provided to our internal employees and contractors during the on-boarding process which covers the importance of and best practices for handling customer data.

Within Atlassian, only authorized Atlassian employees have access to customer data stored within our applications. Authentication is done via individual passphrase-protected public keys, and servers only accept incoming SSH connections from Atlassian and internal data center locations. All access is restricted to privileged groups unless requested and reviewed, with additional authentication requiring 2FA.

With stringent authentication and authorization controls in place, our global support team facilitates maintenance and support processes. Hosted applications and data are only able to be accessed for the purpose of application health monitoring and performing system or application maintenance, and upon customer request via our support system. Our customers are also provided with options regarding explicit consent as to which support engineers are appropriate to access their data through our **consent control checker**.

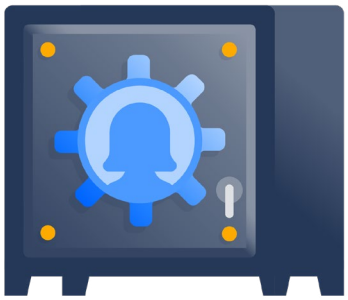
Unauthorized or inappropriate access to customer data is treated as a security incident and managed through our incident management process. This process includes instructions to notify affected customers if a breach of policy is observed.

Retention and deletion of data

We have provisions in place so that we can respond to **user requests to delete personal information**, and we also help end users with Atlassian accounts delete their personal information. We also have **import and export tools** so that our customers can access, import and export their data using Atlassian's tools.

Customer sites are deactivated 15 days after the end of a customer's current subscription period. Atlassian retains data for deactivated sites for 15 days (for evaluation sites) or 60 days (for paid subscription sites) after the end of the customer's current subscription period. Note that in the case of Jira, data will only be deleted if you unsubscribe from all Jira products you were previously subscribed to.

Additional information is available on our **Security Practices page** or on our **Data Storage FAQ**.



Securing our people

We are intent on making sure all of our staff know how to do their work securely and are empowered to act accordingly. Embedding a security mindset is at the forefront of Atlassian's culture, and contributes towards lifting our overall resiliency against potential cyber attacks.

Security awareness training

We make sure all staff undergo security awareness training during the onboarding process and then on an ongoing basis so that security remains 'front of mind'. We understand that many of the threats faced by our team are the same threats faced by our contractors and other partners we work with, so we extend security awareness training to cover those contractors and partners as well. Topics addressed in our security awareness training program include current threats and scams, secure working practices, potentially risky behaviours that create security risks, and compliance and regulatory issues.

In addition to general information security training, more targeted training is available to our developers on secure coding. Development teams are also supported through both security champions or embedding a security engineer in those teams to help with security-related operational tasks.

We also maintain open channels of communication between our employees and the security team through instant messaging channels, blog posts, FAQs, etc., so that the security team is as accessible as possible to all Atlassian staff.

During the month of October, Atlassian Security hosts Security Awareness Month for all employees and partners. This is a time to celebrate the achievements everyone has made toward keeping our company secure, as well as reinforce important security education with fun games and internal talks.

Security champions program

In 2017 we started rolling out a security champions program across Atlassian to nominate a security lead within every one of our product and service teams. The goal of this program is to have dedicated champions within each product who assume responsibility for promulgating key security messages and practices among fellow team members and raises any security issues with our central security team to facilitate improved communication flows.

Our champions are also provided with dedicated training to help them understand and identify application security vulnerabilities, leading secure development practices, as well as processes for writing secure code.

Atlassian's security champions meet on a regular basis to share tools and knowledge around the latest security issues and challenges they're facing so that all our teams can benefit. The program has served as a springboard for enabling security to form an even more integral part of our culture.

Background checks

We want to hire people that will go on to positively shape the security-embedded culture we have built. Background checks are performed on all new recruits to aid in this process. A criminal check is run on all recruits across the board; education verifications, employment verifications, and credit checks are added if the role requires it. A full background check is always performed for senior executives, and for roles that handle financial aspects of Atlassian.

Securing our products

Atlassian is focused on ensuring that security forms a key part of all phases of our product life cycles. There are a number of methods we utilise to achieve this.

Security scorecards

We're focused on ensuring that security is front and center of mind across our entire product suite. To this end, we've implemented an accountability and monitoring system referred to as "product security scorecards" to measure the security posture of all products at Atlassian. This is an automated process Atlassian has created whereby we use a broad range of security-focused criteria (e.g. current vulnerabilities, training coverage, recent security incidents and security champions coverage) to provide an overall security score for each of our products.

