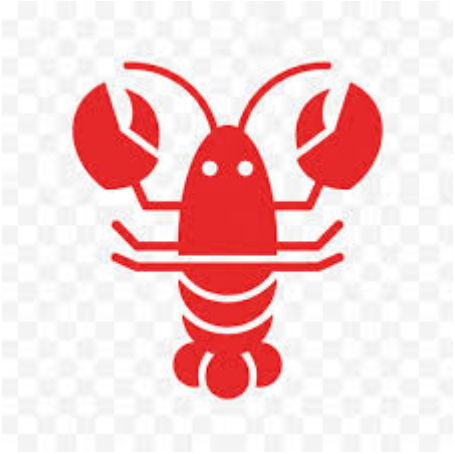
OpenClaw: The Future of Personal AI Agents

A Deep Dive for IT Management & Operations Teams



Presented by: Matthew Liu February 2026

Before We Begin: Two Critical Questions

A. Why You Need to Know OpenClaw

Reason	Impact
Fastest-growing GitHub repo	150K+ stars; your team will discover it
Users deploying without IT approval	Shadow IT risk is real
Represents a paradigm shift	From chatbots to autonomous agents
Enterprise implications	Security, compliance, cost considerations
Industry direction	Anthropic's Cowork followed this pattern

> "If you don't understand it, you can't govern it."

B. Why You Should Be Very Careful

Risk	Severity	Description
Full system access	Critical	Reads/writes files, executes shell commands
API key exposure	Critical	Keys stored on server, potential leakage
Prompt injection	High	Malicious inputs can hijack agent behavior
24/7 autonomous operation	High	Actions taken without human oversight
Early-stage software	Medium	Vulnerabilities actively being discovered

> **Feb 2026**: Critical LFI vulnerability discovered in OpenClaw

---

Meet the Creator

Peter Steinberger

- **Austrian Software Engineer**
- Founder of **PSPDFKit** (PDF SDK used by millions)
- Serial open-source contributor
- Built OpenClaw in late 2025

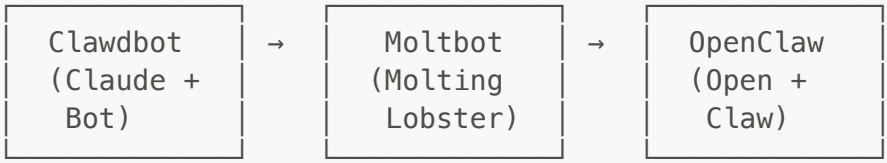
Philosophy

> "A personal AI assistant that feels less like a chatbot and more like a true digital employee."

