Managed IT Services | blueAPACHE

Canonical: https://www.blueapache.com/empower-services/managed-services

Details:

Connecting endpoint operations with employee experience

Our announced partnerships with NinjaOne and ControlUp describe complementary roles in managed services. The 24 August 2026 ControlUp announcement describes real-time device and application telemetry, user experience history, performance trends, device health and automated remediation.

A useful operating model connects those capabilities. Device and application information helps identify what is installed and what needs attention; performance and experience signals help explain how a problem affects users. Support teams can then assign the action, record the result and check whether the user's experience improved.

For deployment, agree the device population, telemetry and integrations, access permissions and approved automation. Define patch approval and maintenance windows, escalation for failed actions and the reporting baseline. The partnership announcements establish the relationships; the service proposal should identify which products and managed activities are included for the customer.

Key facts

Fact	Value
Service name	emPOWER Managed Services
History	blueAPACHE was founded in 1998; its company timeline records the first Facilities Management contract in 2001 and the emPOWER Managed Services name in 2003
Delivery models	Fully outsourced IT, or augmentation of an in-house team with selected services and resources
Customer base cited in the brochure	More than 300 mid-tier and enterprise-sized customers; a brochure figure rather than a current customer count
Help desk coverage	Unlimited 24/7 support; business-hours staff in Australia, after-hours and follow-the-sun coverage from our global team; no part of the help desk outsourced
Help desk scope	Desktop, server, telephony, networking, cloud, backup and security
Account team	Account Executives, Service Delivery Managers, Engineers, Technical Account Managers

Monitoring toolset	Managed services portal covering monitoring, alerting and capacity baselining, shared with the customer
Environment reviews	Regular environment reviews highlighting key issues, with predictive capacity monitoring to manage growth
Pricing model	Predictable fixed monthly pricing; unlimited access without fluctuating costs
Contract schedule	Schedule 2 of the General Terms and Conditions v3.6
Default term in the referenced General Terms	36 months for services other than Professional Services, unless the Service Description or Service Order specifies otherwise
Monthly reporting	Within 5 Business Days of month end, including Service Level reporting
ISO/IEC 27001:2022 scope	Certificate 202507-118 lists emPOWER Managed Services within the ISMS scope. It certifies the management system, not the service itself
Customer Zero	Our managed-services page and April 2026 NinjaOne announcement describe applying the same service architecture, automation workflows and reporting internally before scaling capability across customer environments

What the pillar covers

The emPOWER Managed Services brochure describes an integrated, enterprise-grade IT support ecosystem made up of an on-shore support team, a local account management team, regular strategic and technology reviews, application management, monitoring and reporting, proactive security management, backup and disaster recovery solutions, end-user device provisioning, and unlimited 24/7 support. The four service areas named in the brochure are summarised below; the customer's agreed service scope determines inclusions.

Service area	Brochure description
Help desk	Technical support team available around the clock, wherever the customer is in the world
Server and desktop	Lifecycle management of infrastructure and devices: provisioning, maintenance, management and performance reporting
Network and infrastructure	Complete network and infrastructure monitoring and management
Security	Security Gap Analysis audits and managed detection and response built on leading tools

The current managed-services page presents six capabilities: automation-led operations (proactive remediation, self-healing, automated patching), security-first delivery, experience-led support (real-time

digital experience visibility across applications, devices and endpoints), AI-ready foundations, operational visibility, and governance and accountability.

Monitoring, reporting and environment reviews

Tooling is shared with the customer. Our managed services portal and toolset handle monitoring, alerting and capacity baselining , and customers are given access to the same toolset so they can see their whole production environment, managed and unmanaged. The published functions are:

Management and reporting — system monitoring reviews, resource usage and reporting across servers, desktops and networks, co-authored by our specialists

Lifecycle management — network, server and desktop management across the full lifecycle of infrastructure and devices, from provisioning through patching to maintenance

Environment reviews — regular reviews of the customer environment that highlight key issues for closer examination, with predictive capacity monitoring used to manage growth before it becomes a constraint

Remote monitoring and management — tooling across servers and endpoints driving automated patching and compliance

Environment reviews use monitoring and capacity information to identify issues for examination and support growth planning. The Archers case study separately describes monthly operational reviews and quarterly business reviews focused on continual service improvement; agree the review cadence and reporting inputs for your engagement.

Managed Service Bundles

Integrated bundles that combine the core operational capabilities (service desk, monitoring, patching, security operations, reporting) into a simpler service model with clearer ownership and predictable delivery.

