Q-SOLUTION

Secure Infrastructure Software as a Service

Service Description

PRINTED COPIES ARE NOT CONTROLLED

Crown Commercial Service Supplier

ISO 27001 Certified

CYBER ESSENTIALS PLUS

For more information about our services please contact us:

Tel: +44 (07538) 023530 | email: contact@q-solution.co.uk

or write to:

Customer Services, 2 Tallis Street

London, EC4Y 0AB

Disclaimer

Any views, opinions and guidance set out within this document are provided for information purposes only and do not purport to be professional advice. No responsibility or liability is accepted for any errors or omissions in this document or related documents.

Crown Commercial Service Supplier

Information Security Management System ISO 27001 Certified

CYBER ESSENTIALS PLUS

Q-SOLUTION

Table of Contents

1 Overview

The UK Public Sector places a high emphasis on securing applications deployed to public and private clouds, as well as those hosted in-house. Organisations frequently experience an extension of their digital transformation delivery schedules beyond acceptable limits when the design, construction, security, and accreditation of the underlying Infrastructure for their applications are introduced.

Q-Solution has been delivering Secure Infrastructure Software as a Service for several years, significantly speeding up project delivery within the public sector. We offer a secure and accredited AWS Infrastructure Software as a Service, constructed with native cloud services and linked to the government's PSN Protected network.

Customers can thus develop and build their applications locally before deploying them to the scalable and robust Infrastructure, where all supporting services like User Authentication, PSN network connectivity, Protective Monitoring, and System Monitoring are already in place and operational.

1.1 Features

The following features are delivered as part of the Secure Infrastructure Software as a Service from day one

- A secure landing zone utilising Security Control Policies (SCP) and appropriate guard rails
- PSN Protected connection accredited to hold up to OFFICIAL data
- Protective Monitoring and real time alerting
- System Monitoring and alerting via services such as Slack, OpsGenie, email, SMS and .GOV notify
- Anti Malware for data in transit
- Dedicated Support desk
- 99.9% availability
- Built to scale
- Certified against Cyber Essentials Plus
- Certified against ISO27001
- Data held entirely within UK Sovereign Data Centres
- Designed against NCSC Cloud Security Principles and Architecture Patterns
- Assessed against AWS Well Architected Framework
- Assessed against Article 28 - GDPR Data Processor

1.2 Benefits

Infrastructure Benefits

Adopting this Secure Infrastructure to host your live and/or test applications comes with enormous benefits including;

- Accelerates Digital Transformation Programmes by deploying to a ‘production ready’ Infrastructure instantly using containerisation tools such AWS EKS and ECS
- Reduced Capital Expenditure (CapEx) by eliminating Infrastructure design and build costs, procuring the Infrastructure as a Service
- Deploy your applications through CI/CD Pipelines such as AWS CodePipeline or GitHub
- Connection to PSN Protected at the outset enabling early integration and testing with external systems residing on the same secure network
- Reduced maintenance overhead
- User security inherently built into the Infrastructure through Microsoft Entra SAML services
- Integrate Management information (MI) and System Monitoring into your own in house systems as required
- No requirement to build complex and time-consuming Protective Monitoring services
- Comfort that the service undergoes regular assessments against Cyber Essentials Plus, ISO27001 and independent CHECK based IT Health Checks

1.3 Monitoring

Q-Solution conducts infrastructure monitoring as a component of the Managed Service, encompassing both System Monitoring and Protective Monitoring. The accounting data, specific to the customer's infrastructure, can be made accessible for integration with the customer's internal systems upon request.

System Monitoring and Alerting

System Monitoring involves the monitoring of the underlying AWS services supporting the cloud Infrastructure. Thresholds are set for these services to generated automated alerts if they are breached. Details of these thresholds and the alerting and communication with customers will be provided during the on-boarding process and are fully customisable.

System Monitoring and alerting is provided by a variety of recognised industry leading technologies including

- OpenSearch
- Grafana Cloud
- Slack, OpsGenie, SMS and Email

Application Monitoring and Management Information

Application Monitoring can be provided for customers applications they deploy to the cloud Infrastructure. The requirements for the customers monitoring will be specific to that application and will be determined during the

on-boarding process. Q-Solution can provide custom dashboard analysis to the customer through either CloudWatch, AWS QuickSight or the System Monitoring tools noted above.

