Solvace SAAS SUITE FOR BUILDING EXCELLENCE CAPABILITIES

SECURITY & PRIVACY REFERENCE

This Security & Privacy reference was last updated on May 12th, 2018.

1 DATA CENTER SECURITY

Services run on infrastructure from Rackspace, an IT hosting company with SOC 2, SOC 3 and ISO 27001 security certifications and compliance verifications. The full list is maintained at https://www.rackspace.com/compliance.

A few key facts about Rackspace's infrastructure:

Factor	Description
Network	• 9 network providers, for multiple redundancies • 219 CDN edge locations on 6 continents optimize content delivery: North America (77); Europe (36); Asia-Pacific (70); Africa (17); South America (15); Middle East (4) • Fiber carriers enter at disparate points to guard against failure • Network topology and configuration automatically improves in real time • Configuration, co-developed by Rackspace and Cisco, guards against single points of failure at the shared network • Cisco and Arbor Networks work with Rackspace to continually improve monitoring and security
Precision environment	• N+1 redundant HVAC (Heating Ventilation Air Conditioning) system • Every 90 seconds, all air is circulated and filtered to remove dust and contaminants • Advanced fire suppression systems

Core routing equipment	• Fully redundant, enterprise-class routing equipment only • Fiber carriers enter at disparate points to guard against service failure • Application updates do not involve any noticeable downtime
Physical security	• Keycard protocols, biometric scanning protocols, and around-the-clock interior and exterior surveillance • Access limited to authorized data center personnel; no one else can enter the production area without prior clearance and appropriate escort • Every data center employee undergoes multiple and thorough background security checks before hire
Conditioned power	• UPS (Uninterruptible Power Supply) for all servers • N+1 redundant UPS power subsystem, with instantaneous failover if the primary UPS fails • If an extended utility power outage occurs, our routinely tested, on-site diesel generators can run indefinitely
Network technicians	• Networking and security teams must be certified and thoroughly experienced in managing and monitoring enterprise-level networks • Our Certified Network Technicians are trained to the highest industry standards

2 SYSTEM SECURITY

Services are operated on Cloud Servers with a hardened Linux distribution (currently Ubuntu 16.04 LTS). Cloud Servers exchange information with each other through a dedicated virtual network.

3 APPLICATION SECURITY

3.1. User authentication

Users authenticate to the Services through the use of single sign-on authentication logic, available for around 175 third-party services, from Google to Microsoft to LDAP. The full list of available services is maintained at https://github.com/intridea/omniauth/wiki/List-of-Strategies.

Services also feature a built-in authentication mechanism with email validation. Passwords of the built-in authentication mechanism are encrypted using BCrypt. Passwords can be set to automatically expire at a specified interval.

3.2. User authorization

Access control to models, controllers and views across the Services is defined in a single authorization logic file.

3.3. Code releases

Manual and automated testing is conducted for each code release of the Services. Automated testing includes unit tests, integration tests, and code quality tests.

4 DATA TRANSFER SECURITY

All client-server communication is encrypted using TLS 1.2. A securely configured SSH setup is in place for all system administration access.

5 LOGGING AND MONITORING

Rackspace actively monitors the data center environment (power access, temperature, access), network and servers, and notifies Supplier as soon as any issues are identified. Automated tickets are immediately opened to address any issues.

Supplier uses robust monitoring solutions (New Relic, Pingdom, StatusCake) to proactively monitor hardware and the Services around the clock in order to maintain uptime and proactively resolve issues. Automated notifications are in place to notify Supplier of issues or outages.

6 BACKUPS AND DISASTER RECOVERY

Customer Data are backed up to Rackspace cloud files service which replicates three full copies on different storage nodes. Backup files are encrypted using AES-256-CBC. Only authorized users can access backup files.

Supplier performs disaster recovery exercises on at least quarterly basis. They include a variety of tests to validate adequate recovery times.

7 INCIDENT MANAGEMENT AND NOTIFICATION

Supplier has implemented and maintains security incident management policies and procedures. Supplier will promptly notify any impacted customer of verified or believed security incidents, such as any unauthorized disclosure of Customer Data, to the extent not prohibited by law, regulation or the order of any court or legal authority.