Your data is important *TO US*

Total Synergy's core values are respect, integrity, and care. Nowhere is this more evident than in our treatment of customers' data. Read on for details about how we keep your information safe, and private.

Customer on-premises backup

1. We believe that customers own their data.
2. Synergy cloud provides a built-in tool to manually extract a full backup of a customer database into an excel file.
3. Our roadmap includes an automation of this tool to export a customer backup weekly to an FTP site/email. This allows customers to automate downloading to an on-premises backup if they choose.

Monitoring

Synergy cloud is monitored using a combination of the following items:

a. Application insights used to continuously monitor for system exceptions, performance behavior, and anomalies.

b. Azure Alerts are used to monitor the environment – these are emailed to the team and are monitored proactively.

c. Pingdom is used to monitor the environment availability - SMSs are used to alert down time and immediately deal with it.

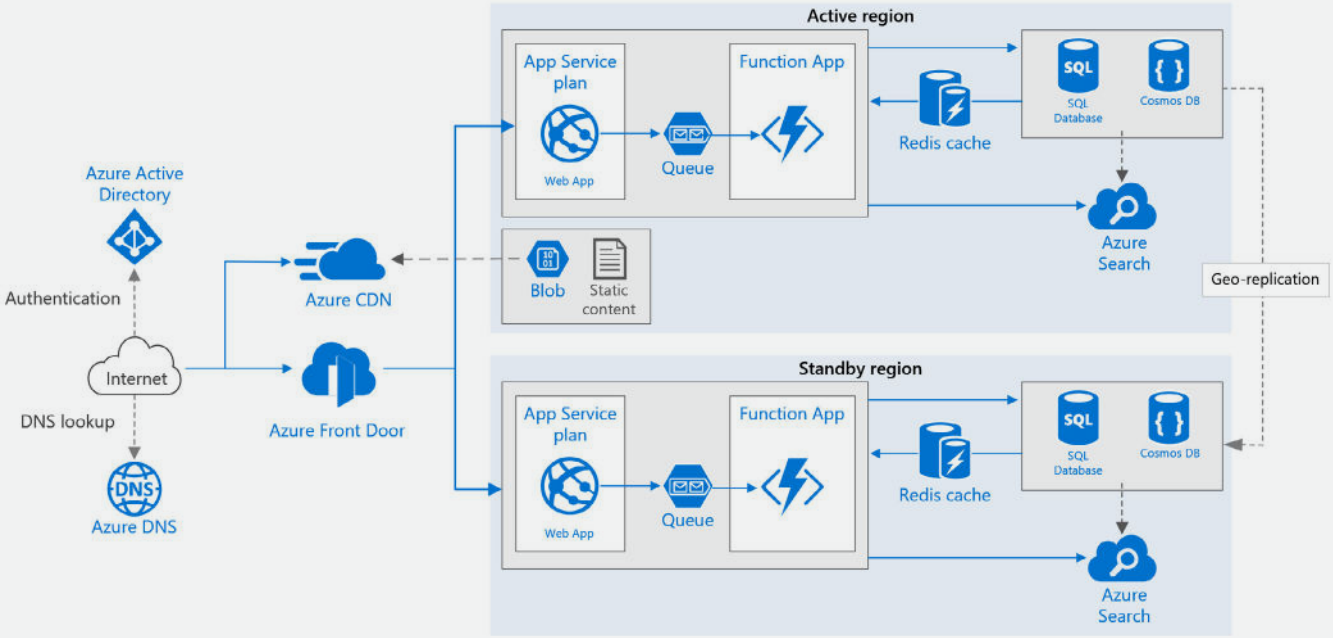
The set of three monitoring technologies, in addition to our 'follow the sun' support model, enables us to proactively reduce platform risks and achieve high availability.

Secure cloud architecture

To achieve a high level of availability for our Synergy web app, Total Synergy follows Azure reference architecture to run in multiple Azure regions. In general, Synergy cloud follows this architecture with subtle differences as follows:

1. Synergy cloud uses a separate DNS provider (not Azure DNS) to comply with Synergy DNS architecture.
2. Synergy cloud uses 'Azure Cloud Service' instead of 'Azure Function Apps' as this has proven to be most reliable and cost effective over the years of our usage.
3. Synergy cloud uses Azure SQL Database (not Cosmos DB).
4. We plan to use Azure Search in the future.
5. All components of Synergy cloud use either Azure Standard components or Azure Premium components to achieve high availability and high redundancy:
   - All components used have an uptime SLA of no less than 99.9%.
   - All customer data is geo-replicated and backed up (see diagram over page).

