Agilisys

Cloudflare Zero Trust and SASE

G-Cloud 15 Service Definition

Lot 2a – Software as a Service

Table of Contents

1 Introduction

Agilisys is a leading innovator in Zero Trust and Secure Access Service Edge (SASE) solutions for the UK public sector. With over two decades of experience supporting local authorities, central government, healthcare, and emergency services, Agilisys leverages advanced artificial intelligence and cloud technologies to deliver transformative outcomes across a wide range of services.

Our commitment to continuous innovation empowers public sector organisations to modernise operations, enhance service delivery, and meet evolving regulatory and operational challenges. By combining deep domain expertise with innovative digital platforms, Agilisys enables clients to unlock new efficiencies, improve citizen experiences, and build resilient, future-ready organisations.

As a Cloudflare PowerUP Powered+ Partner, Agilisys is best placed to implement your Cloudflare solution.

2 Who this Service is For?

This service is designed for UK public sector organisations seeking to strengthen their security posture, modernise connectivity, and protect both internal and external digital services. This includes local authorities, central government departments, blue-light services, healthcare organisations, and multi-agency partnerships that require robust Zero Trust security, high-performance networking, and protection from evolving cyber threats.

Agilisys has extensive experience delivering Cloudflare solutions across the UK public sector. Our team has deployed Cloudflare services at scale to address challenges such as secure remote access, DDoS protection, phishing mitigation, policy-based access control, and the convergence of networking and security. As a result, this service is ideal for organisations looking for a trusted, proven partner to help modernise their security and network architectures in alignment with government best practice.

3 Agilisys Cloudflare Services - an overview

Agilisys delivers Cloudflare services as outcome-focused implementation programmes, helping public sector organisations modernise their digital infrastructure through a unified, cloud-native platform. Through the Cloudflare global network, Agilisys can provide secure, performant, and scalable services tailored for both external-facing systems and internal applications.

Cloudflare's Zero Trust and SASE capabilities allow organisations to move away from legacy, perimeter-based solutions and adopt modern cybersecurity frameworks that minimise risk and improve user experience. As a long-standing partner to the UK public sector, Agilisys brings deep expertise in implementing Cloudflare's services.

Our experience ensures rapid, secure adoption of Cloudflare technologies, enabling organisations to improve resilience, reduce complexity, minimise costs, and provide secure access to systems for employees, partners, and citizens.

3.1 Complimentary Services

Building on our extensive public-sector expertise, we provide not only ongoing SASE platform management but also the wider ICT foundations required to ensure its success. This includes identity and access management through Entra ID, secure hosting services, network design and architecture, implementation support, and operational optimisation delivered through our wider G-Cloud portfolio. By integrating these capabilities, we ensure that Zero Trust and SASE controls are implemented holistically, aligned to identity, network, application, and data layers, to maximise security posture while improving user experience.

4 Service Description

As a Cloudflare PowerUP Powered+ partner, Agilisys provides a comprehensive suite of Cloudflare services through structured service bundles, enabling public sector organisations to secure their networks, applications, users, and data through a unified, cloud-native approach. Each bundle has been designed to simplify procurement while offering the full depth of Cloudflare's Zero Trust, SASE, network optimisation, and security capabilities.

As part of our engagement, Agilisys works in close partnership with Cloudflare to fully scope your requirements, ensuring the proposed configuration of Cloudflare services aligns with your organisation's operational environment, risk profile, and strategic objectives. This collaborative approach allows us to accurately define the most appropriate mix of services, ensuring maximum value, optimal performance, and rapid adoption.

Please refer to the accompanying Terms and Conditions and Pricing Documentation.

4.1 Internal Bundle – Protecting Internal Users, Applications & Networks

The Internal bundle offers public sector organisations a comprehensive, integrated Zero Trust architecture designed to protect internal systems, applications, and users. By moving away from traditional perimeter-based security models, the Internal package enables organisations to adopt modern identity and context-driven controls that significantly reduce risk while improving user experience.

