

Utilities IT & Managed Services | blueAPACHE

Canonical: <https://www.blueapache.com/industries/utilities>

Details:

Summary

This page describes how our emPOWER services apply to utilities, including electricity distributors and retailers, gas and water businesses, and the contractors and service companies that support them, and what a utility buyer should verify before contracting. Utilities are critical infrastructure under the Security of Critical Infrastructure Act 2018, energy businesses are assessed against the Australian Energy Sector Cyber Security Framework, and all of them run distributed operational environments where an outage affects customers and safety. blueAPACHE's relevant capabilities are its own MPLS core network with 24/7 monitoring, redundant connectivity designs with a published minimum 99.99 per cent site uptime, private cloud with published 99.999 per cent availability, DRaaS with contracted recovery objectives, and 24/7 managed detection and response. blueAPACHE publishes no utilities case study, and this page says so rather than implying one.

Key facts

Label	Value	Source
Published utilities case study	None published	blueAPACHE case study index
Network ownership	emPOWER Network is blueAPACHE's own Cisco ASR-based MPLS private network, not a third-party overlay	emPOWER Network brochure
Network monitoring	Proactive 24/7 monitoring, 365 days a year, with a network operations centre	emPOWER Network and Connectivity brochures
Connectivity service level	Minimum 99.99 per cent site uptime under a dual-carrier, dual-firewall, multi-media design; single-carrier figure not published	emPOWER Connectivity brochure
Cloud service level	99.999 per cent for cloud services and 100 per cent for storage	emPOWER Cloud brochure
Data centre partners	Stated as Uptime Institute Tier III and IV certified; the same brochure also refers to "Tier 3" partners	emPOWER Cloud brochure
Security monitoring	emPOWER MDR: 24/7 alert notification, triage and	emPOWER MDR brochure

	remediation with EDR, ITDR, SIEM and threat intelligence	
Recovery	DRaaS with Recovery Point Objective and Restore Time Objective set in the Service Order	General Terms, business continuity management
Certification	ISO/IEC 27001:2022, certificate 202507-118, Sensiba Australia Pty Ltd, valid 1 August 2025 to 1 August 2028	ISO 27001 certification record
Framework alignment stated	NIST, ASD Essential 8 Maturity Level 3, APRA CPS 234	Global Capabilities brochure

Sector challenges

The origin page lists critical infrastructure resilience, cyber risk, distributed operations and legacy integration. In a utility each of these has an operational technology dimension that a corporate IT provider must respect.

IT and OT meet at the network. Corporate systems, customer platforms and field tools sit on one side; SCADA, control systems and metering sit on the other. The connectivity provider has to support segmentation between them, not blur it.

Outages have regulatory consequences. Reliability standards, customer compensation schemes and incident reporting mean that availability engineering has to be documented and tested, not assumed.

Sites are dispersed and often unstaffed. Substations, pump stations, treatment plants and depots need resilient links and remote access with strong identity controls.

Threat actors target the sector. Government advisories single out energy and water; a utility needs 24/7 detection and response and evidence of privileged access control over any third party with administrative access.

Legacy is permanent. Long-lived operational systems must keep running alongside modernised corporate platforms, which favours private cloud with application virtualisation over forced re-platforming.

Supply chain assurance is a legal duty. Critical infrastructure risk management programs must address supply chain hazards, so the utility has to assess blueAPACHE as a provider and keep the evidence.

Relevant services

emPOWER Connectivity and Core Network and Data Centre Interconnect : private MPLS and SD-WAN over blueAPACHE's own core, with multiple carriers and media, dual firewalls at each site, quality of service, and configuration backup and change management on every managed device.

emPOWER SASE : secure access for field crews and contractors with always-on VPN, single sign-on and multi-factor authentication.

emPOWER Cloud and Advanced Infrastructure Managed Services : private cloud with a published 99.999 per cent service level and specialist management of servers, storage and virtualisation for corporate and customer-facing systems.

