Managed Cyber Security Services | blueAPACHE

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

Details:

Key facts

Fact	Value
Pillar name	emPOWER Security
Core services	Managed Detection and Response; Human Risk Management; Exposure Management; Governance, Risk and Compliance
MDR coverage	24/7 alert notification, triage and remediation across the full IT environment and security stack
MDR detection layers	EDR, ITDR, SIEM and threat intelligence feeds
MDR integrations named	Microsoft Security, Microsoft Identity, Microsoft Sentinel, CrowdStrike
MDR process framework	ITIL-aligned incident management
Response targets	The MDR brochure gives no MTTD, MTTR or triage-time figures; obtain any agreed targets from the applicable service documents
Human Risk Management components	Security awareness and phishing simulation; email threat detection and alerting; user-reported phishing response; insider risk and data exposure protection
Email authentication service	DMARC advisory, implementation and ongoing management using Mimecast
Our own certification	ISO/IEC 27001:2022, certificate 202507-118, Sensiba Australia Pty Ltd, valid 1 August 2025 to 1 August 2028
Stated framework alignment	APRA CPS 234; NIST; ASD Essential 8 Maturity Level 3
MDR compliance alignment stated	ISO/IEC 27001, Australian Privacy Principles, Essential Eight, NIST CSF, SOC 2 Type II, GDPR (alignment, not attestation)
Customer Zero	We apply the same security architecture, processes and control to our own environment and the emPOWER platform

What the pillar covers

Function	Scope
Detect and Respond	Continuous monitoring, managed detection, threat investigation and incident response to reduce dwell time and contain threats earlier
Human Risk	Awareness training, phishing simulations, behavioural insights and practical education to strengthen user behaviour
Threat Exposure	Visibility across vulnerabilities, misconfigurations, cloud services, identities and attack surfaces so remediation focuses on the risks most likely to affect the organisation
Governance, Risk and Compliance	Governance, reporting and cyber maturity through practical frameworks that manage risk, improve controls and align security investment with business objectives

Security also runs through the other pillars. The emPOWER Network carries Palo Alto Networks virtual firewalls, emPOWER Connectivity delivers unified threat protection on dedicated next-generation firewalls, emPOWER Cloud operates under our ISMS with an accountable information security officer, and emPOWER Managed Services includes proactive security management and Security Gap Analysis audits.

emPOWER Security

The integrated portfolio page: managed detection, exposure management, governance and human risk services combined to strengthen cyber resilience. This is the entry point for organisations that want the whole security operating model rather than one component.

Managed Detection and Response

emPOWER MDR combines continuous monitoring with EDR, ITDR, SIEM and threat intelligence feeds, human investigation, and rapid triage, containment and remediation, on a 24/7 basis. It integrates with Microsoft Security, Microsoft Identity, Microsoft Sentinel, CrowdStrike and other tooling, provides dashboards and monthly reporting for leadership, and follows ITIL-aligned incident management. Our differentiators are 24/7 coverage, bridging Security Operations and IT Operations to shorten response and recovery, and scalable options for different maturity levels and budgets. The MDR brochure also names Vulnerability Management, an Incident Response Retainer, vCISO Advisory and Human Risk Management without establishing their inclusion in every engagement; treat them as separately scoped until confirmed on the Service Order.

Exposure Management

Continuous visibility of assets, vulnerabilities and security exposure across infrastructure, cloud services, identities and attack surfaces, so remediation can be prioritised around the risks most likely to affect the organisation.

Human Risk Management

A fully managed service with four components: security awareness education with regular phishing simulations aligned to current attack techniques and identification of high-risk users; detection and real-time alerting of malicious and suspicious email; investigation and classification of user-reported phishing with containment guidance; and monitoring for accidental or malicious data exposure across endpoints, browsers and cloud applications. We describe the lifecycle as prevent, detect, respond and reduce, and the stated outputs include auditable reporting aligned to GRC. Ask us to document the platform, baseline, targets, simulation frequency, reporting cadence and licensing in the agreed service scope.