This scoring process gives each of our product teams an objective view into what areas of security require attention, and identifies existing gaps that need to be addressed and actions to address these gaps. The security scorecards process also enables the Atlassian security team to easily keep track of how all products are tracking from a security perspective over time, particularly as our product suite continues to scale.

Embedded security engineers

Our product security team runs a security embedding program providing guidance to product teams and ensuring security processes are integrated into the development lifecycle. All products are supported through this program, either with dedicated embedded engineers for our most security critical products, or via a rotation of engineers available for other teams. Embedded engineers provide security consulting support, and also help teams monitor, interpret, and promptly action findings that are identified through the scorecard system.

Targeted security assurance

The product security team also runs a security review process to provide security assurance across software projects. A risk-based process is used to prioritise where to focus assurance activities, and identify what actions are required to mitigate project risk. Depending on the identified level of risk, assurance activities include a combination of:

- Threat modeling
- Design review
- Code review (manual and tool assisted)
- Security testing
- Independent assurance using expert third party researchers and consultants

As we discuss elsewhere in this paper, we also have an industry leading Bug Bounty Program which provides ongoing security assurance using a trusted, crowd-sourced group of security researchers.

Secure design through threat modelling

During the planning and design phases for our products, threat modelling to understand better security risks when projects face complex threats or involve development of security critical features. This involves a table-top/ brainstorm session between our engineers, security engineers, architects and product managers to identify and priority relevant threats. This information feeds into the design process and ensures appropriate controls are implemented. It also supports targeted review and testing in later phases of development.

Code analysis

We have an automated code analysis platform (called Security Assistant) that covers all code repositories at Atlassian. This platform runs a variety of static analysis tools (which we are continually adding to and improving) that help to ensure the overall security of our code. Any time a pull request is raised in a repository, the platform:

- Finds and identifies outdated code dependencies that may introduce vulnerabilities (we discuss these in more detail in the part of this paper that discusses our approach to vulnerability management)
- Identifies any accidental or inadvertent disclosure of secrets in code repositories (e.g. authentication tokens or cryptographic keys)
- Undertakes an analysis to identify any problematic coding patterns that could lead to vulnerabilities in our code

Security knowledge base

To ensure we build the most secure products possible, we make sure our developers have access to the support they need to build their knowledge continually regarding relevant security issues and threats they need to be aware of. To this end, we maintain an application security knowledge base internally that our developers can access whenever required. This is supported by our Security Champions program; providing presentations to our development teams on specific patterns and issues that we have observed which may have security implications.

How we identify, protect against and respond to security threats

Security testing

Our security testing approach is built around the concept of 'continuous assurance' – not only do we make use of targeted, point-in-time penetration tests, we also have an always-on testing model using a crowd-sourced bug bounty. We believe this multi-faceted approach maximises our chances of finding vulnerabilities and providing our customers with the most secure products possible. More information is available in our separate paper covering our **approach to external security testing**, and a summary of our testing measures is provided below:

- **Internal Security Review** - As mentioned above, our Product Security team runs a security review program including security testing as a regular activity. Testing consists of code review and application security testing, targeting areas of weakness highlighted by risk assessment
- **External Penetration Testing** - We use specialist security consulting firms to conduct white-box, code assisted and threat based penetration tests on high risk products and infrastructure (whether this be in our cloud environments, a new product or a fundamental re-architecture)

- **Atlassian's Red Team** – We have an internal red team whose role is to simulate adversaries attempting to identify and exploit vulnerabilities that exist within our systems, processes, and environments, so that we can ensure they are identified and addressed as promptly as possible
- **Bug Bounty** - We also make use of Bugcrowd's community of trusted security researchers to run our acclaimed bug bounty program, so that we can continually identify vulnerabilities in our products and ultimately make the cost for the bad guys in finding and exploiting those vulnerabilities higher over time. Our **bug bounty program** has been recognised on multiple occasions as **the best in the industry**. More than 25 of our products or environments – ranging across our server products, mobile apps and Cloud products – are in-scope for our bug bounty program. More information about the bug bounty program, including access to current bug bounty reports, is available on the **Atlassian Trust Center**

Vulnerability management

Atlassian is constantly striving to reduce the severity and frequency of vulnerabilities in our products, services and infrastructure. To this end, we have a multi-faceted and continually evolving approach to vulnerability management that utilises both automated and manual processes across both our products and infrastructure.

