TECHNICAL DATA SHEET / R5

CLAWOLF AS-OS

Autonomous Security Operating System
AI runtime governance, trust and security for enterprise operations.

AS-OS connects detection, investigation, decision, authorized action, independent verification and learning in a governed operational runtime. It gives security teams an accountable path from an observation to a decision and its actual outcome, while preserving customer policy, tenant boundaries and human oversight.

DETECTION	DECISION	ACTION	CONTROL	LEARNING

At a glance	Technical profile
Architecture	Five orchestration layers; eight runtime systems on a Governed Runtime Kernel. Investigation is a cross-layer capability.
Decision method	21 versioned deterministic evaluators with attributable inputs, risk, confidence, uncertainty and explainability.
Execution model	Policy-bound intents, explicit approval obligations, scoped executor bindings, action receipts and outcome verification.
Deployment	Air-gapped on-premises; connected on-premises; VMware Kubernetes private cloud; customer-account AWS EKS, Azure AKS and Google GKE.
Adoption	Starter, Core and Governance are independently licensed packages. Specialist add-ons extend selected capabilities.
Evaluation	R5 delivery-package evidence and technical assurance materials are available for review. Customer activation is a separate acceptance step.

Reader map: architecture 2 | intelligence 3 | decisions 4 | governance 5 | evidence 6 | validation 7 | deployment 8 | integration 9 | security 10 | operations 11 | packaging and evaluation 12.

01 / ARCHITECTURE

A governed operational runtime

Five layers describe responsibility. The runtime systems provide the technical services used across that lifecycle.

Layer	Operational function	Retained output
Detection	Normalize source observations and produce attributable signals.	DetectionSignal and source provenance.
Decision	Correlate context, investigate, assess risk and select a bounded response.	DecisionBundle, evidence graph and evaluator contributions.
Action	Prepare permitted execution intents and dispatch through enrolled bindings.	ExecutionIntent and ActionReceipt, or a recorded block.
Control	Apply policy and human obligations before dispatch; verify effects and govern recovery afterward.	ControlVerdict, approvals and VerificationResult.
Learning	Retain verified outcomes, recurrence and revalidation context for later decisions.	LearningEvent and linked revisions.

Eight AS-OS Runtime Systems	Role
Telemetry & Data Fabric	Attributable observations, normalization and data provenance.
Domain Intelligence Layer	Organization, sector, jurisdiction and business constraints.
Autonomous Decision Engine	Deterministic evaluation, risk and decision packages.
Decision DNA	Revisioned lineage linking context, authority, action and outcome.
Autonomous Trust Engine	Policy, entitlement, human obligations and execution authority.
Autonomous Validation Fabric	Isolated analysis and independent validation evidence.
Continuous VulnOps	Exposure-to-remediation, verification and recurrence lifecycle.
Autonomous Customer Deployment	Placement, enrollment, configuration and lifecycle readiness.

From observations to context

Preserve the source of a finding, the business conditions that constrain it and the evidence an analyst needs to investigate.

Capability	Technical behavior	Enterprise contribution
Source provenance	Retain tenant/run identity, source references, hashes, time ranges and normalization/detector versions.	Make findings reproducible and distinguish source evidence from replay or evaluation labels.
Evidence correlation	Link observations, assets, identities and case context in an evidence graph.	Review why several observations belong to the same decision.
Business applicability	Use organization facts such as sector, jurisdiction, regulated activity and deployment context.	Apply relevant constraints instead of treating every customer as the same environment.
Risk and confidence	Retain the basis for risk, confidence, uncertainty and contributing evaluations.	Expose missing or conflicting evidence before a consequential action.
Investigation workflow	Provide root cause, timeline, related assets/identities, attack paths, findings and recommended next actions.	Give analysts an actionable investigation package, linked to the same case.
Sector context	Relate applicable requirements and customer policy to runtime decisions.	Connect technical risk to institutional operating obligations.

Analyst deliverables

Decision and investigation packages retain summaries, confidence, evidence references, reasoning, recommended actions, alternatives and audit references. The Runtime Proof Dossier connects these outputs to the trace, receipt, verification and integrity records.

A catalog entry is not a certified control. Applicability, source-content readiness and actual runtime enforcement are separate. Missing facts and unavailable sources remain explicit.

03 / DECISION INTELLIGENCE

Explainable decisions with bounded authority

The Autonomous Decision Engine uses versioned deterministic evaluators. Optional AI-assisted reasoning does not grant execution permission.

