

Business Connectivity & Network Services | blueAPACHE

Canonical: <https://www.blueapache.com/empower-services/connectivity>

Details:

Key facts

Fact	Value
Service name	emPOWER Connectivity, delivered over the emPOWER Network
Network ownership	Our owned and operated MPLS private network; platform established in 2010
Core routing	Cisco ASR carrier-grade routers; IPv6 ready
Firewalls	Palo Alto Networks virtual firewalls (network); dedicated hosted next-generation firewalls per customer; FortiGate CPE used in the Archers deployment
Core points of presence	Pacific (Australia), United States, Europe (London), Asia (Singapore)
Data centre interconnection	165+ data centres
Carrier model	Tier 1 carrier-agnostic: globally recognised tier 1 carriers plus specialised regional carriers; no individual carrier named
Published site uptime	Minimum 99.99 per cent, conditional on multiple carriers, multiple media, dual CPE and firewalls in high availability, dual carriage at each site
Service desk	7am to 7pm on all business days, by phone, email or client web portal
Monitoring	24x7 priority monitoring with a Network Operations Centre; unified threat protection supported 24x7
Public cloud connections	Direct connection to Azure or AWS with a VPN-over-internet secondary path; Azure ExpressRoute; AWS Direct Connect
Internet exchange	Traffic transits the Australian Internet Exchange; emPOWER Internet is part of the IX peering network
Voice carriage	Microsoft Teams Direct Routing, SIP trunking, hosted PBX, contact centre

Contract schedules	Schedule 5 emPOWER Network Services; Schedule 6 emPOWER Voice Carriage Services
ISO/IEC 27001:2022 scope	Certificate 202507-118 names Network and Voice Carriage Services within the certified ISMS scope; confirm current standing and engagement scope

What the pillar covers

Its capability list is: resilient business network and internet connectivity; secure cloud, data centre and site interconnect; SASE; ongoing network monitoring and operational management; visibility across performance and availability; and governance and accountability through one connectivity partner.

Capability	Description
Highly redundant designs	Multiple carriers, multiple media (fibre and fixed wireless given as examples), multiple CPE devices and firewalls in high-availability configuration
Business-grade MPLS data services	Extends the corporate private network without a VPN; each office becomes another IP address on the network
Quality of Service end to end	We work with the customer to define business-critical applications and apply QoS policies; voice and video can be prioritised
Internet scalability and IX peering	emPOWER Internet port bandwidth scaled up or down on request; part of the IX peering network for lower latency to major SaaS applications
Public cloud connectivity	Direct connection to Azure or AWS plus a secondary VPN-over-internet route
Next-generation firewalls	Unified threat protection: intrusion prevention, advanced malware protection, application control, web filtering and antispam, supported 24x7
Remote-user VPN	Always-on VPN, configurable with single sign-on and multifactor authentication; confirm endpoint and processing locations for the deployment
Direct connection into emPOWER Cloud	Connectivity to cloud infrastructure, with backup and disaster recovery available under the agreed service scope
Voice carriage	Microsoft Teams Direct Routing, SIP trunking, hosted PBX and contact centre solutions

Two architecture options are offered: a hybrid of MPLS and internet SD-WAN, or a hub-and-spoke secure SD-WAN using emPOWER Connectivity appliances, with the SD-WAN hub and hosted SD-WAN firewalls located in multiple data centres on the emPOWER Network. Additional SD-WAN appliances at a site allow local internet breakout to be added and scaled later.

What we proactively manage on the customer's behalf is also stated: monitoring, operating system patching of the CPE and firewalls, configuration documentation, nightly configuration backups, and change management.

emPOWER SASE

Secure Access Service Edge combines network and security controls for access to applications. The Connectivity offering describes SASE alongside SD-WAN and next-generation firewalls, with always-on VPN, single sign-on and multifactor authentication options. Confirm the controls, endpoint locations and user policies included in the specific deployment.

emPOWER Core Network and Data Centre Interconnect

The emPOWER Network itself, offered as the resilient foundation connecting offices, data centres and cloud environments. It is a fully meshed MPLS core on Cisco ASR routing with core points of presence in Australia, the United States, London and Singapore, interconnection into 165+ data centres, ExpressRoute and Direct Connect on-ramps to Azure and AWS, and proactive 24/7 monitoring 365 days a year using our own monitoring console, to which customers are also given access. This is the service under Schedule 5.

