digital space

Service Definition Document

Managed SD-WAN Service (Meraki or Fortinet)

1. Service Summary

The managed SD-WAN service provides a secure, resilient and centrally managed wide area networking solution for public sector organisations.

The service enables organisations to connect sites, users and cloud services using a software-defined overlay that optimises application performance, improves resilience and embeds security controls by design.

The service is technology-agnostic, allowing customer to utilise the most suitable vendor while still having a consistent service experience provided by a credible service provider. The SD-WAN can be delivered using either Cisco Meraki or Fortinet SD-WAN platforms, selected during design to align with customer requirements, existing infrastructure and security policies.

1.1.1 Service description

The Managed SD-WAN service delivers a fully managed, software-defined wide area network across one or more connectivity underlays, including broadband, Ethernet, cellular and approved third-party connections.

By intelligently steering traffic across multiple links based on application performance, latency and availability, the service improves network resilience, maximises available bandwidth and ensures consistent user experience for business-critical applications.

The service can be deployed as an overlay to an existing WAN, allowing organisations to enhance performance and resilience without wholesale replacement, or as part of a wider network transformation programme. This flexibility enables customers to modernise their network incrementally, reduce dependency on single connectivity providers, and support cost-effective migration to cloud-hosted and SaaS applications.

Digital Space provides end-to-end responsibility for the design, deployment, configuration, monitoring, optimisation and ongoing support of the SD-WAN service. This removes the operational burden from internal IT teams and ensures the solution is delivered and operated in line with best practice and agreed service levels. Centralised, cloud-hosted management enables consistent policy enforcement across all sites, rapid deployment of changes, and simplified governance of network and security controls.

Real-time visibility of network, application and security performance allows proactive identification and resolution of issues before they impact users. Built-in analytics and reporting support operational assurance, capacity planning and service improvement, while enabling customers to demonstrate performance and compliance outcomes to stakeholders.

2. Features & Benefits

The service is designed to support multi-site organisations, hybrid and remote working models, and secure access to cloud-hosted and on-premise applications. Integrated security capabilities, including encrypted connectivity, application-aware routing and unified threat protection, help protect users and data regardless of location, while enabling safe local internet breakout and improved performance for modern digital services.

Features	Benefits to the Customer
Physical and virtual SD-WAN devices	Enables flexible deployment across on-premise sites, data centres and cloud environments. Supports hybrid estates and future change without redesigning the network, reducing implementation risk and supporting long-term scalability.
Centralised cloud-hosted management platform	Enables flexible deployment across on-premise sites, data centres and cloud environments. Supports hybrid estates and future change without redesigning the network, reducing implementation risk and supporting long-term scalability.
Encrypted site-to-site and site-to-cloud VPNs	Protects data in transit across public and private networks using strong encryption. Enables secure connectivity between sites and cloud services while supporting compliance and data protection requirements.
Application-aware traffic steering and prioritisation	Ensures business-critical applications receive priority and are routed over the best-performing network paths. Improves user experience, reduces service disruption and supports consistent application performance.
Integrated firewall and security services (where required)	Embeds security directly into the network, reducing complexity and the need for additional appliances. Enables consistent security policy enforcement and supports protection against modern cyber threats.
Performance, utilisation and security reporting	Provides clear insight into network performance, application usage and security activity. Supports operational assurance, service reviews and informed decision-making.
24x7 monitoring and incident management	Enables proactive detection and resolution of issues before they impact users. Provides continuous operational support and faster incident response, improving service availability.
Hardware replacement and break/fix support	Minimises downtime by ensuring rapid replacement of failed equipment and coordinated restoration of service. Reduces risk to service continuity and operational delivery.

3. Service Scope

3.1.1 In scope

- SD-WAN solution design and implementation.
- Supply and configuration of SD-WAN devices and licences.
- Central management and orchestration.
- Proactive monitoring and alerting.
- Incident, problem and change management.
- Performance and utilisation reporting.
- Security policy configuration (where specified).
- Hardware break/fix for supplier-provided equipment.

