Managed Firewall Service

Service Definition

G Cloud 15

Lot 2a – Infrastructure Software as a Service (iSaaS)

January 2026

redcentric

AGILE • AVAILABLE • ASSURED

Contents

1. Service Description

Managed Firewall Service is delivered on virtual firewalls on a shared platform, or where required, on one or more dedicated hardware firewall appliances. The firewall(s) control traffic between devices on different networks providing a degree of perimeter protection. The firewall is configured to meet a customer's specific requirements. Redcentric monitors the firewall for hardware failure and other alerts and staff manage the firewall configuration and provide advice on proposed configuration changes.

1.1 Feature Summary

- Based on cost-effective, highly available virtual-firewall platform
- Available at multiple locations for geographic diversity
- Dedicated single or high availability firewall appliance pairs also available
- Appliance firewalls can be deployed on a customer's site or within a Redcentric data centre
- Layer-7, application aware firewalling as standard
- Unified Threat Management (UTM) functionality options
- Portal access to configuration, dashboard, and reporting
- Support for site-to-site virtual private networks (VPN)
- Support for client VPNs for remote workers
- Fully configurable rule-base managed by Redcentric trained professionals
- Customers receive advice and guidance on the effectiveness of the implemented rule-base, and any proposed changes.

Also available are dedicated appliance firewalls from specific vendors where some of the features above are not offered.

Zero Touch Network Access (ZTNA) and Endpoint Management Services are available as an added option to enhance the firewall functionality and features.

1.2 Tailored Managed Firewall Service solutions

The capabilities detailed in this section are based on a comprehensive set of products from a single vendor. Redcentric also specifies, deploys, monitors, and manages firewalls from other vendors to meet specific customer requirements. For these solutions, the features and capabilities detailed in the sections below may not necessarily apply.

1.3 Firewall platform

The platform delivers an extremely robust, flexible, and cost-effective virtual firewall solution to meets the needs of most customers. The platform is built using resilient components, so Service Availability is very high. Additionally, the platform is present at several key locations, which supports disaster recovery design objectives.

Customers may elect to deploy dedicated firewall appliances where their requirements or policy dictates:

- Physical deployment of appliances is required at a customer site
- Dedicated firewall appliance infrastructure is required
- Bandwidth throughput and/or other resources exceed those available on virtual firewalls

Please see below for details.

1.4 Virtual Firewall Resource Specification

Redcentric currently offers two virtual firewalls sizes. Specifications are detailed below:

Resource	Size 1	Size 2	Size 3	Size 4
L7 Bandwidth throughput Mbps	50	200	500	1000
Sessions	60000	240000	500000	500000
IP Sec S2S VPN	25	50	100	200
Remote User VPN	5	10	15	30
Firewall Policy	1000	2000	4000	5000
Locally Configured Users	20	50	65	100

Other resources (e.g. proxy-services & address definitions, virtual-IP addresses etc.) are allocated on a fair-use basis. In the rare case that a customer consumes one or more of these resources excessively, they will be given the option to reduce consumption, upgrade to a higher specification virtual firewall or migrate to dedicated appliance(s) at additional cost.

1.5 Portal access

One major feature of the Managed Firewall Service is the customer access portal. Managed Firewall Service customer access portal provides the following capabilities:

- View configuration, policies, objects, and profiles
- Access near-real-time analytic dashboard
- Access and generate pre-defined reports
- Inspect real-time log view (application, attack etc.)
- Offers the ability to make minor configuration changes customers are issued with a portal user guide that explains how to access information and undertake tasks.

1.6 Account Set-up and Permissions

Redcentric staff set-up or modify customer administrator portal accounts during initial set-up or throughout the Service Period.

1.7 Viewing Configuration

Customers can use the portal to view firewall ruleset, objects and addresses etc. customers taking the Advanced service option can also view UTM configuration details.

1.8 Minor Configuration Changes

Redcentric support staff manage the configuration on the firewall, evaluating and implementing formal change requests submitted by the customer. If required, customer administrators may be issued credentials for the portal which will allow them to make configuration changes. The aspects of the configuration that can be modified by the customer's administrator is limited to those that will not have major impact on the overall level of security the firewall provides. The list of aspects is subject to change but is currently limited to:

- Content-filter policy including modification of exception (AKA black/white) lists
- Database of user credentials required for remote access VPNs

The customer agrees to reasonable charges for fault investigation work where faults are traced to issues resulting from configuration changes made by the customer.

1.9 Logging

The platform stores traffic log data so that it can be analysed and used in reports. Managed Firewall Service recurring charge includes 25GB storage. For most customers this storage volume is sufficient to retain a good level of log and analytical information for several months. Customers can optionally extend this volume for an additional charge.

By default, the platform will be configured with a 90%:10% allocation of log vs archive analytic data where old data is overwritten. Consequently, Redcentric makes no commitment to make log data available medium to long term.

1.10 Reporting

The following reports are configured on the platform:

- Bandwidth and Applications Report
- Cyber Threat Assessment
- Hourly Website Hits
- Top 20 Categories & Applications (Bandwidth)
- Top 20 Categories & Applications (Sessions)
- Top Allowed and Blocked with Timestamps

The customer administrator can run and access these reports via the portal.

Redcentric staff can set-up or tailor other reports limited by the capability of the platform, as a chargeable Professional Services exercise.

1.11 Alternative Dedicated Appliance Option

Redcentric will specify, design, and deploy dedicated firewall appliances to meet specific customer needs where virtual firewalls are unsuitable. Firewalls are chosen from a range that is compatible with the service options and portal capability.

1.12 Service Versions

Regardless of the customer's choice of virtual firewalls or dedicated appliance(s), Redcentric offers three service options, as detailed below:

- Standard
- Advanced
- Static-configuration

The Standard service delivers a high level of perimeter security based on Layer-7 application-aware firewalling performing network address translation with a level of denial-of-service capability (e.g. Mitigate sync. packet flooding).

The Advanced service builds on the Standard service by additionally offering three Unified Threat Management functions: Anti-virus, web filtering and intrusion detection.

The Static-configuration option is particularly cost-effective and suitable for environments where the ruleset is dictated by a governing body and rarely changes (e.g. where a firewall protects the interface to certain public sector networks). UTM functionality is not included. To minimise costs and service charges, fewer change requests are accepted for the static configuration option. No portal access is provided to the customer using a static configuration option. Redcentric recommends the standard or Advance service for all customers using the firewall to protect their enterprise network edge.

2. Service Options

Redcentric offers several managed services that complement the Managed Firewall Service including an extensive connectivity portfolio and a variety of pay-as-you-use unified communications, compute, storage, and hosting services. Redcentric Two-Factor Authentication service can be integrated with Managed Firewall Service to provide secure, remote access solutions for remote and home-working staff.

As an alternative to the managed service, Redcentric is happy to work with customers to specify, deploy and configure devices including firewalls as part of a Professional Services project.

