DDoS Mitigation Service

Service Definition

G Cloud 15

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

January 2026

redcentric

AGILE • AVAILABLE • ASSURED

Contents

1. Service Definition 4

1.1 Service Overview 4

1.2 Service Description 4

1.3 Key Features and benefits 5

1.4 Levels of Service 6

1.5 Service Implementation 6

1.6 Monitoring 7

1.7 Reporting 7

1.8 Incident Management 7

1.9 Maintenance Notice and Scheduled Downtime 7

1.10 Change Notice 8

1.11 Customer Requested Changes (DDoS Pro only) 8

2. Onboarding and Offboarding 11

2.1. Onboarding 11

2.2. Acceptance Criteria 11

2.3. Offboarding 11

3. Services Availability 12

3.1 Service Availability 12

3.2 Exclusion from Availability 12

3.3 Service Levels 12

3.4 Service Credits 12

4. Associated Redcentric Services 13

5. Responsibilities and Accountabilities 14

5.1 High Level Redcentric Responsibilities 14

5.2 High Level Customer Responsibilities 14

6. Business Continuity and Disaster Recovery 15

6.1 Business Continuity 15

6.2 Disaster Recovery 15

7. Data Processing 16

7.1 Data Processing Scope 16

7.2 Data Storage and Encryption 16

7.3 Data Processing Decisions 16

7.5 Customer Access to Data 16

7.6 Security Arrangements and Options 16

8. Exit Plan 17

9. Project management 18

10. Account management 20

11. Service management 21

12. Support Services 22

13. Information assurance 23

14. Professional services 24

15. Company profile 25
16. Why choose Redcentric? 26

1. Service Definition

1.1 Service Overview

Distributed denial of service (DDoS) is a type of cyberattack that attempts to make online services unavailable by flooding them and/or any or all upstream network assets with malicious traffic where an attacker overwhelms its target with unwanted internet traffic so that normal, legitimate traffic cannot reach its intended destination or be processed successfully. Remember that it's relatively rare a web site is targeted directly.

During a DDoS attack, attackers may use large numbers of exploited machines and connected devices across the Internet including Internet of Things (IoT) devices, smartphones, personal computers, and network servers to send a flood of traffic to targets.

A DDoS attack on a company's website, web application, network, or data centre infrastructure can cause downtime and prevent legitimate users from buying products, using a service, getting information, or any other access.

How does a DDoS attack work?

DDoS attacks exploit networks of Internet-connected devices to cut off users from a server or network resource, such as a website or access to any online service application they may frequently access

1.2 Service Description

The Redcentric DDoS Mitigation service provides multiple service levels which caters for any size of customer, ranging from a small business with a minimal online presence to a large enterprise with a significant online presence. These are broken down into 3 services.

DDoS Essentials and DDoS Essentials Plus are very similar in that they are both a reactive service and require the customer to contact Redcentric when they suspect that they are being targeted by a DDoS event, the couple of key differences are that DDoS Essentials Plus offers the ability to activate the DDoS service pre-emptively when a plausible threat has been received, in addition providing basic reporting capabilities. These service packages are only suitable for dealing with a volumetric type of event.

Once notified of a DDoS event, Redcentric will offload the traffic into the on-net scrubbing centre or if very large >1Gb to an upstream scrubbing service, mitigating the volumetric traffic and passing the cleaned traffic back into the network to be routed on to the customer. Outbound traffic will not return via scrubbing centre but be sent out of the customers' default traffic path.

DDoS Pro service is a fully managed Enterprise grade DDoS mitigation solution which includes a rapid automated response to DDoS attacks by providing immediate detection and mitigation capability. This design and approach reduce risk to the Customer by ensuring full Layer 3-7 mitigation protection.

The Redcentric DDoS mitigation service provides protection for both volumetric and sophisticated attacks along with being able to monitor all inbound and outbound traffic for the detection of DDoS attacks and redirect any traffic for scrubbing to specialised equipment, hosted both in the Redcentric internet infrastructure and large upstream providers.

