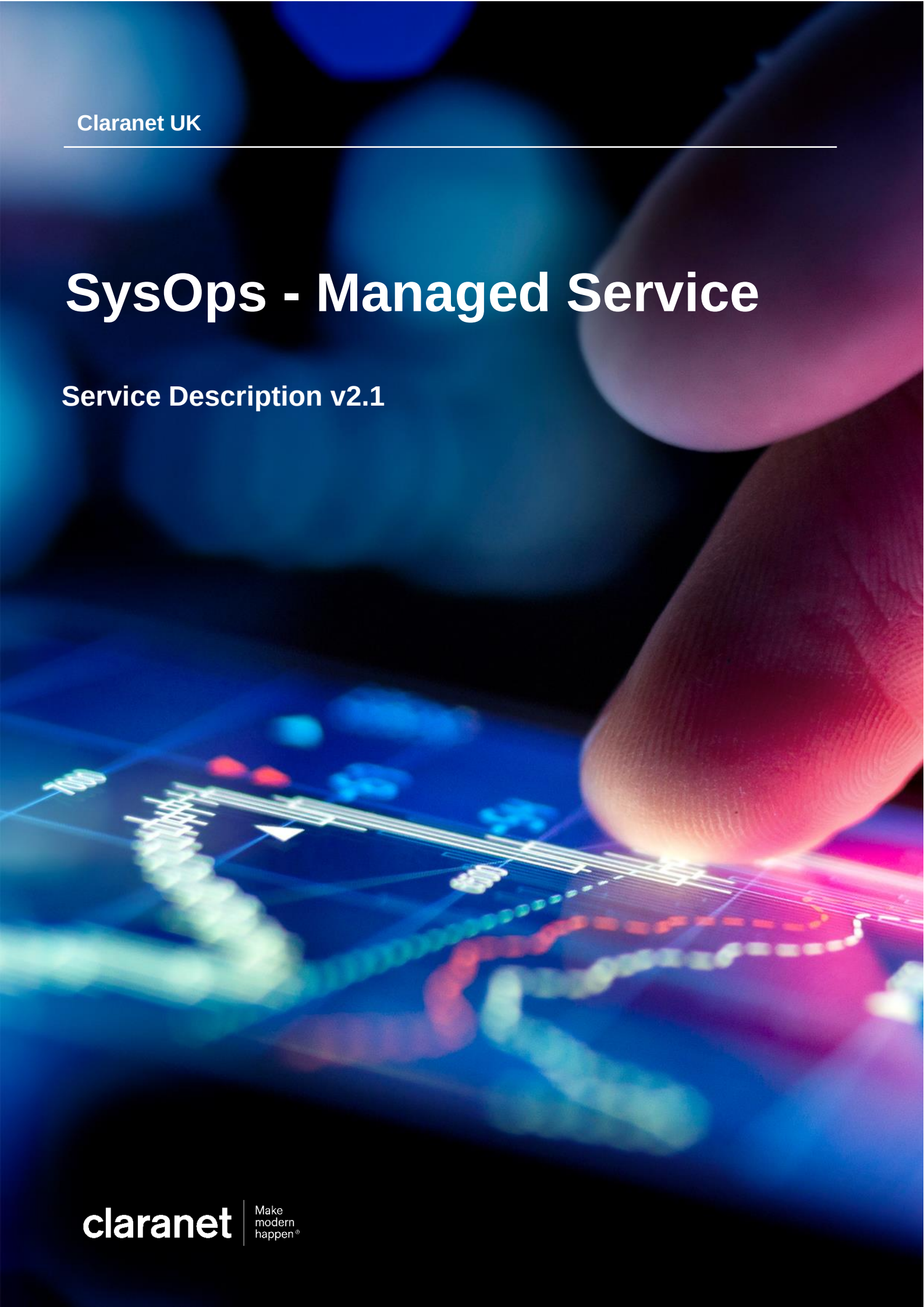
Claranet UK

SysOps - Managed Service

Service Description v2.1



claranet | Make modern happen®

Contents

1. Introduction 3

2. Scope of Service Description 3

3. Service Overview 4

4. Service Components 4

4.1. Monitoring 4

A. Standard offering 5

B. Roles and Responsibilities 5

C. Onboarding 6

4.2. Patching 6

A. Standard offering 7

B. Optional/Additional 7

C. Roles and Responsibilities 8

D. Onboarding 8

4.3. Operating System Management 8

A. Standard offering 9

B. Optional/Additional 10

C. Roles and Responsibilities 11

D. Onboarding 11

4.4. Security Controls 11

A. Standard offering 12

B. Optional/Additional 12

C. Roles and Responsibilities 13

D. Onboarding 13

4.5. Reporting 13

A. Standard offering 13

B. Optional/Additional 14

5. Delivery Matters 14
5.1. Change Management 14
5.2. Service Levels 15
6. Assumptions and Exceptions 15
7. Terminology 16
8. Appendices 17
Reporting sample 17

1. Introduction

This Service Description outlines the service provided by Claranet for the standard SysOps Managed Service (“SysOps”) and is an integral part of the Agreement between Claranet and the customer. The document is subject to the terms of the Claranet Master Services Agreement (“MSA”) which can be found at www.claranet.co.uk/legal and the Customer Experience for Managed Services Document (“CXMS”) which can be found on Claranet Online Portal, or as otherwise agreed by the Parties. All terms used in this document are in accordance with the terms set forth in these documents.

CXMS provides a framework for Claranet’s core support experience and describes what a customer can expect from any standard Managed Service solution provided by Claranet. It outlines the responsibilities of both Claranet and the customer, including how to log and escalate cases, how SLA targets are prioritized, set, and achieved, as well as the tools used to perform these functions.

This Service Description is intended to complement the CXMS and provides details specific to the SysOps Managed Service. It describes any additional solution-specific components that the customer can expect and defines the responsibilities of both Claranet and the customer in relation to this Service.

The latest version of this document can be found on the Claranet Online Portal.

2. Scope of Service Description

