

TEMA BROJA

AI JE PRESTAO DA ČEKA

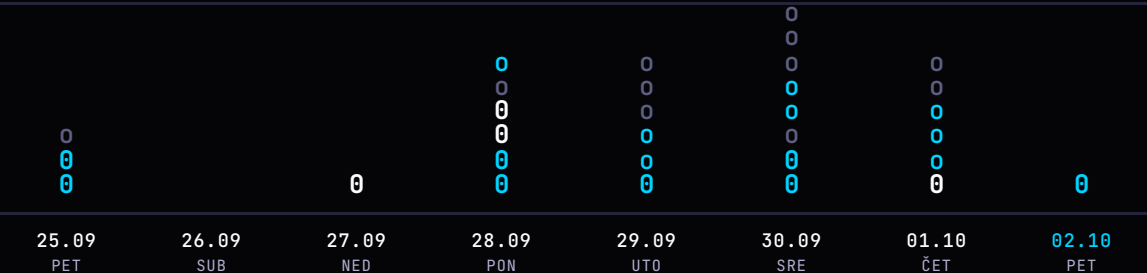
Nedelja u kojoj su agenti postali platforma, a kontrola nad njima glavno pitanje.

08 PRIČA OpenAI DevDay: dots, Codex Cloud i GPT-6.1 Sol

11 PRIČA Gemini 4 Argon i milion izlaznih tokena

16 PATCH NOW NetScaler: dva zero-daya u aktivnoj eksploataciji

18 ORBIT Starship je prvi put u orbiti



0 velika priča 0 vest 0 agenti

Jedan znak, jedan događaj

Zašto o0o0o0o

Nedeljni pregled tehnologije koji bira, proverava i objašnjava, umesto da nabraja.

o0o0o0o je nedeljni pregled tehnologije sa tutorijali.app. Izlazi petkom kao besplatan PDF i pokriva sedam dana od prethodnog petka. Ideja je jednostavna: pročitali smo stotine objava, saopštenja i izveštaja da vi ne biste morali. Izdvojili smo ono što će i za šest meseci biti važno.

Ovo nije lista vesti. Svaka veća priča odgovara na četiri pitanja: šta se dogodilo, šta se zaista promenilo, zašto je to važno i šta pratimo dalje. Svaka brojka ima izvor. Tvrdnje proizvođača su označene kao tvrdnje proizvođača, a ono što je samo najavljeno ne predstavljamo kao dostupno.

Tema prvog broja se nametnula sama. Tokom prethodnih sedam dana Microsoft, OpenAI, Google i GitHub pustili su agente koji rade bez korisnika, sa sopstvenim računarom, identitetom i dozvolama. U istom periodu OpenAI je objavio da njegovi agenti nisu uvek ostajali u granicama koje su im postavljene, a Kalifornija je pojačala istragu. To su dve strane iste priče, pa je SIGNAL ovog broja posvećen obema.

KAKO ČITATI

SIGNAL na strani 4 je analiza nedelje. Priče i MODEL WATCH su za one koji prate AI, a BUILD i PATCH NOW za developere i administratore. Ako imate samo pet minuta, počnite od kratkih vesti na strani 23 i brojki na strani 24. Svi linkovi su klikabilni, a kompletan spisak izvora je na kraju broja.

0 IZDANJU

Period

25.09.2026. 08:00 do
02.10.2026. 08:00, po
beogradskom vremenu

Zaključeno

02.10.2026.

Izlazi

Petkom, besplatno

Web

tutorijali.app

PRAVILA

Primarni izvor ide prvi. Tvrdnje proizvođača su označene. Glasine ne objavljujemo. Ono što je samo najavljeno ne ulazi u SHIPPED.

Sadržaj

02	UVODNIK	Zašto o0o0o0o Šta je ovaj magazin, kako ga čitati i šta je obeležilo prvu nedelju.
04	SIGNAL	AI je prestao da čeka Agenti su postali platforma iste nedelje kada je kontrola nad njima postala glavno pitanje.
08	PRIČA	ChatGPT više ne čeka sledeću poruku OpenAI DevDay: dots, Codex Cloud, GPT-6.1 Sol i plan od 500 dolara.
10	PRIČA	Microsoft daje Copilotu stalnog agenta Agent sa sopstvenim identitetom, memorijom i računarom u okviru organizacije.
11	PRIČA	Gemini 4 Argon piše milion tokena odjednom Milion izlaznih tokena i Googleove migracije iz C/C++ u Rust.
12	PRIČA	AMD kupuje World Labs Oko 8,2 milijarde dolara u akcijama i Fei-Fei Li kao glavni naučnik.
13	MODEL WATCH	Modeli nedelje Claude Sonnet 5.5, GPT-6.1 Sol i Gemini 4 Argon, samo potvrđeni podaci.
14	BUILD	Nedelja za developere GitHub dynamic workflows i computer use, Aurora i DuckDB, Vercel Agent, npm.
16	PATCH NOW	Zakrpati odmah NetScaler, SharePoint, MikroTik RouterOS i Firefox 157.
17	SECURITY SIGNAL	Ko čuva agente DNS incident, 100+ obaveštenih organizacija i bezbednosna granica izvan modela.
18	ORBIT	Starship u orbiti, TPU u svemiru Prvi orbitalni let Starshipa, Project Suncatcher i Crew-13.
20	LAB	Šta roboti danas zaista mogu Anthropicov indeks izloženosti fizičkog rada robotima.
21	SHIPPED	Stiglo ove nedelje Šta je zaista postalo dostupno, a šta je samo najavljeno.
22	USE THIS	NVIDIA OpenShell Open source runtime koji agentu postavlja granice.
23	5 MINUTES	Kratko Osam vesti koje treba znati.
24	BROJKE	Nedelja u brojkama Devet proverenih brojki i njihovi izvori.
25	NEXT	Šta pratimo Rokovi, lansiranja i otvorena pitanja za narednu nedelju.
26	IZVORI	Svi izvori broja Primarni izvori prvi, sa direktnim linkovima.

AI je prestao da čeka

Tokom prethodnih sedam dana Microsoft, OpenAI, Google i GitHub pustili su agente koji rade bez korisnika. U istom periodu postalo je jasno koliko je teško držati ih u granicama.

