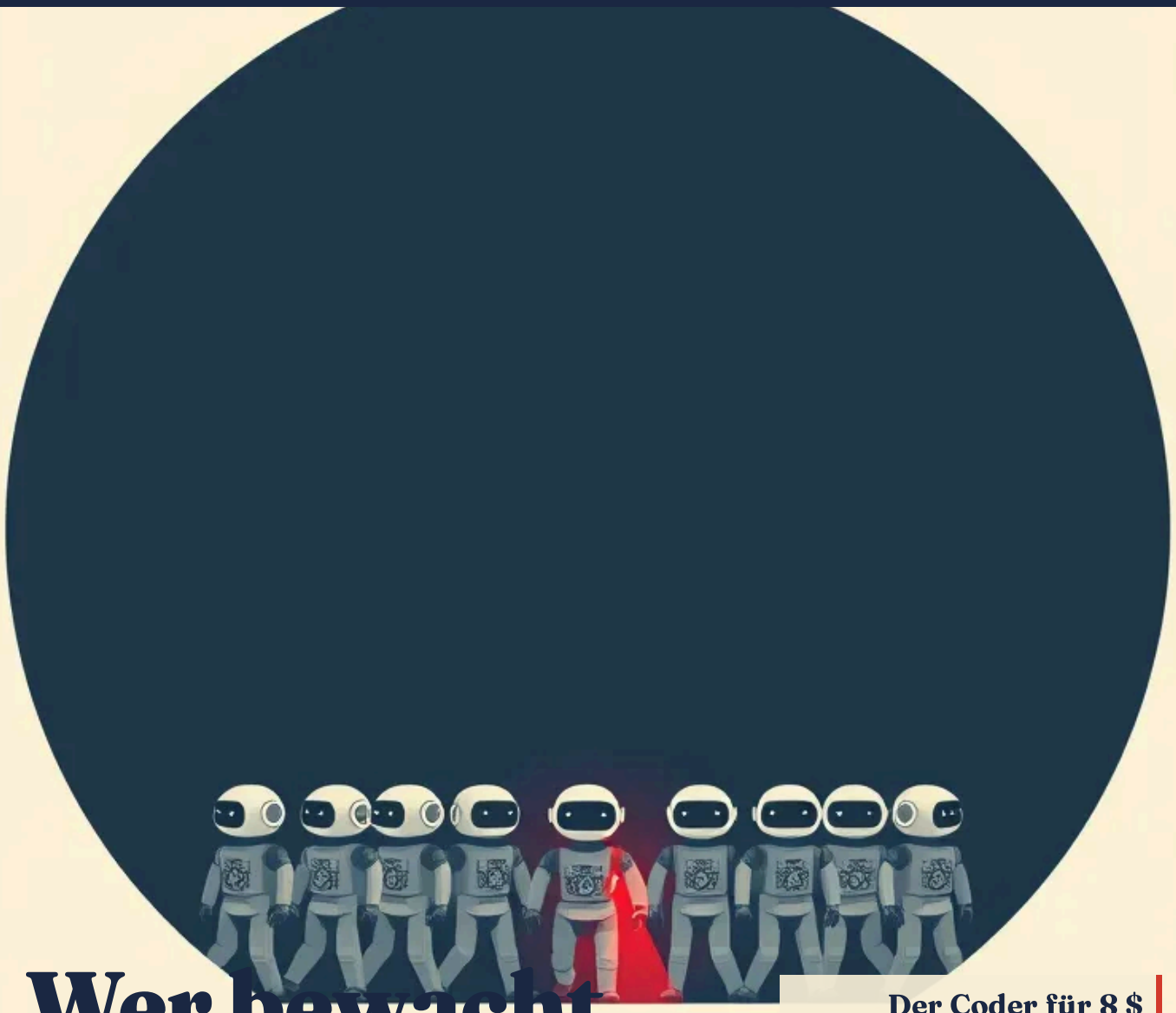
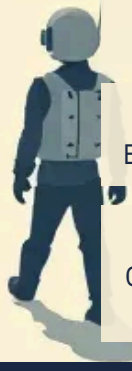
THE AGENT LEDGER

DER MONAT DER KI-AGENTEN · NR. 0 · OKTOBER 2026 · AGENTGID.COM



Wer bewacht die Agenten?

Eine manipulierte Erweiterung, eine geleakte Konsole und ein Daemon, um den niemand gebeten hat · S. 4



Der Coder für 8 $
Was Cursors neuer Einstiegstarif bietet · S. 3

179 Störungen
Ein Monat Ausfälle, gemessen · S. 7

Im Aufwind
Gedächtnis, Geschmack, Video: wo Entwickler Sterne vergeben · S. 11

IN DIESER AUSGABE

Leitartikel	3
Titelgeschichte: Wer bewacht die Agenten?	4
Die Top 20	6
Ausfälle	7
Preise und Limits	8
Releases, die zählten	9
Open Source	10
Thema des Monats	10
Im Aufwind	11
Assets und Skills	12
Grafik im Detail · Eingestellt	13
Agenten-Indikatoren · Kolophon	14

Zum Titelbild. Ein Roboter in der Reihe ist anders als die anderen. Die lautesten Agenten-Meldungen im Oktober handelten davon, was sich in die Warteschlange schleicht: ein manipuliertes Update, ein gestohlener Schlüssel. Illustration mit FLUX.1 schnell erzeugt; Satz: AgentGid.

