

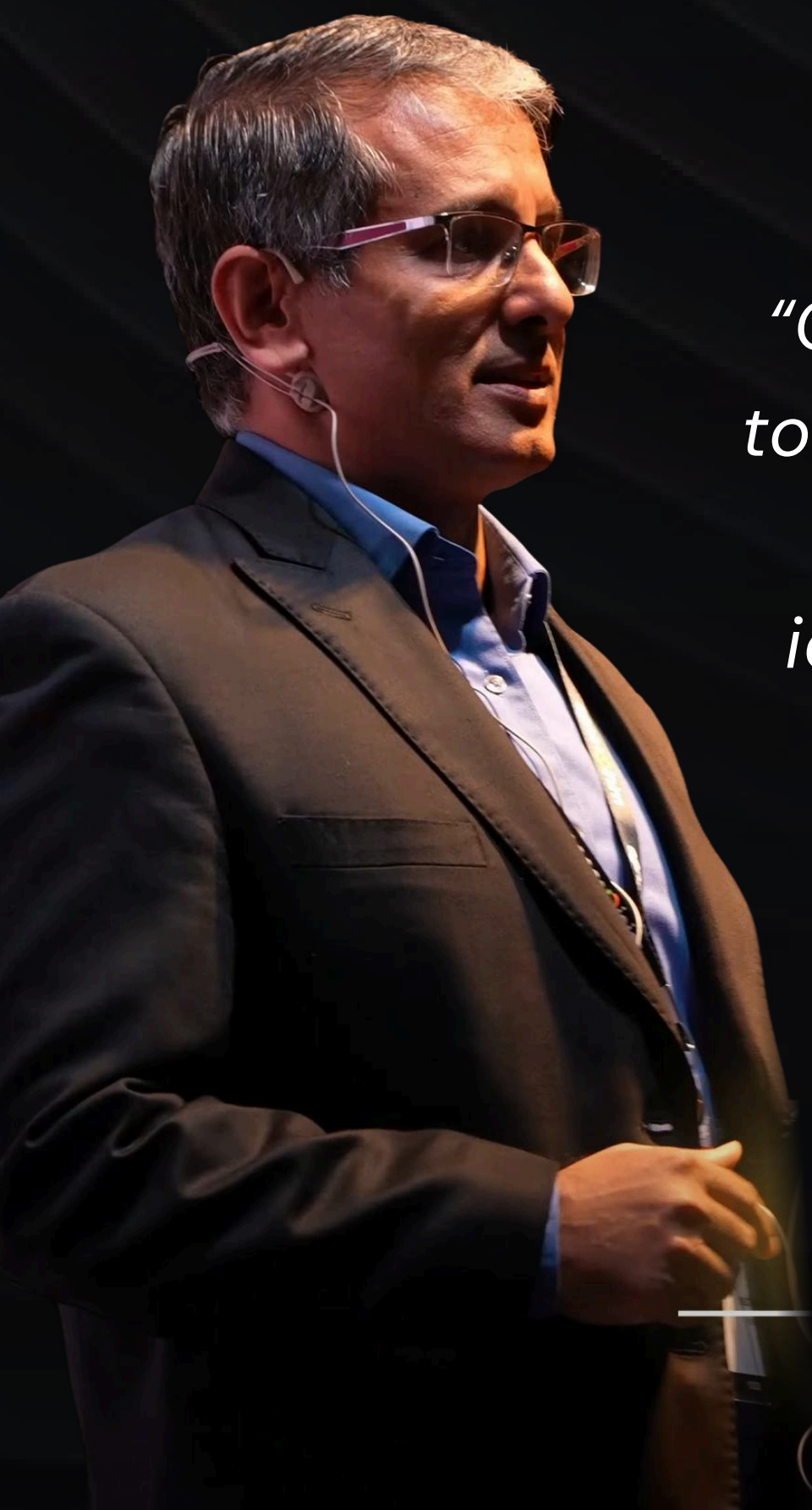


miniOrange FOR  ATASSIAN

# Identity, Access, and Data Security for Atlassian Apps

# TRUSTED ON THE ATlassian MARKETPLACE FOR 10+ YEARS

miniOrange expertise spans identity, access governance, data protection, user lifecycle, and developer tooling across Jira, Confluence, Bitbucket, JSM and others. Every app is built to solve a real problem Atlassian admins face, backed by round-the-clock engineering help when you need it.