Governance, Risk and Compliance

Security governance, risk and compliance support that helps organisations understand obligations, strengthen controls and manage cyber risk through a practical framework. Our own reference points are ISO/IEC 27001, the Australian Privacy Principles, ASD Essential Eight, NIST CSF and, for financial services customers, APRA CPS 234 alignment and the CPS 231 clause in its General Terms and Conditions.

Our Mimecast-based DMARC service provides advisory, implementation and ongoing management of SPF, DKIM and DMARC. The brochure relates it to tighter sender requirements introduced by major email providers during 2024–2025. Applicability and volume thresholds differ by provider; check each destination provider's current sender rules for your sending domains.

How it is delivered

MDR is delivered from our security operations function with 24/7 alert notification, triage and remediation. The stated advantage of bridging SecOps and IT Ops is that the team that detects an incident is connected to the team that can change the environment, which is the practical reason we give for shorter response and recovery.

Human Risk Management runs continuously: education and simulations on an ongoing cycle, email threat detection and prioritised alerting in real time, investigation of what users report, and behavioural insight used to target repeat risk.

Contractually, security services are ordered on a Service Order under the General Terms and Conditions v3.6. The eleven listed Schedules do not identify a standalone security Schedule. Confirm the Schedule, classification, term and reporting obligations for the particular MDR, HRM or GRC engagement instead of inferring them from the portfolio label. The referenced General Terms provide standard monthly reports within 5 Business Days of month end and six-monthly service reviews, subject to the governing agreement and variations. Clause 17 obliges blueAPACHE to take all reasonable steps to prevent unauthorised access to Customer Records and Customer Data and to implement the security features set out in the relevant Schedule; clause 18.4 governs eligible data breach notification between the parties. Clause 19.4(e) specifies $1 million per event or series of connected events and $2 million in aggregate for breaches of clauses 16, 17, 18 or 20. Read clause 19 with its other qualifications, applicable law and any agreed variations.

Support and service levels

Published. MDR coverage is 24/7 for alert notification, triage and remediation across the full IT environment and security stack. Unified threat protection on emPOWER Connectivity firewalls is supported 24x7. Monthly reporting and leadership dashboards are included in MDR.

The MDR brochure does not state detection or response-time targets, and the Managed Services brochure describes a customer-specific priority and escalation matrix. The Human Risk Management brochure does not give numeric baselines, targets or simulation frequency. Obtain the relevant service

catalogue, Service Order and Schedule to establish the commitments needed for a tender.

Compliance alignment versus attestation. Our MDR service is compliance-aligned with ISO/IEC 27001, the Australian Privacy Principles, Essential Eight, NIST CSF, SOC 2 Type II and GDPR. We hold an ISO/IEC 27001:2022 certificate for our own ISMS. The General Terms and Conditions also exclude GDPR-subject personal data: the customer warrants it will not provide, or ask us to process, personal data subject to the EU GDPR.

Data handling. Our data sovereignty statement says customer data is stored and processed in Australian data centres with role-based access, MFA and audit logging, and clause 17 prohibits blueAPACHE from using Customer Data for marketing or profiling. Customers with fourth-party obligations should note that clause 27.4 lets us subcontract without notification, and clause 18.3 records a standing consent to overseas transfer of Personal Information to listed countries.

How it integrates with the other pillars

Connectivity. Network telemetry, Palo Alto Networks virtual firewalls, intrusion prevention, application control and web filtering sit in the emPOWER Network and emPOWER Connectivity; Agree which telemetry sources feed MDR, the required integrations and who authorises and performs response actions across the network, endpoints and identities. See the Connectivity hub .

Cloud. emPOWER Cloud operates under our ISMS, is in scope of the ISO/IEC 27001:2022 certificate, and hosts emPOWER Backup for Microsoft Entra ID, the identity-resilience counterpart to MDR's identity threat detection. See the Cloud hub .