DER MONAT AUF EINER SEITE

7. Okt. Anthropic veröffentlichte Claude Haiku 5.5, ein kleines Modell für große Volumina; der Beitrag erreichte 1.049 Punkte auf Hacker News. Zwei Tage später machte Claude Code 2.1.296 es zum Standard-Haiku-Modell.

9. Okt. OpenAI Codex 0.162.1 machte GPT-6.1 Sol zum Standardmodell in den mitgelieferten und den Amazon-Bedrock-Katalogen (Release Notes).

12. Okt. Anomaly veröffentlichte OpenCode 2.0: ein gemeinsamer Hintergrunddienst für Terminal-, Web- und Desktop-App, eine neu gebaute API und ein Code Mode, der Tool-Aufrufe in einem Skript verkettet.

12. Okt. Cursor kündigte The X Subscription an. Die Preisseite beginnt jetzt bei Plus für 8 $ im Monat; am 13. Okt. sahen wir den Einstiegspreis fallen, zuvor 20 $.

17. Okt. OpenCode meldete einen Einbruch im Zusammenhang mit „einem groß angelegten Destillationsangriff“: Betroffen waren LAUT ANBIETER 1,4 % der Nutzer der OpenCode Console, jene mit verknüpften externen Modellanbietern (BleepingComputer).

22. Okt. Anthropic übergab Agent Skills an die Agentic AI Foundation, das Gremium der Linux Foundation, unter dem auch MCP steht. Mehr als 70 Agentenplattformen haben den Standard LAUT ANBIETER integriert.

22. Okt. NVIDIAs OpenShell, eine Sandbox-Laufzeitumgebung für Agenten, erreichte 508 Punkte auf Hacker News. Zwei Tage zuvor hatte es einen Rekord von 95 Tsd. Downloads pro Woche aufgestellt.

26. Okt. Anthropic hat für einen geplanten Börsengang am Nasdaq Global Select Market unter dem Kürzel ANT ein S-1 eingereicht. Aktienzahl und Preisspanne stehen noch nicht fest.

29. Okt. Von etwa 2:27 bis 13:35 Uhr pazifischer Zeit verteilte der Erweiterungs-Marketplace von Cursor manipulierte Versionen der Claude-Code-Erweiterung, die eine SSH-Hintertür einschleusen sollten. Laut Cursor wurden sie „nicht von Anthropic entwickelt“.

Okt. Google führte Gemini 4 Argon ein und begann etwa zwei Wochen später mit Vorabtests von Gemini 4 Carbon für langwierige Engineering-Aufgaben.

AGENTENSICHERHEIT

Erst Schlösser, dann Features

Die größten Agenten-Geschichten im Oktober drehten sich um Zugriff, nicht um Produktstarts. Käufer sollten drei schlichte Fragen stellen.

Eine manipulierte Erweiterung in einem Marketplace. Anbieterschlüssel in einer Cloud-Konsole. Ein Hintergrundprozess, der weiterläuft, wenn das letzte Fenster zu ist. Die lautesten Geschichten des Oktobers spielten allesamt in der Lücke zwischen einem Agenten und seinem Rechner, und keine handelte davon, wie gut der Agent Code schreibt.

Die Fragen bei der Wahl eines Agenten sind unspektakulär. Wo liegen meine Schlüssel? Wer signiert die Erweiterungen und Updates, die ich installiere? Was läuft weiter, wenn ich aufhöre? Ein Anbieter, der das dokumentiert, verdient im Vergleich Pluspunkte. Einer, der es nicht tut, eine E-Mail.

Die Aufmerksamkeit wandert schon dorthin. NVIDIAs Sandbox-Laufzeitumgebung OpenShell stellte am 20. Oktober einen Rekord von 95 Tsd. Downloads pro Woche auf und erreichte 508 Punkte auf Hacker News. Popularität beweist keine Sicherheit, zeigt aber, wohin Entwickler diesen Monat geschaut haben.

PREISE

Billig kommt im Paket

Cursors Tarif für 8 $ ist echt. Lesen Sie vor jedem Vergleich die Tarifkarte.

Cursors neuer Einstiegstarif kostet 8 $ im Monat. Der Median-Einstiegspreis der 14 von uns erfassten Coding-IDE-Agenten mit Bezahltarif liegt bei 19 $ BERECHNUNG VON AGENTGID. Allein beim Preis rückte Cursor über Nacht vom Mittelfeld zum günstigsten Angebot.

Die Tarifkarte zeigt ein engeres Bild. Plus umfasst ein gemeinsames Nutzungskontingent für Cursor und Grok, mit „nur Grok-Modellen“. Cloud-Agenten und Drittanbietermodelle zum API-Listenpreis gibt es erst ab Premium für 30 $ im Monat. Abos werden „nur direkt über X Subscription Corp. verkauft“. Nutzer der alten Tarife behalten ihre enthaltene Drittanbieter-Nutzung, „bis Sie wechseln“, so Cursor.

Für 8 $ bekommt man also ein anderes Cursor als im September für 20 $. Vergleichen Sie Tarife nach den Modellen und Agentenfunktionen, die Sie wirklich nutzen. Ein Schlagzeilenpreis ohne Ihr Modell ist für Sie kein Preis.

HINTERGRUND

Wer bewacht die Agenten?