2.1 Address Translation and remote connections

2.1.1 Network and Port Address Translation

The firewalls are configured to translate addresses as part of the standard security implementation. Depending upon the number of addresses available and the required functionality, network address translation (NAT), port address translation (PAT), or a combination of the two may be deployed.

2.1.2 Site-to-site Virtual Private Networks

Redcentric supports secure, authenticated, and encrypted connections/tunnels, commonly referred to as virtual private networks (VPNs) to firewalls, routers, and other devices where compatibility exists. Compatibility of VPN endpoints varies between devices and manufacturers and compatibility assurance can only be offered when Redcentric designs, specifies, and manages the devices at both ends.

2.1.3 Remote User Virtual Private Networks

Redcentric supports remote user VPNs using standards-based IP-sec and client-based SSL protocol suites. Redcentric supplies a client that is supported on the major operating systems including Windows, MAC OS, Android, and iOS. Redcentric supports basic remote user tunnels only - for example, posture-checking is not supported.

Users can be configured on the firewall for static username/password authentication. See virtual firewall resource specification for the number of users supported. Maximum number of statically configured users on physical appliances is 100.

Use of static username/password is considered a weak authentication method by security professionals and Redcentric strongly recommends use of its two-factor authentication service for secure authentication of remote user VPNs.

User authentication may also be possible through integration with corporate directory structures (e.g. Lightweight Directory Access Protocol – LDAP). Such integration is undertaken as a Professional Services exercise.

2.2 Monitoring / Alarms

Redcentric polls managed firewalls regularly to check for availability and critical events (these include hardware failures, environmental alarms etc. where available). Service tickets are automatically generated on the Redcentric system when faults are detected. Additionally, the firewall platform is configured to send alerts to the monitoring platform. Tickets are managed by engineering professionals in Redcentric operations centre 24x365.

2.3 Syslog

Both virtual and appliance firewalls can be configured to send Syslog feed to a customer’s server. This is undertaken as a Professional Services exercise.

2.4 Professional Services Consultancy

Charges for the Managed Firewall Service do not include consultancy to help the customer define the security policy or establish UTM configuration details. Also, certain other functionality (e.g. IDS) generally requires a bedding-in and tuning process to minimise false alerts. Occasionally this may need to be repeated throughout the Service Period, for example if the customer makes changes to their infrastructure or systems. Redcentric provides chargeable Professional Services consultancy to undertake this, and other work mentioned throughout this definition on request.

2.4.1 Limit of liability

Protocol and application vulnerabilities are identified and exploited regularly, and no firewall can offer absolute protection. Redcentric recommends that customers make regular use of security scanning services and use the output along with log and report data as part of a continual security improvement cycle. It is essential that Redcentric is notified in writing of the intent to perform scans beforehand.

2.4.2 Customer dependencies

The customer is responsible for the following functions:

- Define firewall rule base and other security parameters
- Update Redcentric with changes to list of staff authorised to submit change requests

2.4.3 Limitations

The platform does not support OSI Layer 2 transparent mode.

2.5 System Provisioning

2.5.1 Hardware Support

If a firewall appliance develops a fault, hardware support results in replacement of the faulty unit. Redcentric aims to replace faulty hardware located within a Redcentric data centre within four hours and hardware at other locations within the UK next working day. This level of hardware support is included within the Managed Firewall Service. Expedited hardware replacement options are available to meet specific customer requirements. Requirements and provision for expedited hardware replacement must be agreed in writing by both parties prior to finalising a Service Agreement.

2.5.2 Customer Security Policy

Redcentric configures the firewall(s) with rules that meet the customer's operational requirements. Redcentric recommends that prior to implementing any firewall solution, the customer undertakes a full security review. One component of this security review should be the creation of a network security policy. The security policy can form the basis of the firewall rule base and UTM configuration that will be implemented on the firewall(s). Redcentric recommends that the firewall rule-base should be based on the premise that all traffic is to be denied both inbound and outbound. The rule-base should be written to permit only valid traffic according to the customer’s security policy. The configuration can be modified throughout the Service Period by approved personnel to meet changing requirements.

2.5.3 Anti-virus (AV)

AV signature definition updates are periodically downloaded to the firewall automatically. A single AV policy/profile will be defined which can be tailored and applied to certain traffic as required. This single policy/profile is sufficient for most customers, but Redcentric will create and administer additional policy/profiles as required. Creation and administration of additional policy/profiles is

chargeable. When the firewall detects that an AV signature has triggered, the customer will be emailed immediately but no ticket is raised within the Redcentric ticketing system.

2.5.4 Web Filtering

Website category lists are managed and maintained centrally by the firewall vendor to provide the best possible service. The customer can dictate the action to be taken when users attempt access to disallowed sites. Options include denying access, permitting access after a warning message has been presented to the user, and generation of an email notification to the customer. Redcentric does not raise tickets when a user attempts to access a disallowed site. A single web filtering approved category list profile will be defined which can be tailored and applied to IP addresses and/or user groups as required. This single profile is sufficient for most customers, but Redcentric will create and administer additional category lists as required. Creation and administration of additional category lists is chargeable. Please see Price Card for details.

2.6 IDS/IPS

IDS definition updates are periodically downloaded to the firewall automatically.

Customers are encouraged to determine IDS policy carefully to maximise firewall performance. For example, if a customer has no devices with a particular operating system, the firewall should not be configured to check for exploits relating to that operating system. Where performance issues are related to poorly defined IDS policy, Redcentric consultants can provide system audit and advice as part of a Professional Service exercise.

A single policy containing some or all the signatures will be defined which can be tailored and applied to certain traffic as required. This single policy is sufficient for most customers, but Redcentric will create and administer additional policies as required, in which case additional charges may apply. The customer can dictate whether traffic is to be allowed or blocked when an IDS signature triggers the system at the set-up stage. Events will be logged, a ticket raised within the Redcentric system for awareness only, and an email is sent to the customer for further investigation.

2.7 Software and Subscription Licensing

Software subscription and licensing costs required to deliver the service are included in the charges for the Managed Firewall Service.

2.8 Data Processing

- Managed Firewall Service delivers a degree of IP network perimeter protection.
- Managed Firewall Service may involve the storage of summarised traffic and user activity.

2.9 Storage and encryption

- Firewalls may be configured to encrypt traffic across certain networks.
- By the very nature of the Service, it is necessary for Redcentric to capture, inspect, analyse, and store the customer's traffic/data.
- Redcentric would not have access to the content of the customer's traffic/data in normal circumstances. Under certain circumstances, when managing a support ticket, Redcentric may further capture, inspect, analyse and/or store samples of the customer's traffic to investigate and diagnose specific problems. Such actions will only be undertaken at the request of and in conjunction with the customer.
- The period for which data is stored in relation to the Managed Firewall Service is decided by the customer.

2.10 Data processing decisions

- Redcentric does not make any data processing decisions in relation to the Managed Firewall Service. Any processing of data over customer systems when using Managed Firewall Service is instigated, configured, and managed by the customer.
- Redcentric Support can be asked by the customer to intervene in the event of an issue with the Managed Firewall Service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the customer.

