AVERTORY

SERVICES CATALOGUE

Qualys

AVERTORY LIMITED

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

QUALYS-Deploy	VMDR deployment
QUALYS-Discover	Asset discovery and baseline
QUALYS-Manage	Continuous vulnerability management
QUALYS-Remediate	Remediation tracking

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	Qualys Enterprise TruRisk
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 QUALYS-Deploy as the default attach to a new licence. Add Discover, Track or Manage 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 QUALYS-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

Four SKUs on Qualys. Deploy gets VMDR 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.

Qualys — Vulnerability Management as a Service

SKU	Service	Typical duration	Attach when
QUALYS-Deploy	VMDR deployment	8–12 days	New VMDR or agent/scanner rebuild
QUALYS-Discover	Asset discovery and baseline	5–8 days	Unknown estate, M&A, EASM need
QUALYS-Manage	Continuous vulnerability management	2 or 4 days / month	Ongoing TruRisk operating rhythm
QUALYS-Remediate	Remediation tracking	5 days + cadence	SLA visibility and exception control

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.

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

03

Qualys services

Platform reference: qualys.com. Avertory designs and runs Qualys as Vulnerability Management as a Service — meaning we operate the platform. We do not patch, harden or otherwise remediate the estate.

Solution areas we service

Qualys is delivered on the Enterprise TruRisk Platform. Most partner deals start with VMDR. Asset visibility (CSAM / EASM) and a managed tracking loop are what turn a scanner into an operating service. Adjacent modules are configured when the customer has licensed them. Patch Management, if licensed, is configured as a tool for the customer's IT owners — Avertory does not apply patches.

Solution area	What the platform provides	What Avertory configures and runs
VMDR	Discover, assess, prioritise and respond to vulnerabilities with TruRisk scoring	Agents, scanners, authenticated scans, tagging, SLA views, dashboards
CSAM + EASM	Internal and internet-facing asset inventory, criticality, security-tool coverage	Discovery design, unmanaged-asset process, CMDB alignment
TruRisk / ETM	Unified risk across Qualys and third-party findings; board-level risk view	Risk model, source onboarding, reporting the findings; partner presents
Patch Management (PM)	A platform the customer's IT owners can use to deploy patches	Ring design and window templates only. We do not push patches.
Policy Compliance / FIM	Configuration baselines and file-integrity monitoring	Policy packs, evidence for audit, drift reporting
WAS / TotalAppSec	Web application and API discovery and DAST-style testing	App inventory, scan cadence, ticket workflow
TotalCloud CNAPP	Cloud / container posture, CWP, CDR, IaC and SSPM modules	Connectors, cloud assessment cadence, priority backlog
Container Security	Build-to-runtime container and image security	Registry / pipeline connectors and runtime coverage
CAR / custom assessment	Custom checks and response actions on Cloud Agent	Use-case design where licensed. Customer owners execute any action.

QUALYS-Deploy — VMDR deployment

Designs the Qualys landing: Cloud Agents, scanner appliances, cloud connectors, authenticated assessment and the first TruRisk-ranked view. This is the SKU partners attach to a VMDR transaction.

Best for	New VMDR, a scanner-only estate that needs agents, or a rebuild before an audit or renewal.
Typical duration	8–12 days for a mid-market hybrid estate. Enterprise scoped for OT, multi-tenant MSSP or global scanner farms.
Maps to	Commercial pack Qualys VMaaS Foundation / Standard / Enterprise envelopes.
Customer outcome	Sensors deployed, first authenticated cycle complete, asset groups live, partner handover.

In scope

- Architecture: Cloud Agent vs scanner appliance vs passive / cloud connector mix.
- Agent deployment plan (Windows, Linux, macOS) including packaging for partner or customer distribution tools.
- Virtual scanner placement, network paths and authenticated scanning credentials — handled under agreed secret-management rules.
- Cloud connectors for AWS, Azure and GCP where in scope.
- Asset tagging, grouping, business criticality and RBAC.
- First full and authenticated assessment cycle, with TruRisk baseline.
- Dashboard and reporting pack designed for the partner to present.
- Knowledge transfer and operating notes.

Assumptions

- Scanner network paths and credential owners are identified at kick-off. OT / isolated networks are declared. Agent distribution tooling exists or is agreed.

Out of scope unless added

- Full CSAM / EASM programme (QUALYS-Discover). Standing scan operations (QUALYS-Manage). Closure tracking (QUALYS-Remediate). Patch execution is never in scope.

QUALYS-Discover — Asset discovery and baseline

Closes the ‘we do not know what we have’ gap. Uses CSAM, EASM and native Qualys sensors so VMDR is scoring a real estate rather than a partial CMDB.

