ATLASSIAN

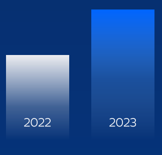
Safeguard your enterprise

with centralized cloud administration

Connecting teams and managing risk

As an admin, you're responsible for connecting teams across your enterprise and managing its cloud footprint. This means balancing supporting teams who want flexibility to innovate and move fast, with the visibility and controls needed to protect your organization's data. This is amidst the increased challenges resulting from remote and hybrid teams, growing cloud adoption, shifting environments, and more.

$591.8
Billion



cloud spend forecasted in 2023, up from $490.3 billion in 2022 (Gartner)

53

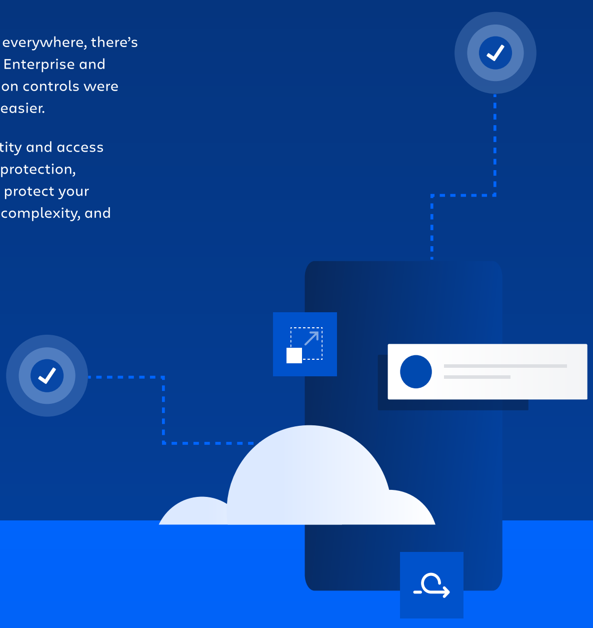
the avg number of cloud apps an enterprise uses
(Thales Group)

40%

of orgs reported an increase in cloud-based threats
(PwC)

With risks originating from everywhere, there's a lot to do. Atlassian Cloud Enterprise and its centralized administration controls were designed to make your life easier.

With tools to manage identity and access management, information protection, and threat detection, you'll protect your organization, reduce cloud complexity, and work smarter.



IDENTITY AND ACCESS MANAGEMENT

Upgrade your security system

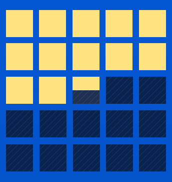
and keep intruders out

Evolving your security practices

Threats are evolving, and your security practices need to evolve with it. You now have to keep up with growing teams, new ways of working, and more advanced threats such as stolen passwords, phishing attempts, and information breaches.

80%

of corporate web app security breaches are due to stolen credentials
(Verizon)



53%

of users admit to reusing passwords across different accounts
(SecureAuth)

48%

of teams spend too much time manually provisioning and deprovisioning users
(Productiv)

Feature spotlight

Customize and apply multiple authentication policies to specific user groups to ensure they are compliant and have the right level of access.

Control authentication for users outside of your organization with external user security *(coming soon)* for secure collaboration.

Automate user provisioning by syncing your directories across products to automatically give and revoke user access as employees join or leave.

With Atlassian's comprehensive approach to identity and access management (IAM):

Deploy multiple authentication methods such as two-factor authentication and single sign-on (SSO)

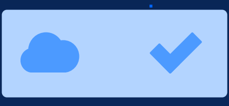
Customize and enforce identity-related controls for different departments, teams, or user groups with a multi-instance model

Automate and streamline access management by integrating your user directory and cloud products to save time and focus on more strategic work, and reduce errors

INFORMATION PROTECTION

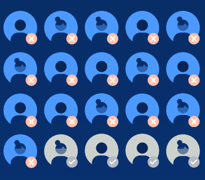
Protect your enterprise

from the dangers lurking in the shadows



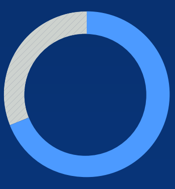
Visibility over your Atlassian footprint

Having visibility over your Atlassian footprint and verifying your teams are using managed and secure products is critical for security and compliance. But it's hard to account for employees who spin up their own instances. You don't want to block work, but this can introduce external threats, operational complexity, and bill shock from spiraling costs.



80%

of employees admit to using applications without IT approval (Axonius)



69%

of tech executives believe Shadow IT is a top concern (Torii)

Shadow IT doesn't have to be the enemy

It can lead to standardized tools and provide teams with more flexibility to decide how they work. However, you need the visibility to uncover cloud sprawl upfront and act on it, and have absolute control over sensitive data to reduce the risk of unauthorized access.

Feature spotlight

Know when your users create product instances with automatic product discovery and secure your organization.

Proactively control your Atlassian products and your end-users' ability to create new instances using product requests *(coming soon)*.

Encrypt cloud product data with keys hosted in your own AWS account and revoke access for end-users and Atlassian systems as needed using BYOK encryption *(coming soon)*.

INFORMATION PROTECTION

Detect and resolve security threats

by following the clues

Advanced monitoring and reporting for proactive threat detection

If you needed information about your team's specific actions, could you easily access it? This may be helpful for auditing and compliance, but it is essential during the day-to-day. The more that you know about your cloud environment and where the potential vulnerabilities are, the better positioned you are to respond.

39%

of security leaders cite visibility as their biggest security concern (Safeguard Cyber)

31%

of business leaders have a high level of confidence they have the full visibility needed to safeguard their organization (Gartner)

Advanced tools

Advanced monitoring and reporting tools will ensure you're well equipped to proactively detect and resolve security threats across your cloud products, and make data-driven decisions on business operations to inform resourcing and investments.

Feature spotlight

See detailed user and admin-initiated activity including permission change events and triage suspicious behavior with advanced audit logs.

Track usage metrics across Atlassian products such as active users and evaluate your organization's security posture with org insights.

Solve for inefficiencies, product access gaps, and billing confusion with near real-time data on user access using user counts.

Contact us to learn more about Cloud Enterprise

Contact us

Atlassian has made continued investments in Cloud Enterprise and admin.atlassian.com as a centralized mission control center to provide admins like you with the tools needed to safeguard and future-proof your enterprise at scale. Contact us to learn more about Cloud Enterprise and how it can help you maintain visibility and control, while still providing teams with the flexibility to innovate and do their best work.

©2023 Atlassian. All Rights Reserved. CSD-4415_DRD-05/23

ATLASSIAN