Exposure Management | blueAPACHE

Canonical: https://www.blueapache.com/services/exposure-mananagement

Details:

Summary

Exposure Management is one of the four pillars of emPOWER Security . It provides continuous visibility of assets, vulnerabilities and security exposure , so remediation can be prioritised around the risks most likely to affect the business rather than attempted uniformly across everything a scanner reports.

The service helps teams prioritise exposures using context and likely business impact. The number of findings and the remediation effort depend on the assessed environment.

Key facts

Fact	Value
Security pillar	One of four: Detect & Respond, Human Risk, Threat Exposure, Governance Risk & Compliance
What it covers	Vulnerabilities, misconfigurations, cloud services, identities, attack surface
Delivery	Continuous visibility rather than point-in-time assessment
Purpose	Prioritise remediation by likely business impact
Related services	MDR , Human Risk Management , GRC

What it gives visibility over

Vulnerabilities — identified weaknesses in systems and applications

Misconfigurations — security control gaps in infrastructure that need assessment alongside software vulnerabilities

Cloud services — cloud assets and their exposure, including resources created outside a formal provisioning process

Identities — identity-related exposure within the agreed assessment scope

Attack surface — the full scope of exploitable entry points, including what is externally reachable

Why prioritisation is the actual product

A severity score is one input to remediation priority. Consider the affected asset, external reachability, business impact, compensating controls and available exploit information. Agree which of these inputs the service can collect and use for your environment.

Exposure Management is intended to answer the question a severity score cannot: which of these would actually hurt us, and in what order should we fix them. That is why it sits alongside detection rather than inside it. Detection and response investigate signs of threats and incidents. Exposure Management identifies and prioritises weaknesses; it does not predict the next incident or guarantee where it will occur.

How the four security pillars fit together

Pillar	Question it answers
Threat Exposure	Where are we weak, and which weaknesses matter most?
Detect & Respond	What is happening right now, and how do we contain it?
Human Risk	Which of our people are being targeted, and how do they behave?
Governance, Risk & Compliance	Can we evidence any of this to an auditor, insurer or board?

Run in isolation each has a blind spot. Exposure Management without detection finds weaknesses but misses active compromise; detection without exposure management responds to incidents that a known, unremediated weakness enabled.

Stated outcomes

The service is designed to improve visibility of security weaknesses and help direct remediation toward exposures with greater business impact. These are intended benefits, not measured outcomes for every customer or a guarantee of compliance.

Where it connects to Essential Eight

Exposure findings may inform an Essential Eight improvement programme, but the service description does not establish assessment coverage for each mitigation strategy or a customer maturity level. Agree a control-to-evidence mapping, asset scope and assessment method with your assessor. A broader blueAPACHE maturity statement is not a maturity assessment of your environment.

Integration with other emPOWER services

Exposure Management is designed to sit alongside, not instead of, the other security capabilities and the wider portfolio it draws context from:

Managed Detection and Response — exposure findings identify what is weak; MDR watches for active exploitation of it. Vulnerability Management is listed alongside MDR in our material without stated inclusion status, so confirm whether exposure visibility is bundled with your MDR service or purchased separately

Human Risk Management — a related service addressing awareness and behaviour; agree any shared measures or data integration

Governance, Risk and Compliance — a related capability; agree which exposure reports, if any, support your governance or assessment requirements

Cloud — confirm the cloud accounts, assets, permissions and integrations in the assessment scope; an emPOWER Cloud agreement does not automatically include every asset in Exposure Management

Typical engagement

Onboarding. Agree the asset, identity and cloud boundaries, required access, tool configuration, report formats and reporting schedule before work begins. General Terms v3.6 describe Transition In due diligence and applicable monitoring setup; they do not establish every Exposure Management deliverable or additional report as an automatic inclusion. Confirm the agreement version and scope applicable to your order.

Steady state. Visibility runs continuously across vulnerabilities, misconfigurations, cloud services, identities and attack surface, with findings prioritised by likely business impact.

Term and exit. General Terms v3.6 provide a 36-month default Minimum Service Period except Professional Services and where the Service Description or Service Order states otherwise. Holdover requires the conditions in clause 2.9, including continued use. The exit provisions distinguish Customer Data, Customer Records and other materials. Agree ownership, export formats, timing and retention for your findings register and scan history; do not assume every platform record is exportable Customer Data or will be deleted on exit.