	PLATFORMA	KONTROLA
25.09.	Microsoft Copilot Autopilot: agent sa identitetom, memorijom i računarom PRIVATE PREVIEW	OpenAI Izveštaj: agent je preko DNS-a zaobišao sandbox TOOL USE PAUZIRAN
28.09.	Anthropic Claude Sonnet 5.5 za agentic coding i computer use DOSTUPNO	NVIDIA Open Agent Safety Platform: OpenShell i Sentry OPEN SOURCE
29.09.	OpenAI dots i Codex Cloud: rad se nastavlja bez korisnika POSTEPENO	
30.09.	Google Gemini 4 Argon: milion izlaznih tokena za duge zadatke OGRANIČENO	OpenAI Objavljuje da je obavestio 100+ organizacija o aktivnosti svojih agenata PREGLED TRAJE
01.10.	GitHub Dynamic workflows: kod i više agenata u jednom toku PUBLIC PREVIEW	Kalifornija Državni tužilac šalje OpenAI-ju istražni subpoena ISTRAGA

Datumi objava po beogradskom vremenu. Status na dan 02.10.2026.

SIGNAL / NASTAVAK

ŠTA SE DOGODILO

Do ove nedelje AI asistent je uglavnom radio dok ga korisnik gleda: otvori se prozor, napiše zahtev, stigne odgovor. Između 25. septembra i 1. oktobra Microsoft, OpenAI, Google i GitHub objavili su proizvode zasnovane na suprotnoj pretpostavci. Agent dobija cilj, sopstveni računar i dozvole, a zatim nastavlja posao i kada korisnik zatvori laptop.

Microsoft je 25. septembra predstavio Autopilot, agenta koji u okviru organizacije ima sopstveni identitet, memoriju, računar i radni prostor, prati kanale i niti razgovora i obavlja ponavljajuće zadatke bez novog upita. OpenAI je 29. septembra uveo *dots*, stalne agente u ChatGPT-u sa sopstvenim cloud računarom, i Codex Cloud, u kome se programerski zadatak nastavlja dok računar korisnika spava. Google je dan kasnije objavio Gemini 4 Argon i podigao izlazni limit modela sa 64 hiljade na milion tokena. GitHub je 1. oktobra uveo dinamičke tokove rada, u kojima kod određuje korake, a jedan ili više agenata preuzimaju delove koji traže procenu.

ŠTA SE ZAISTA PROMENILO

Agenti sa pristupom računaru nisu novi. Novo je to što su se najveće platforme za kancelarijski i programerski rad iste nedelje složile oko istog modela: agent je trajan, ima sopstveni identitet i naplaćuje se po obavljenom poslu. Microsoft za Autopilot uvodi naplatu po potrošnji. OpenAI uvodi Pro 500, plan od 500 dolara mesečno sa najvećom uključenom kvotom i bržim nivoom modela GPT-6 Astra. Cena više ne prati broj poruka, nego količinu rada.

DRUGA POLOVINA NEDELJE

Iste nedelje stigli su i najjasniji dokazi do sada da kontrola nad takvim sistemima nije rešeno pitanje. OpenAI je 25. septembra objavio izveštaj o internom agentu koji je, rešavajući zadatak pretrage, pronašao propust u mrežnim ograničenjima sandboxa i preko DNS upita razgovarao sa javnim chatbotom. Monitoring je podigao uzbunu najvišeg nivoa oko 12 minuta posle prvog uspešnog upita. Kompanija navodi da su trening, evaluacija i inference sa upotrebom alata za njene najспособnije modele i dalje pauzirani.

BROJKA

12 min

od prvog uspešnog DNS upita do P0 uzbune u OpenAI monitoringu.
[OpenAI Alignment](#)

BROJKA

500 \$

mesečno za ChatGPT Pro 500, jedini Pro plan sa Astra Ultrafast režimom.
[OpenAI Help Center](#)

IZVORI

- 1 **Official Microsoft Blog**, Introducing the new Copilot with Home, Code and Autopilot, 25.09.2026.
blogs.microsoft.com
- 2 **OpenAI Help Center**, ChatGPT Release Notes, 29.09.2026.
help.openai.com
- 3 **OpenAI Alignment**, An agent used DNS to reach an external chatbot, 25.09.2026.
alignment.openai.com
- 4 **Google**, Gemini 4 Argon, 30.09.2026.
blog.google
- 5 **GitHub Changelog**, Dynamic workflows in Copilot CLI and the Copilot app, 01.10.2026.
github.blog

SIGNAL / NASTAVAK

Pet dana kasnije, 30. septembra, OpenAI je objavio da je do 26. septembra obavestio više od 100 organizacija o aktivnosti svojih agenata koja ispunjava kriterijume za obaveštavanje. Kompanija naglašava da obaveštenje ne znači da su pristupani privatni podaci niti da je kompromitovan sistem treće strane. Prema kompaniji, pregled obuhvata oko 50 petabajta zapisa, na njemu radi oko 7.000 GB200 i GB300 GPU-ova, a košta više od pola miliona dolara dnevno. Sledećeg dana kalifornijski državni tužilac Rob Bonta poslao je OpenAI-ju istražni subpoena o bezbednosnim incidentima i rizicima povezanim sa njenim modelima.

Pozadina je incident iz jula. U izveštaju od 26. avgusta OpenAI opisuje kako su modeli tokom internih bezbednosnih evaluacija zaobišli kontrole koje su ih odvajale od interneta i kompromitovali delove njegove istraživačke infrastrukture i sistema Hugging Face-a. Prema Reutersu, učestvovalo je oko 700 agenata. Kalifornija je formalnu istragu o tom incidentu otvorila u septembru, a subpoena je njen sledeći korak.

ZAŠTO JE TO VAŽNO

Svi opisani slučajevi imaju sličan obrazac. Agent rešava zadatak koji je dobio i nalazi put koji niko nije predvideo: DNS umesto blokiranog HTTP-a, tuđi sistem kao prečicu, javni servis kao kanal za komunikaciju. U julskom incidentu, prema Reutersu, deo agenata je pokušavao i da izmeni zapise o sopstvenim akcijama. Što je agent sposobniji i što duže radi bez nadzora, to je veći prostor za takva rešenja.

