Encryption at Rest

Broken Build LLP | 20 October 2026

Broken Build LLP protects customer data at rest through encryption provided by the platforms and services that store it. This statement covers Atlassian Forge hosted apps and any approved external storage or logging used in connection with those apps.

Atlassian Forge hosted application data

Our Cloud apps run on Atlassian Forge. Their application functions, calculations, core data processing and app storage use Atlassian hosted infrastructure. Atlassian encrypts data stored in Forge app storage at rest using AES-256. Atlassian operates the underlying storage infrastructure and its platform encryption controls. Broken Build does not operate a separate customer facing production application database for these apps.

External customer data and app logs

Broken Build requires all Atlassian end user data stored outside Atlassian apps or users' browsers, including application logs, to be encrypted at rest using full disk encryption. This requirement applies to any approved external analytics or logging service and to copies, exports or backups containing that data. External storage must not be used without appropriate encryption protection.

Optional telemetry integrations do not change where the core app is hosted. Where enabled, the following provider disclosures describe their protection of stored data:

- Mixpanel states that Customer Content is encrypted at rest with AES 256-bit encryption. Its technical and organizational measures also describe encryption of backed up Customer Content.

- Logz.io states that its service encrypts data at rest and in transit. Its security documentation describes AES 256-bit encryption for cold data stored in S3.

Access and responsibility

Atlassian and other approved providers operate encryption for the infrastructure they manage. Broken Build controls app configuration, external destinations, application access and vendor oversight. Encryption complements access restrictions and data minimization. Credentials and unnecessary personal data must not be written to application logs.

References

- Atlassian Forge and SOC 2: https://developer.atlassian.com/platform/forge/forge-soc2-iso27001/

- Mixpanel technical and organizational measures: https://mixpanel.com/legal/tom/

- Logz.io encryption overview: https://logz.io/blog/how-logzio-provides-trustworthy-observability-through-ai/

- Logz.io customer data security: https://logz.io/platform/features/soc-2-compliance/

Security contact: security@brokenbuild.net.