*"Our mission is simple:  
to create a safer digital  
world by providing  
identity solutions that  
balance security,  
efficiency, and trust"*

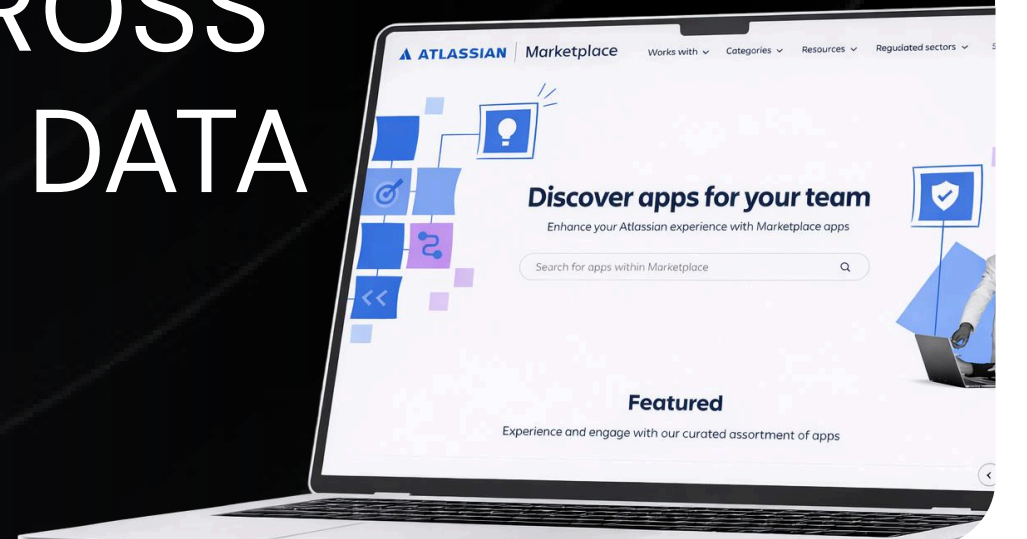
**ANIRBAN  
MUKHERJI**

CEO / Founder  
miniOrange

**3,000+**  
ATLASSIAN CUSTOMERS  
WORLDWIDE



**50+**  
APPS ACROSS  
CLOUD & DATA  
CENTER



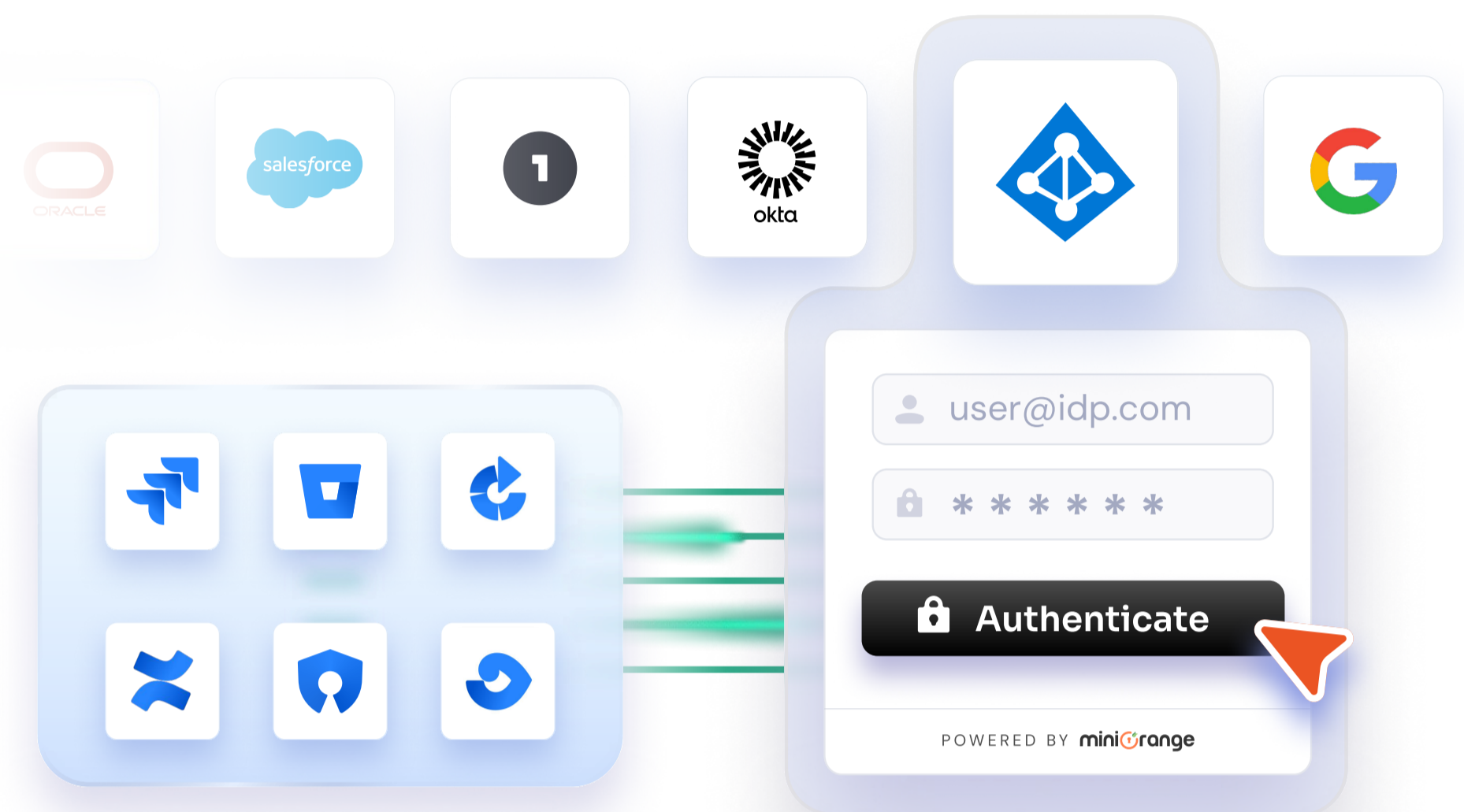
**24x7**  
DEVELOPER-FIRST  
SUPPORT

## SSO & Provisioning for Atlassian Cloud

# SSO For Atlassian Cloud

Single login for Jira, Confluence, and Bitbucket, with your choice of SAML or OAuth/OIDC provider.

- **Multi-IDP Flexibility:** Break free from plan limitations. Authenticate different user groups or departments across multiple SAML and OAuth/OIDC providers without the need for high-tier enterprise licensing.
- **Smart Login Routing:** Route users automatically based on email domains or group memberships, ensuring every user redirects to the right identity provider every time, creating a friction less login experience.



# SCIM/REST API Provisioning For Atlassian

Automate user, group and portal only customer sync from your IDP to Jira, Confluence, and Bitbucket.

- **Multi-IDP & LDAP Support:** Effortlessly sync users, groups, and portal-only customers from multiple IDPs or legacy LDAP/AD sources simultaneously.
- **REST API based Provisioning :** Securely sync users from IDPs that don't support SCIM protocol like Keycloak, Partner.net etc and efficiently provision users & groups via API based provisioning.
- **Custom Attribute Mapping:** Continuously map custom attributes from your IDP to Atlassian profiles, ensuring your workflows are powered by real-time, accurate data.

JSM Portal SSO & MFA

# SSO For JSM Customer Portals

Secure your JSM portals with enterprise-grade SSO that turns complex access requirements into a seamless journey.