2.12 Customer Access to Data

The customer controls its own platforms which use Managed Firewall Service to carry data, and the customer therefore has full access to its own data.

2.13 Security arrangements and options

Redcentric core infrastructure and hosting locations comply with ISO27001 / ISO27002 information security standard and controls.

3. Implementation and Acceptance

Firewalls can be located on a customer site or within a Redcentric data centre. If the firewall is to be deployed within a Redcentric data centre, by default it will be installed within a rack dedicated to managed devices. If the customer subscribes to the Redcentric co-location service, the firewall(s) can be located in the customer's colocation facility to simplify connectivity to multiple Demilitarised Zone (DMZ) devices. If the firewall is to be deployed on a customer site, a Redcentric engineer will visit the site and undertake installation, configuration, and basic testing between 9am and 5pm.

3.1 Implementation of change requests

During the implementation phase, the customer will be provided with a firewall change request form. This should be used to submit change requests throughout the Service Period.

The validation and subsequent implementation or rejection of change requests will be performed Monday to Friday between 8am and 6pm, with a target completion time of 48 hours for routine changes. Emergency changes are prioritised accordingly, and performance targets are detailed in a Redcentric Customer Service Plan (CSP).

In accordance with the Redcentric change request procedure, all change requests must be submitted by a designated and authorised customer technical contact. If Redcentric security engineer cannot validate the change requester against the authorised list, then Redcentric will place the change request on hold and attempt to contact one of the alternative authorised contacts. Redcentric must wait for the request to be ratified by a known authorised contact before proceeding with any firewall change. It is therefore essential that customers provide accurate and current contact information for their designated and authorised staff.

It is extremely easy to weaken network security by submitting a seemingly innocuous change request. Redcentric staff review change requests based only on the information they have available, and therefore Redcentric cannot take responsibility for network weakness resulting from rule-base changes. If Redcentric support staff believe that a rule-base change request compromises the security of the customer's network, Redcentric may ask the customer to sign a disclaimer stating that they wish to go ahead regardless of the advice offered. In extreme cases, staff reserve the right to reject the change outright; for example, if the weakness could affect other Redcentric customers.

3.2 Acceptance

The following are the Acceptance Criteria applicable to the Managed Firewall Service.

- Confirm Redcentric Support contact details have been supplied
- Check that customer administrators can access the portal
- Check the LAN connections to the firewall(s) for speed and duplex mismatches and errors (where possible).
- Test IP connectivity by using permitted protocol traffic from permitted devices on each interface destined for permitted addresses on the other interfaces (e.g. test traffic on port 80 from a device on the internal network destined for a server on the outside network; repeat for server on the DMZ network if applicable)
- Use vulnerability scanning service to confirm traffic is permitted and denied according to required rule-base
- Test connectivity to/from devices which are connected to the firewall using secure tunnels if required
- Test functionality and notification mechanisms of UTM capabilities if chosen

3.3 Offboarding

Redcentric project, delivery and support teams will work closely with customers to gracefully closedown any services at their contract end and, if required, assist in any transition or migratory tasks with the customer and any new service provider.

Redcentric will not be obliged to disclose any confidential information to the customer or replacement supplier, or to transfer any assets, contracts, employees, or third-party licences.

3.3.1 Principles

Redcentric will assist the customer in facilitating the orderly transition of the services (in whole or part) from Redcentric to the customer or any replacement supplier upon the expiry or earlier termination of the Order Form for Access as a Service.

3.3.1.1 Removal of Customer Premises Equipment

“Customer Premise Equipment (CPE)” is defined in paragraph 1.6 of this Service Definition. On termination or expiry of the Call-Off Contract, the customer must undertake the following responsibilities:

- agree a time and date for the CPE to be removed by Redcentric; and then
- permit Redcentric to remove the CPE at the agreed time on the agreed date in a sequence to be specified by the customer.

3.3.1.2 Removal of Customer Premises Equipment

Where the customer requests the provision of additional transitional assistance, in addition to that required under this section, Redcentric shall provide such assistance as additional Professional Services upon agreement and signature of a Variation Order. The additional transitional assistance detailed here shall be chargeable at the Redcentric prevailing time and materials consultancy day rates.

4. Associated Redcentric Services

The table below provides details of other compatible services with Managed Firewall Service available from Redcentric via G-Cloud 15.

Service Name	Service Summary
Network as a Service	**Network as a Service** provides a secure internal / external network connection. It meets compliance standards and various Redcentric services such as internet and security can be overlayed over this single connection into the Redcentric Network.
DDOS Mitigation Service	**DDoS Mitigation Service** consists of three services. DDoS Essentials and DDoS Essentials Plus, ensures customer protection within 60 or 15 minutes respectively, upon attack notification. DDoS Pro offers comprehensive management with instant detection and automated response. Monitoring at the ISP level enables pro-active attack identification, enhancing network security measures.
Managed Firewall Service	**Managed Firewall Service** The service is delivered on virtual firewalls on a shared platform or on one or more dedicated hardware firewall appliances. The firewalls control traffic between devices on different networks and provide perimeter protection. The firewall is configured by our staff to meet customer's requirements. Firewalls are monitored for alerts.
Managed SD WAN Service	**Managed SD WAN Service** is designed to complement traditional private IP-VPN networks. It allows customers to make optimum use of the available bandwidth at sites, and to supplement private connections with cellular, low-cost Internet and other links. Application visibility, control and performance can be enhanced, delivering greater efficiency and user satisfaction.
Managed Wireless LAN Service	**Managed Wireless LAN Service** offers design, deployment, monitoring, support, and management of wireless LAN infrastructure deployed on Customer sites. The service uses products from leading Wireless LAN manufacturers. The service delivers enterprise features and uses local or cloud-based systems for provisioning, monitoring, and management.
Meraki Connectivity and Security	**Meraki Connectivity and Security.** Meraki's range of connectivity and security devices are proving to be popular due to the market leading traffic visibility and diagnostic capabilities, also the scalability and ease of management using the cloud-based management portal. Redcentric Meraki service provides the design, deployment and ongoing support of Meraki's connectivity and security devices.
Two Factor Authentication	**Two Factor Authentication** (2FA) service offers a robust, flexible, and secure way to authenticate user connection requests to network devices. The 2FA service can be deployed on both Customer managed and Redcentric managed network devices. The 2FA service offers a more secure and scalable alternative to static passwords.

