

emPOWER Security | blueAPACHE

Canonical: <https://www.blueapache.com/services/empower-security-top-level>

Details:

Summary

emPOWER Security is our integrated security operating model. Rather than a single product, it is four pillars run together, each answering a different question, with reporting that feeds compliance evidence.

The portfolio connects technology, process and people. Define how exposure findings, human-risk signals, incident investigations and governance reporting will inform one another, including the responsibilities retained by internal teams and other suppliers.

How the vendor capabilities fit together

Our Mimecast-powered Human Risk Management announcement identifies the technology behind its managed human-risk service. Awareness, behavioural signals and policy visibility help prioritise interventions; onboarding needs an agreed user population, directory integration, reporting access and follow-up ownership.

The expanded Huntress partnership adds Managed EDR and Managed ITDR to the endpoint and identity discussion. The August 2026 announcement describes managed and reseller options that extend Microsoft Defender and Entra investments through Managed EDR and Managed ITDR. Confirm detection coverage, investigation responsibilities and containment authority for the option you purchase.

These are complementary parts of the service design. Connect an endpoint or identity alert to the investigation and containment workflow, and connect human-risk findings to targeted training or corrective action. Agree coverage, integrations and authority to act in the service scope so that the customer can distinguish technology availability from the managed work being purchased.

The four pillars

Pillar	Question it answers	Service
Detect & Respond	What is happening now, and how do we contain it?	Managed Detection and Response
Human Risk	Who is being targeted, and how do they behave?	Human Risk Management
Threat Exposure	Where are we weak, and what matters most?	Exposure Management
Governance, Risk & Compliance	Can we evidence this to an auditor or board?	Governance, Risk and Compliance

Detect & Respond

Continuous monitoring, managed detection, threat investigation and incident response — 24/7 alert notification, triage and remediation across the IT environment and security stack, combining EDR, ITDR, SIEM and threat intelligence.

Human Risk

Awareness training, phishing simulation and behavioural insight. For historical context, Proofpoint's summary of Verizon's 2022 DBIR reports that 82% of breaches involved a human element; this is not a current universal rate or a claim that those breaches all started with human behaviour. Also covers email threat detection, user-reported phishing response, and insider risk and data exposure monitoring.

Threat Exposure

Continuous visibility across vulnerabilities, misconfigurations, cloud services, identities and attack surface, prioritised by likely business impact rather than raw severity.

Governance, Risk & Compliance

Frameworks to manage risk, improve controls and align security investment — producing auditable reporting as an output of the services rather than as a separate exercise.

Security is embedded, not bolted on

Our approach embeds security across the portfolio. The following are capabilities described in the relevant service material; the agreement and architecture determine which controls, locations and integrations apply:

Connectivity — Palo Alto Networks firewalls integrated through the core network, with intrusion prevention, advanced malware protection, application control, web filtering and antispam, supported 24x7

Cloud — cloud services within the stated ISMS scope, with Australian data hosting, role-based administrative access, MFA and audit logging described in our cloud and data-sovereignty material; confirm locations and transfer arrangements for the agreed service

Managed Services — proactive security management, Security Gap Analysis audits, and automated patching

Microsoft Practice — Microsoft Security, Entra ID and Sentinel integration

Certification and framework alignment

ISO/IEC 27001:2022 — certificate 202507-118, issued by Sensiba Australia Pty Ltd, with stated dates of 1 August 2025 to 1 August 2028 and ten service offerings listed within the ISMS scope; the certificate does not certify individual services

ASD Essential Eight — Maturity Level 3

APRA CPS 234 — stated compliance

NIST — stated compliance

Australian Privacy Principles , NIST CSF , SOC 2 Type II , GDPR — MDR is described as compliance-aligned with these

Customer Zero

Our published Customer Zero approach describes using security architecture and controls internally before extending capability to customers. The CyberArk case study documents identity controls in our business and managed services; it does not establish identical architecture or controls for every customer. Confirm the controls included in your agreed design.

That is a reasonable thing to probe in evaluation: ask which controls we run internally that we do not yet offer as a service, and vice versa.

