AVERTORY

SERVICES CATALOGUE

Orca Security

AVERTORY LIMITED

Implementation, optimisation and lifecycle management for Orca Security — sold by you, delivered by us.

ORCA-Deploy	Cloud onboarding and baseline
ORCA-Remediate	Risk prioritisation programme
ORCA-Operate	Continuous CSPM / CWPP management

Version 1.1 · August 2026 · Partner-confidential
Avertory Limited · Companies House 16542620 · UK professional services only

AT A GLANCE

The catalogue in context

Item	Detail
Audience	Channel distributors, resellers, VARs and security vendors
Use	Price book, portal, SOW annex or partner enablement pack
Platform	Orca Security CNAPP
Commercial model	Partner-first. Licensing stays on partner paper. Avertory supplies certified delivery.
Service boundary	Implementation, configuration, integration, prioritisation and tracking. Not mitigation or remediation execution.
Version	1.1 · August 2026 · Split from the combined Services Catalogue
Legal	Avertory Limited · Companies House 16542620 · UK professional services only

This catalogue is the service menu partners attach to a licence sale. Fixed-price SKUs are delivery envelopes with written assumptions. Anything outside those assumptions is scoped before work starts. Wholesale rates and recommended retail sit in the Partner Commercial & Delivery Pack — they are not repeated here so this document can travel to pre-sales and, where you choose, sit behind a white-label cover.

> Avertory does not sell software licences, does not compete for the customer relationship, and does not provide mitigation or remediation execution. The end-user organisation meets us only through you.

01

How to use this catalogue

- Paste SKU names and short descriptions into your price book, bid portal or statement of work. Replace [Partner] with your trading name if you white-label.
- Sell the outcome. Lead with time-to-value, a documented build and a partner-owned operating rhythm — not hours.
- Use ORCA-Deploy as the default attach to a new licence. Add Prioritise or Operate when the estate or the RFP needs them.
- Sell Operate or a lifecycle retainer once the platform is live. That is how you protect renewal and CSAT without hiring a bench.
- Foundation and Standard envelopes in the Commercial & Delivery Pack map to Deploy SKUs. Enterprise work is always scoped.
- End-user contact, reporting packs and licence expansion conversations stay under your control. Operating rules are in section 8.

HARD BOUNDARY

What Avertory is not

Not a mitigation or remediation specialist

Avertory implements, configures, optimises, integrates and operates SentinelOne, Orca Security and Qualys. We design prioritised backlogs and track whether owners have closed items. We do not apply patches, change cloud or identity configurations, execute compensating controls, or act as an incident-response / SOC mitigation function.

Where a platform includes native response features (for example SentinelOne containment and rollback, Orca suggested fixes, Qualys Patch Management), we configure those features so the customer's operational owners can use them. Pressing the button, making the change, and owning residual risk stay with the customer — presented through you.

SKU names such as ORCA-Remediate refer to prioritisation and tracking workstreams on the platform. They are not an offer to remediate or mitigate.

What we sell — and what we do not

We deliver	We do not deliver
Platform implementation and configuration	Software licences and renewals
Policy, detection and posture design	Mitigation or remediation execution
Integrations and workflow design	Patching, hardening or configuration change in production
Risk prioritisation and owner-ready backlogs	Incident response, containment or forensics as a service
Closure tracking and exception registers	Acting as the customer's IT operations or SOC
Monthly operation and second-line on the platform	The customer relationship, QBR or upsell
Partner-branded handover and reporting	First-line service desk, unless separately scoped

Engagement models

Model	When to use it	Customer sees
White-label	You want Avertory invisible	Your brand only
Co-delivery	Your team leads; we supply specialists	Your account team, our engineers behind them
Named delivery partner	Vendor or distributor wants us visible	Avertory on the SOW; you on the commercial
Retainer / Operate	Post go-live tuning and second-line on the platform	Recurring line you sell and present

02

Catalogue at a glance

Three SKUs on Orca Security. Deploy gets the CNAPP into production. The remaining SKUs deepen platform value after the first landing, or keep the estate healthy. None of them is a mitigation or remediation execution service.

