AVERTORY

SERVICES CATALOGUE

SentinelOne

AVERTORY LIMITED

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

S1-Deploy	Fixed-price deployment
S1-Optimise	Policy, detection and configuration
S1-Integrate	SIEM, identity, ticketing, cloud
S1-Operate	Monthly platform 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	SentinelOne Singularity
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 S1-Deploy as the default attach to a new licence. Add Optimise, Integrate 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.

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

Four SKUs on SentinelOne. Deploy gets Singularity 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.

SentinelOne — Singularity XDR / SIEM / Identity / Cloud

SKU	Service	Typical duration	Attach when
S1-Deploy	Fixed-price deployment	8–12 days	New Singularity landing or rebuild
S1-Optimise	Policy, detection and configuration	5–10 days	Noise, gaps, or unused modules
S1-Integrate	SIEM, identity, ticketing, cloud	4–8 days	XDR / AI SIEM or workflow design
S1-Operate	Monthly platform management	2 or 4 days / month	Live estate that must stay sharp

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.

03

SentinelOne services

Platform reference: sentinelone.com. Avertory implements and operates the Singularity platform; we do not sell the licence and we do not act as the customer's responder.

Solution areas we service

Singularity is an AI-native platform covering endpoint, identity, cloud and security operations from one console, one agent family and one data layer. Partners typically land Endpoint first. The SKUs below also cover the modules that sit around it when the customer has licensed them. Autonomous containment, rollback and response actions are product capabilities we configure. Executing those actions in an incident remains with the customer's operating team.

Solution area	What the platform provides	What Avertory configures and runs
Endpoint security (EPP + EDR)	Static and behavioural AI, autonomous containment, rollback, device and firewall control	Agent rings, policy packs, exclusions, response-policy design, health and version control
Identity security (ITDR / ISPM / IdP)	Human and non-human identity threat detection; AD / Entra attack-path visibility	Connector design, identity policies, noisy-account hygiene, detection use-cases
Cloud workload security	CWS for servers and containers; CNAPP / cloud-native modules where licensed	Workload policy, Linux/K8s coverage, cloud connector alignment
AI SIEM / Data Lake	Correlation of native and third-party telemetry; OCSF-normalised lake	Source onboarding, parsers/use-cases, retention, investigation workflows
Purple AI & Hyperautomation	Natural-language investigation, triage and cross-surface response features	Playbook design and automation bounds. Customer owners approve any live action.
Exposure / Ranger / RemoteOps	Network discovery, suspicious-device isolation features, remote investigation tools	Discovery scope, auto-deploy rules, investigation runbooks
STAR detections	Custom IOC / behavioural rules mapped to MITRE ATT&CK	Environment-specific rules, testing, exception process

S1-Deploy — Fixed-price SentinelOne deployment

Gets Singularity into production with a change-safe agent rollout, a policy baseline the customer can live with, and a handover pack the partner can stand behind at QBR.

Best for	New licence landings, neglected default builds, or a controlled rebuild before renewal.
Typical duration	Foundation 8 days (up to 1,000 endpoints). Standard 12 days (up to 5,000). Enterprise scoped.
Maps to	Commercial pack S1-FND / S1-STD / S1-ENT.
Customer outcome	Agents on the agreed estate, policies live, console hardened, two agreed integrations, knowledge transfer.

In scope

- Discovery workshop: estate, outcome, change windows, exclusion candidates, success criteria.
- Console hardening: roles, SSO, MFA, site/group design, notification and audit settings.
- Policy design: prevention, detection, response, device control and firewall aligned to risk appetite.
- Phased agent rollout plan for Windows, macOS and Linux workstations and servers, with rings and rollback points.
- Health monitoring, upgrade cadence and first-week hypercare within the envelope.
- Up to two standard integrations in Foundation; identity / email / cloud connector set in Standard.
- Partner-branded build record, operating notes and knowledge-transfer session.

Assumptions

- Licensing, tenant and support entitlement sit with the partner. Local admin or equivalent is available for agents.
- Change approval is timely. Endpoints are reachable. Legacy or air-gapped pockets are called out before kick-off.

Out of scope unless added

- Purple-team style detection engineering, full AI SIEM use-case design, complex multi-forest identity — those sit in S1-Optimise, S1-Integrate or S1-ENT.
- Incident response retainers, threat hunting as a managed service, or executing containment / rollback during a live incident.

