ConvergenceGroup

G-Cloud 15

Service Description Document

SASE Assurance Services

Convergence Group Lot 3

Cloud Support

Table of Contents

Section 1
Introduction

Why Convergence Group?

At Convergence Group (CG), we want to change the world of telecoms and network infrastructure for the better - giving you fast and reliable connectivity in a fairer and more flexible way.

Founded in 2004, Convergence Group has built an enviable reputation as an expert with LAN, Wi-Fi, WAN, Security and all the vital elements of business networking. With our highly skilled engineers, established network inventory build process and UK-based Network Operations Centre, our technological expertise combines to provide you with a complete network solution.

We are a well-capitalised and financially robust business, currently employing approximately 130 people, with annual turnover of £46 million and annual EBITDA of £9 million. We have provided connectivity to business locations for 20 years and we have organically built a network platform to support the successful transportation of an estimated 745,000 business users, across 6,300 fibre and copper connections. This connects over 4,000 buildings throughout the United Kingdom and Ireland.

Convergence Group at a glance:

- Tier 1 carrier grade network with accredited infrastructure (HSCN)
- UK-based Network Operations Centre (NOC)
- Highly skilled and experience engineers
- Our strategically positioned UK workforce ensures comprehensive coverage and expertise nationwide.
- We can provide a total network solution including LAN, Wi-Fi, WAN and security
- Range of private, direct connections to cloud providers such as Azure, AWS, Oracle, IBM and Google Cloud Platform
- Our services are underpinned by heightened government-grade security across internet, voice, cloud & private WAN site-to-site inter-connectivity solutions
- Financially strong and stable organisation

Section 2
SASE Overview

Modern organisations don’t work from one fixed place any more. People log in from home offices, branch sites and public sites while on the move, using cloud-based applications to get their jobs done. As a result, traditional perimeter-based security models aren't always the right option.

FortiSASE is a cloud-delivered Secure Access Service Edge (SASE) that fundamentally changes how organisations provide secure access to users, applications and data.

Designed for how people actually work today, FortiSASE follows users, wherever they are, to provide consistent protection and reliable access so they enjoy a seamless connection experience.

Instead of relying on a patchwork of separate security tools and on-site appliances, FortiSASE brings everything together in one cloud-native platform. That instantly eliminates the complexity and security gaps in legacy architecture that relies on multiple tools and appliances. The result is clearer oversight, stronger protection and a setup that’s far easier to manage day to day.

Built on Fortinet’s proven security technology and delivered through a global cloud platform, FortiSASE protects your users wherever they work and whatever device they’re using. As your connectivity MSSP partner, we take care of the full FortiSASE service, from initial design and implementation to ongoing optimisation and 24/7 platform monitoring.

The benefits are easy to see. Your team is allowed to focus on your priorities, while we make sure your people have fast, secure access to the tools they need, whenever and wherever they need them.

SASE Framework

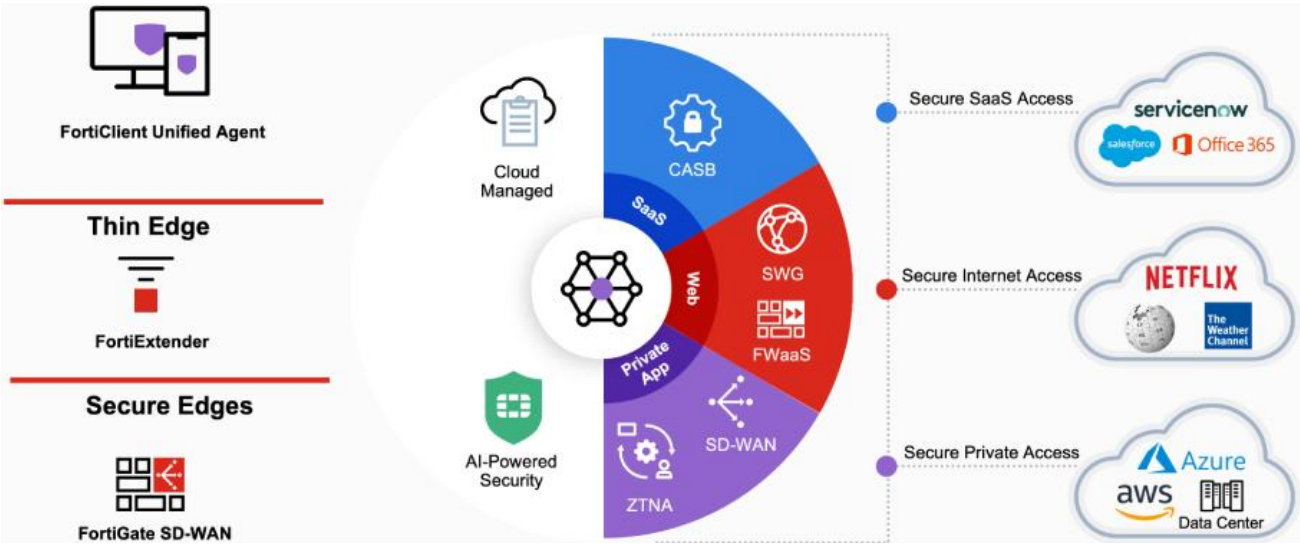
SASE architecture is made up of two main parts: Security Service Edge (SSE) and Software Defined Wide Area Networks (SD-WAN). SSE is focused on securing users no matter where they work. SD-WAN is about connecting physical sites, such as offices and branches.

