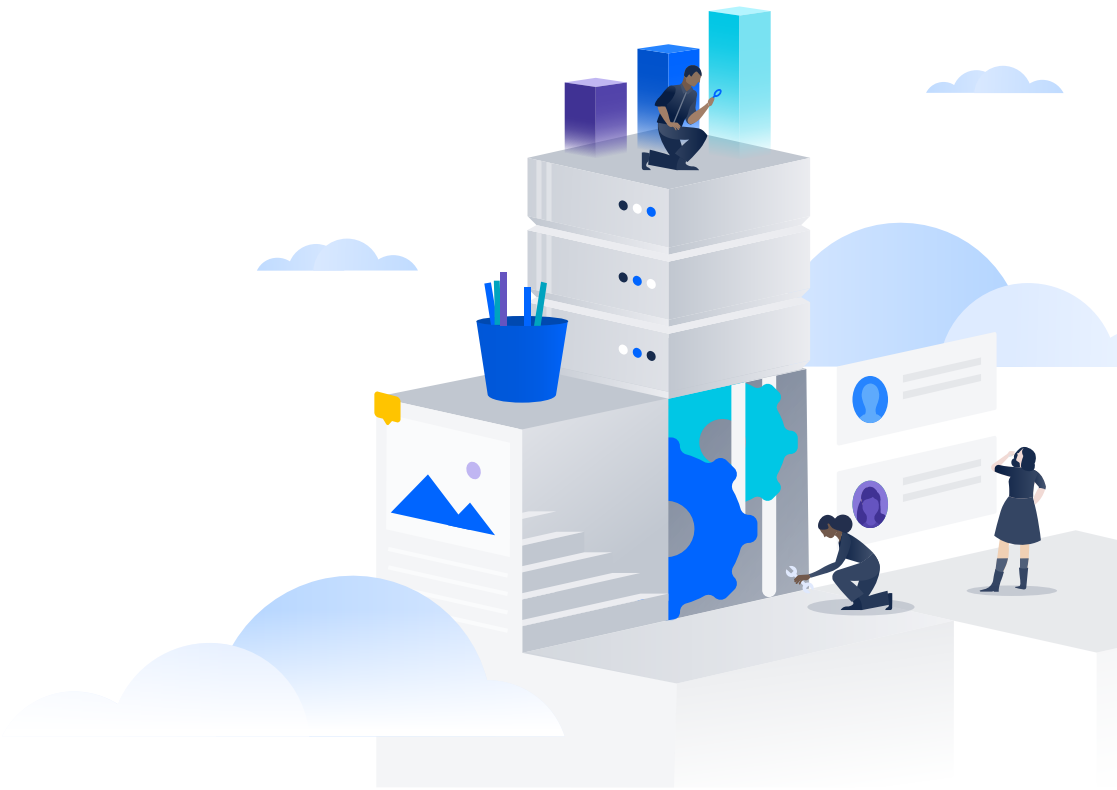
ATLASSIAN

How Atlassian cloud achieves enterprise-grade security and compliance

Table of contents



In today's quickly evolving digital landscape, cloud has unlocked unlimited scale and the ability to collaborate across remote, distributed teams. However, rise in devices and channels to access cloud applications have also increased the risk of data breaches and the need to ensure compliance with evolving data privacy obligations across the globe. At Atlassian, we are fully committed to helping our 190,000+ customers enjoy all of the benefits of scaling in the cloud while meeting the highest bar for security and data privacy. This paper explains our five-pronged approach to making Atlassian cloud products enterprise-ready from a security and compliance standpoint.

Securing our cloud architecture with a ZeroTrust approach

Our approach to cloud security starts at the network architecture level. We implement controls at each layer of our cloud environment and have a ZeroTrust security approach for access to our corporate network, systems and services.

End-to-end data security with advanced controls for residency and encryption

We understand just how important it is to keep customer data safe so we have numerous safeguards in place to offer complete peace of mind. All customer data is hosted on the industry-leading Amazon Web Services platform with multi-level redundancy. For additional control, we offer data residency - the ability to pin product data to certain geographic regions. We also encrypt all customer data, both at rest as well as in transit and continue to invest in advanced controls such as bring-your-own-key encryption (BYOK).

Continuous investment in complying with global data privacy obligations

For starters; we incorporate data privacy by design into all our products. Additionally, our Risk and Compliance team continuously works on your behalf to ensure Atlassian cloud products comply with global standards including SOC, ISO, GDPR and industry-specific regulations.

