CLAWOLF
ART OF GOVERNED AUTONOMY

CLAWOLF CHANNEL ALLIANCE

Autonomous Security Operations And AI Protection

CLAWOLF



YOUR NEXT GROWTH CHAPTER

Build With A Partner Focused On Governed Autonomy

A security company and product roadmap for partners who want a wider enterprise conversation.

A Security Company Built Around Governed Autonomy

CLAWOLF Inc. is a Delaware C-Corp incorporated in April 2026, built on security research that began in September 2024.

We develop autonomous security operations for cloud, on-premises and hybrid enterprises. AS-OS connects security decisions to authorized response, with human oversight and evidence of the outcome.

NIST GUIDANCE

26 FEB 2024
Cybersecurity Framework 2.0
Final framework. Introduces GOVERN.

26 JUL 2024
Generative AI Profile
NIST AI 600-1. Final publication.

16 DEC 2025
Cyber AI Profile
Initial preliminary draft.

5 FEB 2026
AI Agent Identity & Authorization
Concept paper. Initial public draft.

7 APR 2026
Trustworthy AI in Critical Infrastructure
Concept note. Profile development.

CLAWOLF MILESTONES

SEP 2024
Foundational Research
Security architecture research begins.

JUL 2025
Architecture Planning
Autonomy defines the operating approach.

OCT 2025
Runtime Kernel Architecture
Five-layer operating lifecycle.

JAN 2026
Multi-Pipeline & 21 Logic Cores
Specialist analysis and decision context.

FEB–APR 2026
Context, VulnOps & Incorporation
CLAWOLF becomes a Delaware C-Corp.

Parallel chronology only. NIST does not endorse or certify CLAWOLF.

EXPAND YOUR INSTALLED-BASE OPPORTUNITY

Grow Beyond Point-Product Sales

An operating layer opens new modernization, integration and managed-service conversations around existing security investments.

AS-OS coordinates security analysis and response across connected threat-domain products, SIEM and SOAR tools and your SOC workflows. Your team sets the authority. The operating layer connects the evidence, the decision, the permitted action and its recorded result.

YOUR ORGANIZATION — Policy, protected assets and human approval boundaries

CLAWOLF AS-OS
Governed Operating Layer

Detection	Decision	Action	Control	Learning
Connect the evidence	Assess the business risk	Execute within authority	Check policy and effects	Retain outcomes

CONNECTED SECURITY ESTATE — **Threat-Domain Products / SIEM / SOC Workflows / SOAR**

Supported integrations and authorized actions only. Existing products retain their native controls.

TURN PRODUCT CAPABILITY INTO CUSTOMER VALUE

Sell Outcomes Your Customers Can Trust

Connect business risk, controlled response and reviewable outcomes. Give your team a stronger value-led sales conversation.

UNDERSTAND THE RISK

What Matters To This Business?

A suspicious login may threaten a critical service. Relate the evidence to asset importance, sector context and your policy.

Your team sees why a finding deserves attention.

CONTROL THE RESPONSE

What May The System Do?

Use operating modes, approval thresholds and protected targets to define the permitted response.

Your team retains an explicit boundary around autonomy.

REVIEW THE OUTCOME

What Actually Happened?

Follow the selected run, its decisions and recorded outcomes. Review missing evidence before closure.

Your team can explain the result and the remaining gaps.

A connected customer-value story: business context, bounded action and reviewable outcomes.

YOUR COMPETITIVE SALES FOUNDATION

Win On Intelligence. Defend Your Value.

Business context, 21 specialist logic cores, independent validation and Decision DNA give your team more than an automation pitch.

Domain Intelligence Layer

98 Instruments

US / EU / TR / ME / GCC

Used in the Decision layer. Organization, sector and regulatory context informs specialist analysis and remains in the recorded decision for review.

Autonomous Decision Engine

21 Logic Cores

Threat-Domain Analysis

Specialist cores assess domains such as identity, network, cloud and adversarial AI. Evidence-weighted verdicts support consensus, abstention or human review.

Autonomous Validation Fabric

12 Validation Domains

Forensic Sandbox Mesh

A sandbox mesh spans malware, identity, cloud, network and more. Supported checks validate evidence and effects. Unavailable checks remain explicit.

