Comark Cloud Security Overview

Issue 1 – Oct 2019

Introduction

The Comark Cloud service is owned and managed by an approved UK based third-party supplier. All access to the database and customer information is strictly controlled.

All procedures and work is carried out within the guidelines of the UK Data Protection Act 1988 and General Data Protection Regulation (GDPR).

Data Centre

The Comark Cloud service is run using servers hosted and maintained by Rackspace in the UK. Rackspace is a subsidiary of Rackspace Inc and is an internationally renowned provider of Cloud computing servers and associated services. Rackspace UK provides security certifications to;

- ISO 27001:2005
- Level 1 Payment Card Industry (PCI) Service Provider
- SSAE16 Type II SOC1, SOC2 (Security & Availability Only) and SOC3
- Safe Harbour Certified
- CDSA Content Protection and Security Standard Certified

Comark or any other Rackspace customers are not physically allowed access to the servers within the datacenter.

Rackspace provides effective protection and mitigation from distributed denial of service attacks (DDoS).

Servers

Main Web Server: Windows Server 2012 R2

Main Database: Linux CentOS & MySQL

Servers and databases will have security and update patches applied as and when necessary to minimize downtime. Patches that are critical will be applied within 24 hours.

Customers will be advised via email at least 24 hours prior to any scheduled maintenance window that could result in a temporary loss of service.

Workforce Security

Access to customer's data is strictly controlled.

Direct access to the servers and database is reserved for the 3rd party senior management team.

Comark Instruments
52 Hurricane Way, Norwich, Norfolk, NR6 6JB, UK
Tel: +44 207 942 0712
www.comarkinstruments.com

Comark Instruments
PO Box 500, Beaverton, OR 97077, USA
Tel (503) 643 5204
www.comarkUSA.com

User Passwords

Passwords for user accounts must be at least 8 characters long and must contain a number and an upper-case character.

Passwords for access to the servers are independent to that of users.

Backup & Disaster Recovery

The main database is comprised of two sets of dedicated hardware configured in a master – slave configuration. In the event of a failure of the master database the slave will automatically take over the role of the database within 15-30 seconds.

The Comark Cloud is backed up every 24 hours and backups are kept for 2 weeks. In the event of a total loss of systems new servers and databases along with a restore of the last backup point will take place within a 24-hour period.

The backup system is designed to restore a system in the event of failure, not to recover deleted records.

Data Deletion

Once a customer chooses to close their Comark Cloud account all their data including account details will be permanently deleted from the Comark Cloud database. Once data has been deleted from the cloud, it is not possible for it to be recovered beyond that of a backup.

Auto Logout

Once signed in to the Comark Cloud and there is no activity on a user account, the user will be automatically logged out. Each user can individually configure the auto log out interval or turn this feature off.

Data Transmission

All user access to the cloud is done using HTTPS, an encrypted version of HTTP. Only port 443 is available for HTTPS communications. HTTPS data uses TLS encryption methods. HTTP port 80 is open but will redirect to HTTPS.

All data sent by the WiFi sensors to the Comark Cloud is done in a non-human readable proprietary format. Only TCP port 14354 is available for sensor communications.

The sensors do not offer any kind of web page and will not respond to any request on any port other than required by essential network services e.g. DHCP.

The sensor does not offer any kind of web page and will not respond to requests on typical HTTP ports 80 and 443.

The WiFi sensor will turn its radio off between WiFi transmissions and will not respond to communication.

When the sensor is ready to send logged data to the Comark Cloud it will enable the radio, re-establish connection to the WiFi network and initiate a TCP connection on port 14354 to the Comark Cloud. The Comark Cloud never initiates, polls or pings any connection to the sensor.

The sensor does require a DNS service and will use the DNS service IP address as directed by DHCP to resolve the URL https://comark.wifisensorcloud.com/

If the sensor is configured for static IP then it will revert to using either Google DNS (8.8.8.8) or OpenDNS (208.67.222.222) for DNS

Firewall

The servers are protected by a dedicated firewall. Only TCP ports 80, 443 and 14354 are accessible to users. Ports required for maintenance of the servers are locked down so access can only be from Comark offices.

Security Compliance

Trustwave PCI Compliance: Pass

Qualys SSL labs scan: A

WiFi Sensors

The WiFi sensors are compatible to the 802.11 b, g and n (2.4GHz) standard. The sensors support the following WiFi encryption and authentication methods.

- WEP
- WPA
- WPA-2 Personal
- WPA-2 Enterprise, including
    - PEAP
    - TTLS
    - FAST

Note; TLS1.2 as the underlying encryption on PEAP is not currently supported on RF400. RF300 Loggers with firmware version 5.5.x do support it. Please contact Comark for more information.

All information such as access point passwords is stored securely in the WiFi sensor and it is not possible to read out such information.