The scope of this Service Description includes only the services, activities, and deliverables that are expressly set out within it. Any components that are described as optional or additional will be charged at additional costs to the Customer and must be expressly referenced as such in the relevant Customer Order Form or Statement of Work.

If the Customer requests a change to the scope of work under this Service Description, the request will be subject to additional costs and must be agreed upon by the Parties through an Order Form or Change Request. Claranet reserves the right to charge for any additional work on a time and materials basis.

The Customer shall cooperate with Claranet and be responsible for the performance of its resources, representatives and agents in the Customer’s Roles and Responsibilities in this Service Description. The Customer will provide a suitable primary contact for the length of the Service with the necessary knowledge and experience to provide required assistance to Claranet pursuant to this Service Description and/or SOW. The Customer will provide access to key staff, stakeholders and third parties, where relevant, and ensure all are available for any meetings and/or workshops. Additionally, the Customer is responsible for notifying Claranet of any changes which may affect platform stability or security. The Customer acknowledges and agrees that Claranet’s performance of the Service is dependent upon, among other things, timely access to all data, information, and personnel by Claranet, that all information provided is accurate and up to date as well as the timely and effective completion of the Customer’s Roles and Responsibilities as set out herein or requested of the Customer from time to time by Claranet.

3. Service Overview

Claranet's Managed SysOps service is designed to provide comprehensive support for server operating systems irrespective of where the Customer's solution is hosted. SysOps (short for Systems Operations) is the discipline of managing and maintaining IT infrastructure, including servers, storage, and networks. Our team of experienced professionals will ensure that your server infrastructure is optimized, secure, and available at all times. A Customer may have already been through a process to design and build their solution and are now looking for Claranet to manage their environment. Alternatively, the Customer may be looking to Claranet to take over the management of an existing environment not built or managed by Claranet. Our team will work with you to assess your existing infrastructure and determine the best approach for managing your systems going forward.