Managed Services. Proactive security management and Security Gap Analysis audits are part of the managed services scope; the 24/7 MDR service, HRM and Exposure Management are the dedicated security layer on top. See the Managed Services hub .

Microsoft Practice. MDR integrates with Microsoft Security, Microsoft Identity and Sentinel, and the Microsoft Practice's Security solution area is described as Zero Trust aligned. See the Microsoft Practice hub .

Collaboration. Email and collaboration platforms are the attack surface Human Risk Management and DMARC address. See the Collaboration hub .

Our client outcomes

Customer	What was delivered	Stated outcome
Honan Insurance (c. 2020-2021)	Palo Alto Networks remediation of a failing data and Wi-Fi network during the tender, then firewalling within the WAN transformation	Network outages resolved; our ISO certification supported Honan's ability to bid for work where it had become a mandatory customer requirement
Archers The Strata Professionals (2026)	Dedicated FortiGate firewalls replacing a shared firewall, unified threat protection with web filtering and intrusion prevention, FortiClient EMS VPN, decommissioning of end-of-life Windows Server 2012	High-level security risks mitigated; journey towards ISO 27001 alignment started; security assessment completed for future AI capabilities including Microsoft Copilot
Brotherhood of St. Laurence (2016)	Security measures deployed for 17 new NDIS sites; support for	Client states we helped it achieve ISO 27001 certification in as little

	the client's own ISO 27001 certification	as six months to support its NDIS bid

Distinguishing the four security functions

A proposal should identify the exposure management, detection and response, governance, and human risk functions included and their hand-offs. Identifying an exposure differs from implementing a fix; investigating an alert differs from authorising disruptive containment. Record covered assets, the customer decision-maker, escalation and evidence retained. Framework alignment and our own certification do not, on their own, establish the customer's compliance or the inclusions of a specific service.

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.

How liability differs from service performance

Clause 19 separates performance obligations from financial liability. Under General Terms v3.6 clause 19.3, subject to clauses 19.1, 19.2 and 19.4 and applicable law, the per-single-claim limit is the greater of amounts paid under the agreement in the three months before the claim first arose or $25,000. Clause 19.4(e) specifies $1 million per event or series of connected events and $2 million in aggregate for breaches of clauses 16, 17, 18 or 20. Confirm the version and variations applying to your agreement. 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.

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.

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.

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.

Related

emPOWER Security
Managed Detection and Response
Exposure Management
Human Risk Management
Governance, Risk and Compliance
Private and Public SaaS Backup
Connectivity hub
Cloud hub
Managed Services hub
Microsoft Practice hub
blueAPACHE Security case study
Honan Insurance case study
Archers case study
Financial Services industry page
Healthcare and Aged Care industry page
Government and Public Sector industry page
Service agreement
Home

Is emPOWER MDR a 24/7 service?

Yes. Our MDR service provides 24/7 alert notification, triage and remediation across the full IT environment and security stack, using EDR, ITDR, SIEM and threat intelligence feeds with human investigation. The MDR brochure gives no detection, triage or response-time figures; confirm applicable targets in the service catalogue and agreement.

Does MDR replace the security tools we already own?

Not necessarily. The MDR brochure names Microsoft Security, Microsoft Identity, Microsoft Sentinel and CrowdStrike among its integrations. Confirm compatibility, licensing and responsibilities for your

existing tools.

Are vulnerability management, an incident response retainer and vCISO advisory included in MDR?

Human Risk Management is sold as its own service, which suggests these are separately scoped. Confirm inclusion in writing on the Service Order.

What does Human Risk Management actually include?

Four managed components: security awareness education with regular phishing simulations and identification of high-risk users; detection and real-time alerting of malicious and suspicious email; investigation and classification of user-reported phishing with containment guidance; and monitoring for accidental or malicious data exposure across endpoints, browsers and cloud applications.