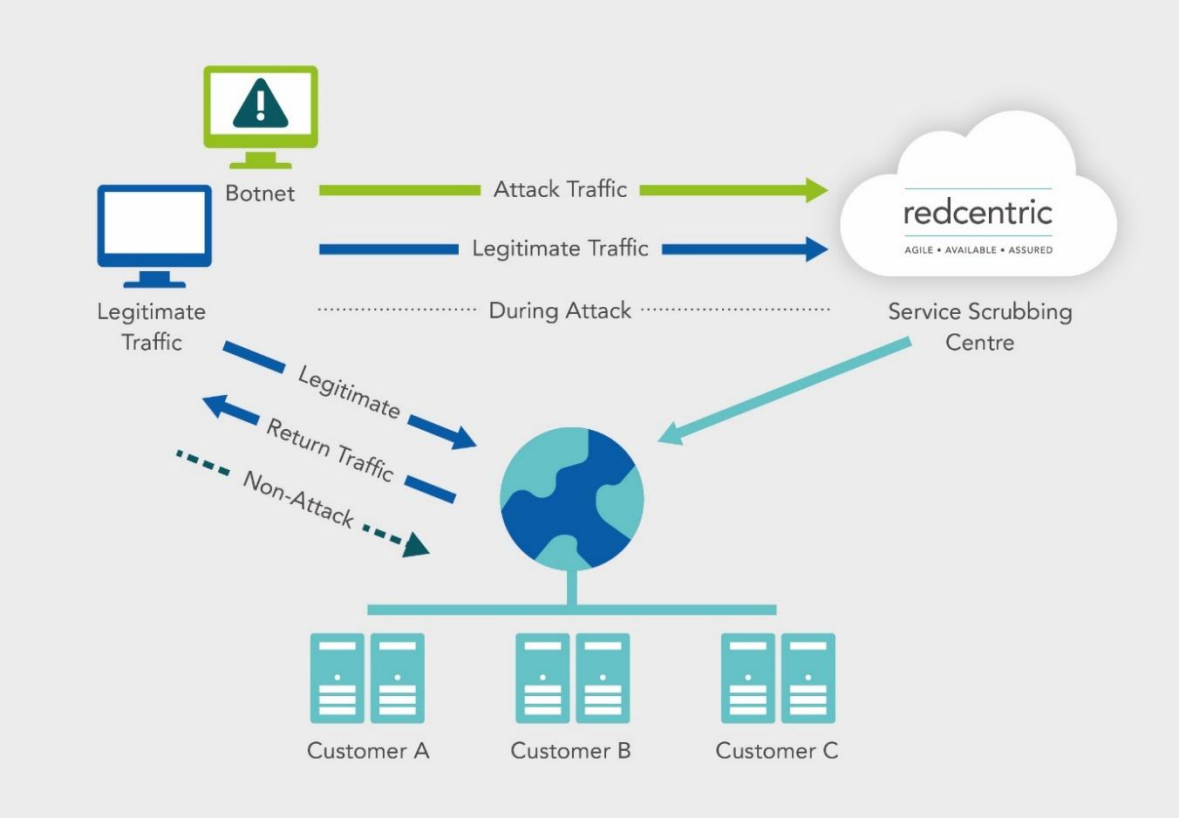
A major advantage of this service is that no network changes or configuration is required for a customer to become protected, all the traffic is analysed and scrubbed at the service provider level, when required. There is no need for complex tunnels or any peering to be established between the Redcentric network and the customer.

During normal ‘peace’ time, traffic will flow in and out of the Redcentric network via normal service. If attack traffic detected or Redcentric see a High-Level Alert. Redcentric will offload the traffic into the on-net scrubbing centre, mitigating the volumetric traffic and passing the cleaned traffic back into the network to be routed on to the customer. Outbound traffic will not return via scrubbing but be sent out of the customers’ default path. When a DDoS attack is detected our scrubbing service will re-route the IP address under attack directing just traffic destined for that IP to be cleaned, all remaining traffic will pass to the customer. Multiple IP’s can be mitigated concurrently.

This service monitors the flow of data from the Redcentric internet edge routers using Netflow. The routers are configured to send the flow data to the service flow collectors via dedicated links. Because traffic is monitored at the ISP (internet service providers) level, Redcentric gain visibility of the traffic into the customer network allowing us to determine when any attacks begin.

The dedicated links are used to pass the cleaned traffic back to the network. This design allows for zero touch configuration upon customer mitigation.

DDoS Essentials and DDoS Essentials Plus have a pre-defined mitigation policy that is non customisable. If a customer takes the DDoS Pro service a mitigation policy is designed to meet customer requirements, which is a is a bespoke set of enabled counter measures assigned to a managed object which is applied as the default set of rules in the event of a DDoS attack. This allows for whitelist/blacklists to be applied immediately, unused ports and protocols to be blocked and much more. In the Appendix 1 is a list of the available countermeasures, any one of them can be applied to a mitigation template.



1.3 Key Features and benefits

Subject to the DDoS service offer, the DDoS Mitigation service provides:

- Mitigations are continually updated to ensure DDoS traffic is scrubbed and ‘clean’ legitimate traffic is passed successfully back into the customer network.
- Monthly reports and annual service reviews.
- Bespoke attack thresholds reviewed by Redcentric.

- Tailored mitigation templates ensuring optimised performance when attacks are mitigated.