Our FortiSASE service focuses on the SSE side. It delivers enterprise-grade security and optimised access through a global cloud platform, helping users work securely from any location without slowing them down.

Behind the scenes, FortiSASE brings together key security capabilities. These include zero-trust network access (ZTNA), Firewall-as-a-Service (FWaaS), secure web gateway (SWG) and cloud access security broker (CASB) capabilities. Together, these ensure your workforce can work securely from any location without compromising performance or protection.

Equally, we also recognise that one size rarely fits all. That's why SD-WAN is offered as a separate service with its own Service Description and definition. That means you can deploy FortiSASE SSE on its own, or combine it with our SD-WAN service, to create a fully unified SASE solution.

Whatever you decide, we can tailor any solution to your architecture, your priorities and the way your organisation actually works.



SASE Components

- **Secure Web Gateway (SWG) -** This protects users whenever they access the internet. It filters web traffic, blocks known threats and helps prevent sensitive data from being exposed – all the while enforcing your organisation's acceptable use policies. Web access is controlled using FortiGuard web filtering categories, with the flexibility to 'allow' and 'block' lists, where needed.
- **Zero Trust Network Access (ZTNA)** - Identity-based access controls that verify users and devices before granting access to specific applications and services. This acts as an alternative method to traditional VPNs, with a more secure, granular approach.
- **Firewall-as-a-Service (FWaaS)** - Cloud-delivered, next-generation firewall protection that includes intrusion prevention, malware detection and application control for all user traffic.
- **Cloud Access Security Broker (CASB)** - Visibility and control over cloud application usage with data protection, compliance monitoring and threat detection for SaaS applications.
- **SD-WAN Integration -** Intelligent traffic routing and WAN optimisation that ensures maximum performance for business-critical applications while maintaining security.

Use Cases

Secure Internet Access (SIA)

Protect users online, wherever they're working, using one consistent set of web security policies.

With FortiSASE, internet traffic no longer needs to be routed back through corporate data centres. Instead, users connect directly to the internet, with full security inspection applied at the cloud edge. This approach is ideal for organisations with distributed teams that need advanced threat protection, web filtering and acceptable use controls, no matter where they're working from.

Secure Private Access (SPA)

Provide secure access to internal applications without the complexity of traditional VPNs.

FortiSASE uses a zero-trust approach, granting access based on identity and application, not broad network reach. Applications remain hidden from unauthorised people, while legitimate users can access only what they need to do their job.

This is particularly valuable for organisations using zero-trust security, managing third-party access, or looking to reduce their attack surface by removing unnecessary network exposure.

Secure SaaS Access (SSA)

Gain clear visibility and control over how SaaS applications are used across your organisation.

FortiSASE helps uncover shadow IT, protects sensitive data and monitors compliance across cloud services such as Microsoft 365, Salesforce and other business-critical applications.

This use case supports organisations moving more of their workloads to the cloud, helping them maintain consistent security policies across both sanctioned and unsanctioned applications.

Benefits

- Unified Security Policy: Consistent protection across all locations, users and devices managed through a single console.
- Improved Performance: Direct-to-cloud connectivity and global points of presence reduce latency and improve user experience.
- Simplified Management: Converged platform eliminates the complexity of managing multiple point solutions.
- Scalability: Cloud-native architecture that grows with your business needs.
- Enhanced Visibility: Comprehensive insights into user activity, application usage and security threats.

Section 3
Deployment Scenarios

Effective deployment of FortiSASE begins with a clear understanding of endpoint software and configuration requirements. Ensuring endpoints are correctly prepared allows the solution to align seamlessly with the way users work across your business.