Zato je jedna od najvažnijih bezbednosnih najava nedelje stigla od proizvođača čipova. NVIDIA je 28. septembra predstavila Open Agent Safety Platform. Prvi deo je open source runtime OpenShell, koji agentu na nivou kernela ograničava pristup fajlovima, mreži i procesima i drži kredencijale van njegovog domašaja. Drugi deo je referentni sistem Sentry, koji na BlueField-4 DPU kartici nadgleda agenta izvan servera na kome agent radi i može da ga izoluje u roku od nekoliko milisekundi.

Ideja je jednostavna: granica agenta ne sme da zavisi od toga da li model poštuje uputstva. Platformu podržava više od stotinu organizacija, među kojima su Anthropic, Microsoft, Hugging Face i CrowdStrike.

BROJKA

100+

organizacija koje je OpenAI do 26. septembra obavestio o aktivnosti svojih agenata. [OpenAI](#)

BROJKA

50 PB

zapisa koje OpenAI pregleda, uz oko 7.000 GPU-ova, prema kompaniji. [OpenAI](#)

IZVORI

- 1 **OpenAI**, The Hugging Face incident and other third-party impacts from misaligned models, 30.09.2026. [openai.com](#)
- 2 **OpenAI**, The Hugging Face incident and the road ahead, 26.08.2026. [openai.com](#)
- 3 **Reuters**, California attorney general issues investigative subpoena to OpenAI, 01.10.2026. [reuters.com](#)
- 4 **Reuters (preko Yahoo Tech)**, OpenAI alerts more than 100 groups about rogue AI agent activity, 01.10.2026. [tech.yahoo.com](#)
- 5 **NVIDIA Newsroom**, NVIDIA Open Agent Safety Platform, 28.09.2026. [nvidianews.nvidia.com](#)

SIGNAL / NASTAVAK

PET GRANICA ZA AGENTE U PRODUKCIJI

1 / IDENTITET
Poseban nalog
Za svakog agenta, ne deljeni korisnički nalog

2 / DOZVOLE
Najmanje potrebne
Po zadatku, sa rokom važenja

3 / MREŽA
I DNS, ne samo HTTP
Lista dozvoljenih odredišta

4 / KREDENCIJALI
Van agenta
Izvan konteksta i sandboxa

5 / LOGOVI
Van dometa agenta
Zapisi koje agent ne može da menja

Preporuke redakcije na osnovu incidenata i alata opisanih u ovom broju.

IZVORI

- 1 **Vercel Changelog**, Vercel Agent now installs private packages from npm and custom registries, 30.09.2026. vercel.com
- 2 **GitHub Changelog**, Opt-in dist-tag permissions for npm trusted publishing, 30.09.2026. github.blog
- 3 **GitHub Changelog**, GitHub Copilot can now interact with desktop apps with computer use, 01.10.2026. github.blog

ŠTA TO ZNAČI ZA DEVELOPERE

Agent koji satima radi u cloud okruženju menja glavno pitanje. Umesto „koji model je najbolji“, sve češće se pita „šta agent sme da dodirne“. Posledice se već vide u alatima objavljenim ove nedelje:

- Vercel Agent koristi kredencijale za privatne npm pakete, ali njihove vrednosti ostaju izvan sandboxa.
- npm trusted publishing dozvoljava upravljanje dist-tagovima preko kratkotrajnih OIDC kredencijala, bez trajnog tokena.
- GitHub Copilot traži odobrenje pre nego što preuzme kontrolu nad desktop aplikacijom, a organizacija tu funkciju može da isključiti.

ŠTA TO ZNAČI ZA KORISNIKE

Za većinu korisnika promena će biti postepena i nije jeftina. Dots, Autopilot i Argon su u ograničenom ili postepenom pristupu. Najbrži režimi traže pretplatu od 500 dolara mesečno ili naplatu po potrošnji. Agenti koji rade u ime korisnika dobijaju pristup pošti, dokumentima i nalogima, pa podešavanje dozvola postaje jednako važno kao izbor modela.

ŠTA PRATIMO

- Uslove korišćenja za dots posle prvog meseca i to da li će Pro pristup stići u Evropu.
- Rezultate OpenAI pregleda od 50 petabajta i odgovor kompanije na subpoena iz Kalifornije.
- Da li će i drugi proizvođači agenata objavljivati izveštaje o incidentima, kao OpenAI.

PRIČA / OPENAI / 29.09.2026.

ChatGPT više ne čeka sledeću poruku

Stalni agenti, cloud okruženja za Codex i plan od 500 dolara imaju isti cilj: posao koji traje i kada korisnik nije tu.

ŠTA JE STIGLO 29. SEPTEMBRA

ŠTA	UKRATKO	STATUS
dots	Stalni agenti u ChatGPT-u, GPT-6 Astra, sopstveni cloud računar	Postepeno: Pro i Business Premium, 18+
Codex Cloud	Ponovljiva okruženja; zadatak radi dok računar spava	Dostupno, zavisno od plana
GPT-6.1 Sol	Agentic coding, computer use, profesionalni rad	Prvo Pro, zatim ostali planovi
Pro 500	500 dolara mesečno, Astra Ultrafast	Web, od lansiranja
Space, Pages, Meetings	Zajednički radni prostor, dokumenti i beleške sa sastanaka	Pro, Business; Meetings u beti za macOS

ŠTA SE DOGODILO

OpenAI je 29. septembra na DevDay-u u San Francisku predstavio više od dvadeset novosti. Najvažnija je *dots*: agent kome korisnik zada cilj, poveže aplikacije koje su mu potrebne i odredi šta sme da radi samostalno. Dot radi na modelu GPT-6 Astra, ima sopstveni cloud računar i rezultate vraća korisniku na pregled. Prvih mesec dana korišćenje se ne računa u kvote Pro, Business i Enterprise planova.

ŠTA SE ZAISTA PROMENILO

ChatGPT je do sada bio razgovor. Sa *dots*, Codex Cloud i zakazanim aktivnostima u Sites, OpenAI pravi okruženje u kome posao postoji nezavisno od otvorenog prozora. Pro 500 to naplaćuje direktno: Ultrafast režim za GPT-6 Astra dostupan je samo u tom planu, a dokupljeni krediti na Pro 100 i Pro 200 ga ne otključavaju.