1.4 Levels of Service

	Standard	DDoS Essentials	DDoS Essentials Plus	DDoS Pro
Response Time	Black Hole	60 minutes	15 minutes	Automatic
Reactive Service	N/A	Yes	Yes	Always On
Shared Policy	N/A	Yes	Yes	No
Dedicated Policy	N/A	No	No	Yes
Periodic Reporting	No	Quarterly	Monthly	Monthly
Incident Reporting & Analysis	Cost Option	Cost Option	Cost Option	One per year
Edge ACL's	No	No	No	Optional
External Mitigation	RTBL	Yes >5Gb	Yes >5Gb	Yes >5Gb

1.5 Service Implementation

Standard

- Customers IPv4 public address space is added to the Black Hole policy.

The service is delivered by a Redcentric engineer who will be appointed as part the project plan.

DDoS Essentials

- Customer IPv4 public address space is added to the DDoS Essentials policy.
- Customer contacts verified and tested.

The service is delivered by a Redcentric engineer who will appointed as part the project plan.

DDoS Essentials Plus

- Customer IPv4 public address space is added to the DDoS Essentials DDoS policy.
- Customer contacts verified and tested.
- Reporting configured, enabled, and tested / confirmed.

The service is delivered by a Redcentric engineer who will appointed as part the project plan and will work alongside the customers technical representative to define the required bespoke policy.

DDoS Pro

A pre-requisite to deployment is a technical information gathering exercise. Information required to deploy the Service includes but is not limited to the following aspects:

- Service Mitigation Templates

- Contact details for report recipient(s).
- Customer Technical Representative contact information.

A Redcentric Project Manager will engage with the customer and establish a project plan. The Project Manager coordinates procurement/ordering, configuration, deployment, testing and hand-over tasks.

The service is delivered by a Redcentric engineer who will appointed as part the project plan and will work alongside the customers technical representative to define the required bespoke policy.

If the configurations/templates are to be deployed by a Redcentric engineer, installation. Configuration, and basic testing will be undertaken between 9:00 and 17:00. Deployment work outside of these hours can be accommodated with explicit up-front agreement in writing by both parties prior to finalising a Service Agreement.

1.6 Monitoring

Redcentric will monitor the DDoS mitigation platform to ensure Redcentric can meet the defined service levels.

1.7 Reporting

Standard

- No service reporting included.
- Incident Analysis (available as a Professional Service exercise) / Advanced Incident Reporting.

DDoS Essentials

- Scheduled Quarterly Reporting of DDoS events.
- Incident Analysis (available as a Professional Service exercise) / Advanced Incident Reporting

DDoS Essentials Plus

- Standard Incident reporting.
- Incident Analysis (available as a Professional Service exercise).

DDoS Pro

- Monthly Scheduled Reporting of DDoS events.
- Incident Analysis (1 included annually, additional can be provided as a Professional Service exercise) / Advanced Incident Reporting.

1.8 Incident Management

When a high severity event is triggered or identified and validated by a member of the Redcentric support team, an interaction is raised. Tickets are managed by the Redcentric operations centre 24x365.

If the issue relates to an element not supplied by Redcentric, Redcentric will notify the customer contact in accordance with the Customer Welcome Pack. Redcentric is unable to engage with customers third-party suppliers directly.

1.9 Maintenance Notice and Scheduled Downtime

To provide a robust service, Redcentric occasionally performs upgrade and maintenance tasks on systems and platforms. Details of maintenance windows and how they are communicated are detailed in the Redcentric Customer Welcome Pack and Master Service Agreement documents which should be read in-conjunction with this document.

1.10 Change Notice

Redcentric occasionally updates and improves services and adds new features as it strives to provide Customers relevant and valuable services. The Redcentric Master Service Agreement details the implications of Service Change and how it will be communicated.

1.11 Customer Requested Changes (DDoS Pro only)

Redcentric support staff manage the configuration of the DDoS Mitigation service, evaluating and implementing formal change requests submitted by the customer.

The evaluation and subsequent implementation or rejection of change requests will be performed Monday to Friday between 8:00 and 18:00, with a target completion time of 48 hours for routine changes where a scheduled date/time is not agreed. Emergency changes are prioritised accordingly, and performance targets are detailed in Redcentric Standard Service Level Targets and Priorities document.

In accordance with the Redcentric change request procedure, all change requests must be submitted by a designated and authorised Customer technical contact. If the 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 service change.

It is extremely easy to weaken service integrity and/or security by submitting a seemingly innocuous change request. Redcentric review change requests based only on the information they have available, and therefore Redcentric cannot take responsibility for service weakness resulting from rule-base changes.

If Redcentric support team believe that a change in mitigation policy request compromises the security of the customer 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, we reserve the right to reject the change outright; for example, if the weakness could affect other Redcentric customers.

