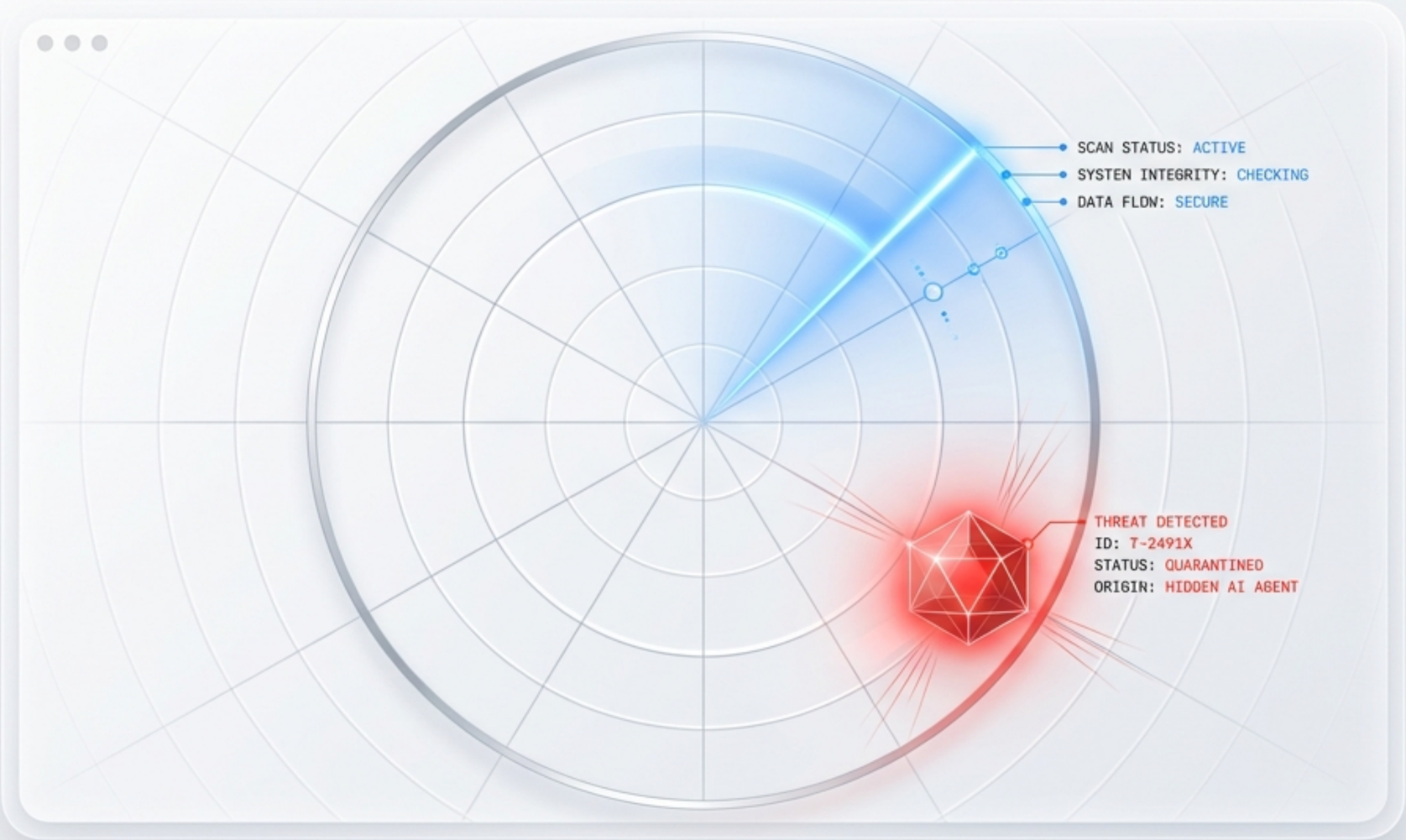
ClawSafe.net · 龙虾安全网

AI 智能体安全的战略切入与平台演进



智能体的爆发与失控

40%

企业应用正在快速引入特定任务 AI 智能体。

69%

组织怀疑或已有证据表明存在被禁止的公共 GenAI 使用。