Protective Monitoring

Protective Monitoring encompasses

- Monitoring for configuration changes
- Threat Detection
- Audit Logging
- Security Alerting and Compliance

Our SIEM and Vulnerability Management tooling as well as our alerting services operate as part of the service to provide this Protective Monitoring capability. As part of the onboarding process, we will work with the customer to onboard their specific application(s) into this service.

1.4 Security and Information Assurance

Security and your data protection is the foundation of the design of the Infrastructure . The Infrastructure is subject to annual independent audits including:

- IT Health Check
- ISO27001 Information Security Management
- Cyber Essentials Plus

In addition to this, the Infrastructure provides security in the form of:

- Boundary Malware protection
- User Account auditing and suspicious activity monitoring and alerting
- Ingestion of all AWS service logs into a central Protective Monitoring solution
- Account separation

All staff operating the service are UK based and hold current government SC level security clearance.

Our Information Security Policy (which can be provided on request) further details our approach to Information Security and the controls we have in place to ensure the highest standards are maintained.

1.5 Limitations

The following are the current limitations of the service. We do however encourage customers to review these pages and the dashboard for changes made to the service as we aim to continually improve the capacity, availability and overall service provision.

- The Infrastructure is currently only accessible on the PSN Protected network and indirect networks. e.g. PSN in Policing as managed through the GCN by Vodafone
- AWS Connect PSN Protected bandwidth over VPLS port limited to 100Mbps
- The customer is responsible for the ITHC of the application they deploy and this must be concluded and the output reviewed by Q-Solution Information Assurance before access to the PSN network is granted
- The Infrastructure is available within the AWS London Region (eu-west-2) ONLY

2 Secure Infrastructure SLA

2.1 Support Hours

Support hours for the service desk is between 8am and 6pm, Monday to Friday excluding UK Public Holidays. Our Protective Monitoring and System Monitoring however operates 24/7/365 and will generate alerts throughout this period in the event of any priority incidents occurring. Agreement on how these incidents outside of core hours are resolved will be agreed during the on-boarding process

2.2 Service Level Agreement Target

Measure	SLA Component	Target Value	SLA Value
Incident Response time	P1 Response time	10 minutes	100%
	P2 Response time	30 minutes	100%
	P3 Response time	1 Hour	100%
	P4 Response time	8 Hours	100%
Incident Restoration time	P1 Restoration time	1 Hour	98%
	P2 Restoration time	4 Hours	100%
	P3 Restoration time	24 Hours	100%
	P4 Restoration time	3 Days	100%
Incident Resolution time	P1 Resolution time	4 Hours	98%
	P2 Resolution time	8 Hours	98%
	P3 Resolution time	3 Days	98%
	P4 Resolution time	7 Days	98%
Change Management	Emergency Change	12 Hours	100%
	Standard Change	2 Days	100%

Measure	SLA Component	Target Value	SLA Value
	Planned Maintenance Notification	14 Days	100%
Problem Management	Root Cause Analysis Delivery	1 Day	98%
Availability	Monthly Availability	99.95%	100%
Business Continuity	Recovery Point Objective	Zero hours	100%
	Recovery Time Objective	30 minutes	100%

2.3 Availability Target

Type	Measurement	SLA (over month)
Availability	Availability of the Infrastructure during working hours (8am to 6pm, Monday to Friday excluding Bank Holidays)	99.9%
	Availability of the Infrastructure outside of working hours.	99.5%
Service Desk	Monday to Friday, 8am to 6pm excluding UK Public Holidays	See Secure Messaging Incident Management

The Infrastructure availability outside of core hours allows for patches, change requests and enhancements to be made to the service. A scheduled maintenance window will operate typically between 8pm and 10pm with notification of changes published to the customer portal as well as communicated via the customers preferred channel.