We track vulnerabilities we identify using our internal ticketing systems in Jira, and we have created a purpose-built tool that provides a 'single pane of glass' view for tracking the current status of vulnerabilities that exist across our products and infrastructure throughout the Atlassian environment. This means we have a central point from which we can track every vulnerability that has been identified to ensure that nothing accidentally gets forgotten or overlooked. A summary is provided below, and more information is available in our dedicated paper on **Atlassian's approach to vulnerability management**.

Infrastructure

We use a range of vulnerability detection tools that are run regularly across our infrastructure to automatically scan for and identify vulnerabilities. This includes:

- **Network scans** – to identify active services, open ports and applications running across our environment, as well as any vulnerabilities at the network level
- **Continuous asset discovery** – we undertake continuous asset discovery and security analysis across our external network perimeters. We also have an internally developed asset inventory and discovery mechanism
- **AWS Configuration Monitoring** – we monitor the configuration of our AWS environments against established configuration baselines

We are continually reviewing the latest tools available and adding them to the suite we use if we believe they will enhance our vulnerability detection capabilities.

Products

As part of our development process – and in addition to our previously mentioned bug bounty program - we use a range of tools to try to identify and prevent as many vulnerabilities and bugs as possible from making their way into our products by the time our customers and users have access to them. We use a platform to facilitate the deployment of these tools across our code repositories. These include the following:

- Atlassian deploys the bulk of its services using Docker container images. These images provide a packaged, self-contained environment consisting of relevant system libraries, tools, configuration settings and any other dependencies required so that our products are able to run regardless of individual machine configuration parameters. We integrate a full container security scanning process into our **CI/CD pipeline** for any containers that are deployed into our development, staging or production environments
- Our products and services rely on numerous open source libraries. We use a combination of internally built, open source, and commercial tools to scan for and identify dependencies and compare these to a database of known security vulnerabilities

In addition, when a vulnerability is identified by one of our users during standard use of a product, we welcome notifications and respond promptly to any vulnerabilities submitted. We keep the submitter updated as we investigate and respond to the issue.

As we have also mentioned previously in this paper, we use a “Peer Review, Green Build” (PRGB) process that means that any change in code to a product is reviewed by one or more peers to identify any issues the change may potentially cause.

We have a documented **bug fix policy** which defines the timeframes for resolving security issues in our products, depending on the severity level of the bug.

More information about our bug fix policy is available here. Information about recently fixed bugs, as well as bugs we’re currently working on addressing for our various products, are available at our **public bug tracker**.

Incident response

Atlassian has a comprehensive approach to handle security incidents. We consider a security incident to be any instance where there is a negative impact to the confidentiality, integrity or availability of customers’ data, Atlassian’s data, or Atlassian’s services.

We have a clearly defined internal framework that includes documented playbooks for different incident types. The framework covers the steps we need to take at all stages of incident response to ensure our processes are consistent, repeatable and efficient. These include coverage of incident detection and analysis, incident categorization, containment, eradication and recovery. This consistency is supported through the use our own products, including Confluence, Jira and Bitbucket as part of our incident response processes:

- Confluence is used to create, document and update our response processes in a central location
- Jira is used to create tickets for tracking progress on the response process for security incidents (potential and actual) from start to finish
- Bitbucket is used in instances where we develop code-based solutions for responding to certain edge-case problems that arise with certain incidents

Comprehensive and centralized logging and monitoring of our products and infrastructure is in place to ensure we quickly detect potential incidents, supported by a team of highly-qualified on-call incident managers who have significant experience in coordinating an effective response. We also have access to a range of external experts to assist us with investigating and responding as effectively as possible.

We have notification processes in place for our customers if their data is involved in a confirmed incident, as well as a robust post-incident review process so we can take any lessons from an incident to improve our practices to make the job of malicious actors harder in the future. For more information, please see our separate paper our Atlassian Trust Center on **Our Approach to Managing Security Incidents**.

Security detections program

In recognition of the need to build upon our approach to incident management in the context of an increasingly complex threat landscape, Atlassian has introduced what we call our "security detections program". Detections are searches that run proactively on a scheduled basis on Atlassian's Security Incident and Event Management platform to detect malicious activity targeting Atlassian and its customers.

Our security intelligence team focuses on the regular creation of new detections, tuning and improving existing detections, and automating detection responses. They do this across a number of dimensions, including products, attack types and log sources so as to ensure the coverage of our detections is as effective and comprehensive as possible.

