Central Networks & Technologies Ltd.
Bryon House, Green Lane
Heywood
OL10 2DY

Central Networks & Technologies Ltd - SDWAN

Crown Commercial Service

Prepared by: Vicki Coleman
Date: 12/01/2026

info@centralnetworks.co.uk
+44 (0)1706 747474
www.centralnetworks.co.uk

Citation ISO Certification Quality management ISO 9001: 2015 REGISTERED
Certificate No:124522006

Citation ISO Certification Environmental management ISO 14001: 2015 REGISTERED
Certificate No:211602014

Citation ISO Certification Information security management ISO 27001: 2013 REGISTERED
Certificate No:211592014

Central Networks and Technologies Ltd (Central) was founded in September 1991 by Christopher Mycock. In the earlier years Central was responsible for running the core ICT systems for many of the UK Magistrates Courts Services, which involved moving and hosting the mainframes and employing staff via TUPE. We also have a focus in the Housing Association and not-for-profit sector. In the last 10 years we have migrated many of our customers to cloud or partial cloud provision.

Our customer base is diverse in terms of size, geography, skills, business requirements and objectives. We have recognised this and created a solutions and services portfolio that can be tailored to meet the individual requirements of all our customers. Some of our customers have large ICT teams and only look for assistance where they have investigated and exhausted every avenue. Others are far smaller, where finance officers often take on ICT responsibility and need additional help and assistance. Central provides a bespoke service to each of our customers, providing best value for money and an ICT service which matches their requirements which assists them in delivering their objectives.

Central Networks and Meraki SDWAN

Introduction

SDWAN is becoming the baseline for most networks which require ease of use and simplified administration by allowing management of the entire WAN from a pane-of-glass centralised dashboard. Almost every single business or organisation in today's world relies on connectivity of some form; whether a public website, e-mail services, e-tailing or EPOS.

Organisations are growing more reliant on advanced distributed networks and new network topologies that are constantly emerging to accommodate the accelerating adoption of SaaS solutions and public cloud platforms. It is increasingly critical to ensure predictable application performance and reliability, along with secure uninterrupted connectivity at all locations.

SDWAN allows organisations to work more flexibly, providing seamless scaling to the network as business requirements change therefore offering a solution where colleagues can access data and applications securely from anywhere and at any time.

What is SDWAN

SDWAN is a networking solution that combines the functionality of a traditional wide-area network with an easy to use software based management platform to monitor and administer the network. Meraki SDWAN allows superior control over all traffic paths and incorporates the ability to integrate intrusion prevention, malware protection, adaptive content control, firewalling, pre-emptive link failure detection and QoS queues across the entire network from within one interface.

SDWAN focuses on many of the limitations seen in traditional networks and now provides local administrators with the tools to gain total control rather than relying on the provider's own NOC or SOC teams for troubleshooting and fault resolution.

Meraki SDWAN can proactively detect PLOS/TLOS faults on the network and intelligently re-route traffic across alternative paths before service impact becomes an issue. Early warning monitoring thresholds alert administrators before the end user is aware of a problem.

An SDWAN network negates the need for expensive MPLS or leased line links and allows a secure and scalable solution to be built across multiple lower cost connections, whether these are broadband, fibre, DIA or even cellular.

Benefits of Meraki SDWAN

Benefits of Meraki SDWAN include:

1. **Single pane-of-glass:** The entire Meraki SDWAN solution (which may include MX firewalls, MS switching, MR wireless) can be controlled and configured through a single cloud managed dashboard. The dashboard allows full control of each device and is not restricted to being only accessible from on-premise locations. IP whitelisting, delegated user account control and multi-factor authentication protect the dashboard from unauthorised access. Logging and real-time analytics of the network and its operation are available from within the dashboard.

2. **One-touch Deployment:** It Is possible to deploy an entire Meraki SDWAN solution at the touch of a button. Utilising device templates and port profiles, It Is possible to group device types into the same configuration template allowing the device to be automatically configured upon first connection to the Internet.

3. **Cloud Integration**: As well as physical hardware firewall appliances, Meraki provide cloud-deployable virtual appliances to allow seamless connectivity into many of the public/hybrid cloud environments. Azure and AWS are supported, as well as many others.

4. **Scalable:** Scale your network up or down by bundling additional Internet connections into an existing environment. Meraki SDWAN can load-balance over multiple WAN links to maximise bandwidth and performance. Even if you outgrow the existing Meraki firewall, configuration can be replicated to a new device for plug-and-play hardware upgrades.

5. **Reduces independence on a traditional MPLS WAN:** Advantage of using low-cost broadband links throughout the WAN. Most types of xDSL/FTTx/DIA and cellular connections are supported.

Key features of Meraki SDWAN

Key features and functionalities of Meraki SDWAN include:

1. **Cloud Managed:** The Meraki SDWAN solution is a fully cloud managed environment, negating the need for on-premise centralised controllers that require upkeep and maintenance. The Meraki cloud is built up from global datacentres which are replicated in real-time.

2. **Meraki AutoVPN:** Allows SDWAN site-to-site VPN connections to be established with no extensive knowledge of VPNs and the necessary authentication protocols. VPN parameters are negotiated directly between appliances with no user configuration required. AutoVPN connections can recover automatically across redundant links meaning very high levels of uptime and connectivity.

3. **Resilience:** SDWAN allows the building of scalable and reliable networks using a whole host of different connectivity methods. Zero reliance on private MPLS or IPVPN networks, Meraki can connect any form of broadband, DIA, leased line or cellular connectivity to provide unparalleled uptime

4. **Local Breakout:** The Meraki MX firewall appliances that make up the SDWAN topology are capable of firewalling and filtering inbound and outbound traffic. Integrated web filtering as well as layer 3, 4 and layer 7 application firewalls provide superior next-generation content controls allowing a secure local Internet breakout at every MX site. There is no longer a need to tunnel outbound Internet traffic to a centralised proxy server for filtering.

5. **Traffic Management:** Meraki SDWAN allows full control over traffic paths and link selection based on a 5 tupple approach. Protocol, IP addresses and service ports can be configured to prioritise traffic to use a certain path through a network.

Summary

Overall, Meraki SDWAN provides a powerful yet simple to manage wide area network solution incorporating many of the leading edge technologies into one platform, greatly simplifying the process of building and running a complex yet intelligent network.

Proactive monitoring and redundant links can introduce class-leading levels of uptime. Through the use of radio or cellular networks, the solution becomes incredibly scalable and adaptable and also allows network administrators to deploy SDWAN sites into temporary locations where committing to a long-term connectivity contract isn't feasible.

Firewall and content control functionality on all Meraki MX firewall appliances ensures all users of Meraki SDWAN networks stay safe and secure online, as well as maximising bandwidth efficiency and throughput by allowing Internet traffic to break-out locally rather than traversing across the SDWAN.

The cloud dashboard allows both an overall review of the entire network as well as a more detailed view into the health and status of each piece of equipment, the links and any end user client devices. Traffic inspection allows administrators to monitor the types of traffic passing across the network to which further controls can quickly be implemented to permit or deny, either globally or on a per-device basis.

Extensive logging and reporting tools allow the review of recent and past events to which they can be extracted to an external logging server for archival and storage purposes.

Finally, access to the dashboard can be configured on a granular level, allowing access to be provided as required to the different levels of IT staff within an organisation. For example, 1st line teams may only require access to view the operating status of the network, while 2nd and 3rd line system administrators will need full access in order to make changes and configure the system.

Confidentiality and Copyright