5. Service Levels and Service Credits

5.1 Service Levels

The Service Level applicable to the Managed Firewall Service is as follows:

Applicable Managed Firewall Service	Service Availability	Service Credit
Virtual firewall	=100%	none
	≥99.0% but <100%	5% of MS
	≥97.0% but <99.0%	15% of MS
	<97.0%	20% of MS
Single firewall located in a Redcentric data centre	≥99.5%	none
	≥99.0% but <99.5%	5% of MS
	≥97.0% but <99.0%	15% of MS
	<97.0%	20% of MS
Pair high availability firewalls located in a Redcentric data centre or on customer site.	=100%	none
	≥99.0% but <100%	5% of MS
	≥97.0% but <99.0%	15% of MS
	<97.0%	20% of MS
Single firewall installed on a customer site	≥99.0%	none
	≥98.0% but <99.0%	5% of MS
	≥96.0% but <98.0%	15% of MS
	<96.0%	20% of MS
Portal access for analysis and visibility etc.	≥99.5%	none
	≥99.0% but <99.5%	5% of MS
	≥97.0% but <99.0%	15% of MS
	<97.0%	20% of MS

5.2 Exclusions from availability

In calculating Availability, in addition to the exclusions listed in the General Terms of the Redcentric G Cloud 15 Supplier Terms the following shall be excluded:

- Unavailability due to tasks required to implement and test change requests.
- Unavailability due to malicious activity of any kind. e.g. a Denial-of-Service attack (DOS)
- Unavailability due to customer misconfiguration

5.3 Floor service level

The Floor Service Level applicable to the Managed Firewall Service in respect of Availability shall be 85% in any given Month.

5.4 Service Credits

The Service Credits applicable to the Managed Firewall Service shall be calculated as follows. In the following table:

"≥" means "greater than or equal to"

"<" means "less than"

"MS" means the total Charges payable in respect of the Managed Firewall Service for the same Month

Applicable Managed Firewall Service	Service Availability	Service Credit
Single firewall located in a Redcentric data centre	≥ 99.5%	none
	≥ 99.0% but <99.5%	5% of MS
	≥ 97.0% but <99.0%	15% of MS
	< 97.0%	20% of MS
Single firewall installed on a customer site	≥ 99.0%	none
	≥ 98.0% but < 99.0%	5% of MS
	≥ 96.0% but < 98.0%	15% of MS
	< 96.0%	20% of MS

6. Responsibilities and Accountabilities

6.1 High Level Redcentric Responsibilities

Redcentric is responsible for the following aspects:

- Solution design based on information and requirements provided by the customer
- Initial installation and testing of equipment with agreed success criteria
- Configuration of the centralised management, reporting, etc. components
- General upkeep of the service including hardware and software upgrades
- Ongoing support of customer-specific configuration, including advice and implementation of minor changes
- Continued monitoring of equipment with our support teams and pro-active management of faults
- Arranging replacement of faulty hardware

6.2 High Level Customer Responsibilities

The Customer is responsible for all other aspects including, but not limited to:

- Providing Redcentric with the Customer's detailed functional and other requirements
- Providing Redcentric with the technical details required for the design. E.g. Firewall rulesets, Port speeds/duplexes, uplink/downlink specifications to other equipment, IP address ranges, VLAN assignments, local DNS servers, DHCP scopes and options, NAT translations, etc.
- Where equipment is be located at customer premises, providing an appropriately physically secured location to house equipment, typically a communications rack in a separate communications room, or similar
- Where equipment is be located at customer premises, providing appropriate power, rack space and heating/ventilation/cooling (HVAC) for any equipment housed on the customer's site
- Where equipment is be located at customer premises, unless otherwise agreed with the customer, providing appropriate LAN side cabling, cables, patch panels, etc beyond the service demarcation point, unless a Redcentric managed LAN service is taken
- Where equipment is be located at customer premises, arranging and allowing access to site facilities at agreed times and for an appropriate window of time for the installation of any equipment related to the delivery of the service
- Where equipment is be located at customer premises, completion of any required site risk assessment information prior to engineer site visits
- Supply and upkeep of staff entitled to request changes with our support teams
- Completion of appropriate forms to request any changes to rulesets, policies, etc

7. Business Continuity and Disaster Recovery

7.1 Business Continuity

Redcentric under its ISO22301:2019 Business Continuity certification, operates and maintains a robust Business Continuity Management System (BCMS). The BCMS scope includes;

- Data Centres
- Managed Services
- ICT technologies and systems
- Staff and business functions

and is externally assessed by the BSI annually to ensure continued effectiveness in line with BSI published standards.

Our Business Continuity Policy Plan (BCP) is fully supported by the Board and is designed to enable a return to normal operations in the shortest practical time, with minimum disruption. The primary objective is to restore and deliver continuity of key services in the event of a critical incident.

Our overall Business Continuity strategy is to provide resilience for all systems that support critical processes, by having data backed up to alternative Data Centres, or dual site services configured as active-active.

We use the same cloud backup service (Acronis BaaS) for our own IT and services as we do for our customers, ensuring fully secure, encrypted data is available off-site when needed. Departments and services are required to test backup and restore annually.

Testing

Our BCP is routinely tested annually, and as Redcentric is a provider of critical services to the NHS (Peering Exchange and Consumer Network Service Provider), is independently witnessed by a member of NHS England.

Disaster Recovery plans underpinning the BCP have been developed for each Department and Service and these are externally audited and tested annually.

Network Resilience

Our network has been designed and engineered to deliver highly available, stable connectivity to maintain business access to critical applications. To maximise resilience, multiple carriers provide the core connectivity and routing, and switching devices are used from market leaders Cisco Systems. The network design and build are geographically resilient providing a minimum of 99.99% availability (to resilient end points).

The Redcentric highly resilient, high-capacity core has connections to several carriers providing multiple options for our internal business operations and critical services, and customers wishing to access cloud services, applications, and data:

- Geographically resilient connectivity to multiple Tier1 Internet transit providers and Internet exchanges.
- Geographically resilient connectivity directly into the inner core of the HSCN network.
- Core network engineered to withstand multiple concurrent failures and to re-route around a failed transit path in under a second.

7.2 Disaster Recovery

Since firewalls are typically deployed to secure and offer aggregated services (e.g. Internet, VPN ingress/egress), they represent a risk to any organisation during a loss of service event. As such, we recommend that customers take a pragmatic approach to the deployment of firewall services and encourage customers to consider taking appropriate resiliency options for firewalls, including high availability (HA) pairs of devices and/or geographically diversely located firewalls to mitigate against any disaster. The appropriateness of any firewall resiliency options should be considered as part of an overall resiliency strategy.

Resiliency, where used, is designed in such a way as to offer automated failover and failback in the event of service interruption on any one single firewall device. Where resiliency is employed, we offer enhanced SLAs for site availability.

8. Data Processing

8.1 Data Processing Scope

- The Redcentric Managed Firewall Service delivers design, deployment, and support functions.
- The Redcentric Managed Firewall Service may involve the storage and capture of log data from the firewall service as required by the customer.

8.2 Data Storage and Encryption

- Redcentric configures equipment to encrypt traffic according to Customer requirements.
- Redcentric may capture, inspect, analyse, or store the Customer's traffic/data dependent upon the additional services the customer requires, e.g., Firewall log data storage and analysis where required by the customer and for the purposes of compliance with regulations on log storage and for report production.
- Under certain circumstances, when managing a support ticket, Redcentric may capture, inspect, analyse and/or store a small sample of the Customer's traffic to investigate and diagnose a very specific problem, e.g., to help resolve a problem relating to packet corruption. Such diagnosis would involve the examination of a small sample of packets, and this will only be undertaken at the request of and in conjunction with the Customer.

