CLAWOLF
ART OF GOVERNED AUTONOMY

AS-OS OPERATING PLATFORM / AIS FLAGSHIP / CNDA PORTFOLIO

AI Freedom. Without Losing Control.

CLAWOLF AS-OS + AIS

Autonomous Security Operations
And AI-Agent Security

A governed operating platform and native defense products for enterprise adoption and partner-led growth.

AS-OS IN PRODUCTION / AIS TARGET: 30 NOVEMBER 2026

A Unique Architecture For Security Operations

Five governed layers. Eight runtime systems. One security operating platform.

Detection / Decision / Action / Control / Learning

Business-Aware Decisions

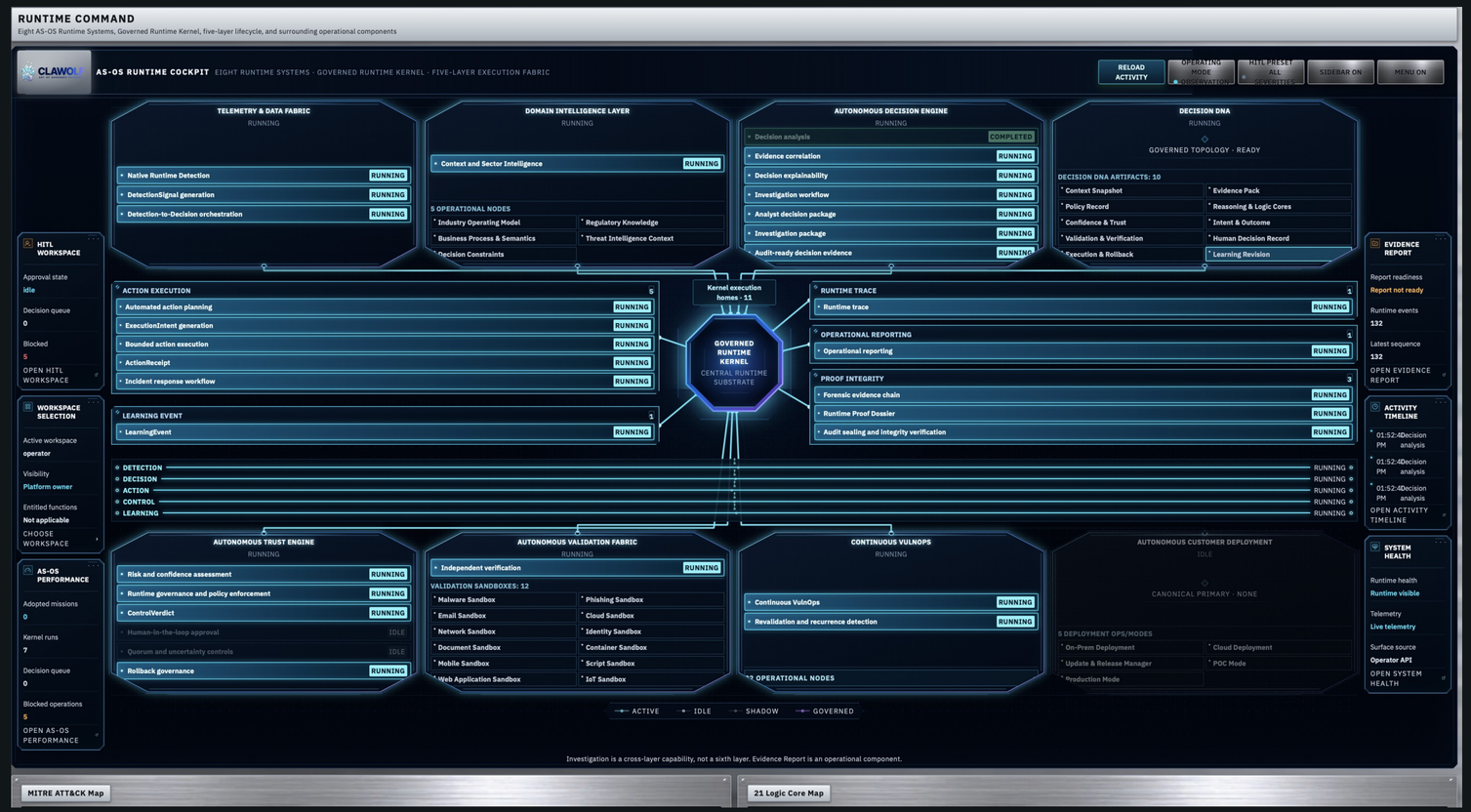
UNIQUE METHOD Domain Intelligence Layer adds sector and regulatory context. The UNIQUE METHOD Autonomous Decision Engine uses 21 specialist logic cores.