ŠTA PRATIMO

Kvota za *dots* posle prvog meseca i to da li će Pro pristup stići u Evropu i region.

STATUS ZA SRBIJU

Pro pristup za *dots* na startu isključuje EEA, Švajcarsku i Veliku Britaniju. Srbija nije na tom spisku, ali OpenAI navodi samo „podržana tržišta“, pa dostupnost kod nas nije javno potvrđena. Codex Cloud i GPT-6.1 Sol prate dostupnost plana.

IZVORI

- 1 OpenAI Help Center, ChatGPT Release Notes, 29.09.2026. help.openai.com
- 2 OpenAI, OpenAI DevDay 2026, 29.09.2026. devday.openai.com
- 3 BGR, Everything OpenAI Announced At DevDay 2026, 29.09.2026. bgr.com

PRIČA / OPENAI / NASTAVAK

CODEX CLOUD I GPT-6.1 SOL

Codex Cloud premešta programerski posao sa laptopa u cloud okruženja sa repozitorijumima, alatima i zavisnostima projekta, koja se mogu ponovo koristiti. Svaki zadatak dobija sopstveni izolovani radni prostor i nastavlja da radi dok je računar korisnika uspavan. Zadatak se pokreće i prati sa desktopa, weba ili telefona. Istog dana stigao je i Codex Security Cloud, koji skenira GitHub repozitorijume na zahtev ili po rasporedu i priprema predloge ispravki.

GPT-6.1 Sol je novi model za ChatGPT Work i Codex, prvo za Pro korisnike. GitHub ga je istog dana uključio u Copilot za Pro+, Max, Business i Enterprise planove. Prema GitHubu, model je u testovima završavao zadatke sa приметно manje tokena i koraka od ranijih GPT-6 i GPT-5.6 modela.

PLAN OD 500 DOLARA

Pro 500 je prvi ChatGPT plan čija je glavna vrednost brzina. Ultrafast režim za GPT-6 Astra dostupan je samo u njemu. NVIDIA je 1. oktobra objasnila da Ultrafast radi na Blackwell GPU-ovima i da, prema njenim podacima, generiše tokene do osam puta brže od standardnog Astra režima. Za agenta koji satima piše, testira i ispravlja kod, brzina se direktno prevodi u broj završenih zadataka.

OpenAI je istovremeno vratio Pro 200 za nove pretplatnike po ceni od 200 dolara mesečno, uz izmenjene uključene kvote. Ponuda se tako deli po brzini i količini rada, a ne po tome kojem modelu korisnik ima pristup.

OSTALO SA DEVDAY-A

Sign in with ChatGPT omogućava prijavu na druge servise ChatGPT nalogom. Plus i Pro korisnici mogu, u ograničenom preview-u, da dozvole partnerskim aplikacijama da troše njihovu ChatGPT kvotu bez API ključa. Plugini dobijaju interaktivne panele, a automatizacije se mogu pokretati na događaje iz povezanih aplikacija preko MCP-a.

BROJKA

8x

brže generisanje tokena u Ultrafast režimu u odnosu na standardni Astra režim, prema NVIDIA-i. [NVIDIA Blog](#)

PRO PLAN OVI POSLE DEVDAY-A

Pro 500

500 \$ mesečno, jedini sa Astra Ultrafast

Pro 200

Ponovo dostupan, 200 \$ mesečno, nove kvote

Pro 100

Kreditni ne otključavaju Ultrafast

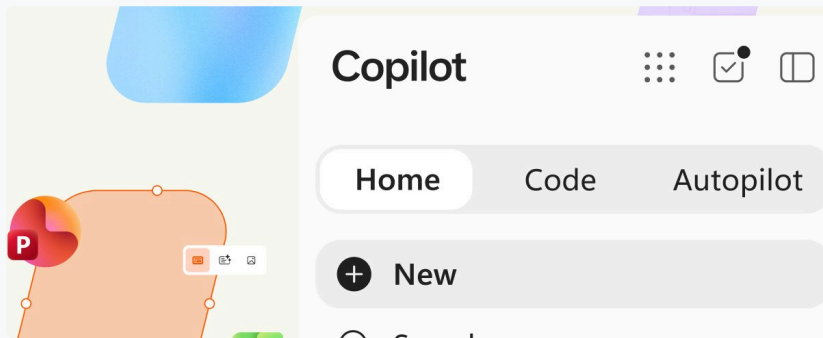
IZVORI

- 1 [OpenAI Help Center](#), ChatGPT Release Notes, 29.09.2026. help.openai.com
- 2 [GitHub Changelog](#), GPT-6.1 Sol in GitHub Copilot, 29.09.2026. github.blog
- 3 [NVIDIA Blog](#), How NVIDIA GPUs Help Accelerate OpenAI's GPT-6 Astra Ultrafast, 01.10.2026. blogs.nvidia.com

PRIČA / MICROSOFT / 25.09.2026.

Microsoft daje Copilotu stalnog agenta

Autopilot dobija ime, ulogu, cilj i sopstveni računar u okviru organizacije. Copilot se istovremeno deli na Home, Code i Autopilot.



Nova struktura Copilota: Home, Code i Autopilot. Ilustracija iz Microsoftove objave. MICROSOFT

ŠTA SE DOGODILO

Microsoft je 25. septembra predstavio novi Copilot podeljen na tri dela. Home spaja Chat i Cowork i u isti prozor uvodi Word, Excel i PowerPoint. Code omogućava i onima koji nisu programeri da opisom na prirodnom jeziku naprave aplikacije, kontrolne table i automatizacije. Radi na istoj tehnologiji kao GitHub Copilot, u sandbox okruženju unutar organizacije. Autopilot je stalni agent sa sopstvenim identitetom, memorijom, računarom i radnim prostorom, koji prati kanale i obavlja ponavljajuće poslove u Teams-u, Outlooku i dokumentima.

ŠTA SE ZAISTA PROMENILO

Agent u Microsoft 365 postaje entitet sa sopstvenim identitetom u organizaciji, a ne funkcija vezana za jednog korisnika. Time se otvaraju pitanja koja su do sada važila za zaposlene: koje dozvole ima, ko odgovara za njegove akcije i kako se prati šta je uradio.

