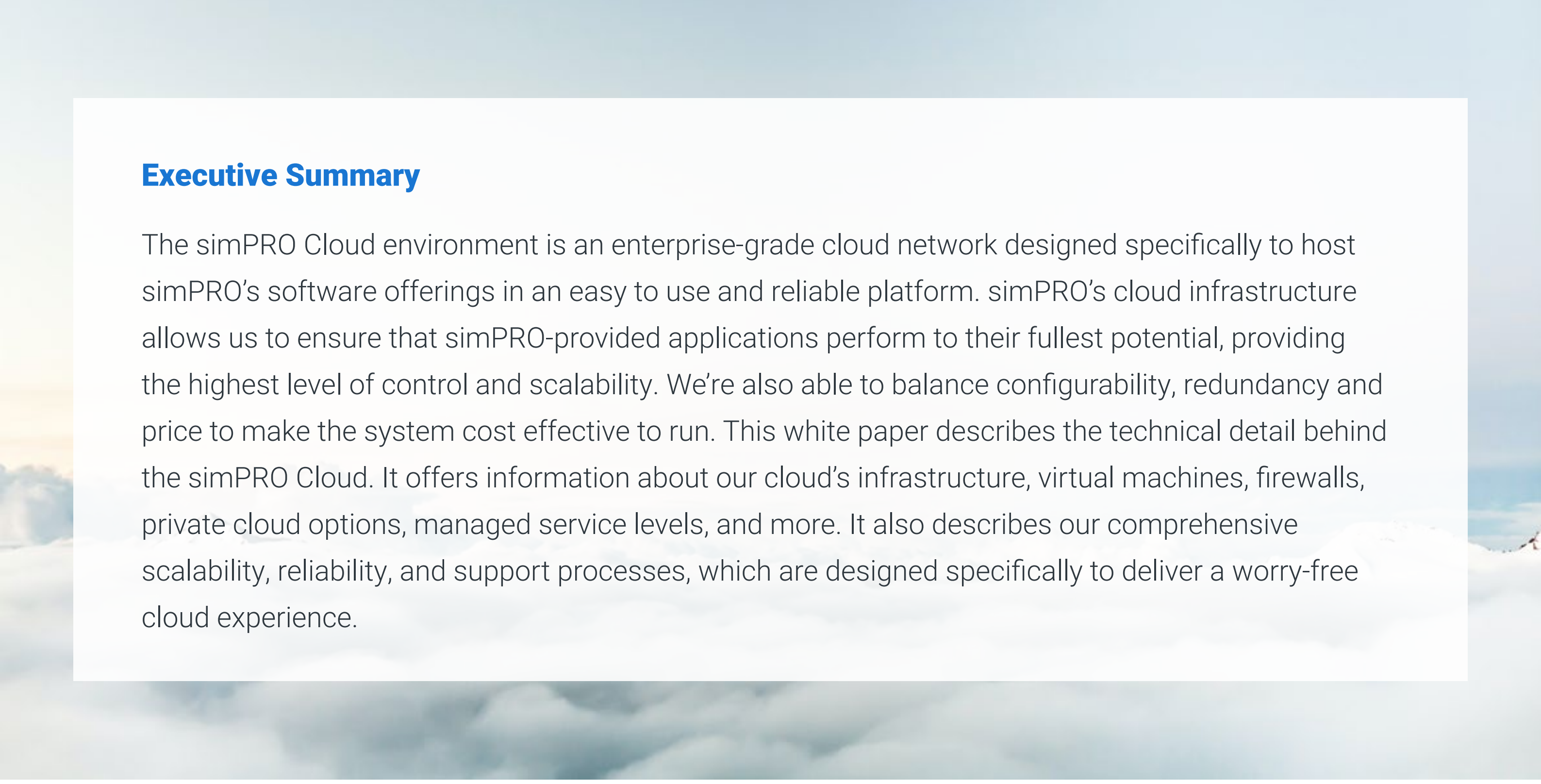
simPRO

The simPRO Cloud



Executive Summary

The simPRO Cloud environment is an enterprise-grade cloud network designed specifically to host simPRO's software offerings in an easy to use and reliable platform. simPRO's cloud infrastructure allows us to ensure that simPRO-provided applications perform to their fullest potential, providing the highest level of control and scalability. We're also able to balance configurability, redundancy and price to make the system cost effective to run. This white paper describes the technical detail behind the simPRO Cloud. It offers information about our cloud's infrastructure, virtual machines, firewalls, private cloud options, managed service levels, and more. It also describes our comprehensive scalability, reliability, and support processes, which are designed specifically to deliver a worry-free cloud experience.