Decision DNA

Decision History

Context, Policy And Evidence

Preserves the context, core reasoning, policy version and confidence behind a decision, together with validation, human approvals and the recorded execution outcome.

Catalog includes metadata-only entries. Decision DNA retains run context. Validation follows available checks.

Make Governed Autonomy Your Competitive Edge

Help customers adopt autonomy with confidence. Policy, authority and human boundaries remain connected before, during and after action.

Before Action

Who May Act, On What?

Checks the tenant, permitted scope and operating policy. Protected targets, uncertainty and approval rules can block or escalate a response.

Your rules define the boundary.

During Action

What May Actually Execute?

The governed runtime dispatches bounded, authorized actions. Human approvals preserve their identity and timestamp. Receipts record the execution result.

Only authorized actions proceed.

After Action

Did The Response Work?

Supported verification checks the observed effect. Failures remain visible. Recovery and rollback follow the applicable control and validation gates.

Evidence supports closure.

Control spans Detection, Decision, Action, Control and Learning. Autonomous Trust Engine / Governed Runtime Kernel.

CLAWOLF
ART OF GOVERNED AUTONOMY

ONE CONNECTED LIFECYCLE / MORE PARTNER VALUE

More Customer Value. More Services To Sell.

Connect detection, authorized response and evidence-informed learning. Build integration, policy and managed-operation services around one lifecycle.

Autonomous Detection

The Evidence For A Decision

01 Ingest and normalize telemetry
02 Create traceable detection signals
03 Correlate activity across domains
04 Add business and threat context
05 Route evidence to specialist analysis

Your team sees a connected case.

Autonomous Action

The Authorized Response

01 Plan the response from the decision
02 Generate bounded execution intents
03 Respect approvals and target limits
04 Collect action receipts
05 Verify supported effects and recovery

Your team controls what may execute.

Autonomous Learning

The Recorded Outcome

01 Retain verified outcome events
02 Distinguish success from failure
03 Preserve decision and policy lineage
04 Support recurrence revalidation
05 Use evidence in subsequent analysis

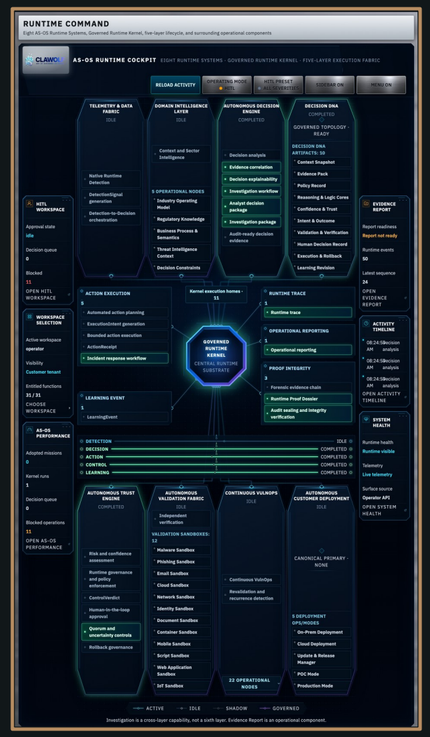
Your team keeps a reviewable history.

Canonical layers: Detection, Decision, Action, Control, Learning. Learning does not self-authorize policy changes.

AS-OS Dashboard Real View

The full cockpit connects eight runtime systems and their surrounding workspaces to the governed runtime.

FULL COCKPIT



RUNTIME DETAIL



The selected run ties the diagram to its recorded activity and evidence.

Full Context Around Every Run

HITL, workspace, performance, evidence, activity and system health remain visible around the operating architecture.

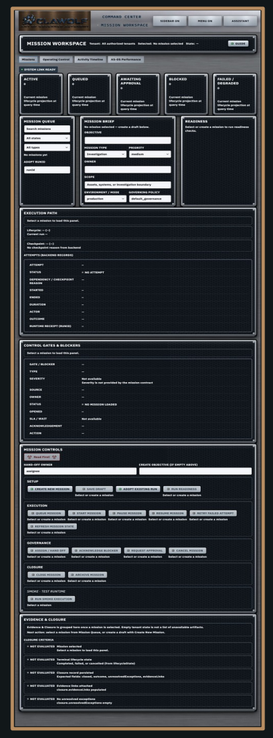
Full cockpit: demonstration environment. Center detail: recorded controlled-lab run.