Appendix 1 - IPV4 countermeasures

Policy	Description
Invalid Packets	Drops invalid Packets
IPv4 Address Filters	Uses address filters to block
IPv4 Black/Whitelists	Uses black and whitelists to allow or deny
IP Location Filter Lists	Block or Deny based on GeoIP
Zombie Detection	The Zombie Detection countermeasure uses configured threshold values to identify and block hosts (“zombies”) that send excessive amounts of IPv4 traffic to be protected hosts or networks. This packet-based countermeasure can protect against common attacks including flood, TCP SYN, and protocol attacks. It should be noted that this mitigation may cause disruption to aggregated traffic such as a VPN concentrator or firewalls
Per Connection Flood Protection	The Per Connection Flood Protection countermeasure monitors IPv4 traffic on a per-connection basis (5tuple) rather than on a per-source basis. When the IPv4 traffic of any connection exceeds the maximum configured rates for bps or pps, then the countermeasure can block all of the traffic of that connection or limit the rate of the traffic of that connection.
TCP SYN Authentication	The TCP SYN Authentication countermeasure intercepts and authenticates all inbound IPv4 and IPv6 TCP connections to the protected hosts. It can protect against TCP SYN flood attacks and any TCP flag attack, such as ACK floods or illegal TCP flag combinations. In these attacks, the TCP protocol is misused to

Policy	Description
	consume a target's resources. In this countermeasure, the TMS appliance acts as a proxy for the protected hosts to verify that the source host completes a three-way SYN/ACK handshake. If the source host is authenticated, then that host is approved and allowed to connect to the protected hosts. The host remains approved until it does not send a TCP packet within the configured timeout period. If the source host is not authenticated, it is assumed to be malicious, and the connection is not allowed. A host that fails TCP SYN authentication is not blacklisted; any subsequent TCP connection attempt can be used to authenticate that host. Note: If you enable DNS Authentication in Active TCP mode, then TCP SYN Authentication is disabled for port 53.
DNS Scoping	Inspects each request and compares reg-ex to a query and is applied to DNS counter measures
DNS Authentication	The DNS Authentication countermeasure authenticates DNS requests before they reach the DNS server and drops the requests that cannot be authenticated within a specified time. This countermeasure can protect your network against spoof attacks, which occur when an attacker spoofs multiple source addresses in an attempt to overload a DNS server with queries. This countermeasure filters traffic at the packet level.
TCP Connection Limiting	The TCP Connection Limiting countermeasure limits the number of concurrent TCP connections that can originate from a single host. This countermeasure prevents attacks that overwhelm the victim's connection resources with an excessive number of TCP connections. The TCP Connection Limiting countermeasure mitigates IPv4 attack traffic. For example, some botnets open hundreds of active or inactive TCP connections. A sufficiently substantial number of connections can consume all of the resources of a server and prevent the server from accepting legitimate traffic.
TCP Connection Reset	The TCP Connection Reset countermeasure tracks established TCP connections and drops the traffic when a connection remains idle for too long. This countermeasure can prevent idle TCP connections from filling server connection tables. This countermeasure also allows you to blacklist hosts that send extremely slow requests. Although TCP Connection Reset is primarily event-driven, it includes per-packet monitoring of TCP packets so that TCP packet fragments are detected both to reset idle timers and to detect highly fragmented slow application requests.
Payload Regex	Regex checked against the payload data
Source /24 Baselines	No Longer Used
Protocol Baselines	The Baseline Enforcements countermeasure helps protect your network from uncharacteristic surges in traffic volume. For this countermeasure, Peak flow SP collects historical traffic data from the configured managed object. If traffic rates exceed a calculated baseline threshold, then the TMS appliance dynamically blacklists the traffic.
DNS Malformed	Malformed DNS Packets
DNS Rate Limiting	The DNS Rate Limiting countermeasure limits the number of DNS queries that a host can send per second. This countermeasure prevents attacks from legitimate hosts who misuse DNS requests to flood DNS servers. After a host is authenticated, this countermeasure monitors the DNS queries from the source IP address. Any traffic that exceeds the configured rate limit is dropped and the source is blacklisted.
DNS NXDomain Rate Limiting	The DNS NXDomain Rate Limiting countermeasure monitors response packets for hosts that send requests that might cause non-existent domain (NXDomain) responses to be generated. This countermeasure protects against DNS cache poisoning and dictionary attacks. Any host that generates more consecutive failed DNS requests than the configured limit is blacklisted. This countermeasure requires that the TMS appliance be configured in the following ways: ● The appliance must be deployed inline to receive requests and responses. This allows it to detect and correlate the domain-specific relationship. ● The appliance's mitigation capability option must be enabled on both the input and output interfaces.
DNS Regex	Regex checked against the payload data
HTTP Malformed	Malformed HTTP Packets

