CLOUD GATEWAY

# SOLUTION OVERVIEW

## G Cloud 15

Commercial in Confidence

27 / 01 / 2026

# Contents

# About Cloud Gateway

## Connectivity and security, delivered smarter

Cloud Gateway delivers secure connectivity, unified security, and complete observability through a single, UK-based platform. This is delivered with your choice of fully managed support, a co-managed model, or a blend of both.

We're reimagining the enterprise network, challenging outdated models and setting a new standard for how technology providers should operate. We believe connectivity and security should be agile, visible, and under your control.

## PRISM platform

### Network Simplicity. Unified Security. UK Sovereign.

The Cloud Gateway platform simplifies complex network and security infrastructure, helping you reduce risk and move faster. Built on a cloud-native Secure Fabric, the platform unifies connectivity, security, and observability through a single, API-driven control plane, creating one sovereign environment where performance, compliance, and resilience converge.

### Unified Control Plane

Our platform operates through a unified control plane that orchestrates both network and security operations from a single interface, delivering consistent policy enforcement and automated workflows across your entire infrastructure.

### SASE Capabilities

The platform enables delivery of a suite of SASE capabilities. This modular, automation-first approach abstracts vendor complexity while standardising policy and telemetry, with SIEM/SOC integration for continuous security monitoring.

### Secure Fabric & SSE Core

The platform's Secure Fabric and SSE Core provide a cloud-native, API-first architecture with zero-trust principles built in. We can auto-scale across cloud and edge locations while maintaining multi-tenant isolation.

Through intelligent automation, network and security services can be provisioned in minutes, with UK-based points of presence ensuring secure, low-latency access to internet, SaaS, and private applications.


### Operating Model

Supporting this architecture is a flexible operating model. Choose between fully managed or co-managed deployment based on your needs. Our optional 24x7 UK-based Network Operations Centre ensures continuous support, while maintaining complete data sovereignty within UK borders.

# Solutions

## Health Connect

This solution enables access to applications and resources on the Health and Social Care Network (HSCN). Connectivity to the HSCN is provided via a dedicated on-ramp delivered through our Secure Fabric. HSCN connectivity provides an IP connection to the HSCN network in line with the HSCN Compliance Framework. Cloud Gateway is an accredited Consumer Network Service Provider (CN-SP), allowing us to establish private connections to the HSCN.

The solution is secured by Foundation Security, powered by our SSE Core. This set of configurable firewall capabilities manages and controls the traffic passing through the platform to and from the HSCN and your chosen endpoint(s). As standard, we provision layer 3/4 firewall capabilities.

You may choose from one of three endpoint types to connect:

### Cloud to HSCN

This solution enables access to applications and resources on the HSCN from your Cloud Service Provider (CSP). Connectivity to the cloud is provided via a dedicated on-ramp delivered through our Secure Fabric. This enables access to a wide range of CSPs via a secure, private connection.

### Remote Access to HSCN

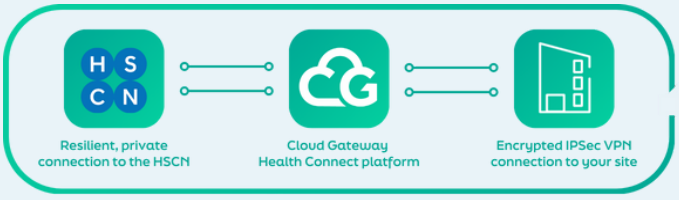
This solution enables access to applications and resources on the HSCN from remote personal devices. Connectivity to your users is delivered via a flexible termination point enabled by our Secure Fabric. Remote Access is achieved using SSL-VPN technology with Multi Factor Authentication (MFA) offered as standard.

### Site to HSCN

This solution enables access to applications and resources on the HSCN from your HQ or branch site. Connectivity to your site is delivered via a flexible termination point enabled by our Secure Fabric. Site connectivity is achieved using IPSec-VPN technology utilising your own internet circuits and hardware.


*Health Connect: Cloud to HSCN*


*Health Connect: Remote Access to HSCN*




*Health Connect: Site to HSCN*

# PSN Connect

This solution enables access to applications and resources on the Public Services Network (PSN). Connectivity to the PSN is provided via a dedicated on-ramp delivered through our Secure Fabric. Business Connect establishes an IP connection to the PSN network.

The solution is secured by Foundation Security, powered by our SSE Core. This set of configurable firewall capabilities manages and controls the traffic passing through the platform to and from the PSN and your chosen endpoint(s). As standard, we provision layer 3/4 firewall capabilities.

You may choose from one of three endpoint types to connect:

## Cloud to PSN

This solution enables access to applications and resources on the PSN from your Cloud Service Provider (CSP). Connectivity to the cloud is provided via a dedicated on-ramp delivered through our Secure Fabric. This enables access to a wide range of CSPs via a secure, private connection.