Beyond the technical components, the Internal bundle provides a transformative shift in how organisations secure their internal environments. Agilisys works with each client to understand existing infrastructure, identify security gaps, map user journeys, and determine the best migration path away from legacy VPNs and siloed security products. This ensures that Zero Trust principles are applied consistently and effectively across all user and application access patterns.

To deliver these benefits, the Internal bundle includes a suite of deeply integrated Cloudflare technologies that work together to secure internal access, protect sensitive data, and optimise performance:

- Zero Trust Network Access (Access)
- Secure Web Gateway (Gateway)
- Cloud Access Security Broker (CASB)
- Data Loss Prevention (DLP)
- Remote Browser Isolation (RBI)
- Magic WAN & Advanced Magic Firewall for internal connectivity and security

- Digital Experience Monitoring (DEX)
- Optional Email Security (pre-, link-, and post-delivery protection)

Internal Bundle	Definition
Zero Trust Network Access	Augments or replaces corporate VPN clients by securing SaaS and internal applications. Access works with your identity providers and endpoint protection platforms to enforce default-deny, Zero Trust rules limiting access to corporate applications, private IP spaces, and hostnames.
Secure Web Gateway	Keeps data safe from malware, ransomware, phishing, command and control, Shadow IT, and other Internet risks over all ports and protocols.
Cloud Access Security Broker	Cloud Access Security Broker (CASB) gives customers comprehensive visibility and control over SaaS applications to easily prevent data leaks, block insider threats, and avoid compliance violations.
Data Loss Prevention	Enables customers to detect and prevent data exfiltration or data destruction. Analyse network traffic and internal endpoint devices to identify leakage or loss of confidential information and stay compliant with industry and data privacy regulations.
Remote Browser Isolation	Makes web browsing safer and faster, running in the cloud away from your network and endpoints, insulating devices from attacks.
Magic WAN & Advanced Magic Firewall	Magic WAN enables IP level connectivity as well as a full suite of virtual network functions, including IP packet filtering and firewalling, load balancing, and traffic management tools. Magic Firewall is a cloud-based firewall enabling administrators to set policies for all traffic entering and leaving the network.
Digital Experience Monitoring	Visualize user, application, and network performance data to proactively detect and mitigate connectivity issues
Email Security	Crawls the Internet to stop phishing, Business Email Compromise (BEC), and email supply chain attacks at the earliest stage of the attack cycle and enhances built-in security from cloud email providers.

This bundle is ideally suited for organisations seeking to modernise internal security controls, replace VPNs, strengthen data protection, and streamline connectivity for distributed hybrid workforces.

4.2 External Bundle – Protecting External-Facing Systems

The External bundle provides robust protection and performance enhancement for public facing websites, applications, and APIs. Designed for councils, government bodies, and organisations delivering digital services to citizens, the bundle ensures that public facing services remain secure, resilient, and responsive, even under high load or targeted attack.

Agilisys supports clients by working directly with Cloudflare to understand service dependencies, identify externally exposed assets, and tailor the bundle to meet specific operational, compliance, and resilience requirements. The result is a unified security and optimisation layer that protects external digital touchpoints from sophisticated cyber threats while improving overall user experience.

The External bundle includes the following Cloudflare services:

- Web Application Firewall (WAF)
- Content Delivery Network (CDN) & content optimisation
- Advanced DDoS protection
- API Shield & API security
- Bot Management
- Page Shield (client-side security)
- Advanced Rate Limiting
- Load Balancing
- Magic Transit & Magic Firewall for L3 protection and routing

Externa Bundle	Definition
Web Application Firewall	Cloudflare's Web Application Firewall (WAF) blocks attacks heading towards applications - including L7 DDoS attacks - and offers better security with sophisticated, layered rulesets.
CDN & content optimisation	A CDN helps address the challenges customers face around latency, performance, availability, redundancy, security, and costs. The core goal is to decrease latency and increase performance for websites and applications by caching content as close as possible to end users or those accessing the content.
Advanced DDoS protection	In addition to protecting against Layer 3 and 4 attacks, including TCP/UDP, Cloudflare Advanced DDoS automatically detects sudden changes in traffic and protects against layer 7 DDoS attacks, so they never reach the origin server.
API Shield & API Management	API Shield helps to identify and address API vulnerabilities and comes with a dedicated certificate authority (CA) to provide strong encryption for mobile applications and IoT device traffic. API Management takes it beyond basic analytics (e.g. viewing the # of exposed APIs or % of API traffic) by including authentication through mutual TLS and a preview of discovery, for instance, identifying the number of endpoints found and showing the top issues.