Policy	Description
HTTP Scoping	Inspects each request and compares reg-ex to a query and is applied to HTTP countermeasures
HTTP Rate Limiting	The HTTP Rate Limiting countermeasure limits the rates at which a host can send HTTP requests. This countermeasure prevents a host from overwhelming the resources of a Web server, either by sending too many requests or by requesting too many unique objects. After a host is authenticated, this countermeasure monitors the HTTP requests from the source IP address. Any traffic that exceeds either of the configured rate limits is dropped and the source host is blacklisted. The default HTTP rate limits are usually acceptable for typical users. Because a Web server can be heavily loaded by a small number of HTTP requests, do not increase the limits by substantial amounts without careful consideration. If you must make an exception for a content mirror server, you can add it to a pass rule in the Black / Whitelist filter.
AIF and HTTP/URL Regex	Regex checked against the URL (Uniform Resource Locator) Structure
SSL Negotiation	Monitors SSL Handshakes
SIP Malformed	Drops Malformed SIP Packets
SIP Request Limiting	Limit on number of concurrent or per second SIP Requests
Shaping	Traffic Shaping
IP Location Policing	When you enable IP Location policing rate suggestions on a managed object, peak flow SP creates per-country traffic baselines that you can use to mitigate the managed object's traffic. This countermeasure allows you to mitigate traffic by doing the following: allowing all traffic to enter your network from either specified or unspecified (Other) countries All "allowed" traffic is not necessarily passed. Some allowed traffic could ultimately be dropped as the result of other enabled countermeasures. blocking all traffic from entering your network from either specified or unspecified (Other) countries limiting (rate shaping) the rate of traffic that enters your network from either specified or unspecified (Other) countries

2. Onboarding and Offboarding

2.1. Onboarding

Our project and delivery teams implement the service. In conjunction with the customer, our project, delivery, and support teams will work with the customer to agree a window where a period of baseline network activity is carried out to populate the scrubbing service with “normal” traffic patterns. This involves turning on the service prior to any DDoS event. Information on DDoS event notification by the customer to our support desk is shared and general communications protocols for any attack notifications are established, as several DDoS attacks are pre-empted by the bad actor to the end customer.

2.2. Acceptance Criteria

Acceptance Criteria applicable to the DDoS Mitigation Service are:

DDoS Essentials

- Confirm Redcentric support contact details have been supplied.
- Contact details for report recipient(s) have been received from the customer and verified.

DDoS Essentials Plus

- Confirm Redcentric Support contact details have been supplied.
- Contact details for report recipient(s) have been received from the customer and verified.

DDoS Pro

- Confirm Redcentric Support contact details have been supplied.
- Contact details for report recipient(s) have been received from the customer and verified.
- DDoS Mitigation policy defined and implemented.
- Test the functionality and notification mechanisms of the service.

2.3. Offboarding

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

3. Services Availability

3.1 Service Availability

Service Level: Availability Measurement Period: Month	
DDoS Mitigation Service	Not less than 99.5%

3.2 Exclusion from Availability

In calculating Availability, in addition to the exclusions listed in clause 7.9 Part A - General Terms of the Redcentric G Cloud Supplier Terms the following shall be excluded:

- Unavailability due to tasks required to implement and test change requests.
- Unavailability due to scheduled maintenance windows.

3.3 Service Levels

The service level applicable to the Redcentric DDoS Mitigation service in respect of availability shall be 99.5% in any given month.

3.4 Service Credits

The Service Credits applicable to the DDoS Mitigation service shall be calculated as follows.

In the following table:

"≥" means "greater than or equal to".

"<" means "less than".

"MS" means the charges payable in respect of the DDoS Mitigation Service for the same month.

Service Availability	Service Credit
≥ 99.5%	none
≥ 99.0% but < 99.5%	5% of MS
≥ 97.0% but <9 9.0%	15% of MS
< 97.0%	20% of MS

4. Associated Redcentric Services

The table below provides details of other compatible services with DDoS Mitigation Services available from Redcentric via on 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.
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 firewall control traffic between devices on different networks and provides perimeter protection. The firewall is configured by our staff to meet customer's requirements. Firewalls are monitored for alerts.
Managed LAN Switch Services	**Managed Local Area Network (LAN) Switch Services** provides an Ethernet LAN switch located on a customer site to provide connectivity between compatible, hard-wired Ethernet LAN devices. Typically, the switch would be the central connectivity point for PCs, Internet Protocol (IP) phones, servers, printers etc.
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.
Secure Remote Access Service	**Secure Remote Access Service** offers a robust, scalable, flexible, and secure way for remote users to access information and business applications whilst away from their usual work location. Software on the user's device communicates with the remote access platform across any Internet connection and a secure tunnel is established.
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 Management and Redcentric managed network devices. The 2FA service offers a more secure and scalable alternative to static passwords.
Wireless Guest Access	**Wireless Guest Access** is an analytics and marketing service provided by our partners Purple. Redcentric resells, integrates, and supports the service. Used with wireless services to provide guest Wi-Fi experience, and venue owners valuable information on their customers and visitors, focused marketing communication and assists in the compliance implications associated.