Authority And Outcome Together

UNIQUE METHOD Trust Engine governs execution. UNIQUE METHOD AVF checks evidence. UNIQUE METHOD Decision DNA links intent, approval and observed effects.

Repeatable Customer Deployment

UNIQUE METHOD Autonomous Customer Deployment prepares placement, configuration and readiness within the customer's authorized environment.



CLAWOLF AS-OS / Runtime Command Dashboard

Beyond SOC Automation: The AS-OS Difference

Compare what makes the decision, governs execution, validates the result and preserves proof.

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.

Why Buy CLAWOLF AS-OS?

The purchase case is control of the operating layer, with contextual decisions and evidence the customer can follow.

The Customer Need	The CLAWOLF Approach	The Purchase Reason
Automate Across An Existing Estate	A five-layer operating architecture connects evidence, decision, permitted action, control and recorded outcomes.	**Adopt an operating layer around supported existing tools rather than buy only another alert queue.**
Keep Authority While Increasing Autonomy	Operating policy, human approval and bounded execution share a decision identity. Decision DNA preserves the rationale and outcome.	**Your team can review who allowed a response, what ran and which effects the system actually observed.**
Make Decisions In Business Context	Domain Intelligence Layer and 21 specialist logic cores inform risk, policy and uncertainty. Missing checks remain explicit.	**Prioritize the organization’s exposure and send uncertain or protected decisions to the right human.**
Deploy And Expand On Your Terms	Autonomous Customer Deployment prepares placement and readiness. AIS and the CNDA products add separately adoptable defense scope.	**Choose the operating platform, the AI-defense entry product or both, then expand against a named customer need.**

AS-OS Market & Framework Alignment

Agentic SOC and detection-and-response categories mapped to CLAWOLF's operating architecture.

Authority	Date / Official Source	Public Category / Framework	AS-OS Mapping & Buyer Meaning
IDC	10 Jul 2026 IDC Agentic SOC article	Autonomous planning, reasoning, execution and learning. Multi-agent collaboration with trustworthy operations.	Specialist decision analysis, governed execution, recorded outcomes and operator review connect into one operating platform.
Gartner	25 Feb 2026 Gartner doc. 7503053	Detection and Response AI SOC Agents. Vendor selection for improved workflows and incident response.	Contextual decisions combine with authorized response and evidence in the AI SOC buying conversation.
NIST	26 Feb 2024 / Apr 2025 NIST CSF 2.0 NIST SP 800-61r3	CSF: GOVERN, IDENTIFY, PROTECT, DETECT, RESPOND, RECOVER. SP 800-61r3 places incident response in risk management.	Policy and asset context inform detection and response. Supported control, recovery and retained evidence support review.
MITRE	Live knowledge bases MITRE ATT&CK / D3FEND Accessed 17 Oct 2026	ATT&CK describes adversary behavior. D3FEND models defensive techniques and their relationships.	Threat-domain analysis and evidence mapping explain the case. References do not imply complete technique coverage.

CLAWOLF's mapping of public research and frameworks. No analyst endorsement or certification. Source names are clickable.

Comprehensive AI-Agent Security

Protect agents, data, memory and tools with native AS-OS governance and CLAWOLF CNDA threat-domain intelligence.

THE AI ACTIVITY AIS PROTECTS — **Models / Agents / Retrieval & Memory / Tools & MCP / Enterprise Data & Resources**

CLAWOLF AIS

AI-Agent Security / CNDA Flagship

Core Features

Discover the AI estate. Protect identities, prompts, memory, tools, models and data. Detect and contain harmful agent activity.

Signature Features

Preserve evidence provenance. Check cumulative actions and real effects. Remove poisoned context and continue only verifiably safe work.

Operating Principle — **Identify The Actor / Evaluate Authority & Purpose / Constrain The Action / Verify The Effect**

Native CLAWOLF AS-OS Integration

AIS evidence enters one policy, approval, action and outcome-verification chain. AS-OS retains decision authority.