FortiSASE supports three primary deployment models:

- **Managed / Agent-based**
- **Unmanaged / Agentless**
- **Site-based**

Each deployment type offers different levels of control, visibility and security coverage to meet user and business needs.

Managed Endpoints – Agent-based

An agent-based deployment is designed for devices that are managed by your organisation.

These are typically corporate endpoints, joined to your domain and governed by your existing security and compliance policies. Management is handled centrally, using Mobile Device Management (MDM) or similar platforms capable of distributing the required software and certificates. This approach provides a controlled, consistent setup that's easy to manage at scale.

In this model, the FortiClient agent and a security certificate are installed on each managed device. Once in place, FortiClient creates a secure connection to the FortiSASE Points of Presence (PoPs), allowing users to access applications safely from anywhere. This supports zero-trust access, consistent security policies and centralised management, while integrating seamlessly with the wider Fortinet security platform. The result is secure remote access that's easy for users and straightforward for IT teams to manage.

Security Internet Access (SIA)

Through an agent-based deployment, all internet-bound traffic from managed devices is securely routed through the FortiSASE cloud. This allows security policies to be applied consistently, no matter where your users are working.

This service can enforce a range of protections, including:

- DNS Filtering
- Web Filtering
- AntiVirus Protection
- Video Filtering
- File Filtering
- Application Control
- Zero Trust Network Access (ZTNA)

Secure Private Access (SPA)

FortiSASE provides two straightforward ways to create secure, private access to internal applications and networks. The right connection depends on your existing setup and how you want users to connect.

1. SD-WAN On-Ramp Integration
    - FortiSASE integrates directly with Fortinet SD-WAN, a Fortinet Branch device or third-party firewalls using industry-standard protocols such as IPSec and BGP.
    - This approach extends the enterprise network securely into the cloud while maintaining performance and policy consistency across sites.
2. ZTNA Reverse Proxy Method
    - FortiSASE can provide access to private resources without traditional VPN connectivity.
    - A FortiGate appliance (physical or virtual) is deployed at the network edge or application location, acting as a ZTNA gateway.
    - Endpoints using FortiClient establish direct, encrypted DTLS tunnels to the FortiGate, securely accessing authorised resources based on user identity and device posture.

Both SPA methods may need additional licensing or configuration and should be scoped as part of the solution design.

Secure SaaS Access (SSA)

Access to SaaS applications is routed through the FortiSASE cloud platform and enforced by inline Cloud Access Security Broker (CASB) policies. This ensures all interactions with business-critical SaaS apps, such as Microsoft 365, Google Workspace, and Salesforce are monitored and protected.

Inline-CASB enables organisations to:

- Detect and manage sanctioned and unsanctioned applications in motion.
- Enforce access and data protection policies based on user identity and device posture.
- Prevent data loss through real-time content inspection.
- Maintain compliance with corporate and regulatory requirements.

This approach provides consistent visibility and security for SaaS use without affecting user experience.

Unmanaged Endpoints – Agentless

An agentless deployment is designed for devices that aren't owned or centrally managed by your organisation using MDM software.

These devices may still be joined to your domain and able to receive settings through Group Policy Objects (GPO), but no software installation is required. Instead, browser-based traffic is securely routed through FortiSASE using a proxy auto-configuration (PAC) file. This approach provides controlled, web-level protection without the overhead of managing software on the device itself.

For agentless deployments, users are prompted to sign in when accessing web-based resources. This usually happens once per browser session, with a default idle timeout of one hour, which can be extended up to 72 hours, if required.

Authentication can be linked to your existing identity systems, such as Active Directory/ LDAP, RADIUS or SAML. This ensures access remains secure and controlled even when devices aren't centrally managed.

Secure Internet Access (SIA)

With an **agentless deployment,** Secure Internet Access uses the FortiSASE **Secure Web Gateway** (SWG) to protect users as they browse the web.

Only web traffic (HTTP and HTTPS) is routed through FortiSASE, where security policies, threat detection and content filtering are applied. Other types of traffic remain unaffected.

To inspect encrypted web traffic and apply deeper security controls, additional security certificates may be required. These certificates are generated, distributed and managed by the customer and will be discussed as part of the overall solution.

Secure Private Access (SPA)

In an **agentless deployment,** access is limited to browser-based connections. As a result, Secure Private Access is supported only for private web applications connected using the **SD-WAN On-Ramp** method.

Access is granted based on user identity and the specific application being requested. This ensures users can only reach the internal resources they're authorised to use – nothing more.