The aim of the program is to ensure we not only ensure we are prepared for the threats we face today, but sufficiently anticipate and prepare for the threat landscape of the future. Our security intelligence team has also created a tool to standardize the detections we create to ensure a high level of consistency and quality amongst the detections we execute – something we believe is a first in the industry.

For more information about our detections program, please visit this page on our **Atlassian Trust Center**.

Securing our ecosystem and supply chain partners

Supplier risk management

Where Atlassian engages any third-party suppliers (including contractors and cloud service providers) we are intent on making sure those engagements do not in any way jeopardise our customers or their data. To this end, a review process is undertaken by our legal and procurement teams for any proposed third-party supplier engagements. For any engagements we deem high or critical risk, these are subject to additional reviews by our security and risk and compliance teams. Ongoing due diligence also occurs via subsequent reviews - either upon contract renewal or annually depending on the risk level of the engagement.

Atlassian also requires its suppliers to comply with minimum security requirements as part of their engagement with us. These are enforced via inclusion in our supplier contracts. These requirements will vary depending on the risk level of the engagement, and includes the following:

- SAML integration with Atlassian's single sign on platform
- Encryption for data in transit and at rest using non-deprecated algorithms
- Having sufficient logging mechanisms in place to provide Atlassian with relevant information regarding potential security incidents

The Atlassian marketplace

Atlassian's marketplace is a platform where users of our products are able to buy apps that provide add on-functionality to Atlassian products, or enable our products to connect with third party tools. While most of the applications made available in the marketplace are produced by third-party developers, Atlassian takes a number of steps to ensure that security still forms a central part of the marketplace ecosystem. These include:

- **The Marketplace Bug Bounty Program** – this program enables our marketplace partners to improve the security posture of their apps by leveraging the crowdsourced vulnerability discovery methods available through a bug bounty. Any of our marketplace vendors can apply to participate in the program, and apps that participate in the program are highlighted on the Atlassian marketplace
- **Mandatory security requirements** – Atlassian has defined a minimum set of baseline security requirements that are mandatory for all Marketplace cloud applications to adhere to. These are defined in our **Marketplace Partner Agreement**
- **The Security Self-Assessment Program** – this program is designed to increase overall levels of security awareness and security practices of our marketplace partners. Marketplace partners can apply to participate, and then complete an annual security self-assessment covering key security domains that Atlassian reviews. Partners who participate in this program are highlighted in the marketplace

More information about our approach to security in the marketplace is available via our **Atlassian Trust Center**.

Compliance and risk management

Our policy and risk management programs

Atlassian has a **Trust Management Program (TMP)** which is based on the ISO 27001 Information Security Management System Standard. This program takes our customer's security needs into consideration and arrives at a set of security requirements unique for Atlassian - taking into account controls listed across a range of international security standards.

We then consider whether those controls are contextually appropriate for our particular environment and company, and the best way to implement them. Our TMP has multiple pillars:

- **Our Policy Management Program (PMP) –** The PMP forms the basis of our TMP. It consists of a series of security policies covering the domains listed in both the ISO 27001 standard as well as the Cloud Security Alliance's Cloud Controls Matrix (CCM). The security policies we have created are made available internally to all of our teams to ensure they understand the bar they are expected to meet when it comes to security. The policies are updated annually and in particular whenever we observe new threats and risks that require modifications to our security approach. Excerpts of our technology policies are available **here**

- **Our Risk Management Program (RMP)** – We undertake on-going risk assessments to our environments and products in order to evaluate the current risks we face and ensure the controls we have in place effectively manage those risks. The nature of how these risk assessments are conducted will vary depending on the environment/ product being assessed – for example, in the case of our products, these will often be technical risk assessments or code reviews. However, we also consider and seek to uncover higher level business risks as well. We perform and undertake an annual risk assessment in support of our Enterprise Risk Management Program and implement projects to mitigate identified risks at least quarterly. For more information on our approach to Enterprise Risk Management, visit our **Atlassian Trust Center**

Our TMP includes weekly compliance health reviews and other meetings which are documented internally, to ensure it continues to operate effectively.

Compliance with laws, regulations and standards

Our security program has been developed and run in compliance with a number of industry standards. Complying with well-known industry standards is an integral part of our approach to security because we understand they provide independent assurance to our customers that Atlassian's security program meets a baseline of security controls.