5. Responsibilities and Accountabilities

5.1 High Level Redcentric Responsibilities

Redcentric is responsible for the following:

- Configuration of the DDoS Mitigation Service and the associated systems.
- Management / upgrade / patching, reporting and Change Management.
- Alerting platforms.
- Notify Customer of high severity incidents.
- Provide reporting dependent on service level.
- Provide IP addresses seen in significant attacks such that the customer can report to the Police.
- Service Availability.
- Routing traffic during incidents to the mitigation platform.

Redcentric will work with customers of the DDoS Pro service to produce, agree, and implement a service design based on information supplied by the customer.

5.2 High Level Customer Responsibilities

Standard

No customer responsibilities.

DDoS Essentials

- Contact details for report recipient(s).
- If the customer suspects that a DDoS event is underway in their environment, the customer informs Redcentric of this occurrence via the normal Redcentric support contact channels.

Note Redcentric may engage the service earlier if the level of traffic causes, or risks causing network disruption in any way.

DDoS Essentials Plus

- Contact details for report recipient(s).
- If the customer suspects that a DDoS event is underway in their environment / has received a plausible threat of an impending DDoS event occurring, the customer informs Redcentric of this via the normal Redcentric support contact channels.

Note Redcentric may engage the service earlier if the level of traffic causes, or risks causing network disruption in any way.

DDoS Pro

- The customer will work with Redcentric to define the mitigation template for the required service.
- Contact details for report recipient(s).
- Customer Technical Representative contact information.
- The customer will provide Redcentric with up-to-date list of staff authorised to submit change requests.

Note DDoS Pro is an automated service; therefore, no input is needed from the customer with regard to the ‘normal operation’ of this service.

6. Business Continuity and Disaster Recovery

6.1 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 Centers
- 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 Centers, 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 is designed and engineered to deliver available, stable connectivity to maintain business access to critical applications. To maximise resilience, multiple carriers provide core connectivity and routing, and switching devices are 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 Tier-1 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.

6.2 Disaster Recovery

The service is comprised of multiple resiliency elements and thus has no specific disaster recovery. Any interruption in primary service automatically fails over to secondary services to ensure continuity of service. There are multiple levels of resiliency built into the service, including multiple levels of filtering services and geographic resiliency across multiple locations.

7. Data Processing

7.1 Data Processing Scope

The Redcentric DDoS Mitigation Service delivers a degree of IP network perimeter protection and may involve the storage of summarised traffic and user activity.

7.2 Data Storage and Encryption

By the very nature of the service, it is necessary for Redcentric to capture, inspect, analyse, and store summaries the customer traffic flow data. It is possible that unencrypted packet headers may be stored during an active mitigation.

Redcentric would not have access to the content of the customer 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 traffic to investigate and diagnose specific problems.

7.3 Data Processing Decisions

Redcentric does not make any data processing decisions in relation to the Redcentric DDoS Mitigation Service. Any processing of data over customer systems when using the Redcentric DDoS Mitigation 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 Redcentric DDoS Mitigation 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.

7.4 Sub-processors

The Redcentric DDoS Mitigation Service may make use of services provided by its validated partners. These services assist with the identification and mitigation of security vulnerabilities, weaknesses, exploits, virus, worms etc.

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

7.5 Customer Access to Data

The customer controls its own platforms which use Redcentric DDoS Mitigation Service, and the customer therefore has full access to its own data.

7.6 Security Arrangements and Options

The Redcentric DDoS Mitigation Service may be hosted at both Redcentric and third-party locations. All Redcentric appointed locations meet physical security standard ISO27002 section 11.1.

8. Exit Plan

Upon expiration of the Contract where the customer chooses not to renew with Redcentric, the steps set out in paragraph 2.3 will apply.