Please note that our Managed SysOps service only covers server operating systems. Desktop operating systems and management services are excluded from this service. Our focus is on ensuring that your server infrastructure is reliable, secure, and performing at its best, so you can focus on running your business.

4. Service Components

4.1. Monitoring

Our Managed SysOps service includes comprehensive 24/7 monitoring of your server infrastructure to ensure that your systems are available and performing optimally at all times. Our monitoring tools are designed to detect issues before they become major problems, and our team of experienced professionals will work quickly to resolve any issues that do arise.

Key features of our Monitoring service component include:

Proactive monitoring: Our monitoring tools continuously monitor your servers, applications, and network infrastructure to identify potential issues before they impact your business. We use a combination of automated monitoring tools and manual checks to ensure that we catch issues as soon as possible.

Performance monitoring: We'll monitor your servers' performance metrics, including CPU usage, memory usage, disk utilization, and network traffic loss/latency, to ensure that your systems are performing optimally. If we detect any issues, we'll work with you to identify the root cause and take appropriate action.

Our Monitoring service component is a critical part of our Managed SysOps service, providing you with the peace of mind that comes with knowing that your infrastructure is being closely monitored around the clock.

A. Standard offering

The standard Service will include the following:

a) Platform Monitoring:

- Manage platform quotas and hard limits - ensure any managed deployments or infrastructure changes are successful.
- Planned maintenance – ensure notification is provided of any planned infrastructure maintenance that could impact the services.
- Security configuration – ensure that any events relating to changing the secure configuration of the platform creates appropriate Incidents and Risks.

b) System Monitoring:

- CPU, memory, disk utilization
- Network performance - packet loss and latency
- IP based up/down availability.
- System errors and warnings
- Services - monitor OS specific services including:
  - Windows: windows update, firewall, event log and time
  - Linux: system, syslog, ntp

B. Roles and Responsibilities

Responsibility	Claranet	The Customer
Standard Offering: All items referred to in A. Standard Offering	✓	
Application Incidents – For application incidents it is expected that one or more of the Customer's engineering team will be available alongside the Claranet team to assist in timely resolution.	✓	✓

C. Onboarding

The onboarding phase covers the steps involved in ensuring that Claranet can manage the Customer's environment as effectively as possible. It also covers any additional tasks that may have been outlined as part of the Statement of Work.

Scope:

- Platform access – ensure that service account access is provided between the customers environment and Claranet's monitoring platform with sufficient permissions to monitor all required resources.
- Agent deployment – where agents are required to monitor the platform then it will be required to deploy those agents onto those resources using the standard Change Management process.
- Gateway deployment – ensure that gateway appliances are deployed into the customer environment for communication between the monitoring agents and Claranet's monitoring platform. Deployment of these gateways will be managed using the standard Change Management process.
- Tagging – where resources are in-scope for monitoring they must be tagged using Claranet's tagging standards.

4.2. Patching

One of the most important aspects of maintaining a secure and reliable server infrastructure is keeping your software up to date with the latest security patches and updates. Our Managed SysOps service includes comprehensive patch management services to help ensure that your systems are protected from known vulnerabilities.

Key features of our Patching service component include:

Patch identification: Our team will do monthly reviews on the latest security bulletins and updates from software vendors to identify any patches that need to be applied to your systems.

Patch testing: Where Customers make use of staging environments, Claranet will facilitate patching the staging environment first, to allow you to test updates so they don't cause any compatibility or stability issues with your existing software before they are rolled out to production environments.

Patch deployment: Once patches have been tested and approved, we'll deploy them to your production environment during a maintenance window that minimizes disruption to your business operations. Out of hours work will be costed accordingly.

Rollback capability: In the unlikely event that a patch causes unexpected issues, we have the capability to roll back the changes and restore your system to its previous state.