- **Multiple IDP & Protocol Support:** Easily integrate with multiple identity providers (IDPs) and protocols, including SAML and OAuth/OIDC, ensuring seamless compatibility.
- **Granular Portal Access Control:** Restrict portal access efficiently by restricting users based on Jira organizations, customer domains, and IDP groups, ensuring your portal remain exclusive to authorized users.
- **Custom Field Mapping:** Seamlessly map user attributes from multiple IdPs into Jira custom fields

# MFA For Atlassian Cloud

Enterprise-Grade Multi-Factor Authentication For JSM Customers

- **Support for Multiple MFA methods:** Choose from multiple 2FA methods to fit your user's workflow. We support all Authenticator apps, Duo Push, hardware tokens, OTP via email/SMS, security questions, etc
- **IP Based Restriction:** Use IP Whitelisting to offer frictionless login for trusted networks without compromising safety.
- **Organization-Specific Security:** Apply 2FA rules to specific JSM Organizations for surgical access control.
- **Detailed Audit Logs:** Ensure complete transparency for administrators by comprehensively logging authentication activities.

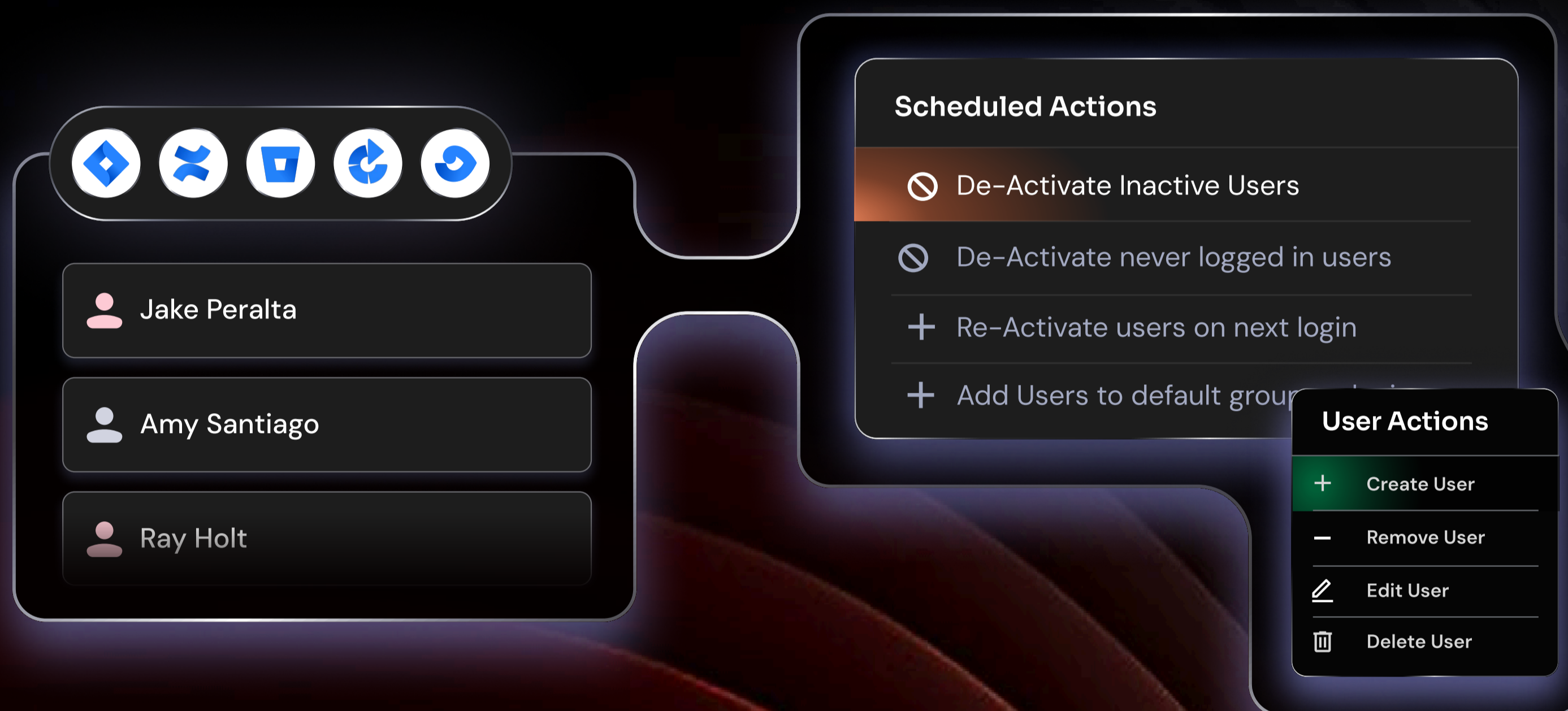


## User Lifecycle

# Automated User Management

Deactivate inactive users, reclaim licenses, and automate lifecycle actions in Atlassian.

