Understanding Sage CRM Cloud

Data centre and platform security whitepaper

Document version 2016

Table of Contents

1.0 Introduction

Ensuring the availability, reliability, security and performance of mission-critical applications is a growing challenge for today's organisations. This is particularly important to small and medium businesses with limited IT resources. As a result, an increasing number of companies are turning to software-as-a-service or cloud providers to minimise the infrastructural complexity and overhead associated with these applications. As such, the use of on-demand CRM, such as Sage CRM Cloud, has become widely adopted, particularly for companies looking to implement a Customer Relationship Management (CRM) solution for the first time.

While most companies will focus on functionality and subscription charges when comparing cloud-based CRM providers, the potential supplier's data centre facilities are generally overlooked. Security, availability and performance are considered to be givens. This however, is a precarious assumption to make. In reality, there is significant variance between potential suppliers in this area and companies should give careful consideration to the facilities and provisions that have been put in place to protect their data and ensure suitable performance and availability for their business.

This document is aimed at providing public releasable information about the leading-edge data centre facilities that underpin the security, performance and availability of the Sage CRM Cloud Platform through our global data centre partner Rackspace Limited. This document will provide an overview of the data centre infrastructure, platform security and the independent audits and reviews employed by Sage and Rackspace to ensure that the risk of compromise is kept to a minimum at all times.

2.0 Sage CRM Cloud Data centre Infrastructure

2.1 Site location

The Sage CRM Cloud platform is currently hosted with our data centre partner, Rackspace Limited., across two of their data centre facilities, located in the United States and the United Kingdom.

These data centre locations were chosen due to the fact that there are no major geographic risk based FEMA criteria; the area is not prone to seismic activity, floods, tornadoes or hurricanes. The data centre is located in an area where the risk of man-made disasters is low. Rackspace personnel are on duty 24 hours a day, 7 days a week at all of Rackspace's data centre facilities.

2.2 Infrastructure – Electrical power

he data centres are equipped with Uninterruptible Power Supplies (UPS) to mitigate the risk of short-term utility power failures and fluctuations. The UPS power subsystems are N+1 redundant with instantaneous failover in the event of a primary UPS failure. The UPS systems are inspected at least twice annually. Both data centre facilities are equipped with diesel generators to mitigate the risk of long-term utility power failures and fluctuations. Generators are regularly tested and maintained to provide assurance of appropriate operability in the event of an emergency.

2.3 Infrastructure – Heating, ventilation, air conditioning

The data centres feature N+1 redundant Heating Ventilation Air Conditioning (HVAC) units, which provide consistent temperature and humidity within the raised floor area. HVAC systems and chillers are inspected regularly (at least quarterly) and air filters are changed periodically. Redundant lines of communication to telecommunication providers provide Rackspace customers with failover communication paths in the event of data communications interruption.

2.4 Infrastructure – Fire suppression and detection

The data centres are equipped with sensors, including smoke detectors, and floor water detectors, to ensure the detection of environmental hazards. In addition to this, the data centre facilities are equipped with raised flooring to protect hardware and communications equipment from water damage. The data centres are also equipped with fire detection and suppression systems and fire extinguishers, all of which are inspected at least twice annually.

2.5 Infrastructure - Physical security

The security of the data centre is considered paramount; best practice procedures are in place to ensure the highest levels of security for customer data. Two-factor authentication is required to gain access to the data centre facilities and electromechanical locks are controlled by biometric authentication and a key-card/badge. Access to secure sub-areas

is allocated on a role specific basis and only authorised data centre personnel have access to data halls.

Rackspace employees utilise proximity badges and access cards to enter the building. Only employees with a business need for access to the server floor or other secure data centre areas are provided such access. Employee entry access is controlled by two-factor authentication (biometric authentication and proximity access cards). Rackspace policy strictly prohibits employees from tailgating at the data centres. Additionally, visitors must be escorted at all times and are strictly forbidden from accessing the data halls themselves.

All entrance points, on the interior and exterior of the buildings housing data centres are secured with 24/7 monitored closed circuit video surveillance. Cameras support data retention for 90 days and are monitored 24/7 by on-site security personnel. Sensitive equipment such as plant and information processing facilities, including customer servers, are housed in secure sub areas within the secure perimeter and are subject to additional controls.

Centralised Security Management Systems are deployed at all data centres to control the Electronic Access Control Systems and CCTV networks. The data centres maintain 24/7/365 monitored CCTV coverage, with CCTV/DVRs supporting data retention for 90 days due to PCI compliance requirements.

Visitor access to the data centres must be granted by appointed authorised approvers before the scheduled visit meaning unauthorised visitors are not permitted access to the data centres. When commencing a visit to the data centre, all visitors must present photographic ID when logging in and are strictly escorted at all times. All visitor access is logged, this policy applies equally to Rackspace employees not assigned to the data centre in question. Visitors, including customers, are strictly forbidden from accessing the data halls themselves and other secure sub areas.