Secure Saas Access (SSA)

Agentless Secure SaaS Access is delivered using FortiCASB, which connects directly to cloud applications such as Microsoft 365 or Dropbox.

This connection uses secure, API-based integration with OAuth 2.0 authentication. FortiCASB collects and analyses user activity for monitoring, reporting and detecting suspicious behaviour. Operating out-of-band, FortiCASB does not impact application performance. Administrators can respond to alerts by updating FortiSASE policies, adjusting FortiGate NGFW rules, or restricting access within the SaaS application retrospectively.

Site-based

Thin Edge Deployment

The Thin Edge approach involves using lightweight FortiGate or FortiSASE-capable appliances at branch or office locations. These devices serve as local security gateways, providing:

- Full tunnel capabilities that forward all traffic to FortiSASE, regardless of the user or device connected.
- Policy enforcement at FortiSASE for both managed and unmanaged devices.
- Simplified onboarding for devices and users at the branch location.
- This method is ideal for smaller sites or locations with minimal infrastructure but still requires consistent security policies and centralised management.

SD WAN

For larger sites or locations with more complex networking requirements, FortiSASE can integrate with Fortinet SD-WAN or compatible third-party SD-WAN solutions. This integration provides a secure, high-performance and resilient network foundation for both users and applications. Key benefits include:

- Optimised Connectivity: Traffic is intelligently directed to FortiSASE Points of Presence (PoPs) based on application type, performance and latency requirements, ensuring efficient and reliable access.
- Policy-Driven Routing: Internet, private and SaaS traffic is routed securely according to centrally defined policies.
- Enhanced Resiliency: Dynamic path selection and failover capabilities maintain connectivity in the event of circuit or device issues.
- Centralised Management: Site connectivity and security policies can be managed centrally using the FortiSASE cloud to simplify operations.
- Support for Diverse User Types: Enables connectivity for users who do not need to route traffic through FortiSASE, such as guest users.
- Branch-Specific Requirements: Supports additional branch requirements, including segregated guest and IoT networks.
- Comprehensive Site Connectivity: Addresses full network needs, including circuit redundancy, device resiliency and wireless connectivity at the site.

By combining SD-WAN with FortiSASE, organisations can ensure secure, resilient and optimised connectivity for all users and devices. This extends the benefits of cloud-delivered security to branch locations.

Section 4

Key Considerations

A key part of any SSE deployment is deciding how to protect users and devices that sit outside the main access models – such as guest users or IoT devices in offices and branch locations. These devices still need connectivity and a basic level of protection.

SD-WAN with integrated LAN and Wi-Fi can help address these scenarios by:

- Providing controlled guest access through captive portals, backed by Next-Generation Firewall (NGFW) security.
- Protecting IoT devices using Unified Threat Protection (UTP) to reduce risk and limit exposure.

Planning for these 'edge' cases helps ensure that security, compliance and performance remain consistent across all connected devices – not just the obvious ones.

Section 5
Service Overview

FortiSASE is delivered as a fully managed service, providing comprehensive coverage across the entire solution lifecycle. Our service includes:

Initial Deployment

Tailored solution design, architecture planning and implementation to meet your exact needs. Our team works with you to understand security policies, user populations and application landscapes, configuring FortiSASE to deliver top-level protection and performance from day one.

Monitoring

We provide 24/7 operations centre monitoring of your FortiSASE environment to ensure continuous availability, security enforcement and operational health.

Incident Management & SOC Integration

Our security operations team monitors FortiSASE around the clock, investigating and responding to security events as they happen. Alerts are quickly assessed, threats are contained and remediation is coordinated to minimise disruption and reduce the risk of repeat incidents. The focus is simple: to keep your environment secure and your teams free to get on with their work.

Policy Management

We take care of the ongoing management of your security policies, access controls and threat prevention rules. Policies are regularly reviewed, updated and refined to reflect changes in your business and the evolving threat landscape. This keeps your security posture strong, without adding any day-to-day burden to your internal teams.

Regular Service Reviews

Regular reviews of your **FortiSASE** service, including performance, security posture and opportunities for improvement. These sessions include clear reporting on usage patterns and threat activity, along with practical recommendations to strengthen security and improve the user experience.

Co-Management

Flexible operational support allows responsibilities to be shared, creating a seamless partnership between your IT team and our experts.

24/7 Technical Support

Round-the-clock access to our support team for technical issues, service requests and incident escalation. Multiple support channels and guaranteed response times ensure your FortiSASE service remains operational and effective.

