ATLASSIAN

Zero Trust: Improved security and user experience in Atlassian Cloud

Threats are increasing – your users are the prime target

Sophisticated attacks are not just aimed at large, global organizations; growing businesses have become a leading target due to their rapid scaling and varying levels of security controls.

Despite foundational security measures put in place at most organizations – the threat landscape has changed dramatically as more teams work remotely, access sensitive data from personal devices, and weak passwords are used to protect overprivileged accounts. Malicious attackers are often able to successfully infiltrate growing organizations through their users.

54%

of security incidents at small to mid-sized businesses resulted in the compromise of user credentials (Verizon)

82%

of organizations allow some bring-your-own-device (BYOD) usage in the workplace (Bitglass)

36%

of respondents revealed that departing employees were not off-boarded within 24 hours of leaving the organization (BetterCloud)

74%

of all breaches include the human element, either through error, privilege misuse, use of stolen credentials, or social engineering (Verizon)

Invest in an IAM strategy that can scale with your organization

Building a scalable identity and access management (IAM) strategy can be achieved through identifying and implementing best practices using people, processes, and technology to improve your security posture and address your regulatory compliance requirements.

As you look to implement a cloud IAM strategy, review the principles of zero trust. Zero trust principles help your organization create an IAM strategy that is secure and flexible enough to support remote work, allow access to company data from personal devices, and improve overall user experience. This approach provides a consistent experience for users and up-levels your security regardless of user device or location.

Never trust, always verify

Taking a zero trust approach means regardless of device or location, your organization will always require users to verify they are who they say they are.

Principle of least privilege

Ensure access to data is restricted to what is necessary to complete job tasks. This reduces the organizational risk if credentials are compromised.

Assume breach

Automatically require users to re-authenticate after a set session duration and require step-up authentication to defend against anomalous behavior.

Making zero trust a reality for your organization

Putting zero trust into action at your organization is a multi-step and iterative process. Create policies to manage user access and implement them across all users who interact with your data and applications. Policies should apply the maximum restrictions on access to sensitive data and include additional safeguards to keep any bad actors with compromised credentials from accessing privileged information.

Once you've created these policies, continually monitor activity across your organization, audit privileges for user groups, and ensure your organization isn't experiencing configuration drift. Continually iterate on your policies and revisit your configurations to meet your organizations evolving needs.

55%

of SMBs admit they are not very aware of multi-factor authentication (MFA) and its security benefits (Cyber Readiness Institute)

Enforce single sign-on (SSO) and multi-factor authentication for every session. Requiring users to explicitly verify their identity helps reduce the risk of someone using a stolen device to access your data.

Reduce the chance of overprivileged accounts and revoke unnecessary permissions as soon as possible.

Set parameters like session duration, password strength requirements, and up-level permission requirements based on groups.

Applying your zero trust approach in Atlassian Cloud

Extend your organization-wide IAM policies and zero trust approach across your Atlassian Cloud products with Atlassian Access. Enforce single sign-on, accelerate user onboarding for Atlassian products, and reduce manual IAM tasks to keep pace with your scaling organization.

Learn More

ATLASSIAN