ATLASSIAN

How to bolster your enterprise cloud security

Keep your company safe with five proven cloud security measures from Atlassian customers

Table of contents

Business operations are almost entirely digital now, so it's no surprise that more and more organizations are embracing the cloud. According to **Flexera's 2021 State of the Cloud Report**, 90% of companies anticipate their cloud usage to surpass previous plans because of the COVID-19 pandemic – and 36% of businesses are investing over $12 million in cloud spending annually.

Cloud technology is known for being secure. In a TechValidate survey of 311 Atlassian customers, "92% of surveyed IT organizations said that security is better or equal on the cloud."

These respondents are right – but that doesn't mean there aren't ways to enhance cloud technology and make it even more secure. Security threats are constantly evolving, so it's best to be prepared and stay on top of cybersecurity risks to combat them.

92% of surveyed IT organizations said that security is better or equal on the cloud.

Security threats may still creep in via shadow IT, outdated software permissions, poor password hygiene, and other factors. But the good news? There are measures you can take to keep your company secure on the cloud. In fact, enterprises just like yours have adopted these cloud security measures:

- **Automate the user lifecycle management process**
- **Implement SAML single sign-on for stronger password hygiene**
- **Enforce two-step verification to prevent account breaches**
- **Check for shadow IT to eliminate unauthorized software usage**
- **Centralize admin control to manage cloud security**

Learn how you can implement the same security practices to enhance your own cloud technology.

1: Automate the user lifecycle management process

As employees join or leave your company, it's up to your admins to grant or revoke software access as needed. If they complete this process manually, they run the risk of human error – especially as your company grows.

Admins will find it challenging to keep up with provisioning and de-provisioning so many users at once. If admins miss removing software permissions for any departing employees, unauthorized users will have access to company tools and data, and accounts will be left vulnerable to hackers – opening up your company to potential security breaches.

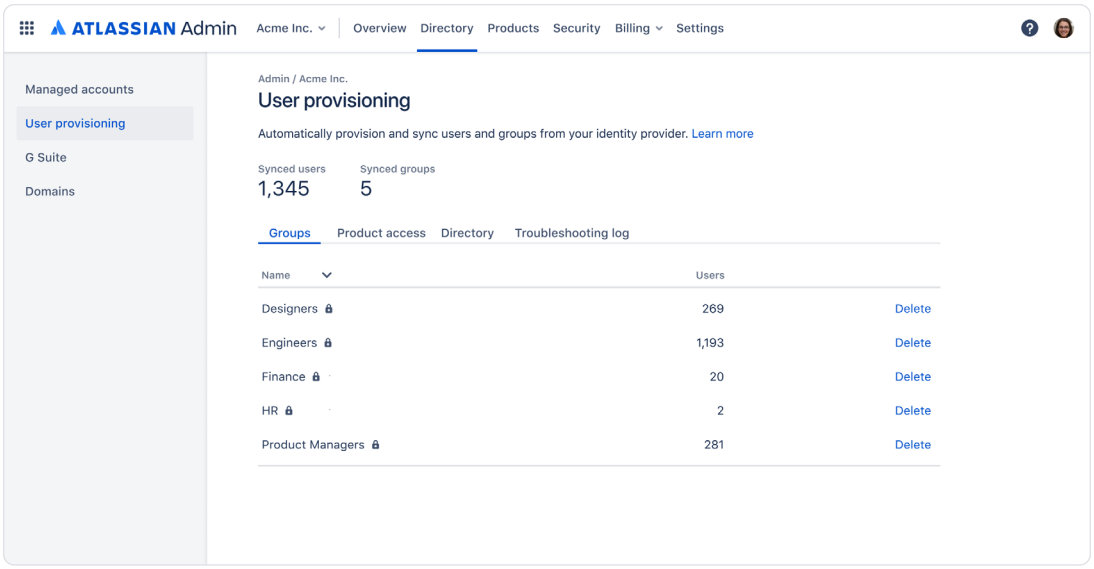
According to IBM's latest Cost of a Data Breach Report, the average cost of a data breach in 2021 is $4.24 million – the highest it's been in 17 years. You can't afford to fall behind on user provisioning and de-provisioning, and with automated user lifecycle management, you're less likely to.

According to IBM's latest Cost of a Data Breach Report, the average cost of a data breach in 2021 is $4.24 million – the highest it's been in

By automating user provisioning and de-provisioning, admins can automatically give or remove software permissions for employees who are onboarding, offboarding, or transitioning to new teams. This automation keeps systems and data in the right hands and secure.