CLAWOLF CNDA Portfolio Contribution

Separately adopted CLAWOLF products add identity, data, behavior, insider, supply-chain and cloud attack-path context.

AIS Core And Signature Features

Eight protection groups cover the AI estate. Six signature mechanisms connect protection to evidence, effects and safe continuation.

CORE FEATURES

AI Discovery & Security Posture
Inventory AI, owners, permissions, dependencies and reachable attack paths.

Agent Identity & Delegated Authority
Trace delegation, excessive privilege, token misuse and tool access.

Prompt Injection & Multimodal Protection
Inspect direct / indirect injection across content, code and tool responses.

RAG & Memory Protection
Protect retrieval, vector stores, memory integrity and context confidentiality.

MCP, Tools, Skills & AI Supply Chain
Inspect definitions, arguments, behavior, provenance and component integrity.

Models, Sensitive Data & Output Protection
Address model attacks, extraction, secrets, data access and exfiltration.

Continuous Red Teaming & Resource Defense
Test agent attacks and constrain recursion, compute abuse and runaway tasks.

Runtime Detection & Governed Containment
Detect harmful activity. Constrain calls, revoke access or isolate under policy.

SIGNATURE FEATURES

Causal Evidence Integrity
Copies of one source never count as independent evidence.

Semantic Effect Assurance
Check permitted scope against what the action actually changed.

Joint-Outcome Defense
Detect harmful combinations across agents and concurrent tasks.

Causal Decontamination
Quarantine poisoned context and derivatives. Retain trustworthy work.

Mission-Preserving Defense
Continue only verifiably safe work. Otherwise stop or escalate.

Continuous Assurance Invalidation
Recheck after changes to models, tools, permissions or context.

AI-Agent Security: Current Market State

Market capabilities and their functional counterparts across CLAWOLF AIS, native AS-OS and the CNDA portfolio.

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**

CUSTOMER & INVESTOR VALUE

Why Choose CLAWOLF AIS?

Core Protection, Signature Features And Native Integration Connected To Business Outcomes.

Market Baseline Covered By AIS	What CLAWOLF Adds	Why It Matters To Your Business
Stop Risky Agent And Tool Actions	Semantic Effect Assurance + native AS-OS control checks authorized scope against the observed result.	**Catch harmful effects behind an allowed call. Base response on what actually changed.**
Protect Retrieval And Agent Memory	Causal Evidence Integrity + Causal Decontamination trace poisoned sources and affected derivatives.	**Reject false corroboration. Remove poisoned context while preserving trustworthy work.**
Control Coordinated Agent Activity	Joint-Outcome Defense evaluates combined data access, authority and effects across the task.	**Catch harmful combinations that individual, apparently permitted actions can conceal.**
Contain Threats Without Losing The Task	Mission-Preserving Defense + AS-OS policy and approval isolate the unsafe branch within existing authority.	**Continue verifiably safe work. Stop or escalate when no safe continuation exists.**
Prioritize AI Risk In Business Context	Native CLAWOLF CNDA products add identity, sensitive-data, behavior and enterprise attack-path context.	**Focus on agents that can reach critical assets. Coordinate response around business exposure.**
Keep Protection Current As AI Changes	Continuous Assurance Invalidation ties evidence to model, tool, permission and context versions.	**Recheck controls affected by change. Avoid trusting a test that no longer represents the system.**

CLAWOLF AIS + CLAWOLF AS-OS

AI Security That Becomes Operational Control

Deploy CLAWOLF AIS independently or connect it natively to CLAWOLF AS-OS for one governed decision-to-outcome chain.

CLAWOLF AIS Protection + Evidence › **Detection** Identify The Risk › **Decision** Apply Context & Authority › **Action** Execute Within Policy › **Control** Govern & Verify Effects › **Learning** Retain Decision Evidence

One Decision Authority

Domain intelligence and 21 specialist logic cores add context; AS-OS owns policy, approval and action.

Evidence You Can Follow

Trust checks, on-demand UNIQUE METHOD Validation Fabric and UNIQUE METHOD Decision DNA link authority, action and observed outcome.

Less Operational Fragmentation

AI, identity, data and infrastructure evidence inform the same case—not separate, manually reconciled queues.