Orca Security — agentless CNAPP

SKU	Service	Typical duration	Attach when
ORCA-Deploy	Cloud onboarding and baseline	6–10 days	First accounts or a clean rebuild
ORCA-Remediate	Risk prioritisation programme	8–15 days + cadence	Findings exist; owners need a ranked plan
ORCA-Operate	Continuous CSPM / CWPP management	2 or 4 days / month	Multi-cloud estate in production

Durations are starting envelopes for a typical mid-market UK estate delivered remotely in UK business hours. Multi-site, multi-tenant, OT, air-gapped or heavily regulated estates are scoped as Enterprise before you quote.

ORCA-Remediate is named for the platform workstream it supports. Scope is prioritisation, workflow design and tracking only.

03

Orca Security services

Platform reference: orca.security. Avertory onboards and operates the Orca Cloud Security Platform; we do not sell the licence and we do not change the customer's cloud accounts.

Solution areas we service

Orca is an agentless-first CNAPP. Patented SideScanning typically produces a usable inventory and risk view within hours of connecting cloud accounts, without an agent rollout tax. A lightweight Sensor is available where selected critical workloads need runtime depth. Partners sell speed-to-visibility; we make that visibility operational. Closing the finding remains a customer-owner task.

Solution area	What the platform provides	What Avertory configures and runs
CSPM	2,500+ configuration controls; misconfiguration and compliance monitoring across AWS, Azure, GCP	Frameworks, alert routing, exception register, posture baseline
CWPP	Agentless workload inspection of VMs, containers, images, Kubernetes and serverless	Coverage confirmation, package / malware / secret findings triage
CIEM	Identity, role, permission and trust-path mapping; least-privilege context	Toxic-combination review and a privilege-reduction plan for customer IAM owners
DSPM	Sensitive data discovery in workloads and object storage (PII, credentials, secrets)	Data-at-risk backlog and owner mapping
Attack-path analysis	Crown-jewel context combining misconfig, identity and lateral movement	Prioritised 30 / 60 / 90-day plan for customer owners to execute
K8s / container / API	Cluster posture, image and API risk in cloud context	Scope, baselines and ticket workflows
Code & AI security	IaC, SCA, secrets in code; AI-SPM inventory of models, packages and shadow AI	Shift-left connectors and backlog into the same prioritisation programme
CDR & Sensor	Runtime detection plus optional Sensor on critical workloads	Detection routing and Sensor design where licensed
Compliance	Multi-cloud frameworks with scheduled reporting	UK-relevant packs (e.g. Cyber Essentials themes, ISO 27001, PCI) as licensed

ORCA-Deploy — Cloud onboarding and baseline

Connects the agreed cloud organisations, lets SideScanning build the inventory, sets the first posture baseline and puts alerts where the operating model needs them. No agents required for the core landing.

Best for	First Orca landing, additional cloud, or a rebuild after a neglected proof of concept.
Typical duration	Foundation 6 days (one cloud). Standard 10 days (up to three organisations / richer identity and ticketing). Enterprise scoped.
Maps to	Commercial pack ORC-FND / ORC-STD / ORC-ENT.
Customer outcome	Accounts connected, inventory live, baseline posture, alert routing, partner handover.

In scope

- Organisation and account design: AWS Organisations / Azure Management Groups / GCP folders as applicable.
- Least-privilege onboarding roles and connector health checks.
- SideScanning coverage confirmation across compute, storage, identity and Kubernetes in scope.
- Baseline posture: severity model, mute/exception rules, first compliance framework.
- Alert routing to Slack, email, SIEM or ticketing as licensed and agreed.
- Role design for the partner and the customer security / cloud teams.
- Optional Sensor design for a defined set of crown-jewel workloads.

Assumptions

- Cloud admin access is granted on time. Account lists are complete. GovCloud, China regions or air-gapped clouds are declared at scoping.

Out of scope

- Fixing findings, changing IAM or network configuration, or applying compensating controls. That work stays with customer cloud owners. Prioritising what they should fix first is ORCA-Remediate. Ongoing coverage is ORCA-Operate.

