



Atlassian PTY Ltd.

Service Organization Controls (SOC) 3 Report

Report on Bitbucket Cloud

**Based on the Trust Services Principles and Criteria
for Security, Availability, and Confidentiality**

For the period November 1, 2017 through October 31, 2018



Management's Assertion Regarding the Effectiveness of Its Controls
Over the Bitbucket Cloud
Based on the Trust Services Principles and Criteria for
Security, Availability and Confidentiality

We, as management of, Atlassian Pty Ltd. ("Atlassian") are responsible for designing, implementing and maintaining effective controls over the Bitbucket Cloud system (System) to provide reasonable assurance that the commitments and system requirements related to the operation of the System are achieved.

There are inherent limitations in any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in Security controls, an entity may achieve reasonable, but not absolute, assurance that all security events are prevented and, for those that are not prevented, detected on a timely basis. Examples of inherent limitations in an entity's Security's controls include the following:

- Vulnerabilities in information technology components as a result of design by their manufacturer or developer
- Ineffective controls at a vendor or business partner
- Persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity

Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

We have performed an evaluation of the effectiveness of the controls over the system throughout the period November 1, 2017 to October 31, 2018, to achieve the commitments and system requirements related to the operation of the System using the criteria for the security, availability and confidentiality (Control Criteria) set forth in the AICPA's TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. Based on this evaluation, we assert that the controls were effective throughout the period November 1, 2017 to October 31, 2018 to provide reasonable assurance that:

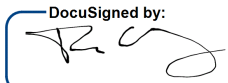
- the System was protected against unauthorized access, use, or modification to achieve Atlassian's commitments and system requirements
- the System was available for operation and use, to achieve Atlassian's commitments and system requirements
- the System information is collected, used, disclosed, and retained to achieve Atlassian's commitments and system requirements



based on the Control Criteria.

Our attached description of the boundaries of the Bitbucket Cloud identifies the aspects of the Bitbucket Cloud covered by our assertion.

Very truly yours,

DocuSigned by:

D9F75B69402F4F6...
Tom Kennedy
Chief Legal Officer



Ernst & Young LLP
303 Almaden Boulevard
San Jose, CA 95110

Tel: +1 408 947 5500
Fax: +1 408 947 5717
ey.com

Report of Independent Accountants

To the Management of Atlassian PTY Ltd.

Approach:

We have examined management's assertion that Atlassian PTY Ltd. ("Atlassian") maintained effective controls to provide reasonable assurance that:

- the Bitbucket Cloud System was protected against unauthorized access, use, or modification to achieve Atlassian's commitments and system requirements
- the Bitbucket Cloud System was available for operation and use to achieve Atlassian's commitments and system requirements
- the Bitbucket Cloud System information is collected, used, disclosed, and retained to achieve Atlassian's commitments and system requirements

during the period November 1, 2017 through October 31, 2018 based on the criteria for security, availability and confidentiality in the American Institute of Certified Public Accountants' TSP section 100, *2017 Trust Services Principles and Criteria for Security, Availability, Processing Integrity, Confidentiality, and Privacy*. This assertion is the responsibility of Atlassian's management. Our responsibility is to express an opinion based on our examination.

Our examination was conducted in accordance with attestation standards established by the American Institute of Certified Public Accountants. Those standards require that we plan and perform our examination to obtain reasonable assurance about whether management's assertion is fairly stated, in all material respects. An examination involves performing procedures to obtain evidence about management's assertion, which includes: (1) obtaining an understanding of Atlassian's relevant security, availability and confidentiality policies, processes and controls, (2) testing and evaluating the operating effectiveness of the controls, and (3) performing such other procedures as we considered necessary in the circumstances. The nature, timing, and extent of the procedures selected depend on our judgment, including an assessment of the risk of material misstatement, whether due to fraud or error. We believe that the evidence obtained during our examination is sufficient and appropriate to provide a reasonable basis for our opinion.

Our examination was not conducted for the purpose of evaluating Atlassian's cybersecurity risk management program. Accordingly, we do not express an opinion or any other form of assurance on its cybersecurity risk management program.



Inherent limitations:

There are inherent limitations in the effectiveness of any system of internal control, including the possibility of human error and the circumvention of controls. Because of inherent limitations in its internal control, those controls may provide reasonable, but not absolute, assurance that its commitments and system requirements related to security, availability and confidentiality are achieved.

Examples of inherent limitations of internal controls related to security include (a) vulnerabilities in information technology components as a result of design by their manufacturer or developer; (b) breakdown of internal control at a vendor or business partner; and (c) persistent attackers with the resources to use advanced technical means and sophisticated social engineering techniques specifically targeting the entity. Furthermore, projections of any evaluation of effectiveness to future periods are subject to the risk that controls may become inadequate because of changes in conditions or that the degree of compliance with the policies or procedures may deteriorate.

