

AI::Sec - Enterprise Sales Pitch & Adoption Strategy

1. Executive Summary

AI::Sec is an AI-powered Application Security (AppSec) solution designed to enhance security teams by automating key application security workflows in enterprises, MSSPs, and regulated industries. It automates **90% of AppSec tasks**, vulnerability management, compliance enforcement, and secure development practices, reducing operational costs and improving efficiency. AI::Sec scales instantly—offering seamless integration into DevSecOps pipelines.

2. The Pain Points AI::Sec Solves

The Current Challenges in Enterprise Application Security:

- **Growing Application Security Demands:** As software development accelerates, security teams struggle to keep pace with code reviews, vulnerability management, and compliance requirements.
- **Skill Gap & Talent Shortage:** Over **4 million unfilled cybersecurity jobs** globally, with a significant shortage in **AppSec engineers**.
- **Time-Consuming & Costly Security Reviews:** Manual security testing slows development cycles and increases costs.
- **Compliance & Regulatory Complexity:** Enterprises must adhere to **NIST, ISO 27001, PCI-DSS, GDPR, and industry-specific security policies**.
- **Limited Availability of Commercial LLMs for On-Prem Deployment:** Most large language models (LLMs) are not licensed for commercial on-premises use, restricting enterprise adoption.
- **High Infrastructure Costs for On-Prem AI Inference:** Running LLMs on-prem requires significant **GPU and RAM resources**, making it costly and difficult to scale.

💡 **AI::Sec addresses these challenges by accelerating and automating secure application development without disrupting engineering workflows.**

3. AI::Sec's Solution: AI-Powered Application Security Automation

🚀 **AI::Sec automates and enhances application security tasks, seamlessly integrating into DevSecOps workflows.**

- ✅ **Automated Secure Code Review:** Identifies security flaws in real-time, reducing vulnerabilities before production.
- ✅ **Compliance & Policy Enforcement:** Ensures adherence to industry standards and security best practices.
- ✅ **DevSecOps Integration:** Automates security testing in CI/CD pipelines without slowing down releases.
- ✅ **Threat Intelligence:** Analyzes and prioritizes vulnerabilities using risk-based scoring.
- ✅ **Efficient On-Prem AI Deployment:** Optimized AI inference that significantly reduces GPU and RAM resource consumption.

✅ **Commercially Licensed LLM Solution:** Al::Sec provides an enterprise-ready, on-prem-compatible LLM solution that overcomes licensing restrictions.

💡 *"Think of Al::Sec as your **automated AppSec engineer**, working 24/7 to secure your applications at scale."*

4. Al::Sec's Key Buyers & Decision-Makers

Who Owns Al::Sec in Enterprises?

- 🔪 **Chief Information Security Officer (CISO):** Ensures overall security posture, risk reduction, and compliance.
 - 🔪 **DevSecOps / Application Security Leader:** Drives secure software development initiatives.
 - 🔪 **Engineering & Development Teams:** Benefit from automated security feedback without disrupting workflows.
 - 🔪 **Compliance & Risk Management Officers:** Require automated policy enforcement and audit-ready reports.
 - 🔪 **CIO / CTO (For Tech-Driven Enterprises):** Focused on improving security automation and digital transformation.
-

5. Competitive Differentiation: Why Al::Sec?

Unlike traditional AppSec tools (e.g., Snyk, Veracode, Checkmarx) that focus **only on vulnerability scanning**, Al::Sec **automates the entire AppSec workflow**, including **secure code reviews, compliance enforcement, and DevSecOps automation**.

- 🔪 **Zero Hallucinations:** Al::Sec is built on a deterministic AI model using **finite automata & DAG workflows**, ensuring security actions are predictable and reliable.
- 🔪 **Full AppSec Automation:** Goes beyond scanning—Al::Sec enforces security policies, automates vulnerability triage, and accelerates secure development.
- 🔪 **Seamless DevSecOps Integration:** Works within existing CI/CD pipelines (GitHub, GitLab, Jenkins, AWS CodePipeline).
- 🔪 **Enterprise-Ready LLM for On-Prem Deployment:** Al::Sec provides an optimized, **resource-efficient AI model** designed to run cost-effectively in enterprise data centers.
- 🔪 **Commercially Licensed AI Model:** Unlike other LLMs restricted to cloud use, Al::Sec offers a fully licensed on-prem solution.

How Al::Sec Outperforms ASOC, Snyk, and Other AppSec Tools

- ✅ **Al::Sec is not just a vulnerability scanner—it automates full security workflows, including remediation and policy enforcement.**
- ✅ **Zero AI hallucinations:** Unlike LLM-based tools that produce unreliable security recommendations, Al::Sec ensures deterministic security decisions.
- ✅ **Optimized for On-Prem:** Runs efficiently with reduced GPU and RAM costs, overcoming commercial AI licensing restrictions.
- ✅ **AI-Powered AppSec Engineer:** Al::Sec acts as a **full-time security engineer**, replacing manual AppSec processes that competitors still rely on humans to complete.

💡 *"Al::Sec is not just another security tool. It's an autonomous AppSec engineer that scales security without scaling headcount."*

6. Pricing & Adoption Model

- 📌 **Pricing Model:** Subscription-based AI-powered AppSec Engineer.
- 📌 **Cost:** \$80K–\$120K per year per AI agent (compared to **\$150K–\$250K per human AppSec engineer**).
- 📌 **Deployment:** Fully managed SaaS or on-prem integration.
- 📌 **Scalability:** Start with **1 AI agent**—expand to **5+ within 12 months** based on security needs.

💡 *"Al::Sec enables enterprises to scale AppSec without increasing headcount."*

7. The Investment Ask: Why Invest in Al::Sec?

- 💰 **Raising:** \$250K SAFE @ \$4M post-money valuation.
- 🎯 **12-Month Goal:** Reach \$2M ARR, onboard **10+ enterprise customers**.
- 📈 **Break-even in 12 months, \$50M ARR by Year 2, \$150M ARR by Year 3.**
- 📌 **Exit Strategy:** Acquisition by **Palo Alto, CrowdStrike, Wiz, or IPO within 5 years.**