Infrastructure, Practices and Security Overview

Introduction

The ThinkSafe platform provides robust, scalable and secure capabilities for the rapid creation and deployment of connected, data-driven business applications. Our native app technology and cloud-based software utilises industry standard architectures built on world class, highly available hosted infrastructure.

Built on Microsoft Azure

ThinkSafe is hosted on Microsoft's Azure cloud infrastructure, which enables us to deliver highly scalable, available and fault tolerant services. Our application architecture has been designed to leverage Azure's strong geo-redundancy, replication and recovery options, and follows Microsoft recommended best practices and processes.

Azure meets a broad set of international and industry-specific security, privacy and compliance standards including ISO 27001, HIPAA, FedRAMP, SOC 1 and SOC 2, as well as country-specific standards like Australia IRAP, UK G-Cloud, and Singapore MTCS. More information, including white papers and other resources can be found at: https://azure.microsoft.com/en-us/support/trust-center

Operational Practices

ThinkSafe utilises industry standard tools and practices to perform software development, quality assurance, deployment and configuration during daily operations of the ThinkSafe platform.

Software and environment changes are versioned and committed to source control systems, with continuous integration tools providing automated testing and build procedures.

Application updates are deployed to a staging environment and then promoted to production using Azure's Virtual IP address mechanism to avoid downtime. In the event of issues with the new production deployment, we are able to immediately roll back to the prior stable version. All environmental aspects are defined via controlled configuration files, ensuring that application deployments execute on a consistent infrastructure and operating system environment.

We employ robust monitoring tools to log, analyse and constantly measure platform performance, availability and responsiveness. Automated alerts and notifications are raised when key measures approach acceptability limits, allowing our team to respond timeously and proactively to issues.

Data Replication and Backup

Data generated and stored on the ThinkSafe platform is replicated between two physical data centres via Azure's paired region approach. We utilise Azure geo-replication and geo-redundancy features for storage and database operations, guided by Microsoft recommended practices. Point in time backups are also automatically executed hourly for database and daily for general file storage.

System Failover and Disaster Recovery

Our application architecture follows best practices to ensure failover and recovery can occur across multiple levels and scenarios. At a hosting level, ThinkSafe is deployed across a primary and secondary data centre pair. These data centres are sufficiently physically distant from each other to reduce the likelihood of natural disasters, civil unrest, power outages, or physical network outages affecting both regions at once. In the event of tier failure or outright disaster, failover procedures will transition services from our primary to the secondary centre.

Network and Platform Security

ThinkSafe server instances run behind Azure's comprehensive firewall and load balancing solution. Inbound connections from both the Internet and remote management ports are blocked by default, with access tightly restricted to legitimate protocol and traffic only. All firewall configurations are version controlled and peer reviewed as part of our standard change management processes. For more information on Azure-specific security, refer to Microsoft's self-assessment paper here: https://cloudsecurityalliance.org/star-registrant/microsoft-azure

Backend access to ThinkSafe databases, storage accounts and server instances is restricted to qualified ThinkSafe team members only, with all actions performed using Microsoft provided management tools across SSL secured connections.

All app, web browser and REST API interactions with the ThinkSafe platform occur using 256 bit SSL/TLS encryption (HTTPS protocol). Users are required to log in with an email and password, and their login and access activity is recorded. API access is authenticated against a platform generated 32 character secret key token. Passwords stored on mobile devices and ThinkSafe servers are always encrypted using AES 256 bit encryption algorithms according to industry standard practices. When a user account is terminated or deactivated, an automatic wipe of local app data is executed when/if the user next attempts to access the app.