Integration with other emPOWER services

The portfolio is designed to work alongside our managed services, cloud and connectivity offerings. Agree the following interfaces for your deployment:

Connectivity — confirm which network and firewall logs feed detection and exposure services, with required permissions, retention and response ownership

Cloud — identify the cloud assets, identities and configurations included in Exposure Management ; ISMS scope and administrative access controls do not by themselves establish scan coverage

Managed Services — agree how Security Gap Analysis findings, patching responsibilities and Exposure Management remediation actions connect, including what the managed-services bundle covers

Microsoft Practice — the MDR brochure names Microsoft Security, Microsoft Identity and Sentinel integrations; confirm which are configured for Managed Detection and Response in your environment

Collaboration — confirm the Microsoft 365 identities, applications and signals covered by detection, and the separate protection requirements for Microsoft Teams and SharePoint data

Typical engagement

Onboarding. As with other emPOWER services, Transition In Services begin immediately after the Service Commencement Date: due diligence to catalogue the environment and existing security tooling, configuration of monitoring where applicable, documentation on how to engage our teams, and an agreed reporting cadence. Because security engagements typically bring one or more of the four pillars together, scoping which pillars are included — and which existing tools they integrate with rather than replace — is the substantive part of transition.

Steady state. The MDR brochure describes 24/7 alert notification, triage and remediation. Confirm the contracted assets and handling arrangements. Agree the exposure-monitoring coverage, human-risk education and simulation schedule, and governance/reporting cadence for the other purchased services.

Term, renewal and exit. Confirm each service's classification and term. The referenced General Terms set a 36-month default excluding Professional Services, unless the Service Description or Service Order states otherwise. Clause 9 addresses deletion of defined Customer Data and Customer Software from our environment and the customer's responsibility to take a copy before expiry or termination. This does not establish ownership, export rights or deletion requirements for every security configuration, incident log or training record. Agree those items, retention exceptions and any migration assistance in the exit plan.

Choosing security components deliberately

Use this portfolio page to decide which functions to purchase rather than treating it as one all-inclusive service. Exposure management prioritises risk; MDR addresses detection and response; GRC addresses governance; Human Risk Management addresses people-related risk. Record the interfaces and work retained by the customer, including who implements remediation and approves incident actions. A common brand does not establish that every platform or advisory activity is included.

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.

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.

How liability differs from service performance

Clause 19 separates performance obligations from financial liability. Subject to clauses 19.1, 19.2 and 19.4 and applicable law, the general cap per single claim is the greater of amounts paid under the agreement in the three months before the claim first arose or \$25,000. Clauses 16, 17, 18 and 20 are

subject to a \$1 million cap per event or series of connected events and \$2 million in aggregate under clause 19.4(e). 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.

Is emPOWER Security one product or several?

Four pillars run as one operating model: detection and response, human risk, threat exposure, and governance risk and compliance. Discuss which components are available and appropriate for the engagement, and document their inclusions and interfaces in the proposal.

What response time do you commit to?

The MDR brochure describes 24/7 alert notification, triage and remediation. Obtain the response targets, priorities and escalation arrangements applicable to the services you purchase; do not infer them from the portfolio name.

Do we have to replace our existing security tools?

No. MDR integrates Microsoft Security, Microsoft Identity, Microsoft Sentinel, CrowdStrike and other third-party tooling.

Are you certified?

Certificate 202507-118 concerns Blue Apache Pty Ltd's ISO/IEC 27001:2022 ISMS, with ten service offerings listed within its scope; it does not certify the services themselves. Separate material states Essential Eight Maturity Level 3 and APRA/NIST alignment or compliance. Those statements are distinct from certification. The MDR brochure's SOC 2 alignment statement is not a SOC 2 attestation; request the relevant assessment evidence.

Which pillar should we start with?

It depends on the gap. If you have tooling but no one watching it, start with Detect & Respond. If your incidents start with phishing, start with Human Risk. If you cannot answer an auditor, start with GRC. If you have a backlog of findings you cannot prioritise, start with Threat Exposure.

Is security included in managed services?

Proactive security management and Security Gap Analysis audits are within managed services scope. Dedicated 24/7 detection and response, human risk and exposure management are sold through this pillar — confirm inclusion on the Service Order.