Built-in controls for identity and access management

Our built-in controls allow IT administrators to enforce enterprise-grade authentication protocols including SAML single sign-on, multi-factor authentication and more. Admins can also customize authentication policies for different subsets of users, automate user provisioning and deprovisioning to reduce the risk of unauthorized access, and enforce security controls for mobile usage with support for mobile device and app management (MDM / MAM).

Proactive threat monitoring and protection

Atlassian offers comprehensive security testing and vulnerability management programs to prevent threats. Additionally, with Atlassian Access, customers get organization audit log that offers comprehensive insight into admin activity such as changes to users, groups, permissions in the organization to help triage suspicious activities.

Let's examine each of the above security elements in detail.

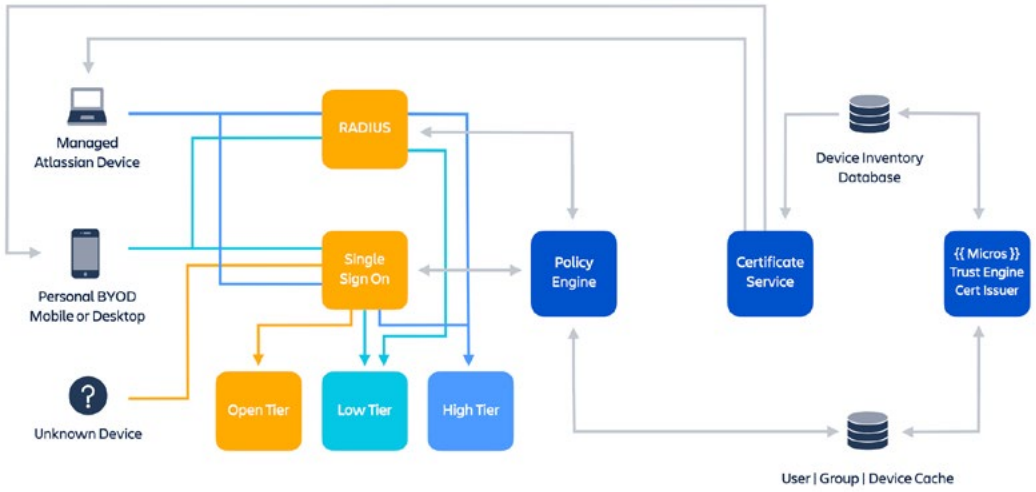
Secure cloud architecture

At Atlassian, we take **a layered approach** to security by dividing our cloud infrastructure into zones, environments, and services, and implementing controls at each of these layers. We limit the staff, customer data, continuous integration and deployment (CI/CD), and demilitarized zone (DMZ) network traffic that can flow through each zone. We also use authentication allowlists to control and explicitly authorize which services can interact with one another.

ZeroTrust approach

In terms of network access, we take a more granular approach using a system that we call **ZeroTrust** - never trust, always verify. This takes into account not only authentication credentials but also resource confidentiality when determining how a resource can be accessed on our networks. Depending on a resource's sensitivity, we make it available at an open tier, low tier, or high tier of security.

- Open-tier resources can be accessed through successful user authentication into Atlassian's network.
- Low-tier resources require both user authentication and the use of a trusted corporate device (whether Atlassian-issued or enrolled in our mobile device management program).
- High-tier resources require user authentication and can only be accessed on Atlassian-issued corporate devices.



Disaster recovery and business continuity

Finally, we know that disruptions can happen – so we actively plan for them by building disaster recovery (DR) and business continuity (BC) plans into our processes. To meet our DR and BC needs, we build redundancy measures into all of our products, and our site reliability engineers regularly test those redundancies to identify any gaps. Every Atlassian team works with a disaster recovery champion who ensures that DR is built into all projects produced by the team, and we regularly carry out disaster recovery tests to improve our processes and technology.

End-to-end data security

According to IBM, the average company affected by a data breach will spend $3.86 million per breach in detection and escalation, lost business, notification efforts, and ex-post response. The idea is enough to make any security leader's skin crawl. Hence data security lies at the heart of the Atlassian cloud products. This includes keeping customer data securely stored, encrypted, and private, and ensuring customers retain control over their data to the fullest extent possible.

Industry-leading hosting infrastructure

We host Atlassian products and data with Amazon Web Services (AWS), an industry-leading cloud hosting provider. Within AWS's network, we host customer data within **multiple, geographically diverse regions**, including cities across the east and west coast of the United States, the European Union, and the Asia Pacific region. Data is always replicated to other geographically isolated data centers (known as availability zones) so that in the event of the failure of one availability zone, our customers remain unaffected.