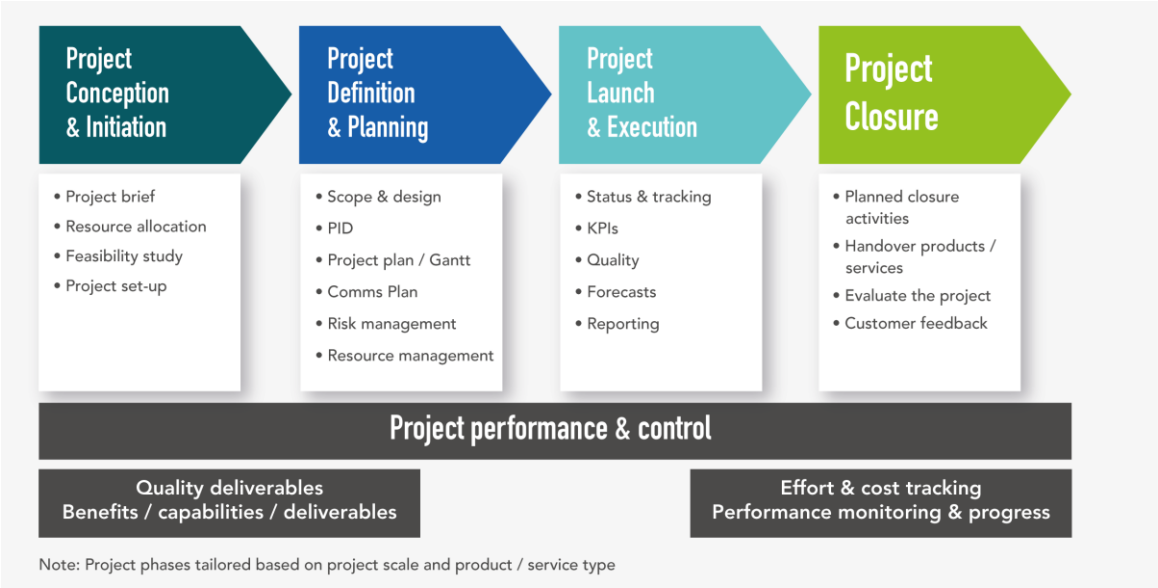
9. Project management

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

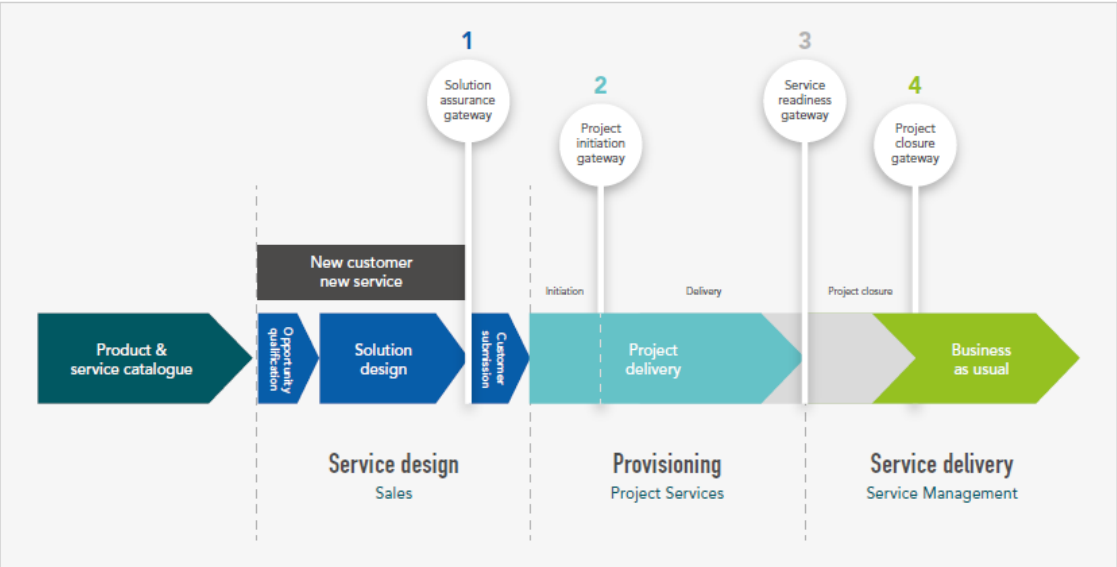
- Test plan to minimise disruption to your business operations
- Communications plan that defines what information to share and with whom
- Site implementation tracker to record the migration progress
- Weekly highlight report providing project updates
- Customer Service Pack
- UAT Test Report – per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

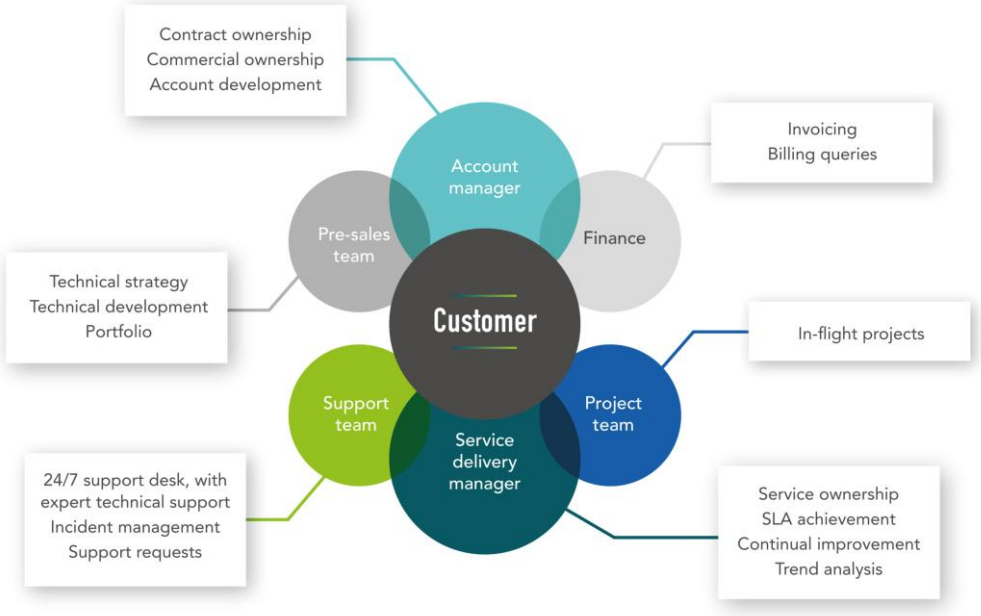
- Technical delivery is achieved on time and to specification
- The support model is fit for purpose and available at service commencement
- You will experience a ‘soft landing’ with minimal disruption to service.