Do you use your own services internally?

The CyberArk case study describes identity controls across our own business and managed services. This illustrates internal use alongside our Customer Zero positioning; confirm the controls and scope of your particular deployment.

What is the contract term for emPOWER Security?

The referenced General Terms set a 36-month default for services other than Professional Services, unless the Service Description or Service Order specifies otherwise. Confirm the classification, governing documents and term for each security service.

What happens if we let the term lapse without notice?

If the customer gives no notice under clause 2.8 but continues to access or use services after the Service Period ends, clause 2.9 extends all Services on the agreement by three months at the then-current full list price, with the defined Service Levels not applying during that period. This does not remove all other contractual security obligations.

Can we terminate early if we are not satisfied?

Check the termination ground, notice requirements, applicable Schedule and negotiated variations. Early termination payments and unmet minimum commitments depend on those provisions; dissatisfaction alone does not establish a particular right or charge.

What happens to our incident history and training records if we leave?

Clause 9 addresses defined Customer Data and Customer Software, including the customer's responsibility to take a copy before expiry or termination. Incident history, audit evidence and training records may have different ownership, licence and retention rules. Agree export formats, access deadlines, assistance costs and legally required retention before exit; do not assume every record is customer-owned or immediately deleted.

Does emPOWER Security cover data breach notification obligations?

The General Terms and Conditions require each party to notify the other of an eligible data breach within 24 hours of discovery. That is a contractual obligation on both parties, separate from, and in addition to, the technical detection and response this service provides.

What support window applies to a security incident?

The MDR brochure describes 24/7 alert notification, triage and remediation without MTTD or MTTR figures. Confirm coverage, response handling and any measurable targets in the applicable service documents.

Related

Security hub · Managed Detection and Response · Human Risk Management · Exposure Management · Governance, Risk and Compliance · Connectivity · emPOWER SASE · Cloud · Managed Services · Glossary · Contact

What is emPOWER Security?

emPOWER Security is our integrated security portfolio that combines managed detection and response, exposure management, governance, risk and compliance, and human risk management to strengthen cyber resilience for organisations.

What are the four components of the emPOWER Security portfolio?

The four components are Managed Detection & Response, Human Risk Management, Governance, Risk & Compliance, and Exposure Management.

Does emPOWER Security operate as a standalone security layer?

No, emPOWER Security is designed to work alongside our managed services, cloud and connectivity offerings rather than operate as a disconnected security layer.

What benefits does emPOWER Security aim to deliver for organisations?

It aims to improve visibility, help organisations prioritise action, and build stronger cyber resilience by bringing together detection and response, governance, and human risk management across technology, process and people.

Who is the target audience for emPOWER Security?

The portfolio supports organisations seeking integrated security across technology, process and people. blueAPACHE's August 2026 Huntress announcement describes Australian organisations of different sizes, including SMB and mid-market customers; discuss suitability and scope for your organisation.

What does the Managed Detection and Response (MDR) service within emPOWER Security include?

The MDR brochure describes 24/7 alert notification, triage and remediation, using Endpoint Detection and Response (EDR), Identity Threat Detection and Response (ITDR), SIEM and threat intelligence, with ITIL-aligned incident management. It names Microsoft Security, Microsoft Identity, Sentinel and CrowdStrike integrations. Confirm covered assets, integrations and response authority in the agreement. Framework alignment is distinct from certification or a customer maturity assessment.

What does the Human Risk Management (HRM) service within emPOWER Security cover?

HRM is a managed security awareness service that includes ongoing security awareness education, regular phishing simulations aligned to current attack techniques, email threat detection and alerting, user-reported phishing response and investigation, insider risk and data exposure protection monitoring across endpoints, browsers, and cloud applications, and behavioral insights with remediation guidance.

How can someone contact you for support related to emPOWER Security?

Support options include calling 1300 135 548 (Australia) or +61 3 8696 9369 (international), emailing support@blueapache.com, using the Remote Access or Client Portal links, or speaking to the team via the contact page. The general contact number listed for the service is 1800 248 749.