CLAW ECOSYSTEM MONTHLY

JUNE 2026

003

WHAT CHANGED IN MAY 2026 AND WHY IT MATTERS TO YOU

May 2026 is the month the outside world showed up. Professional investors, major security organizations, and the biggest names in technology all turned their attention to a space that started as a developer side project. Whether you self-host, use a managed service, or are still deciding, this month changes what those choices mean. Everything in this issue is labeled by tier so you can jump straight to what applies to you and skip the rest.

THIS ISSUE COVERS:

- **NanoClaw: FIRST FUNDED CLAW** $12M seed, $62M valuation, Docker/Vercel/HuggingFace CEO backing (pg 5)
- **Claw Chain: NAMED ATTACK** 4 linked security flaws, named by researchers, covered in major cybersecurity news (pg 8)
- **Config Mutation CVEs: MAY 11** 5 security flaws published in a single day, biggest single-day disclosure to date (pg 9)
- **Anthropic June 15 Billing Change** A monthly credit replaces unlimited subscription use for all Claude OpenClaw user (pg 4)
- **OpenClaw v2026.5.26** Discord voice, Meeting Notes, 4,100x model speedup, Node.js 22.16+ (pg 6)
- **375,000+ GitHub Stars** Up from 320K in April, · 14,706+ ClawHub skills · 1,103 confirmed malicious (pg 3)
- **Watch List Updates** (still on Watch List) NemoClaw still Early Preview · ClawX v0.4.6 · KiloClaw (pg 7)
- **SkillSpector + Skill Card** Two new ClawHub safety features launched May 31 (pg 9)

THE BOTTOM LINE

Tier 1 self-hosted users have two security patches to apply this week. The flaws they fix are serious and now documented in enterprise security research. Tier 2 managed users are largely covered on security and should focus on the June 15 billing change. Everyone using Claude through OpenClaw needs to understand the new cost model before June 15 arrives.

ISSUE 003

JUNE 2026

SUBSCRIBER EDITION

THE 60-SECOND BRIEF

EVERYTHING THAT CHANGED IN MAY 2026

First claw gets professional investor funding. First named security attack chain. End of the billing cost gap. Google enters the race.

NanoClaw raised $12M from professional investors (Docker, Vercel, Monday.com, Slow Ventures, and the CEO of HuggingFace, one of the most influential AI platforms online) at a $62M company valuation. This is the first claw bot to receive real investor backing. Researchers named four linked security flaws 'Claw Chain'. This was covered by Dark Reading, The Hacker News, and SentinelOne. This is the first time an OpenClaw security issue has appeared in major cybersecurity news. Google's cybersecurity research team (GTIG) officially confirmed ClawHub is being used to distribute harmful software. On May 11, five security flaws were published in one day. Anthropic announced that from June 15, automated agent use moves from included subscription use to a measured monthly credit limit. OpenClaw shipped Discord voice and Meeting Notes features, and ClawHub launched two new safety tools: SkillSpector and Skill Cards.

375K+
GitHub Stars
Was 320K in April;
Fastest-growing OSS project ever

14,706+
ClawHub Skills
1,103 confirmed malicious 7.5%
RankClaw / 36.82% ToxicSkills

38
Published CVEs
Claw Chain + May 11 batch
Total through May 2026

$12M
NanoClaw Raised
$62M valuation First funded claw

WATCH LIST STATUS — JUNE 2026 EDITION

NemoClaw	[■ STILL EARLY PREVIEW]	NVIDIA docs still read "alpha software — do not use in production" as of May 27.
KiloClaw	[★ WATCH LIST]	$9/mo compute + zero-markup API. GitLab co-founder backing. Beta status unchanged
ClawX	[★ APPROACHING]	v0.4.6 (May 20). Four versions in 11 days. Still pre-1.0. Full profile when v1.0
OpenClaw Desktop	[★ WATCH LIST]	v0.7.0, pre-release, Windows-primary. Less frequent updates than ClawX.

