INSIDEOUT AI - CUSTOMER SECURITY REVIEW

Sprint Guide Security Overview

CISO decision brief for the Jira Cloud integration

Last verified: 2026-10-06 - Document owner: InsideOut AI

Product information: **insideoutai.io/SprintGuide**

Purpose

This document provides security and privacy information for organizations evaluating Sprint Guide for use with Jira Cloud. It focuses on the controls and data flows most relevant to a security approval decision.

Sprint Guide is a read-only analytics and guidance application. Jira remains the system of record. The application does not modify Jira data and is not required for Jira to operate.

Executive security position

- **Read-only Jira access.** The requested OAuth scopes permit reading the Jira data required for analysis. Sprint Guide does not request Jira write, delete, configuration, or administrative scopes.
- **User-scoped authorization.** Jira access is limited by both the granted OAuth scopes and the permissions of the individual Jira user who connects the application.
- **No Jira credentials.** Atlassian handles Jira authentication and consent. Sprint Guide does not receive the user's Atlassian password or organizational SSO credentials.
- **Protected backend handling.** OAuth code exchange, token refresh, and Jira API requests are performed by backend functions. OAuth tokens are not exposed to browser code.
- **Data minimization.** Sprint Guide retrieves selected planning and delivery data needed to calculate and display its analyses. It is not designed to retrieve issue descriptions, comments, attachments, or worklogs.
- **No AI-model processing.** The reviewed application does not send customer Jira data to an LLM or other generative AI model.
- **Low operational dependency.** An interruption to Sprint Guide does not modify, block, or interrupt the customer's Jira service.

This overview reflects the application reviewed on 6 October 2026. It is not a penetration-test report, certification, service-level agreement, or substitute for the assurance documentation of the underlying service providers.

Architecture and trust boundaries

Sprint Guide operates across three principal trust boundaries:

1. **User browser.** The user signs in to Sprint Guide, initiates the Jira connection, selects configuration options, and views analysis results.
2. **Sprint Guide on Base44.** Base44 provides the application runtime, identity mechanism, backend functions, data storage, encryption services, and email delivery used by Sprint Guide.
3. **Atlassian Jira Cloud.** Atlassian authenticates the Jira user, presents the OAuth consent screen, issues tokens, and enforces Jira permissions.

The user first signs in using Base44's email and password mechanism. This establishes access to the Sprint Guide application and enables application communications. It does not provide access to Jira data. Jira data becomes available only after the user separately completes Atlassian OAuth authorization.

After authorization, a Base44-authenticated Sprint Guide session can request analysis using the stored OAuth grant. Backend functions call Jira over HTTPS and return the requested analysis to the application. The Jira client secret and OAuth token operations remain on the backend.

Sprint Guide does not use a shared Jira service account. Each Jira connection is associated with the authorizing user, and Jira continues to apply that user's project and issue permissions.

Security boundary in practice

- A user who can sign in to Sprint Guide but has not connected Jira cannot view Jira analysis data.
- Connecting Sprint Guide does not grant broader Jira access than the authorizing user already has.
- Disconnecting Jira removes the application's usable connection data from the active user record.
- Jira remains independently available if Sprint Guide is unavailable.

Authentication and Jira authorization

Authorization model

Sprint Guide uses Atlassian's OAuth 2.0 authorization-code flow for Jira Cloud. A per-connection state value is generated before redirecting the browser and is validated on return. The authorization code is exchanged by a backend function, not by browser code.

Access tokens are used for Jira API calls. The `offline_access` scope permits the application to refresh an authorized connection without asking the user to repeat consent for each session. When Atlassian rotates a refresh token, Sprint Guide replaces the stored value.

Requested OAuth scopes

`read:me` - identifies the connected Atlassian user.

`read:jira-user` - reads Jira user information needed for names and assignments.

`read:jira-work` - reads Jira work items and related fields used by the analysis.

`offline_access` - enables refresh-token use for a persistent authorized connection.