Get started with a security solution that will connect to your user directory to update cloud product access for new or departing employees. So whenever there are employment status changes in your identity provider (such as Okta or Microsoft Azure), permissions are modified to reflect that.

With Atlassian Access, the user directory syncs with Atlassian's cloud applications to keep permissions in line with your identity provider at all times.



Set up automated user provisioning and de-provisioning with Atlassian Access.

It's no wonder then that "85% of surveyed IT organizations said that user management is better or equal on the cloud," according to a TechValidate survey of 311 Atlassian customers.

85% of surveyed IT organizations said that user management is better or equal on the cloud.

Canva keeps data secure with automated user provisioning and de-provisioning

Global design enterprise **Canva** has scaled to over 1,000 employees since the company's beginnings in 2013. Adopting cloud technology was necessary to carry out sustainable collaboration and meet increasing consumer demand.

So Canva's engineering teams turned to Atlassian cloud products – specifically Jira Software, Jira Service Management, and Confluence – to make it easier to work in sync and innovate. And the company secured its cloud experience with Atlassian Access.

Using Atlassian Access' user lifecycle management feature, Canva gives new employees limited access to specific systems and documents ahead of their start date. The company synced its identity provider Okta with Atlassian Access, so admins could see up-to-date information on users and groupings and assign or remove permissions accordingly.

"[New hires] aren't able to see anything but the documents we send them because access is restricted through user group access mapping," says Jeff Lai, Canva internal infrastructure guru. "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."

Canva uses Atlassian applications to document policies, support employee onboarding, set internal goals, and enable self-directed incident reporting and HR payroll insights and management.

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

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

2: Implement SAML SSO for stronger password hygiene

The more passwords employees are required to create, the more likely they are to revert to poor password hygiene. After all, they just want to log in to their accounts and start working, and remembering multiple complex passwords gets in the way of that. If team members in your organization are setting weak passwords or using the same password across different applications, they're making your company vulnerable to a security breach.

In the **LastPass Psychology of Passwords Report**, 44% of the 3,250 worldwide respondents indicated that they set passwords that are identical or alike for multiple accounts, knowing the security risk this poses. Additionally, more than half of those surveyed reported that they haven't updated their password in a year despite learning of security breaches.

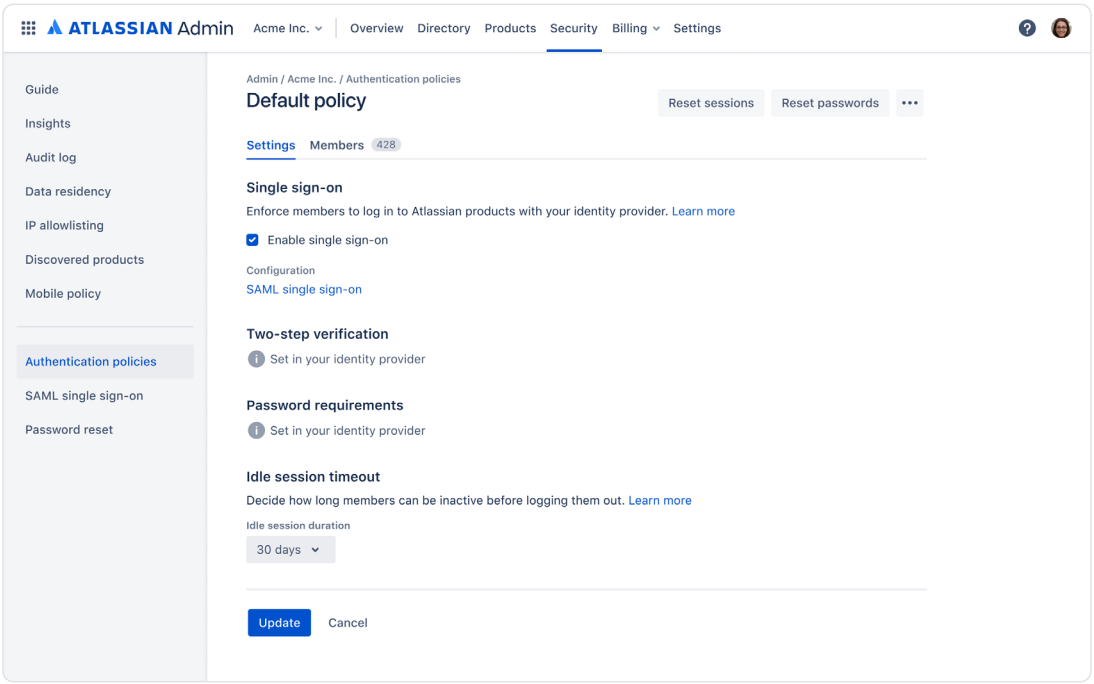
It's likely that some of your employees may have similar responses to their password practices – and all it takes is one bad password for a breach to occur.