T1 EXECUTOR | T1 EDGE | T1 SECURITY | T1 MEMORY | T2 MANAGED | T3 GUI | COMPANION

clawecosystem.co/glossary
clawecosystem.co/cost-calculator
clawecosystem.co/matrix

MAJOR UPDATES

BILLING & COST INTELLIGENCE — THE JUNE 15 ANTHROPIC CHANGE

IMPORTANT: Anthropic billing changes on June 15, 2026. Affects every OpenClaw user using Claude

Before June 15: Many users ran OpenClaw on Claude using their subscription at a flat monthly rate.

After June 15: When your OpenClaw agent does automated work, it now draws from a separate monthly credit allowance, priced at Claude's standard pay-per-use rates. These credits do not carry over to the next month. Normal back-and-forth conversations with Claude are not affected, only automated agent activity counts against this limit.

This is the most significant cost change since the April 4, 2026 subscription policy change. For users on the Max 20x ($200/month) plan who were running OpenClaw at scale, the new ceiling is $200 in agent credits per month at standard API list rates — versus the effectively uncapped workload that was possible before. Interactive Claude chat and Claude Code interactive sessions are NOT affected — only automated and agent use is metered. You can opt in to overflow billing for uncapped access at direct API rates. Default: overflow is off. The True Cost Calculator at clawecosystem.co/cost-calculator has been updated with all June 15 scenarios.

ANTHROPIC AGENT SDK CREDIT POOLS — EFFECTIVE JUNE 15, 2026

PLAN	AGENT CREDIT POOL	NOTES
Pro ($20/month)	$20 in agent credits / month	Standard API rates. Credits do not roll over.
Max 5x ($100/month)	$100 in agent credits / month	You can choose to allow charges above this limit — but you must actively turn this on. It is off by default.
Max 20x ($200/month)	$200 in agent credits / month	Hard ceiling for subscription-based agent use.
Team ($30/seat/month)	$100/seat in agent credits / month	Most affected tier for org deployments.
Enterprise	$200/seat in agent credits / month	Same ceiling as Max 20x per seat.

> **THE COST ADVANTAGE IS GONE. IN EARLY 2026, A $20 MONTHLY SUBSCRIPTION COULD BE USED VIA OPENCLAW TO RUN AI AGENT WORK THAT WOULD NORMALLY COST HUNDREDS OF DOLLARS AT STANDARD PAY-PER-USE RATES.**
>
> *VentureBeat, May 2026*

COMPETITIVE SIGNAL — GOOGLE GEMINI SPARK AT I/O

At its annual developer event (I/O) on May 19, Google announced Gemini Spark: an always-on AI agent running 24/7 in Google's cloud, built directly into Gmail, Docs, Sheets, Slides, and Calendar. Included in the $200/month AI Ultra plan (Google lowered the price from $250 at the same event). Notably, Google referenced OpenClaw in its own official documentation as a comparable platform, which is a significant public acknowledgment. Three of the world's largest technology companies are now in the personal AI agent space: Microsoft (ClawPilot, going public June 2), Google (Gemini Spark), and OpenAI (Workspace Agents).

T1 EXECUTOR | T1 EDGE | T1 SECURITY | T1 MEMORY | T2 MANAGED | T3 GUI | COMPANION

clawecosystem.co/glossary
clawecosystem.co/cost-calculator
clawecosystem.co/matrix

FEATURE UPDATES

Feature updates are labeled by tier. If it doesn't apply to your tier, skip it. **Tier 2** and **Tier 3** users: your provider or the app update handles most of these automatically.

Open Claw v2026.5.26 [TIER 1 EXECUTOR — LATEST STABLE]

Discord Voice — Agent Joins Your Calls

The agent now joins Discord voice calls automatically with live steering and cancellation from Web UI. Wake-name is more tolerant. For anyone using Discord for team coordination, this is the most significant usability change in months.

Meeting Notes Plugin — Your Agent Now Captures Information Without Being Asked

Auto-start capture, manual transcript imports, and Discord voice as the first live source. Access it from OpenClaw or type 'openclaw meeting-notes' in your terminal (the text-command window on your computer). This is the first time OpenClaw can capture information in the background without you asking it to. More sources beyond Discord voice are planned.

The AI Model List Now Loads 4,100 Times Faster

The screen showing available AI models previously took about 20 seconds to load. It now loads in milliseconds, fixed by pre-loading your account connection details when the app starts, rather than each time you open the model list. If you manage many different AI service connections, this change alone makes the update worthwhile.