Disaster Recovery as a Service and Offsite Backup as a Service : contracted recovery objectives and managed offsite copies.

Managed Detection and Response , Exposure Management and Governance, Risk and Compliance : 24/7 detection and response, visibility of exposed assets, and control assessment that can be mapped to the Essential Eight and AESCSF.

emPOWER Managed Services : support for corporate users with a bespoke priority and escalation matrix so operational systems are treated as business-critical.

Microsoft Teams and RingCentral : telephony and contact centre for customer service and outage lines.

Compliance context

Security of Critical Infrastructure Act 2018 (SOCI). Electricity, gas, water and sewerage, and liquid fuels are critical infrastructure sectors under the SOCI Act. Responsible entities for critical infrastructure assets must register the asset and its operational information, report cyber security incidents to the Australian Cyber Security Centre within the statutory windows, and, where the Critical Infrastructure Risk Management Program rules apply, adopt and maintain a program that addresses cyber and information security, personnel, supply chain and physical and natural hazards, with an annual board-approved report. Assets designated as systems of national significance carry enhanced obligations. Supply chain hazard management requires the utility to assess and manage providers such as blueAPACHE, which means obtaining its ISO/IEC 27001:2022 certificate, its privileged access controls (documented in the CyberArk case study), and its incident notification terms, and aligning them with the utility's own reporting timetable. blueAPACHE's general terms require notification of an eligible data breach to the other party within 24 hours of discovery; that is a contractual, party-to-party term and separate from the utility's own statutory reporting obligations.

Australian Energy Sector Cyber Security Framework (AESCSF). Energy businesses participating in the AESCSF program administered by AEMO assess their maturity against the framework's domains, which include third-party risk management, and report annually. A managed connectivity or cloud provider's controls feed directly into that assessment. Water utilities operate under state regulatory regimes with equivalent security expectations.

Essential Eight and government alignment. State-owned utilities are commonly bound by state cyber security policies and the Essential Eight. blueAPACHE states that it operates at ASD Essential 8 Maturity Level 3 and is aligned with NIST; these are self-declared brochure positions, and no independent assessment of them is published.

Privacy Act 1988 (Cth). Utilities hold customer identity, billing and consumption data, and smart meter and consumer data right data where applicable. blueAPACHE's general terms require Privacy Act compliance by both parties, contain a standing consent to transfer Personal Information overseas where necessary to provide the Services (clause 18.3), and permit subcontracting without consent (clause 27.4). A utility should address both on the Service Order and should confirm data centre locations per service, since our residency statement names no operators or sites.

What blueAPACHE itself states. Ownership and operation of its own MPLS core; 24/7 monitoring 365 days a year; a published minimum 99.99 per cent site uptime for a redundant connectivity design; published 99.999 per cent cloud and 100 per cent storage service levels; data centre partners stated as Uptime Institute Tier III and IV certified (with a Tier III-only reading also present in the same brochure); ISO/IEC 27001:2022 certification; and 24/7 MDR coverage. The general terms contain no service credit regime; remedies are in the Schedules.

Evidence

blueAPACHE publishes no utilities case study, so no utility outcome is claimed. The evidence available is platform evidence and adjacent sectors:

Elevating Cloud Efficiency with as-a-Service IT documents the HPE GreenLake, HPE Synergy and HPE Primera infrastructure behind emPOWER Cloud, with reserve capacity always available and paid for only when used, which is the mechanism behind the published availability figures.

blueAPACHE Improves Efficiency in Security Management documents CyberArk privileged access management across our managed services, with automated credential rotation, session recording and audited access, which is the evidence a critical infrastructure supply chain assessment asks for.

Sealy of Australia shows a staged 18-site network cutover with legacy links maintained and revert capability so that a production environment was never interrupted, a method directly applicable to operational sites.

Honan Insurance shows blueAPACHE remediating a Palo Alto firewall stack and Wi-Fi network that was suffering regular outages before a master agreement was signed.