8.3 Data Processing Decisions

Redcentric does not make any data processing decisions in relation to the Managed Firewall Service. Any processing of data over Customer systems when using the Managed Firewall Service for transit is instigated by the customer and configured either by the Customer or Redcentric staff.

Redcentric Support can be asked by the Customer to intervene in the event of an issue with the Managed Firewall service. In such a case Redcentric may make decisions that affect data processing, but such actions will only be undertaken at the request of and in conjunction with the Customer.

8.4 Subprocessors

Managed Firewall Service may make use of services provided by the selected firewall vendor (e.g. Fortinet, Cisco Systems etc.). These services assist with the identification of security vulnerabilities, weaknesses, exploits, virus, worms etc.

No other parties are involved in delivering the Managed Firewall Service, and no other sub-processors are appointed by Redcentric.

9. Exit Plan

Upon expiration of the Contract where the customer chooses not to renew with Redcentric, the steps set out in paragraph 3.3 will apply.

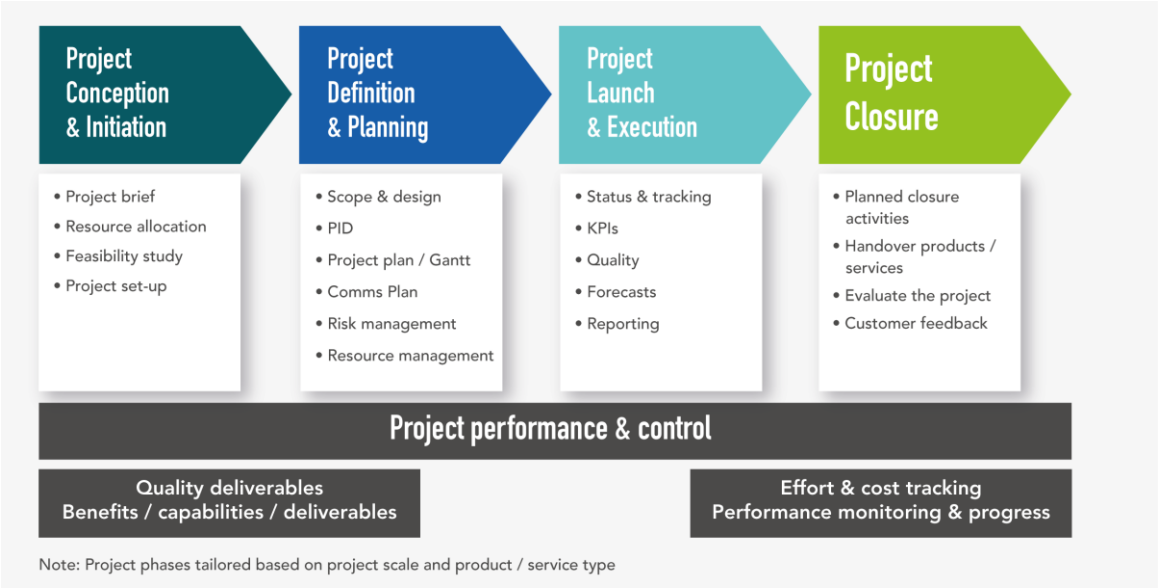
10. Project management

We understand you need to be confident we can deliver projects successfully and without risk to you or your customers. We know collaboration and communication with you is the key to successful project delivery, and the best way to ensure we can deliver the business value you expect from us.

Redcentric uses a hybrid project approach based on PRINCE2 and Waterfall methodologies, that is strengthened by ITIL project best practise. Our approach has been honed to foster a close working relationship between you and the dedicated project team that will be responsible for the onboarding of your new services.

The 4 phased approach that will steer your project delivery is:

- **Phase 1 – Conception and initiation**
- **Phase 2 – Definition and planning**
- **Phase 3 – Execution**
- **Phase 4 – Handover and closure**



Note: Project phases tailored based on project scale and product / service type

We recognise the importance of making sure your project and programme of work is delivered on time and meet your quality and cost considerations. Our highly skilled team of project managers have years of project management and solutions expertise which enables us to provide you a clear understanding of when your solutions will be delivered in preparation for a seamless handover into live service.

You will benefit from our experience of managing a very broad spectrum of complex projects across our range of solutions for customers in a variety of sectors including highly sensitive sectors such as healthcare where disruption to BAU might result in a risk-to-life, or commercial sectors for example, retail or legal, where any disruption would have a significant impact on operational or commercial outcomes for the customer.

To meet your individual needs, we understand we need to be flexible to ensure we can deliver results quickly and with the expected outcome for the project. To achieve this, we will work closely with you to understand your needs and learn how issues impact your business. This will provide a clear insight into working together to resolve any challenges.

The main advantage of our meticulous approach is the handover process at each stage of the project. Risk is a key part of the agenda, which in turn promotes the continuity of risks and the identification of assumptions, issues, and dependencies. This early and continuous detection of risk means we can promptly and effectively mitigate any challenges as early as possible.

Quality assurance processes are embedded throughout the delivery lifecycle, underpinned by our ISO 9001, 14001, 20000, 22301 and 27001 certifications and supported by our centralised programme management office.

The project toolbox

We will use a suite of project tools designed to ensure your project delivery is seamless, transparent, managed effectively, and delivered to your agreed specification. Each device has been refined over time based on our experience and as our knowledge evolves with the introduction of new technologies.

- Project initiation document to develop a detailed scope of your requirements
- Comprehensive project plan to refine the delivery approach
- High level solution design
- Low level solution design
- RAID Log to identify, control and govern project risks
- Site audit report to help identify issues and challenges at each project location