Opinion:

In our opinion, Atlassian's management's assertion referred to above is fairly stated, in all material respects, based on the aforementioned criteria for security, availability, and confidentiality.

Ernst & Young LLP

San Jose, California
December 28, 2018



Atlassian's Bitbucket Cloud Description of System Relevant to Security, Availability, and Confidentiality

Company Overview and Background

Atlassian was founded in 2002 by Scott Farquhar and Mike Cannon-Brookes and had their Initial Public Offering (IPO) in 2015. They have offices in San Francisco and Mountain View, California, Sydney, Australia, Manila, Philippines, Yokohama, Japan, Amsterdam, Netherlands, Austin, Texas and Bengaluru, India.

Atlassian's mission is to unleash the potential in every team. Their collaboration software helps teams organize, discuss and complete shared work. Teams of more than 65,000 staff, as well as large and small organizations use Atlassian's project tracking, content creation and sharing, real-time communication, and service management products to work better together and deliver quality results on time. Their products include Jira Software, Jira Service Desk, Confluence, Bitbucket, and Trello.

The system in-scope for this report is primarily the Bitbucket Cloud system and supporting IT infrastructure and business processes.

Overview of Products and Service

Bitbucket Cloud is a web application that allows individuals and organizations to store and collaborate on source code using the Git or Mercurial distributed version control systems. Bitbucket is one of several products offered by Atlassian and offers seamless integration with other products offered such as Jira and Confluence. Bitbucket also offers issue tracking, asset downloads, static site hosting, a wiki, Git Large File Support and automated build functionality. While these features and functions are available to customers, these are out of scope for the purpose of this report.

Infrastructure

Bitbucket Cloud's services and features are provided by a set of services running in the NTT datacenter in Ashburn, Virginia, with backup services on standby in the NTT datacenter in Santa Clara, California.

Separate application nodes handle web, SSH, HTTPS Git, and HTTPS Mercurial requests. A cluster of NetApp appliances provide persistent storage while PostgreSQL databases contain account and repository attributes and wiki data. Redis is used primarily as a data store for customers to gain insight on the recent activities for a given user or repository. Load balancers help ensure that incoming traffic is properly sorted by type and evenly distributed amongst application nodes. The load balancers, clusters, and Redis are out of scope for this report. Only the NetApp appliances, access to the postgresql database, and backups of customer data are in scope for this report.

Bitbucket Cloud's additional functionalities are hosted at Amazon Web Services ("AWS") including web hooks, Atlassian account and media services. These functionalities are out of scope for this report.

The processes and controls managed by the NTT datacenter and AWS are excluded from the scope of this report.

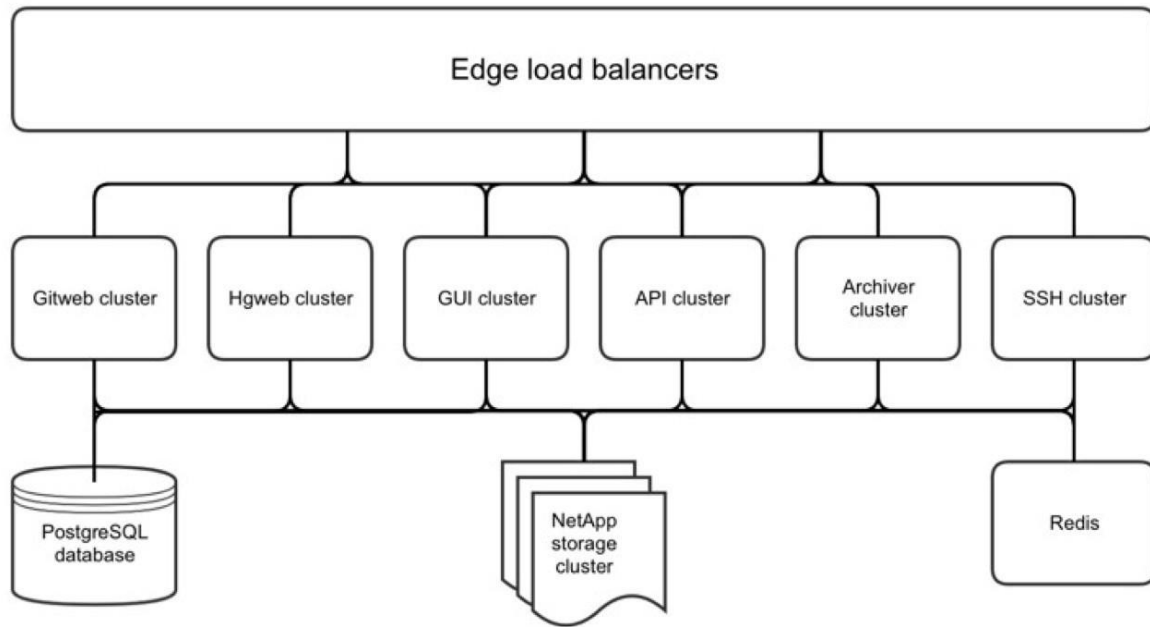


Figure 1: Architecture Diagram

Bitbucket Cloud's public network connectivity is maintained by Atlassian's Network Engineering team. Inbound packets route through Akamai, where engineers can mitigate denial-of-service attacks; outbound packets are routed through either NTT or Level 3, as appropriate for the destination.