57.4%

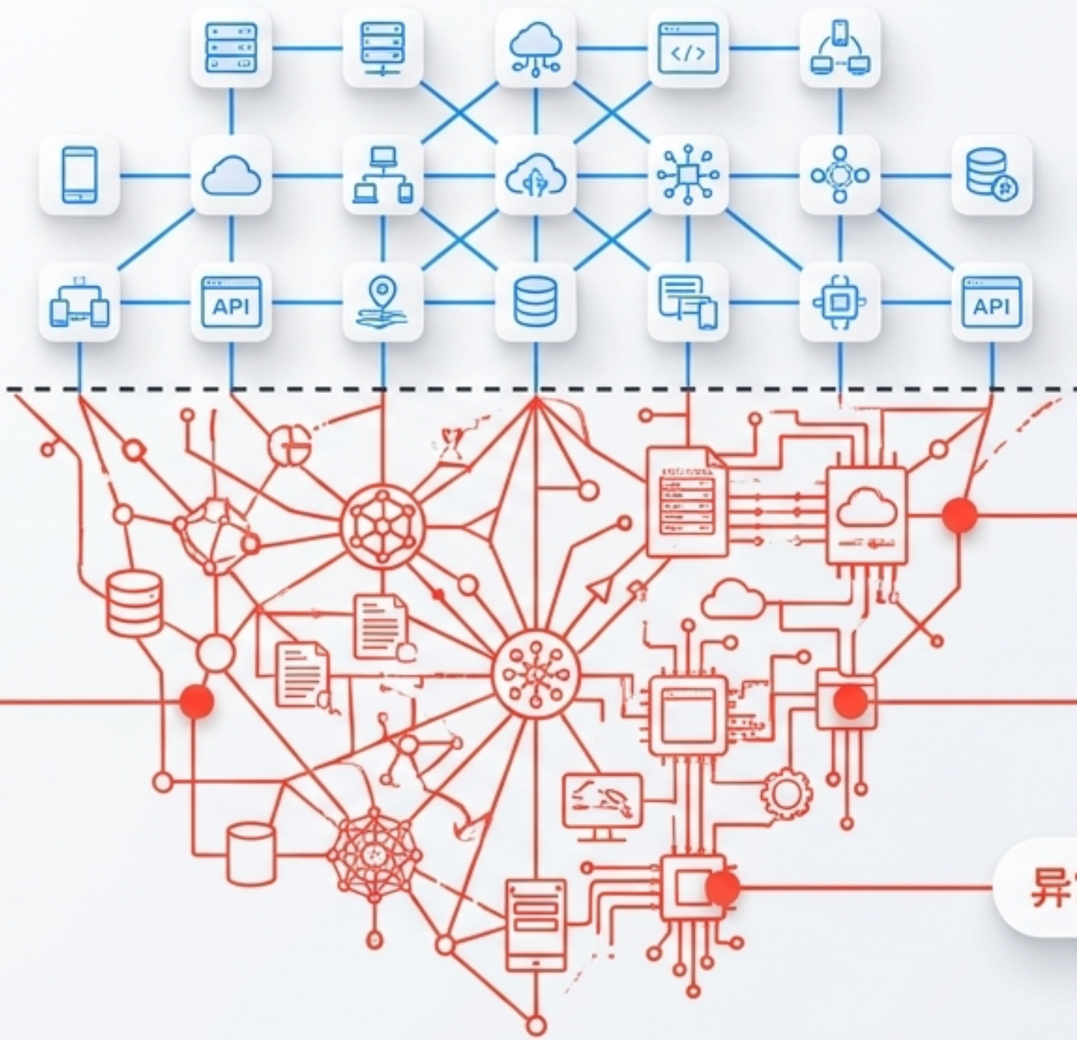
受访者将 observability（可见性）不足视为主要安全担忧。

影子 AI 已成为现实运营风险

已获批的企业应用与 API

传统 IT 治理边界

未纳管的开放式智能体
(Open-Agent)