CUSTOMER EXPERIENCE / YOUR SALES DIFFERENTIATOR

Give Customers A Better Operating Experience

Show one place to prepare the mission, follow readiness and review the outcome. Make the customer demonstration easier to understand.

FULL WORKSPACE



MISSION PREPARATION / DETAIL



A Defined Objective And A Visible Readiness Path

Prepare The Mission

Set the objective, owner, priority and scope. Adopt an existing run where appropriate.

Check The Path

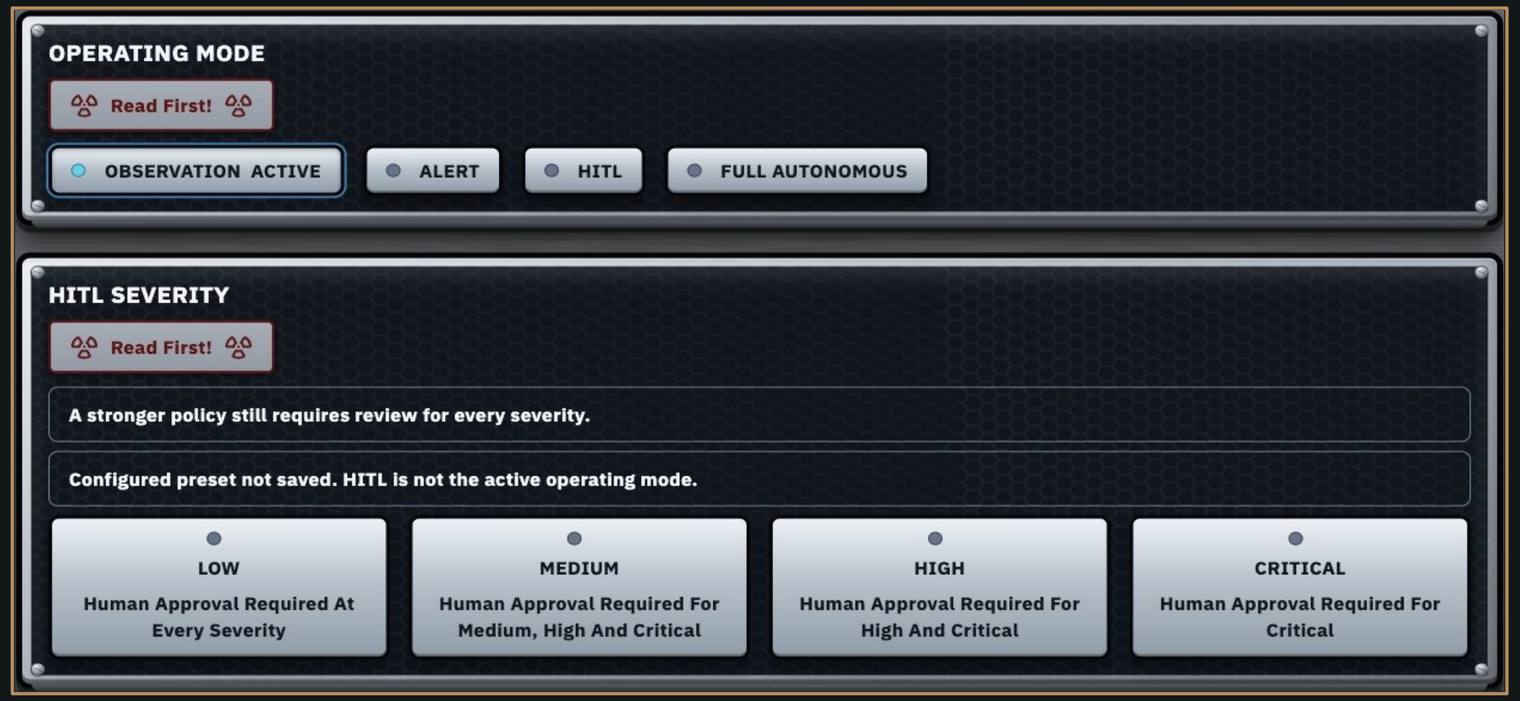
Review readiness, attempts and closure evidence. Help stays beside the operational UI.