How it is delivered

Design starts with the customer's sites and applications. We work with you to define which applications are business-critical so that QoS policies can be applied end to end, and choose between MPLS, internet SD-WAN or a hybrid per site. The redundancy level is a design decision per site: single carrier and single CPE, or the dual-carrier, dual-firewall, dual-carriage configuration that the published uptime figure depends on.

Deployment is staged where the estate is large or international. The Sealy of Australia case study describes six Australian sites first, then one in New Zealand, one in the United Kingdom and ten across Asia-Pacific, with legacy links kept live so voice and data could revert to the old network at any point; the 18-site network went fully live in April 2022, roughly twelve months after the engagement began. The Archers case study describes site links upgraded from 20/20Mbps to 400/400Mbps fibre with FortiGate CPE at each Queensland office connected to a hosted FortiGate high-availability firewall hub in emPOWER Cloud.

Once live, we manage the CPE and firewalls: monitoring, OS patching, configuration documentation, nightly configuration backups and change management. Customers are given access to the same network monitoring and management tools we use. Moves, adds and changes, including scaling internet port bandwidth, are requested through the standard change process and any additional fees are notified at the time. The published terms require best efforts to carry out scheduled maintenance within the Schedule's window or, at other times, with at least three Business Days' prior notice and minimum disruption. Emergency notice and restoration follow separate provisions.

Network Services under Schedule 5 follow the standard commercial model: a default 36-month Minimum Service Period, fixed fees billed monthly in advance, usage-based fees monthly in arrears, monthly reporting within 5 Business Days of month end, and 6-monthly service reviews. Where third-party carriage costs change, clause 12.5 allows us to vary fees by the same proportion from the date the carrier changed its charges.

Support and service levels

Published availability. The Connectivity brochure states a minimum 99.99 per cent uptime for its specified redundant design. Confirm the contracted Service Level, measurement, exclusions and remedies in the Service Order and Schedule 5 Service Description; the brochure figure is not an unconditional commitment for every site.

Support hours, stated precisely. These two figures are different and are easy to conflate:

Function	Availability
Service desk (phone, email, client web portal)	7am until 7pm on all business days
Priority network monitoring and NOC	24x7
Unified threat protection support	24x7

The General Terms and Conditions define Business Hours as 0700 to 1900 AEST/AEDT on Business Days, consistent with the service desk window. emPOWER Managed Services separately advertises unlimited 24/7 help desk support. A customer holding both services should confirm on the Service Order which desk handles network incidents outside 7am to 7pm.

Our client outcomes

Customer	What was delivered	Stated outcome
Sealy of Australia (live April 2022)	International voice and data network designed and deployed in stages across 18 sites in Australia, New Zealand, the UK and Asia-Pacific, with ongoing management	No disruption to business activity during migration; supports made-to-order manufacturing with a three-day lead time and real-time factory-to-head-office data
Honan Insurance (c. 2020-2021)	Palo Alto network remediation during the tender, then whole-of-WAN transformation including international sites, Wi-Fi support and new Sydney data links	Regular outages resolved; telecommunications bill reduced by around 65 per cent; office move completed on schedule when the incumbent could not deliver links
Archers The Strata Professionals (2026)	Private MPLS WAN, FortiGate CPE at each office, hosted FortiGate high-availability firewall hub with unified threat protection, FortiClient EMS VPN	Site links upgraded from 20/20Mbps to 400/400Mbps fibre; shared firewall replaced with dedicated firewall; web filtering and intrusion prevention added
Brotherhood of St. Laurence (from late 2015)	WAN evaluated and upgraded across call centres, offices, care facilities and social enterprises; further links, LAN and security for 17 new NDIS sites	Upgrade completed in 12 weeks with immediate performance impact; network operated with consistent reliability for the first time

Defining the network boundary

Establish responsibility site by site: customer premises, access circuits, the managed network, cloud interconnects and destination services. The published availability figure depends on the specified redundant design; it should not be applied to a single-link site. Record who owns each circuit and device, how an upstream fault is escalated and which support window applies. Monitoring coverage, fault response and restoration are separate questions that need answers for the actual network.