Section 6
Information assurance

Convergence Group is proud to hold both the ISO 27001:2013 and Cyber Essentials accreditations, demonstrating our unwavering commitment to information assurance and cybersecurity. ISO 27001:2013 certification attests to our adherence to international standards for establishing, implementing, maintaining and continually improving an information security management system (ISMS). This certification validates our robust approach to identifying and managing risks, ensuring the confidentiality, integrity and availability of sensitive information. Additionally, our attainment of the Cyber Essentials accreditation underscores our dedication to implementing essential cybersecurity measures, safeguarding against common cyber threats and vulnerabilities. These accreditations serve as testament to our proactive stance in safeguarding our data assets and providing assurance to our stakeholders regarding the security and resilience of our information systems.

Section 7
Social value

Convergence Group understand the significance of Social Value and the profound impact that advancing the 5 social value themes can have on society as a whole. That's why we've integrated several initiatives and actions aligned with the central government's objectives outlined in the Social Value Model. While some of these efforts may not be directly tied to specific contracts, they serve as a testament to our commitment to the Social Value Model. Partnering with CG means collaborating with an organisation dedicated to championing this agenda and actively working to drive positive change.

The Social Value Model: Theme 1 - Covid-19 recovery

- Run our 'CG Academy'; an entry-level intake programme which provides an opportunity to those who are perhaps out of work or have little experience.
    - All training is provided across a 12-week programme and successful candidates are taken on full-time
- All employees are empowered to take ownership of their personal development and can create a Personal Development Plan (PDP) to help us understand their career aspirations and agree steps/objectives to help them achieve this as well as any additional training or support that is required.
- Employees have access to various learning management systems and resources to help further their personal development and learning:
    - Go1 Learning Management System, CBT Nuggets & INE

The Social Value Model: Theme 2 - Tackling economic inequality

- We have worked with local charity Birmingham Pathfinder to understand how we can support and give back to our community, specifically the children and families whom they partner with. This support includes:
    - Providing resource (donating equipment, mobiles/laptops) to the charity to support them to do their job.
    - Donating unwanted furniture which was used to furnish their support centre but also donated to families in need.
    - Food bank collections, including gifts over festive periods.
- We have more recently partnered with a local secondary school which provides placements to students for whom mainstream education is simply not working (for a range of reasons), to run an 'apprentice' style programme.

    - Applicants gain interview experience as part of our intake process.
    - Each applicant is asked to create a business proposal which could win £5k investment at the end of the programme.
    - The programme shall run over the course of 8 weeks and each student gets 1:1 mentoring/support from one of our employees.
- Across this programme they shall engage in various team building exercises to help improve and develop their skillsets ready for the world of work.

The Social Value Model: Theme 3 - Fighting climate change

- ISO14001 Certified since 2017, we are continually working to minimise the environmental impacts of our organisation's activities.
- ISO9001 Certified to drive conforming products and services and prevents duplicate emissions as a result of failing to get things 'right first time'.
- Home based engineers across the UK to minimise travel required to customer sites and reduce emissions.
- Strategically placed stores/spares to ensure SLA's are met and again minimise travel required to fulfil contractual obligations.
- Established Carbon Reduction Plan and associated NetZero objective available via our website.

The Social Value Model: Theme 4 Equal opportunity

- We are an equal opportunities employer with an established Equal Opportunities Policy.
- We are a Living Wage Employer which shows that we pay all our employees the 'Real Living Wage'.
- Well established learning and development processes, including transparent Skills Matrices that are regularly reviewed and can help identify opportunities to upskill.
- Compliance with Modern Slavery Act 2015, our statement is available via our website and relevant employee training/awareness undertaken.
- Established Whistleblowing Policy.

The Social Value Model: Theme 5 - Wellbeing

- ISO45001 Certified to promote employee health, safety and wellbeing.
- Employee NPS undertaken to gain direct feedback from our employees and understand what actions we can take to improve the workplace environment and promote positive wellbeing.
- Qualified Mental Health First Aider
- Employee benefits include Private Medical insurance and 24/7 access to an Employee Assistance Programme.

In addition to the above we are looking to formalise our Social Value Policy and associated objectives to further promote the Social Value Model and provide a framework for monitoring/measuring our success toward achieving this.

Section 8
Contact information

We are committed to providing exceptional service and ensuring your satisfaction. Should you have any questions, concerns, or require further assistance, please do not hesitate to contact us. Our customer support team is available 9:00am – 5:30pm, Mon-Fri on 0845 270 2709 or email us at sales@convergencegroup.co.uk and we will be more than happy to assist you. Thank you for considering Convergence Group for your service needs.