Bot Management	Bot Management stops malicious bots connecting to web sites and uses machine learning on a curated subset of hundreds of billions of requests per day to create a reliable bot score for every request.
Page Shield	A client-side security technology designed to protect users from malicious code that executes in their web browsers, especially threats that originate from third-party JavaScript, supply-chain compromises, or injected scripts.
Advanced Rate Limiting	Rate Limiting provides the ability to limit the rate of requests and gain valuable insights into specific URLs of websites, applications, or API endpoints.
Load Balancing	Improves application performance and availability by steering traffic away from unhealthy origin servers and dynamically distributing it to the most available and responsive server pools.
Magic Transit & Magic Firewall	Magic Transit provides near-instant mitigation of network-layer threats (L3 DDoS attacks) from the Cloudflare global network, alongside next-generation firewall and traffic acceleration. Magic Firewall is a cloud-based firewall enabling administrators to set policies for all traffic entering and leaving the network.

This bundle is particularly valuable for organisations operating citizen facing services, transactional portals, public APIs, and high availability digital platforms.

4.3 Magic WAN & Network Services Bundle

The Magic WAN & Network Services bundle supports organisations looking to modernise their wide-area network architecture by transitioning away from costly, rigid MPLS networks toward cloud-native, software-defined connectivity. This bundle enables organisations to simplify site-to-site connectivity, enhance security controls, improve performance, and support hybrid and multi-cloud environments.

Agilisys work with you to assess existing network topology, performance requirements, and future-state connectivity goals. This collaborative approach ensures organisations receive a design that optimises routing efficiency, strengthens security, and reduces operational overhead.

This bundle includes:

- Magic WAN – WAN-as-a-Service replacing MPLS
- Magic Firewall – cloud-native L3/L4 firewalling
- Magic Transit – DDoS protection for entire IP ranges
- Argo Smart Routing – performance optimisation using real-time network intelligence

Magic WAN	Definition
Magic WAN	Extends the benefits of Cloudflare's network to customers' private networks. Magic WAN enables IP level connectivity as well as a full suite of virtual network functions, including IP packet filtering and firewalling, load balancing, and traffic management tools.
Magic Firewall	Cloud-based firewall enabling administrators to set policies for all traffic entering and leaving the network.
Magic Transit	Provides near-instant mitigation of network-layer threats (L3 DDoS attacks) from the Cloudflare global network, alongside next-generation firewall and traffic acceleration.
Argo Smart Routing	Improves Internet performance by intelligently routing end users through less congested and more reliable paths over the Internet using the Cloudflare network.

Ideal for organisations undertaking digital transformation, cloud migration, or large-scale network modernisation, this bundle delivers faster, more secure, and more resilient inter-site and cloud connectivity.

4.4 Email Security Bundle

The Email Security bundle provides advanced, multi-layered protection against phishing, impersonation, and email borne threats, the most common attack vector in the public sector by augmenting native Microsoft 365 and Google Workspace security, Cloudflare Email Security dramatically reduces risk while simplifying security operations.

Working in partnership, Agilisys and Cloudflare analyse each organisation's email architecture, inbound and outbound flows, authentication posture, and historical attack patterns. This allows us to propose the most effective configuration of pre-delivery, link time, and post-delivery controls, ensuring optimal threat detection and user protection.