Which document defines the commitment

The published General Terms v3.6 give the Service Order precedence over the General Terms, followed by the Schedules and then the Acceptable Use Policy (clause 2.3). Record the agreed scope, exclusions and negotiated departures in that document set. Keep the versions supplied at signing with the executed order and signed variations. Two offers with the same service name can cover different systems, operating hours or responsibilities.

Responsibility across the delivery chain

The published terms permit subcontracting all or part of the Service Agreement without prior written customer consent. Confirm any separate notification obligations and negotiated conditions in the applicable agreement. Clause 27.5 nevertheless makes us liable for our subcontractors' acts and omissions to the same extent as for our employees. This differs from a third-party supplier contracted directly by the customer. Identify which arrangement applies to each dependency in the design. Where supplier identity, delivery location or change notification matters, request a documented supplier list and put any agreed notification or approval requirement in the Service Order; the general clause does not supply that visibility automatically.

Continuity when an external event interrupts service

Clause 23 addresses force majeure separately from normal incident management. Performance is suspended to the extent a qualifying event causes delay or failure. The definition includes specified events outside reasonable control; it is not a blanket classification of every outage. If the delay exceeds 20 Business Days, the other party may terminate by written notice. The clause also requires payment for services to termination and the applicable Early Termination Payment. A continuity plan should cover operational recovery and the commercial consequences of prolonged interruption. Confirm the Schedule's exit calculation rather than assuming an externally caused outage creates a cost-free exit.

Escalating a contractual dispute

A support escalation and a formal contractual dispute are different processes. Clause 26 begins with a Dispute Notice giving adequate particulars. Representatives meet within three Business Days; unresolved matters then move through the clause's senior-representative referral and meeting stages before court proceedings. Urgent equitable relief and disputes over whether the agreement was validly terminated are exceptions. Keep incident records, service measurements, approvals and correspondence together so the disputed obligation and requested outcome can be identified. Raising a ticket does not necessarily satisfy a formal notice requirement; use the agreement's notice process for contractual disputes.

Customer content and take-down requests

Clause 14 distinguishes operating the service from responsibility for the customer's content. It requires the customer to notify us promptly of relevant take-down notices or directions and comply with them. The terms also reserve rights for us to restrict or remove Customer Data in specified circumstances, including suspected agreement breaches or exposure to harm or liability. These rights are separate from routine availability commitments. Agree who receives regulatory notices and who can authorise operational action, and retain the notice and decision record. The full clause, including its discretion and good-faith wording, is explained in the terms guide.

Related

emPOWER SASE

emPOWER Core Network and Data Centre Interconnect

Cloud hub

Security hub

Collaboration hub

Managed Services hub

emPOWER Cloud

Public Cloud: Microsoft Azure

Managed Detection and Response

Sealy of Australia case study

Honan Insurance case study

Archers case study

Retail and Consumer Services industry page

Transport and Logistics industry page

Service agreement

Home

Do you own the network or resell a carrier's?

We own and operate the emPOWER Network, established in 2010. Its published architecture describes a Cisco ASR-based MPLS private core. The founding date does not date every current hardware component; the contracted service defines our responsibility for CPE, firewalls and monitoring.

Does the 99.99 per cent uptime apply to every site?

No. A single-carrier or single-CPE site is not covered by that published figure. The enforceable Service Level for each site is the one in the Schedule 5 Service Description.

What are the support hours for connectivity?

The service desk is available from 7am until 7pm on all business days by phone, email or the client web portal. Priority network monitoring, the Network Operations Centre and unified threat protection support run 24x7. If your organisation also holds emPOWER Managed Services, which advertises unlimited 24/7 help desk access, confirm on the Service Order which desk handles after-hours network incidents.

Where are the network's points of presence?