> By offloading infrastructure and the maintenance required for it, **CHG Healthcare** have saved almost $120,000 so far and up to 30 hours per week, which they can dedicate to innovation instead of administration. Plus, now that Atlassian handles patching and security updates, CHG never has to worry about vulnerabilities.

Data residency controls

With the rollout of geographic data regulations, such as the European Union's General Data Protection Regulation (GDPR), we've made it easier than ever for Atlassian clients to control where their data is stored. Using our **data residency feature** (available in all our paid plans), IT administrators can now pin user-generated product data – such as Confluence pages and Jira tickets or comments – to certain data realms.

Our data residency options allow greater control for our customers. For example, if only a certain portion of a company's data needs to be pinned to a region, IT administrators can choose to isolate that data in a **unique product instance** in order to ensure data isolation and compliance.

At the moment, we support data residency in the European Union and the United States, but we have plans to further **expand our supported regions** to Australia, the United Kingdom, Canada, and Japan by mid-2022. And as part of our commitment to continually improving our product, we plan to support **data residency for third-party apps** by the end of 2021.

In order to meet performance requirements for users located around the world, user account information data is replicated globally. Hence data residency currently does not apply to user account data. Neither GDPR nor Schrems II say data residency is required. Instead, they focus on the need to provide European data adequate safeguards when it leaves Europe. Hence, Atlassian adheres to Standard Contractual Clauses to ensure that all user data is adequately protected as required under the General Data Protection Regulation. For more information on where and how we store user data, see the **Atlassian Trust center**.

Encrypting data in transit and at rest

When it comes to cloud security, **encrypting sensitive data** should be table stakes for anyone in the space. As part of our commitment to layering security throughout our cloud architecture, we provide data encryption at rest for all customer data and attachments in Jira Software Cloud, Jira Service Desk Cloud, Jira Work Management, Confluence Cloud, Statuspage, Opsgenie, and Trello.

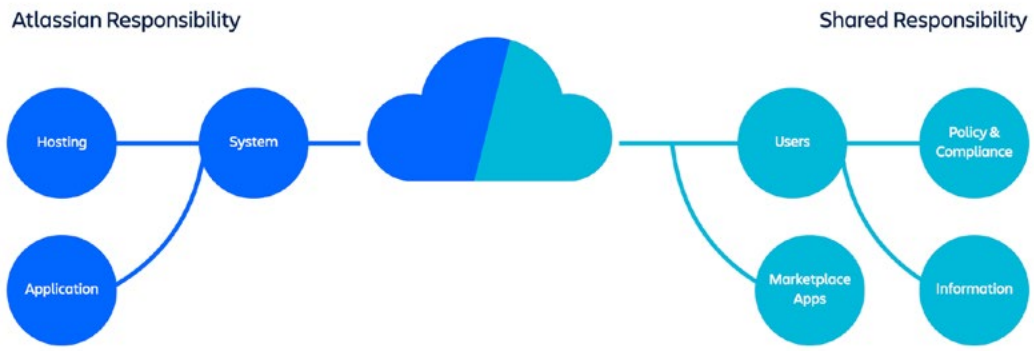
Any inactive data held in servers is encrypted at rest using industry-standard Advanced Encryption Standard 256. Any customer data that's in transit over public networks is encrypted using Transport Layer Security 1.2+ with Perfect Forward Secrecy, which ensures data is encrypted using strong ciphers and key-lengths. These measures help protect data from any unauthorized disclosure or modification while in transit.

Bring Your Own Key (BYOK) encryption coming soon to Atlassian Cloud Enterprise

For enterprises looking for additional control, we plan to roll out **bring your own key (BYOK) encryption** feature for Jira and Confluence by early 2023. This will allow companies to manage their own cryptographic keys through Amazon Web Services' Key Management Service. In addition to being able to grant or revoke access, BYOK also offers compensating control to meet compliance needs for data security.

Collaborating to keep data secure

Atlassian fully assumes the responsibility for the security, performance, and availability of our systems, but we need customers' full participation in order to keep all of your data safe.



There are **four shared responsibilities** that users should take note of:

Policy and compliance

We've publicly shared our **privacy policy** and **the multiple regulations** we are compliant with. However, it is ultimately up to the user to ensure that our system meets your business and compliance needs.

Users

Our products are designed to enable both open collaboration and privacy as needed. Users should ensure that they are granting employees and external users the appropriate permissions to their Atlassian apps and data.

Information

Any content that you store within Confluence Cloud, Jira Cloud, Trello, and Bitbucket Cloud will be available to any users and apps with the appropriate permissions. Make sure that your Atlassian products and instances have been set up to reflect the information accessibility required by your content.