What does your ISO certificate cover, and is SOC 2 alignment an attestation?

Blue Apache Pty Ltd holds ISO/IEC 27001:2022 certificate 202507-118 from Sensiba Australia Pty Ltd, valid 1 August 2025 to 1 August 2028, covering our emPOWER infrastructure and managed service offerings. The certificate concerns our ISMS, not certification of individual services. The MDR brochure describes SOC 2 Type II alignment; that statement does not establish a SOC 2 attestation. Request the relevant audit evidence if required.

Which frameworks do your security services align to?

Our published material states alignment with APRA CPS 234, describes NIST-compliant data management controls and cites ASD Essential 8 Maturity Level 3. Confirm the scope and supporting assessment evidence for your requirements. Note that the General Terms and Conditions exclude GDPR-subject personal data from the services.

What security is already built into the network and cloud services?

The emPOWER Network runs Palo Alto Networks virtual firewalls with intrusion detection, application-level monitoring, perimeter protection and secure VPN provisioning. emPOWER Connectivity adds dedicated next-generation firewalls with intrusion prevention, malware protection, application control, web filtering and antispam, supported 24x7. emPOWER Cloud operates under our ISMS with an accountable information security officer.

Do you offer email authentication or DMARC help?

Yes. We provide DMARC advisory and assessment, implementation and configuration, and ongoing monitoring using Mimecast, covering SPF, DKIM and DMARC alignment and safe progression from monitoring to enforcement.

What happens if we suspect a security compromise from our equipment?

Clause 3.26 of the General Terms and Conditions allows us to suspend or cancel a service on a reasonable suspicion that its continued provision compromises the security of our environment, for example a vulnerability in customer equipment or a denial of service attack, without fees accruing during the suspension. We must give as much notice as reasonably possible and both parties must use

best efforts to find a solution.

Can we see evidence of your security work with named clients?

Our case studies describe Palo Alto Networks remediation and firewalling for Honan Insurance, a FortiGate firewall hub with unified threat protection for Archers, and security deployment across 17 new sites for the Brotherhood of St. Laurence.

What is emPOWER Security?

emPOWER Security combines managed detection and response, exposure management, governance and human risk services to help organisations strengthen cyber resilience.

Who provides the emPOWER Security service and where is it offered?

The emPOWER Security service is provided by us, and it is offered within Australia.

Is security treated as a standalone service by you, or is it integrated elsewhere?

Security is not treated as a separate siloed practice by us. Instead, it is described as being 'built into the DNA' of each of the four core service pillars within the emPOWER portfolio: Connectivity, Collaboration, Cloud, and Managed Services.

What security capabilities are included in emPOWER Managed Services?

The Managed Services brochure names proactive security management, Security Gap Analysis audits and managed detection and response capabilities. Confirm the security services included in the customer's agreement.

What security features does the emPOWER Network provide?

The emPOWER Network, our private MPLS core network infrastructure, provides Palo Alto Networks firewall infrastructure for integrated security, edge or perimeter monitoring and protection, secure VPN provisioning, security monitoring with real-time detection and interdiction capabilities, and application-level monitoring.

What security services are delivered through emPOWER Connectivity?

The connectivity portfolio describes Unified Threat Protection including intrusion prevention, malware protection, application control and web filtering, with 24x7 support, alongside next-generation firewalls and SASE capabilities. The proposal and service agreement define the components included in a deployment.

What is your approach to aligning security with business governance?

We are dedicated to aligning business governance requirements to support the risk profile of organisations, applying a security-by-default principle that permeates all service delivery.

How does ISO/IEC 27001 certification relate to emPOWER Cloud?

Certificate 202507-118 lists emPOWER Cloud Services within the scope of Blue Apache Pty Ltd's ISO/IEC 27001:2022 Information Security Management System. The certificate concerns the management system and expressly does not certify individual products or services.