`read:board-scope:jira-software` - reads Jira Software board data.

`read:epic:jira-software` - reads epic data.

`read:sprint:jira-software` - reads sprint data.

`read:project:jira` - reads project metadata.

These scopes are read-oriented. Sprint Guide does not request Jira scopes for creating, updating, deleting, configuring, or administering Jira content.

The deployed Atlassian consent screen is the authoritative presentation of the permissions requested at connection time. The authorizing user can review and revoke their personal OAuth grant through Atlassian. Customer administrators can remove Jira product access or restrict or uninstall the application using the Atlassian controls available to their organization.

Data handling and privacy

Jira data accessed

Depending on the analysis and configuration selected by the user, Sprint Guide may access:

- Atlassian user and Jira site identifiers;
- project, board, sprint, and epic metadata;
- issue key and summary;
- issue type, status, assignee, project, parent, and sprint membership;
- relevant planning and completion dates;
- configured story-point and team fields; and
- selected change history needed for delivery analysis.

Sprint Guide is not designed to retrieve issue descriptions, comments, attachments, or worklogs. Jira permissions remain effective for every request.

Processing and retained data

Analysis is performed on demand using data retrieved from Jira. Sprint Guide stores the connection and configuration information needed to operate the authorized integration, including Jira site metadata, selected field identifiers, analysis preferences, and OAuth tokens. Tokens are designated as encrypted fields in the platform data model.

Analysis results are primarily displayed to the user rather than maintained as a separate Jira issue archive. Limited diagnostic, audit, and reliability records may be retained as described in the next section.

The browser may retain non-sensitive presentation and configuration preferences to improve the user experience. Jira OAuth tokens and the Jira client secret are not stored in browser-local storage.

AI processing

The reviewed application does not invoke an LLM or generative AI service to process customer Jira data. Product calculations are deterministic application logic.

User controls, diagnostics, and offboarding

Diagnostic reporting

Diagnostic reporting is user-configurable and can be disabled. When enabled or explicitly submitted by a user, diagnostic information may include:

- account and Jira-site identifiers;
- selected configuration and filter context;
- aggregate analysis metrics;
- actions leading to a reported problem; and
- error, browser, and application-path information.

Diagnostic reporting is designed to exclude passwords, OAuth tokens, issue descriptions, comments, query strings, referrers, and browser-storage contents. Reports are delivered through Base44's email capability to a dedicated support mailbox accessible only to authorized InsideOut AI personnel. Limited operational metrics may also be retained to identify recurring reliability problems.

Disconnect Jira

The user can disconnect Jira from Sprint Guide. The application attempts to revoke the refresh token with Atlassian and clears locally stored connection and token fields. Local cleanup proceeds even if Atlassian's remote revocation endpoint is unavailable. The authorizing user can also revoke the personal OAuth grant through Atlassian. Customer administrators can remove Jira product access or restrict or uninstall the application using their available Atlassian controls.

Delete My Data

The application provides a **Delete My Data** control. It removes stored Jira credentials, connection metadata, and identifying Jira-derived diagnostic information associated with the user. Limited anonymized operational, audit, or organizational metrics may remain where they no longer identify the user or expose Jira content.

These controls do not delete or modify any data in Jira.

Platform and operational controls

Service providers and encryption

Sprint Guide is implemented on Base44 and connects to Atlassian Jira Cloud. Base44 states that its platform provides TLS 1.2 or later for data in transit, AES-256 encryption for data at rest, managed key handling, and encrypted backups. Base44 also states that it maintains SOC 2 Type II and ISO 27001 assurance. These are Base44 platform controls and certifications, not independent certifications of Sprint Guide. Customers may request current supplier evidence directly from Base44 as part of due diligence.

Base44's default hosting region is the United States. Sprint Guide makes no separate regional-hosting commitment.