THE CUSTOMER OUTCOME / PROTECT / GOVERN / CONTROL / PROOF

PROTECT

Detect hostile agent behavior and constrain unsafe actions as the task executes.

GOVERN

Apply purpose, permitted scope, policy and the human-approval boundary.

CONTROL

Check actual effects and contain deviation within authorized controls.

PROOF

Link intent, decision, action and observed results in UNIQUE METHOD Decision DNA.

CLAWOLF AIS + CLAWOLF CNDA

Clawolf Native Defense Armory: six additional CLAWOLF products connect AI activity to enterprise risk.

	CLAWOLF AIS +	COMBINED CUSTOMER VALUE
Dec 2026	**CLAWOLF Identity Defense Intelligence**	Agent Identity Security connects each agent to its owner, delegated authority and reachable resources. Constrain stolen or excessive access without stopping every agent.
Dec 2026	**CLAWOLF Data & Database Intelligence**	Agent-to-Data Intelligence connects agent actions to sensitive records and database reachability. Reveal when an authorized query becomes an exfiltration path.
Jan 2027	**CLAWOLF Behavioural Intelligence**	Behavior In Context combines agent, user and workload baselines with task purpose. Expose stealthy misuse and harmful sequences that isolated calls conceal.
Jan 2027	**CLAWOLF Insider Defense Intelligence**	Human-to-Agent Risk links employee behavior, privileges and data access to agents acting on that person’s behalf. Reveal insider misuse and compromised-account abuse.
Feb 2027	**CLAWOLF Supply Chain Exposure**	Third-Party Attack Paths connect suppliers, SaaS, MCP services and delegated tokens to agent dependencies. Trace and constrain the spread of a compromised component.
Feb 2027	**CLAWOLF Cloud Exposure & Attack In Motion Intelligence**	Identity-Aware Attack Paths combine agent permissions, cloud exposure and active runtime evidence. Prioritize reachable business risk as an attack path begins to activate.

AIS Market & Taxonomy Alignment

AI-security categories and threat frameworks mapped to AIS and its native AS-OS / CNDA contributions.

Authority	Public Concepts	CLAWOLF AIS / AS-OS / CNDA Mapping
IDC	AISPM, non-human identity, agent zero-trust authorization, runtime security, skills inspection and continuous risk governance.	AI estate and delegated authority, tool/runtime controls and ongoing assurance. Native AS-OS adds governed response and evidence.
Gartner	Security-relevant AI TRiSM categories: AI Governance, AI Runtime Inspection and Enforcement, Information Governance.	Agent and decision traceability, runtime protection and sensitive-data controls. Scope is security, not a complete responsible-AI program.
MITRE ATLAS	AI Agent Tool Poisoning, Exfiltration via AI Agent Tool Invocation and AI Supply Chain Rug Pull.	Tool / skill inspection, supply-chain integrity, sensitive-output controls, evidence provenance and adversarial tests.
NIST	AI RMF: GOVERN, MAP, MEASURE, MANAGE. AI 100-2: evasion, poisoning, privacy breach and abuse.	Policy and estate mapping, model / input / memory protection, red teaming, controlled containment and outcome evidence.
OWASP	Agentic Top 10: goal hijack, tool and identity misuse, supply chain, code, memory, communications and cascading risk.	Prompt, tool and identity controls, cumulative-outcome defense, causal cleanup and human-approval boundaries.
CSA	MAESTRO: a seven-layer reference architecture from Foundation Models through Agent Ecosystem.	Model and data protection, tool/framework inspection, deployment boundaries, assurance and cross-domain governance.

Security design mapping, not certification or full framework conformity. IDC China concepts are English translations.

STRATEGIC ARCHITECTURE VALUE

CLAWOLF For Hyperscalers

A customer-controlled operating and AI-defense option across the environments that enterprises already run.

Connect The Customer Estate

Carry a case across supported cloud and on-premises systems while retaining the customer’s policy, approvals and evidence.

Cross-Environment Operations

Protect Business Use Of AI

AIS targets agent, memory, tool and model risk. AS-OS connects an AI finding to an authorized operational response.

AI Defense + Governed Response

Respect Native Control

Retain native identity, policy and security enforcement. Evaluate CLAWOLF where a distinct customer deployment or evidence requirement remains.