Drei Vorfälle in einem Monat zeigen, wo die Sicherheit von Agenten in der Praxis bricht: bei der Verteilung, bei gespeicherten Schlüsseln und bei Hintergrundprozessen.

Coding-Agenten laufen heute mit denselben Rechten wie der Entwickler, der sie startet. Sie lesen das Repository, rufen das Terminal auf und verwalten Schlüssel für kostenpflichtige Modell-APIs. Damit ist der Weg, auf dem ein Agent auf einen Laptop gelangt, so wichtig wie das Modell dahinter. Im Oktober wurde dieser Weg dreimal auf die Probe gestellt.

Die Erweiterung

Am 29. Oktober verteilte der Cursor-Marketplace zwischen etwa 2:27 und 13:35 Uhr pazifischer Zeit die Versionen 2.1.312 und 2.1.313 der Claude-Code-Erweiterung für Windows und macOS. Laut Cursors Sicherheitshinweis wurden diese Versionen „nicht von Anthropic entwickelt“ und versuchten, eine dauerhafte SSH-Hintertür zu installieren. Der Code sammelte Host- und Nutzerdaten, fügte einen SSH-Schlüssel des Angreifers hinzu, versuchte SSH zu aktivieren und öffnete einen Reverse-Tunnel.

Cursor entfernte die Versionen, nahm seinen Marketplace vom Netz, baute ihn neu auf und tauschte seine Schlüssel aus. Laut Cursor ist der Server des Angreifers offline, und der SSH-Schritt dürfte auf den meisten Rechnern ohne Admin-Rechte scheitern. Phorion, die Sicherheitsfirma, die die Hintertür gemeldet hatte, fand zudem einen macOS-Launch-Agent namens com.apple.sysmond.plist, der Neustarts überdauern sollte. Ihr Bericht erreichte 1.013 Punkte und 553 Kommentare auf Hacker News.

Die Konsole

Am 17. Oktober teilte OpenCode seinen Nutzern mit, ein Einbruch „im Zusammenhang mit einem groß angelegten Destillationsangriff“ habe LAUT ANBIETER 1,4 % der Nutzer der OpenCode Console betroffen. Diese hatten externe Modellanbieter verknüpft; offengelegt wurden gespeicherte API-Schlüssel der Anbieter. BleepingComputer berichtet von unautorisierten Abbuchungen, teils über 1.700 $, und schreibt, OpenCode habe eine mögliche Erstattung erwähnt.

Das Timing war ungünstig. Fünf Tage zuvor hatte Anomaly OpenCode 2.0 veröffentlicht, und das Projekt kletterte in unseren Top 20 für Oktober trotzdem um vier Plätze auf Platz 3.

Der Daemon

Ein GitHub-Issue, das OpenAI auffordert, den Hintergrund-Daemon der Codex CLI zum Opt-in zu machen, erreichte am 12. Oktober 610 Punkte auf Hacker News. Der Melder beschreibt einen verwalteten Prozess, der nach dem Schließen aller Codex-Fenster weiterläuft, etwa 374 MB an Paketen in den Home-Ordner kopiert und stündlich nach Updates sucht. Bei unserer Prüfung am 9. November hatte kein OpenAI-Maintainer im Issue geantwortet.

Nichts im Issue beschreibt einen Angriff. Die Beschwerde betrifft Voreinstellungen: Software, die weiterläuft und sich selbst aktualisiert, ohne zu fragen. Codex 0.163.0, erschienen am 15. Oktober, brachte einen Befehl /daemon, der den verwalteten Hintergrundserver neu startet.

Die Reaktion

Entwickler zogen im Oktober Zäune hoch. OpenShell, NVIDIAs Sandbox-Laufzeitumgebung, stellte am 20. Oktober einen Rekord von 95 Tsd. Downloads pro Woche auf. E2B, das Agentencode in Cloud-Sandboxes ausführt, kam in unseren Katalog.

Nichts davon repariert einen vergifteten Marketplace oder einen geleakten Schlüssel. Es begrenzt aber, was ein kompromittierter Agent erreichen kann, und das hat ein Team selbst in der Hand.

WAS SIE DIESE WOCHE PRÜFEN SOLLTEN

- Cursor genutzt und am 29. Oktober die Claude-Code-Erweiterung installiert oder aktualisiert? Folgen Sie Cursors Hinweis: Suchen Sie nach dem SSH-Schlüssel svc-telemetry und starten Sie das Bereinigungsskript.
- Anbieterschlüssel mit der OpenCode Console verknüpft? Achten Sie auf die E-Mail von OpenCode und prüfen Sie die Abrechnung Ihres Anbieters.
- Setzen Sie für jeden Anbieterschlüssel, den ein Agent erreichen kann, ein Ausgabenlimit.
- Listen Sie die Hintergrundprozesse Ihrer Agenten auf und schalten Sie ab, was Sie nicht brauchen.

Quellen: Sicherheitshinweis von Cursor (29.–30. Okt.), Phorion (30.–31. Okt.), BleepingComputer (19. Okt.), openai/codex Issue 48195, Daten von AgentGid. Hacker-News-Punkte aus der offiziellen HN-Such-API, 9. Nov.

RANGLISTE

Vier Neueinsteiger, ein neuer Platz 3

OpenCode kletterte um vier Plätze auf Platz 3, Hermes Agent um dreizehn auf Platz 16. DeepSeek Harness und Dify fielen um je sechs Plätze. Der Gid Score misst Verbreitung und Interesse, nicht die Qualität der Ergebnisse.