Reporting: We provide a monthly report that summarizes the status of your patch management program, including any patches that were applied during the reporting period, and any outstanding patches that still need to be applied.

Compliance: Our patch management program is designed to help ensure that your systems comply with relevant regulatory requirements.

Our Patching service component is an essential part of our Managed SysOps service, helping to keep your systems secure and up to date. With our comprehensive patch management program, you can rest assured that your servers are protected from known vulnerabilities and that your infrastructure is fully compliant with industry regulations.

A. Standard offering

The standard Service will include the following:

a) Virtual Machine patching – ensure that any supported virtual machine has the latest operating system security patches that are updated monthly.

b) Virtual Machine minor upgrades – ensure that any supported virtual machine is updated to the latest minor version release of the operating system.

c) Standard Reporting as per appendix

B. Optional/Additional

Additional charges will apply in the following cases:

(a) Frameworks – ensure any application frameworks (such as Java or .NET) that are installed as part of the supported machine Operating System are updated monthly to the latest minor version release.

(b) Pre-patching Backups and snapshots to provide roll back option.

(c) Where additional update categories are required (more than security)

(d) Bespoke Reporting from standard above.

(e) Where patching is to be performed outside of standard business hours.

C. Roles and Responsibilities

Responsibility	Claranet	The Customer
Standard Offering: All items referred to in A. Standard Offering	✓	
Software Patching Ensure that all application software is kept up to date with security patches.		✓

D. Onboarding

The onboarding phase covers the steps involved in ensuring that Claranet can manage the Customer's environment as effectively as possible. It also covers any additional tasks that may have been outlined as part of the Statement of Work.

Scope:

- Health check to evaluate environment readiness. This may lead to a remediation quoted project if current environment is not deemed to be ready to onboard.
- **Agent deployment** – where agents are required to patch the platform for example: virtual machines, then it will be required to deploy those agents onto those resources using the standard Change Management process.
- **Tagging** – where resources are in-scope for patching, they must be tagged with the corresponding pre-agreed patch schedules, in accordance with Claranet's tagging standards.

4.3. Operating System Management

Managing the operating system (OS) on your servers is a critical part of ensuring that your infrastructure is reliable, secure, and performing optimally. Our Managed SysOps service includes comprehensive OS management services to help ensure that your servers are always up-to-date and configured to meet your specific needs.

Key features of our Operating System Management service component include:

Installation and configuration: We'll work with you to install and configure the operating system on your servers, ensuring that it's optimized for your specific use case.

Ongoing maintenance: We'll provide ongoing maintenance services to ensure that your operating system is up to date with the latest patches and updates, and that it's configured to meet your specific needs.

Compliance: Our OS management services are designed to help ensure that your servers comply with relevant regulatory requirements.

Our Operating System Management service component is a critical part of our Managed SysOps service, helping to ensure that your infrastructure is secure, reliable, and performing at its best. With our comprehensive OS management services, you can rest assured that your servers are configured to meet your specific needs and are fully compliant with industry regulations.

The following are the current supported Operating Systems:

- Linux:
    - CentOS 7, 8
    - Red Hat Enterprise 7, 8, 9
    - Ubuntu 14.04, 16.04, 18.04, 20.04, 22.04
- Windows:
    - Windows Server 2012, 2012 R2, 2016, 2019, 2022

A. Standard offering

The standard Service will include the following:

a) Resource management – ensure the capacity and performance of the Virtual Machine, including CPU, Memory and Disk utilization meets the customer set requirements for the applications running on that Virtual Machine.

b) Operating system configuration – ensure the configuration and maintenance of the Virtual Machine and its Operating System. This includes:
    - Enabling/Disabling specific OS features.
    - Configuring System logging.
    - Adding/Removing additional disks and/or network devices.
    - Configuring and managing clustering.