More than half of [respondents] reported that they haven't updated their password in a year despite learning of security breaches.

But what if your employees only had to remember a single set of credentials? They'd probably be more inclined to select stronger passwords.

Security Assertion Markup Language (SAML) single sign-on (SSO) makes this scenario a reality. Employees use one username and password to access applications across the cloud. Meanwhile, admins can rest assured knowing that only authenticated users will be able to log in to company cloud tools based on the integrated identity provider in place – whether that's Okta, OneLogin, or Microsoft Azure.

Atlassian Access integrates with identity providers so admins can implement **SAML SSO** for Atlassian cloud products. That way, only authorized users noted by a company's identity provider will be able to log in with their distinct credentials.



Integrate your identity provider with Atlassian Access to set up SAML SSO for Atlassian cloud solutions.

You can also set an authentication policy to enforce single sign-on for a specific group of users. For example, an Atlassian customer in the computer technology space quickly enabled SSO for a smaller subset of users to test their SAML configuration before it was rolled out to the 13,000 users working under their domain.

Nextiva encourages better password practices using SAML SSO

In three years, voice-over-internet-protocol (VoIP) company **Nextiva** nearly doubled its employees. As the company's workforce grew, overseeing internal tools started taking too much time and too many resources. Additionally, employees having to jump back and forth from tool to tool every day was taking a toll on their workflows.

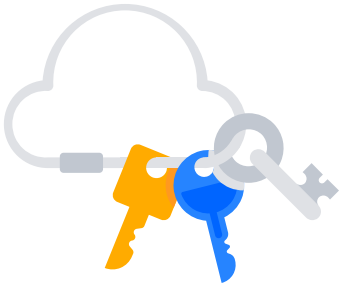
Moving to the cloud was a logical route for the company as Nextiva's leadership wanted to improve employee productivity and continue delivering the great customer experience the company had a reputation for.

As the enterprise adopted more and more Atlassian cloud products – like Jira Software, Jira Service Management, and Confluence – Nextiva went all-in and migrated to the cloud. During this time, they adopted Atlassian Access and Okta to implement SAML SSO and enhance security for the company.

"We've been able to improve our level of security with the integration of our SAML/SSO provider (Okta) and Atlassian Access," said Josh Costella, Senior Atlassian Solutions Specialist. "Atlassian Access made the login process with Okta and SSO a lot simpler than what we had before. It has made our user de-provisioning a lot more efficient and accurate as well."

> "Atlassian Access made the login process with Okta and SSO a lot simpler than what we had before. It has made our user de-provisioning a lot more efficient and accurate as well.