Complement Rather Than Bypass

Hyperscaler Contribution

Native cloud products, complementary CLAWOLF functions and the customer value of combining them.

Ecosystem	Current Platform	CLAWOLF Contribution	Customer Value
Microsoft / Azure	Agent 365, Entra, Defender and Purview govern agents. Sentinel / Security Copilot support the SOC.	Connect a Sentinel incident to AS-OS policy, approval and supported response in the wider estate. Add AIS causal evidence and effect assurance around AI actions.	**A customer-controlled case and evidence path across Azure and non-Microsoft systems, without replacing native enforcement.**
AWS	AgentCore Policy, Identity and Evaluations govern agents. Security Hub and EventBridge support response automation.	Relate AgentCore and Security Hub findings to AS-OS business context and bounded cross-environment actions. Qualify AIS cumulative-effect and memory defenses.	**Join cloud findings to on-premises or multi-cloud operations with one reviewable decision and outcome record.**
Google Cloud	Google SecOps offers agentic investigation and automation. Model Armor screens AI content. SCC provides AI protection.	Use AS-OS for customer-specific authority and decision evidence beyond the selected SecOps workflow. Add AIS mission integrity and CNDA enterprise-risk context.	**Extend customer deployment and case continuity while keeping Google’s agents, intelligence and native controls in place.**

Proposed integration scope, not a claim of native-platform absence or proven feature superiority.

DIRECT CUSTOMER VALUE

CLAWOLF For Enterprise

An operating platform for the security estate. A dedicated defense product for the AI systems entering the business.

Coordinate The Estate

Reduce manual reconciliation between supported security tools, policy decisions, response actions and evidence.

Fewer Disconnected Handoffs

Increase Safe Autonomy

Set the operating mode, human boundary and protected scope. Analysts retain an accountable decision and a visible outcome.

Control Without Every-Step Approval

Expand Against A Need

Buy AS-OS for operations, AIS for AI-agent risk, or combine them. Add a CNDA product when its threat domain becomes a priority.

A Clear Adoption Path

CLAWOLF
ART OF GOVERNED AUTONOMY

ENTERPRISE / BUYING SITUATIONS

The Problem, The Product And The Result

Four buying situations, the product to adopt and the operational value to expect.

Customer Situation	The Operational Problem	What The Customer Buys	The Intended Gain
Mixed SIEM, EDR And Cloud Tools	The analyst reconciles findings, permissions, response and closure across separate workspaces.	AS-OS operating layer, with qualified connections to the existing estate.	**A contextual decision, authorized action and evidence trail the team can review together.**
AI Agents Reach Enterprise Data	A permitted prompt or tool call can still leak data, poison context or produce a harmful combined outcome.	AIS, independently or with native AS-OS response.	**Protect AI work and constrain unsafe actions while preserving work that remains verifiably safe.**
A Regulated Or Sovereign Environment	Policy, evidence handling, human responsibility and deployment placement must meet local requirements.	AS-OS deployment preparation and configured authority boundaries.	**A reviewable operating model in a supported customer deployment.**
A New Identity, Insider Or Cloud Risk	An AI-only view misses the wider path from account and permission to a business asset.	Separately adoptable CNDA domain products as they reach release.	**Prioritize AI and enterprise findings with the owner, data and attack-path context relevant to the business.**

AS-OS is the operating platform. AIS and the additional CNDA products retain their published development targets.

MANAGED-SERVICE BUSINESS VALUE

CLAWOLF For MSSPs And Telcos

A licensable operating architecture and AI-defense portfolio that a service provider can evaluate for its own customer offerings.

Repeat The Deployment

Use a governed preparation and readiness path for each customer instead of recreating the implementation approach.

Repeatable Service Preparation

Package An AI-Defense Service

Offer AIS around agent exposure, tools, memory and runtime risk. Connect authorized response through AS-OS where the service scope requires it.

A Named New Service Offer

Keep Customer Boundaries

Separate tenant evidence, delegated authority and approvals. Extend the service with individually adopted CNDA products.

Customer-Specific Operations

AI-Defense Service Expansion

Specialist AI-defense offers beside established managed security, agent platforms and customer operations.