Find him on X: @steipete

The Evolution Story

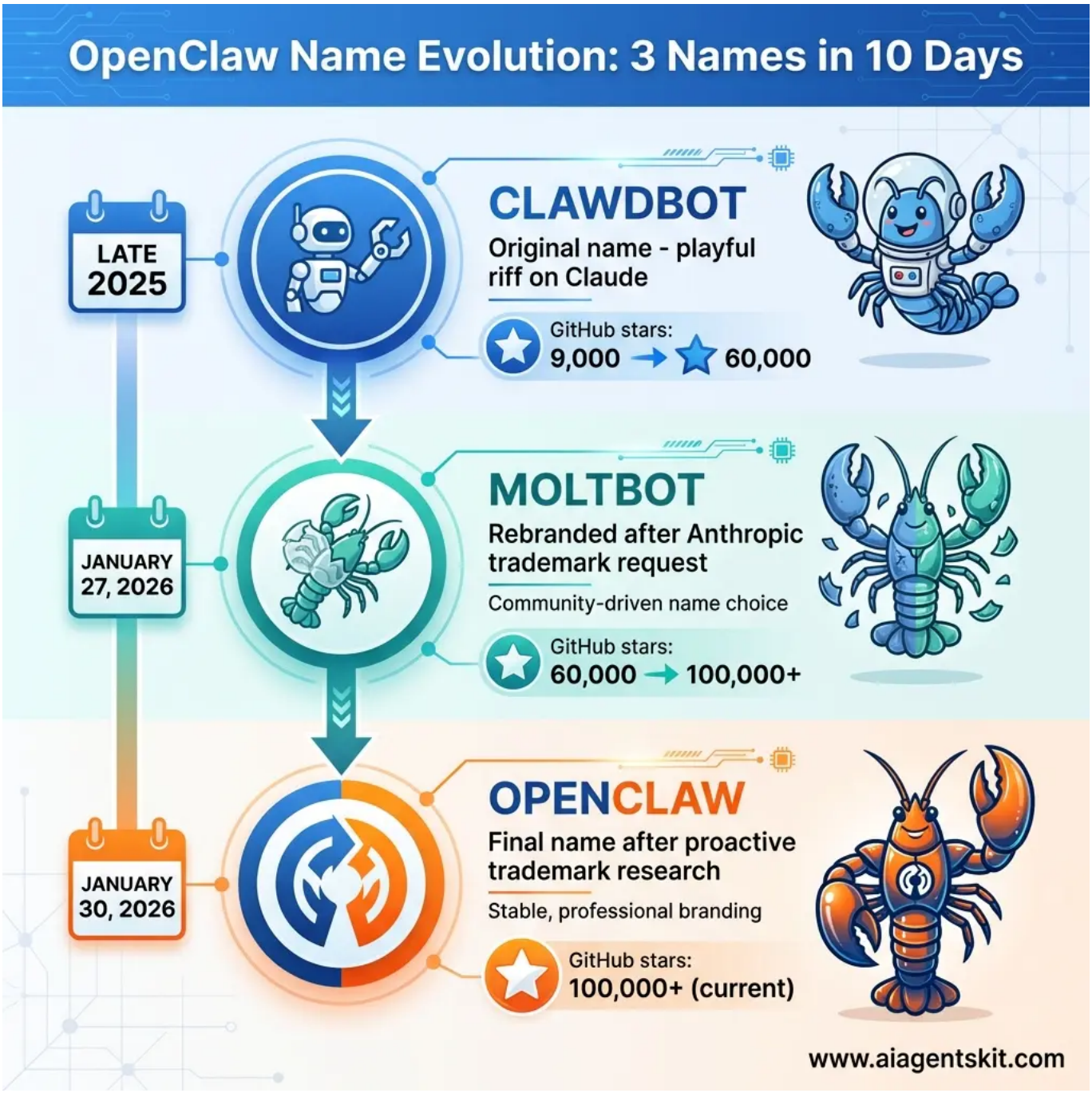
From Clawdbot to Moltbot to OpenClaw



The Name Changes

Date	Name	Reason
Nov 2025	**Clawdbot**	"Claude" + "Bot" - Initial launch
Jan 2026	**Moltbot**	Anthropic sent polite trademark request
Jan 30, 2026	**OpenClaw**	Final rebrand after trademark search

---



The Chaotic Rebrand Day

Peter's words on the Moltbot → OpenClaw rebrand:

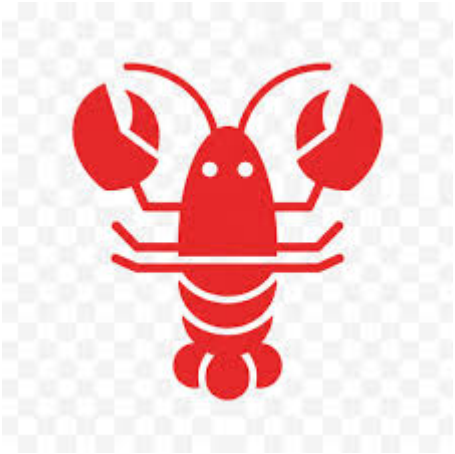
> "Everything that could have gone wrong today went wrong"

- X account briefly hijacked by crypto sellers
- Community confusion across three names
- Documentation scattered

But the project grew despite this:

- **40,000+ GitHub stars** in under 3 months
- Described as "one of the fastest-growing repos ever"

Why "Space Lobster" Mascot?



