MLL Telecom Ltd

SD-WAN and SASE Overlay

Service Definition

Date: January 2026

MLL Ref: G Cloud 15 - RM1557.15

SASE - Service Definition

About MLL

MLL Telecom is a leading provider of managed Wide Area Networks and telecommunication services including LAN, Unified Communications (UC), Wi-Fi, and Security to the UK public sector. Our services are provided through our MLL's UK based support teams and engineering service and selected partners. Formed in 1991, MLL has established a reputation for customer-focused service delivery and agility.

Service Overview

MLL's SD-WAN and SASE services provide secure access to cloud, internet, internal applications and data. This is regardless of where your users are physically located. It incorporates SD-WAN and Security Service Edge (SSE) to provide seamless connectivity for users.

The service is fully supported by MLL's UK based 24x7x365 NOC and field engineering services.

Service Description

MLL SASE

MLL SASE is a fully cloud hosted platform, with a software client (or clientless option) for users who consume the service, with a single dashboard for management and analytics.

The core platform is fully diverse, resilient and fully managed.

At a basic level, MLL SASE provides the below CORE components,

Network Services,

- SD-WAN for optimized connectivity
- WAN optimization and traffic routing
- Quality of Service management

Security Services,

- Cloud access security broker for cloud application security
- Secure Web Gateway for web filtering and threat protection
- Zero Trust Network Access for application access control
- Firewall as a Service for network security
- Data Lost Prevention to prevent sensitive data leakage
- Advanced threat protection and malware detection

Connecting People, Not Premises

This solution works, regardless of the location of the user or application allowing for true hybrid working.

This service allows customers to grant per-user and per-session secure access to web, cloud, and applications regardless of where they have been deployed, combined with fully integrated enterprise-

grade security and ensures that the same level of protection, visibility, and user experience is extended to every user, anywhere.

Features List

- FWaaS - FortiSASE FWaaS is a cloud-based service that provides hyperscale, next-generation firewall (NGFW) capabilities, including web filtering, advanced threat protection (ATP), intrusion prevention system (IPS), and Domain Name System (DNS) security.
- Secure Web Gateway (SWG) - is delivered through FortiGate and FortiProxy Solutions, offering complete websecurity and content filtering to safeguard users against online threats.
- ZTNA - a capability within Zero Trust Access (ZTA) that controls access to applications. It extends the principles of ZTA to verify users and devices before every application session. ZTNA confirms that they meet the organisation's policy to access that application.
- API-CASB - API based CASB is a cloud security solution that integrates directly with cloud applications via their Application Programming Interfaces (APIs) instead of intercepting network traffic. This method delivers visibility into how cloud applications are used, their configuration settings, and stored information by connecting with the cloud service's underlying infrastructure.
- Inline-CASB - a cloud security function that sits directly in the data path between users and cloud applications, actively intercepting and inspecting traffic in real time. This routes traffic to cloud applications through the CASB infrastructure before it reaches its destination.
- Data Loss Prevention (DLP) - constitutes a security strategy combined with technological solutions designed to find, monitor, and prevent sensitive or confidential information from moving beyond an organization's authority.
- Botnet-protection - security defences and technologies intended to find, prevent, and mitigate hazards from botnets. These are networks of infected computers, servers, IoT devices, or other internet-linked systems remotely managed by hostile actors.
- Secure SD-WAN - integrates with MLL's Secure SD-WAN service while optimising the connectivity between distributed locations, data centres and cloud resources.
- SOCaaS Integration - Security Operations Centre as a Service integration refers to the process of connecting an outsourced Security Operations Centre with an organisation's existing IT infrastructure, security tools and business systems.
- Unified agent - One agent supporting multiple use cases. The agent can be used for ZTNA, traffic redirection to SASE, and Endpoint protection without requiring multiple agents for each use case.
- Agentless connectivity - This enables users and devices to securely access the internet, SaaS applications and private web-based applications without the need to install the FortiClient endpoint agent. This is particularly useful for BYOD devices.
- Endpoint protection - offers security, compliance and authorised access controls while eliminating threats on a single device.

Standards based delivery

MLL uses industry standards for project and service delivery as summarised in the table below:

Delivery and Service Management	Industry Standard
Service Management	ITIL
Project Management	PRINCE2
Quality Management	ISO 9001
Security Management	ISO 27001 and Cyber Essentials Plus
Environmental Management	ISO 14001
Health and Safety Management	ISO 45001

Delivery

large scale deliveries are supported by one of MLL's Project Managers. The scale of the solution required will be determined during assessment of the initial enquiry from the Buyer. MLL's technical engineer will hold a technical workshop with the Buyer's technical team to assess the Buyer's SASE requirements, and the range of optional services required.