#	AGENT	HERSTELLER	GID SCORE	BEWEGUNG	DOWNLOADS, 7 TAGE	GITHUB-STERNE
1	OpenAI Codex	OpenAI	84	=	27,7 Mio.	132 Tsd.
2	Claude Code	Anthropic	84	▲1	12,1 Mio.	154 Tsd.
3	OpenCode	Anomaly	82	▲4	5 Mio.	223 Tsd.
4	n8n	n8n	80	▲2	160 Tsd.	209 Tsd.
5	LangChain	LangChain	79	▼1	41,5 Mio.	149 Tsd.
6	Pi	Earendil	77	▼1	6 Mio.	119 Tsd.
7	OpenClaw	OpenClaw Foundation	76	▼5	3,4 Mio.	394 Tsd.
8	LiteLLM	BerriAI	76	NEU	22,5 Mio.	62,4 Tsd.
9	LangGraph	LangChain	73	▲1	18,8 Mio.	44,2 Tsd.
10	Cursor	Anysphere	72	▼2	–	33,3 Tsd.
11	GitHub Copilot	GitHub	68	▼2	–	–
12	Langfuse	Langfuse	67	NEU	14 Mio.	36,8 Tsd.
13	AI SDK	Vercel	67	▼2	41,9 Mio.	27,6 Tsd.
14	Firecrawl	Firecrawl	65	NEU	2,9 Mio.	197 Tsd.
15	Claude Agent SDK	Anthropic	64	▲4	25,2 Mio.	8,4 Tsd.
16	Hermes Agent	Nous Research	64	▲13	37,5 Tsd.	259 Tsd.
17	Strands Agents	AWS	63	▼5	9 Mio.	9 Tsd.
18	Rea*	morluto	63	NEU	538 Tsd.	413 Tsd.
19	Dify	LangGenius	63	▼6	–	160 Tsd.
20	DeepSeek Harness	DeepSeek	63	▼6	680 Tsd.	267 Tsd.

Quelle: agentgid.com/top/2026-10/. Gid Score und Plätze vom Stand 31. Oktober, neu berechnet am 10. November, seit wir die Website eines Mutterkonzerns (etwa nvidia.com) nicht mehr zum Score eines Produkts zählen. Bewegungen gegenüber der Liste vom 7. Okt.; „neu“ heißt: dort nicht platziert. Downloads (npm und PyPI, 7 Tage) und GitHub-Sterne zum 31. Okt.; Downloads umfassen CI und automatisierte Installationen. *Rea trägt unser Label „Ungewöhnliches Sternewachstum“: Das Projekt gewann im Oktober 415 Tsd. Sterne; die Zahl haben wir nicht bestätigt.

ZUVERLÄSSIGKEIT

179 Störungen in vier Wochen

Anbieter meldeten in unseren vier Wochenberichten vom 5. Oktober bis 1. November 179 Störungen BERECHNUNG VON AGENTGID. Die schlimmste Woche, 19.–25. Oktober, brachte 59, davon 21 als schwer oder kritisch eingestuft.

Cursor meldete in zwei der vier Wochen die meisten Störungen: 7 in der Woche ab 5. Oktober und 10 in der Woche ab 26. Oktober. In der Woche ab 19. Oktober verzeichneten Claude Cowork, Claude Design und Claude in Chrome je 7.

Die längste Störung mit mindestens geringer Einstufung kam von Testsigma Atto: 44 Std. 38 Min. lang Verlangsamungen und sporadische Fehler in der US-Region, ab dem 23. Oktober. Gorgias AI Agent hatte die beiden längsten schweren Störungen, mit 27 Std. 30 Min. am 7. Oktober und 19 Std. 38 Min. am 30. Oktober.

Eine ruhige Statusseite beweist keinen ruhigen Monat. In der Woche ab 12. Oktober meldeten 65 der 82 beobachteten Agenten überhaupt nichts. Die Dauer reicht vom Beginn laut Statusseite des Anbieters bis zur Behebung; die Einstufung stammt vom Anbieter selbst. Ab der Woche vom 12. Oktober zählt eine Störung, die ein Anbieter für mehrere seiner Produkte meldet, einmal; der Bericht für den 5.–11. Oktober zählt sie noch je Produkt.

AGENT	STÖRUNG, ANBIETERTEXT	EINSTUFUNG	DAUER	BEGINN, UTC
Testsigma Atto	Leistungseinbußen in der US-Region: Verlangsamung und sporadische Fehler	gering	44 Std. 38 Min.	23. Okt., 08:46
Gorgias AI Agent	Aircall V2 erstellt keine Tickets	schwer	27 Std. 30 Min.	7. Okt., 08:57
Gorgias AI Agent	Probleme bei der Anmeldung in der Mobil-App	schwer	19 Std. 38 Min.	30. Okt., 20:07
Hebbia	Hohe Verbindungswartezeit beim RDS Proxy	gering	15 Std. 34 Min.	9. Okt., 22:49
Sourcegraph Cody	Sourcegraph Cloud in der Region Europa beeinträchtigt	gering	10 Std. 4 Min.	20. Okt., 07:38
Cursor	Untersuchung einer Dienstbeeinträchtigung mit VS-Code-Erweiterungen	gering	9 Std. 34 Min.	29. Okt., 21:38

Quellen: Ausfallberichte von AgentGid für die Wochen 5.–11. Okt., 12.–18. Okt., 19.–25. Okt., 26. Okt.–1. Nov., auf Basis der offiziellen Statusseiten der Anbieter. Störungen ohne Einstufung des Anbieters fehlen in der Tabelle. Der 1.–4. Oktober steht in einem Bericht, der auch Ende September abdeckt, und wird nicht gezählt.