Mission Workspace / UI: 22 October 2026. Help Tutorial and Assistant open in separate tabs.

COMPETITIVE ADVANTAGE / CUSTOMER CONFIDENCE

Turn Trust Into A Reason To Buy

Customers set the boundaries of autonomy. You gain a stronger answer to the buying objection: can we trust it?



Admin Or Explicitly Delegated User

Observation: observe and enrich.
Alert: observation plus notifications.
HITL: response follows approval gates.
Full Autonomous: only eligible, authorized actions may proceed.

Low Means More Human Review

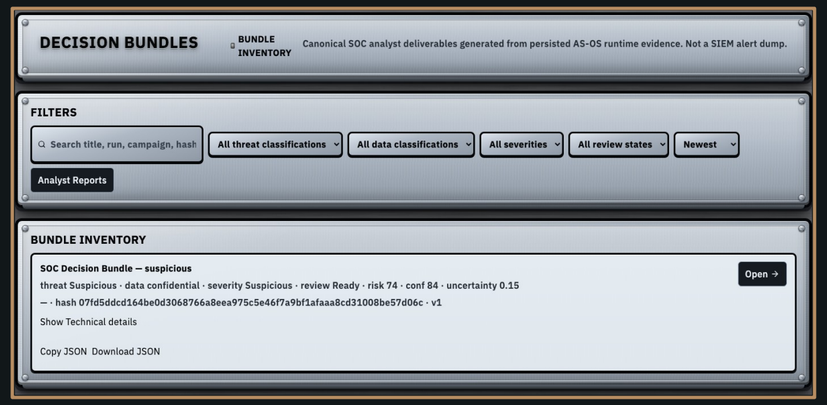
Low requires approval at every severity. Higher thresholds still respect protected targets, policy and uncertainty controls.

Operating Control / UI: 22 October 2026. No settings changed. Policy and other safety gates remain in force.

Make Richer Analysis A Stronger Closing Argument

Go beyond alert-led investigation: show connected context, reasoning, recommended actions and evidence in the customer demonstration.

DECISION BUNDLE / 13 SECTIONS



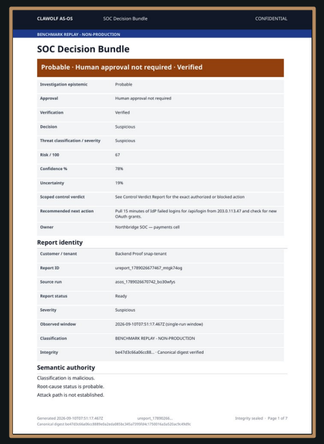
Executive summary, decision, confidence, risk, evidence summary and graph, intent, 21-core outputs, sector and context intelligence, uncertainty, next action and audit reference.

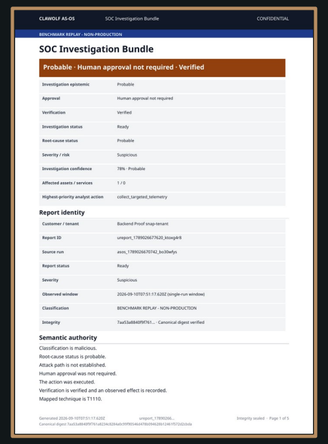
INVESTIGATION BUNDLE / 10 SECTIONS



Root cause, timeline, related assets, identities and events, attack path, MITRE mapping, evidence expansion, findings and recommended actions.

ACTUAL PDF EXPORTS





Real Backend Output

PDF + JSON reports share the source run and preserve evidence integrity.

Runtime Evidence And Recommended Actions For A Better-Informed Decision

UI: demonstration records. PDF covers: non-production benchmark replay. Report content follows available evidence.

Think 10×: Deploy Faster. Sell More.

Turn less repeated setup into more evaluations, shorter sales cycles and greater revenue opportunity. Put your technical team closer to customer value.