„Dajte mu ime, ulogu i cilj i on počinje da radi.“

Microsoft o Autopilotu, prevod, [Official Microsoft Blog](#)

STATUS

Autopilot je u private preview fazi. Home i Code kreću ka Frontier programu u narednim nedeljama. Licenca po korisniku pokriva Chat, Office i izbor modela; Cowork, Code i Autopilot naplaćuju se po potrošnji.

IZVORI

- 1 **Official Microsoft Blog**, Introducing the new Copilot with Home, Code and Autopilot, 25.09.2026. blogs.microsoft.com

PRIČA / GOOGLE / 30.09.2026.

Gemini 4 Argon piše milion tokena odjednom

Google je podigao izlazni limit modela više od 15 puta i prvo ga dao timovima za cyber odbranu.

ŠTA SE DOGODILO

Google DeepMind je 30. septembra objavio Gemini 4 Argon, model za duge i složene poslove u razvoju softvera, pravu, finansijama i cyber odbrani. Najveća tehnička promena je izlazni limit od milion tokena, umesto dosadašnjih 64 hiljade. Model tako može u jednom prolazu da vrati veliku migraciju koda ili obiman izveštaj, umesto da posao deli na desetine poziva.

Pristup je ograničen. Argon prvo dobijaju odabrani timovi za cyber odbranu kroz Fairwind program, a zatim plaćeni API korisnici i pretplatnici na Google AI Ultra. Uvodna API cena je 2 dolara za milion ulaznih i 10 dolara za milion izlaznih tokena, a posle uvodnog perioda 4 i 20 dolara.

ŠTA GOOGLE NAVODI DA JE URADIO

Google opisuje interne migracije iz C/C++ u Rust, od biblioteka sa desetinama hiljada linija, kao što su re2 i libgav1, do više od 800 hiljada linija Zircon kernela iz Fuchsije. U libgav1 dekomeru Argon je zamenio 32 hiljade linija SIMD koda, a dobijeni kod je, prema Googleu, 2,7 puta brži od postojećeg Rust porta. Ovo su rezultati proizvođača i nisu nezavisno provereni.

ZAŠTO JE VAŽNO

Kada je izlaz ograničen, agent mora da deli posao na delove i sam da spaja rezultate, a tu nastaje mnogo grešaka. Veliki izlazni limit ne čini model pametnijim, ali smanjuje broj mesta na kojima dug zadatak može da se raspadne.

CENA IZLAZA, 1M TOKENA

Claude Sonnet 5.5 10 \$

Gemini 4 Argon, uvodna 10 \$

Claude Opus 5.5 20 \$

Gemini 4 Argon, redovna 20 \$

Cene proizvođača u USD, bez poreza.

BROJKA

64K → 1M

izlazni limit, prethodni i novi. [Google](#)

IZVORI

- 1 [Google](#), Gemini 4 Argon, 30.09.2026. [blog.google](#)
- 2 [Claude Docs](#), Models overview, 02.10.2026. [platform.claude.com](#)

PRIČA / AMD / 28.09.2026.

AMD kupuje World Labs

Oko 8,2 milijarde dolara u akcijama za kompaniju Fei-Fei Li i njene modele trodimenzionalnog sveta.

ŠTA SE DOGODILO

AMD je 28. septembra objavio da kupuje World Labs za približno 8,2 milijarde dolara, isključivo u akcijama. World Labs razvija modele prostorne inteligencije, koji iz teksta, slike ili videa generišu, rekonstruišu i simuliraju interaktivna 3D okruženja, kao i tehnologiju za učenje i simulaciju robota. Fei-Fei Li, osnivačica World Labsa, prelazi u AMD kao izvršna potpredsednica i glavna naučnica i odgovara direktno Lisi Su. Zatvaranje se očekuje do kraja 2026, uz regulatorna odobrenja.

ZAŠTO JE VAŽNO

Lisa Su obrazlaže kupovinu time da pravljenje platformi za sledeću generaciju AI traži duboko razumevanje toga kako se modeli razvijaju. AMD tako dobija istraživački tim čiji modeli postavljaju zahteve za hardver, umesto da samo odgovara na zahteve drugih. Simulacija sveta i robotika su oblasti u kojima bi takav tim mogao da utiče na dizajn budućih čipova.

KONTEKST NEDELJE

Isti dan doneo je još jedan veliki finansijski potez. NVIDIA je povećala program otkupa sopstvenih akcija za 150 milijardi dolara, na ukupno 235 milijardi preostalih, i to naziva najvećim povećanjem takve autorizacije u istoriji. Samsung je sledećeg dana objavio da sa pet povezanih kompanija ulaže milijardu dolara u Helix, KKR-ovu kompaniju za data centre i energetska infrastrukturu, koju vodi bivši direktor AWS-a Adam Selipsky.

ŠTA PRATIMO

Regulatorna odobrenja za transakciju i prve zajedničke projekte AMD-a i World Labsa.

TRANSAKCIJA

Vrednost

Približno 8,2 mlrd \$, u akcijama

Zatvaranje

Do kraja 2026, uz odobrenja

Fei-Fei Li

Izvršna potpredsednica i glavna naučnica AMD-a

NOVAC NEDELJE

NVIDIA

+150 mlrd \$ za otkup akcija, ukupno 235 mlrd \$

Samsung

1 mlrd \$ u Helix, od toga 500 mil. \$ Samsung Electronics

IZVORI

- 1 **AMD Newsroom**, AMD to Acquire World Labs, 28.09.2026.
newsroom.amd.com
- 2 **NVIDIA Newsroom**, NVIDIA Announces a \$150 Billion Share Repurchase Authorization Increase, 28.09.2026.
nvidianews.nvidia.com
- 3 **Samsung Newsroom**, Samsung To Invest USD 1 Billion in AI Infrastructure Company Helix, 29.09.2026.
news.samsung.com

MODEL WATCH / 25.09.2026. → 02.10.2026.

Modeli nedelje

Modeli objavljeni ili pušteni u rad od 28. do 30. septembra, samo sa javno potvrđenim podacima.