The Email Security bundle includes:

- Pre-emptive phishing detection
- Malicious link & attachment analysis
- Deep contextual analysis using AI/LLM models
- Email authentication support (SPF, DKIM, DMARC)
- Post-delivery threat mitigation
- Email MDR (PhishGuard) for accelerated incident response

Email Security	Definition
Pre-emptive phishing detection	Uses AI-powered detection across hundreds of attributes from sender reputation and message sentiment to conversation context, allowing it to block phishing attacks before they reach users as well as pre-emptive campaign intelligence to stop targeted phishing attacks before delivery.
Malicious link & attachment analysis	Isolates or blocks malicious links and scans attachments, preventing ransomware and malicious code from reaching inboxes and can also isolate threats delivered through obfuscated URLs.
Deep contextual analysis	Analyses each email across hundreds of attributes using AI, ML, threat intel, and sentiment/context modelling. It uses layered, ML-based contextual analysis to detect business email compromise and impersonation attacks.
Email authentication	Strengthens SPF, DKIM, and DMARC authentication measures, which help prevent spoofing and impersonation. This reduces risk by enforcing proper sender authentication standards.
Post-delivery threat mitigation	Provides post-delivery retractions and continuous scanning, allowing it to remove or neutralise threats after an email is delivered. It also isolates deferred or multi-channel attacks that may only become malicious after initial delivery.
PhishGuard - Post-delivery threat mitigation	Managed detection and response. Cloudflare's analysts review suspicious messages and accelerate investigation and remediation. This MDR service supports organisations by reducing the SOC burden and providing expert-led post-delivery threat handling.

This bundle is ideal for public sector organisations seeking comprehensive protection from increasingly sophisticated phishing and email based cyber-attacks.

5 Managed Zero Trust and SASE services

Our Zero Trust and SASE management services provide continuous, end-to-end operational support for organisations adopting Cloudflare's modern security and connectivity architecture. Delivered by experienced security, networking, and cloud professionals, the service ensures that Zero Trust controls, secure access policies, and threat protection operates reliably and consistently. Through proactive monitoring, configuration management, optimisation, threat-driven tuning, and governance oversight, we help organisations maintain a resilient, secure, and scalable Zero Trust environment across users, devices, applications, and networks.

Our service is designed to provide flexible operating models and round-the-clock response for critical security incidents, ensuring Zero Trust protections remain active and effective at all times. We manage the full lifecycle of your SASE environment, from policy design and identity integration to secure web filtering, CASB configuration, remote browser isolation, WAN policy optimisation, and continuous enhancement based on threat intelligence. With routine compliance checks, configuration audits, and operational reporting, we ensure organisations remain aligned with UK Government, NCSC, and NHS security standards.

From identity-centred policy enforcement to hosting optimisation, we maintain the operational stability, performance, and governance of your Zero Trust and SASE platform. Whether you are securing cloud-native workloads, modernising remote access, uplifting data protection policies, or converging network and security functions under a unified operating model, our service ensures your organisation can operate with agility, resilience, and confidence while we manage the complexity on your behalf.

6 Onboarding and Offboarding

Agilisys provides a structured onboarding and offboarding process for programmes and professional services engagements.

6.1 Onboarding Professional Services Engagements

Onboarding for our professional services engagements begins with a structured mobilisation phase, designed to establish a shared understanding of the project's scope, objectives, and success criteria. This phase includes collaborative discovery workshops with key stakeholders to assess the current IT landscape, business drivers, and organisational readiness for change.

Our team conducts a review of the existing infrastructure, applications, and operating model, identifying interdependencies, risks, and opportunities for optimisation. Where appropriate, we deploy clientless discovery tooling to gather system insights with minimal disruption. This enables us to produce a tailored delivery plan, including a high-level design, migration strategy, and resource model aligned to your priorities.

We work closely with your teams to define governance structures, communication protocols, and decision-making frameworks. As part of mobilisation, we confirm all necessary access requirements, including the verification of staff security clearances (e.g. SC) to ensure compliance with your organisational and regulatory standards.

This approach ensures a secure, efficient, and low-risk start to the engagement, enabling rapid progress while maintaining full visibility and control for your organisation.

6.2 Offboarding Professional Services Engagements

At the conclusion of a professional services engagement, Agilisys ensures a structured and secure transition of responsibilities to the client's internal teams or a nominated third-party provider. Our offboarding process is designed to maintain service continuity, preserve institutional knowledge, and uphold compliance with security and governance standards.