ORCA-Remediate — Risk prioritisation programme

Converts Orca's contextual risk view into a ranked programme the partner can run with the customer's cloud and application owners. Focus is toxic combinations and attack paths to crown jewels — not a 10,000-row CSV, and not Avertory making the change.

Best for	Estates that can see risk but lack an owned, ranked plan. Board or audit pressure. Pre-renewal value proof.
Typical duration	8–15 day design and first cycle, then a monthly cadence or handover to ORCA-Operate.
Customer outcome	Ranked backlog, named owners, 30 / 60 / 90-day plan, ticket workflow, exception register.
Boundary	Prioritisation, workflow and tracking only. Customer owners execute every cloud, identity and code change.

In scope

- Crown-jewel and business-context workshop with the partner and customer stakeholders.
- Attack-path and toxic-combination review across CSPM, CWPP, CIEM and DSPM findings.
- Prioritised backlog with owner, effort band and a suggested fix for the owner to apply (including IaC / code where licensed).
- Ticketing integration and SLA model the partner can report against.
- Exception and risk-acceptance process that will survive audit.
- Facilitation of planning sessions. We do not log on and change customer cloud accounts.

Out of scope

- Remediation or mitigation execution: security-group changes, IAM edits, encryption settings, secret rotation, image rebuilds, or any other production change.
- Acting as the customer's cloud operations or DevOps function.

Assumptions

- Cloud and application owners exist and will attend the working sessions. Residual risk after an accepted exception sits with the customer.

ORCA-Operate — Continuous CSPM / CWPP management

Keeps the CNAPP honest as accounts, subscriptions and AI services appear. Monthly certified capacity, partner-owned reporting, licence-expansion flags handed back to you. This is platform operations, not a managed remediation desk.

Best for	Multi-cloud estates, continuous compliance evidence, and partners who want a cloud-security line item.
Typical duration	LC-2 or LC-4 retainers. New-account onboarding inside the retained days or as a mini Deploy.
Customer outcome	Coverage integrity, posture trend, priority backlog, compliance pack, second-line on the platform.

Monthly rhythm

- Connector and coverage health. New account / subscription detection.
- Posture trend across CSPM, workload, identity and data-at-risk.
- Priority attack-path review and backlog refresh for customer owners.
- Compliance evidence pack aligned to the agreed frameworks.
- Code, IaC and AI-SPM findings where those modules are licensed.
- Partner reporting pack and recommended commercial next steps for you to own.

04

Lifecycle, overflow and packaging

Deploy SKUs create the landing. Operate / Manage SKUs keep the platform healthy. Capacity products underneath are defined in the commercial pack. None of them converts Avertory into a mitigation bench.

Capacity SKU	Commitment	How partners use it
LC-2 Lifecycle retainer	2 days / month	ORCA-Operate on a smaller estate
LC-4 Lifecycle retainer	4 days / month	Preferred mid-market cadence; room for second-line on the platform
HC-10 Hypercare	10 working days	Post go-live cover after Deploy; unused days can convert to retainer
OV-20E / OV-20S	20 prepaid hours	Short platform tasks and cover. Not incident response and not an unscoped Deploy

Suggested bundles partners can sell

Bundle	SKUs	Story you can tell
Orca value path	ORCA-Deploy + ORCA-Remediate + ORCA-Operate	See the estate, rank the risk, keep coverage honest. Owners close the items.

05

Delivery method

How an engagement runs

- Partner desk receives the opportunity. We confirm platform, SKU, envelope and brand model (white-label / co-delivery / named).
- Written assumptions and acceptance criteria before kick-off. No verbal start. The service boundary in section 1 is restated on every SOW.
- Named lead engineer, plan, access request and comms path agreed with you.
- Build against the SKU. Scope change is a change note you approve — not silence.
- Partner-branded handover pack: what was built, how the platform is operated, open risks for customer owners, licence flags for you.
- Optional hypercare, then Operate / Manage retainer if you sell it.

