

Managed Detection and Response - blueAPACHE

Canonical: <https://www.blueapache.com/services/managed-detection-response>

Details:

Summary

Managed Detection and Response is blueAPACHE's managed security operations service, sold as emPOWER Managed Detection and Response (MDR). It combines continuous monitoring across endpoints, identities and security events with human investigation, triage, containment and remediation, delivered 24/7 without the customer building its own Security Operations Centre. blueAPACHE states the service is ITIL-aligned, integrates with Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike, and is compliance-aligned with ISO/IEC 27001, the Essential Eight, NIST CSF, the Australian Privacy Principles, GDPR and SOC 2 Type II. It also states that it applies the same security architecture, operational processes and controls to its own environment as to customer deployments — a "Customer Zero" position. blueAPACHE does not publish detection or response time targets; those are set in the customer's contract. This page sets out the inclusions, the items whose inclusion status is unstated, and the contractual terms that govern the service.

Key facts

Label	Value	Source
Service name	emPOWER Managed Detection and Response (MDR)	emPOWER MDR brochure
Coverage	24/7 alert notification, triage and remediation across the full IT environment and security stack	emPOWER MDR brochure
Detection technologies	EDR, ITDR, SIEM and threat intelligence feeds	emPOWER MDR brochure
Integrations named	Microsoft Security, Microsoft Identity, Microsoft Sentinel, CrowdStrike "and more"	emPOWER MDR brochure
Process framework	ITIL-aligned incident management	emPOWER MDR brochure
Own-environment posture	"Customer Zero" — the same security architecture, operational processes and controls are applied to blueAPACHE's own environment and to customer deployments	emPOWER security material
Reporting	Dashboards and monthly reporting for leadership visibility	emPOWER MDR brochure

Compliance alignment stated	ISO/IEC 27001, Australian Privacy Principles, Essential Eight (ASD), NIST CSF, SOC 2 Type II, GDPR (alignment, not attestation)	emPOWER MDR brochure
blueAPACHE certification	ISO/IEC 27001:2022 certificate 202507-118, emPOWER Managed Services in scope; ASD Essential 8 Maturity Level 3 stated in brochures	ISO 27001 certification record; emPOWER Cloud brochure
Published MTTD, MTTR or response SLA	None; set per customer in the Service Agreement	emPOWER MDR brochure
Items with unstated inclusion status	Vulnerability Management, Incident Response Retainer, vCISO Advisory, Human Risk Management	emPOWER MDR brochure
Vendor recognition	Rapid7 APAC Fastest Growth Partner 2022; CrowdStrike named as an integration, not a partnership	Vendor partner record
Default contract term	36 months unless the Service Order states otherwise	General Terms cl. 2.6

What is included

The emPOWER MDR brochure lists four key features. Threat detection and hunting: continuous monitoring with EDR, ITDR, SIEM and threat intelligence feeds. Incident response: rapid triage, containment and remediation. Compliance and reporting: dashboards and monthly reporting for leadership visibility. Integration: support across Microsoft Security, Microsoft Identity, Sentinel, CrowdStrike and more. blueAPACHE states it goes beyond standard MDR by providing 24/7 alert notification, triage and remediation, by bridging Security Operations and IT Operations to shorten response and accelerate recovery, and by offering scalable options for different maturity levels and budgets.

The brochure frames identity as the primary attack surface ("Attackers don't break in, they log in") and names five threats the service is built around: credential theft, adversary-in-the-middle session hijacking that bypasses MFA, shadow workflows such as hidden mailbox rules, rogue applications, and session hijacking with stolen tokens. Three illustrative scenarios are published: a 2am brute-force attack on remote desktop isolated before lateral movement, a ransomware payload quarantined by EDR before execution, and a compromised Microsoft 365 account with a rogue OAuth app disabled and remediated with the customer's team. These are blueAPACHE scenarios, not named-customer case studies.

Within emPOWER Managed Services, security scope is described as proactive security management, Security Gap Analysis audits and managed detection and response built on leading tools, so Managed Services customers reach the same security operations through their existing account team.

Customer Zero: blueAPACHE runs what it sells

blueAPACHE states that it applies the same security architecture, operational processes and security controls across its own environment as it does across customer deployments, and describes itself as its own first customer.