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.

10. 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.

11. 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.

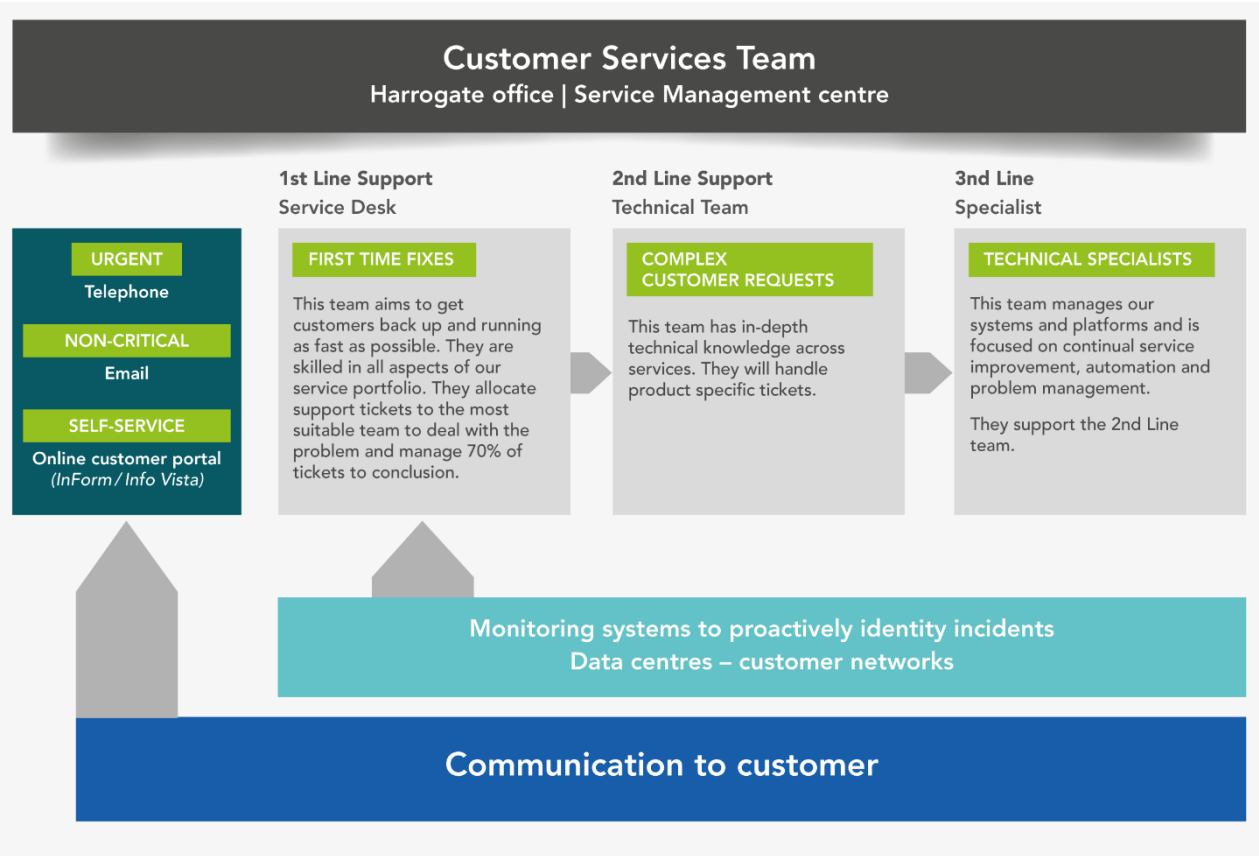
12. Support Services

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.

13. 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.

14. 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.

15. 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.

16. 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

ISO 9001 Quality Management
ISO 14001 Environmental Management
ISO/IEC 20000-1 Information Technology Service Management
ISO 22301 Business Continuity Management
ISO/IEC 27001 Information Security Management