All changes to the Infrastructure are automated using Infrastructure as Code and Continuous Integration processes. The above SLA for out of hours availability allows for approximately 1 deployed per week (assuming a 30 minute outage) if required.

Backup and Retention

The Secure Infrastructure as a Service is built using Infrastructure as code. The platform itself is backed up inline with Q-Solution Backup Policy and all appropriate regulations under GDPR.

Customers deploying their applications into the Secure Infrastructure are responsible for the own backup implementations.

3 Secure Infrastructure Incident Management

Users have two channels for raising incidents on the service:

- Email
- Online Portal

Emails can be sent to a centralised email address that will generate a ticket to be triaged and raised with the support desk. Alternatively, a portal is available that allows users to raise specific service requests directly, ensuring the information required by the service desk is provided and therefore a quick response to the incident can be achieved.

3.1 Incident

Incident Management and the response to incidents is defined through a combination of two factors:

- Urgency of the incident
- Impact of the incident

Incident Urgency

The *urgency* of the incident is defined as how quickly a resolution to an incident is required.

Category	Description
High (H)	• The damage caused by the Incident increases rapidly. • Work that cannot be completed by staff is highly time sensitive. • A minor Incident can be prevented from becoming a major Incident by acting immediately.
Medium (M)	• The damage caused by the Incident increases considerably over time.
Low (L)	• The damage caused by the Incident only marginally increases over time. • Work that cannot be completed by staff is not time sensitive.

Incident Impact

The *impact* of the incident is defined by what impact this incident is having on live operations and specifically the number of users and/or systems affected.

Category	Description
High (H)	• A large number of staff are affected and/or not able to do their job. • A large number of customers are affected and/or acutely disadvantaged in some way. • The damage to the reputation of the business is likely to be high. • Someone has been injured.
Medium (M)	• A moderate number of staff are affected and/or not able to do their job properly. • A moderate number of customers are affected and/or inconvenienced in some way. • The damage to the reputation of the business is likely to be moderate.
Low (L)	• A minimal number of staff are affected and/or able to deliver an acceptable service but this requires extra effort. • A minimal number of customers are affected and/or inconvenienced but not in a significant way. • The damage to the reputation of the business is likely to be minimal.

The diagram below defines the Priority assigned to incidents raised.

Response times for Priority incidents are defined in the Service Level Agreement Target section

Please note that as part of the On Boarding process, our Incident Management as well as our Problem Management processes will be shared with the customer and integrated into their own operating model as necessary.

Following the onboarding process, the Secure Infrastructure Service Design will be shared and where necessary, customised with the customer.

4 Secure Infrastructure Pricing

4.1 Billing and Charging

Our charging model for the Secure Infrastructure as a Service is designed to be simple and cost effective. With that goal in mind, the charges for the Infrastructure consist of 3 items

- On-Boarding Charge
- Fixed Monthly Service Charge
- AWS Services usage

4.2 Onboarding Charge

An initial onboarding charge of £5,000 applies to set a new client up with the Infrastructure. This charge provides for:

- AWS Account creation and access
- PSN-P enablement
- Registration onto the Secure Infrastructure as a Service Portal
- 1 day Protective Monitoring walkthrough

Further details of this Fixed Onboarding Charge, including the scope, responsibilities and activities can be found in the Onboarding Process Manual

4.3 Fixed Monthly Service Charge

There is a fixed monthly service charge of £1,500 per VPC (effective 30 days post completion of the onboarding process and invoiced monthly in advance) that provides the Value Add of the Secure Infrastructure as a Service including:

- Protective Monitoring
- System Monitoring
- Threat Detection
- Ongoing PSN accreditation and connectivity
- Management Information Reporting
- Service Desk

Further details of this Monthly Service Charge, including the scope, responsibilities and activities can be found in the Monthly Service Charge Process Manual.

4.4 AWS Services Charge

Consumption of AWS services by a customer will be charged back to the customer at cost plus a 3% Management Charge. As the customer will be responsible for any services used on the Secure Infrastructure, so they can remain in control of the associated costs. AWS Budgets can be configured to help customer manager their spend

Services used must be tagged in accordance with our AWS Tagging Policy and the AWS Service Usage Manual