Provider	Existing Public Offer	Proposed CLAWOLF Service	Potential Service Value
LevelBlue / Trustwave	Managed security, MDR, offensive security and incident response.	AIS agent-risk defense with governed AS-OS response for a defined customer scope.	**A specialist AI-defense service beside established MDR.**
Vodafone Business	Google SecOps-enabled MDR and agentic AI concierge services.	AIS protection for business agents, joined to customer-specific response authority.	**Protect the AI services the provider helps customers adopt.**
Verizon Business	24/7 MDR, risk-driven investigation and closed-loop response.	AIS agent/tool/memory defense and portable AS-OS decision evidence.	**An AI-risk service with a clearer approval-to-outcome record.**
Deutsche Telekom / T-Systems	AI-agent security concepts, T-AI platforms and agent governance.	Evaluate AIS causal cleanup and effect assurance in a sovereign customer deployment.	**Specialist AI-defense scope around existing agent platforms.**
Telefónica Tech	AI-Native SecOps combining agents, analysts and governance.	AIS mission-integrity mechanisms and cross-domain CNDA risk context.	**A product-level AI-defense add-on to the operating service.**
e& enterprise / Help AG	Managed cybersecurity and AI security / governance capabilities.	AIS plus scoped AS-OS operating authority for GCC customer environments.	**A separately packaged AI-defense and governed-response offer.**
sirar by stc	Managed SOC, MDR, intelligence and operational reporting.	AIS protection and AS-OS decision/effect evidence for authorized customer cases.	**Expand from monitoring into a qualified AI-risk service.**

CLAWOLF For Platforms, GSIs And Fintech

Reusable operating software and native AI defense for an established service portfolio or distribution channel.

Embed An Operating Product

Evaluate AS-OS as a licensed or OEM operating layer where the buyer wants customer-controlled authority and reusable evidence contracts.

Product IP + Existing Distribution

Add Targeted AI Defense

Evaluate AIS signature mechanisms as specialist capability within an existing managed-security or AI-adoption service.

A Defined Portfolio Extension

A Strategic Technology Asset

A reusable operating architecture and native defense portfolio can support product licensing, an OEM arrangement or a strategic acquisition.

Licensing / OEM / Acquisition

Strategic Product & Service Fit

Product licensing and service integration are the primary routes. Payment-network use cases are an adjacent opportunity.

Candidate	Existing Portfolio	Proposed CLAWOLF Contribution	Commercial Rationale
Accenture	Cyber.AI, managed security and secure-AI services.	AS-OS operating software with reusable decision and evidence contracts. Add AIS defense.	**Reusable software IP inside a transformation or managed service.**
Deloitte	Cyber AI blueprints, Zora agents and cyber managed services.	Use AS-OS governed execution and Decision DNA in a defined service. Add AIS mission integrity.	**Product-backed delivery of repeatable customer services.**
Atos / Eviden	Published AIsaac MDR and sovereign service options.	Add AIS causal evidence and effect assurance beside existing MDR, with scoped AS-OS response.	**Specialist AI defense for sovereign and enterprise services.**
Kaseya	AI-enhanced Kaseya MDR, response automation and MSP distribution.	Package AIS for the MSP channel. Add scoped AS-OS response where the service requires it.	**An AI-risk product for existing MSP distribution.**
Mastercard	Recorded Future, cyber services and Verifiable Intent.	Apply AIS tool, memory and cumulative-effect protection to a defined agentic workflow.	**An adjacent trust extension, not a payment-control replacement.**
Visa	Intelligent Commerce and Trusted Agent Protocol.	Apply AIS mission-integrity checks beyond agent authentication, within transaction boundaries.	**Agent-risk extension alongside native trust and fraud controls.**

One Platform. Two Entry Products. Several Buyers.

AS-OS sells governed security operations. AIS sells AI-agent protection. CNDA expands the customer relationship by threat domain.

Direct Enterprise

License AS-OS for the operating layer or AIS for AI risk. Qualify deployment, controls and evidence against the buyer’s own use case.

Enterprise Software Revenue

MSSP / Telco / GSI

Combine licensed software with a partner’s managed service, distribution and implementation expertise. Add AIS and other CNDA products over time.

Partner-Led Recurring Services

Platform / Strategic Buyer

Evaluate technology licensing, an OEM arrangement or acquisition for a reusable security operating layer and a native AI-defense portfolio.

Strategic Architecture & IP