Appropriate additional perimeter defence measures, such as walls, fencing, gates and anti-vehicle controls are in place at Rackspace data centre locations. The delivery and loading bays at all data centres are separate areas secured by defined procedures and security controls.

2.6 Infrastructure – Monitoring

The Rackspace Network Operations Centres (NOCs) continually monitor the health and performance of the data centres on a 24/7/365 basis.

The data centres are also monitored 24/7 by Building Management Systems and dedicated engineering teams.

2.7 Infrastructure – Network

The data centre network has been engineered from the ground up to accommodate the high availability demands of outsourced solutions. The Rackspace NOC continually monitor the health and performance of the network and add capacity as required.

3.0 Sage CRM Cloud Platform Security

3.1 External firewalls

A redundant pair of Stateful Inspection Firewalls is used to provide controlled access to the Sage CRM Cloud Platform. These firewalls provide the initial and essential network security functions by applying security policies to all inbound and outbound traffic. These firewall policies have peer review audits conducted monthly, as well as bimonthly external validation from vulnerability audits.

3.2 Intrusion and malicious software detection

In addition to the secure firewall architecture, Rackspace monitor their internal networks and have security systems in place to identify incidents of network intrusion or malicious software. All servers have enterprise class anti-virus and malware protection installed, monitored and regularly updated.

3.3 Secure systems management

Each server is scanned daily and swept for virus patterns ensuring infected files are automatically cleaned, quarantined or deleted. Notifications of the detection, cleansing or deletion are sent to the NOC where they are recorded.

3.4 Secure data connectivity utilising SSL certificates

By utilising Secure Sockets Layer (SSL) certificates, all transfers of customer data from the customer to the Sage CRM Cloud Platform are encrypted using SSL. The secure connection between the client and our services is encrypted using 2048bit key and certificates.

3.5 Restricted access

There is a strict access policy that prevents unauthorised access to the Sage CRM Cloud Platform. Access to the operating system, application and data storage is limited to the Sage CRM Cloud and Rackspace Operations Teams. There is a strict no access policy given to individuals outside of these teams.

3.6 Identity management

Administrative changes to the application may only be carried out by the authorised administrator, whereby their email address has been registered in the application. This prevents unauthorised access to the application configuration and prevents an unauthorised backup of the customer's database being taken.

3.7 User authorisation

Access to the Sage CRM Cloud application is controlled by a username and password. This only gives access to the customer's Sage CRM Cloud account. User rights, once in the application, are dependent upon the level of security set by the customer's CRM administrator.

3.8 Real-time application monitoring

Application and platform monitoring is carried out 24/7. This is automated and provides notification of a failure or impending failure of the application or component of the infrastructure.

4.0 Verification

4.1 Vulnerability audits

The security of the data centre is validated by Rackspace, with an external network vulnerability audit carried out on a regular basis. In addition to this, Sage CRM carries out ad-hoc security checks against its own platform, exclusive of any Rackspace testing. This security review includes validating the Sage CRM Cloud application and platform against the Open Web Application Security Project (OWASP) top ten application security risks, as well as other important and confidential security aspects. The results of these audits are confidential and are not shared outside of the Sage CRM management team.

4.2 Data centre certification

Rackspace data centres have been audited and certified to leading industry standards. Further details of these accreditations can be found below. For more detailed information on the Rackspace data centre accreditations please visit the Rackspace website (www.rackspace.co.uk/about-us/accreditations/).

ISO 27001:2005 (Information Security)
This standard provides a framework for managing a business' security responsibilities and provides external assurance for customers as to the scope and scale of the Rackspace secure environment via Rackspace Business Security Management System. It is subject to on-going external assessment by Certification Europe with a full re-assessment every three years.

ISAE 3402 Type II Service Organisation Control

Rackspace utilises this globally recognised standard for reporting on service organisation controls to demonstrate that selected Rackspace processes, procedures and controls have been formally evaluated and tested by an independent accounting and auditing company (service auditor) for their managed hosting customers, cloud servers & cloud files customers and all of their data centres. The examination includes controls relating to security monitoring, change management, service delivery, support services, back-up, environmental controls, logical and physical access and provides a detailed description of Rackspace controls and the effectiveness of those controls.

Rackspace has worked with the service auditor to have the report issued with a joint opinion that satisfies the requirements of both the ISAE 3402 and the SSAE 16 (created by AICPA (American Institute of Certified Public Accountants) for use in the US mirroring ISAE 3402).

This is a rigorous audit repeated on an annual basis for each reporting period and is carried out by external auditors on behalf of Rackspace.

ISO 14001:2004 (Environmental Management)

Rackspace takes its environmental responsibilities seriously, from ensuring they provide a safe and healthy working environment to their commitments to the wider world, legally and morally.

In support of this, the Rackspace UK data centre and head offices are certified to the international environmental management standard, ISO 14001, which provides a framework for managing environmental responsibilities, including energy and waste management

It is subject to on-going external assessment by the certification body, BSI (British Standards Institution), with a full re-assessment every three years.

For further information on the information contained within this document, please contact your local Sage office.