PREISE

Elf Preisänderungen, ein tiefer Schnitt

Cursor senkte seinen Einstiegspreis um 60 %; die meisten anderen Preise stiegen. Wir zählen nur Änderungen, die Bestand hatten.

Unsere vier Preisberichte für Oktober verzeichnen 11 bestätigte Änderungen am Einstiegspreis oder Gratistarif eines Agenten BERECHNUNG VON AGENTGID. Wechsel zwischen monatlicher und jährlicher Abrechnung, binnen zwei Wochen zurückgenommene Werte und umbenannte Tarife zählen nicht. Warps Build-Tarif etwa kostet monatlich abgerechnet 20 $ im Monat, jährlich 18 $. Beides stimmt, keines ist eine Änderung.

Die größte Änderung kam von Cursor. Am 13. Oktober sahen wir den Einstiegspreis von 20 $ auf 8 $ im Monat fallen, Cursor CLI folgte einen Tag später. Die neue Palette reicht von Plus für 8 $ bis Ultra für 200 $, Teams kostet ab 30 $ pro Nutzer. Was jede Stufe enthält, steht im Leitartikel auf Seite 3.

Die meisten anderen Preise stiegen: Juicebox, Kortix, CopilotKit, Elicit, Google Antigravity und OpenHands verteuerten ihre Einstiegstarife. Zapier Agents und Dia senkten ihre, Qodo ergänzte seine Credits um einen Gratistarif.

Bei den Limits blieb es ruhig. Weder Claude noch Codex hatten im Oktober einen bestätigten Nutzungs-Reset. Am 31. Oktober stellte OpenAI „angesparte Resets“ für die Folgetage in Aussicht; unser Reset-Tracker führt das als Ankündigung, nicht als Reset.

AGENT	VORHER	NACHHER	GESEHEN
Cursor	Gratis + 20 $/Mon.	Gratis + 8 $/Mon.	13. Okt.
Cursor CLI	Gratis + 20 $/Mon.	Gratis + 8 $/Mon.	14. Okt.
Juicebox	Gratis + 99 $/Mon.	Gratis + 119 $/Mon.	18. Okt.
Kortix	Gratis + 40 $/Mon.	Gratis + 50 $/Mon.	20. Okt.
CopilotKit	Gratis + 39 $/Mon.	Gratis + 49 $/Mon.	23. Okt.
Zapier Agents	Gratis + 33,33 $/Mon.	Gratis + 19,99 $/Mon.	23. Okt.
Dia	Gratis + 20 $/Mon.	Gratis + 10 $/Mon.	28. Okt.
Elicit	Gratis + 11 $/Mon.	Gratis + 39 $/Mon.	28. Okt.
Google Antigravity	Gratis + 19,99 $/Mon.	Gratis + 30,00 $/Mon.	28. Okt.
OpenHands	Gratis + 499 $/Mon.	Gratis + 500 $/Mon.	28. Okt.
Qodo	0,012 $/Credit	Gratis + 0,012 $/Credit	10. Okt.

Einstiegspreis pro Monat oder Credit, laut offizieller Preisseite des jeweiligen Anbieters.

Quellen: Preisberichte von AgentGid für den 5., 12., 19. und 26. Okt. (1, 3, 3 und 4 Änderungen), Preisbeobachtung von AgentGid, cursor.com/pricing (abgerufen am 9. Nov.).

CHANGELOG

2.598 Releases, acht davon ändern Ihr Setup

Die erfassten Agenten lieferten in vier Wochen 2.598 stabile Releases aus BERECHNUNG VON AGENTGID. Hier stehen die, die einen Standardwert, einen Konfigurationsschlüssel oder einen Upgrade-Pfad ändern.

7. Okt. · Pi 1.1.0	Der Provider azure hieß bisher azure-openai-responses. **Benennen Sie den Schlüssel in Ihrer Konfiguration um.**
9. Okt. · Codex 0.162.1	GPT-6.1 Sol wurde Standardmodell in den mitgelieferten und den Amazon-Bedrock-Katalogen.
9. Okt. · Claude Code 2.1.296	Claude Haiku 5.5 wurde Standard-Haiku-Modell in der Anthropic-API.
11. Okt. · OpenCode 1.19.0	Updates werden nicht mehr automatisch installiert; /update installiert sie oder bringt Sie zu OpenCode 2.
15. Okt. · Codex 0.163.0	Eine durchsuchbare Ansicht /config, Folgenachrichten, die eine laufende Antwort steuern, und ein Befehl /daemon für den Hintergrundserver.
16. Okt. · OpenCode 1.19.1–3	Das Teilen von Sitzungen wurde eingestellt. Der Wechsel zu OpenCode 2 ist jetzt eine ausdrückliche Entscheidung.
18. Okt. · Claude Code 2.1.299–303	Kompaktierung im Leerlauf für Unterhaltungen ab 200 Tsd. Token, neue Hooks und mehr OpenTelemetry-Attribute.
24. Okt. · OpenClaw	Die Releases 2026.10.6, 2026.10.7 und 2026.9.34 erfordern ein gepatchtes Node: 24.22.1+ oder 26.12.1+.