IMPORTANT: Check Your Software Version Before Updating OpenClaw

OpenClaw now requires a newer version of Node.js (the software engine it runs on. Think of it as the engine under the hood) version 22.16 or higher. If you update OpenClaw without checking first, it will stop working on startup. To check: open your terminal and type 'node --version'. If the number shown is below 22.16, update Node.js first. Not sure how? Ask your IT person or hosting provider. It is a common, quick step.

Webhook Security Audit Flag

Running 'openclaw security audit' now finds a specific hidden problem: if any of your automatic notification connections between apps (called webhooks. For example, a message that fires when a new email arrives) are sharing the same password as your main OpenClaw login, your credentials could be exposed with no visible sign. Run this command, review what it finds, and change any shared passwords it flags.

DigitalOcean 1-Click OpenClaw Droplet [TIER 1 DEPLOYMENT — NEW MAY 22]

Security-Hardened Self-Hosting in Under 60 Seconds

DigitalOcean (one of the most popular cloud server companies) launched an official one-click OpenClaw server setup on May 22. It creates a ready-to-use server with security measures already built in, no manual configuration required. This makes Tier 1 self-hosting significantly more accessible.

ClawHub Safety Features [ALL TIERS — NEW MAY 31, 2026]

SkillSpector — Automated Pre-Marketplace Scanner

An automated safety scanner built into ClawHub that checks every skill for hidden instructions and risks before making it available to download. It works alongside VirusTotal (a free Google service that checks files using 70+ security tools). Community shorthand: 'Did it pass SkillSpector?' means 'is it safe to install?' You can see the result on every skill's page in ClawHub. Check it every time before installing.

Skill Card — Documentation for Every Skill

A standardized documentation card shipping with every ClawHub skill: what it does, where it came from, VirusTotal scan result, and SkillSpector status. The first thing to check before installing anything from the store. Make reading the Skill Card a non-negotiable step.

NemoClaw [TIER 1 SECURITY LAYER — ⚠ EARLY PREVIEW (STILL ALPHA — DO NOT DEPLOY IN PRODUCTION)]

⚠ Status Unchanged — Two Claw Chain CVEs Target This Bot's Sandbox

NVIDIA's own documentation still reads 'alpha software. Do not use in production' as of May 27, 2026. Alpha means it's a first-stage experimental version, not ready for real use. Even more importantly: two of the four Claw Chain security flaws specifically target the security isolation layer that NemoClaw relies on. If you have any version of NemoClaw running, confirm that OpenClaw has been updated to version 2026.4.22 underneath it.

T1 EXECUTOR | T1 EDGE | T1 SECURITY | T1 MEMORY | T2 MANAGED | T3 GUI | COMPANION

clawecosystem.co/glossary
clawecosystem.co/cost-calculator
clawecosystem.co/matrix

WATCH LIST

This month has four items on watchlist: NemoClaw GA (Tier 1), KiloClaw (Tier 2), ClawX and OpenClaw Desktop (Tier 3).
They are classified by the tier they would join once they qualify. If it doesn't apply to your tier, skip it.

NEMOCLAW GA — NVIDIA'S ENTERPRISE SECURITY STACK — would be: Tier 1 Security Layer

WHY IT'S INTERESTING:
NVIDIA's backing means it will almost certainly reach production-ready status eventually. It would add three protections in one command on top of your existing OpenClaw: deep security isolation (below the app layer, deeper than a standard container), a simple text file where you define exactly what your agent can and cannot do, and a privacy router that keeps sensitive data on your own hardware. Would be the most thorough security option in the ecosystem, once ready.

WHY IT DIDN'T QUALIFY:
NVIDIA GitHub README still reads 'alpha software — do not use in production' as of May 27, 2026. Three months since GTC announcement. No GA date announced. Two of the four Claw Chain CVEs target its underlying OpenShell sandbox.

WATCH FOR: Official docs remove "not production-ready" language. No timeline announced yet.