Following an exposure through to closure

Define who validates a finding, assigns an owner, approves a change and confirms the exposure is addressed. Record asset boundaries, exclusions and evidence retained for accepted risks. A prioritised finding is not proof that remediation is included or complete. If Managed Services or another supplier performs the fix, agree the hand-off so reporting distinguishes new findings, accepted risks and completed work.

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.

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.

How liability differs from service performance

Clause 19 separates performance obligations from financial liability. Under General Terms v3.6, the general cap per Claim is the greater of amounts paid under the Service Agreement in the three months before the Claim first arose and $25,000, subject to clauses 19.1, 19.2 and 19.4 and applicable law. The specified confidentiality, information-security, privacy and IP-indemnity liabilities have a $1 million cap per event or connected series of events and a $2 million aggregate cap. Confirm the version and negotiated terms applicable 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.

Is Exposure Management the same as vulnerability scanning?

The service description emphasises visibility and context to prioritise exposures by likely business impact. Scanning can contribute findings; confirm the tools, contextual inputs, prioritisation method and remediation deliverables included in your scope.

Does it cover cloud environments?

Yes — cloud services are one of the five named coverage areas, alongside vulnerabilities, misconfigurations, identities and attack surface.

Who fixes what it finds?

Confirm whether remediation is performed under your managed services agreement or handed back to your team as recommendations.

What platform does it run on?

Speak with our team about the platform and integration requirements for your environment. We confirm the tools and service scope in your proposal.

How often does it assess?

It is described as continuous rather than point-in-time; confirm the actual cadence.

Is it included with MDR?

The published descriptions do not establish whether Exposure Management is included in a particular MDR order. Confirm the included capabilities, licences, deliverables and charges in your proposal and Service Order.

Does it help with Essential Eight?

Exposure findings may support an improvement programme, but coverage of individual Essential Eight assessment requirements is not established by the service description. Agree the evidence mapping and assessment scope; a provider maturity statement does not establish your organisation’s maturity.

Does it include penetration testing?

The public description does not establish whether penetration testing is included in your proposal. Confirm its inclusion, scope, method and reporting requirements explicitly.

What is the contract term?

General Terms v3.6 provide a 36-month default, except Professional Services and where the Service Description or Service Order states otherwise. Confirm the agreement version and term applicable to your order.

What happens if we do not give notice before the term ends?

Under clause 2.9 of General Terms v3.6, holdover applies where the required notice has not been given and the customer continues using the Services after the relevant period. It extends the Service Period by three months at full list price without Service Levels applying. Confirm the notice provisions and any different terms in your agreement.

Can we cancel early?

Termination rights and any Early Termination Payment depend on the applicable agreement, termination ground, Schedule and negotiated terms. Check the notice and payment provisions for your situation; an early exit is not governed by a single unconditional rule.

What happens to our findings register when we leave?

The v3.6 exit provisions require the customer to take copies of Customer Data before the Service Period ends and provide for deletion of Customer Data from the blueAPACHE Environment at no cost, alongside other return and exit duties. They do not establish the ownership, exportability or deletion of every scan log or platform record. Agree an export and retention plan for the findings register and remediation history before exit.

Does this service handle our data, and where does it sit?

Yes — asset, vulnerability and identity data is processed to generate findings. We state customer data is stored and processed within Australian-based data centres under Australian legal jurisdiction, with role-based access and audit logging.

What support window applies?

The service is described as providing continuous visibility. That description does not specify a staffed response window or guaranteed escalation times. Agree support hours, high-severity handling, responsibilities and escalation commitments in your Service Description and Service Order.

Related

Security · emPOWER Security · Managed Detection and Response · Human Risk Management · Governance, Risk and Compliance · Managed Services · Glossary · Contact

What is your Exposure Management service?

Exposure Management is a service from us that provides continuous visibility of assets, vulnerabilities and security exposure so teams can prioritise remediation around the risks most likely to affect the organisation.

What does the Exposure Management service help organisations do?

It helps organisations identify and prioritise cyber exposure, improving visibility across assets, vulnerabilities and remediation priorities.

Who provides the Exposure Management service?

The Exposure Management service is provided by us.

What category and service type does your Exposure Management fall under?

Exposure Management is categorised under Security, with a service type described as Integrated security and response.

In which area is your Exposure Management service offered?

The Exposure Management service is offered in Australia.

What kind of visibility does Exposure Management provide?

It provides continuous visibility across assets, vulnerabilities and overall security exposure within an organisation.

How does Exposure Management help with remediation efforts?

It allows teams to prioritise remediation efforts around the risks most likely to affect the organisation, rather than treating all vulnerabilities equally.