S1-Optimise — Policy, detection and configuration optimisation

Turns a default or noisy Singularity estate into a tuned operating platform. Used after a third-party build, after a year of drift, or when the customer has licensed modules that were never switched on properly.

Best for	High false-positive load, unused Identity / Cloud / Ranger modules, pre-renewal health checks.
Typical duration	5–10 days, or a defined optimisation sprint inside a retainer.
Customer outcome	Quieter console, documented detections, exception process, and a backlog the partner can present.

In scope

- Policy and exclusion review against current risk appetite and change history.
- Detection quality: STAR rules, threat-intelligence sources, MITRE coverage gaps.
- Identity posture where ITDR / ISPM / IdP modules are licensed.
- Cloud workload and container policy where CWS is licensed.
- Purple AI investigation patterns and analyst notes the partner can reuse.
- Upgrade and feature-adoption plan so the customer uses what they already pay for.

Out of scope unless added

- Standing SOC analyst coverage, live incident handling, or new product licences. We will consume red-team results; we do not run the exercise.

S1-Integrate — SIEM, identity, ticketing and cloud integrations

Connects Singularity to the rest of the customer stack so detections become tickets, identity context flows, and telemetry lands where the operating model needs it.

Best for	XDR programmes, AI SIEM landings, ServiceNow / Jira operating models, Entra / AD identity context.
Typical duration	4–8 days depending on source count and whether AI SIEM ingest is in play.
Customer outcome	Documented integration map, working connectors, tested response paths, support runbook.

Typical integration catalogue

- Identity: Microsoft Entra ID, Active Directory, identity-provider signals into Singularity Identity.
- Ticketing and ITSM: ServiceNow, Jira and equivalent webhook / API workflows.
- Email and collaboration signals where licensed connectors exist.
- Cloud: AWS, Azure and GCP connectors; Cloud Funnel streaming where licensed.
- AI SIEM / Data Lake: third-party source onboarding, normalisation and priority use-cases.
- Hyperautomation: bounded playbooks. Live actions stay under customer change control.

Assumptions

- The customer or partner supplies API credentials, connector licences and a named owner on each target system.
- Custom parser engineering beyond vendor-supported sources is estimated separately.

S1-Operate — Monthly platform management

Certified monthly capacity against the live Singularity estate. Sold by the partner as a line item. Reporting packs are written for the partner to present — we do not build a parallel customer-success brand, and we do not become the customer's SOC.

Best for	Any live estate where the partner wants to own renewal quality without hiring a Singularity engineer.
Typical duration	LC-2 (2 days / month) or LC-4 (4 days / month). Overflow blocks available.
Customer outcome	Health, detection quality, version posture and a monthly pack the partner presents at QBR.

Monthly rhythm

- Console and agent health, version drift, failed upgrades and isolated devices.
- Detection and prevention review: noise, missed coverage, new STAR candidates.
- Policy and exception hygiene. Identity and cloud connector health where in scope.
- Second-line platform support within the retained days — configuration and investigation guidance, not incident command.
- Partner reporting pack: status, risk themes, recommended actions for customer owners, licence-expansion flags handed back to you.

Minimum two days a month. Unused hypercare days can convert to retainer by agreement.

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	S1-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
S1 Landing + Care	S1-Deploy + S1-Operate (LC-2)	Live in production this quarter; tuned every month.
S1 XDR programme	S1-Deploy + S1-Integrate + S1-Optimise	Endpoint plus identity, ticketing and SIEM use-cases.

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.

SentinelOne

S1-Deploy — Deployment and configuration of SentinelOne Singularity, including agent rollout planning, policy design, console hardening and agreed integrations. Delivered under [Partner] by platform-certified engineers. Licensing remains on [Partner] paper. Does not include incident response or remediation execution.

S1-Optimise — Policy, detection and configuration optimisation of a live Singularity estate, including custom detections, exclusion hygiene and adoption of licensed identity or cloud modules. Delivered under [Partner]. Does not include managed SOC or live incident handling.

S1-Integrate — Design and build of Singularity integrations spanning identity, ticketing, cloud connectors and AI SIEM / data-lake sources. Delivered under [Partner].

S1-Operate — Monthly certified management of the live SentinelOne estate: health, tuning, detection quality and a reporting pack presented by [Partner]. Minimum two days a month. Platform operations only — not mitigation or incident command.

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 Integrate 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 SentinelOne 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