Here are a few of the key standards that we comply with:

ISO 27001	The basis of ISO 27001 is the development and implementation of an Information Security Management System (ISMS), and then implementing and managing a suite of controls covered under 'ISO 27001: Annex A' through that ISMS. **View our ISO 27001 certificate**
ISO 27018	ISO/IEC 27018 is a code of practice which provides additional implementation guidance for applicable ISO/IEC 27002 controls for the protection of Personally Identifiable Information (PII) in cloud environments. **View our ISO 27018 certificate**

PCI DSS	When you pay with your credit card for Atlassian products or services you can rest assured that we handle the security of that transaction with appropriate attention. Atlassian is a PCI DSS compliant merchant. View the Attestation of Compliance (AoC) for **Jira, Confluence, Bitbucket and LearnDot**, **Trello and Statuspage**.
CSA CCM/STAR	The CSA Security, Trust & Assurance Registry (STAR) is a free, publicly accessible registry that documents the security controls provided by various cloud computing offerings. The CSA STAR Level 1 Questionnaire for Atlassian is available for download on the **Cloud Security Alliance's STAR Registry**.
SOC2 AND SOC3	These reports help our customers and their auditors understand the controls established to support operations and compliance at Atlassian. Atlassian has achieved SOC2 certifications for many of our products. **View our SOC2 and SOC3 certification reports**
GDPR	We appreciate that our customers have requirements under the Global Data Protection Regulation (GDPR) that are directly impacted by their use of Atlassian products and services, which is why we have devoted significant resources toward helping our customers fulfill their requirements under the GDPR. Learn more about our approach to GDPR compliance on our **Atlassian GDPR Compliance** page.
FEDRAMP	The Federal Risk and Authorization Management Program (FedRAMP) is a U.S. Federal government-wide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. View individual status on FedRAMP.Gov for the following Atlassian products; Trello

Further to what is listed above, a complete list of industry standards that we comply with is provided on our **Compliance Program page**.

Privacy at Atlassian

Atlassian has a comprehensive privacy program in place to ensure that we not only commit to meeting the highest bar for personal data privacy, but support our customers in meeting their data privacy obligations.

We have invested significant resources in maintaining compliance with current privacy requirements in jurisdictions across the world – the Global Data Protection Resolution (GDPR) and the California Consumer Protection Act (CCPA) being two examples. We have ensured Atlassian staff that access and process Atlassian customer personal data have been trained in handling that data and are bound to maintain the confidentiality and security of that data. We also hold any vendors that we engage that handle personal data to the same data management, security, and privacy practices that we hold ourselves and are subject to.

Where applicable, we institute appropriate international data transfer mechanisms by executing standard contractual clauses through our updated **data processing addendum**. We have made a number of data management and portability tools available to our customers as well, including:

- **Profile deletion tool**: We help customers **respond to user requests to delete personal information**, and we also help **end users with Atlassian accounts delete their personal information**
- **Import and export tools**: Customers may access, import, and export their Customer Data using Atlassian's tools. For more information on Atlassian Cloud data export see our **import and export documentation**

More information about our privacy program is available on our **Atlassian Trust Center**. You can also view our current privacy policy here.

Internal and external audit

We perform comprehensive security audits through well-known audit firms at least annually. Additional internal audits are performed in areas that are deemed 'high risk' and are reported to the audit committee. Audit outputs are all fed into a continuous improvement cycle which helps us keep sharpening the overall security program.

Law enforcement and government requests for data

As part of our commitment to earning and maintaining your trust, we publish an annual **Atlassian Transparency Report** with information about government requests for data (whether a request for user data or a request to remove content/suspend user accounts). Atlassian will scrutinize every request for legal validity, and if required to comply, we will respond as narrowly as possible to the specific request.

Atlassian's values underpin our approach to responding to law enforcement requests for customer data. To protect customers' data privacy and rights, we only provide customer information to law enforcement when we reasonably believe there's a legal requirement to do so and after comprehensive legal review. To obtain customer information from Atlassian, law enforcement officials must provide legal processes appropriate for the type of information sought, such as a subpoena, court order, or a warrant. We have detailed guidelines for handling law enforcement requests available at our **Atlassian Trust Center**.

Further questions and inquiries

While this paper has provided a broad overview of our approach to security, naturally given this is a complex area and Atlassian is doing a significant amount in this space, we haven't been able to cover everything in detail here.

If you need more information, visit our **Atlassian Trust Center**. You can also contact Atlassian's Trust Team, via our **support portal** if you still need further clarification on anything to do with Atlassian's Security or ask a question in our **Atlassian Trust and Security Community**.

Learn more at
atlassian.com/trust

ATLASSIAN