Multi-Layer Defense Comparison

Security: ASR

Attack Success Rate (↓ better)

- SkillGuard (Pre-deploy): 25%
- AgentShepherd (Runtime): 15%
- Spider-Sense (Runtime): 5%
- Integrated (Both): 3%

Usability: FPR

False Positive Rate (↓ better)

- SkillGuard (Pre-deploy): 5%
- AgentShepherd (Runtime): 8%
- Spider-Sense (Runtime): 2%
- Integrated (Both): 3%

Performance: Latency

Latency Overhead % (↓ better)

- SkillGuard (Pre-deploy): 0.0%
- AgentShepherd (Runtime): 5.0%
- Spider-Sense (Runtime): 8.3%
- Integrated (Both): 10.0%