- **Auto-deactivate** inactive and never-logged-in users
- **Bulk activate**, deactivate, delete, and group-manage
- **CSV import/export** and batch group creation
- **Email notifications** for deactivation alerts and license limit warnings
- **Audit logs** and ticket reassignment on deactivation



# Migration Assistant

Sanitize your DC instances with automated PII/PCI redaction and automated user cleanup.

- **Smart Data Profiling:** Automatically identify oversized & unwanted attachments and data, giving admins the actionable insights needed to optimize migration for a leaner, more cost-effective cloud transition.
- **Deep History Inspection:** Scan every ticket, page, and version history to detect PII, secrets, and credentials, ensuring your data is audit-ready.
- **One-Click Remediation:** Instantly encrypt, redact, or delete exposed sensitive content in Data Center before it ever reaches the Cloud.
- **Automated User Optimization:** Effortlessly identify dormant users to bulk-deactivate or remove licenses, slashing your Cloud migration overhead while generating audit-ready analytics for license planning

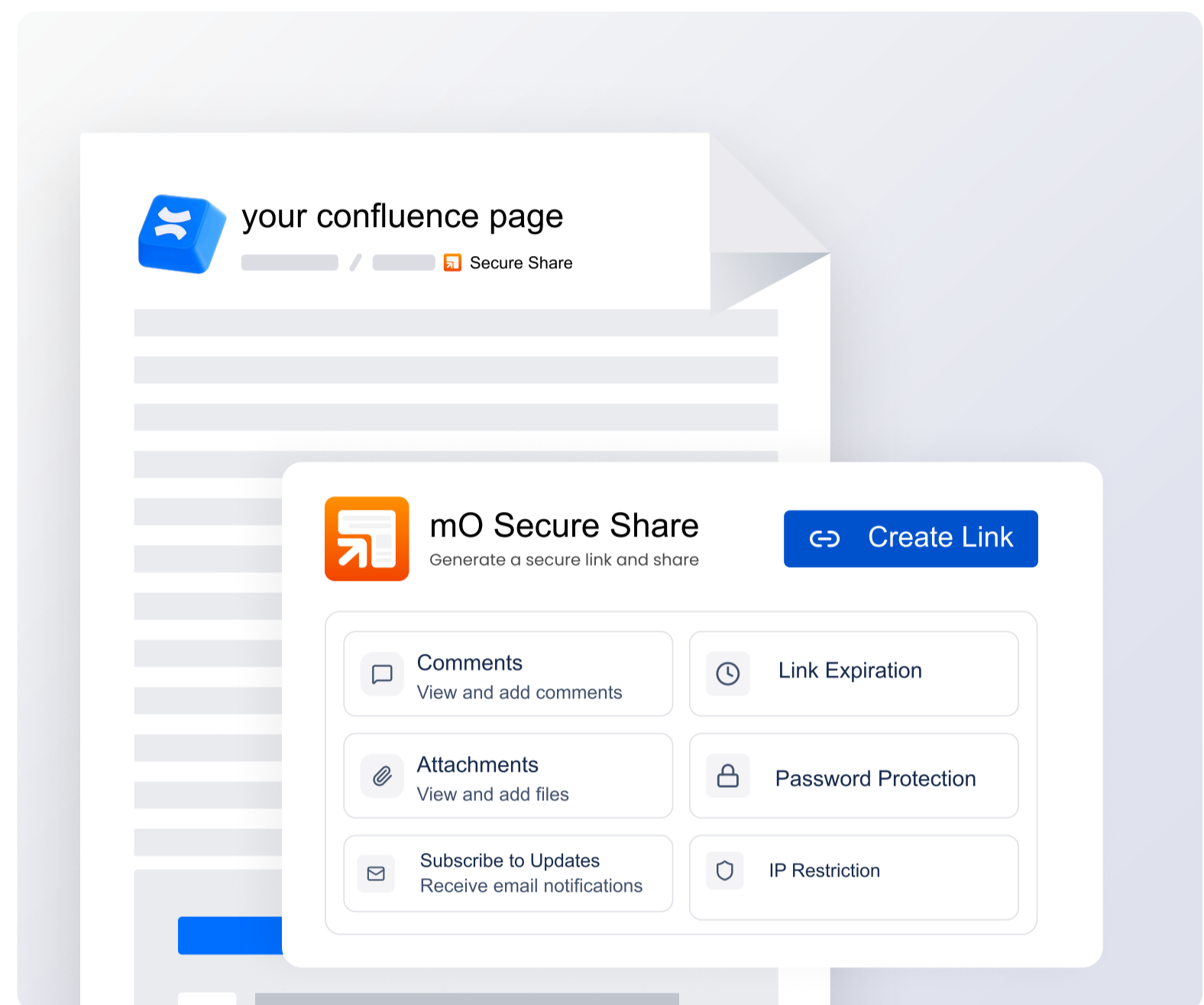
## Data Security &amp; DevOps

# Secure Share ✨

Share pages and issues with external users without buying extra licenses.

Give vendors, clients, and partners controlled access to specific Confluence pages or Jira content through secure links. External users can view, comment, and attach files on your terms, with no seat cost.

- **Password-protected links** with expiry dates
- **IP restrictions** and SSO-enforced access
- **Permission control** per shared page (view, comment, attach)
- **Subscription-based** notifications for page changes
- Allow external users to edit Confluence pages



## AI Code Reviewer ✨ For Bitbucket

AI code review for Bitbucket pull requests. Line-by-line suggestions, custom rules, and your choice of LLM.

Automate the first pass of every pull request review. AI reads the diff, flags bugs and security issues, and posts inline comments directly in the Bitbucket PR so developers stay in their workflow.