Advanced Infrastructure Managed Services

Specialist management of critical infrastructure across servers, storage, virtualisation and data centre environments, backed by our operational engineers. Agree which application and platform responsibilities remain with your team. The referenced General Terms define Scheduled Maintenance for managed services as manufacturer-recommended routine maintenance of Customer Managed Equipment. Clause 3.10 requires best efforts to use the Schedule's maintenance windows or give at least 3 Business Days' notice, and to keep disruption to a minimum.

Field Services and Staff Augmentation

Flexible access to experienced technical resources for on-site field work, project delivery and additional capability when internal teams need extra hands. Our Global Capabilities material describes a field services network across Australia, the United States and the United Kingdom. Confirm the classification and billing of each engagement. Where work is contracted as Professional Services, Schedule 1 applies and the General Terms' default 36-month Minimum Service Period excludes that category.

How it is delivered

Transition in. Immediately after the Service Commencement Date, we must confirm the start date, run a due diligence process to collect the information we need on the systems and services to be supported,

configure our monitoring platforms where applicable to report on availability and performance, provide documentation on how to use its support services, and agree a regular meeting and reporting schedule. The customer must promptly supply firewall, network, password and procedure details and approve documentation in a timely manner.

Operating rhythm. Each customer has an assigned account team. Account Executives own the strategic relationship and the commercial model; Service Delivery Managers own the operational relationship and are accountable for delivery; Technical Account Managers are accountable for technical service delivery; engineers do the work. The Archers case study describes this in practice as monthly operational reviews and quarterly business reviews focused on continual service improvement, run by an Account Executive, Service Delivery Manager and Portfolio Engineer.

Reporting and governance. Within 5 Business Days of the end of each month we provide our standard reports on performance against key delivery metrics, including Service Levels; additional reports can be agreed at additional fees. Each party appoints an Account Representative with authority to make binding day-to-day decisions, and the parties meet every 6 months to review the services. We retain records for the term plus 7 years and must allow customer audits on 5 Business Days' notice (1 Business Day for regulatory audits).

Security is embedded in the same model: integrated monitoring, automated patching, operational controls and defined governance. Where a customer wants dedicated detection and response, that is provided through the Security pillar's MDR service rather than assumed within a managed services bundle.

See Managed Detection and Response for the dedicated security service and confirm its inclusion in the agreed scope.

Support and service levels

What is published. Unlimited 24/7 help desk access, with Australian-based staff during business hours and our global team after hours. The first point of contact is always a member of our team and no part of the help desk is outsourced. The General Terms and Conditions define Business Hours as 0700 to 1900 AEST/AEDT on Business Days, and Customer Operating Hours default to the same window unless the Service Order says otherwise.

The Managed Services brochure describes a customer-specific priority and escalation matrix without giving default response or resolution targets. Obtain the applicable targets and any credit entitlement from your agreement and Schedule 2. The referenced General Terms define a "Compliance Target" as the target time to resolve each Support Centre call by priority, and distinguish Service Levels identified under that heading in the Service Description from other obligations.

How Service Levels operate. We must meet or exceed any applicable Service Level except to the extent a failure arises from, or is contributed to by, a Reasonable Excuse: a long defined list that includes customer-supplied scripts and equipment, customer-directed outages, third-party software used by us, Emergencies, and acts of third parties. Service Levels are measured with our tools and the results are final and binding. Under clause 2.9, if the customer gives no Written Notice and continues using the service after an unrenewed term, all services under the agreement extend for three months at full list price, without Service Levels.

Related obligations worth knowing. Anti-virus on customer equipment is the customer's responsibility unless the Service Description says otherwise. Clause 17.3 limits the backup obligation to what is expressly agreed in the Schedule and Service Order. Unless otherwise agreed in the Service Order, it is to run the backup software at agreed intervals and re-run reported failures. A customer wanting blueAPACHE to participate in its business continuity plan requests an Action Plan, which is chargeable as a Professional Service.

How it integrates with the other pillars

Cloud. The Honan Insurance and Archers case studies describe engagements combining emPOWER Managed Services with emPOWER Cloud. Cloud, backup and DRaaS responsibilities depend on the services and obligations expressly included in each agreement. See the Cloud hub .

Connectivity. We monitor and manage customer networks as part of the pillar, and where the WAN is emPOWER Connectivity the carriage, firewalls and monitoring sit under one accountable party. Archers' private MPLS WAN and FortiGate security uplift were delivered inside its managed services engagement. See the Connectivity hub .