3.1.2 Out of scope

- End user device support.
- Application support beyond network performance.
- Remediation of faults caused by customer-owned equipment outside the agreed design.
- Training services unless explicitly agreed.

3.1.3 Deployment model

The service is delivered as a fully managed service with optional co-managed access allowing simple day-to-day changes such as port opening, IP whitelisting, etc.

Deployment models include:

- On-premise physical SD-WAN appliances.
- Virtual SD-WAN appliances in private or public cloud.
- Hybrid deployments combining physical and virtual devices.

Installations may be completed remotely or on-site depending on site complexity and customer requirements.

3.1.4 Service Management

Digital Space's Managed SD-WAN is underpinned by a set of managed services aligned to the needs, capability and ultimately risk appetite of our customers.

This shared responsibility model leverages the established cloud models in IaaS, PaaS and SaaS and applies them to create a holistic set of option below:

Assure

Proactive strategic insight and optimisation ensure your services are always ready to deliver your business outcomes, increasing productivity, reducing risk and improving growth.

Operate

Monitoring and proactive maintenance of Digital Space provided solutions ensures the services are available to support your business systems reducing downtime and impact to your end users. Best practice change management ensures risk-free evolution ensuring the network continues to meet your needs.

Respond

24x7 technical support desk and monitoring to ensure you are back up and running ASAP, reducing the impact of downtime to your business. If you need to contact us, Digital Space teams can be reached via portal, email or phone to help resolve your issues, working with Digital Space colleagues and partners to deliver a service that is right for your business.

Core Service Functions			
Incident Management	24 x 7 x 365		
Event Monitoring	24 x 7 x 365		
Asset & Configuration Management	✓		
Service Governance	M-F: 8-6pm		
Outcome-Specific Service Functions	**ASSURE**	**OPERATE**	**RESPOND**
Vulnerability Management	Critical & High	Critical & High	Critical Only
Problem Management	M-F: 8-6pm	M-F: 8-6pm	**Customer Responsibility**
Change Management	✓	✓	
Patching	✓	✓	
Capacity Management	✓	**Customer Responsibility**	
Availability Management	✓		

Service Portal

All Digital Space customers will be able to access our ServiceHub customer portal which provide the following functionality:

- Overview of active incidents, service requests and orders along with any open service notices.
- Raising tickets and service requests.
- Utilisation from our monitoring platform.
- Service status.
- Billing details

Interoperability has been designed into the portal to enable core functions to be accessed via API further improving potential ways of working with our customers.

Incident Management

Incident Management delivered by our 24x7 operations teams provides the customer with the function to resolve issues which cause disruptions to the supported solution and restore within agreed SLAs.

The scope of incident management starts with an event raised by either the customer or our monitoring platform which is then managed as an incident within our industry leading ITSM platform to resolution via a permanent resolution or provision of suitable workaround.

Problem Management

Our problem management is our internal function responsible for the mitigation of future impacts to customers' environments through the ownership and management of the identification, investigation and remediation of the root cause of recurring incidents or incidents without a permanent resolution.

Vendor Management

Our internal vendor management function governs how our suppliers interact with our teams interact ensuring the quality of experience for the end users.

This function can extend to our customer's third parties delivering associated services related to the Digital Space solution (e.g. Digital Space SD-WAN running over non-DS provided connectivity).

This extension is a chargeable service and delivered by exception where the customer wishes to reduce their operating costs through managing multiple suppliers delivering a single outcome.

Change Management

Delivered by our expert engineers and governed by our change managers, the change management function enables our customer to modify their Digital Space solutions safely and efficiently in line with their current business needs.