JOSH COSTELLA
SENIOR ATLASSIAN SOLUTIONS SPECIALIST



3: Enforce two-step verification to prevent account breaches

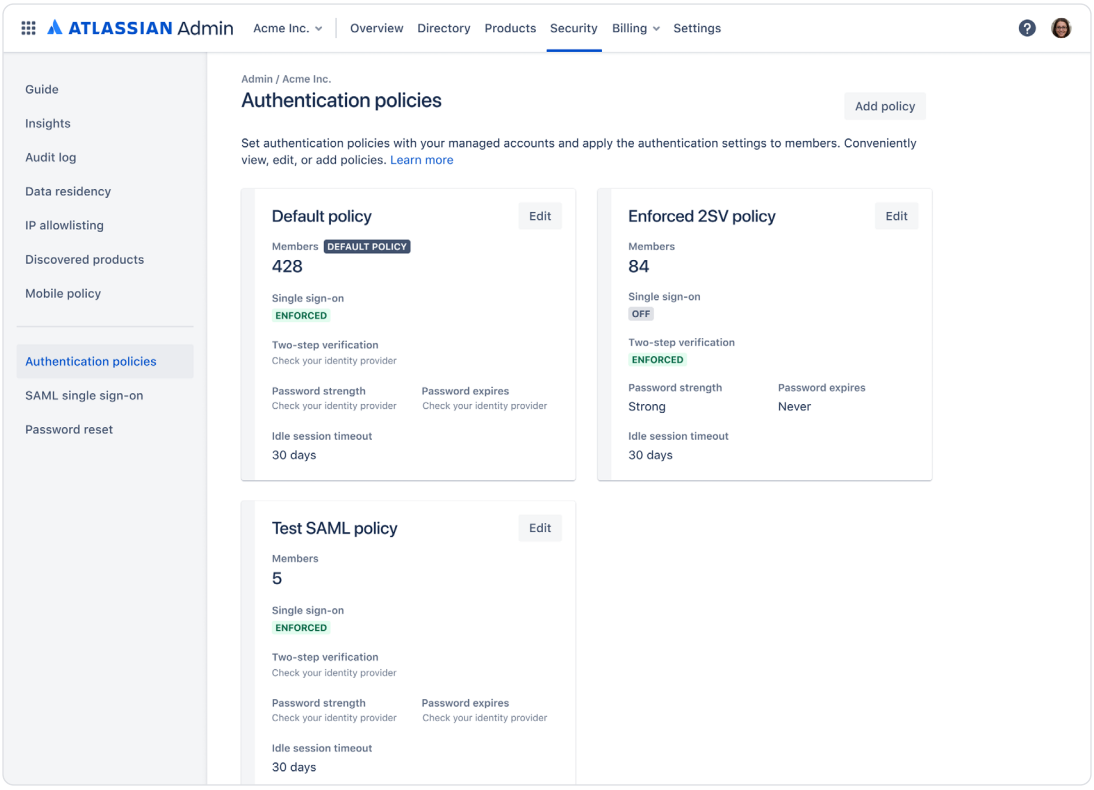
The IBM 2021 Cost of a Data Breach Report states that 20% of data breaches were the direct result of credentials being compromised. In other words, login information was stolen for unauthorized company data access. Credential theft was also found to be the most frequent target area of security vulnerability.

Credential theft was also found to be the most frequent target area of security vulnerability.

There's an additional layer of security that likely would've prevented these breaches – two-step verification. Many companies have policies that ask employees to set up two-factor authentication for their cloud accounts but don't enforce them. And to no surprise – many employees never enable this security feature.

There is, however, a way to ensure that your entire workforce adopts this secondary authentication method. With enforced two-step verification, new and existing users are required to set up two-step verification when logging in and using cloud products. Even if a user's credentials are compromised, you know their cloud account has extra protection with the second verification step.

Atlassian Access allows companies to establish an authentication policy with enforced two-step verification for employees using Atlassian cloud products. Once this functionality is turned on, it will automatically log out existing Atlassian cloud users. When they log in again, they will be prompted to set a secondary authentication method in order to use company cloud software. New users will be asked and required to do this during the employee onboarding process.



Implement enforced two-step verification to add a second layer of security to user accounts.

Homegate AG creates another security barrier with two-step verification

The largest Swiss online real estate platform, **Homegate AG**, has over 110,000 property listings posted and more than 200 million monthly website views. With the growing demand came increasing effort needed to support the company's servers. This overwhelming server maintenance made a transition to the cloud necessary so IT admins could reallocate time to higher-priority organization initiatives.

The company decided to migrate to the cloud with Atlassian. In the transition period, Homegate AG made cloud security a priority – relying on Atlassian Access to keep the organization safe on the cloud when using Jira Software and Confluence.

Among the security features they adopted from Atlassian Access was enforced two-step verification. This feature, in addition to automated user lifecycle management and SAML SSO, augmented security for the business.

“It’s such a big improvement. I almost can’t imagine what it was like before,” says Peter Grube, Homegate AG Software Engineer. “Before, we had to manually add and remove users for each platform and manually manage permissions. And in that process, which happened once or twice a week, you had to think about so many things: who needs access, what permissions they need, which boxes to check, etc. Now [with Atlassian Access], user management is automatic and centralized in one place.”

> “Now [with Atlassian Access], user management is automatic and centralized in one place. It’s such a big improvement. I almost can’t imagine what it was like before.
>
> **PETER GRUBE**
> Software Engineer

