Platform Policy

Usama Musthafa - 2022-12-02 - Comments (0) - Formpipe Cloud General Information

Formpipe.cloud

Overview

This page outlines the Platform Policy for the Formpipe.Cloud platform.

Roles and Access Restrictions

Only the cloud services and support team staff have permanent access to Formpipe Cloud resources.

Members of the Formpipe delivery team may be granted temporary access to specific environments on a project-by-project basis.

All platform user accounts have Two-Factor Authentication (2FA) applied to mitigate the threat of account hijacking.

Access to customer environments via platform accounts is limited by default. Access is granted using on-demand privilege escalation for a limited time and is administered by us as the solution provider.

Uptime Commitments

We provide the following uptime commitments for each of our service tiers (excluding maintenance windows, planned downtime and agreed downtime):

Test: 99%
Standard: 99%
Premium: 99.5%

Infrastructure Security

All Partner and Customer connections to the service are accessible through the Gateway-based external access system.

Environments are partitioned into network segments and restrictions are applied to only allow specific communication between them.
Formpipe support is carried out only via authorised Formpipe addresses.

Data Security
Application traffic uses end-to-end transport layer encryption and/or application-specific encryption mechanisms (e.g. message-level encryption when sending payloads over other communication channels).
Data at rest is encrypted for Azure services and storage (Azure Blob Storage, and Azure SQL).
Environments have storage encryption applied and use Azure Key Vault to securely store encryption keys.

High Availability
Formpipe Cloud's Premium tier provides a highly available service by utilising multiple production nodes of our Lasernet product to provide increased resilience to node failures. These nodes are also spread across different data centre locations, providing resilience to data centre level disruption.

Backups
This applies to service components that hold data or configuration, such as:

- Service Nodes
- Databases
- Storage accounts

As part of Formpipe Cloud environments, Geo Redundant Storage (GRS) is utilized to offer a global multi datacentre level of redundancy for data and services. GRS allows the backup data to be replicated to another Azure region for additional redundancy. The weekly backup is stored for 4 weeks and the daily backup is stored for 7 days.

Key Vaults are by default protected with Zone Redundant Storage (ZRS). No further protection is required for this resource.

Disaster Recovery
Formpipe Cloud hosted environments provide Disaster Recovery by utilising Backups stored within Recovery Services Vaults. This provides replication of our production node backups to another geographical location.

This allows us to quickly restore nodes in a customer environment in a disaster scenario and provides resilience to geographic-level disruption.

The Recovery Time Objective (RTO) is set to 6 hours and a Recovery Point Objective (RPO) is set to 24 hours.

Platform Updates

Platform updates are applied in a controlled way.
To ensure we are up to date with the latest Microsoft patches, in particular security updates, we use the Update Management feature in Azure to schedule automatic deployment of updates to each node.

Nodes are split up into Four groups for patching:

Update Group - Test Group: Internal Test Nodes
Update Group 1: Test Nodes
Update Group 2: Primary Nodes
Update Group 3: Secondary Nodes

Regression testing is carried out on our internal test nodes to ensure that the functionality of the system is not affected prior to roll out of updates to customer environments.

Update Schedule:

Update Group - Test Group - Wednesday, the 2nd week of each month.
Update Group 1 - Monday, the 3rd week of each month.
Update Group 2 - Wednesday, the 4th week of each month.
Update Group 3 - Thursday, the 4th week of each month.

All updates are scheduled for 1 a.m. local time to customer region. The servers are set to reboot automatically if required.

Software Updates

Software updates are offered to the partner and end customer on a yearly basis. These upgrades require that the partner and customer undertake appropriate testing before any updates are applied to Production.
Releases that include critical bug or security fixes may be applied immediately if the potential risk of leaving the system unpatched is too high.
After the patch has been applied, the partner/customer will be sent a report detailing the changes and justification for applying an emergency change.

Rollbacks procedures are set in place for any uncommon circumstances.

Maintenance Policy

Day/time of the set maintenance windows are listed below:

Monday: 8 p.m. to 10 p.m. local time

Tuesday: 8 p.m. to 10 p.m. local time

Wednesday: 8 p.m. to 10 p.m. local time

Thursday: 8 p.m. to 10 p.m. local time

Related Content

- An Introduction to Formpipe Cloud