TOTAL SYNERGY



Backup and disaster recovery

1. Synergy cloud database (business data).
   a. The Synergy Cloud database uses multiple technologies for backup.
      i. Point-in-time restore is supported for the last 35 days of operation. We can restore the database to any point within the last 35 days.
      ii. Long term backup is used to backup the database in the following frequencies:
         1. 15 x weekly backups are stored.
         2. 12 x monthly backups are stored.
         3. 8 x yearly backups are stored.
   b. When restore is required (extremely rare).
      i. A new environment is built.
      ii. This environment is restored to an historical time as required.
      iii. Data can then be inspected or even fixed for one or multiple tenants by querying the data from the restored database and comparing it to the data in the production database.
      iv. A restore takes between 2-4 hours.
2. Synergy cloud 'blobs' (files).
   Blobs host files uploaded to the cloud.
   a. A blob versioning solution is implemented in code to make sure files are never deleted. Any new file created gets a new version and the original file is stored and made available to the user as an old versioned file.
   b. For additional safety, soft delete is used to prevent data loss even if a blob is accidentally deleted. A retention policy of 200 days is used to prevent data loss for blobs accidentally being deleted.

Fault tolerance

Synergy cloud data is stored in Azure using platform-as-a-service (PaaS) components with high built-in availability. This solution involves several levels of protection to ensure that high availability.

1. Synergy cloud database.
   a. The Synergy database uses Azure SQL PaaS solution which guarantees availability (even when the machine running the SQL database fails). Microsoft guarantees 99.99% availability.
   b. The Synergy database is also geo-replicated (read-only replica) between two Azure regions - this guarantees availability in case of complete site failure.
2. Synergy cloud blobs (files).
   a. Synergy cloud uses geo-redundant storage to guarantee availability in case of complete site failure and Microsoft guarantees 99.99999999999999% (16 9's) durability of objects over a given year for Geo redundant storage. This solution replicates data between multiple disks in multiple regions to guarantee data availability.
3. Synergy application components (web app and cloud services).
   a. The synergy application components use a standby region technology to provide fault tolerance. A standby app server is available in a separate Azure environment to become primary in case of a fault scenario.

TOTAL SYNERGY

Security

1. Network security.
   a. The Synergy cloud internal data is not exposed to external networks - all data is secured behind a firewalled network and using strong passwords to prevent unauthorised access.
   b. Azure Vnets are used to separate internal Synergy cloud components from externally exposed components.
2. Infrastructure / operating system security.
   a. Synergy cloud is deployed on PaaS environment (no IaaS is used). Our PaaS services are hardened by Microsoft as part of the Azure hardening process.
   b. Synergy cloud is deployed on the Azure Web Apps service, which are hardened and secured by Microsoft as part of the web app platform release cycle.
3. Synergy cloud security.
   a. Synergy cloud supports the following login models:
      i. Username/Email and password.
      ii. Social login - (gmail/linkedin/Microsoft live account).
      iii. Microsoft Active Directory accounts.
      iv. Customers can enforce their organization to require active directory login - this feature can be combined with multi-factor authentication to provide a highly secured and integrated environment.
   b. Captcha is used to prevent brute force password attacks.
   c. The Synergy cloud APIs are protected using Oauth 2, which is documented in the developer integration guide.
4. Synergy cloud follows the GDPR 'secure by design' principles:
   a. All team members are trained on GDPR compliance.
   b. All internal and third-party components are checked for GDPR compatibility.
   c. All private data usage is governed by our Agreement and terms:
      - https://app.totalsynergy.com/Content/pdf/Synergy_Subscription_Agrement.pdf
      - https://totalsynergy.com/terms-of-use

Multi-tenant architecture

Synergy cloud is multi-tenanted. The key reasons for choosing a multi-tenant solution are:

1. Multi-tenancy reduces the cost per seat/user due to efficiencies achieved by sharing hardware between different tenants.
2. Multi-tenant solutions provide better performance over single-tenant solutions.
3. Multi-tenancy allows Synergy cloud to be upgraded as a whole application for all users - as an agile, fast delivery organization, we release new software monthly and make sure all tenants get the update on the same day, providing critical business value to all our customers.
4. On-boarding of new customers and software trialing periods are simpler in a multi-tenant solution as it enables us to provide multiple free trials for new and existing customers.
5. Multi-tenancy is simpler and faster to support, allowing us to offer a better customer experience.
6. Our API and integration vision (building an ecosystem of connected open apps) is scalable with a multi-tenant solution.
7. Our BI vision fits well with a multi-tenant solution.

To ensure data isolation between tenants, Synergy cloud uses a special data access layer which verifies the tenant correctness for each entity loaded from the database. Automatic code testing verifies our data isolation to make sure future code cannot break data isolation.

For more information or support, contact your customer success manager.

TOTAL SYNERGY