User-initiated connections are available using IPv4 or IPv6 addresses and are available on TCP ports 22 (SSH), 80 (HTTP) or 443 (HTTPS). A special hostname, altssh.Bitbucket.org, provides SSH connectivity over port 443 for users whose networks restrict outbound connections to port 22.

All unencrypted HTTP connections are redirected to an equivalent HTTPS endpoint. Bitbucket Cloud also publishes a Strict-Transport-Security header for user agents to redirect internally to HTTPS. All inbound connections are then load-balanced, based on factors such as traffic type, host header, request path and user agent.

User requests may also be redirected to Amazon S3 for user downloads, Amazon Cloudfront for static assets in the user interface, or to a service managed by Atlassian's Media Services team for Git LFS objects or Mercurial clone bundles. These are out of scope for this report.

Bitbucket Cloud initiated connections are currently limited to notification mail to user-configured webhooks. Mail is encrypted in transit to third-party providers. Webhooks may be unencrypted at user request, or they may be sent to HTTPS servers with unverifiable

certificates at user request, though both of these cases are discouraged. Both mail and webhooks originate from consistent IP addresses within Atlassian-managed space.

Within the datacenter, Bitbucket Cloud systems use logical binding on multiple network interfaces to provide redundancy against hardware failures. A dedicated VLAN connects application nodes to repository storage; other VLANs connect application nodes, load balancers, database servers and other resources to each other. All internal resources are isolated from the Internet by firewall.

Servers

Application nodes are stateless and clustered based on their primary service. Cluster types include, but are not limited to, the user interface; API; Git or Mercurial repository operations over SSH; Git or Mercurial repository operations over HTTP; asynchronous tasks.

Physical server configurations are managed using various tools including Puppet.

Database

Bitbucket Cloud's customer data is stored in PostgreSQL and NetApp filers (database). PostgreSQL contains account attributes, permissions, issues, pull requests and wiki data while NetApp contains customer repository data. All primary database servers reside in the physical data centers with replication nodes and backups being stored in both physical datacenters as well as AWS.

Software

In-scope production servers run on CentOS servers. The following software and tools support the Bitbucket Cloud control environment:

- www.atlassian.com (WAC) - Where customers order products, and the shopping cart is hosted
- my.atlassian.com (MAC) - Where customers manage their current products
- Centrify - Single sign on service used for Atlassian
- Jira - Ticketing system used for incident management, user access provisioning, and change management process.
- Bamboo - Bamboo is Atlassian's developed continuous integration tool used to perform automated testing and deployment activities
- Bitbucket Server - Atlassian's developed source code and development projects tool
- Puppet - open-source software configuration management tool
- AWS Glacier - data archiving and long-term backup storage service
- NetApp - database for customer data
- Workday - Human Resource (HR) system
- Impraise - performance feedback tool
- SmartRecruiters - Hiring tool (used between the period from November 1, 2017 to June 30, 2018)

- Lever - Hiring tool (effective as of July 1, 2018)
- Datadog - monitoring tool
- StatsD - monitoring tool
- Stride - Messaging tool for alerting on availability
- Pollinator - monitoring tool

NTT and AWS Glacier are managed by a third-party vendor; Atlassian performs a review of the SOC 2 reports as discussed below. The evaluation of the SOC report is performed and reviewed by the Risk and Compliance Team, which includes an assessment of the complementary user entity controls, subservice organizations, and mapping of the controls to key risks. If there are exceptions, Atlassian evaluates the severity and impact of the exceptions, and if needed, follows up with the individual vendor.

Datadog, Pollinator, StatsD, Workday, Centrify, Impraise, Lever, and SmartRecruiters are also managed by a third party vendors, however, customer data is not stored in these applications. These are supporting and monitoring tools, and are only applicable to support certain controls and criteria.

WAC, MAC, Jira, Bamboo, Bitbucket Server, NetApp and Puppet are Atlassian managed tools and are in-scope in the controls as discussed below.

Vendor agreements, including any security, availability, and confidentiality commitments, are reviewed by appropriate Atlassian management during the procurement process. Prior to services rendered, vendors are required to sign the vendor agreements.