The lobster represents:

- **Molting**: Continuous evolution and growth
- **Claws**: Capability to take action
- **Resilient**: Survives trademark changes
- **Open**: Embracing the community

> Molty the Space Lobster became the beloved mascot

What Makes OpenClaw Unique

OpenClaw vs. The Competition

Feature	OpenClaw	Claude Code	Manus AI
Hosting	Self-hosted	Desktop app	Cloud
Data Sovereignty	100% yours	Local	Cloud
24/7 Operation	Yes	Manual	Limited
Multi-Channel	Telegram, WhatsApp, Discord, Slack	None	Chat only
Persistent Memory	Yes	Session-based	Cloud-stored
Open Source	Yes	No	No
Cost Model	API usage only	$100-200/mo	Subscription

The "Digital Employee" Philosophy

What makes OpenClaw feel like a colleague, not a chatbot:

1. Persistent Memory

- Remembers conversations across sessions
- Recalls your preferences and past requests
- Builds context over time

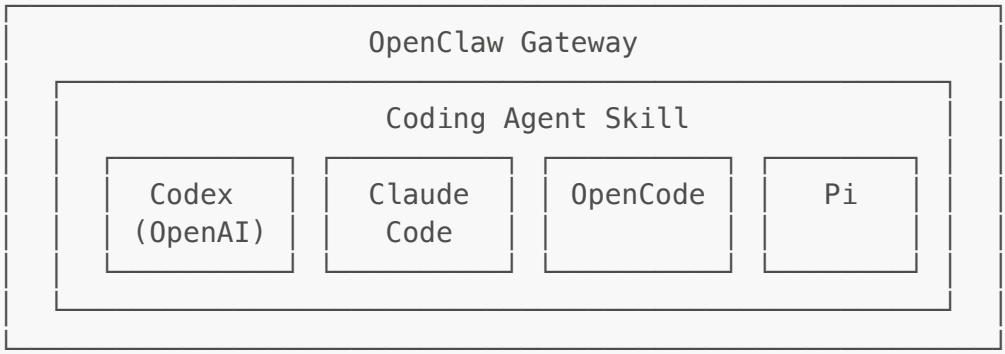
2. Local Privilege

- Full filesystem access (with permissions)
- Can execute shell commands
- Integrates with local tools and services

3. Real Agentic Behavior

- Works until objective is complete
- Breaks complex tasks into steps
- Makes autonomous decisions

Relationship with Claude Code



OpenClaw can **orchestrate** Claude Code as one of its coding tools:

- Code generation, review, debugging, refactoring
- Uses `claude` CLI as a background process
- Choice of AI coding tools per task

How OpenClaw Inspired Claude Cowork

The Pattern Anthropic Noticed

Users were adapting **Claude Code** (developer tool) for non-technical tasks:

- Vacation research
- Expense management
- File organization

Anthropic's Response: Claude Cowork (Jan 2026)

> "Claude Code for the rest of your work"

Feature	OpenClaw	Claude Cowork
Released	Nov 2025	Jan 2026
Approach	Gateway + Skills	Desktop Agent
File Operations	Yes	Yes
Multi-channel	Yes	No
Self-hosted	Yes	No

Why OpenClaw Became Popular

The Perfect Storm

1. **180x Efficiency Claims** — Viral demos showing massive productivity gains
2. **"It Just Keeps Working"** — Unlike chat, it continues until done
3. **Community Enthusiasm** — Hacker News, Reddit, X/Twitter, TikTok
4. **Open Source** — Full transparency, community contributions
5. **Developer First** — Built by developers, for developers
6. **Multi-Platform** — Works where your team already communicates

---

Live Demos & Use Cases

Demo Categories

Category	Examples
Information Assistant	RSS feeds, news briefing, research
Communication Hub	Multi-channel messaging, email management
Development Buddy	Code review, PR analysis, coding agent
System Administration	Server setup, file management, automation
Content Creation	TTS, document creation, Notion integration
Smart Automation	Scheduled tasks, cron jobs, monitoring

Demo 1: Daily Tech Brief to WhatsApp

Setup RSS Feeds → Automatic Daily Summary

Feeds Configured:

- MIT Technology Review
- Synced Review (机器之心 - Chinese AI)

- Hacker News
- OpenAI Blog

Result:

- Daily brief at 8:00 AM China time
- Top 5 articles summarized
- Delivered directly to WhatsApp

"Good morning! Here are 5 new articles from your feeds..."