Marketplace apps

We independently verify the developers of Atlassian Marketplace third-party apps and **regularly monitor apps for vulnerabilities**. And, with **Forge**, we now offer a cloud platform that allows third-party developers to build enterprise-ready apps with the same best-in-class security that Atlassian offers for its products. However, it is also up to you to assess any third-party services you choose to work with since you will be granting those apps access to information stored in your Atlassian products.

Compliance with global data privacy obligations

By choosing to use a cloud platform like Atlassian Cloud Enterprise, IT administrators can offload the task of monitoring and ensuring compliance across their tech stack. At Atlassian, we aim to remove the stress of ensuring compliance from your shoulders – both now and in the future.

Privacy program

Our privacy program is designed to offer customers the highest standards of protection. For us, that means going beyond what is required by law and building privacy by design into everything we do.

We design our cloud products in line with widely accepted privacy standards and certifications, and Atlassian staff that handle customer data are regularly trained on security and confidentiality protocols. We aim to provide Atlassian customers with confidence through control. Organization admins within customer teams can easily manage end user profiles and even **facilitate the account deletion** of their managed users from the admin console. This deletes their personal data from all organizations and sites used to access Jira Cloud, Confluence Cloud, Bitbucket Cloud and Trello. Unmanaged end users may also request that their personal data be deleted by **initiating an account deletion request**.

At the end of each year, we also publish **our annual Transparency Report**, openly sharing information on the government requests we received that year and our responses to those requests. Atlassian is **transparent** about government requests for user data or removal of content or suspension of user accounts. We follow **policies and procedures** for responding to any government requests. To obtain Customer Information from Atlassian, law enforcement officials must follow legal process appropriate for the type of information sought, such as a subpoena, court order, or a warrant. You can find more information on our **Trust Center.**

CURRENT CERTIFICATIONS

We understand that our customers have diverse compliance needs, which is why we've developed our products in compliance **with multiple industry-leading standards and regulations**. Currently, Atlassian products comply with:

System and Organization Controls (SOC) 2, SOC 3

ISO/IEC 27001, ISO/IEC 27018

Payment Card Industries Data Security Standard (PCI DSS)

The Voluntary Product Accessibility Template (VPAT 508)

GDPR

Commitment to GDPR

Over the years, we've built our cloud products in accordance with many security and privacy standards that meet the requirements of the GDPR. We've always been committed to leading the way in terms of data privacy and security, and as part of that commitment, we've made sure our products abide by GDPR standards.

International data transfers

In light of the most recent Schrems II decision, we currently provide a pre-signed **Data Processing Addendum** (DPA) that includes a full copy of the Standard Contractual Clauses (SCCs) and serves as a valid mechanism for lawful transfer of personal data to Atlassian cloud products outside of the European Economic Area. This addendum contains specific provisions to assist customers in their compliance with the GDPR. Additionally, in accordance with **GDPR guidance**, we continue to invest in advanced encryption features such as BYOK to protect personal data.

Individual privacy rights and consent

In order to comply with GDPR regulations around individuals' right to erasure, we also make it easy for administrators to delete users' personal data from Atlassian cloud products. Both managed and unmanaged end users can request that their personal data be deleted, and organization admins can easily **facilitate account deletion** through Atlassian's admin portal.

Choice and consent

Finally, to ensure we're offering EU end users transparency and choice around how we use their information, we surface consents for cookies and marketing messages at any collection points. This allows users to understand exactly how we're collecting and using their information, and gives them a choice in how to share it with us.

Customer data and third parties

Atlassian works with third party sub-contractors to provide website, application development, hosting, maintenance, back-up, storage, virtual infrastructure, payment processing, analysis and other services.

These service providers may have access to or process PII for the purpose of providing those services for us. Atlassian discloses to its relevant customers any use of sub-contractors whom may process their PII, via notification before processing occurs. An external facing list of sub-contractors Atlassian works with is provided on the **Atlassian Subprocessors** page. Visitors are invited to subscribe to an RSS feed to be notified when we add new Atlassian Subprocessors.