Data

Customers sign up to Bitbucket Cloud using the website and, upon accepting the terms and conditions, the customer account is created in PostgreSQL. Once a repository is created in Bitbucket Cloud, it creates a specific folder in the Netapp file server (database). The path is automatically assigned by Bitbucket Cloud and creates the volume where the repository is stored and the volume contains a number of directories. The directory contains the specific repository number to which the customer is routed. Bitbucket isolates each customer's data per volume and directory in NetApp. The path can be seen by the customer in their Bitbucket website.

Organizational Structure

Atlassian's organizational structure is managed by a committee consisting of Human Resources, Financial Planning and Analysis, as well as Senior Management and Leadership (including the Co-Founders).

The following organizational chart identifies the teams responsible for human resources, strategic planning, education/training, legal matters, business growth/modeling, finance, accounting, and technology operations:

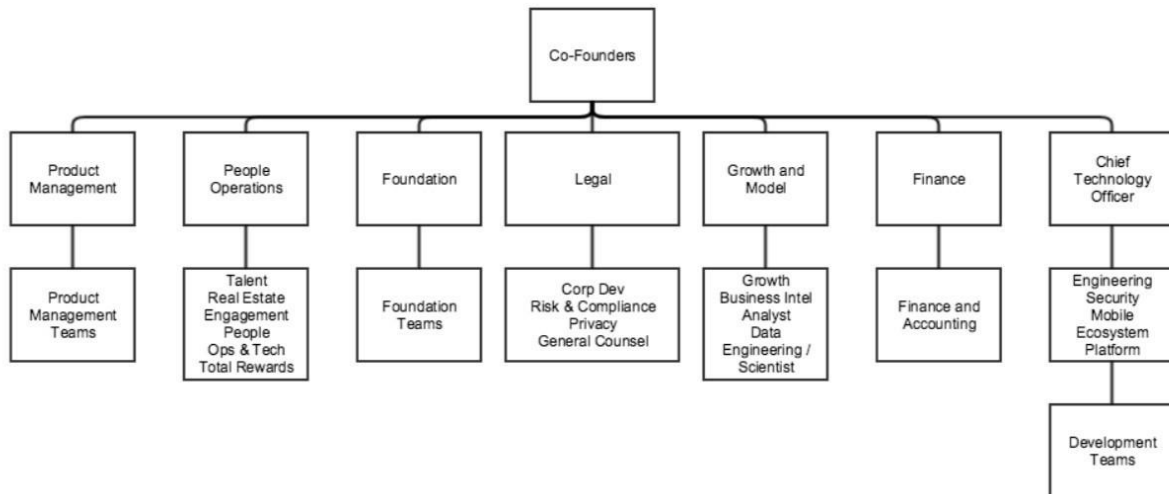


Figure 2: Atlassian's Organizational Chart

The organizational charts are reviewed by appropriate Atlassian management and updated semi-annually. Additionally, organizational charts are automatically updated based on employee action notices and is available to all Atlassian employees via Atlassian's HR system, Workday.

The Co-Founders are responsible for directing all designated areas including Product Management, People Operations, Foundation, Legal, Growth and Modeling, and the Technology teams. All teams have full responsibility over key operations within Atlassian:

- Product Management - focuses on validating the demands of customers, provides insight and guidance around minimum viable product and user experience.
- People Operations (in partnership with the people leaders) - focuses on determining the right talent strategy to deliver against the needs of Atlassian. People team is responsible for talent acquisition and learning, total rewards and technology, and workplace experiences.
- Foundation - Exists to harness the resources of Atlassian to champion organizations who believe that education is the key to eliminate disadvantage. This is accomplished by improving educational outcomes in developing countries, increasing skill-based volunteering and leveraging Atlassian's products.
- Legal - responsible for matters related to corporate development, privacy, general counsel operations, public relations, risk and compliance.
- Growth and Model - responsible for monitoring business trends, analytics, data engineering and data science.
- Finance - responsible for handling finance and accounting.
- Chief Technology Officer (Technology Operations) - oversees Engineering, Security, Mobile, Ecosystem and Platform.
- Head of Engineering, Software Teams oversees all operations for the products.
- Development Manager:

- Drives and improves product quality and innovation, team productivity, manages simultaneous projects in an agile fashion, customer satisfaction and product supportability.
- Coordinate multiple streams of software development, involving multiple teams, geographic distribution and indirect reports.
- Collaborate with Product Management by contributing to roadmaps, setting priorities, and providing estimates.
- Collaborate with Customer Support to help ensure customer success and drive quality improvements.
- Promote, define, refine and enforce best practices and process improvements that fit Atlassian's agile methodology.
- Provide visibility through metrics and project status reporting.
- Set objectives for people and teams and holds them accountable.
- Work with Recruitment to attract and hire outstanding individuals to create high performing balanced teams.
- Lead by example and practice an inclusive management style.