Demo 2: Multi-Channel Communication

X/Twitter Integration

OpenClaw can:

- Read tweets by URL or ID
- Search Twitter content
- Access home timeline
- View user tweets
- Access bookmarks and likes

Other Channels

- **Telegram**: DMs and groups
- **Discord**: DMs and servers
- **Slack**: DMs and channels
- **WhatsApp**: Personal DMs
- **iMessage**: Mac-based messaging

Demo 3: Coding Agent Integration

Supported Coding Tools

Tool	Provider	Installation
`codex`	OpenAI	`npm install -g @openai/codex`
`claude`	Anthropic	`npm install -g @anthropic-ai/claude-code`
`opencode`	OpenCode	Official docs
`pi`	Mario Zechner	`npm install -g @mariozechner/pi-coding-agent`

Capabilities

- Code generation & bug fixes
- Code review & PR analysis
- Debugging & refactoring

- Project scaffolding

Demo 4: Research Assistant

Camera Recommendation Example (Chinese)

When asked about RTSP/ONVIF cameras:

OpenClaw researched and provided:

- TP-LINK models (¥100-150)
- 360 cameras (¥80-120)
- Hikvision options (¥150-200)
- Dahua recommendations (¥120-180)

Including:

- Price comparisons
- Feature analysis
- RTSP URL formats
- Setup instructions

Demo 5: Text-to-Speech (Multi-language)

Chinese TTS Demonstration

Components Automatically Downloaded:

- Runtime environment
- Chinese model (60MB)
- Phoneme dictionary (cmn_dict)

Result:

- Natural-sounding Chinese voice
- Delivered via WhatsApp audio message

Also demonstrated:

- Hamlet's soliloquy in English
- "To be or not to be..." as audio

Demo 6: Notion Integration

Creating Content via API

OpenClaw created:

- Notion workspace integration

- Pages with embedded content
- YouTube video embeds
- Dynamic content updates

Security:

- OAuth integration secret
- Read/write content capabilities
- Workspace-scoped access

Demo 7: System Administration

Server Configuration Tasks

OpenClaw helped with:

- Caddy web server configuration
- File copying and deployment
- `systemctl` service management
- Configuration file editing

Demonstrated Commands:

```
cp /home/admin/clawd/xxx /var/www/openclaw-web/
cp /home/admin/clawd/Caddyfile_modified /etc/caddy/Caddyfile
sudo systemctl restart caddy
```

Demo 8: Email & Document Processing

Security Questionnaire Analysis

Email from: Michelin's Security Team **Subject:** Customer Service AI LLM Security Review

OpenClaw extracted 7 key questions:

1. Data storage location & encryption
2. Voice data handling & model training
3. Audit logs availability
4. SLA & compensation
5. Pen testing reports
6. Compliance certifications (ISO 42001)
7. AI-BOM (supply chain transparency)

Action: Offered to download and analyze attached PDF

Demo 9: GUI Remote Access (Xpra)

Running GUI Applications Remotely

Demonstrated:

- `xeyes` — Classic X11 application
- Running via Xpra remote display
- GUI accessible from OpenClaw chat

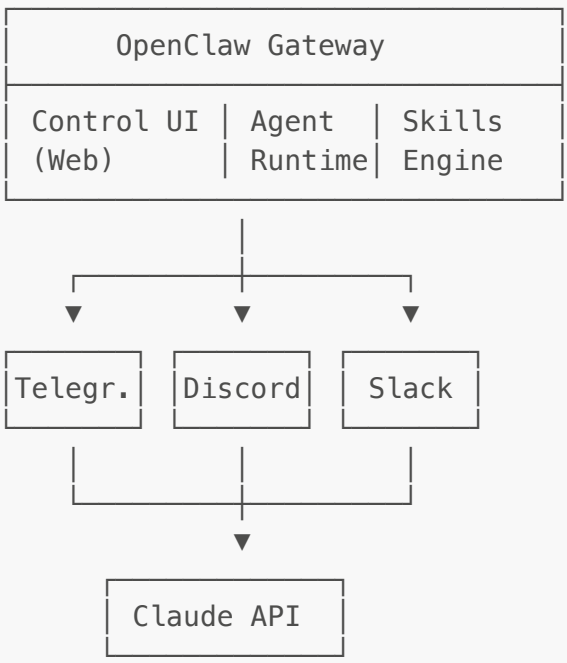
Use Case:

- Remote server management
- Visual application control
- Headless server GUI access

Architecture Deep Dive

Architecture Overview

High-Level Architecture



Key Components

Component	Purpose
Gateway	Routes messages, manages sessions
Control UI	Web-based admin dashboard

Component	Purpose
Agent Runtime	Claude Opus 4.5 / LLM brain
Skills Engine	50+ extensible modules
Device Pairing	Explicit approval per device
Channels	Multi-platform messaging

Skills System

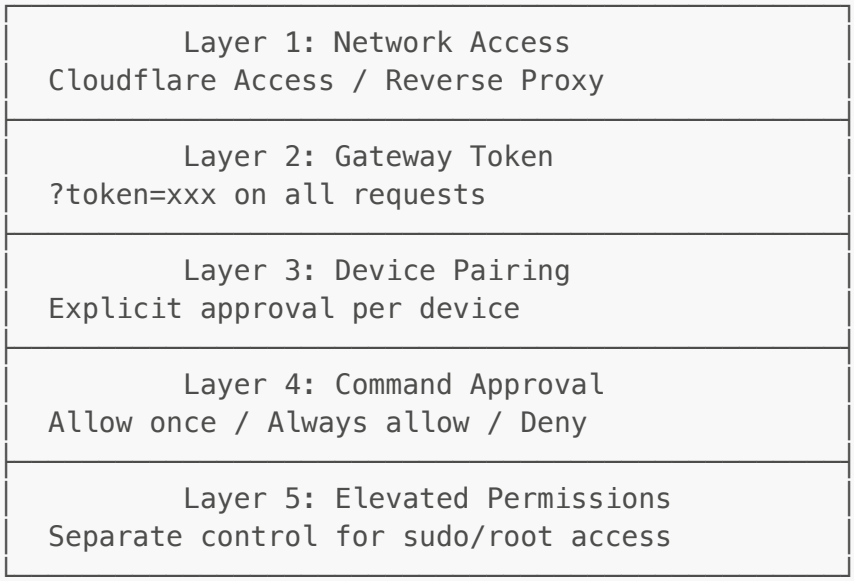
Built-in Skills (50+)

Category	Skills
Communication	WhatsApp, Telegram, iMessage, Discord, Slack
Productivity	Calendar, Notes, Tasks, Email
Development	GitHub, Coding Agent, Code Review
Media	TTS, Image Generation, Video
Automation	RSS Feeds, Browser Control, File Management
Integration	Notion, camsnap (RTSP cameras)

Extensibility

- ClawdHub: Skills marketplace
- Custom skill development
- Community contributions

Security Layers



Elevated Permissions System

What It Controls

Setting	Meaning
`tools.elevated.enabled`	Master switch for elevated execution
`tools.elevated.allowFrom.webchat`	Allow webchat to use elevated commands
`agents.list[].tools.elevated.*`	Per-agent overrides

With Elevated ON:

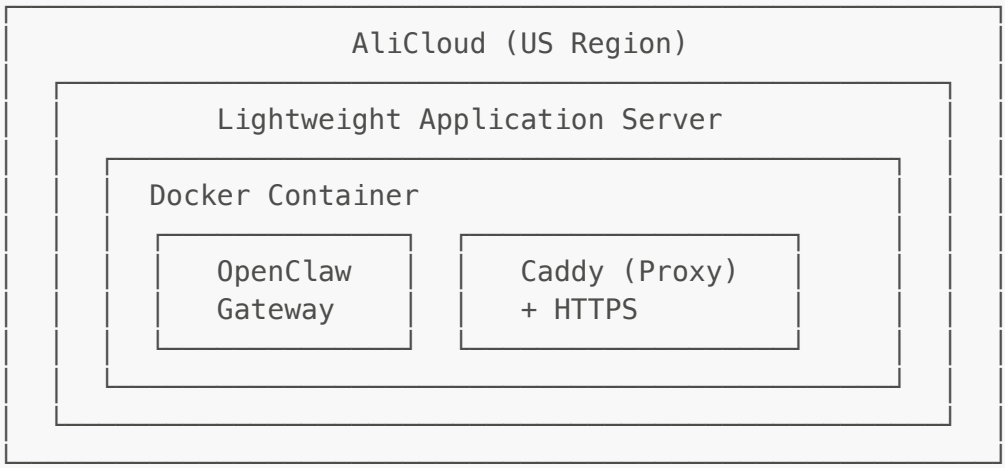
- `dnf install ...`
- `systemctl restart ...`
- Any `sudo` command

Without It:

Even `sudo echo "hi"` fails

My Setup: AliCloud Light App Server

Deployment Architecture



Why AliCloud US Region?