Less Manual Implementation Work

Environment Placement

Select cloud, on-premises, hybrid or air-gapped placement within the supported delivery scope.

Policy Before Connection

Prepare operating rules, engagement and governance before ingestion and execution.

Controlled Go-Live

Review entitlement, credentials and connector readiness. Keep blockers visible before Base-Live & Go.

10× is a partner growth ambition, not a measured sales result. Prepared-environment ACD target: one day; scope and access matter.

Compete With A More Powerful Sales Story

Differentiate through connected decision intelligence, governed execution, independent validation and native customer deployment.

Platform	Decision Method	Runtime Governance	Validation Method	Evidence & Proof	Deployment
Cisco / Splunk	ES agents + entity context	SOAR policy + approval gates	Agent findings + analyst validation	Case evidence + agent / action audit	ES / SOAR installation
Palo Alto Cortex	Agent planning + Cortex context	RBAC + policy + action approvals	Tool action-contract checks	Agent / incident audit trail	Cortex platform + integration setup
CrowdStrike Falcon	Expert agents + Enterprise Graph	Per-workflow autonomy + permission gates	Agent testing + analyst oversight	Agent traces + workflow audit logs	Falcon + connector configuration
Arctic Wolf Aurora	Expert swarm + customer context	Validated scope + human escalation	Swarm Judge + AI Trust Engine	Swarm / human quality review	Provider-operated managed SOC
Torq HyperSOC	Socrates + agents + business rules	Workflow guardrails + HITL / HOTL	Case / verdict review + memory feedback	Case-thread evidence + action logs	Platform / integration configuration
Microsoft Security	Copilot agents + security context	Agent identity + configured permissions	Tested agents + reviewable node maps	Agent outputs + admin audit logs	Cloud agent / plugin configuration
CLAWOLF AS-OS	**21-Core Decision + Domain Intelligence**	**Native Trust Engine + ControlVerdict / HITL**	**Independent AVF: 12 forensic engines**	**Decision DNA: 10 linked artifacts**	**Native autonomous customer deployment**

CLAWOLF integrates these methods in one five-layer runtime. Workflow controls and an integrated operating architecture are different scopes.

A method comparison, not whole-product parity. Customer value follows the supported deployment and licensed scope.

CLAWOLF
ART OF GOVERNED AUTONOMY

CLAWOLF CNDA
CLAWOLF NATIVE DEFENSE ARMORY
Clawolf Native Defense Armory

CHANNEL PARTNER OPPORTUNITY

Stand Apart With A Wider Product Portfolio

Six specialist product opportunities extend the AI-security conversation into more of the customer estate.

Our Competitive Agentic Portfolio

CLAWOLF IDI
EVERY IDENTITY. BOUNDED AUTHORITY.

Identity Defense Intelligence

Connect agent behavior to responsible owners and delegated privileges.

CLAWOLF DDI
KNOW DATA. PROTECT ACCESS.

Data & Database Intelligence

Relate AI access to sensitive data and database risk.

CLAWOLF BHI
SEE PATTERNS. UNDERSTAND RISK.

Behavioural Intelligence

Connect agent activity with patterns across people and workloads.

CLAWOLF ISD
INSIDER RISK. CLEARER CONTEXT.

Insider Defense Intelligence

Relate trusted-access misuse to delegated AI activity.

CLAWOLF SCE
SEE THE LINKS. EXPOSE THE RISK.

Supply Chain Exposure

Trace compromised dependencies into agent tools and services.

CLAWOLF CAI
EXPOSE RISK. TRACE THE ATTACK.

Cloud Exposure & Attack-In-Motion Intelligence

Relate agent permissions to cloud exposure and active attack paths.

CNDA specialist roadmap. Other products and cross-domain contributions are development targets, not released products.

Open New Accounts With Differentiated AI Security

A broad core offer and six signature capabilities give partners a sharper AI-and-agent security conversation.

Eight Core Feature Groups

AI Discovery & Security Posture

Agent Identity & Delegated Authority

Prompt Injection & Multimodal Protection

RAG & Memory Protection

MCP, Tools, Skills & AI Supply Chain

Models, Sensitive Data & Output Protection

Continuous Red Teaming & Resource Defense

Runtime Detection & Governed Containment

Six Signature Differentiators

Causal Evidence Integrity
Distinguish copies from independent support.