- Automated **line-by-line PR reviews** with inline comments
- **Admin-selectable LLM** (align reviews with your preferred AI provider)
- **Repository-level** custom rules and coding standards
- **Audit logs** retained for 90 days with export support
- **One-click** review trigger from within the PR

# DLP PII Protection ✨

Detect, redact, and prevent sensitive data leaks across Jira and Confluence.

- **Deep-Scan History Inspection:** Scan Jira tickets, comments, attachments and Confluence page/space to uncover hidden PII, credentials, and secrets.
- **Precision Detection Engines:** Leverage powerful pre-built and custom regex rules with smart classification to identify sensitive data across your Cloud instance
- **Automated Bulk Remediation:** Secure your data in seconds with one-click bulk redaction and encryption.
- **Audit-Ready Governance:** Maintain total transparency with comprehensive audit logs that track every finding and remediation action for compliance reporting.



# Access Governance & Auditing ✨

Request, approve, and provision app access through Jira Service Management.

- **Policy-Driven Governance:** Ensure every request follows a defined, governed path with multi-tier approval logic and stakeholder notifications with automated provisioning upon approval
- **PIM & Just-in-Time Access:** Secure sensitive resources with time-bound permissions (e.g., 3 days or 1 week) that automatically revoke to prevent privilege creep.
- **Audit-Ready Compliance:** Generate granular reports with a traceable history of who approved what, when, and why capturing every action directly on the JSM ticket.



**Secure Identity, Access & Data  
Protection – Everywhere Atlassian Runs**

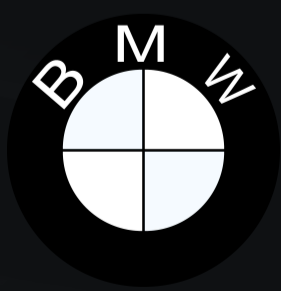
Reach out to us anytime.

+1-978-658-9387 (US)

+91 97178 45846 (India)

[info@securify.com](mailto:info@securify.com)

[miniorange.com/atlassian](https://miniorange.com/atlassian)



SONY

SIEMENS

AIRBUS

Allianz 



Uber