Collaboration. Telephony is inside help desk scope, and Microsoft Teams calling migrations were part of both the Archers and Berry Street engagements. See the Collaboration hub .

Security. Proactive security management and Security Gap Analysis audits are part of the managed services scope; 24/7 managed detection and response is the Security pillar's MDR service. See the Security hub .

Procurement and Microsoft Practice. End-user device provisioning, Intune zero-touch deployment and licensing optimisation appear in managed services engagements and draw on the Procurement and Microsoft Practice hubs.

Our client outcomes

Customer	What was delivered	Stated outcome
Archers The Strata Professionals (2026)	Fixed-price emPOWER IT-as-a-Service: migration to emPOWER Cloud IaaS, private MPLS WAN, FortiGate security, Microsoft Teams calling, Intune, formal account governance	End-of-life Windows Server 2012 decommissioned; site links upgraded from 20/20Mbps to 400/400Mbps fibre; spend stabilised on an opex model; monthly operational and quarterly business reviews in place
Honan Insurance (c. 2020-2021)	Replaced an incumbent MSP after repeated network outages; emPOWER Managed Services, Cloud, WAN, IaaS and DRaaS	Telecommunications bill reduced by around 65 per cent; staff able to work remotely during COVID-19 with no impact on performance
Brotherhood of St. Laurence (2015 to 2020)	WAN upgrade, then a three-year managed services agreement, IaaS, hardware-as-a-service and cloud migration	WAN upgrade completed in 12 weeks; scaled from 900 to 1500 staff and 17 new locations during the NDIS rollout; planning for a new three-year agreement began in 2020
Berry Street (published case study describing a transition from March 2020)	emPOWER managed services with a dedicated service desk team and modernisation roadmap; Microsoft Teams telephony migration was in progress when the case study was written	1400 staff mobilised to work from home; transition delivered on time and within budget

Making operational ownership explicit

Translate the proposal into a responsibility list for each system: monitoring, incident handling, patch approval, lifecycle decisions and communications. Include the interfaces to retained internal IT and directly contracted suppliers. Reduced fragmentation depends on these boundaries being clear. During transition, check that access, escalation contacts, support instructions and reporting arrangements are in place before assuming a system has entered normal service. A bundle name is not a substitute for that handover.

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.

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.

Responsibility across the delivery chain

The published terms allow us to subcontract all or part of the Service Agreement without customer consent or a notification requirement. 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.

Personnel continuity and a later move in-house

Clause 22 contains a mutual non-solicitation restraint covering specified employees and contractors, including indirect engagement arrangements. It runs for 12 months after the last day of service performance and includes a look-back over the personnel involved. Prior written consent can permit an otherwise restricted arrangement. If a future operating model includes hiring a delivery specialist or moving managed work in-house, address that possibility before relying on it in an exit plan. Access to an engineer during an engagement does not establish a right to recruit that person afterwards.

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.

How liability differs from service performance

Clause 19 separates performance obligations from financial liability. The general cap per claim is the greater of the fees paid in the preceding three months or $25,000, with exclusions and specific categories governed separately. Confidentiality, information security, privacy and the IP indemnity have a $1 million per-event and $2 million aggregate cap. Data-loss liability depends on whether we had, and breached, a contracted backup or disaster recovery obligation; the relevant measure is restoration cost to the applicable recovery point, not the value of every business consequence. Read these provisions alongside the negotiated Service Order and Schedule; an availability statement does not describe the liability regime.

Related

Managed Service Bundles
Advanced Infrastructure Managed Services
Field Services and Staff Augmentation
Cloud hub
Connectivity hub
Collaboration hub
Security hub
Managed Detection and Response
Archers case study
Honan Insurance case study
Brotherhood of St. Laurence case study
Not for Profit industry page
Financial Services industry page
Service agreement
Support
Home

Can emPOWER Managed Services work alongside our internal IT team?

Yes. We offer the service either as a fully outsourced IT function or as an augmentation of an existing in-house team, where the customer selects individual services and resources. The Berry Street and Brotherhood of St. Laurence case studies both describe blueAPACHE acting as an extension of an internal ICT team rather than replacing it.

What hours is the help desk available?

Business-hours support staff are located in Australia; after-hours and follow-the-sun support comes from our global team, and no part of the help desk is outsourced. Contractually, Business Hours are 0700 to 1900 AEST/AEDT on Business Days, so confirm on the Service Order which coverage applies to which service.

What response and resolution times do you commit to?