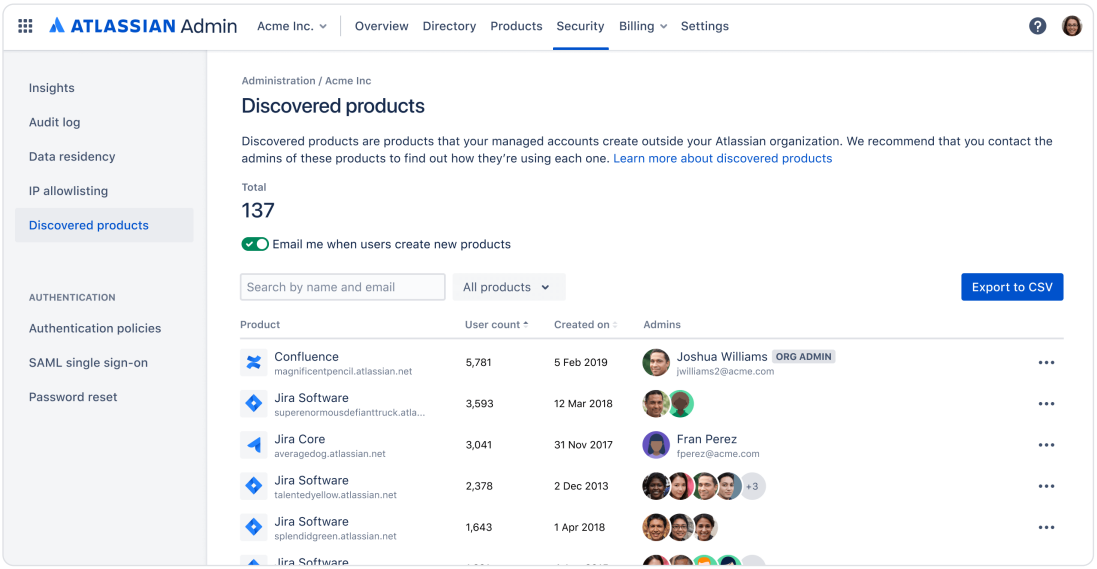
4: Check for shadow IT to eliminate unauthorized software usage

You spend time carefully vetting and approving software options that are safe for your company. Yet **Netskope reports** that 97% of cloud applications adopted by users are shadow IT – meaning that products your employees are creating and using on the cloud may not be monitored or compliant by your organization's IT team.

It's often simple for users to create products to use on the cloud, which often leads to innovation. But for IT admins, this capability brings valid security concerns. For one, they have no way of knowing or regulating what is being done on shadow IT – including if confidential company data is being shared across these applications.

Without insight into unauthorized cloud applications, admins may miss shadow IT that opens your organization to security issues. And as your organization grows, it becomes even tougher for admins to monitor cloud products created and adopted without IT approval. Admins need visibility into these products – not to shut them down, but to determine whether they should become an official solution that IT sanctions.

Atlassian Access includes an **automatic product discovery** feature that will alert you of cloud shadow IT – including when the application was created, how many users are actively using the software, and who the unauthorized product admin is. Admins can then get in touch with users creating these products to identify a more secure process for managing these apps going forward.

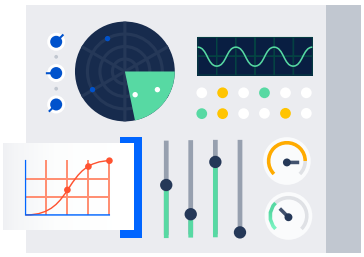


Gain insights into shadow IT with Atlassian Access's automatic product discovery feature.

Admins will regularly receive emails from Atlassian informing them of their organization's shadow IT cloud products and listing out each one of these applications. Detailed information about the software is available in the **Atlassian admin console**, where admins can directly connect with the owners of these products.

Enterprise admins are finding relief with Atlassian Access's shadow IT product discovery feature. One organization admin said, "Just want to say how cool [this] feature is. I got the email today and found out about two other Jira instances we had no visibility of previously."

> "Just want to say how cool [this] feature is. I got the email today and found out about two other Jira instances we had no visibility of previously.