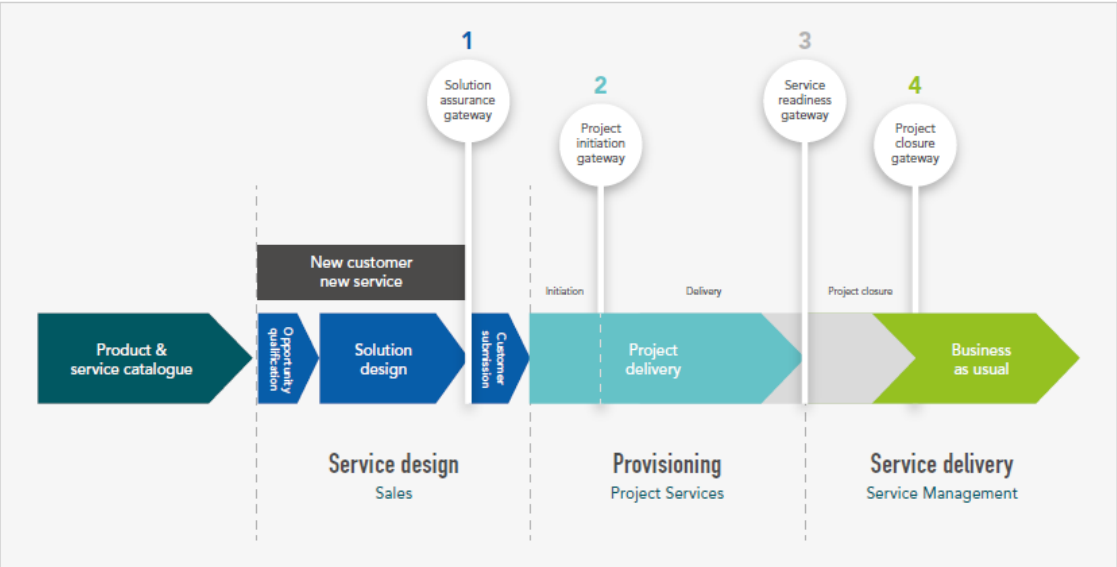
- Test plan to minimise disruption to your business operations
- Communications plan that defines what information to share and with whom
- Site implementation tracker to record the migration progress
- Weekly highlight report providing project updates
- Customer Service Pack
- UAT Test Report – per site (Word)
- Project Closure Report (Word)

Transition management

It is important to Redcentric that you experience a seamless and smooth transition into your service management team. With an established and proven approach to transitioning customers from solution design, through to projects and into your support team. Redcentric are confident you will feel supported and comfortable for the project team to step back, to let the service management team take over.

Using an effective project delivery approach throughout your transition journey, will ensure:

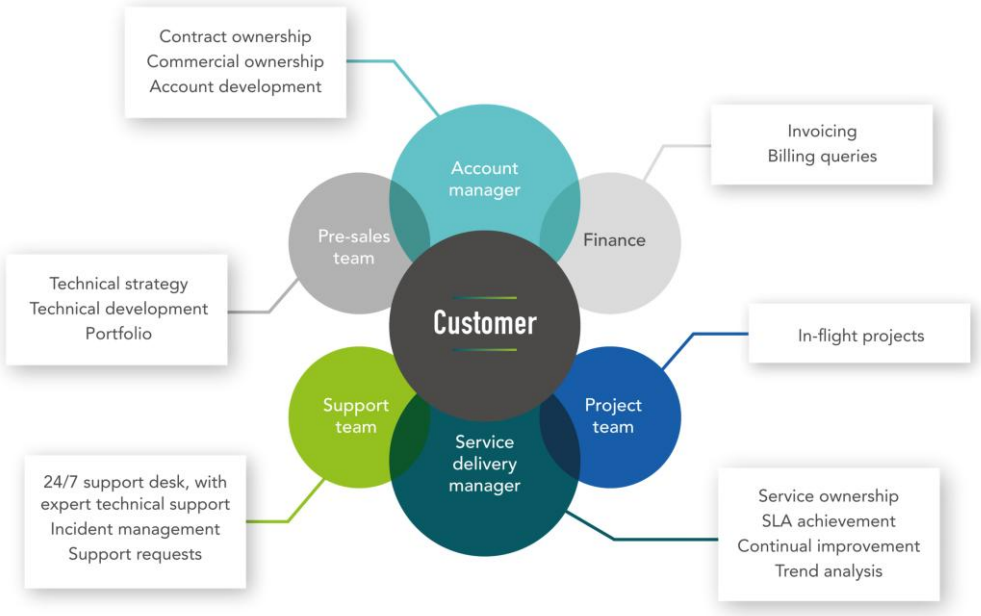
- Technical delivery is achieved on time and to specification
- The support model is fit for purpose and available at service commencement
- You will experience a ‘soft landing’ with minimal disruption to service.



With 30 years of track record of delivering projects, Redcentric is knowledge and approach to mitigating risk during the project transition phase is based on experience. Their mature and proven approach is employed as a standard risk management framework which flows from initial bid stage through to project delivery, and into live service.

11. Account management

We appreciate the nature of your business demands an exceptional service. We recognise you need to be supported by a team who are not only competent and highly skilled, but also passionate about delivering the right outcome, every time. In our experience, this is achieved by aligning our expertise from the very beginning to create a single, cohesive, and focused team.



Your Account Manager will build an understanding of your current and long-term strategy and ensure that the wider Redcentric team understands your needs. They are responsible for the day-to-day commercial relationship between the customer and Redcentric. Our aim is to develop a long-standing partnership with you.

Sharing Technology advancements with you

A key role of your Redcentric account manager is to understand your business and to keep you proactively informed on the technology and industry developments that may be of strategic benefit to you. As part of your monthly service reviews, we will discuss our product and services roadmap and where required involve our technical design resources to better understand your requirement and provide guidance.

Our technology roadmap review forms part of the service delivery programme. Our aim is to ensure you are fully informed of the wider developments that we are planning to introduce and allow us to discuss any requirements you would like us to consider for the future.

Working in partnership to drive continuous improvement.

We fully embrace the continuous service improvement and will work with you to develop a continuous service improvement plan (CSIP). At the simplest level your CSIP will act as a way of prioritising and tracking minor improvement initiatives such as tweaking process to better suit your need but is equally used to drive technology enhancements and innovations to align evolving business requirements, including technology refresh, changes, and upgrades throughout the contract period.

12. Service management

Redcentric will provide a centralised service management model for all services we deliver to you. Our proven model will ensure you receive service management and support services that is easily accessible and effective.

Our mature processes are based on the ITIL framework, fully supported by Gartner-referenced service management tools and process automation which ensures you receive a best-in-class user experience.

The proposed solution is inclusive of our support and account management service, which include:

- Genuine 24/7/365 service desk which is manned, monitored and maintained using as mature ITSM tool
- Best-in-class secure management and monitoring tools, designed to ITIL guidelines.

Our service is underpinned by comprehensive, yet agile, documented processes that include major incident management. We have recently introduced enhanced SLAs within our support services; this means we will respond to you quicker and we are committing to faster fix times.

Service Reviews are an opportunity for us to collaboratively evaluate service performance and ensure it is effective and aligned to your needs. The service reviews seek to understand how we can work in partnership with you and your teams and to identify how we can improve performance. We work proactively to propose solutions to problems and suggest the best way to resolve any issues.

What happens at the monthly service review?

- Review service delivery using performance data and provide this in a graphical format.
- Analyse support tickets to identify patterns that indicate we need to explore further to identify the root cause.
- Review service availability, service exceptions, significant incidents, and related trends.
- Build operational relationships between our customers and the wider Redcentric team.
- Seek to align internal resources within Redcentric to ensure effective service delivery.
- Identify areas for improvement and include them in the service improvement plan.
- Seek your input on how we can evolve our services to suit your future objectives.
- Share our vision to demonstrate how we can support your future strategic aims.
- Create and hold formal records in the Redcentric document management system.