Core points of presence are in Australia (Pacific), the United States, London (Europe) and Singapore (Asia), with interconnection into more than 165 data centres. Network traffic transits the Australian Internet Exchange, and emPOWER Internet is part of the IX peering network, which we state lowers latency to major SaaS applications such as Microsoft 365, Teams, Zoom and Salesforce.

Can emPOWER Connectivity connect us directly to Azure or AWS?

Yes. The Connectivity materials describe direct Azure or AWS connectivity with a secondary VPN-over-internet path. The Network brochure describes Azure ExpressRoute and AWS Direct Connect, plus direct access to emPOWER Cloud. Agree the applications, routing, redundancy and service inclusions for your deployment.

Is SASE included in emPOWER Connectivity or sold separately?

The Connectivity offering brings together SASE, SD-WAN, next-generation firewalls and Cisco core networking. Always-on VPN can use single sign-on and multifactor authentication. Confirm the deployment locations, included controls and pricing on the Service Order.

What security is built into the network?

Unified threat protection on dedicated hosted next-generation firewalls: intrusion prevention, advanced malware protection, application control, web filtering and antispam, supported 24x7. At the core, we run Palo Alto Networks virtual firewalls and state our network security approach covers identity and access management, intrusion detection and mitigation, application-level monitoring, perimeter protection and secure VPN provisioning. Our published ISMS certificate has a defined scope. Essential Eight maturity is a separate stated alignment position; it does not establish the maturity or compliance of every customer deployment.

What do you manage on our behalf?

For the CPE and firewalls that make up emPOWER Connectivity, we manage monitoring, operating system patch updates, configuration documentation, nightly configuration backups and change management. Customers are given access to the same network monitoring tools we use.

Can we use the network for voice?

Yes. Voice carriage is part of the pillar: Microsoft Teams Direct Routing and PSTN services, SIP trunking and terminations, hosted PBX and contact centre solutions. Quality of Service policies can prioritise voice and video end to end. Voice carriage is contracted under Schedule 6 and is within our ISO/IEC 27001:2022 certified scope.

How long is a connectivity contract?

The General Terms describe a default 36-month Minimum Service Period unless the Service Order states otherwise, with separate renewal, provider-advice and continued-use provisions. Clause 12.5 permits proportional pass-through of relevant third-party charge changes. Any Early Termination Payment depends on the termination ground, applicable terms and Schedule 5; confirm the actual calculation before exit.

What is emPOWER Connectivity?

emPOWER Connectivity is our managed wide area network (WAN) service that delivers secure, resilient connectivity keeping users, applications, cloud environments and locations connected with consistent performance, visibility and control.

What core networking technologies does emPOWER Connectivity bundle together?

emPOWER Connectivity bundles Software-Defined WAN (SD-WAN) for flexible network management, Next-Generation Firewalls (NGFW) for advanced security, Secure Access Service Edge (SASE) for secure connectivity, and Cisco carrier-grade core networking for robust infrastructure, all in a single managed solution.

What network is emPOWER Connectivity delivered over, and what does it connect to?

emPOWER Connectivity is delivered over the emPOWER Network, our own MPLS private core network, and connects directly to the emPOWER Cloud fabric for integrated cloud infrastructure and disaster recovery services.

What uptime guarantee does emPOWER Connectivity offer?

The Connectivity brochure states a minimum 99.99% uptime for specified redundant designs using multiple carriers and media, multiple CPE devices, high-availability firewalls and dual carriage. Confirm the contractual Service Level, measurement, exclusions and remedies for each site in the Service Order and Schedule; the figure is not unconditional or uniform across designs.

What support and monitoring is available for emPOWER Connectivity?

The service desk (phone, email, client portal) is available from 7:00 AM to 7:00 PM on business days, while priority network monitoring, the Network Operations Centre (NOC), and unified threat protection support are all available 24x7.

Does emPOWER Connectivity require a VPN to extend corporate private networks?

No, emPOWER Connectivity includes business-grade MPLS data services that extend corporate private networks without requiring a VPN.

What role does Quality of Service (QoS) play in emPOWER Connectivity?

Quality of Service (QoS) management is included in emPOWER Connectivity to prioritize business-critical traffic across the network.

In which country do you provide emPOWER Connectivity services?

We provide emPOWER Connectivity services in Australia.