c) File system management: ensure the file systems and associated disks meet the customer defined capacity and performance requirements of applications running on the Virtual Machine.
    - Increasing file system capacity
    - Growing file systems to span multiple physical devices.
    - Changing the type and/or performance of the physical devices as may be required.

d) Management tools – ensure the installation, configuration and maintenance of all management tools required for the operating of Claranet's services. This includes but not limited to:
    - Monitoring agents.
    - Patching agents.
    - Platform-specific agent software.

e) Licensing and compliance – ensure the Operating Systems are licensed correctly to ensure compliance with legal requirements.

f) Changing network settings

g) Vendor Escalation – ensure Operating System issues that are unable to be resolved by Claranet will be escalated to the appropriate vendor on the Customer's' behalf when:
    - Customer provides the OS license, support contract and an appropriate contract details and escalation path.
    - Claranet provides the OS license and support contract.

B. Optional/Additional

Additional charges will apply in the following cases:

(a) Licensing – provide Operating System licenses where the Customer does not currently have existing licenses that can be utilised. The cloud hosting provider may provide license-included options, or these may be procured separately as may be appropriate. Appropriate support contracts will be required along with any associated licenses.

(b) Anti-malware / EDR agents – where an anti-malware or EDR solution is provided by Claranet, the cost of maintenance is included in the rate for that solution. Symantec Endpoint Protection is only available on private cloud

C. Roles and Responsibilities

Responsibility	Claranet	The Customer
Standard Offering: All items referred to in A. Standard Offering	✓	
Software Installation: Ensure that all application software, software components and associated licensing are installed and configured correctly.		✓
Versions out of vendor support: Operating System versions no longer supported by the vendor are supported on a reasonable endeavor's basis. Monitoring and alerting may be provided if technically feasible but may be limited. The Customer will be responsible for all remediation and maintenance activities.	✓	✓

D. Onboarding

The onboarding phase covers the steps involved in ensuring that Claranet can manage the Customer's environment as effectively as possible. It also covers any additional tasks that may have been outlined as part of the Statement of Work.

Scope:

- Agent deployment – where additional agents are required for example anti-malware, platform-specific agents then it will be required to deploy those agents onto those resources using the standard Change Management process.
- Re-licensing – where machines have been migrated between platforms it may be required to re-apply or re-activate appropriate licenses to ensure legal compliance prior to the commencement of the manage services.

4.4. Security Controls

Ensuring the security of your server infrastructure is critical to protecting your business from cyber threats. Our Managed SysOps service includes a comprehensive suite of security controls designed to minimize the risk of security breaches and ensure the confidentiality, integrity, and availability of your data.

A. Standard offering

The standard Service will include the following:

a) **Access Management –** ensure that Claranet's access to the Customer environments is secure, proportional, and regularly reviewed. This includes:

- Virtual Machine access by SSH or RDP, will use named accounts accessed from secure management systems.
- API Access used by any tools or scripts will be linked to individual applications or named users.
- All named accounts will access the environment using limited and propositional role-based access controls, agreed with the Customer.
- All named accounts managed by Claranet will be subject to Claranet's standard security policies including complex passwords and multi-factor authentication.

b) **Data Encryption –** ensure that all data managed by Claranet is encrypted at rest using either platform-managed or customer-managed keys. Claranet will make recommendations to ensure any deployed infrastructure and applications increase their security posture through encryption in transit, where that is appropriate.

B. Optional/Additional

Additional charges will apply in the following cases:

(a) Participation in compliance audits – from time to time it may be required for Claranet engineers to participate in internal or external customer compliance audits to review policies, controls and provide demonstrations. These should be raised as a Service Request with a minimum of three weeks' notice.

(b) Additional compliance reports or content that may be required.

(c) Security Compliance – Compliance certification remains Customer's responsibility, but Claranet will provide monthly reporting on security and data compliance controls for data under the Customer's control.

(d) Anti-Malware / EDR – there are solutions available as part of the Claranet service offering.