Factor	Reason

Factor	Reason
Latency	Closer to Anthropic API servers
Cost	Lightweight server: ~$5-10/month
Availability	24/7 uptime for always-on agent
Flexibility	Full root access for customization
Region	US for API performance

My Configuration

- Lightweight Application Server
- CentOS / Rocky Linux
- Docker for containerization
- Caddy as reverse proxy with auto-HTTPS
- Persistent storage for memory

Setup Steps

1. **Provision Server**
    - AliCloud Lightweight App Server (US region)
    - 2 vCPU, 4GB RAM recommended
2. **Install Dependencies**

```
dnf install docker nodejs npm
systemctl enable docker
```

3. **Deploy OpenClaw**

```
git clone https://github.com/openclaw/openclaw
npm install
```

4. **Configure Caddy**
    - Reverse proxy to localhost
    - Automatic HTTPS certificates
5. **Security Hardening**
    - See security checklist (next section)

Security Risks & Mitigations

Security Hardening Checklist

Item	Status	Description
Reverse Proxy Configured	✅	Gateway bound to localhost only
Firewall Ports Hardened	✅	Unnecessary ports closed
Device Pairing Enabled	✅	Explicit approval required
Filesystem Permissions	✅	Strict permissions for sensitive data
OAuth Authentication	✅	OAuth for locally hosted pages
Local Embedding Model	✅	Using local LLM for embeddings

Critical Security Risks

1. Prompt Injection (HIGH)

Risk: Malicious content in messages can hijack agent behavior

Mitigation:

- Input validation
- Sandboxing sensitive operations
- Human approval for critical actions

2. API Key Exposure (HIGH)

Risk: Anthropic API keys stored on server

Mitigation:

- Secrets management (not in config files)
- Regular key rotation
- Usage monitoring and alerts

Critical Security Risks (continued)

3. Arbitrary Local File Inclusion (CRITICAL)

Feb 2026 Discovery: LFI vulnerability found

Risk: Attackers could read arbitrary files from server

Mitigation:

- Keep OpenClaw updated
- Apply security patches immediately

- Monitor security advisories

4. Unauthorized Access (MEDIUM)

Risk: Unauthorized users gaining access

Mitigation:

- Gateway token authentication
- Device pairing requirement
- Cloudflare Access for admin routes

Operational Risks

Risk	Description	Mitigation
Cold Starts	Cloud deployment delays	Keep-alive configuration
Rate Limits	API throttling	Caching, request optimization
Cost Overruns	API usage costs	Budget alerts, monitoring
Data Loss	Ephemeral storage	R2/persistent backup
LLM Hallucinations	Incorrect actions	Human review for critical tasks

---

Best Practices

✅ DO

- Enable device pairing for authentication
- Use persistent storage (R2 backup)
- Set up Cloudflare Access for admin routes
- Monitor API usage and costs
- Keep API keys secure and rotate regularly
- Review command approvals carefully

❌ DON'T

- Use in production without security review
- Expose gateway without authentication
- Grant unrestricted device access
- Skip input validation
- Store sensitive data without encryption

Claude Cowork & The Future

Claude Cowork: Born from OpenClaw Patterns

Timeline

```
Nov 2025: OpenClaw (Clawdbot) launches
          ↓
Dec 2025: Users adapt Claude Code for non-coding tasks
          ↓
Jan 2026: Anthropic launches Claude Cowork
          "We built it in 10 days, largely using Claude Code"
```

What Anthropic Learned

1. Users want **autonomous file operations**
2. **Persistent context** is critical
3. Multi-step tasks need **agentic behavior**
4. Security must be **sandboxed**

OpenClaw vs Claude Cowork Today

Aspect	OpenClaw	Claude Cowork
Target User	Developers, Power Users	Knowledge Workers
Hosting	Self-hosted	Desktop (Mac only)
Price	API costs (~variable)	$100-200/month
Channels	Multi-platform	Local files only
Skills	50+ extensible	Built-in only
24/7 Operation	Yes	Manual
Open Source	Yes	No