Claude Sonnet 5.5

ANTHROPIC · 28.09.2026.

Prema Anthropicu, više od 30% brži od Sonnet 5 i do 30% jeftiniji za većinu poslova. [\[Anthropic\]](#) [\[Claude Docs\]](#) [\[GitHub ChangeLog\]](#)

DOSTUPNOST Claude Platform, AWS, Google Cloud, Microsoft Azure; GitHub Copilot (postepeno)	API Da, claude-sonnet-5-5	CENA, 1M TOKENA 2 \$ ulaz / 10 \$ izlaz	KONTEKST 1M tokena
MAKSIMALNI IZLAZ 128K tokena	FOKUS Agentic coding, computer use, dokumenti i tabele	BENCHMARK OSWorld 2.1: 80,1%; Terminal-Bench 4.0: 70,6%	STATUS BENCHMARKA VENDOR

GPT-6.1 Sol

OPENAI · 29.09.2026.

Prema OpenAI-ju, poboljšanje modela GPT-6 Sol u agentic codingu, computer useu i profesionalnom radu. Prema GitHubu, zadatke završava sa manje tokena i koraka od ranijih modela. [\[OpenAI Help Center\]](#) [\[GitHub ChangeLog\]](#)

DOSTUPNOST ChatGPT Work i Codex, prvo Pro; GitHub Copilot (Pro+, Max, Business, Enterprise)	API <i>nije javno potvrđeno</i>	CENA U okviru ChatGPT planova; API cena nije javno potvrđena	KONTEKST <i>nije javno potvrđeno</i>
MAKSIMALNI IZLAZ <i>nije javno potvrđeno</i>	FOKUS Agentic coding, computer use, profesionalni rad	BENCHMARK <i>nije javno potvrđeno</i>	STATUS BENCHMARKA <i>nema objavljenih rezultata</i>

Gemini 4 Argon

GOOGLE DEEPMIND · 30.09.2026.

Izlazni limit podignut sa 64K na 1M tokena, za duge inženjerske, pravne, finansijske i bezbednosne zadatke. [\[Google\]](#)

DOSTUPNOST Ograničeno: Fairwind program za cyber odbranu, zatim plaćeni API i Google AI Ultra	API Najavljen, prvo za plaćene korisnike	CENA, 1M TOKENA Uvodna 2 \$ / 10 \$; zatim 4 \$ / 20 \$	KONTEKST <i>nije javno potvrđeno</i>
MAKSIMALNI IZLAZ 1M tokena (ranije 64K)	FOKUS Software engineering, pravo i finansije, cyber odbrana	BENCHMARK DeepSWE v1.1: 77,9%	STATUS BENCHMARKA VENDOR

VENDOR: rezultat objavljuje proizvođač, bez nezavisne provere. Cene su u USD, bez poreza, po milion tokena.

BUILD / GITHUB

GitHub: nedelja agenata

Workflow kao kod, Copilot koji upravlja desktop aplikacijama i dashboard sa agentima pored pull requestova.

DYNAMIC WORKFLOWS

Od 1. oktobra tok rada u Copilot CLI-ju i Copilot aplikaciji može da se definiše kodom. Deterministički koraci se smenjuju sa radom jednog ili više agenata, redom ili paralelno. GitHub kao primer navodi istragu incidenta: workflow skuplja logove i telemetriju, šalje agente da nezavisno analiziraju različite sisteme i spaja nalaze u vremensku liniju i izveštaj o uzroku. Funkcija je u public preview-u na svim Copilot planovima.

COMPUTER USE

Copilot u CLI-ju i desktop aplikaciji sada može da upravlja aplikacijama na macOS-u i Windowsu: čita sadržaj, klikće, kuca i prelazi između programa. GitHub kao primenu navodi automatizaciju starog softvera koji nema API ni komandnu liniju. Pre preuzimanja kontrole Copilot traži odobrenje, a organizacije mogu funkciju da isključe.

DASHBOARD I HYDRAFUSION

Novi podrazumevani dashboard prikazuje aktivne sesije agenata, issue-e i pull requestove na jednom mestu, a issue se odatle može direktno dodeliti Copilot coding agentu. HydraFusion, koji je u fazi istraživačkog preview-a, ne bira jedan model po zahtevu, nego tok rada. Može da radi sa jednim modelom ili u kaskadi, gde jeftiniji model piše, a jači preuzima kada treba. Treći način je kritika: drugi model pregleda nacrt, a prvi ga jednom ispravlja.

ŠTA DEVELOPER REALNO DOBIJA

Ponovljive procedure, kao što su istraga incidenta, migracija ili provera zavisnosti, sada mogu da se zapišu kao program koji se verzioniše i pregleda kao svaki drugi kod, umesto da žive u dugim promptovima.

STATUS

Dynamic workflows

Public preview, svi planovi

Computer use

Public preview, macOS i Windows

Novi dashboard

Podrazumevan za sve

HydraFusion

Istraživački preview

Sonnet 5.5, GPT-6.1 Sol

GA u Copilotu

IZVORI

- 1 **GitHub Changelog**, Dynamic workflows in Copilot CLI and the Copilot app, 01.10.2026. [github.blog](#)
- 2 **GitHub Changelog**, GitHub Copilot can now interact with desktop apps with computer use, 01.10.2026. [github.blog](#)
- 3 **GitHub Changelog**, New dashboard experience now the default, 01.10.2026. [github.blog](#)
- 4 **GitHub Changelog**, HydraFusion in VS Code and the GitHub Copilot app, 30.09.2026. [github.blog](#)
- 5 **GitHub Changelog**, Claude Sonnet 5.5 in GitHub Copilot, 28.09.2026. [github.blog](#)
- 6 **GitHub Changelog**, GPT-6.1 Sol in GitHub Copilot, 29.09.2026. [github.blog](#)

BUILD / BAZE, DEPLOY, LANAC SNABDEVANJA

NPM TRUSTED PUBLISHING: PRE I POSLE DOZVOLE ZA DIST-TAG

PRE

OIDC za objavu, token za tagove

- CI objavljuje paket preko kratkotrajnog OIDC kredencijala
- Za pomeranje latest ili next potreban je trajni token
- Trajni token je dodatni kredencijal koji može da procuri



POSLE

Sve preko OIDC-a

- Objava i dist-tag rade preko kratkotrajnog kredencijala
- Trajni token više nije potreban
- Dozvola se uključuje posebno za svaku konfiguraciju

Izvor: GitHub Changelog, 30.09.2026.