KILOCLAW — $9/MO + ZERO-MARKUP API — would be: Tier 2 Managed Cloud (strongest current candidate)

WHY IT'S INTERESTING:
Developer-grade managed OpenClaw hosting. 2 CPUs, 3GB RAM, 10GB storage ready in 60 seconds. 500+ AI models, no markup on AI usage. 610+ pre-built automation workflows. Enterprise SSO/SCIM available. Automatic updates, monitoring, daily backups. From team behind Kilo Code (2.3M+ developers). GitLab co-founder Sid Sijbrandij backing. Launched February 2026.

WHY IT DIDN'T QUALIFY:
Still in beta, meaning it is being actively tested and some features are not yet stable. Some self-hosted OpenClaw features are not yet available here. Independent reviewers have reported occasional reliability issues. Limited to one active server per account. No direct command-line server access. Some experienced users find this limiting. The zero-markup pricing claim has not yet been independently verified at high usage levels.

WATCH FOR: Beta flag removed from official docs + 3 independent non-enterprise user reviews confirming stability and zero-markup claim.

CLAWX — v0.4.6 (MAY 20) — would be: Tier 3 GUI Desktop Wrapper (approaching v1.0)

WHY IT'S INTERESTING:
Click-and-point desktop app wrapping OpenClaw, no terminal required. Windows, Mac, Linux. Four new versions in 11 days (v0.4.2 May 9 to v0.4.6 May 20): active Linux packaging, skill preview, localization improvements. MIT license. Most compelling Tier 3 candidate. Enterprise edition teased (no pricing yet).

WHY IT DIDN'T QUALIFY:
Still pre-1.0. Tier 3 threshold is stable v1.0 with real traction. Neither ClawX nor OpenClaw Desktop is recommended for anything important until v1.0 stable. Active shipping pace suggests v1.0 may arrive before the July edition.

WATCH FOR: Stable v1.0 release with no "beta" qualifier in official documentation.

OPENCLAW DESKTOP — v0.7.0 — would be: Tier 3 GUI Desktop Wrapper (Windows-primary)

WHY IT'S INTERESTING:
Installer wizard-based wrapper for OpenClaw. Windows primary. Pre-release v0.7.0. Takes a stable approach, fewer releases, lower regression risk. For Windows users who prefer stability over feature pace.

WHY IT DIDN'T QUALIFY:
Also pre-1.0. Windows-primary limits cross-platform appeal. Less active development pace than ClawX. Neither Tier 3 option earns a compact card before stable v1.0.

WATCH FOR: Stable v1.0 release with no pre-release qualifier.

T1 EXECUTOR | T1 EDGE | T1 SECURITY | T1 MEMORY | T2 MANAGED | T3 GUI | COMPANION

clawecosystem.co/glossary
clawecosystem.co/cost-calculator
clawecosystem.co/matrix

SECURITY INTEL

THE CLAW CHAIN AND THE MAY 11 CVE WAVE

TIER 1 — SELF-HOSTED
■ DIRECTLY AFFECTED
Patch immediately to v2026.4.22 and v2026.4.23.

TIER 2 — MANAGED
✓ LARGELY MANAGED
MaxClaw and Kimi Claw providers patch at infrastructure level. Verify with your provider.

TIER 3 — GUI WRAPPER
✓ INHERITS PATCHES
ClawX and OpenClaw Desktop inherit patches when you update the app.

"CLAW CHAIN" — THE ECOSYSTEM'S FIRST NAMED ATTACK

A cybersecurity researcher at Cyera named and publicly disclosed four linked security flaws called 'Claw Chain.' The disclosure was covered by Dark Reading, The Hacker News, CybersecurityNews, and SentinelOne. This is the first time OpenClaw security has appeared in major cybersecurity news publications. The Cloud Security Alliance (CSA — one of the most respected independent security organizations in the world) published a formal report on May 26. This matters because CSA reports get referenced in the official checklists companies use when approving software, meaning questions about Claw Chain will now appear in corporate security reviews worldwide. Most significantly: Google's cybersecurity research team (GTIG) officially documented that OpenClaw and ClawHub are being used to distribute harmful software. This is the first major security organization to say this on the record. How the attack works: it enters through a harmful skill, a manipulated AI prompt, or compromised external content. It then moves through three stages: stealing data from your system, gaining more access than it should have, and hiding so it stays active even after a restart. Each stage looks exactly like normal agent behavior, so standard security tools won't flag it. All four flaws are fixed in version 2026.4.22.