Cloud Overview

simPRO's cloud environment is a highly available multi-tenant platform architected specifically around superior performance, availability and data protection. The simPRO Cloud spans across data centers in multiple locations globally to ensure reliability and data protection in case of major impact events. simPRO's cloud also enables our engineering team to deploy and support simPRO systems quickly while avoiding issues encountered with on-premise installations and configuration. Some of the benefits that our simPRO Cloud customers can expect when using our service include:

- Automated Software Updates
- 99.5% Service Level Agreement (SLA)
- 24x7 Systems Availability
- Nightly Automated Client Snapshots
- 24x7 Proactive Monitoring
- CapEx Free
- Easy Remote / Mobility Access

There are also a range of security and redundancy systems designed to improve the speed, reliability, stability and security of the simPRO Cloud.

Global Data Center Network

The simPRO Cloud is spread across multiple geographically separated data centers on premier tier one providers such as the leading global data center provider Equinix. They were chosen because of their ability to provide a best of breed platform, on which we were able to build a highly scalable cloud network. simPRO employs its own specialist engineering team to design, deploy, and manage its cloud network with an operations center based in Australia. The team manages the simPRO worldwide network on a 24/7 basis with escalation available to each data center around the clock.

The data centers employed by simPRO have multiple locations including offices in Australia, New Zealand, the USA and the UK. Each office has been configured to run as an integral part of the overall global network - however each center can also run as an independent cloud when required to accommodate for network transmission and other data center unavailability autonomously.

Cloud Architecture

Each cloud in the simPRO data center network is comprised of a range of load balancers, storage arrays, web servers and database servers all synchronously connected to each of the other data centers. This allows for a geographically fault tolerant network and maximizes uptime of simPRO services. The simPRO Cloud is built on technologies and software from leading providers such as Cisco, KVM, FreeBSD, PostgreSQL and Lighttpd. All systems employed have been rigorously tested and are tailored specifically for use on the simPRO network.

Primary Objectives

1. Reliability

The simPRO Cloud utilizes the latest available load balancing and acceleration technologies to ensure we are able to provide a highly consistent operating environment. This includes the ability for our systems to automatically redirect traffic away from outages whilst ensuring performance degradation is kept to a minimum.

2. Performance

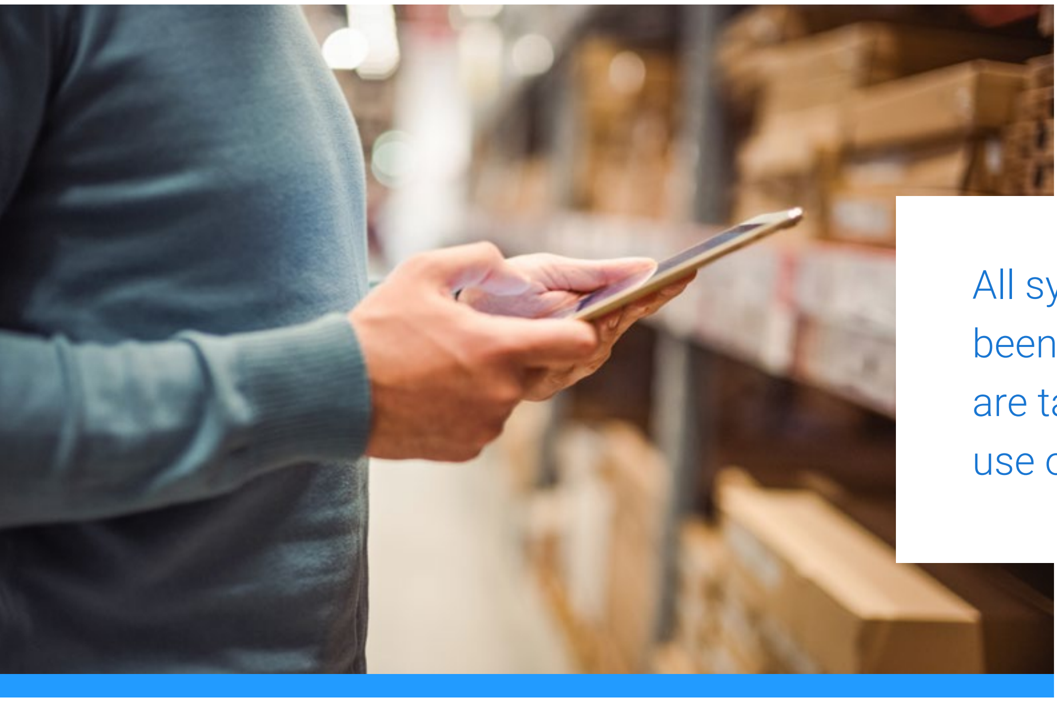
Performance of each system is monitored 24/7 by both automated systems and our engineering team. System performance is managed through a range of automated processes that load balance services across data centers and can provide added capacity when required. Automated geographic configuration enables the system to re-route client access to alternative points based on load in each data center so that traffic spikes in one geographic area can be accommodated and mitigated.