Best for	M&A, sprawling hybrid estates, internet-facing unknown assets, pre-Cyber Essentials or audit preparation.
Typical duration	5–8 days for the discovery design and first baseline. Larger attack surfaces scoped.
Customer outcome	Authoritative inventory, unmanaged-asset process, criticality tags, EASM view of internet-facing exposure.

In scope

- Discovery design across Cloud Agent, scanner, cloud connector and EASM sensors.
- Reconciliation against the customer CMDB or asset register, with a gap register.
- Unmanaged, EOL and missing-control identification (no EDR, no agent, no owner).
- Internet-facing asset review via EASM where licensed.
- Certificate inventory review where CRI is licensed.
- Tagging and criticality model that VMDR, WAS and TotalCloud can inherit.
- Partner-ready baseline report: what exists, what is unknown, what owners should address first.

Assumptions

- CSAM / EASM modules are licensed, or we limit discovery to VMDR-native sensors and say so in the SOW.

QUALYS-Manage — Continuous vulnerability management

The operating service. Scan cadence, TruRisk movement, coverage integrity and a reporting pack the partner takes to the customer. This is VMaaS in the sense partners mean it — we run the Qualys platform, we do not remediate the hosts.

Best for	Any live VMDR estate. Strong attach after QUALYS-Deploy. Pairs with QUALYS-Remediate when SLA visibility matters.
Typical duration	LC-2 or LC-4 retainers. Extra modules (WAS, PC, TotalCloud) add scoped days.
Customer outcome	Predictable scan rhythm, coverage above the agreed threshold, TruRisk trend, partner monthly pack.

Monthly rhythm

- Sensor health: agent version, scanner status, failed authentications, coverage gaps.
- Assessment cadence: unauthenticated and authenticated cycles on the agreed scope.
- TruRisk movement, exploitable-vuln focus and new-threat visibility inside retained days.
- Policy Compliance evidence where PC is licensed.
- WAS / TotalCloud / Container cadence where those modules are in the retainer.
- Partner reporting pack aligned to Cyber Essentials themes, ISO 27001 evidence or board TruRisk — whichever you sell.
- Licence and module-expansion flags handed back to you. We do not open that conversation with the customer.

QUALYS-Remediate

Remediation tracking

Makes vulnerability data visible as owned work. Owners, SLAs, exceptions and — where Patch Management is licensed — ring and window templates for the customer's IT team. Avertory tracks and reports. The customer's operational owners make every change.

Best for	Audit findings that never close, SLA commitments in an MSA, or partners selling visibility of closure — not partners selling Avertory as the patching team.
Typical duration	5-day design plus monthly cadence, often combined with QUALYS-Manage.
Customer outcome	Owned backlog, SLA performance view, exception register, evidence pack.
Boundary	Tracking and reporting only. No patch execution, no configuration hardening, no compensating-control implementation.

In scope

- Remediation SLA model by TruRisk / severity / asset criticality — as a reporting framework.
- Owner mapping and ticket integration (ServiceNow, Jira or partner PSA).
- Exception and risk-acceptance workflow with review dates.
- Patch Management ring and maintenance-window templates where PM is licensed. Templates only.
- Facilitation of planning reviews. Evidence pack suitable for internal audit, Cyber Essentials Plus-style scrutiny or customer QBR.

Out of scope

- Applying patches, changing configuration, rebuilding images, or any other mitigation / remediation execution.
- Acting as the customer's IT operations, desktop, server or cloud-engineering function.

Assumptions

- There is a named operational owner on the customer side for every class of change. Residual risk on accepted exceptions sits with the customer.

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	QUALYS-Manage 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
Qualys VMaaS	QUALYS-Deploy + QUALYS-Discover + QUALYS-Manage + QUALYS-Remediate	Know the estate, scan it, track whether owners closed it.

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.

Qualys

QUALYS-Deploy — Design and deployment of Qualys VMDR sensors (Cloud Agents, scanners and cloud connectors), authenticated assessment and the first TruRisk baseline. Delivered under [Partner] as Vulnerability Management as a Service (platform operation). Licensing remains on [Partner] paper.

QUALYS-Discover — Asset discovery and baseline using Qualys CSAM / EASM and native sensors, with CMDB reconciliation and an unmanaged-asset process. Delivered under [Partner].

QUALYS-Manage — Continuous operation of Qualys: scan cadence, coverage integrity, TruRisk trend and a reporting pack presented by [Partner]. Does not include patching or other remediation execution.

QUALYS-Remediate — Remediation tracking against agreed SLAs, with owner mapping, exceptions and Patch Management templates where licensed. Delivered under [Partner]. Tracking and reporting only — Avertory does not apply patches or implement fixes.

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 Track 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 Qualys 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