Customers can raise change request from our change service catalogue which will be assessed for risk/complexity/urgency. Depending on the assessment and whether we have enough information to proceed, the change will fall into one of three types:

Type	Description	KPI
Standard	Simple and repeatable low risk change	5 working days
Normal	Complex and/or risky change which will need to be assessed, approved and scheduled via our Change Advisory Board (CAB)	Subject to CAB
Emergency	Urgent or retrospective changes commonly required to address a vulnerability or incident	N/A – Completion advised at via Emergency CAB

Change will be delivered at the earliest available opportunity or on an agreed timeframe which will be communicated to the customer through our Change Advisory Board (CAB). All changes are executed via a central management platform where possible, if this is not available for the solution

For managed or enhanced service tiers, five changes from the catalogue are inclusive per month with roll-over or increases to be discussed with your service team.

Asset and Configuration Management

To assist in the delivery of other service management functions, Digital Space identify and track individual Configuration Items (CI) and document their functional capabilities and interdependencies.

This function will maintain an inventory that will contain a register of:

- Physical hardware
- Logical assets
- Support contracts

This will allow us to quickly identify impacted services during an incident and aid in the root cause analysis for resolution of problems.

Where solutions allow, Digital Space will also maintain configuration back-up of key assets to assist in hardware replacement or roll back procedures.

Event Monitoring

Event monitoring provides the alerting of events across a solution as detected by the Digital Space monitoring platforms. These events can be informational, warnings or incidents that require intervention from our technical teams. This foundational function enables our proactive response to a service impacting event reducing the potential risk to the Customer's business.

Vulnerability Management

Vulnerability management is a core function which ensures a customer's environment cannot be exploited or accessed for malicious intent. Digital Space receives vulnerability and patch notifications directly from partners as well as through monitoring of other external sources. Each notification is assessed and classified by our internal teams into Critical, High, Medium and Low.

Our service comes in two variants:

- **Respond**: Digital Space will patch any critical vulnerabilities (CVSS 9.0+) announced by our vendor or security partners within 14 days of a fix or workaround being made available.
- **Operate and Assure**: Digital Space will patch any critical and high vulnerabilities (CVSS 7.0+) announced by our vendor or security partners within 14 days of a fix or workaround being made available.

Medium and low vulnerabilities can be patched on a per request basis and may be chargeable based on scope and service entitlement agreed at time of contracting.

Capacity Management

Digital Space monitor and measure capacity across the customer's solution, and review these against threshold levels that are agreed during the design stage. By measuring and monitoring capacity, where service elements are at risk of over-utilisation, this shall be reviewed against a capacity plan agreed with the customer.

We will maintain a capacity plan on behalf of our customers; the thresholds will be agreed with the customers' team during the design process. The capacity plan will be reviewed as part of the regular service reviews with any remediations agreed as part of a continuous service improvement action or mini project should transformational interventions be required.

Availability & Performance Management

Digital Space will review on a quarterly basis, the customer's solution to determine potential improvements or optimisation to ensure continued attainment of the customer's required performance and availability.

In conjunction with the customer, our expert technical specialists will provide in-life recommendations to improve the interoperability of the overall Digital Space solution whilst also advising on potential changes required to onboard new digital technologies along with their impact.

Service Governance

Designed to encompass all aspects of Digital Space services, our service governance teams act as the customer's representative and provide the governance required to ensure continued value generation.

This includes service reporting, proactive incident and problem management, continuous service improvement, and a dedicated escalation pathway beyond conventional support avenues.

Our commitment to continuous service improvement is not merely an added benefit, embedded in managed and enhanced service tiers, we actively seek out opportunities for enhancement, gathering insights directly from customer feedback and through regular satisfaction assessments.

To ensure that you are provided with an excellent experience and full transparency, our service delivery managers will work with you to provide specific technology, financial and behavioural reports. These can include but are not limited to:

- **Availability:** Ensuring that our products consistently meet the expected standards.
- **Usage and Consumption:** Offering insights into the extent of product utilisation, determining the necessity for modifications or adjustments.
- **Quality and Performance:** Delivering detailed evaluations of the services and technologies we provide, comparing performance against established product and service level agreements.
- **Capacity:** Supplying essential data for effective capacity management.
- **Expenditure**: Presenting a thorough analysis and precise overview of all financial commitments with Digital Space.
- **Adoption:** Leveraging usage data to delve deeper into how end-users are embracing each product.