The monthly service pack provides a basis for discussion. It can be tailored to meet specific customer reporting needs as part of the onboarding process or within the lifetime of the contract. As standard, we provide a service pack that includes up to 12 months of data extracted from the support system and service monitoring systems. We analyse current and previous months' performance and identify any trends.

We operate a Service Management System which meets the requirements of ISO/IEC 20000, which means we have a tried and trusted model for service delivery that provides a consistent approach.

13. Support Services

We understand that our customers trust the Redcentric team to ensure that our services meet your needs. Our relationship with our customers goes beyond just complying with contractual SLAs and meeting industry standards.

We seek to understand the importance of service delivery to your organisation and work with you to provide the support that leads to the rapid resolution of any issues.

We take a pro-active approach to supporting you so you can be sure that the services which your business relies on are in safe hands.

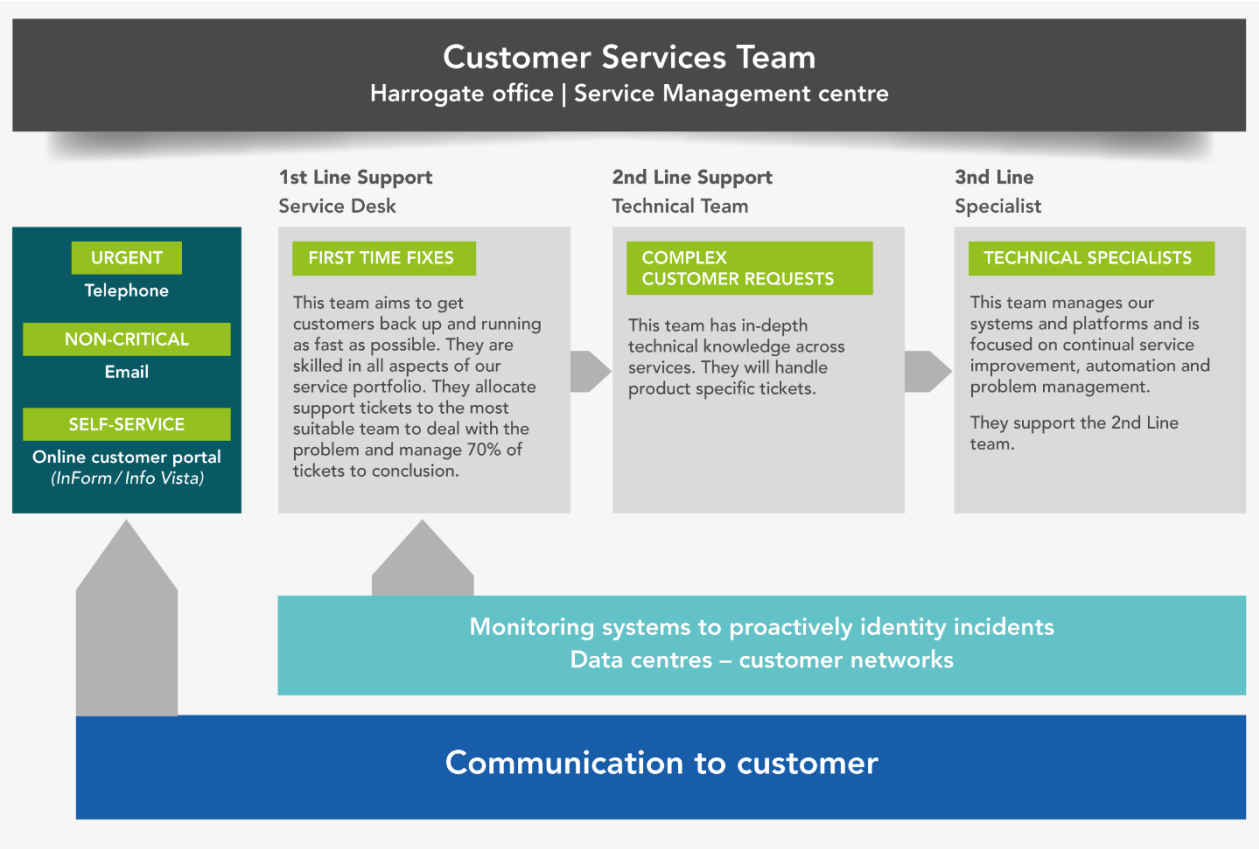
Our support operations meet the highest industry standards, and service management processes are based on the ITIL framework.

We have thoroughly documented the major incident and customer service plans, which detail how we operate in business-as-usual scenarios and during major incidents.

We use best-in-class secure monitoring tools to manage the services we provide to you actively. We use Gartner-referenced service management tools and process automation, which allow us to work smarter.

Our support function is structured to ensure fast resolution of incidents with timely escalation where appropriate.

The service journey you experience is important to us. Every interaction is monitored by our customer services team, who are highly experienced in handling customer interactions, and understand the importance gathering accurate and timely information to ensure the correct resources are allocated to reach a rapid conclusion.



Our incident management process has been engineered to be customer focused and designed to ITIL guidelines. We follow a proven process for incident management, with clear steps marked out for each team to ensure you are supported in the most effective and organised manner.

14. Information assurance

Certifications

Redcentric are ISO 20000-1 certified, demonstrating that we adhere to ITSM (IT Service Management) best practice, and ITIL (Information Technology Infrastructure Library) provides advice on ITSM best practice.

ITIL v4 is at the heart of Redcentric managed service operation and support. Redcentric believes that to deliver a high quality, professional service it is necessary to invest in training people, empowering them to be strong ambassadors of our service model.

Redcentric has provided managed services to the UK public and private sector for over 30 years. As a highly accredited business, we are proud of the standards and processes for which we are certified.

Our data centres and all supporting operations are fully UK Sovereign and are congruent with;

- The Government's Security Classification Policy ('Official-Sensitive')
- The Government's previous Protected Marking Scheme classification (BIL4 - Confidential)

Note – Redcentric can also support information and assets classified above the GSCP level of 'Official-Sensitive'.

ISO

- ISO 27001:2022 Information Security Certified
- ISO/IEC 27017:2015 Cloud Security Certified
- ISO/IEC 27018:2019 Personally Identifiable Information (PII)
- ISO 9001:2015 Quality Management Certified
- ISO22301:2019 Business Continuity Management
- ISO 14001:2015 Environmental Management System Certified
- ISO 20000-1:2018 IT Service Management System Certified

NHS standards

- Registered HSCN CNSP (Health and Social Care Network, Consumer Network Service Provider)
- DSPT (Data Security and Protection Toolkit) assessed as exceeding standards
- NHS Certified Commercial Aggregator
- NHS Business Partner
- Authorised to transmit, process and store Person Identifiable Data (PID)
- NHS England IGSoC Compliant Commercial Third Party (NACS code: YGMAP)
- NHS England accredited Service Provider (Network Access Agreement number: 0740).