Compliance in the works

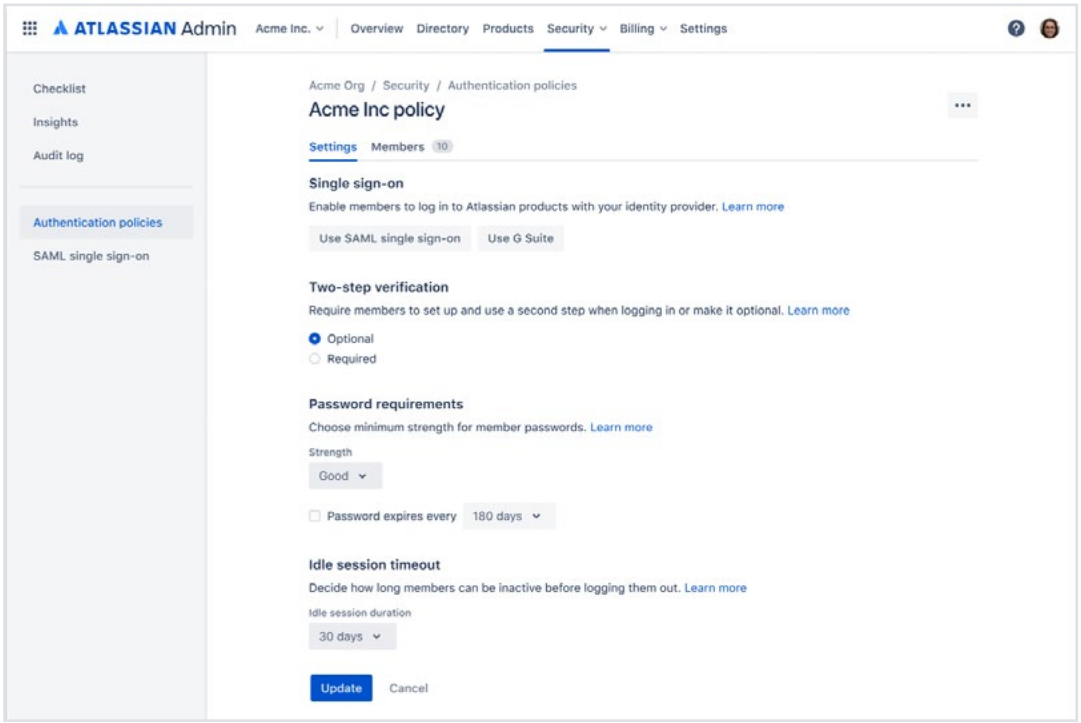
To better serve our customers in regulated industries, Atlassian continues to invest in meeting industry-specific compliance needs. By mid-2022, Atlassian Cloud Enterprise is expected to be in compliance with **financial services industry regulations** in the United States, Germany (Federal Financial Supervisory Authority or BaFin), and Australia (Australian Prudential Regulation Authority). For healthcare companies in the United States, we aim to comply with the **Health Insurance Portability and Accountability Act (HIPAA)** for Jira Software Cloud and Confluence Cloud by mid-2022.

Built-in Identity and Access Management

Even if your organization has complied with industry regulations and ensured that all customer data is encrypted, your enterprise's security is only as strong as your weakest employee. According to Kaspersky, 52 percent of enterprise data breaches in 2019 were caused by employee misuse of IT resources. For that reason, we've provided your administrators with an extensive set of built-in controls to ensure secure access organization-wide while using our cloud products.

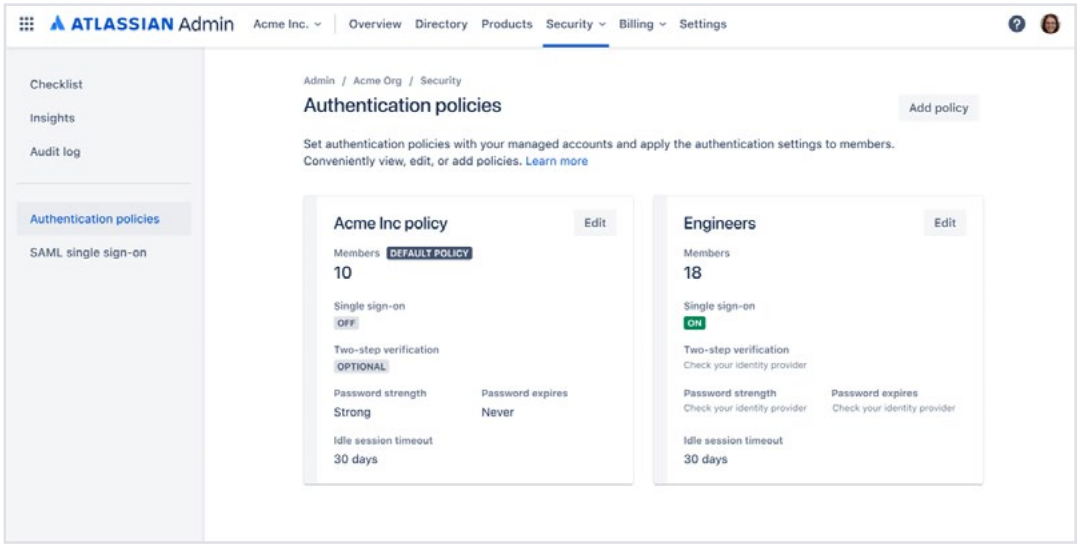
Enterprise-grade authentication protocols