The Future of Agentic AI

2026 Predictions

1. **Hybrid Deployments** — Enterprise: Claude Cowork for workers; Power users: OpenClaw for automation
2. **Multi-Agent Orchestration** — Agents collaborating via MCP protocol; OpenAgents network integration
3. **Security Maturation** — Enterprise-grade sandboxing; Compliance frameworks for AI agents
4. **Skill Ecosystems** — ClawdHub growth; Enterprise skill libraries

---

What This Means for IT

Opportunities

- **Automation**: Reduce manual IT tasks
- **Monitoring**: 24/7 intelligent alerting
- **Support**: AI-assisted troubleshooting
- **Integration**: Connect disparate systems

Challenges

- **Governance**: How to manage shadow AI agents
- **Security**: New attack surfaces
- **Compliance**: Data handling requirements
- **Skills**: Training teams on agentic AI

Key Takeaways

Summary

OpenClaw is...

1. **Revolutionary** — First mainstream local-first AI agent
2. **Powerful** — Full system access, multi-channel, persistent
3. **Risky** — Security vulnerabilities, requires careful setup
4. **Influential** — Inspired Anthropic's Claude Cowork
5. **Open** — Community-driven, transparent development

For IT Leaders

- Understand before governing
- Prepare security policies now
- Consider controlled pilots
- Train teams on agentic AI concepts

Resources

Resource	URL
GitHub	github.com/openclaw/openclaw
Documentation	docs.clawd.bot
Skills Registry	clawdhub.com
Community	Discord / X (@steipete)
Security Advisories	github.com/openclaw/openclaw/security

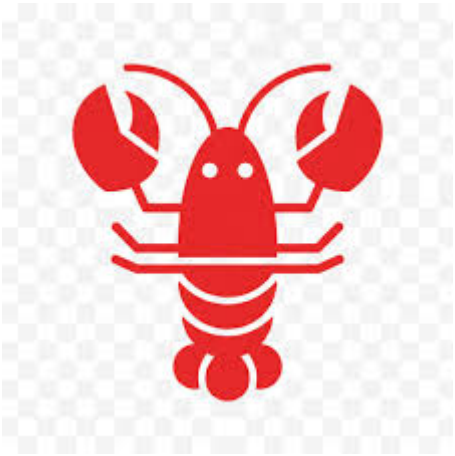
Q&A

Questions?

Thank You

Contact:

- Presenter: Matthew Liu
- Date: February 2026



OpenClaw — Your Personal AI Assistant

Appendix

Appendix A: Installation Quick Start

```
# Clone repository
git clone https://github.com/openclaw/openclaw
cd openclaw

# Install dependencies
npm install

# Configure (edit config files)
cp config/example.yaml config/local.yaml
# Edit local.yaml with your API keys

# Start gateway
npm start

# Access Control UI
open http://localhost:3000
```

Appendix B: Useful Commands

Command	Description
`moltbot gateway restart`	Restart the gateway service
`moltbot config set <key> <value>`	Update configuration
`moltbot skills list`	List available skills
`moltbot skills enable <name>`	Enable a skill
`clawdhub install <skill>`	Install skill from registry

Appendix C: Interesting Online Cases

Viral Demos

1. **Peter's Original Demo** — "72 Hours That Changed Everything"
2. **Data Engineering Use Case** — Medium article on real-world testing
3. **Security Warning Video** — "Don't Run OpenClaw (Moltbot) Yet"

Community Contributions

- Portuguese explanation videos
- Chinese deployment guides
- Enterprise integration patterns

Appendix D: Comparison Matrix

Feature	OpenClaw	Claude Code	Claude Cowork	Manus AI
Self-hosted	✅	❌	❌	❌
Open Source	✅	❌	❌	❌
Multi-channel	✅	❌	❌	❌
24/7 Autonomous	✅	❌	❌	✅
Persistent Memory	✅	❌	❌	✅
File Operations	✅	✅	✅	❌
Coding Focus	✅	✅	❌	❌
Enterprise Ready	⚠	✅	✅	✅