Evolver Integrated Solution Paper (EISP)

Evolver COMMAND

AI-Powered Agentic Command and Control for U.S. Government IT and Cybersecurity Operations

Integrating Evolver IT and Cybersecurity Services with the L2H.ai Agentic Command Center

Customer Challenge: Fragmented IT and Cyber Tools Slow U.S. Government Mission Operations

U.S. Federal agencies operate dozens of mission-critical IT and cybersecurity tools that rarely talk to each other. Security operations centers triage alerts in cyber tools like CrowdStrike, hunt threats using tools such as Splunk, manage tickets in ServiceNow or tools like Elastic ITSM, monitor hybrid cloud infrastructure, and chase vulnerabilities across siloed vulnerability scanners. Analysts switch between consoles, manually correlate data across systems, and spend hours connecting information that should already be integrated, while adversaries operate at machine speed and budgets remain constrained.

Traditional integration platforms and public AI services do not close this gap. They lock agencies into a single vendor stack, push sensitive data outside the security boundary, or require months of custom development for every new tool. U.S. Government leaders need a sovereign, multi-agent AI command and control capability that runs inside the agency boundary, orchestrates the IT and cyber tools the agency already owns, and lets analysts and operators work better, faster, and more cost-effectively without re-platforming.

Solution Overview

Evolver COMMAND combines Evolver's federal IT and cybersecurity operations expertise with the L2H.ai Agentic Command Center to deliver a unified, sovereign, multi-agent AI control plane across the existing IT and cyber tool stack. COMMAND:

- Connects to 100+ commercial IT and cybersecurity tools, including CrowdStrike EDR, Splunk SIEM/SOAR, Elastic ITSM, ServiceNow, Tenable, Microsoft Sentinel, and major cloud providers via existing REST and MCP APIs
- Orchestrates multi-agent workflows that triage, correlate, enrich, and act across IT operations and cyber defense from a single command surface
- Routes each task to the best-fit LLM (frontier or self-hosted open-source) with no vendor lock-in
- Supports customer-hosted deployment on AWS, Azure, Azure GovCloud, on-premises Kubernetes, or air-gapped tactical edge
- Operates inside the agency boundary with full auditability, identity governance, and policy enforcement

COMMAND is a non-disruptive overlay solution that integrates through existing APIs and preserves current tools, workflows, and investments while COMMAND provides agentic AI reasoning capabilities across every IT and cyber function.

Evolver Integrated Solution — Unique Features

Multi-Agent Orchestration Across 100+ Tools

- Pre-built and custom workflows connect CrowdStrike, Splunk, Elastic, ServiceNow, and the broader commercial IT and cyber tool ecosystem via existing APIs.

LLM-Agnostic by Design

- Run any frontier or self-hosted open-source model. Switch or combine models per task with no rebuild and no lock-in.

Sovereign, Customer-Hosted Deployment

- Your cloud, your VPC, your data. IL2 through IL6 ready, with IL5 and JWICS operational today.

Identity, Audit, and Governance

- SAML, OIDC, SCIM, PKI, LDAP, scoped API keys, and append-only audit aligned to federal compliance frameworks.

Workflow-Native Integration

- Agentic reasoning steps drop into existing IT and cyber processes through MCP servers, REST endpoints, and webhooks without re-platforming.

Expected Customer Benefits

Faster Operations

40 to 60 percent faster operator and analyst tasks through automated correlation, enrichment, and AI-recommended actions across IT and cyber tools.

Better Mission Outcomes

Real-time situational awareness, high-fidelity detections, and prioritized response from a unified, multi-source command surface.

Lower Total Cost

Maximize value from tools the agency already owns. Reduce analyst toil and route tasks to the most cost-effective model per use case.

Sovereign and Compliant

Aligned to FedRAMP High, NIST 800-53, NIST AI RMF, FISMA, SOC 2, and ISO 27001. Your account, your VPC, your data.