THREAT	WHO IS AFFECTED	WHAT COULD HAPPEN	WHAT TO DO
★ NEW **CVE-2026-44112 CVSS 9.6 — CRITICAL**	TIER 1 ONLY	A timing flaw that lets an attacker slip through a security gap between two checks. The attacker can install hidden backdoors, change system settings, and take permanent control of your installation, even after you restart.	Update to v2026.4.22 immediately. Verify before allowing external input.
CVE-2026-44113 CVSS 7.7	TIER 1 ONLY	A second timing flaw that lets an attacker read files outside the secure boundary of your installation, potentially exposing your AI service passwords (called API keys), login credentials, and configuration files.	Same patch. Audit MCP server configs and workspace trust boundaries post-patch.
CVE-2026-44115 CVSS 8.8	TIER 1 ONLY	A flaw in how the agent handles certain command blocks that lets an attacker bypass the list of approved actions and run unauthorized commands.	Same patch. Audit shell heredoc usage in custom plugins and workflows.
CVE-2026-44118 CVSS 7.8	TIER 1 ONLY	A flaw in how OpenClaw handles internal app connections (MCP — a standard way for AI tools to talk to other software) that tricks the system into thinking a lower-permission process has full owner-level access.	Version 2026.4.22 now gives owner and non-owner processes separate digital access keys. After updating, confirm this separation is working correctly.

> **BY USING THE AGENT'S OWN PERMISSIONS AGAINST YOU, AN ATTACKER CAN MOVE FROM ACCESSING YOUR DATA, TO GAINING UNAUTHORIZED CONTROL, TO HIDING IN YOUR SYSTEM, USING YOUR AGENT AS THEIR HANDS INSIDE YOUR ENVIRONMENT. EACH STAGE LOOKS LIKE COMPLETELY NORMAL ACTIVITY.**
>
> *Cyera, Claw Chain Research Disclosure, May 2026*

T1 EXECUTOR | T1 EDGE | T1 SECURITY | T1 MEMORY | T2 MANAGED | T3 GUI | COMPANION

clawecosystem.co/glossary
clawecosystem.co/cost-calculator
clawecosystem.co/matrix

ONE BIG IDEA

THE EDITORIAL TAKE ON WHAT MAY 2026 MEANS

The ecosystem got a name, a funder, and a government classification this month. That is not the same thing as maturing. It is more like being discovered.

For eighteen months, the Claw ecosystem lived in a comfortable middle ground: real enough to attract millions of GitHub supporters, but not polished enough to face serious corporate scrutiny. That ended in May 2026 on three fronts at once. Google's cybersecurity team officially putting ClawHub on the record as a distribution point for harmful software gives corporate IT departments a credible source to point to when they want to block OpenClaw from company networks. The Cloud Security Alliance's Claw Chain report means those four security flaws will now appear on the official checklists companies use when approving new software. The question shifted from 'what is OpenClaw?' to 'has your company addressed Claw Chain?' That is a completely different kind of conversation at the point where businesses decide what software to buy and approve.

NanoClaw's $12M funding is not just a business story, it changes the rules for the whole category. Until May 20, every claw in this ecosystem ran on community goodwill: ship fast, fix publicly, no formal contracts, no service guarantees. NanoClaw with Docker and Vercel as investors now operates under a completely different set of rules. It will deliver formal contracts, pass official security audits, and follow a published business plan. The Tier 1 Security Layer category now has its first member backed by professional investors. That changes every conversation a company has when it evaluates this ecosystem for official use.

The Anthropic billing change on June 15 will have the most day-to-day impact on subscribers. The cost advantage is closing: a $200/month subscription that previously let you run far more than $200 worth of agent computing is now capped at exactly $200 in agent use. For most subscribers, the real-world impact is smaller than the community reaction suggests. But if you run heavy automation through OpenClaw on Claude, the numbers changed significantly. The updated True Cost Calculator (www.clawecosystem.co/cost-calculator) now reflects this new reality.