Atlassian allows enterprises to limit their security risks by implementing enterprise-grade authentication protocols across their Atlassian products. Using Atlassian Access, our security and administration hub that is included with our Cloud Enterprise plan for no additional cost, admins can set up SAML SSO using their enterprise's existing identity provider, allowing employees to access multiple Atlassian products and instances using just one set of secure credentials. Admins can also enforce two-step authentication making users enter a 6-digit code sent to their phone when logging in, for an additional layer of security. Additional controls include requiring a minimum password strength for users, forcing passwords to expire after a set amount of time, and forcing idle sessions to automatically log users out after a certain duration.



Customizable authentication policies

Rather than a one-size-fits-all approach, administrators have the flexibility to customize authentication policies as needed for different subsets of users. For instance, they can set up a default password policy for all users but make multi-factor authentication mandatory for a subset of users accessing a product instance with highly sensitive data.



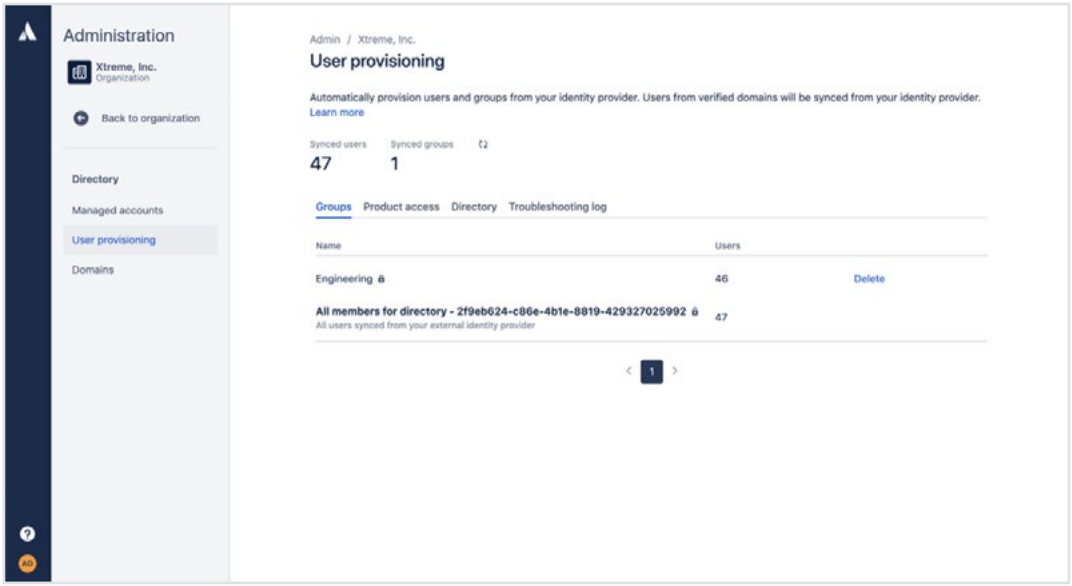
Mobile device and app management

With rise in remote work practices and bring-your-own-device (BYOD), many users access Atlassian products via mobile apps. To prevent data leaks or unauthorized access for mobile apps, administrators can now enforce specific security protocols – such as restricting copy and paste, blocking screenshots, or requiring FaceID, TouchID, or biometric authentication when logging in. Atlassian currently supports built-in integration with leading Mobile device management (MDM) software to enforce security protocols for Jira product family, Confluence and Trello mobile apps used on company-managed devices. By July 2021 we plan to extend support for Mobile App Management that will allow administrators to configure mobile security policies via the **organization admin console** for both managed devices and BYOD.

Automate user provisioning and de-provisioning

According to **Osterman Research**, a full 89 percent of former employees are still able to access at least one application from their former employer after they have left the job. Nearly a third of those former employees have used their ongoing access to view company information, and one in 16 have shared that information externally. For a large enterprise, it isn't surprising that some employee decommissioning may fall through the cracks, but it remains an important part of ensuring cloud security.

To solve this problem, Atlassian Access offers the ability to automate the user provisioning and de-provisioning process. Atlassian Access can be synced to an enterprise's **user directory** – either through our existing integrations to leading identity providers or through our System for Cross-domain Identity Management (SCIM) API for custom integrations – so that users are automatically granted access when they join the team. Depending on the group an employee is added to in your user directory (whether engineering, HR, or marketing), they will automatically be granted access to the Atlassian toolset required by their team. If they switch teams, their permissions will change. If they leave the company, their access will be revoked altogether.