How It Works

Phase 1
Discovery and Baseline (Days 0 to 30)

- Joint Evolver and L2H.ai team inventories the agency IT and cyber tool stack, integrations, and mission workflows
- Baseline metrics captured for MTTR, mean time to detect, analyst hours per incident, and cost per workflow
- Top use cases prioritized across SOC operations, ITSM, ITOM, vulnerability management, and threat hunting
- Data sovereignty, hosting model, identity, and model governance policies defined with agency stakeholders

Phase 2
Agentic Command Center Deployment (Days 30 to 60)

- L2H.ai Agentic Command Center deployed inside the agency boundary in the selected hosting posture
- Tool integrations stood up via existing APIs to CrowdStrike, Splunk, Elastic, ServiceNow, and approved sources
- Multi-model routing configured across frontier and approved self-hosted open-source LLMs
- Identity, audit logging, guardrails, and role-based access enforced across all agent workflows

Phase 3
Workflow Integration and Pilot (Days 60 to 120)

- Pre-built agentic workflows activated for SOC triage, threat enrichment, vulnerability correlation, and ITSM resolution
- Custom multi-agent workflows authored in the visual builder for agency-specific missions
- Side-by-side pilot measured against baseline; success criteria validated with program managers
- Analyst and operator training, change management, and knowledge transfer delivered by Evolver

Phase 4
Sustainment and Scale (Ongoing)

- 24/7 Tier 1 to Tier 4 IT and cyber operations support with continuous AI-assisted resolution
- Quarterly governance reviews with executive dashboards (MTTR, MTTD, deflection, model spend)
- Continuous model and workflow evaluation as new LLMs and tools are approved by the agency
- Phased expansion across additional missions, bureaus, and classification environments

Evolver Integrated Technology Solutions (EITS)

A portfolio of market-leading IT, cybersecurity, and AI solutions delivered as modular capabilities government organizations can adopt quickly, integrate easily, and scale confidently. Each can be deployed independently or combined.

COMMAND — Agentic AI Command and Control

Integrates Evolver IT and cybersecurity services with the L2H.ai Agentic Command Center across 100+ commercial IT and cyber tools (CrowdStrike, Splunk, Elastic, ServiceNow, and more) to unify operations and accelerate mission outcomes.

60 to 120 Day Pilot: Bounded pilot across one mission domain. Deploy the Agentic Command Center inside the agency boundary, integrate top tools via existing APIs, and deliver measurable analyst time savings and MTTR gains.

ASSIST — AI-Powered IT Service Management

Combines Evolver Enterprise IT Help Desk Services with L2H.ai AI orchestration on ServiceNow to accelerate ticket resolution and reduce operational cost.

ENHANCE Cyber- Physical Data Center Security

Unifies electronic security, IT cybersecurity, and AI-powered OT/IoT/ICS protection for data centers facing converged risk from AI-driven compute densification.

GUARDIAN — Vulnerability Management

Risk-based vulnerability management unifies fragmented scanner outputs, normalizes exposure, and applies mission-aligned prioritization with automated remediation.

SPECTRA — SOC Support

AI-powered toolkit that enhances SOC results through high-fidelity detections, enriched telemetry, and governed automation to reduce analyst fatigue.

CLEAR — Procurement and Supply Chain

Expedited, non-intrusive supply-chain risk assessment that accelerates vendor evaluation and supports continuous monitoring at scale.

SHIELD — Post-Quantum Cryptography

Transparent, portable PQC enterprise network security that safeguards critical tunnels with zero disruption and full auditability.

Procurement Options: Existing Evolver master service agreements; GSA, GWAC, and agency contract vehicles; commercial channels and marketplaces; on-premises, cloud, or hybrid deployment per agency environment. 60-to-120-day pilots are available for COMMAND and across the EITS portfolio.

Why Evolver and L2H.ai

Evolver brings decades of federal IT operations, cybersecurity, enterprise help desk, ITSM, SOC, and zero trust experience supporting national security, federal civilian, and commercial missions. L2H.ai brings the Agentic Command Center, a customer-hosted, multi-agent AI platform purpose-built for sovereign, high-security, and hybrid government environments, with 1M+ users served and IL5 plus JWICS operational today.

Combined Capabilities

- Enterprise IT operations and Tier 1 to Tier 4 service desk
- Defensive cyber operations, SOC, threat hunting, and incident response
- Multi-agent AI orchestration across 100+ IT and cyber tools via existing APIs
- LLM-agnostic routing across frontier and self-hosted open-source models
- Customer-hosted, on-premises, hybrid, and air-gapped deployment
- Zero Trust, FedRAMP High, FISMA, NIST 800-53, and NIST AI RMF alignment
- Continuous monitoring, executive dashboards, and audit evidence
- 24/7 mission operations and ITIL v4 governance

Gregory A. Garrett | Chief Operating Officer
Gregory.Garrett@evolverinc.com - 571.991.7768 - www.evolverinc.com