UK operating context

- Remote delivery in UK business hours is the default. On-site is scoped when the estate or the customer requires it.
- Work is framed against UK GDPR handling expectations, NCSC guidance themes and Cyber Essentials language where the customer cares about them. We supply evidence packs; we do not attest.
- Access is least-privilege and time-bound. Credentials are not retained beyond the engagement without a retainer.
- We do not run a generic multi-tool SOC and we do not run a mitigation or patching function. Depth is SentinelOne, Orca Security and Qualys platform delivery.

What success looks like

- Time-to-value: the platform is in production against the envelope, not stuck in a pilot.
- Stability after go-live: health, coverage and noise are inside agreed bounds.
- Partner CSAT: the account team can present the build and the monthly pack without translation.
- Commercial hygiene: expansion ideas come back to you, not around you.
- Clear ownership: every recommended fix has a customer owner. Avertory is not that owner.

06

Catalogue wording you can paste

Short descriptions for a price book or SOW. Replace [Partner] if you white-label. Do not edit these into a mitigation or remediation offer.

Orca Security

ORCA-Deploy — Agentless onboarding of Orca Security across the agreed cloud accounts, with SideScanning baseline, posture settings and alert routing. Delivered under [Partner]. Licensing remains on [Partner] paper.

ORCA-Remediate — Contextual risk prioritisation and a time-boxed programme across CSPM, CWPP, CIEM and DSPM findings, with named owners, tickets and an exception register. Delivered under [Partner]. Customer owners execute every change. Avertory does not remediate or mitigate.

ORCA-Operate — Continuous management of Orca Security CNAPP coverage, posture trend, attack-path backlog and compliance evidence. Sold by [Partner] as a monthly line item. Platform operations only.

07

Scoping notes that protect margin

- Fixed-price means a written envelope, not an open cheque. Endpoint count, cloud-account count, integration count, access and customer decision time are the usual moving parts.
- If those move, we issue a change note before extra work. That protects your margin as much as ours.
- Foundation and Standard assume remote UK-hours delivery and Implementation Engineer grade. Senior or Lead from day one is re-priced before you quote.
- We will not accept overflow hours that are actually an unscoped implementation, and we will not accept overflow that is actually mitigation or remediation execution.
- White-label does not change the technical scope or the service boundary. It changes the cover sheet, the reporting banner and who speaks.

Standard exclusions (all SKUs)

- Software licences, marketplace subscriptions and vendor support contracts.
- Mitigation and remediation execution of any kind — including patching, configuration hardening, IAM or network changes, secret rotation, image rebuilds, compensating controls, and live containment.
- Incident response, digital forensics, threat hunting retainers, or acting as the customer's SOC.
- Acting as the customer's IT operations, desktop, server, cloud-engineering or DevOps function.
- End-user first-line service desk, unless a retainer explicitly includes it.
- Legal, DPIA or audit opinions. We supply evidence packs; you or the customer own the attestation.
- Tools outside SentinelOne, Orca Security and Qualys, except as integration targets.

08

Brief the partner desk

Bring live opportunities, catalogue questions and volume discussions before the customer has already asked who will implement the platform.

We need	Why it matters
Platform and SKU	So the right certified engineer is assigned
Estate envelope	Endpoints, cloud accounts, or asset count — drives Foundation vs Standard vs scoped
Brand model	White-label, co-delivery or named partner
Target go-live and constraints	Change freezes, audit dates, co-term with the licence
Integrations required	Identity, ITSM, SIEM, cloud — decides whether Prioritise is in the first SOW
Purchase order or call-off	Work does not start on a verbal

This catalogue is indicative and does not form a contract. SKUs, assumptions and acceptance criteria are confirmed in the partner agreement and in each statement of work. Avertory Limited does not sell Orca Security licences. Avertory Limited does not provide mitigation or remediation execution. Those remain with the customer's operational owners, through the authorised partner.

Avertory Limited · Companies House 16542620 · 82a James Carter Road, Mildenhall, Bury St. Edmunds, IP28 7DE