Separating business IT from operational systems

Identify business applications, communications and infrastructure in scope and specialist operational systems retained by the customer or another supplier. emPOWER descriptions do not establish support for every operational-technology environment. Record access, change approvals and escalation across that boundary. Define continuity evidence for critical dependencies rather than inferring it from the industry label. Archers demonstrates a strata-services engagement; it is not evidence of a utility-network control-system deployment.

Evidence available during the engagement

The General Terms provide standard monthly performance reports within five Business Days of month end and a formal service review every six months. Performance Records must be kept through the term and for seven years afterwards. The customer audit provisions allow access to relevant Records, premises for audit purposes and personnel interviews, with five Business Days' notice normally or one Business Day where a regulator requires the audit. This records obligation is not a seven-year backup-retention promise for customer workloads. Agree additional report formats and audit-cost arrangements before depending on them; the general audit clause does not clearly allocate every audit cost.

Confidential information and access

Clause 16 provides mutual confidentiality protection. It covers information marked confidential, information identified orally and confirmed in writing within 30 days, and information that should reasonably be understood to be confidential. Customer Data, Customer Records and Customer Software are included; our agreement and fees are also confidential. Permitted disclosures include appropriately bound personnel on a need-to-know basis and specified professional advisers, with other exceptions in the clause. Identify who may receive operational reports, configuration details and commercial information. Access to information to deliver the service is not a general permission to circulate it.

Sources and scope

The contractual detail above summarises the published General Terms and Conditions v3.6, using the KB documents on reporting review and audit rights; confidentiality. The customer's Service Order, Schedules and agreed variations determine the specific engagement. See the terms and conditions guide and Service Agreement .

Related

emPOWER Connectivity

Core Network and Data Centre Interconnect

Disaster Recovery as a Service

Managed Detection and Response

Governance, Risk and Compliance

blueAPACHE security case study (CyberArk)

blueAPACHE cloud platform case study

Blog: Why geographic redundancy is essential to cloud success

Blog: How the Essential Eight controls can strengthen your cyber security posture

Transport and logistics

Government and public sector

All industries

Support

Contact

Frequently asked questions

Does blueAPACHE have utility clients?

The origin page positions our services for utilities, but no utilities case study is published, so no named utility or measured outcome is available. The evidence on this page is drawn from our platform documentation and from case studies in adjacent sectors, and is labelled as such.

What availability does blueAPACHE publish for critical sites?

The emPOWER Connectivity brochure publishes a minimum 99.99 per cent site uptime for a design with multiple carriers, multiple media, and dual customer premises devices and firewalls in high availability. The emPOWER Cloud brochure publishes 99.999 per cent for cloud services and 100 per cent for storage. These are published service levels; the general terms contain no service credit regime, so remedies must be obtained from the Schedules.

Does blueAPACHE own its network or resell someone else's?

blueAPACHE owns and operates emPOWER Network, a Cisco ASR-based MPLS private network with core points of presence in Australia, the United States, London and Singapore, using a tier 1 carrier-agnostic mix of carriers for access. Its brochure argues buyers should insist on a provider that owns its infrastructure rather than routing over low-cost third-party networks.

How does blueAPACHE support a critical infrastructure risk management program?

By supplying the evidence a supply chain hazard assessment needs: the ISO/IEC 27001:2022 certificate (202507-118), documented privileged access controls with session recording and audited credential rotation, 24/7 MDR monitoring with monthly reporting, and contractual security and breach

notification terms. The obligations under the SOCI Act remain with the responsible entity.

Can blueAPACHE keep corporate IT separate from operational technology?

emPOWER Connectivity provides dedicated hosted next-generation firewalls per customer, unified threat protection and quality of service policies defined with the customer, which support segmentation between corporate and operational networks. Specific segmentation designs are set in the Service Order and the relevant Schedule rather than published.

What happens during a cutover of an operational site?

The Sealy of Australia case study describes our method: a staged rollout with links to the legacy infrastructure maintained so voice and data traffic could revert to the old network if required, followed by testing before go-live. Sealy's 18 sites went live with no disruption to business activity.