3. Security

Our security systems encompass both server and data. A range of processes are used across servers to ensure that the best proactive security measures are adhered to at a systems level. Monitoring of all events and access is also conducted in real time along with monthly reviews. Data storage is segregated across private networks within each data center and not made accessible on public networks.

4. Scalability

Each system and service within the simPRO Cloud is designed to scale horizontally so that service capacity can be increased as required to meet growing demand in real time. Overhead allocation also ensures that the system has plenty of headroom to handle load spikes.



All systems employed have been rigorously tested and are tailored specifically for use on the simPRO network.

Data Security

Data security has and always will be a primary focus of both our engineering and development processes. We've published policies on how we deal with data on our website.

Visit:

- Privacy policy
- Personal data protection policy

Each data center and peering point selected are based within countries that are signatories to cross border privacy enforcement agreements. The data centers employed are world-class facilities and SOC 2 accredited. SOC 2 accreditation stipulates no public access to the data center floor at any time.

Each data center has systems in place to securely encrypt all data during replication to other data, centers as all data in the simPRO network is synchronously replicated across the centers for maximum data integrity.

At a systems level, a range of private networks and firewalls are employed within the primary stages of each data center installation to ensure segregation of systems where required. This also serves to firewall data stored so that it is inaccessible from public networks and can only be accessed securely by applications over encrypted private network services.

The simplest way to explain our overall data protection policy is that all production environments are secured and selected for PCI compliance to ensure maximum security of housed data - and to limit access to such data even at the server administration level. PCI compliance is the same strict standard adhered to by banks and credit card companies when handling financial and transaction information.

Clients with policies around offshore storage of sensitive data should contact simPRO to ensure that the storage of their data within the simPRO network meets these policies. simPRO can provide private cloud installations to overcome issues around offshore storage of data and any other geographic data access/hosting policies.

Certification and Testing Standards

A range of certifications are employed to provide formalized processes around handling of physical and application security. These include the following:

Infrastructure (DC) Certification

- ISO 27001 Certified
- PCI-DSS Certified
- SOC 2 Type I/II Certified
- GDPR and CDSA Content Protection and Security Standard Compliant

Application Testing Standards

- ISO/IEC 27001 (using the PDCA model)
- ISO 27001:2005
- ISO 9001:2008 (under review for adoption and certification)
- ISO27002:2013 (under review for adoption)
- SoGP
- OWASP

Data Redundancy

Each data center has multiple levels of redundancy to ensure data integrity.

Database Data

All active database servers are replicated in real time to secondary servers within the same data center. This means that every time a transaction occurs on the database, the exact same transaction occurs on the secondary servers. In the unlikely event of a problem occurring on the primary server, we can switch users to the secondary server without any loss of data.

File Data

All file data is replicated in real time across all data centers and slave file servers are kept hot for failover purposes. Data can also be segregated at a server level during maintenance and outages and resynced automatically on service restoration prior to re-inclusion in the cloud pool.

Snapshots

Whilst the range of systems in place are designed to ensure against failure we still adopt a catastrophic event approach to data security as well. All database and file data (including file attachments, databases and customization code) is snapshotted every 24 hours and then archived on a backup private network within each data center in the event of catastrophic failure. This ensures that in the event of a failure across our data center network we have the ability to fall back to the previous night’s backups should the need ever arise.