Katchr Cloud Security FAQs

Katchr software runs from the Microsoft Azure cloud platform. Below is a guide to the common questions Katchr receive around security and the Microsoft Azure platform.

How can I be confident in how Katchr manages my data?

Katchr has been accredited to ISO 27001:2013 since 2019 for the management of information security in the provision of software solutions, including development, support, project management and consultancy.

Application security: how is this controlled and maintained?

- Authentication is managed through either Katchr user accounts or federated to Azure AD.
- Authorisation is managed through a customisable user management system within Katchr.
- Data:
    - The Katchr data warehouse is encrypted at rest,
    - Data is encrypted in transit - from site (PMS location) to Katchr via the Microsoft Integration Runtime, and by https/TLS when dashboards are accessed by an end user.

Review of our development team and process is a major part of the ISO 27001 certification audits. All code is peer reviewed prior to merging into our main development branch, and we run general acceptance testing prior to release. OWASP vulnerability scanning via ZAP is done on every new release.

System failure: in the event of a system crash who manages the recovery process, what is involved and what timescales do you work to?

The Katchr dashboard solution is run on an MS Azure App Service, with individual client databases hosted in an Azure SQL Elastic Pool. Both are backed by a standard Microsoft SLA committing to 99.95% availability.

Recovery time to restore a database varies depending on several factors:

- Size of database
- The compute size of the database
- The number of transaction logs involved
- The amount of activity that needs to be replaced to recover to the restore point
- The network bandwidth

Quoted statistics are from Azure UK Automated Backup:

- RPO 10 Minutes – Based on Compute Size and Database Activity
- RTO 12 Hours – Restore usually less than this, however could take longer, depending on size and activity

By default, databases are configured to restore to any point in the last 7 days.
Backups are stored using geo-redundant storage – 3 copies (Azure UK South), plus 3 copies in a secondary region (Azure UK West)

Incident response and resolution SLAs:

- Microsoft SLA for Azure App Service and Azure SQL Elastic Pool as above
- Katchr support response in normal business working hours Monday to Friday

Patch Management: how often is it performed and who is responsible?

Azure PaaS handles the cloud platform automatically. Katchr releases typically go out every 6 weeks with patches deployed in between if necessary.

User access: is 2FA available?

Multi Factor Authentication (MFA) will be handled by the client's AD configuration as part of the sign in process if using Azure AD federation.

What Cyber Protection controls are in place?

The Katchr cloud solution is periodically penetration-tested by our external security consultants.

The Katchr cloud solution is built on a serverless architecture, so there is no virtual machine or operating system requiring anti-virus protection.

The Azure environment itself provides built in DDoS protection.

What controls do you have in place to alert users and remediate any issues you experience with Third Party Software?

The Third Party Software is incorporated into the build of the Katchr software for each new version. It is then included into integration testing for that version, enabling us to identify any issues. Any issues of significance would either be documented as known issues in the release notes, or if judged serious, would delay the release of that version until resolved.