That claim has some published support rather than being assertion alone. The blueAPACHE security case study documents the company deploying CyberArk identity security and privileged access management across its own business and its managed services, and blueAPACHE is cited as CyberArk Global MSP of the Year 2021. The HPE GreenLake case study does the same for its cloud platform. Two of the eight published case studies have blueAPACHE as the customer, which is unusual and is the evidence behind this position.

For a buyer the question this should prompt is a specific one rather than a general reassurance: ask whether the controls applied to your tenancy are the same ones blueAPACHE applies to itself, and where they differ. A provider running its own estate on the stack it sells has a genuine incentive alignment; it does not automatically follow that every control is configured identically for every customer, and the brochure does not claim that it is.

What is not included

Four services appear in the brochure's key features block as a separate list with no inclusion statement: Vulnerability Management, Incident Response Retainer, vCISO Advisory and Human Risk Management. Human Risk Management is marketed by blueAPACHE as its own service, which suggests these are add-ons rather than standard inclusions; treat this as a material scope question to settle in writing.

blueAPACHE publishes no mean time to detect, mean time to respond, or triage and response targets. Under the general terms a Service Level exists only where stated under the "Service Level" heading in the Service Description, and a "Compliance Target" for support-call resolution is defined separately and is not a Service Level. The brochure's compliance list is alignment language: alignment with SOC 2 Type II is not the same as holding a SOC 2 attestation, and blueAPACHE does not claim a SOC 2 report. The service does not replace the customer's own duties under clause 3.19 to follow blueAPACHE's security directions and to report suspected compromises promptly, nor the customer's anti-virus responsibility on its own equipment under clause 3.18.

Who it is for

The brochure states MDR is designed for businesses seeking proactive protection against cyber threats, IT teams looking to reduce operational burden across security, organisations needing to demonstrate compliance, and leadership teams seeking visibility and assurance around cyber risk. In practice that is the mid-market organisation with a Microsoft-centred estate, an existing EDR or SIEM investment it wants to keep, and no capacity to staff a 24/7 SOC. Archers' representative in the 2026 case study cites access to a blueAPACHE technical team "with experience across application virtualisation, MDR, and Microsoft platforms" as a benefit of the relationship.

How it is delivered

Onboarding follows clause 8: due diligence on the environment and security stack, connection of blueAPACHE's monitoring to the customer's EDR, identity and SIEM sources, support documentation, and an agreed meeting and reporting schedule. Incident handling follows ITIL-aligned processes. Detection runs continuously; alerts are triaged by blueAPACHE analysts, contained and remediated, and escalated to the customer where action on their side is needed. Because blueAPACHE bridges SecOps and IT Ops, a Managed Services customer's remediation is carried out by the same organisation that administers the environment. Monthly reporting and dashboards are provided; under

clause 4.9 standard reports arrive within five Business Days of month end, and the parties review the Services every six months.

Customers must provide 24x7 remote access to the relevant components (clause 7.1) and must inform blueAPACHE promptly of any suspected security compromise (clause 3.19). Where blueAPACHE reasonably suspects that continued provision of a Service compromises the security of its environment, it may suspend that Service under clause 3.26 with as much notice as reasonably possible, without fees accruing during the suspension.

Commercial model

MDR is contracted on a Service Order as a fixed monthly fee invoiced in advance (clause 12.1), direct debit by default, GST additional. The brochure describes scalable options to fit different needs, maturity levels and budgets, but publishes no price. Where blueAPACHE's own third-party tooling vendors change their charges, clause 12.5 allows proportionate pass-through without a signed Variation. An Incident Response Retainer, if taken, is a separate line item.

Support and service levels

Coverage is stated as 24/7 alert notification, triage and remediation. Managed Services customers additionally hold the unlimited 24/7 help desk, Australian-based in business hours and follow-the-sun after hours. The contractual Service Levels are those in the Service Description, measured with blueAPACHE's tools whose results are final and binding, and subject to the Reasonable Excuse carve-out, which includes third-party software used by blueAPACHE and acts of third parties. The general terms contain no service credit regime; any remedy sits in the Schedule. blueAPACHE's liability for breach of its information security obligations under clause 17 is capped at \$1 million per event and \$2 million in aggregate.