HMG / other standards

- PCI-DSS Compliant for physical hosting and managed firewall services within our data centre locations
- Cyber Essentials Plus Certified
- Data Centres are externally certified to attest they have the necessary physical security measures to process HM Government 'Official-Sensitive' classified data
- Main data centres are certified as Police Assured Secure Facilities
- Full alignment with the Security Policy Framework
- All services are designed, built, implemented, and supported using all relevant and appropriate NCSC GPGs, Cabinet Office and NHS England standards

Networks Connectivity

- The Public Internet via Private or Public IP VPN
- The HSCN Peering Exchange
- PSTN
- PSN (Public Sector Network) certified as one of the few DNSPs (Direct Network Service Provider)
- PSN Gateway Access for both PSN-Assured and PSN-Protected
- JANET (Joint Academic Network)

Further information with regards to the Redcentric assurance and governance framework can be found within the Redcentric customer security pack which consist of the following documents:

- Cloud Security Principles (aligned with the NCSC 14 principles)
- Security Management Plan
- Security Statement
- Accreditations and Mappings (lists all business accreditations and relevant controls and standards utilised for Redcentric G-Cloud services)
- Security Control Framework

Copies are available under NDA upon request.

15. Professional services

The Redcentric Professional Services team is drawn from across the organisation, bringing together a unique mix of experience, know-how and talent to help deliver substantive value to its consulting assignments.

Strategists, designers, developers, technicians, engineers, analysts, security specialists and project managers from the worlds of infrastructure, networks, applications, communications, and mobile can come together to deliver expert, targeted, outcome-driven assistance where it's needed.

The common denominator in every professional services engagement is that we are responding to a specific client need. We provide tailored responses to your requests for assistance, whether that's for help of a strategic or tactical nature, short or long-term, on premises or off, single vendor or multi-vendor environment, in a lead role or in support.

Redcentric provide Professional Services using either our in-house team or approved third parties. Professional Services are not part of the service unless so specified in the customer's order. Professional Services require a separate order or change control procedure.

Available services

- IT strategy.
- Project management.
- Change management.
- Design integration.
- Staging and installation.
- Integration design.
- Service migration.
- Optimisation and performance tuning.
- Physical lift and shifts.
- Audits and compliance.
- Application development.
- On premise and/or remote access support.

16. Company profile

Redcentric is a managed service provider, delivering highly available network, cloud and collaboration solutions that help public and private sector organisations succeed.

We provide:

Assured availability – Delivering highly available solutions that organisations can rely on to improve productivity and performance

Organisational Agility – Helping organisations to address operational, financial, and regulatory challenges at speed

Smarter Working – Enabling and empowering organisations to connect, communicate and collaborate

Our aim is to work in partnership with you to improve efficiencies, drive transformation and enhance the services you provide to your citizens, patients, students and tenants and our services are provided in line with the most stringent public sector standards.

We are here to support you, whether that be with traditional infrastructure or making the move and taking advantage of what the cloud and hybrid environments have to offer.

Today we can offer a rich end-to-end solution portfolio covering the full spectrum of cloud, network and collaboration designed and delivered by our own highly skilled teams from our privately owned, UK based multi-million-pound infrastructure.

Our ethos is one of collaboration; our aim is transformation: helping clients secure desired outcomes, substantive gains, and a measured route forward for the future.

Our assurance comes from a long track record across both the private and public sectors, characterised by deep domain expertise, continuous innovation, proactive management, and an enduring commitment to business improvement through better IT. We'd like to think that there are hundreds of organisations out there where Redcentric has already made a significant and lasting difference.

- Multiple wholly owned UK data centres
- Serving over 800 customers across the UK
- Health and Social Care Network approved CN-SP
- NHS Digital approved N3 Aggregator since 2014
- Accredited to connect and supply over Janet
- Authorised to process HM Government data marked 'Official-Sensitive'
- Accredited to store patient data
- HSCN Peering Exchange Provider
- Accredited to connect and supply over Public Services Network (PSN)
- Accredited and experienced G-Cloud supplier
- 15+ years of N3 experience
- Fully aligned with ITIL Service Management Standards
- ISO 9001, 14001, 27001, 22301 and 20000-1 certified
- Cyber Essentials and Cyber Essentials Plus certified
- PCI Compliant for physical hosting services
- Services designed, built, implemented and supported using appropriate NSCS GPSs, Cabinet Office and NHS Digital standards
- Fully approved HSCN connectivity to Azure and AWS environments.

17. Why choose Redcentric?

Owned infrastructure

We believe that service quality is dependent on end-to-end control and capability, which is why we've spent the past three decades building our own infrastructure and skills base: a UK-wide MPLS network, UK-based data centres, Voice and IaaS platforms, Network and Security Operations Centre, and a large ITIL-based support operation.

Expert guide

We are not about the provision of one-off IT commodities but rather helping clients over the short, medium and long-term through the strategic alignment of our services to organisational requirements. We guide you on your journey at whatever speed and in whatever direction the need dictates.

Customer-centric culture

It is the 'can do' attitude of our teams that we are most proud of and which our customers most value and often comment on. We invest in our staff and work hard to develop and preserve a culture that prioritises staff satisfaction and motivation. We believe that the happier, more engaged, and dynamic we are as a team, the more we can achieve together, ensuring we deliver the best results for our customers.

Open-minded and innovative

We pride ourselves on being an innovative service organisation which means we are always willing to think and do differently and to go beyond norms and conventions. We are always reviewing our proposition, introducing new proven technologies that dovetail with our existing offering; and bringing these opportunities for further gains to our customers. But equally this spirit of innovation may be seen in our flexible approach to project management, and it extends to all aspects of how we work with our customers.

Breadth of services

Our great strength is our ability to be a single unifying partner who can deliver a comprehensive range of IT and Telecoms services across multiple sites with confidence.

Security and integrity

We invest in our systems and processes, that in turn allow us to attain the highest standards of certification and accreditation. These are not badges of honour, but hard-earned evidence of our commitment to quality, security, and integrity, and this supports our aim to be a 'trusted partner'.

Outcomes focused

We believe we have an important role to play in ensuring you have the IT infrastructure and services to help you to achieve your goals. We help you to meet new challenges and to stay agile so that you can respond to change and at the same time keep your data and systems highly secure.

Our teams

We have highly skilled staff, whose average tenure is more than 10 years bringing a huge wealth of experience and a depth of knowledge on which you can rely. We also invest in the development of new team members who bring new or enhanced skills to Redcentric and the training of existing staff to ensure you benefit from a consistent, high-grade delivery of services and support day in, day out.

Continuous Service Improvement

We are committed to investing the most that we can to build a sustainable, successful business that can deliver genuine IT outcomes for our customers. We are continually refreshing our core systems or adding capacity and capability, to the tune of many millions.

Proactive

We think and act quickly

Inspired

We create excitement through innovation

Trusted

We do what we say we will

Collaborative

We work together to deliver a common goal

Transparent

We are open, honest and fair

Head office

Central House
Beckwith Knowle
Harrogate
HG3 1UG

T 0800 983 2522
E sayhello@redcentricplc.com
W www.redcentricplc.com

redcentric

AGILE • AVAILABLE • ASSURED