Application access and security review

Application access is protected by Base44 authentication before a user can initiate or use a Jira connection. Sensitive OAuth operations are limited to backend functions, and application-level records are scoped to the authenticated user. The deployed application has been reviewed using Base44's security scanning capability and is rescanned after material changes.

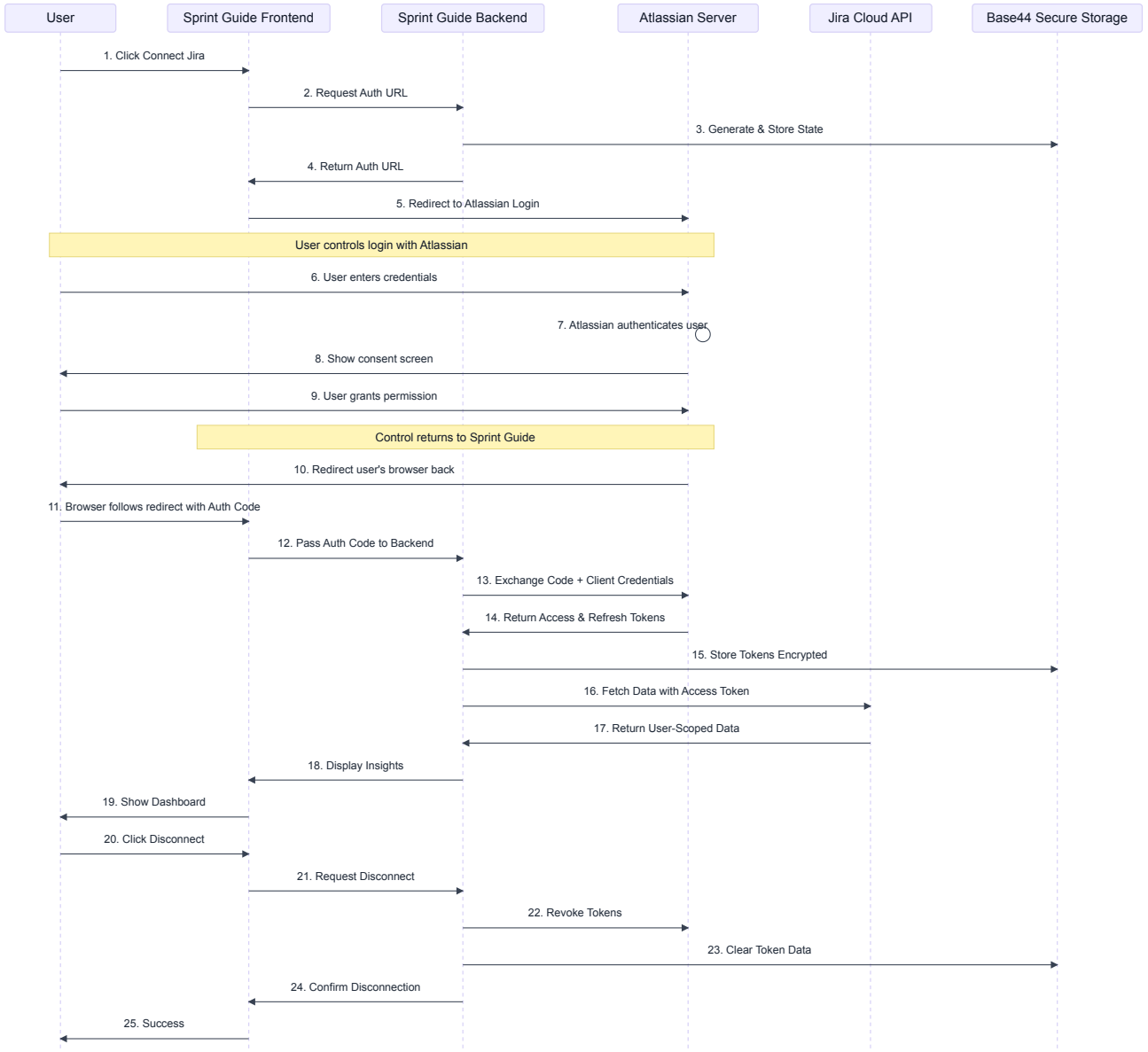
Audit and operational logging

Sprint Guide records limited lifecycle audit events for actions such as connecting Jira, disconnecting Jira, and deleting user data. Backend operational logs support error diagnosis. The application is designed not to deliberately log OAuth token values or Jira issue descriptions and comments.