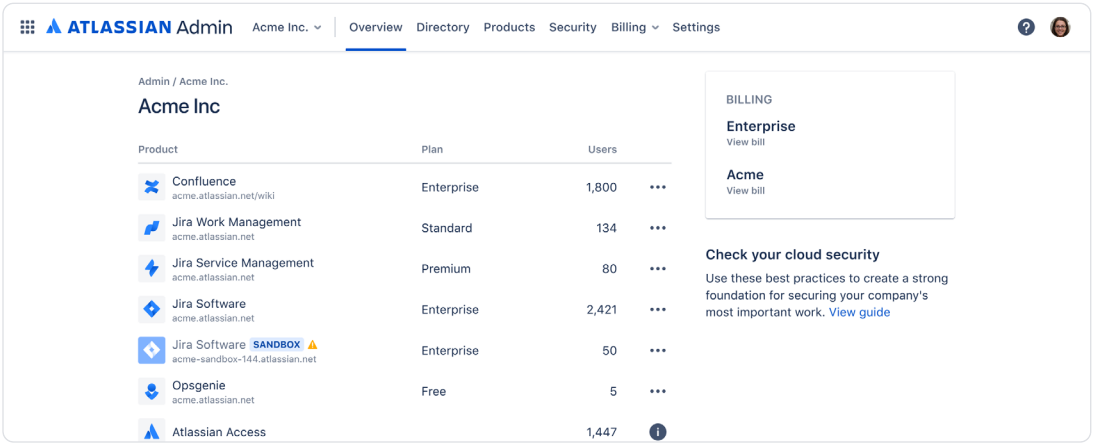


5: Adopt centralized admin control for cloud security management

Keeping a close eye on security across numerous cloud applications is challenging enough. Add in hundreds – or even thousands – of users to monitor, and cloud security management quickly becomes unsustainable for your admin team.

The best solution? Centralize admin control so you can manage cloud security – from authentication controls to organizational oversight – all in one place

With Atlassian Access, admins can use the **Atlassian centralized admin console** to monitor Atlassian cloud product usage for compliance and ensure user software permissions are in line with employment status.



With centralized admin control via Atlassian Access, you have visibility and control over usage, security, and more across Atlassian cloud products.

Admins can also see if users are implementing security measures on Atlassian products, like two-factor verification or SAML SSO. Multiple authentication policies can also be set to designated subsets of users – a feature that Atlassian customers love. One Atlassian Access customer said, "Wow! This is fantastic. It's going to save me a lot of time and give me much greater control over access to the system."

> "Wow! This is fantastic. It's going to save me a lot of time and give me much greater control over access to the system.

Zoom maintains security amid expansion with centralized admin control

Video conferencing company **Zoom Video Communications, Inc.** has relied on a solid foundation of Atlassian cloud solutions since it was a startup. This cloud-based technology helped them grow fast while still maintaining enterprise-level security and keeping admin control via Atlassian Access.

With most of the company using Atlassian, Atlassian Access was a must to keep the business secure on the cloud with centralized admin control.

"It's important to me to be very efficient in my administrative control. Atlassian does that really well," says Gary Chan, Zoom Head of IT Infrastructure and Employee Services. "With just one piece of an element, I can set up SSO and MFA and access all the Atlassian products. That's the kind of centralized admin control that we need."

> "With just one piece of an element, I can set up SSO and MFA and access all the Atlassian products. That's the kind of centralized admin control that we need.
>
> **GARY CHAN**
> Head of IT Infrastructure & Employee Services

Zoom originally adopted Atlassian cloud products to support its engineering teams as the company scaled, starting with Jira Software and Confluence. After seeing the success that engineering was having with Atlassian, other departments decided to leverage Atlassian cloud solutions as well.

Jira Software and Trello support project management, Confluence hosts Zoom's important documents and communications, and Statuspage allows for better communication during the incident management process.

> Atlassian Access is, for us, a mandatory component. Otherwise, my employees will need separate access and entry points for each tool. That would reduce usability and cause security issues.
>
> **GARY CHAN**
> Head of IT Infrastructure & Employee Services

Atlassian Access gives Zoom admins control and visibility over security across all of these Atlassian cloud products – including SSO.

"Atlassian Access is, for us, a mandatory component," Gary says. "Otherwise, my employees will need separate access and entry points for each tool. That would reduce usability and cause security issues."

By having cloud systems and processes in place, Zoom was able to thrive when people needed its product the most during the pandemic. Zoom experienced 10 times more profits and an additional $2 billion in revenue in 2020.

Enhance your company cloud security with Atlassian Access

As you bring your business further into the world of the cloud, take security into account to protect your data and your company's reputation. Keep your company safe on the cloud by putting these cloud security practices into action with Atlassian Access. Our solution offers a wide range of security features – including user lifecycle management, shadow IT monitoring, SAML SSO, enforced two-step verification, and a centralized admin console.

A TechValidate Atlassian customer survey of 318 users found that, "following the migration to Atlassian's cloud products, 60% of surveyed IT organizations experience peace of mind around maintaining security and version upgrades.

Following the migration to Atlassian's cloud products, 60% of surveyed IT organizations experience peace of mind around maintaining security and version upgrades.

Ready to garner improved governance over the cloud with Atlassian Access?

Discover everything it has to offer your company and start a **free 30-day trial today.**

ATLASSIAN