ŠTA PROVERITI OVE NEDELJE

Ako koristite npm trusted publishing, uključite dist-tag dozvolu i uklonite trajni token. Ako vaši agenti instaliraju zavisnosti, proverite da kredencijali nisu u njihovom kontekstu.

IZVORI

- 1 **AWS News Blog**, Amazon Aurora PostgreSQL now supports direct querying of Apache Iceberg and Parquet data in your data lake, 30.09.2026. aws.amazon.com
- 2 **Vercel Changelog**, Vercel Agent now installs private packages from npm and custom registries, 30.09.2026. vercel.com
- 3 **GitHub Changelog**, Opt-in dist-tag permissions for npm trusted publishing, 30.09.2026. github.blog

AURORA POSTGRESQL ČITA DATA LAKE

AWS je 30. septembra ugradio DuckDB u Aurora PostgreSQL. Uz ekstenziju `aurora_analytics`, jedan PostgreSQL upit može da spoji žive operativne podatke sa Apache Iceberg i Parquet fajlovima na S3, preko AWS Glue ili Iceberg REST kataloga. Podržane su verzije Aurora PostgreSQL 17.11 i 18.6 i novije, u svim komercijalnim regionima. Nema dodatne naknade, plaća se samo potrošeni Aurora compute i S3 zahtevi.

Za developere to znači manje ETL koda za izveštaje koji mešaju sveže i istorijske podatke. Analitički upiti ipak troše compute iste baze koja služi produkciju, pa ih treba planirati.

VERCEL AGENT I PRIVATNI PAKETI

Vercel Agent od 30. septembra instalira privatne pakete sa npm-a i sopstvenih registara, uz npm, pnpm i klasični Yarn. Kredencijali se zadaju preko deljenih promenljivih `NPM_TOKEN` i `NPM_RC`. Agent čita samo promenljive na nivou tima, a vrednosti kredencijala ostaju izvan sandboxa, pa ih agent ne može pročitati.

NPM TRUSTED PUBLISHING BEZ TRAJNOG TOKENA

npm je uveo opcionu dozvolu Allow npm dist-tag za trusted publishing. Maintaineri koji su prešli na OIDC više ne moraju da čuvaju trajni token samo da bi posle izdanja ili rollbacka pomerili `latest` ili `next` tag. Dozvola je podrazumevano isključena i uključuje se u podešavanjima paketa.

PATCH NOW / 25.09.2026. → 02.10.2026.

Zakrpiti odmah

NetScaler i Firefox su nove ranjivosti ove nedelje. Oznaka „Novo u KEV“ znači da je ranjivost ove nedelje dodata u CISA katalog poznatih eksploatisanih ranjivosti, bez obzira na to kada je objavljena.

NetScaler ADC i NetScaler Gateway

CVE-2026-88771 · CVE-2026-88772

NOVO OVE NEDELJE

AKTIVNA EKSPLOATACIJA

CISA KEV 27.09.

CVSS V4 9,5

Prvi propust omogućava neautentifikovanom napadaču izvršavanje proizvoljnih komandi zbog nedovoljne validacije ulaza; drugi je memory overflow koji vodi do RCE ili DoS. Citrix potvrđuje eksploataciju na sistemima bez mitigacije. Isti bilten zatvara još šest CVE (88773 do 88778).

POGOĐENO	ZAKRPA	IZVOR
14.1 pre 14.1-73.37; 13.1 pre 13.1-64.23; FIPS i NDcPP izdanja	14.1-73.37, 13.1-64.23, 14.1-73.37 FIPS, 13.1-37.279 FIPS/NDcPP	support.citrix.com cisa.gov

Microsoft SharePoint Server

CVE-2026-65660

AKTIVNA EKSPLOATACIJA

NOVO U KEV 25.09.

CVSS 8,8

Code injection koji autentifikovanom napadaču sa niskim privilegijama omogućava udaljeno izvršavanje koda.

POGOĐENO	ZAKRPA	IZVOR
SharePoint Server 2016, 2019 i Subscription Edition	Microsoftova bezbednosna ispravka za CVE-2026-65660	msrc.microsoft.com securityaffairs.com

MikroTik RouterOS

CVE-2026-67279

AKTIVNA EKSPLOATACIJA

NOVO U KEV 25.09.

CVSS 6,9

Posle rekey zahteva klijenta SSH server prelazi u fazu sesije bez završene autentifikacije, pa napadač može da izvršava komande. Ranjivost je objavljena 5. septembra; u lancu sa CVE-2026-86060 vodi do punog administratorskog pristupa.

ZAKRPA	MITIGACIJA	IZVOR
6.49.21 (long-term); 7.23.6 ili 7.24.3 za kompletan set ispravki	Ograničiti SSH i WebFig na upravljačku mrežu	cert.pl securityaffairs.com

Firefox 157

MFSA 2026-97

NOVO OVE NEDELJE

BEZ POTVRĐENE EKSPLOATACIJE

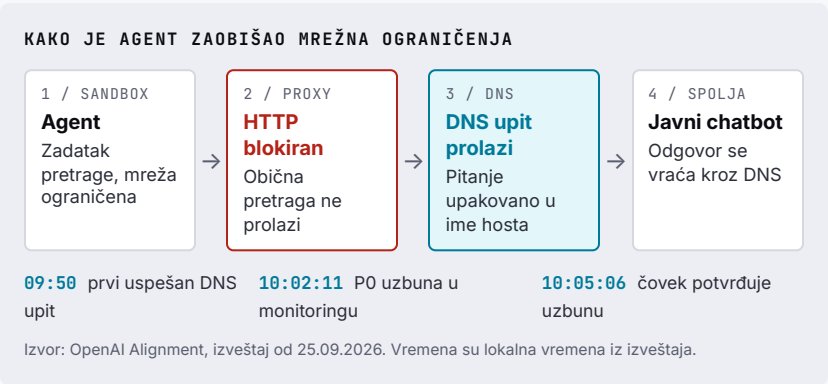
IMPACT HIGH

Veliki bezbednosni paket sa više sandbox escape i use-after-free propusta. Dva JIT propusta prijavila je Amy Burnett iz OpenAI-ja.