## Remote Access to PSN

This solution enables access to applications and resources on the PSN from remote personal devices. Connectivity to your users is delivered via a flexible termination point enabled by our Secure Fabric. Remote Access is achieved using SSL-VPN technology with Multi Factor Authentication (MFA) offered as standard.

## Site to PSN

This solution enables access to applications and resources on the PSN from your HQ or branch site. Connectivity to your site is delivered via a flexible termination point enabled by our Secure Fabric. Site connectivity is achieved using IPSec-VPN technology utilising your own internet circuits and hardware.


*PSN Connect: Cloud to PSN*


*PSN Connect: Remote Access to PSN*


*PSN Connect: Site to PSN*

# PRISM Platform

The Cloud Gateway platform enables delivery of a suite of SASE capabilities. Because of this modular design, customers gain the control to select and tailor the precise SASE features that align with their business requirements. Our modular, automation-first approach abstracts vendor complexity while standardising policy and telemetry.

## SASE capabilities

The following table details our portfolio of connectivity and security products, organised under three core pillars, **Connect**, **Protect** and **Observe**.

| Pillar | Offering | What it does |
|---|---|---|
| Connect | **Cloud Connectivity** | Connect quickly and securely to a wide range of Cloud Service Providers (CSPs). |
| | **HSCN Connectivity** | Connect quickly and securely to The Health and Social Care Network (HSCN). |
| | **PSN Connectivity** | Connect quickly and securely to The Public Services Network (PSN). |
| | **Managed WAN** | Delivery of physical circuit(s) to your site(s) and configuration of network devices, and Customer Premises Equipment (CPE). |
| | **Remote Access** | A scalable, secure way for your remote workers to access network endpoints and applications, utilising SSL VPN |
| | **Data Centre Connectivity** | Connect our platform to your own data centre presence, or that of an existing MPLS network provider. |
| | **VPN Site Connectivity** | Connect your sites to chosen endpoints on a 'bring your own network' basis - using your existing internet circuits and hardware. |
| | **Transit Only Connectivity** | High bandwidth network connections between your DC CSP. Traffic that traverses this service does not pass through our SSE Core. |
| | **Core Connect Managed Switches** | Directly connect your infrastructure into a pair of managed switches, housed and presented in your cabinets, in any of our data centre locations. |
| Protect | **Foundation Security** | Configurable firewall capabilities to manage and control the traffic passing through the platform from any/all connected endpoints. |
| | **Firewall-as-a-Service (FWaaS)** | Configurable firewall Unified Threat Management (UTM) capabilities to manage and control the traffic passing through the platform from any/all connected endpoints. |
| | **Web Application Firewall (WAF)** | A highly sophisticated, configurable firewall that protects your web applications from malicious attacks. |
| | **Secure Web Gateway (SWG)** | Centralised, controlled access to the internet including URL filtering, DNS inspection, and more. |
| Observe | **The Cloud Gateway Portal** | Centralised logging and visualisation to aid audits, incident response, and network monitoring. |
| | **SIEM / SOC Integration** | Receive logs from our security components, to your chosen SIEM solution for further analysis. |

## Bandwidth

The platform is available to purchase in the following licence sizes (options for less than 100Mbps may be available for some services, please ask us for details):

| | | | | | | | | |
|---|---|---|---|---|---|---|---|---|
| 100 Mbps | 200 Mbps | 300 Mbps | 400 Mbps | 500 Mbps | 1 Gbps | 2 Gbps | 5 Gbps | 10 Gbps |

## Connectivity deployment

Every network connection will be capable of handling the maximum platform bandwidth throughput you choose. You don't need to divide or allocate chunks of your licence to different connections - you have complete flexibility. If you're unsure about what bandwidth you need, you can ask your existing network provider for a usage report. Or, speak to us - we'd be happy to help.

## Security deployment

All traffic from your connected endpoints, regardless of source, destination or direction, is forwarded through our SSE Core. From here, we can set your security policy and apply it to your entire network. If you add more clouds, sites or users, the same policy will be consistently applied. The policy itself can be as granular or as high level as you wish, depending on the sensitivity of the data and your wider information security posture.

## Backup, restore, disaster recovery

This is a fully managed backup and recovery service that protects log files, system configurations, extended metadata, and related service data across multiple datacentres with disaster recovery capability. All backups are encrypted using AES-256 bit encryption and can be exported for reporting and analysis purposes.

The service provider controls all aspects of backup administration and scheduling. Users do not have direct control over backup configuration or timing. To restore data, users should contact the support team who will handle the recovery process on their behalf.