Semantic Effect Assurance
Check what an allowed action actually changed.

Joint-Outcome Defense
Detect harmful combinations across agents.

Causal Decontamination
Trace and quarantine poisoned-context derivatives.

Mission-Preserving Defense
Retain legitimate work where provably safe.

Continuous Assurance Invalidation
Recheck protection when assumptions change.

AIS in development. Planned standalone adoption, native AS-OS integration and CNDA cross-domain contribution.

Your AI Security Competitive Edge

Lead with broad AI-and-agent coverage, six signature capabilities and a native governed AS-OS architecture.

Capability	Palo Alto Prisma AIRS	Zenity	Noma	HiddenLayer	F5	CLAWOLF Combined Coverage
AI Discovery & Posture	AI Inventory & AI-SPM	Agent Inventory & Posture	Agents, Apps & MCP Inventory	AI Asset Discovery	AI App, Agent & API Discovery	**AI Estate + Attack-Path Context**
Agent Identity & Context	Identity-Aware Agent Policies	Intent, Memory & Handoffs	Identity, Sessions & Permissions	Agent / Harness Runtime Context	Runtime Access & Traffic Context	**Identity + Purpose + Observed Effects**
Tools & Runtime Enforcement	AI Runtime Inspection	Workflow-Aware Intervention	Inline MCP & Tool Controls	Tool, Code & Action Inspection	API / Gateway Guardrails	**Effect-Aware Governed Actions**
Adversarial & Supply-Chain Testing	Red Teaming + Model Scanning	Agent Exposure Validation	Red Teaming + AI Component Risk	Model Attacks + Supply-Chain Risk	AI Red Team + AI Remediate	**Red Teaming + Guardrail Engineering**
Evidence & Decision Context	Policy / Platform Telemetry	Agent Intent & Behavior Traces	Session & Policy Context	AI Attack & Runtime Events	Explainable Risks & Security Logs	**Causal Evidence + Decision Lineage**
Response & Recovery	Runtime Blocking + Case Response	Block / Steer Risky Agent Actions	Block, Mask or Seek Approval	Runtime Blocking + Integrations	Runtime Guardrails + Risk Mitigation	**Mission-Safe Defense + Causal Cleanup**
Operating Architecture	AI Security + SOC Orchestration	Agent Policies & Runtime Control	Central Policy & Runtime Control	AI Security + SOC Integration	AI Policy + Runtime Enforcement	**Native Five-Layer CLAWOLF AS-OS**
Cross-Domain Contribution	PANW Security Ecosystem	Agent / Business Application Context	AI, Data & Access Context	Model / Agent Dependencies	AI / API Security Context	**Native CLAWOLF CNDA Portfolio**

CLAWOLF AIS | **CNDA Portfolio Contribution** | **Native AS-OS Contribution**

AIS in development / target: 30 November 2026. CNDA roadmap. Functional crosswalk, not whole-product parity.

CHANNEL PARTNER OPPORTUNITY

Differentiate Big. Sell Beyond Fragmented Security.

Expand the opportunity from isolated tools to AI protection, governed enterprise action, services and renewals.

Customer Buying Trigger	Your Competitive Advantage	Your Partner Opportunity
Fragmented SIEM / SOC / SOAR	A connected decision-to-action operating layer	Modernization licences, integration and policy services
AI agents reach sensitive systems	AI-specific protection plus governed AS-OS coordination	AIS at release, native integration and adjacent portfolio growth
Approval bottlenecks / automation risk	Explicit operating authority and human-review boundaries	A stronger trust argument and governance-led selling
Security disrupts legitimate work	Mission-preserving protection targets safe continuity	A business-outcome conversation beyond alert counts
Mixed cloud / private / isolated estates	Deployment choice with scoped, traceable control	Wider territory fit and a repeatable delivery practice

AS-OS in production. AIS and CNDA contributions follow their development scope. enterprise@clawolf.com

CHANNEL ALLIANCE

Why Partners Choose CLAWOLF

A stronger customer proposition, with less repeated implementation work and a clearer buying path.