3.1.5 Security

The Managed SD-WAN service provides integrated security controls delivered directly from the SD-WAN platform, ensuring consistent protection across all sites, users and connections without the need for additional standalone security appliances. By embedding security within the network, the service reduces complexity, lowers operational overhead and improves overall security assurance.

The service includes network firewalling and access control, enabling organisations to control which users, devices and applications can access the network. Security policies are centrally defined and consistently enforced across all locations, reducing the risk of misconfiguration and supporting compliance with organisational and regulatory requirements.

Intrusion detection and/or prevention capabilities continuously monitor network traffic to identify and block malicious or suspicious activity, helping to reduce the risk of service disruption, data compromise and unauthorised access.

Anti-malware and anti-virus protection helps prevent the introduction and spread of malicious software across the network. Threats are detected and contained at the network edge, reducing the impact on end users and critical systems.

Web and content filtering supports acceptable use policies by restricting access to malicious or inappropriate content, reducing exposure to web-based threats and supporting safeguarding and compliance objectives.

All data transmitted across the SD-WAN is protected using strong encryption, ensuring the confidentiality and integrity of data as it traverses public and private networks.

Security features are enabled and configured in line with the agreed service design and customer security policies, ensuring controls remain proportionate, auditable and aligned to organisational risk appetite throughout the service lifecycle.

3.1.6 Compliance

The service is designed to support public sector security and operational requirements. Data generated by the service is used solely for service delivery, monitoring and reporting. No customer data is shared with third parties except where required to deliver the service or by law.

3.1.7 Reporting

Customers receive access to performance and utilisation reporting, including:

- SD-WAN and site availability.
- WAN link performance metrics.
- Application performance visibility.
- Traffic distribution and usage trends.
- Security event summaries (where enabled).

Reports may be provided via dashboards or scheduled outputs.

3.1.8 Support

Support is provided 24x7, 365 days per year via a central service desk. Customers can raise incidents and service requests through agreed channels. Escalation paths and response targets are defined contractually.

Our support comes in three tiers and scopes:

- **Respond**: Incident, Event, Asset & Configuration and Critical Vulnerability Management.
- **Operate**: All above plus, High Vulnerability, Problem, Change and Patch Management.
- **Assure**: All above plus, Capacity, Availability Management and Customer Solution Architect.

We aim to triage all queries, regardless of priority, within two hours. This includes a target response time of 30 minutes. Target time for resolution (TTFR) varies according to priority:

- P1: 24x7x365 support: TTFR is 4 hours, with updates every 30 minutes.
- P2: 24x7x365 support: TTFR is 8 hours, with updates every 4 hours.
- P3: business hours/weekdays (excluding bank holidays) only: TTFR is 24 hours, with updates provided once per working day.
- P4: business hours/weekdays (excluding bank holidays) only: TTFR is 48 hours, with updates provided once per working day.

3.1.9 Service levels

Service levels for availability, incident response and resolution are defined in the service schedule or order form. Service levels may not apply where issues are caused by customer actions, third-party connectivity faults or events beyond reasonable control.

Pricing

Pricing is based on the selected SD-WAN platform, number and type of devices, licence duration, service tier and optional components. Pricing is provided via the G-Cloud pricing document.

Ordering

Customers can order the service through the G-Cloud 15 framework. A statement of requirements and design document will be agreed prior to service commencement.

Termination and exit

On termination or expiry of the service, the supplier will support service exit in line with contractual terms, including recovery of supplier-owned equipment and reasonable assistance with transition to an alternative solution where required.

Contact details

Further information, pricing and ordering guidance is available on request through the G-Cloud 15 framework.