Evaluation coverage	Included evaluator domains
Threat and infrastructure	DDoS, Web, Endpoint, Network, Identity, Email, Cloud, Database, API and DLP.
Advanced risk	Ransomware, Supply Chain, Zero-Day, OT/ICS Safety, Mobile and Physical.
Cross-domain assessment	Governance, Insider Threat, Adversarial AI and Kill Chain.
Runtime assessment	Brain Latency is a meta-evaluator, not a separate threat domain.

Decision property	Technical specification
Per-evaluator evidence	Evaluator identity/version, attributable inputs, verdict, confidence and evidence references.
Aggregation	Applicable contributions and double-counting controls; non-actionable/not-applicable votes are excluded from the actionable denominator.
Quorum	Configured threshold evaluated against actionable verdicts; a passing quorum is evidence, not permission to dispatch.
Uncertainty	Disagreement and evidence gaps remain visible and may require human review.
Explainability	Risk decomposition, contributing evaluators, selected/rejected alternatives and formula versions are retained.
Decision package	Context snapshot, evidence graph, investigation references, recommended actions and audit lineage.

Customer-controlled reasoning

External reasoning is disabled by default in the common distributions. Optional use requires customer-owned credentials in the tenant vault and explicitly approved egress. The customer contracts with and pays its AI provider; provider consumption is separate from the software licence.

04 / GOVERNANCE & RESPONSE

Authorization before action. Proof after action.

The Autonomous Trust Engine keeps identity, policy, entitlement, approvals and observed results distinct.

Control	Behavior
Authority separation	Surface visibility, purchased licensing, active entitlement and permission for an exact action are independently evaluated.
Policy verdict	Allow, deny or require human review; bind the verdict to the intent, tenant and current policy context.
Operating controls	Observation, Alert, Human-in-the-Loop and Full Autonomous contexts retain mandatory policy and approval gates.
Human approval	Approval satisfies a specific obligation. It does not create an action receipt or prove containment.
Protected targets	Target scope, action taxonomy, readiness and other mandatory constraints remain effective at dispatch.
Outcome verification	Evaluate resulting state through the configured verification path; unavailable or failed checks remain unresolved.
Recovery	Govern supported rollback or compensation separately; preserve failure and authorization evidence.

HITL preset	Incident severities requiring human approval
Low	Low, Medium, High and Critical.
Medium	Medium, High and Critical.
High	High and Critical.
Critical	Critical.

Failure semantics

Awaiting approval pauses without dispatch. Blocked and failed paths retain the cause, failing stage and available evidence. A completed runtime may represent a safe block or a workflow without an executed action; terminal artifacts determine what actually happened.

05 / EVIDENCE & LEARNING

Decision DNA and operational proof

Retain one traceable chain from context and intent through approval, execution, verification and later revalidation.

CONTEXT	AUTHORITY	ACTION	EFFECT	LINEAGE

Record	Technical contents and purpose
Decision DNA	Revisioned aggregate with tenant/run/decision identity, sequence, previous hash and current hash.
Context and reasoning	Context snapshot, evidence pack, policy record, logic-core outputs, confidence and trust assessment.
Human decision	Approval/rejection, relevant obligation and actor context, linked to the exact intent and revision.
Execution and outcome	Intent, receipt, verification, rollback record and unresolved effects.
Runtime Proof Dossier	Decision/investigation packages with trace, action receipts, verification and integrity references.
Forensic evidence	Evidence-chain and audit-sealing/integrity functions within their declared verification scope.
Learning revision	Observed outcome, revalidation, recurrence and later decision context; no automatic expansion of authority.

Operator experience

Dashboard activity, the HITL workspace, Mission Workspace, evidence reports and timelines refer to canonical run and artifact identities. A selected tenant or browser label cannot substitute for server-side authorization.

Evidence interpretation

A receipt shows that an executor returned a result. Independent state evidence establishes whether the intended effect held. Verification of a seal establishes integrity of the sealed record; it does not prove every underlying assertion or legal conclusion.

Learning feedback cannot grant a licence, remove a human-approval obligation or make an unsupported control available. Retention and export remain subject to the customer installation and policy.

06 / VALIDATION & EXPOSURE

Validation Fabric and Continuous VulnOps

Bring isolated analysis, response verification and recurrence into the operational lifecycle.

Validation element	Technical scope
Routing domains	Malware, Phishing, Email, Cloud, Network, Identity, Document, Container, Mobile, Script, Web Application and IoT.
Parse profile	Artifact parsing and memory/container inspection within supported workers and formats.
Execute profile	Isolated behavioral and malware execution; requires enrolled machinery and supported isolation.
Network Emulate	Disposable, bounded-network scenarios; not unrestricted access to the customer network.
Admission and evidence	Authorized job, signed ticket, isolated worker and evidence readback. Results include failed or unavailable.
Analysis topology	Separate controller, guest and parser components accompany the application payload; isolate analysis from durable operational data.