Related services

Human Risk Management addresses the people-driven attacks that precede identity compromise and is designed to run alongside MDR. Governance, Risk and Compliance uses MDR's dashboards and monthly reports as evidence. Exposure Management prioritises the vulnerabilities MDR would otherwise have to detect being exploited. emPOWER SASE and emPOWER Core Network and Data Centre Interconnect carry the Palo Alto Networks firewall estate and unified threat protection that feed network telemetry. Private and Public SaaS Backup and emPOWER Backup for Microsoft Entra ID provide the recovery path for identity and SaaS data after an incident.

Evidence

Archers The Strata Professionals (2026): dedicated FortiGate firewall replacing a shared firewall, unified threat protection, and access to a blueAPACHE team with MDR experience.

blueAPACHE on CyberArk: the origin site's case study describes blueAPACHE strengthening its own security posture with CyberArk identity controls across its business and managed services; blueAPACHE is cited as CyberArk Global MSP of the Year 2021. This is the published support for the Customer Zero position above.

Vendor recognition: Rapid7 APAC Fastest Growth Partner 2022; Fortinet Australian Fastest Growth Partner of the Year 2021.

Buying questions

Contract term and renewal. 36-month Minimum Service Period by default (clause 2.6); Written Notice by executed Service Order to renew or exit; otherwise a three-month holdover at full list price with Service Levels off (clause 2.9).

Termination. Customer: unremedied breach after 20 Business Days, blueAPACHE insolvency or ceasing business (clause 24.1). blueAPACHE: non-payment after five Business Days, specified breaches after 20 Business Days, insolvency, change of control (clause 24.2). Early Termination Payment under the Schedule (clause 25.2).

Scope to fix in writing. Which of Vulnerability Management, Incident Response Retainer, vCISO Advisory and Human Risk Management are included; the detection, triage and response targets and whether they are Service Levels or Compliance Targets; which log sources and identities are in scope; who may authorise containment actions such as isolating an endpoint or disabling an account; and which controls applied to blueAPACHE's own environment are, and are not, applied to yours.

Data and privacy. Security telemetry may contain Personal Information; both parties must comply with the Privacy Act and notify eligible data breaches within 24 hours of discovery (clause 18.4). Clause 18.4(c) restricts either party from disclosing a breach to third parties, including the Information Commissioner, without the other's approval save for a narrow legal carve-out; regulated customers should reconcile this with their own reporting duties. Clause 18.3 records a standing consent for overseas transfer of Personal Information, relevant if follow-the-sun analysts work outside Australia.

Audit. The customer may audit blueAPACHE's records on five Business Days' notice, or one Business Day where a regulator requires it (clause 4.13).

Agreeing incident authority before an alert

Record covered systems and telemetry, available decision-makers and actions blueAPACHE may take without further approval. Detection, investigation, containment and recovery are separate steps. Confirm whether the retainer, advisory work, vulnerability management or Human Risk Management mentioned alongside MDR is included or separately purchased. Keep escalation and evidence handling with the Service Description so an incident does not depend on settling scope in real time.

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. A brochure or a procurement discussion does not, by itself, define the customer-specific commitment. 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; blueAPACHE's 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 blueAPACHE to subcontract all or part of the Service Agreement without customer consent or a notification requirement. Clause 27.5 nevertheless makes blueAPACHE liable for its subcontractors' acts and omissions to the same extent as for its 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.

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 blueAPACHE 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.

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.

Sources and scope

The contractual detail above summarises the published General Terms and Conditions v3.6, using the KB documents on service agreement formation and document precedence; confidentiality; subcontracting and assignment; liability and indemnity; dispute resolution. The customer's Service Order, Schedules and agreed variations determine the specific engagement. See the terms and conditions guide and Service Agreement .

Related

Security pillar hub

emPOWER Security

Human Risk Management

Governance, Risk and Compliance

Exposure Management

emPOWER SASE

Private and Public SaaS Backup

Managed Services pillar hub
Microsoft Practice hub
Case study: blueAPACHE security with CyberArk
Case study: blueAPACHE on HPE GreenLake
Case study: Archers The Strata Professionals
Industry: Financial services
Industry: Healthcare and aged care
Service Agreement terms
Support
Contact blueAPACHE

Frequently asked questions

Is emPOWER MDR a 24/7 service?

Yes. The brochure states 24/7 alert notification, triage and remediation across the full IT environment and security stack, combining continuous monitoring with human investigation rather than automated alerting alone.