The Managed Services brochure gives no default response or resolution targets and describes a bespoke priority and escalation matrix for each customer. Obtain the targets applicable to your services from the agreed contract and service catalogue. Any response or resolution commitment that counts as a Service Level must be written under that heading in the Service Description; obligations described elsewhere, including a Compliance Target, are not Service Levels under the General Terms and Conditions.

Are there service credits if a Service Level is missed?

Check Schedule 2 and the agreed Service Description for any applicable credit entitlement and its conditions. The General Terms alone do not establish a credit amount for your service. They provide for Service Level measurement using our tools, with the results final and binding, and include Reasonable Excuse exclusions.

What is included in the monthly price?

The brochure describes predictable pricing with unlimited help desk access, delivered as an integrated support ecosystem: on-shore support, local account management, strategic and technology reviews, application management and reporting, proactive security management, backup and disaster recovery solutions, and end-user device provisioning. The exact inclusions and exclusions for a given customer are defined in the Service Description and Schedule 2.

What is an environment review and how often does it happen?

A regular review of the customer environment that highlights key issues for closer examination, supported by predictive capacity monitoring to manage growth. Fix the cadence on the Service Order.

How long is the contract and what happens at the end?

The referenced General Terms set a default 36-month Minimum Service Period for services other than Professional Services, unless the Service Description or Service Order specifies otherwise. Renewal is in 36-month periods unless we advise otherwise. Under clause 2.9, if the customer gives no Written Notice and keeps using the service after an unrenewed term, all services under the agreement extend for three months at full list price without Service Levels. Early termination charges depend on the termination ground and the applicable Schedule 2 provisions; obtain the calculation for your agreement.

Who owns patching and maintenance of our servers and devices?

Under emPOWER Managed Services, we manage the complete lifecycle of infrastructure and devices from provisioning to patching and maintenance, using remote monitoring and management tooling for automated patching and compliance. Scheduled Maintenance on Customer Managed Equipment follows manufacturer recommendations. Clause 3.10 requires best efforts to use the Schedule's maintenance windows or give at least 3 Business Days' notice, and to minimise disruption.

Do we get visibility of what you are doing?

Yes. Customers are given access to the same monitoring and management toolset we use, covering monitoring, alerting and capacity baselining, so they can view their entire production environment. We also provide standard monthly reports within 5 Business Days of month end, samples of which are available on request, and the parties meet every 6 months for a service review.

Is security included in managed services?

Proactive security management, Security Gap Analysis audits and managed detection and response built on leading tools are named in the managed services security scope. The dedicated 24/7 emPOWER Managed Detection and Response service, Human Risk Management and Exposure Management are sold through the Security pillar, and their inclusion in any bundle should be confirmed in writing on the Service Order.

Where do you deliver managed services from?

Business-hours support is delivered from Australia, with offices in Melbourne (head office), Sydney and Brisbane, and after-hours coverage from our teams in the United States and United Kingdom. emPOWER Managed Services is within the scope of our ISO/IEC 27001:2022 certificate, which lists the Melbourne, Sydney and Brisbane offices.

What is emPOWER Managed Services?

emPOWER Managed Services combines IT support, automation-led operations, security, digital experience visibility and governance. It can operate as a fully outsourced service or augment an existing internal IT team. blueAPACHE was founded in 1998; its company timeline records the first Facilities Management contract in 2001 and the emPOWER Managed Services name in 2003.

What kind of help desk support does emPOWER Managed Services provide?

It provides unlimited 24/7 help desk support available globally, with an Australian-based service desk for business hours and a global team providing after-hours and follow-the-sun coverage. Technical expertise spans desktop, server, telephony, networking, cloud, backup, and security, and all support is provided directly by our team members with no outsourcing of help desk functions.

How does emPOWER Managed Services handle infrastructure and device management?

It offers complete server and desktop lifecycle management, including provisioning, maintenance, and performance reporting, plus device lifecycle management covering infrastructure and devices from provisioning to patching and maintenance. It also includes network and infrastructure monitoring and a monitoring/management portal for visibility across IT production environments.

What other capabilities does emPOWER Managed Services offer beyond help desk and infrastructure management?

The Managed Services brochure describes application management, monitoring and reporting, backup and disaster recovery solutions, technology roadmap planning and regular reviews. Confirm the activities and systems included in your agreement; backup and recovery obligations depend on the expressly agreed scope.

How is the emPOWER Managed Services team structured?

We deliver the service through a structured account management team that includes Account Executives, Service Delivery Managers, Engineers, and Technical Account Managers.

Which organization provides emPOWER Managed Services and where?

emPOWER Managed Services is provided by us, an organization serving Australia.