Continuous VulnOps stage	Operational result
Ingest and correlate	Normalize a finding and associate asset, exposure and business context.
Validate and decide	Assess exploitability, retain independent evidence and form a remediation decision.
Authorize and execute	Apply required approval and dispatch only the supported, scoped target action.
Verify and recover	Observe remediation; retain unresolved/failed outcomes and supported compensation.
Revalidate and learn	Schedule later checks, identify recurrence and retain operational feedback.

Twelve validation domains are a routing taxonomy, not a promise that every artifact or target supports all three execution profiles. OpenShift is not included in the R5 common distributions; unsupported isolation must not be bypassed.

07 / DEPLOYMENT

Customer-controlled placement

Four deployment choices use two logistics paths. Kubernetes is the application deployment substrate; the customer retains infrastructure and data custody.

Deployment choice	Target environment	Delivery path
Air-gapped on-premises	Customer-owned isolated Kubernetes; no external reasoning or public service dependency for the delivered operating path.	Separate signed R5 air-gap package.
Connected on-premises	Customer-owned Kubernetes with outbound access disabled by default; approved optional reasoning can be enabled.	R5 Common Distributions archive.
Private cloud	Customer-managed upstream Kubernetes on VMware infrastructure.	Same common payload; VMware Kubernetes profile.
BYOC	Kubernetes in the customer AWS, Azure or Google Cloud account: EKS, AKS or GKE.	Same common payload; provider-specific inputs/profile.

Property	Specification / boundary
Runtime artifact	Compiled Linux/amd64 application delivered as a digest-pinned OCI layout, plus required analysis payloads.
Installation	Profile list, validate, render, preflight, install and verify operations through the delivered distribution entry point.
Configuration	Typed customer inputs; credential values stay out of exported JSON and rendered values. Supply Secret references/private custody paths.
Egress	Default deny; explicit DNS plus bounded address/port rules for approved destinations. Reasoning remains disabled until correctly configured.
Ownership	BYOC does not mean a CLAWOLF-hosted service or a required central vendor control plane.

Profiles do not constitute AWS/Azure/GCP, VMware or OpenShift certification, Marketplace listing or automatic cross-cloud failover. Provider, region, runtime, CNI/CSI and version eligibility are checked for the selected customer installation.

Connect to the existing security estate

Separate source collection, runtime analysis, action execution and governance-policy import. A connector name alone does not establish all four.

Interface	Technical contract	Boundary
Source enrollment	Customer-owned source identity, endpoint, schema, version, credential reference, scopes and approved network path.	An enrolled configuration is not evidence of telemetry arrival.
Splunk passive intake	Supported Search v2 export via a read-only management REST token; bounded read of up to 20 events from the last five minutes.	HEC tokens do not authenticate search. This receipt does not prove continuous scheduled collection.
Authenticated HTTPS push	Tenant-bound delivery envelope and matching enrolled method/schema at the log-ingestion endpoint.	HTTPS receipt does not prove a syslog listener, Kafka service or native sensor coverage.
Governance Export v1	Explicit compatible HTTPS baseline-export service; bearer vault credential, verified TLS, bounded response and source digest.	A normal SIEM endpoint does not implement governance export automatically.
Runtime API	Canonical admission retains tenant, workflow, mode, binding and required terminal artifacts.	A successful HTTP request alone is not successful response execution.
AIS native contribution	AI-domain findings and evidence inform institutional decision/response; single assigned authority and executor per action.	AIS remains independently deployable and separately licensed; its release status is distinct.

Integration security

Enrolled endpoints and credentials are tenant scoped. Network policy, TLS validation, endpoint restrictions and current configuration identities apply to collection. A credential or source revision can invalidate earlier observations and pending approvals.

Validate the exact connector version and read/write contract during deployment. No blanket native compatibility with every SIEM, SOAR, EDR, cloud or identity product is implied.

Custody, identity and lifecycle

Customer installation choices define data placement and operator responsibility. The delivery media contains no shared customer credential or manufacturer private key.