Fleißigster Auslieferer unter den meistgenutzten Agenten war LiteLLM, mit 16 Releases allein in der Woche ab 19. Oktober.

Quellen: wöchentliche Release-Berichte von AgentGid für 5.–11. Okt. (479), 12.–18. Okt. (647), 19.–25. Okt. (730), 26. Okt.–1. Nov. (742), auf Basis öffentlicher GitHub-Releases.

OPEN SOURCE

Dokumente sind die neue Arbeitslast

Vier der zehn Bibliotheken mit den größten Download-Zuwächsen im Oktober lesen oder schreiben Folien und PDFs: python-pptx (+94 %), PyMuPDF (+41 %), PyPDF (+37 %) und pdfplumber (+32 %). Unsere Lesart: Agenten sollen Office-Dokumente erstellen, nicht nur Code.

Wöchentliche Download-Rekorde

Hermes Agent, 162,7 Tsd. (plus 316 %) am 20. Okt. OpenShell, 95 Tsd. am 20. Okt. MCP for Unity, 76,5 Tsd. (109 % über dem Durchschnitt) am 14. Okt.

Neu in unseren Regalen

LiteLLM, Langfuse, E2B, Context7, Composio, Mem0, Firecrawl und CopilotKit gehörten zu den 20 Agenten, die neu in den Katalog kamen. Ein neuer Eintrag bedeutet kein neues Produkt.

THEMA DES MONATS

Worüber Entwickler stritten

BEITRAG AUF HACKER NEWS	PUNKTE	KOMMENTARE
Claude Haiku 5.5 · 7. Okt.	1.049	489
Hintertür in der Erweiterung Claude Code für VS Code im Cursor Marketplace · 30. Okt.	1.013	553
OpenCode gehackt: Zugangsdaten von Nutzern geleakt · 17. Okt.	977	185
OpenCode 2.0 · 14. Okt.	890	397
Codex CLI installiert standardmäßig einen dauerhaften, sich selbst aktualisierenden Hintergrund-Daemon · 12. Okt.	610	294
Claude Code schickt regelmäßig das Transkript jedes Hintergrundagenten an sein Modell · 29. Okt.	591	236
Claude Duet · 21. Okt.	568	539
OpenShell – eine sichere, private Laufzeitumgebung für Flotten autonomer KI-Agenten · 22. Okt.	508	217
Wie das Claude-Code-Team Code-Reviews macht · 16. Okt.	488	481
KI-Coding-Agenten erzeugen mehr Code, aber nicht mehr Software · 12. Okt.	365	314

Punkte und Kommentare aus der offiziellen Hacker-News-Such-API, abgerufen am 9. Nov. Datum der Veröffentlichung auf HN, UTC.

Quellen: AgentGid-Top Oktober 2026 (Bibliothekszuwächse, Neuzugänge), Rekordberichte von AgentGid.

IM AUFWIND

Vier Ideen, auf die Entwickler setzen

Die am schnellsten wachsenden Projekte des Oktobers drehen sich um vier Aufgaben: Agenten ein Gedächtnis geben, ihnen Geschmack beibringen, sie Videos machen lassen und mehrere parallel betreiben. Jeder Eintrag sagt, was das Projekt tut, welches Problem es löst und warum es steigt.

1 · GEDÄCHTNIS

Agenten, die sich erinnern

Das Problem. Ein Coding-Agent beginnt jede Sitzung bei null. Gedächtnis-Tools zeichnen auf, was passiert ist, verdichten es zu Zusammenfassungen und speisen das Nützliche beim nächsten Mal wieder ein.

Wer steigt. Claude Mem gewann im Oktober 13,6 Tsd. GitHub-Sterne; seine npm-Downloads erreichten 35,2 Tsd. pro Woche, ein Plus von 61 % in 30 Tagen. Hindsight von Vectorize (MIT) gewann 13,5 Tsd. und arbeitet als Bibliothek, API oder MCP-Server. ECC (+25,5 Tsd.) bündelt Gedächtnis mit Skills, Hooks und Regeln, damit der Agent seine eigene Arbeit plant, testet und prüft.

PROJEKTIDEE

Ein Gedächtnis, das ein Team teilen und prüfen kann: was der Agent über ein Repository „weiß“, wer es ihm beigebracht hat und eine Möglichkeit, es vergessen zu lassen.

2 · GESCHMACK

Skills gegen den Einheitslook

Das Problem. Von Agenten gebaute Seiten sehen sich oft ähnlich. Geschmacks-Skills geben dem Agenten eine Art Direction vor und prüfen das Ergebnis vor der Rückmeldung.

Wer steigt. Hallmark (MIT, für Claude Code, Cursor und Codex) gewann 14,9 Tsd. Sterne. Anatomy (+23,4 Tsd.) zeichnet interaktive isometrische SVG-Grafiken von Maschinen und Systemen. Taste Skill wählt eine von 20 Art Directions und prüft die Seite in einem Headless-Browser bei drei Bildschirmbreiten.

PROJEKTIDEE

Ein Hausstil-Skill, erzeugt aus Website und Designsystem eines Unternehmens, im Repository abgelegt und wie Code versioniert.