C. Roles and Responsibilities

Responsibility	Claranet	The Customer
Standard Offering: All items referred to in A. Standard Offering	✓	
Review of Access and Controls: Complete Bi-Annual Review of all access controls and policies. Customer will be responsible for documenting their requirements, Claranet will be responsible for implementing and maintaining suitable access controls.	✓	✓

D. Onboarding

The onboarding phase covers the steps involved in ensuring that Claranet can manage the Customer's environment as effectively as possible. It also covers any additional tasks that may have been outlined as part of the Statement of Work.

Scope:

- Access Management – ensure that all Claranet engineers that require access to support the customers environment have named accounts and sufficient permissions to do so. This includes:
    - Domain accounts for Windows environments – named accounts in the customers domain(s), within a self-managed group with local machine administrator permissions.
    - SSH access for Linux environments – names accounts with public keys distributed to all machines by infrastructure as code.
    - API access keys – keys required by Claranet's tools and scripts, with documented permissions and requirements.

4.5. Reporting

A. Standard offering

The standard Service will include the following:

(a) Patching – monthly patch reporting will be provided which includes all virtual machines, containers and other PaaS services managed by Claranet that have been patched or otherwise upgraded in the past month. It will include an indication of the patching compliance status against each asset.

(b) Health advisories – an annual health report will be provided which includes a list of any platform issues which may have had an impact to your environments (with or without associated issues)

B. Optional/Additional

Additional charges will apply in the following cases:

(a) Access Management – a report from the past 90 days showing what Claranet access (roles and named accounts) had access to the Customer environment(s).

(b) Security Recommendation (Incidents and Risk) – a monthly report on any security recommendations in the platform. This will include any issues identified as Incidents or known Risks in addition to the impact and recommended resolution.

(c) Bespoke reporting requirements

5. Delivery Matters

5.1. Change Management

Change Management is a process designed to understand and minimise risks while making IT changes. It is defined in the CXMS document along with definitions of Simple, Complex, Complex-Contract Affecting and Emergency Change Requests. Below is a catalogue of Simple Change Requests that can be made at no additional costs. Any change not specifically stated below is excluded from this service and will need to go through a formal quoting process.

Service Component	Action
Operating System Management	Adding new network devices
Operating System Management	Changing network settings
Operating System Management	Re-licensing (+AHUB)
Operating System Management	Additional Tagging

5.2. Service Levels

Service Levels are defined in the CXMS Document that can be found on ClaranetOnline.

6. Assumptions and Exceptions

Claranet excludes responsibility for meeting any service levels to the extent that meeting the service levels is affected by the following items:

(a) if the Customer is in default under the Agreement;

(b) in respect of any non-availability which results during any periods of scheduled maintenance or emergency maintenance;

(c) in the event that the Service is disrupted due to unauthorised users or hackers;

(d) in the event that the Service is unavailable due to changes initiated by the Customer, whether implemented by the Customer or Claranet on behalf of the Customer;

(e) in the event that the Service is unavailable as a result of the Customer exceeding system capacity;

(f) in the event that the Service is unavailable due to viruses;

(g) in the event that the Service is unavailable due to the Customer's failure to adhere to Claranet's implementation, support processes and procedures;

(h) in the event that the Service is unavailable due to the acts or omissions of the Customer, the Customer's employees, agents, third party contractors or vendors or anyone gaining access to Claranet's network, control panel; or to the Customer's website at the request of the Customer;

(i) in the event that the Service is unavailable due a Force Majeure Event;

(j) in the event that the Service is unavailable due to any violations of Claranet's Acceptable Use Policy;

(k) in the event that the Service is unavailable due to any event or situation not wholly within the control of Claranet;

(l) in the event that the Service is unavailable due to the Customer's negligence or wilful misconduct of the Customer or others authorised by the Customer to use the Services provided by Claranet;

(m) in the event that the Service is unavailable due to any failure of any component for which Claranet is not responsible, including but not limited to electrical power sources, networking equipment, computer hardware, computer software or website content provided or managed by the Customer;

(n) in the event that the Service is unavailable due to any failure local access facilities provided by the Customer; and

(o) in the event that the service is unavailable due to any failures that cannot be corrected because the Customer is inaccessible or because Claranet personnel are unable to access the Customer's relevant sites. It is the Customer's responsibility to ensure that technical contact details are kept up to date by submitting a request ticket to confirm or update the existing technical contact details.