Security area	Technical behavior / deployment requirement
Tenant isolation	Resolve tenant and role server side for requests, database transactions, jobs, approvals, reports and evidence.
Operator identity	Named customer/reseller identities with MFA at protected configuration and lifecycle boundaries; reseller authority differs from customer administration.
Database authority	Separate short-lived installation/migration identity from the least-privilege runtime identity. Runtime has no superuser or RLS bypass authority.
Secret custody	Configure runtime secrets, TLS keys and source credentials through customer-approved custody. Export configuration references, not secret values.
Persistent encryption keys	Preserve separate session and persistent-data key lifecycles; historical MFA/vault/evidence readers require the appropriate retained key material.
Retention and hold	Installation policy defines retained data, evidence, backup targets and legal-hold responsibility. Disposition must respect those decisions and its verified scope.
Transport and trust	Customer DNS, certificates, CA trust and internal ingress are installation inputs; certificate rotation is an operational responsibility.
Integrity	Use checksums, supplied Cosign public-key verification, image digests and the delivered provenance/SBOM records.

Regional policy context

Organization and jurisdiction facts can inform applicable policy and operational constraints across US, EU, Middle East/GCC and Türkiye contexts. Catalog visibility or framework mapping is not certification, legal advice or proof that every required control is implemented and effective.

The customer determines its approved storage locations, retention, backup and disposal policy. Data residency is a configured and verified installation property, not an automatic consequence of choosing a cloud region.

Deploy, observe and recover deliberately

Size and qualify the exact customer workload. Asset count alone cannot determine storage, analysis concurrency or a recovery objective.

Technical requirement	R5 package profile
Architecture / substrate	Linux/amd64 Kubernetes; the packaged factory reference is Kubernetes 1.36. A historical chart minimum is not compatibility certification.
Database	External PostgreSQL 16 or the exact compatible application-contract version; DBA preparation includes btree_gist and role separation.
Storage	Customer-approved StorageClass and backup target. RWX support is required for the delivered shared-volume topology when replicaCount exceeds one.
Queue / cache	The delivered profile uses the supported PostgreSQL job queue. Redis is not a required production dependency.
Ingress / network	Customer-managed ingress or gateway, DNS and TLS; explicit internal DNS/database destinations and approved source/action paths.
Analysis capacity	Separate capacity for enrolled analysis controller/guest/parser and selected AVF execution profiles.
Monitoring	Configure customer monitoring endpoints, retention, alerts and operational ownership; distinguish reachability from capability readiness.
Sizing inputs	Source/event volume, peak burst, analysis mix, concurrent jobs, evidence size/retention, replica topology and backup/recovery requirements.

Resilience and lifecycle

The package includes backup/restore, upgrade/rollback, data-key transition, incident-evidence export and troubleshooting guidance. Governance, signed release-bundle, entitlement and approval checks continue to apply to lifecycle actions.

Service objectives

Measure throughput, latency, concurrency, endurance, RPO, RTO and availability for the selected topology/workload. No universal throughput figure or automatic 99.9% SLA is supplied.

Multi-cloud installation does not automatically provide replication or disaster recovery. Configure and test those responsibilities for the selected deployment.

Technical adoption and procurement

Select the capability domains required by the customer. Licence entitlement never substitutes for execution authority.

Package / extension	Included scope
Starter	Decision and Investigation: 9 functions covering analysis, workflow, correlation, risk/confidence, explainability, sector context and analyst/audit evidence.
Core	Detection and Action: 10 functions covering native detection, signal production, orchestration, planning, intents, bounded execution, receipts, response, trace and reporting.
Governance	Control and Learning: 12 functions covering policy, verdicts, HITL, quorum, independent verification, rollback, VulnOps, recurrence, learning and proof integrity.
Autonomous Customer Deployment	Mandatory attachment to a non-empty base-package selection; placement, enrollment and lifecycle configuration.
Specialist add-ons	Domain Intelligence Advanced; Autonomous Validation Fabric Advanced; Continuous VulnOps Exposure Chain.
Suites	Intelligence Assurance: Domain Intelligence Advanced + AVF Advanced. Autonomous Exposure Defense: those two plus VulnOps Exposure Chain.

Offline commercial transition

An air-gapped customer can export an installation/customer-bound activation request. CLAWOLF owner purchase approval and signature produce a licence artifact that is applied to the same installation. Resellers do not issue production licences; PoC-to-production does not require a second installation or a database replacement.

Delivery and assurance materials

The applicable package supplies application/analysis OCI payloads, deployment charts, customer-input contracts, integrity/signature tools, SBOM/scan records and operating guides. Enterprise Validation, Security Assurance and Operational Resilience reports can be reviewed with their exact-version scope and exceptions.

Technical profile: October 2026 / R5. Package acceptance, production deployment observations and full customer-environment acceptance are separate. No broad third-party certification or guaranteed threat-detection rate is asserted. Contact enterprise@clawolf.com for the current release scope, bill of materials and evaluation plan.