How Canva has leveraged Atlassian's security features to fit its needs

As design platform **Canva** has scaled to a workforce of over 1,000 employees worldwide, it has relied on Atlassian Cloud features to ensure security across its cloud apps while still providing employees with the flexibility they need. Across the organization, employees rely on both Jira Software and Confluence to get their work done, and Atlassian Access' features have allowed Canva to easily restrict access to different product instances (such as the HR team's instance of Jira Service Management) and manage employees' security settings.

"Who can view HR information is heavily controlled, and there's a high level of security measures in place too," says Jeff Lai, Canva's Internal Infrastructure expert. "It's only because of those strict features that we felt comfortable putting this kind of information in Jira Service Management."

Canva also uses Atlassian Access' automated user provisioning and de-provisioning feature to easily grant new employees access to Canva's systems and documents. Canva uses external identity provider Okta to sync data with Access, and new employees are given permission to view a restricted amount of Canva's content before their first day. Using Access' SSO and forced two-step verification, external contractors can also access a limited set of Canva's systems.

"They aren't able to see anything but the documents we send them, because access is restricted through user group access mapping," says Lai. "Everyone across the organization also has access to the edit history, so that's another layer of security to make sure no one is doing anything dodgy to the documents."

Proactive threat monitoring and prevention

Even with stringent security measures in place, threats happen – which is why we've taken a multi-faceted and constantly evolving approach to threat prevention and vulnerability management at Atlassian. We use both automated and manual processes to find, monitor, and fix vulnerabilities across all our cloud products, and we make sure to equip our customers' IT teams with similar tools.

Bug bounty program

Our **bug bounty program** encourages over 60,000 cybersecurity researchers to ethically test our products and flag any vulnerabilities they find. Once a vulnerability has been logged, we create a ticket for it and assign it to the system owner or engineering team responsible for the product.

Consistent product testing

As part of our Continuous Integration / Continuous Deployment (CI/CD) pipeline, engineers must run through a full container security scanning process for any containers deployed into our development, staging, or production environments.

If any changes are being made to existing code, our engineers use a "Peer Review, Green Build" process to ensure that the changes won't cause any issues. As part of this process, all changes need to be reviewed by at least one peer before that code change is shipped.

Since many of our products also rely on open-source libraries, we use a combination of open-source, internally built, and commercial tools to automatically scan and identify any dependencies within said libraries that might be linked to security vulnerabilities.

Proactive security detection

With cybersecurity threats constantly evolving, we've made the decision to run proactive, scheduled searches for any malicious activity using our Security Incident and Event Management platform. Our security intelligence team regularly runs searches – or, as we call them, "detections" – for any activities targeting Atlassian or its customers.

Any threats discovered are logged, investigated, and used to improve our threat detections in the future. Our security intelligence team is constantly creating new detections to better hunt down new and existing threats, which helps us better understand the threat landscape today and what it will look like in the future.