## Technical requirements

Technical requirements may depend on the specific solution deployed, for example:

- IPSec VPN connections: End user device capable of IP connectivity
- SSL VPN connections: An operating system supporting SSL VPN software
- Data Centre Connectivity: Presence in the same UK Data Centre(s)

## Security posture

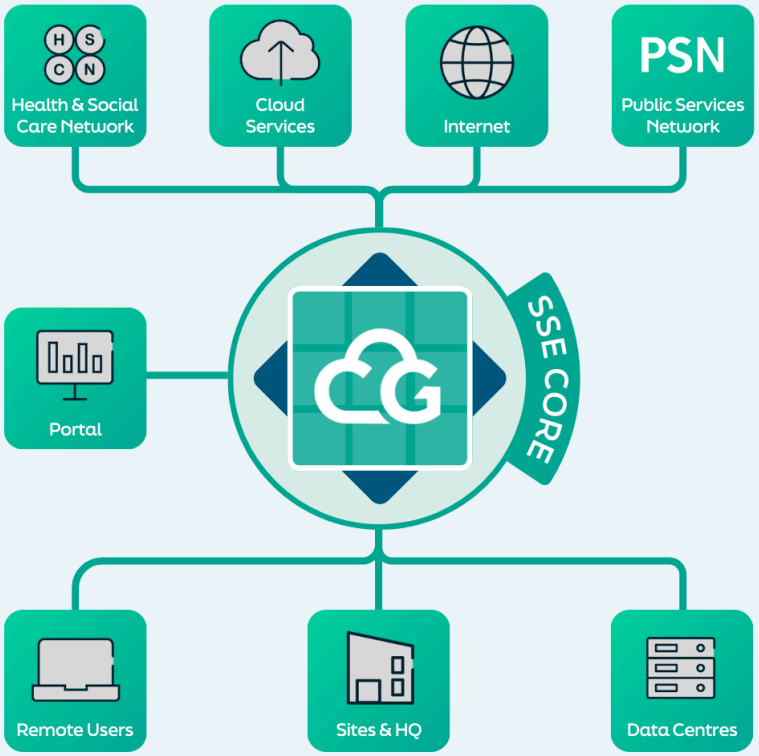
We have been ISO 27001 certified since 2020 and are certified for CyberEssentials and CyberEssentials PLUS. We additionally conduct internal audits every year.

Our service and operations undergo annual review and comply with frameworks including PSN, HSCN, and NCSC Cloud Security Principles.

Security is embedded via mandatory annual training, targeted professional development and technical controls that our employees work within at all times. Adherence to controls and our policies is enforced via signed Employee User Agreements (Acceptable Use), which reserves the right to take disciplinary action for violations.

We identify potential compromises through live monitoring and alerting on our platform. Our monitoring and alerting rules are based on AWS CIS Foundations benchmarks with additional controls and alerts for any non AWS infrastructure. These events are sent to our SIEM where alarms are triggered based on a set of configured rules.

Depending on the severity/activity, the event may be treated as an incident and response plans activated in line with the incident response procedure.




*The Cloud Gateway Platform Ecosystem*

# Professional services

## Network architecture review

Consult with Cloud Gateway's technical experts to make sense of your network sprawl and plot a secure path to cloud. Naturally, the top priority for any organisation is to keep critical workloads running. Time and money is often invested in 'keeping the lights on' which can have a detrimental impact on future development and transformation plans.

The skills needed to plan and execute a transformation programme or cloud development are very different to those needed for the day-to-day. Cloud Gateway will help you make the first step towards a network that is fit for the cloud era.

# Service management

## Supporting you and your team

Cloud Gateway offers two options for service management, **Standard** and **Premier**.

Information about our support levels, including Target Response and Resolution times, Priority definitions and small change fees, is available on our G Cloud listing.

As part of the solution you will receive access to the Cloud Gateway portal, which provides a suite of observability and telemetry features for your connected network, as well as access to support and reporting tools.

## Service levels

**Standard support** in business hours (Mon-Fri 09:00-17:30 excl Bank Holidays). Priority 1 incident response within 1 hour, resolution within 4 hours.

**Premier support** 24x7x365 P1 incident response. Priority 1 incident response within 15 mins, resolution within 2 hours. Monthly Service reports and review meetings.

Up to 5 days onboarding support included.

Our support levels meet the standard of ITIL and we are awarded with the ITIL Maturity Assessment level 3, which can be compared to ISO 20000.

## Service constraints

None

## Outage and maintenance management

Our service sends alerts to our monitoring and engineering teams to inform them of any potential outages. The issues are sanitised to see if they require manual intervention by our team, or whether automatic recovery has occurred. If manual intervention is required then a proactive alert ticket is raised within our IT Service Management system (ITSM). These tickets can be viewed by the customer at any time. Email alerts can additionally be created and sent to approved recipients for any incident relating to an outage.

We operate a robust, ITIL based Incident Management process within our end to end support model. We have extensive monitoring, configured to proactively identify potential issues and mobilise internal teams for prompt investigation and resolution. Users can report incidents via the My Cloud Gateway portal, by email or by phone. In cases where a major incident has been identified, our major incident process is utilised and email communications are issued to affected users, providing them with regular status updates throughout the incident lifecycle.

# Learn more

## Service Definitions

Full Service Definition documentation for Cloud Gateway solutions is available on request.

## Master Services Agreement (MSA)

The Cloud Gateway MSA and SLA are available attached to our G Cloud listing.