7. Terminology

Unless otherwise specified, capitalized terms used in this Service Description shall bear the same meanings as those used in the MSA unless otherwise expressly stated herein. Set out below are a description of key technical terms used in this Service Description.

CPU: Central processing unit: the key component of a computer system, which contains the circuitry necessary to interpret and execute program instructions.

DNS: Domain name system: A hierarchical and decentralized naming system for computers, services, or other resources connected to the Internet or a private network.

IP Address: A unique string of numbers separated by full stops that identifies each computer using the Internet Protocol to communicate over a network.

Malware: Malware is software intentionally designed to cause damage to a computer, server, client, or computer network.

MPLS: Multi-protocol layer switching: A network routing technology that directs data from one node to the next based on short path labels rather than long network addresses, thus avoiding complex lookups in a routing table and speeding traffic flows.

RAM: Random access memory: A form of virtual computer data storage that stores data and machine code and can be searched and changed in any order.

RHEL: Red Hat Enterprise Linux

RIPE: Réseaux IP Européens: Is a forum open to all parties with an interest in the technical development of the Internet.

SSL: Secure Sockets Layer (SSL) certificates are a protocol for securely browsing the web.

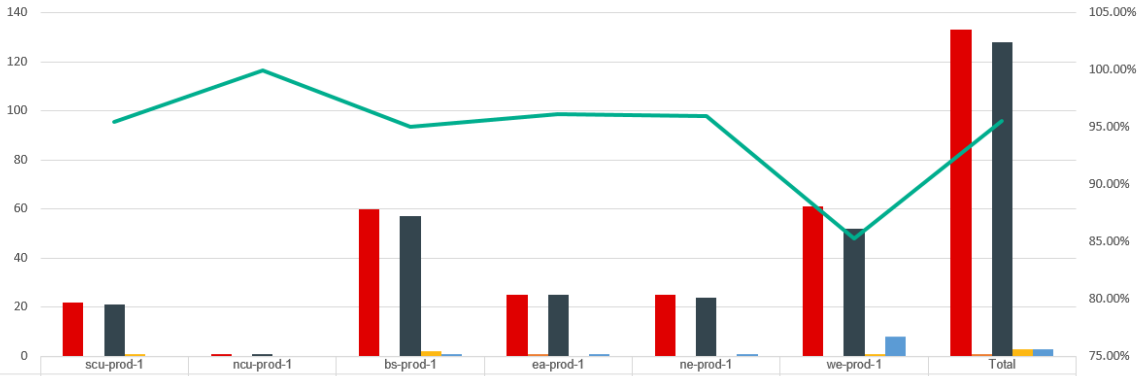
VPN: Virtual private network: Means of extending a private network across a public network and enables users to send and receive data across shared or public networks as if their computing devices were directly connected to the private network.

8. Appendices

Reporting sample

Cloud Services – Patching Report

Azure Patching Overview



	scu-prod-1	ncu-prod-1	bs-prod-1	ea-prod-1	ne-prod-1	we-prod-1	Total
Online Count	22	1	60	25	25	61	133
Offline Count	0	0	0	1	0	0	1
Compliant	21	1	57	25	24	52	128
Non-Compliant	1	0	2	0	0	1	3
Not-Assessed	0	0	1	1	1	8	3
Compliance %	95.45%	100.00%	95.00%	96.15%	96.00%	85.25%	95.52%

claranet

Standard Patch Report