MLL follows an ISO 9001 audited delivery process and maintains an ISO 27001 audited configuration and change management process for customer hosting infrastructure. MLL's Project Managers are PRINCE2-qualified and, where assigned, will be MLL's stakeholder to manage the project delivery. MLL uses PRINCE2 methodologies to deliver projects, typically employing the following 4 stages of project delivery:

- Internal project set-up (including contract award, team assignment, etc)
- Project Initiation (Kick-off meeting, risk assessment, technical discovery, technical workshop, project and technical documentation)
- Project Delivery (solution delivery, risk and issue management, change management, progress reporting, escalation management, governance, progressive handover to MLL's Business as Usual (BAU) team, etc)
- Project Handover (complete handover to MLL's BAU team, project review, lessons learnt, project closure, etc).

MLL's team will undertake regular project reviews with the Buyer to an agreed frequency. For larger projects, governance will be provided through a project board comprising senior sponsors from MLL and the Buyer.

Lead time to deliver services in this offer are expected to range from between 10 and 20 working days from receipt of order, assuming no unexpected delays. The lead time to deliver MLL SASE is entirely dependent on the Buyer's overall requirements. It will be assessed and advised during the technical workshop.

Support

Management

- The service will not be proactively monitored by MLL.
- The Buyer will be responsible for the day to day administration and management.
- The Buyer will raise Incidents to MLL for suspected faults, and MLL will log the Incident with Fortinet.
- Incidents will be managed using MLL's Incident Management Service through to resolution.
- MLL will provide access to the MyMLL service portal to raise and track Incidents.

Service Desk

MLL's Network Operations Centre is based in Marlow, Buckinghamshire, supporting customers on a 24 x7x365 basis.

The NOC and Service Desk undertakes the following functions:

- Receives Incident or Service Requests by agreed contact methods – telephone, email or via MyMLL portal.
- Records Incident or Service Requests on the Service Management System.
- Allocates a Call to Severity 1, 2, 3 or 4 and where relevant manage the Incident through to Resolution in accordance with the Service Levels.

Support Model

MLL's service support model is based on ITIL compliant processes with clearly defined roles and responsibilities, supported by industry recognised systems and tools.

Incidents will be raised reactively by the Buyer and logged in MLL's IT Service Management system.

MLL will log

MLL utilise the following Severity Definitions for Incident Management:

Category	Definition
Severity 1	The Services are Unavailable across the entire Buyer's estate
Severity 2	The Services are Unavailable at one of the Buyer's sites
Severity 3	The Services are Unavailable to an individual user
Severity 4	All other Incidents, including any Incidents raised initially at a higher Severity Level that were subsequently deemed to be attributable to the Buyer or in any other way not attributable to the Supplier.

MLL will ensure that Incidents are resolved within the Incident Resolution Time, based on the Severity Level of the Incident.

Service Hours

Monday – Sunday (including Bank Holidays) - 00:00-23:59, (24 hours per day, 7 days per week).

Service Levels

Incident Resolution

Service	Severity 1	Severity 2	Severity 3	Severity 4 (Indicative Only)
MLL SASE	5 Hours	8 Hours	End of next Working Day	10 Working Days

Availability

Core Infrastructure	Availability
MLL SASE	99.99%

Service Credits

Service Element	Coefficient (m)	Service Level Threshold % (a)	Service Failure Threshold % (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
MLL SASE	5	99.99%	95.99%	5%	25%

Incident Resolution

Number of Incidents per Service Period	Coefficient (m)	Service Level Threshold (a)	Service Failure Threshold (b)	Minimum Service Credit % (c)	Maximum Service Credit % (d)
39 or fewer	Not applicable	No more than 2 Incidents	5 or more Incidents are	2.5% (payable when 3	5% (payable when 4+

		are Resolved in excess of the max Incident Resolution Times	Resolved in excess of the max Incident Resolution Times	Incidents breach the Service Level Threshold in any Service Period)	Incidents breach the Service Level Threshold in any Service Period)
40 and more	0.25	95%	85%	2.5%	5%

Social Value

MLL is committed to providing social value as part of its contractual deliverables which will be agreed with the Buyer and detailed in the call-off contract.

MLL will deliver social value against the following themes:

Fighting Climate Change, underpinned by MLL's existing ISO 14001 environmental management system and published carbon reduction plan with a net zero target date of 2040.

Tackling Economic Inequality, we will deliver tailor-made offers to support the communities and citizens in the localities in which we serve our customers.

Equal Opportunity is a fundamental principle of our business and the basis of our customer relationships.

Wellbeing – MLL will provide offers that support the physical and mental wellbeing of staff and citizens through delivery of in-person and online packages.

Company Information

Company Details

MLL Telecom Limited

Marlow International, Parkway, Marlow, England, SL7 1YL

Company No: 02657917

Date of incorporation: 28th October 1991

VAT No: 203558428

Switchboard: 01628 495400

Website: www.mlltelecom.com

Contacts

Name: Ellie Coome

Position: Bid Manager

Tel: 01628 495 400

Email: gcloud@mlltelecom.com

Copyright