What should you be thinking about that you probably are not? The tier structure is now also a threat model. Every single Claw Chain flaw and every May 11 security flaw targets **Tier 1** self-hosted installations. **Tier 2** users at MaxClaw and Kimi Claw had patches applied at the server level without doing anything themselves. **Tier 3** users just updated the app. Staying on top of security is now a real, ongoing cost of running your own Tier 1 installation. That is still the right choice for many people, the control and privacy benefits are real. But it should be a deliberate, informed decision, not something you stumble into.

NEXT MONTH PREVIEW — WHAT WE'RE WATCHING FOR JULY 2026

- **Microsoft ClawPilot public preview** (Build 2026, June 2).
- **OpenClaw LTS** (the May window closed without shipping, whenever it drops, we will feature it).
- **NemoClaw GA** (if NVIDIA ships it, it would become a Tier 1 Security Layer).
- And the real-world impact of the Anthropic June 15 billing change.

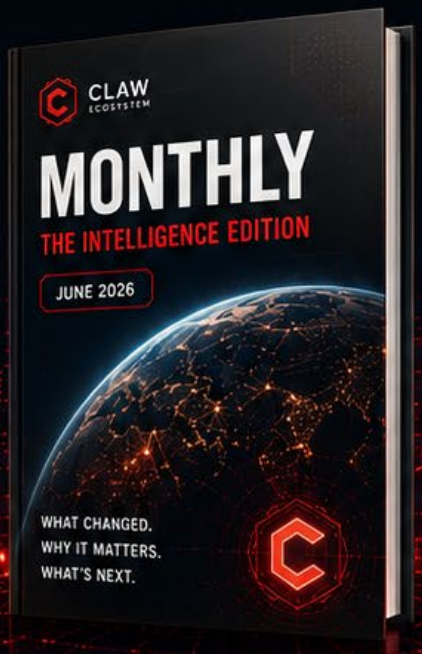
T1 EXECUTOR | T1 EDGE | T1 SECURITY | T1 MEMORY | T2 MANAGED | T3 GUI | COMPANION

clawecosystem.co/glossary
clawecosystem.co/cost-calculator
clawecosystem.co/matrix

CLAW ECOSYSTEM

STAY AHEAD. EVERY MONTH.

Real movement. Real intelligence. Real advantage.



THE CLAW ECOSYSTEM MONTHLY IS THE INTELLIGENCE EDITION.

The Claw Ecosystem Monthly covers what changed in the past 30 days: new bots, security updates, feature changes, and an editorial take on what the month means. Where the Field Guide tells you what everything is, the Monthly update tells you what moved.

$79 FOR 6 MONTHS OF ISSUES
clawecosystem.co/monthly

YOUR MONTHLY INTELLIGENCE. READ IT WHEN IT ARRIVES.

THIS IS THE REFERENCE EDITION.

The Claw Ecosystem Field Guide is a monthly reference product — a complete map of the ecosystem, current as of the edition date. Every bot profile includes its website, realistic costs, pros, cons, best-use cases, and five concrete examples. It reads the same whether you're brand new to the ecosystem or returning to check on a specific bot.

$27 PER EDITION
clawecosystem.co/field-guide

THE COMPLETE PACKAGE

Field Guide + 6 months of the Claw Ecosystem Monthly

clawecosystem.co/monthly

FIELD GUIDE ($27)

- What the ecosystem is
- Full bot profiles with costs, pros, cons, 5 examples
- Glossary of all technical terms
- Reference — consult when you need it

VS

CLAW ECOSYSTEM MONTHLY ($79 / 6 MONTHS)

- What changed this month
- New bot summaries with a link to the Field Guide
- Security updates as they happen
- Intelligence — read it when it arrives

BUIILT FOR CLARITY. DESIGNED FOR ACTION.

EVERY BOT. ONE PLACE.
Complete, accurate, always current.

REAL PRICING. REAL CONTEXT.
Costs, pros, cons, and realistic expectations.

TIME-SAVING INTELLIGENCE.
We track. You stay ahead.

SECURITY YOU CAN TRUST.
Critical updates as they happen.

THE EDGE YOU NEED.
Understand the ecosystem. Stay ahead of it.