Does blueAPACHE use this service itself?

blueAPACHE states it applies the same security architecture, operational processes and controls to its own environment as to customer deployments. Two of its published case studies have blueAPACHE as the customer: the CyberArk identity security deployment and the HPE GreenLake cloud rebuild. Ask which specific controls are identical for your tenancy and which differ.

Do we have to replace our existing EDR or SIEM?

No. The brochure names Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike as supported integrations, with "and more", so existing tooling can usually be retained. Confirm your specific platform before contract.

What response time does blueAPACHE commit to?

blueAPACHE publishes no mean time to detect, mean time to respond or response-time SLA for MDR. Those targets are set in the customer's Service Agreement and are Service Levels only if written under that heading in the Service Description.

Is Human Risk Management included in MDR?

Its inclusion status is not stated. The brochure lists Human Risk Management, Vulnerability Management, Incident Response Retainer and vCISO Advisory separately from the key features, and Human Risk Management is sold as its own service, so treat them as add-ons unless the Service Order says otherwise.

Which threats is the service built around?

Identity-centred attacks: credential theft, adversary-in-the-middle session hijacking that bypasses MFA, shadow mailbox rules that exfiltrate data, rogue applications that escalate privileges, and session hijacking with stolen tokens.

Does MDR help with Essential Eight or ISO 27001?

The brochure states the service is compliance-aligned with ISO/IEC 27001, the Australian Privacy Principles, the Essential Eight, NIST CSF, SOC 2 Type II and GDPR, and blueAPACHE itself holds ISO/IEC 27001:2022 certificate 202507-118 with emPOWER Managed Services in scope. Alignment supports, but does not by itself evidence, a customer's own assessment.

Is blueAPACHE SOC 2 certified?

The brochure describes MDR as compliance-aligned with SOC 2 Type II. That is alignment language; blueAPACHE does not claim a SOC 2 attestation.

Who carries out remediation?

blueAPACHE analysts triage, contain and remediate, and escalate to the customer where action is needed on their side. For Managed Services customers the same organisation administers the environment, which is the SecOps and IT Ops bridge the brochure describes.

What reporting do we receive?

Dashboards and monthly reporting for leadership visibility per the brochure, and standard performance reports within five Business Days of month end under clause 4.9, with a six-monthly service review.

Can blueAPACHE suspend a service for security reasons?

Yes. Under clause 3.26 blueAPACHE may suspend or cancel a Service where it reasonably suspects continued provision compromises the security of its environment, giving as much notice as reasonably possible, and fees do not accrue during that suspension.

What is the minimum contract term?

36 months from the Service Commencement Date unless the Service Order states otherwise. Early termination triggers an Early Termination Payment calculated under the Schedule.

What happens to security data at exit?

blueAPACHE deletes Customer Data on its environment at the end of the Service Period at no cost and the customer must take its own copy first (clause 9.1). Customer Records must be provided within 10 Business Days of request (clause 17.3), and blueAPACHE retains its own records for seven years (clause 4.12).

Source

Drawn from the emPOWER Managed Detection and Response brochure; the emPOWER Managed Services, emPOWER Cloud, Human Risk Management, emPOWER security and vendor partner records; the ISO 27001 certification record; the Archers The Strata Professionals, blueAPACHE

security and HPE GreenLake case studies; and the General Terms and Conditions v3.6 (service delivery and service levels, information security obligations, service suspension and cancellation, customer obligations, data protection and privacy, cross-border data transfers, reporting review and audit rights, liability and indemnity, fees payment and invoicing, service term renewal and minimum service period, termination rights, consequences of termination, transition-in and disengagement services, and reasonable excuse exclusions). Origin pages: blueapache.com managed detection and response, and the blueAPACHE security case study.

Knowledge Base

How does Huntress fit into your security services?

We use Huntress to strengthen endpoint and identity detection and response in Microsoft-centric environments. We combine the selected technology with our Microsoft security practice and service delivery.

Can we access Huntress while keeping our internal security team?

Yes. We offer Huntress through a reseller and implementation route as well as a managed security service. We agree coverage and response responsibilities with your team.

Is Huntress the only technology in your MDR offering?

No. We support a range of selected security technologies and integrations, including Microsoft Security, Microsoft Identity, Sentinel and CrowdStrike. We design the combination for your environment.