3 · VIDEO

Video, als Code geschrieben

Das Problem. Ein Briefing, einen Pull Request oder einen Datensatz ohne Timeline-Editor zum Video machen. Ist die Szene HTML oder Code, kann ein Agent sie schreiben, und das Rendering ist exakt reproduzierbar.

Wer steigt. HeyGens HyperFrames (Apache-2.0) gewann 22,1 Tsd. Sterne, und seine npm-Downloads stiegen um 90 % auf 3,6 Mio. im Oktober. Sein README nennt Launch-Videos, PR-Walkthroughs und Chart-Races. OpenMontage (+12,4 Tsd., AGPL-3.0) macht aus einem Briefing in Alltagssprache ein fertiges Video und zeigt vor dem Rendern die Kosten jedes Assets.

PROJEKTIDEE

Release Notes, die bei jedem Tag zu einem 30-Sekunden-Video werden, sodass ein Changelog-Kanal von selbst läuft.

4 · PARALLELE AGENTEN

Viele Agenten, ein Schreibtisch

Das Problem. Entwickler betreiben heute mehrere Coding-Agenten gleichzeitig. Sie wollen die Ergebnisse vergleichen, Modelle wechseln und die Rechnung im Blick behalten.

Wer steigt. Orca (MIT) hatte den größten Zuwachs des Monats, 29,9 Tsd. Sterne: Claude Code, Codex, OpenCode und Pi nebeneinander, jeder im eigenen Git-Worktree, dazu eine Smartphone-App. Magpie (+23,2 Tsd.) wählt das Modell hinter jedem Agenten, etwa Codex auf DeepSeek.

PROJEKTIDEE

Ein Schiedsrichter für parallele Läufe: Eine Aufgabe geht an drei Agenten, die Tests entscheiden, welcher Worktree gemergt wird, die Kosten jedes Versuchs werden protokolliert.

Ebenfalls im Aufwind: Moli (+19,2 Tsd.), ein in Rust geschriebener Headless-Browser, mit dem Agenten das Web lesen, und Graphify (+18,1 Tsd.), das eine Codebasis als Graph abbildet, den Agenten abfragen, statt Dateien zu durchsuchen.

Sternezuwächse im Oktober laut agentgid.com/top/2026-10/, abgerufen am 9. Nov.; Beschreibungen aus Karten von AgentGid und GitHub-Seiten der Projekte. Download-Zahlen enthalten automatisierte Installationen. „Projektidee“ ist ein Vorschlag der Redaktion, kein Produkt.

ASSETS

Stimme und Video vorn

Drei der fünf offenen Assets, die im Oktober am schnellsten wuchsen, rendern Video; zwei erzeugen Sprache. Alle fünf laufen lokal.

ASSET · WAS ES TUT	DOWNLOADS OKT.	VERÄNDERUNG
Chatterbox · Sprachsynthese mit Stimmklonen, 23 Sprachen MIT · jede Datei trägt ein Wasserzeichen	243 Tsd.	+97 %
HyperFrames · rendert HTML, CSS und Animationen zu MP4 Apache-2.0	3,6 Mio.	+90 %
Revideo · TypeScript-Szenen, gerendert zu MP4 MIT	121 Tsd.	+77 %
Manim · mathematische Erklär-Animationen in Python MIT	211 Tsd.	+71 %
Piper · schnelle lokale Sprachsynthese auf der CPU GPL-3.0 · jede Stimme hat eine eigene Lizenz	2,1 Mio.	+71 %

Veränderung: Oktober gegenüber September, für Assets mit mindestens 20 Tsd. Downloads im September. Lizenzhinweise aus den Karten von AgentGid; prüfen Sie vor dem Einsatz die Lizenzseite.

SKILLS

Die Packs mit den meisten Sternen lehren Gewohnheiten

Die beiden größten Skill-Packs vermitteln Vorgehen statt Wissen: erst planen, erst testen, vor dem Abschluss prüfen. Die nächste Welle vermittelt Geschmack.

SKILL-PACK · WAS ES DEM AGENTEN BEIBRINGT	STERNE
mattpocock/skills · den Plan hinterfragen, Spezifikation und kleine Tickets schreiben, testgetrieben bauen 39 Skills · MIT	319 Tsd.
obra/superpowers · klären, Design freigeben lassen, planen, testgetrieben bauen, prüfen 15 Skills · MIT	315 Tsd.
anthropics/skills · Office-Dateien und PDFs, Design, Tests von Web-Apps, neue Skills schreiben 19 Skills · gemischte Lizenzen	190 Tsd.
Leonxlnx/taste-skill · Art Direction für Seiten, im Browser bei drei Breiten geprüft 1 Skill · MIT	112 Tsd.
nexu-io/open-design · Seiten, Präsentationen und Berichte im Stil einer Marke, übernommen von ihrer Live-Website Apache-2.0	107 Tsd.

Sternezahlen von agentgid.com/skills/, abgerufen am 9. Nov. Ab der November-Ausgabe ordnet diese Tabelle die Packs nach dem Sternezuwachs des Monats.