Sprint Guide is a supplementary service. Jira remains the system of record, and a Sprint Guide outage does not modify or block Jira. Security questions or suspected application-security issues can be reported using the contact on the final page.

OAuth connection and disconnection flow

The sequence below shows the separation between Sprint Guide authentication, Atlassian-controlled login and consent, backend token handling, Jira API access, and disconnection.



Security FAQ

Can Sprint Guide modify Jira data?

No. Sprint Guide requests no Jira write, delete, configuration, or administrative scopes. Its Jira integration is limited to reading the information required for its analyses.

Can Sprint Guide access Jira data that the connected user cannot see?

No. Atlassian applies both the OAuth scopes granted to Sprint Guide and the connected user's existing Jira permissions. Sprint Guide cannot elevate or bypass those permissions.

What happens if a Jira administrator connects?

The connection remains read-only, but Sprint Guide may read Jira information that the administrator is permitted to view. Organizations should therefore connect using a user whose Jira access is appropriate for the intended analysis.

Can Sprint Guide expand its permissions later without approval?

No. Expanding the requested OAuth scopes requires a changed Atlassian consent grant. Users who previously approved the application must re-consent to the changed scopes. The Atlassian consent screen remains the authoritative permission display.

What Jira information does Sprint Guide retain?

Sprint Guide retains the connection and configuration information needed to operate the authorized integration, together with the limited diagnostic, audit, and reliability records described in this document. It does not maintain a general-purpose Jira issue archive.

How can access and stored data be removed?

Users can disconnect Jira, use **Delete My Data**, and revoke their personal OAuth grant through Atlassian. Customer administrators can remove Jira product access or restrict or uninstall the application using their available Atlassian controls. These actions do not delete or modify information in Jira.

What happens when a user leaves the organization?

The organization should remove the user's Jira product access or deactivate the account through its normal Atlassian or identity-provider process. Subsequent Sprint Guide requests remain subject to the user's current Jira permissions. The user can revoke the personal OAuth grant, while administrators can restrict or uninstall the application and remove Jira product access.

Does Sprint Guide send Jira data to an AI model?

No. The reviewed application uses deterministic calculations and does not invoke an LLM or generative AI service to process customer Jira data.

Customer verification checklist

Before approval, the customer security team can independently verify the principal controls:

- Compare the Atlassian consent screen with the exact scope list in this document.
- Connect using a least-privileged Jira test user and confirm that Sprint Guide cannot access projects unavailable to that user.
- Confirm that no Jira write, delete, configuration, or administrative permission is requested.
- Review the listed data categories against the organization's Jira data-classification policy.
- Confirm whether diagnostic reporting should be enabled for the organization.
- Test both **Disconnect Jira** and **Delete My Data** using a test account.
- Review current Base44 and Atlassian supplier assurance documentation under the organization's normal third-party risk process.
- Record the organizational owner responsible for user offboarding and for restricting or uninstalling the application through Atlassian if required.

Security inquiries

Questions about Sprint Guide's security design or suspected application-security issues may be sent to **insideoutaitech@gmail.com**. Sprint Guide relies on Base44 and Atlassian for incidents affecting their respective platforms.

References

- Sprint Guide product information - insideoutai.io/SprintGuide
- InsideOut AI - insideoutai.io
- Atlassian OAuth 2.0 (3LO) apps
- Atlassian Jira Software OAuth scopes
- Atlassian remove app access for users
- Base44 Security

Document owner: InsideOut AI. Review this overview when authentication, data handling, suppliers, or application telemetry materially change.