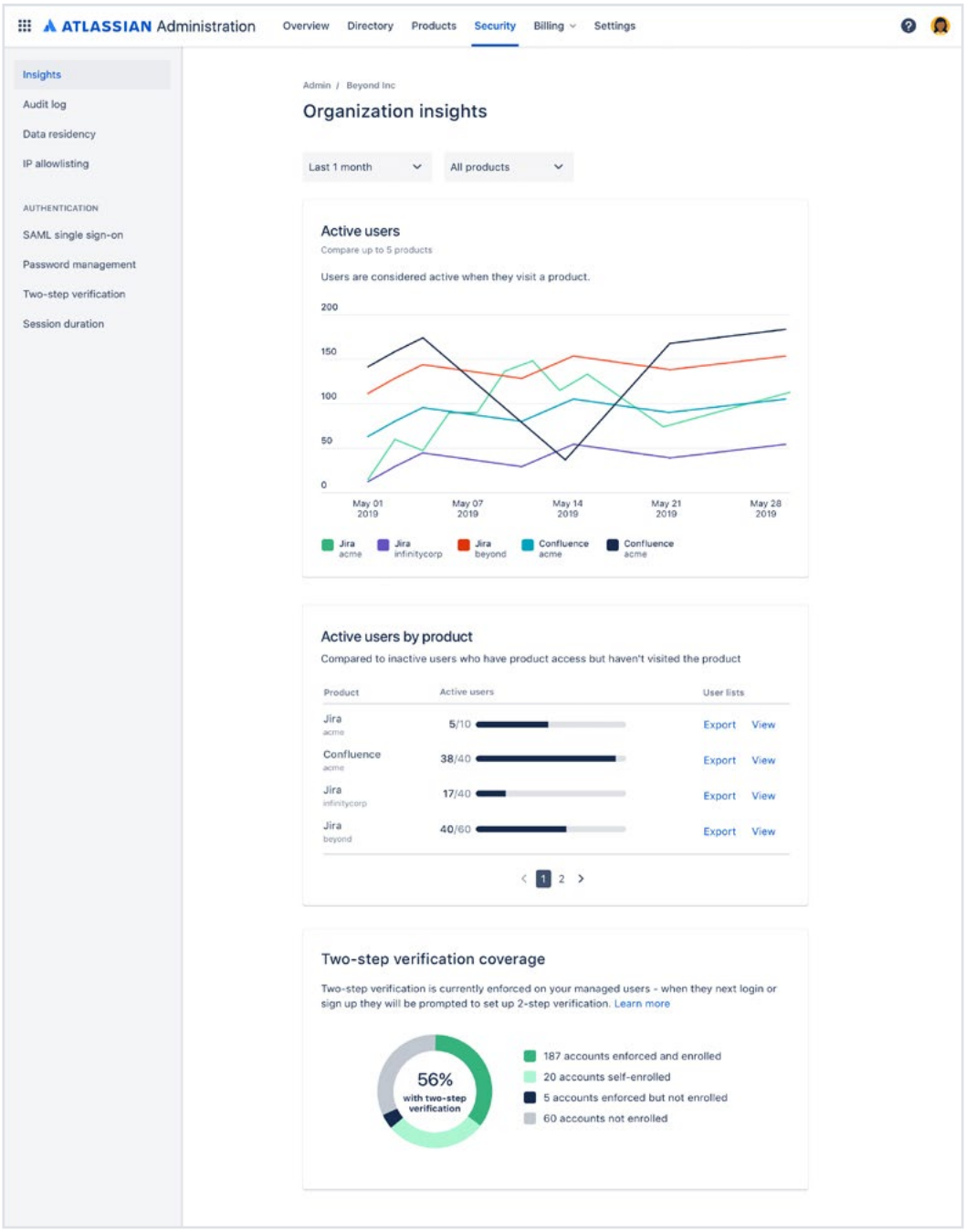
Security insights for admins

Just as we believe in proactively monitoring our systems for threats and vulnerabilities, we want to empower our customers to do the same – which is why we've made it easy for admins to track potential security issues across their Atlassian products.

Atlassian Access' **organization audit log** functions as a comprehensive log of any admin activity that occurs within your Atlassian cloud organization. Organization admins can track exactly which site admins have access to which product instances, along with when they were granted that access. In the event of data loss – such as the loss of proprietary data or confidential information – admins can restrict user access as needed and view records of users' activity in order to identify any suspicious activity.

> We have a lot of highly sensitive information around our IP... and we protect those things. It's important for our Chief Information Security Officer's office to know who has access to it and what they can do with it. Atlassian Access makes sure the right people have access to the right things, and the wrong people do not have access to the wrong things.
>
> **JIM TOMPKINS**
>
> **Program Manager, Rockwell Automation, Atlassian Enterprise customer**

Also available via Atlassian Access, our **organization insights tool** allows admins to get a bird's-eye view of users' security posture across Atlassian products. Using organization insights, admins can track just how many managed users have SAML SSO or two-step verification enabled on their accounts. They can also view a product's daily and monthly active users, helping them better understand which users actually require access and permissions.



Scale securely in the cloud with Atlassian

At Atlassian, we've made security the foundation of our cloud products, and secure practices and processes are built into the fabric of our business. **Atlassian Cloud Enterprise** provides a proven solution for enterprises that require a safe, compliant, and privacy-driven platform to help them scale, offering:

- Support for data residency
- Encryption in transit and at rest
- Compliance with industry-leading regulations including SOC, ISO, GDPR and more
- Included at no additional cost all security features of **Atlassian Access** including SAML SSO, enforced two-step verification, custom authentication policies, automated user provisioning and de-provisioning, organization audit logs, organization insights and more
- 30-minute SLA for critical security issues
- 24/7 phone support with a dedicated senior team

If you have specific questions on how we can offer your enterprise increased security as you scale in the cloud, please don't hesitate to

Contact us

For additional resources see

- **Atlassian Security Practices**
- **Atlassian Trust Center**
- **Security and Compliance Cloud Roadmap**

ATLASSIAN