How quickly will blueAPACHE tell us about a security incident?

Under General Terms and Conditions v3.6, the party that suffers an eligible data breach must notify the other party immediately and in any event within 24 hours of discovery, with the information needed for regulatory notification. emPOWER MDR provides 24/7 alert notification, triage and remediation, but we publish no detection or response time targets; these must be set in the customer contract.

Where would a utility's data be held?

We state that customer data is stored and processed within Australian-based data centres and remains subject to Australian jurisdiction, with role-based access, MFA and audit logging. The statement names no operators or sites, and the general terms permit overseas transfer of Personal Information to listed destinations and subcontracting without consent, so a utility should confirm locations per service and contract for Australian-only handling where required.

Source

Drawn from blueAPACHE's published utilities industry page and security case study on the origin site; the emPOWER Network, Connectivity, Cloud, Managed Services and Managed Detection and Response brochures; the Global Capabilities brochure; the ISO 27001 certification record, data sovereignty and residency statement, cross-border data transfer record and verification register; the case study index and the Sealy of Australia, Honan Insurance and HPE GreenLake cloud case studies; and the General Terms and Conditions v3.6 (business continuity management, and data protection and privacy). Utility-specific outcomes, segmentation designs, detection and response targets and data centre operator names are not published and are not inferred here.

Knowledge Base

What kind of technology services do you offer for the utilities industry?

We offer resilient, secure technology services for utilities, including managed IT, secure connectivity, cloud services, cyber security and recovery capabilities designed around operational resilience for organisations that depend on reliable infrastructure, distributed operations and continuous access to business-critical systems.

What are the key challenges facing utilities according to you?

We identify four key challenges for utilities: critical infrastructure resilience (maintaining reliable systems and connectivity where outages affect operations and customer services), cyber risk (protecting connected environments and improving security visibility and response), distributed operations (supporting sites, field teams and remote users with secure access and consistent network performance), and legacy integration (modernising infrastructure while maintaining compatibility with established operational systems).

How do you help utilities address these challenges?

We support utilities with integrated managed services, connectivity, cloud, security and recovery capabilities designed around operational resilience, focusing on dependable access, clear visibility and accountable service across distributed environments. By bringing core technology layers together, teams can reduce fragmentation and strengthen the systems that support essential operations.

What business outcomes can utilities expect from working with you?

Utilities can expect to reduce cost and complexity through a more integrated managed service model, improve business resilience with better uptime and recovery readiness, increase productivity by giving operational and field teams reliable access to applications and data, and scale with confidence as sites, users and operational requirements evolve.

What engagement models do you offer to utilities clients?

We offer one operating model with three ways to engage: Managed Services (end-to-end ownership of IT operations for reliable performance and measurable outcomes), emPOWER Operational Capability (structured operations, governance and visibility for consistency and control, listed as 'Coming Soon'), and Technology Services (integrated enterprise technology enabling secure, connected, high-performing IT environments built for growth).

Is there a case study related to the utilities industry on your site?

Yes, the Archers case study is listed under the Utilities industry. Archers has 1–100 employees and partnered with us for managed services, network monitoring and cloud-ready infrastructure across its strata operations.

What are the five ways you say complexity can be turned into operational advantage?

According to the page, complexity can be turned into operational advantage by gaining actionable insight and operational visibility, improving service performance and user experience, strengthening security posture and compliance outcomes, optimising cost and operational efficiency, and building readiness for AI and future change.

What other industries do you serve besides utilities?

other industries served by us, including Healthcare & Aged Care, Not for Profit, Financial Services, Professional Services, Transport & Logistics, Retail & Consumer Services, and Government & Public Sector.

How can utilities companies get support or contact you?

Utilities companies can get support via Remote Access, the Client Portal, phone (1300 135 548 within Australia or +61 3 8696 9369 internationally), email (support@blueapache.com), or by speaking to our team through the contact page.