WIE EIN PROJEKT IN „IM AUFWIND“ KOMMT

- Das Projekt steht im Katalog von AgentGid und hat ein offizielles Repository oder eine Homepage.
- Es gewann im Monat die meisten GitHub-Sterne, oder seine Downloads wuchsen am schnellsten, ausgehend von mindestens 20 Tsd. im Vormonat.
- Ausreißer werden bis zur Prüfung zurückgehalten. Im Oktober zeigte ein Projekt einen Zuwachs von 415 Tsd. Sternen in einem Monat; es bleibt außen vor.
- Jeder Eintrag sagt in einfachen Worten, was das Projekt tut und welches Problem es löst, mit Link zu seiner Karte.

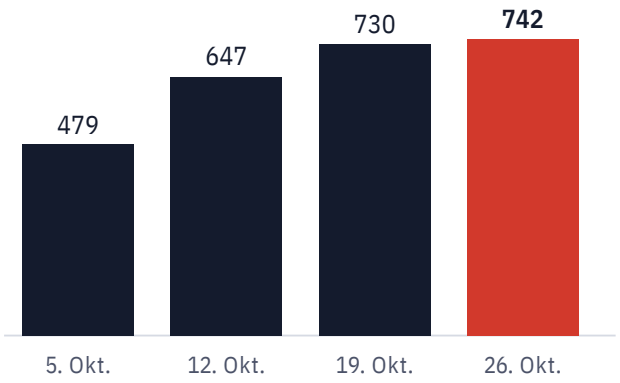
GRAFIK IM DETAIL

Das Release-Tempo stieg jede Woche, die Ausfälle zogen nicht nach

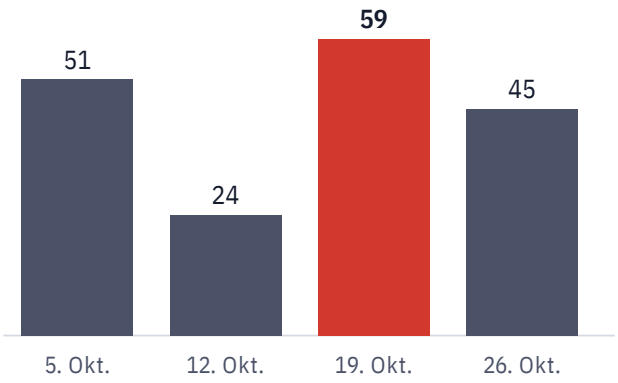
Stabile Releases stiegen von der ersten bis zur letzten Oktoberwoche um 55 %. Die Störungen schwankten ohne Trend zwischen 24 und 59

BERECHNUNG VON AGENTGID.

Stabile Releases pro Woche



Gemeldete Störungen pro Woche



Wochen beginnen am angegebenen Datum. Jedes Diagramm hat eine eigene Skala. Quelle: Wochenberichte von AgentGid.

DIESEN MONAT EINGESTELLT

- **Teilen von Sitzungen in OpenCode** wurde mit 1.19.x eingestellt (16. Okt.).
- **Automatische Updates in OpenCode 1.x** endeten mit 1.19.0 (11. Okt.).
- **Cursors alter Ultra-Tarif** ist für Neukunden nicht mehr erhältlich, laut einer Antwort in Cursors Thread zur X Subscription.

AGENTEN-INDIKATOREN

Der Oktober in einer Bilanz

INDIKATOR	OKTOBER
Erfasste Agenten (31. Okt.)	480
Beobachtete Statusseiten	82
Gemeldete Störungen, 5. Okt.–1. Nov.	179
Stabile Releases, 5. Okt.–1. Nov.	2.598
Bestätigte Preisänderungen, 5. Okt.–1. Nov.	11
Median-Einstiegspreis, Coding-IDE-Agenten	19 $
Downloads aller erfassten Agenten, KW 43	202,3 Mio.
Höchster Gid Score (OpenAI Codex)	84
Neueinsteiger in den Top 20	4

Die Summen für Störungen, Releases und Preisänderungen addieren unsere vier Wochenberichte BERECHNUNG VON AGENTGID.

Spalten mit dem Vormonatsvergleich gibt es ab der November-Ausgabe. Downloads: Index für KW 43.

KOLOPHON

Wie diese Ausgabe entstand

The Agent Ledger ist der monatliche Überblick von AgentGid über KI-Agenten. Die meisten Zahlen stammen aus eigenen Daten von AgentGid: dem Katalog, Statusprüfungen alle 30 Minuten, monatlichen Preis-Snapshots und GitHub-Releases. Der Rest stammt aus offiziellen Quellen: Anbieter-Blogs, Preisseiten, Sicherheitshinweisen und der Hacker-News-API. Jede Zahl verlinkt auf ihre Quelle.

Kennzeichnung von Anbieterangaben: LAUT ANBIETER. Unsere eigenen Berechnungen: BERECHNUNG VON AGENTGID. Der Gid Score misst Verbreitung und Interesse, nicht Qualität. Für dieses Magazin testen wir keine Produkte.

Die Texte entwirft ein KI-Redakteur auf Basis eines eingefrorenen Monats-Snapshots; ein zweiter, unabhängiger Prüfer gleicht sie Zeile für Zeile mit den Quellen ab, und ein menschlicher Redakteur gibt sie vor der Veröffentlichung frei. Die Titelillustration ist mit FLUX.1 schnell erzeugt; Titelkopf und Satz stammen von AgentGid.

Einen Fehler gefunden? Korrekturen erscheinen in der nächsten Ausgabe und, mit Datum versehen, in dieser.