We deliver a comprehensive handover pack, which includes relevant artefacts such as solution designs, configuration documentation, and migration records. Where applicable, we conduct knowledge transfer sessions with technical and operational stakeholders to ensure a clear understanding of the delivered solution, its dependencies, and ongoing management considerations.

Access credentials, administrative rights, and configurations are reviewed and securely transferred to the designated teams. We also confirm the revocation of Agilisys access to client environments and systems, and, where required, provide formal confirmation of data deletion in accordance with our data governance and security policies.

Our offboarding approach is flexible and can be tailored to meet specific client requirements, ensuring a smooth and confident transition to business-as-usual operations or further transformation phases.

7 Support

We offer flexible support options to align with the needs of each engagement, recognising that support requirements vary across the lifecycle of a cloud deployment or migration programme. Our support models are designed to ensure continuity, build in-house capability, and provide assurance during critical transition periods.

7.1 Early Lifecycle Support

Following each deployment milestone or line-of-business system migration, we provide early lifecycle support—typically for a period of two weeks. This is delivered by the same professional services personnel who implemented the solution, ensuring continuity of knowledge and rapid issue resolution. This model is ideal for stabilisation, user onboarding, and addressing any post-deployment refinements.

7.2 Managed Support During Programme Delivery

For clients who require operational support during the delivery phase, Agilisys can provide a managed service that runs in parallel with the professional services engagement. This ensures stability and continuity while new platforms are being deployed or migrated. We also offer a ramped support model, enabling a phased handover to internal teams. This approach allows in-house staff to progressively assume responsibility for managing the cloud environment, with Agilisys providing mentoring, shadowing, and escalation support as capabilities mature.

7.3 Transition to Agilisys Managed Services

Where ongoing operational support is required beyond the project lifecycle, clients can transition into one of our established Managed Service tiers:

7.3.1 Standard Management

Provides core business hours support (08:00–18:00, Monday to Friday), with 24/7 incident response for Priority 1 issues. It includes system management, , monitoring, cost optimisation reporting, and monthly service performance reviews. This tier is ideal for organisations seeking reliable, foundational management with essential governance and support.

7.3.2 24x7 Management

Builds on the Standard offering with enhanced capabilities such as proactive security incident response, and detailed monthly performance reviews led by a dedicated service delivery manager. It also includes proactive execution of optimisation and security recommendations, making it suitable for organisations with complex environments or higher compliance and performance demands.

Each support model is underpinned by our commitment to service quality, security, and knowledge transfer, ensuring that clients receive the right level of assistance at every stage of their Zero Trust journey.

8 Pricing

Pricing is based on the specific service requirements, service levels, scale, and scope of services using the rate card provided in the accompanying pricing document for this GCloud service.

We provide UK based onshore, and offshore resources that can be leveraged to meet your specific needs, the prevailing rates are detailed within our Pricing documents.

Please contact info@agilisys.co.uk to obtain a quote for your required services.

9 Compliance and Security

Agilisys embeds robust compliance and security practices across all stages of cloud transformation and management, ensuring public sector organisations meet regulatory obligations while safeguarding critical assets.

Our services are designed in alignment with UK Government and NHS policies, incorporating National Cyber Security Centre (NCSC) guidance and ISO27001, Cyber Essentials Plus, and other relevant certifications.

- GDPR-compliant and certified to ISO 27001, with adherence to the Data Protection Act 2018 and National Cyber Security Centre (NCSC) Cloud Security Principles.
- Data hosted, stored, and processed inside the UK/EU/EEA, encrypted in transit (TLS 1.2+) and at rest (AES-256).
- Strict access controls, including Single Sign-On (SSO), Multi-Factor Authentication (MFA), and Role-Based Access Controls (RBAC).
- Regular data protection and cyber-security training for staff, with a formal incident response plan aligned with NCSC and ISO 27001 standards.
- Full audit trails and accountability throughout the data lifecycle.

Agilisys is certified/compliant with the following standards and schemes for Managed and Professional Services and is a proud signatory of the Armed Forces Covenant:

10 Contact and Next Steps

We welcome the opportunity to support your organisation's cloud transformation journey. For further information, to discuss your specific requirements, or to request a tailored proposal, please contact us at info@agilisys.co.uk.