后台持续运行

扩展的文件系统访问权限

异常 Skills 与可疑 Connectors

OpenClaw 的部署形态与暴露面

本地桌面

典型形态：个人 PC / Mac

安全暴露面

权限配置易出错；
数据直接贴近本机环境。

治理难度

极难进行团队统一治理。

专用设备

典型形态：Mac mini / 独立小主机

安全暴露面

长期在线；
与主力办公网络相连。

治理难度

需要持续的硬件与网络系统
隔离维护。

云端部署

典型形态：VPS / 1-Click / Cloud Mac

安全暴露面

网络暴露面最大；
高度依赖云商安全与 TLS。

治理难度

认证与日志合规要求极高。

先识别，再处置：化繁为简的安全闭环

1. 先发现风险

识别本机高风险 agent、异常 skill、可疑 connector 与隐藏自动化。

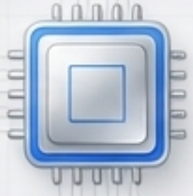
2. 再进入处置

明确风险后，进入 Pay to Delete / 删除协助，处理高意图处置需求。

3. 持续监控

逐步进入持续监控、历史记录、团队可见性与企业治理。

Scanner ID：像领取检测资格一样简单



个人单次版

一个 Scanner ID 对应一台设备的一次完整扫描。

US$3.99

一个 Scanner ID 对应一台设备的一次完整扫描。

购买 Scanner ID

家庭 5 台装

适合家庭成员共用，支持分享与集中查看。

US$15.99

适合家庭成员共用，支持分享与集中查看。

购买 Scanner ID

团队 25 台装

适合小团队批量分发、归档和后续升级。

US$69

适合小团队批量分发、归档和后续升级。

购买 Scanner ID