Let Customers Try. Give Them A Reason To Buy.

Three months FREE with a one-year subscription, or six months FREE with three years. Make customer confidence a sales accelerator.

Less Setup. More Time To Win.

ACD targets prepared deployment within one day. Put technical effort into customer value and the next qualified opportunity.

Make The Buying Decision Easier

Offer approved 12- and 36-month instalments. Help customers manage cash flow and move the buying conversation forward.

Zero Cloud Cost To Your Customers

Cloud costs are FREE for your customers during the agreed subscription plan. Predictable ROI. Confident customers. Faster decisions.

Free-use cloud costs are customer-paid. Subscription cloud coverage, financing and deployment follow the agreed scope and readiness.

CHANNEL ALLIANCE

A Broader Case For Customer Modernization

Use AS-OS and AIS to address more of the customer problem, then expand through a clearly labelled roadmap.

Buyer Priority	CLAWOLF Conversation
AI Agents And Runtime Trust	AIS Core / Signature (In Development)
Governed Autonomy And Auditable Action	AS-OS Five-Layer Operations
Existing-Tool Integration And Sovereignty	Integration Scope And Deployment Choice
MSSP Delivery And Tenant Separation	Delegated Roles And Tenant Workspaces
Predictable Cost And Cross-Domain Growth	Cloud Scope, Financial Facilities And CNDA Roadmap

Ten buyer priorities across five paired conversations. Portfolio breadth supports a replacement or modernization case; outcomes depend on the customer scope.

CHANNEL ALLIANCE

Cloud Licensing For Entry And Expansion

USD list price per billable asset per year. On-premises and air-gapped deployment receive project quotations.

Base Licence / Deployment	USD / Year
AS-OS Starter	$139
AS-OS Core	$219
AS-OS Governance	$269
AS-OS ACD	$5
AIS Core	$229
AIS Signature	$299

Optional Add-On / Suite	USD / Year
Domain Intelligence Advanced	$11
AVF Advanced	$17
Continuous VulnOps Exposure Chain	$50
Intelligence Assurance Suite	$25
Autonomous Exposure Defense Suite	$70

AS-OS packages are independent. Signature includes AIS Core. Choose one suite for the same scope; included components are not billed again.

AS-OS ACD is charged once annually across selected packages. AIS ACD is separately quoted. Optional third-party AI is customer-paid. AIS remains in development.

CHANNEL ALLIANCE

Your Growth Ambition: Think 10×

Faster deployment. Faster sales momentum. More revenue opportunity. Build a more productive partner practice.

A Stronger MSSP Proposition

Assigned-customer lifecycle views, delegated roles and tenant workspaces support a managed operations practice. Confirm fleet-view and OEM scope.

Competition Displacement

Use AS-OS governed coordination and AIS-specific protection to challenge fragmented point-product approaches and support existing investments.

Less Repeated Technical Effort

Reuse the ACD delivery path and agreed prerequisites. Services can focus on integration, policy and customer outcomes.

10x

Partner Growth Ambition

10× is the marketing ambition: turn repeatable deployment into more evaluation capacity, faster sales cycles and greater revenue potential. Actual outcomes depend on your execution and customer scope.

Consolidated incident/detection fleet queues are not yet instrumented in the supplied scope. White-label/OEM requires enablement.

CHANNEL ALLIANCE

Deployment Choice, One Joint Customer Plan

Agree the business outcome, placement, permitted action and commercial scope before the first deployment.

Placement	Customer Choice
BYOC	AWS / Azure / Google Cloud
Private Cloud	VMware
Customer Infrastructure	On-Premises / Air-Gapped

Standard BYOC billing is agreed separately. Program subscription cloud-cost coverage follows the agreed scope. Standard cloud service support and purchased-product updates are included.

Qualify The First Customer

Define licensed scope, success criteria, deployment prerequisites and the named customer authority.

Plan A Renewable Practice

Agree support ownership, renewal follow-through, the accepted payment schedule and partner economics.

Channel Guide + Channel Economics Benefits Program

enterprise@clawolf.com