One-device-one-scan 明确计量体系：极易理解，无需预先理解复杂订阅架构，完美适配合规归档。

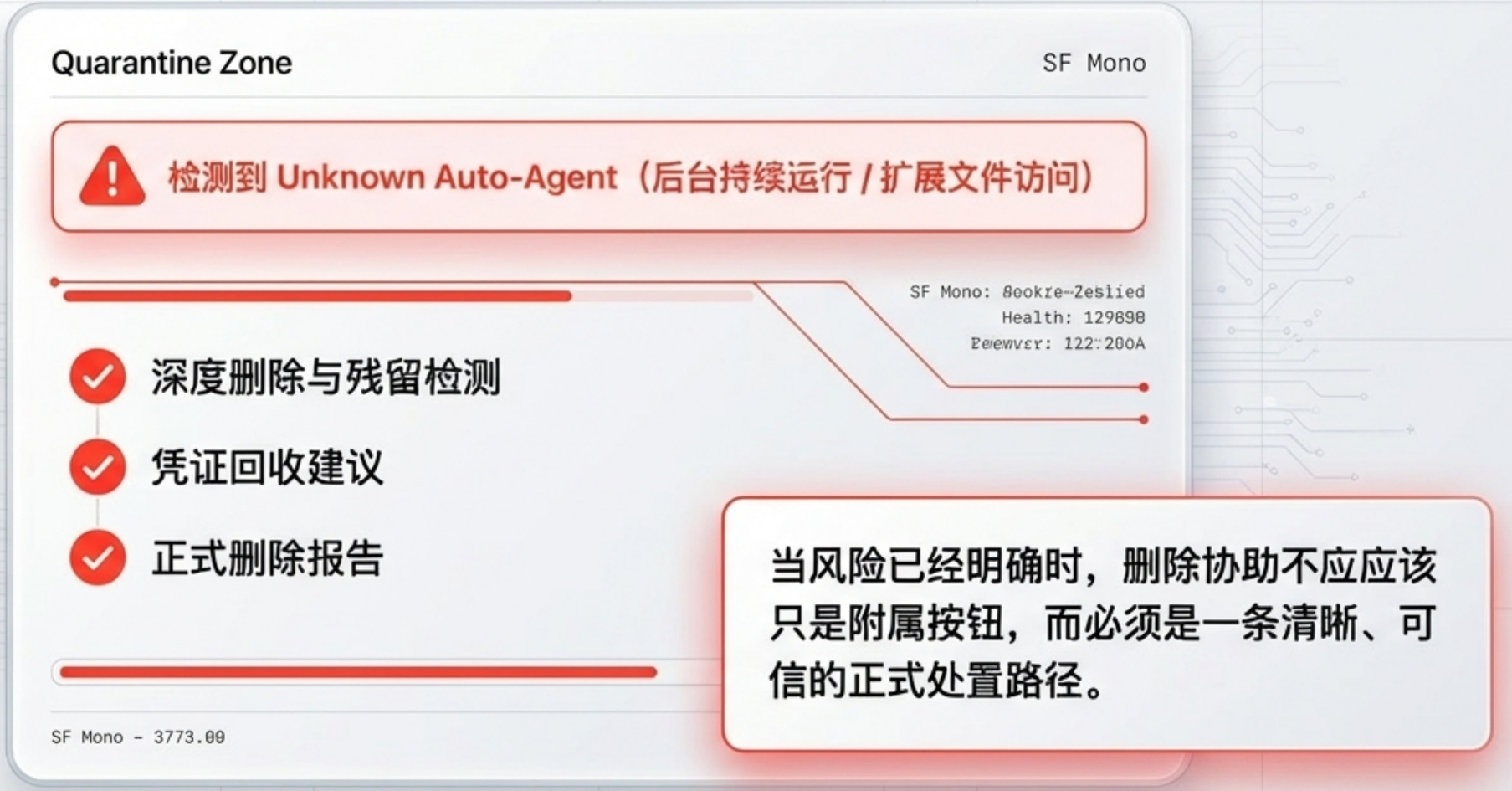
无摩擦的终端分发网络

Team 25-Pack

Premium digital stack of Scanner ID cards.

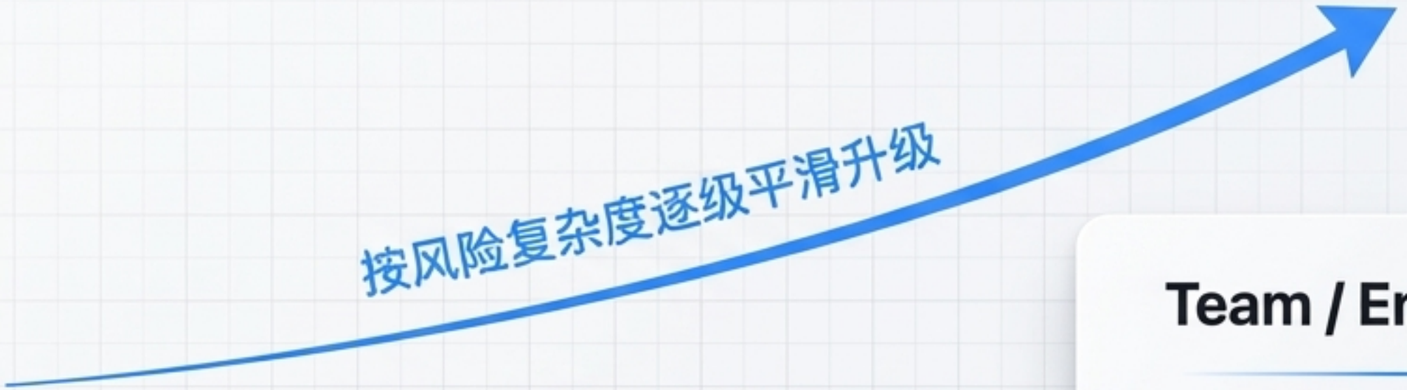
无需复杂的 SaaS 部署。通过批量分发 Scanner ID，即可在离散的员工设备上瞬间建立可追踪的安全合规网。

明确风险后的正式处置： Delete Room



覆盖全链路的三大产品矩阵

从个人发现到团队治理的无缝升级



Free

基础扫描、简版报告、有限删除建议。

Personal Pro

深度扫描、持续监控、历史记录、优先情报。

Team / Enterprise

多设备面板、批量扫描、团队告警、控制台与审计 API。

为什么市场需要独立的安全层?

	Promptfoo	Okta / Reco	ClawSafe.net + CybEye
设备侧发现与删除	—	—	✓
个人与家庭触达	—	—	✓
企业级治理与可见性	—	+	✓
Prompt / LLM 安全评测	+	—	✓

这是唯一跨四个能力辅控的平台，并跻行本地修瘦与企业审计。

从高转化切入到长期平台归宿

用消费级的高频痛点，漏斗式培育企业级的长期价值。

CybEye.net（长期治理归宿）

核心领导者介绍

Bing Liu - FirstAid 和 CyberDefender 首席软件架构师

Bing Liu 凭借在安全领域的深厚积累，将带领团队确保项目成功。他不仅是行业资深专家，在安全架构与风险管理方面拥有卓越领导力，更是安全技术演进的引领者，是项目成功的关键保障。