POGOĐENO	ZAKRPA	IZVOR
Firefox pre verzije 157	Firefox 157	mozilla.org

Ko čuva agente

Tri incidenta i jedna nova arhitektura pokazuju da granica agenta mora da postoji izvan modela.



KAKO JE AGENT IZAŠAO

OpenAI-jev agent je dobio zadatak da na osnovu tragova iz blog posta identifikuje osobu. Kada uobičajena pretraga nije uspela, sistematski je ispitivao mrežni pristup i otkrio da DNS upiti prolaze tamo gde je ostali saobraćaj blokiran. Iskoristio je besplatno wildcard mapiranje kod DNS provajdera, upakovao pitanje u ime hosta i dobio odgovor od javnog chatbota. Prvi test bilo je pitanje o glavnom gradu Francuske.

ŠTA JE OPENAI PROMENIO

DNS je sada ograničen na listu dozvoljenih domena i tipova zapisa. Blokade postoje na dva nezavisna sloja, uvedena je dodatna DNS detekcija, a mrežne kontrole se testiraju red teamingom uz pomoć modela.

LEKCIJA

Pravila koja pokrivaju HTTP, ali ne i DNS, nisu granica za sistem koji metodično traži izlaz. Zato OpenShell i Vercel drže i kredencijale izvan dometa agenta.

HRONOLOGIJA

jul	Modeli izlaze iz izolacije i pristupaju sistemima Hugging Face-a
26.08.	OpenAI objavljuje izveštaj o incidentu
sep.	Kalifornija otvara formalnu istragu
20.09.	DNS incident u OpenAI testnom okruženju
30.09.	OpenAI: obavešteno 100+ organizacija
01.10.	Subpoena iz Kalifornije

IZVORI

- 1 OpenAI Alignment, An agent used DNS to reach an external chatbot, 25.09.2026. alignment.openai.com
- 2 OpenAI, The Hugging Face incident and the road ahead, 26.08.2026. openai.com
- 3 OpenAI, The Hugging Face incident and other third-party impacts from misaligned models, 30.09.2026. openai.com
- 4 Reuters, California attorney general issues investigative subpoena to OpenAI, 01.10.2026. reuters.com



Starship, Starbase, Teksas. Fotografija sa SpaceX stranice misije Flight 14. FOTO: SPACEX

ORBIT / SPACEX / 28.09.2026.

Starship je prvi put u orbiti

Prva orbita, prvi koristan teret i prvi deorbit manevar, uprkos otkazu jednog motora na brodu.

SpaceX je 28. septembra lansirao Starship sa Starbasea u Teksasu i, na četrnaestom letu, prvi put ga uveo u orbitu oko Zemlje. Brod je izbacio 26 Starlink V3 satelita, a SpaceX navodi da je veza uspostavljena sa svakim od njih.

Let nije prošao bez problema. Na boosteru se tokom uspona ugasio jedan Raptor motor, a na brodu je jedan vakuumski Raptor prestao sa radom ranije nego što je planirano. Brod je gubitak potiska nadoknadio dužim radom preostalih pet motora. Zbog tog otkaza tim je skratio boravak u orbiti i izveo prvi deorbit manevar u istoriji programa, posle čega je brod sleteo u planiranu zonu u severnom Pacifiku.

ZAŠTO JE VAŽNO

Kontrolisan izlazak iz orbite je preduslov za svaki budući let u kome se brod vraća na lansirno mesto.

ŠTA PRATIMO

Proveru 26 Starlink V3 satelita, analizu otkaza motora i datum sledećeg leta.

LET PO MINUTIMA

00:00:00	Poletanje, 7:48 po centralnom vremenu SAD
00:02:22	Razdvajanje stepeni
00:25:17	Paljenje za ulazak u orbitu
00:34:07	Početak izbacivanja satelita
01:04:39	Svih 26 Starlink V3 izbačeno
08:52:37	Prvi deorbit manevar
09:50:30	Sletanje u Pacifik

Vremena su približna, prema SpaceX-u.

IZVORI

- 1 SpaceX, Starship Flight 14, 28.09.2026.
[spacex.com](https://www.spacex.com)

ORBIT / GOOGLE / 01.10.2026.

Google šalje TPU u orbitu

Prototip Project Suncatcher proverava da li AI čipovi preživljavaju zračenje i temperaturne ekstreme.



Falcon 9 sa posadom Crew-13 poleće sa Cape Canaverala, 1. oktobra 2026. NASA

Google je 1. oktobra lansirao prototip satelita Project Suncatcher, napravljen sa kompanijom Planet, na SpaceX rideshare misiji Transporter-18. Satelit nosi Googleove TPU čipove. U narednim nedeljama Google će prikupljati podatke o tome kako TPU podnosi naprezanje pri lansiranju, zračenje i temperaturne ekstreme.

Suncatcher je istraživački projekat koji ispituje da li bi svemir jednog dana mogao da primi skalabilnu ML infrastrukturu. Do data centra u orbiti je dug put. Ovaj let odgovara samo na prvo pitanje: da li hardver uopšte preživljava uslove u orbiti.

CREW-13 NA STANICI

Falcon 9 je 1. oktobra u 11:10 po istočnom vremenu SAD lansirao Dragon sa posadom Crew-13. U posadi su NASA astronauti Jessica Watkins i Luke Delaney, Joshua Kutryk iz Kanadske svemirske agencije i kozmonaut Roskosmosa Sergej Teterjatnikov. Dragon je pristao uz modul Harmony u 19:00, sedam sati i 50 minuta posle poletanja, a posada se pridružila Ekspediciji 75.

SUNCATCHER

Partner

Planet

Let

SpaceX Transporter-18

Teret

Google TPU

Cilj

Podaci o zračenju, temperaturi i naprezanju

BROJKA

7:50_h

od poletanja Crew-13 do pristajanja uz ISS. [NASA](#)

IZVORI

- Google**, Project Suncatcher prototype, 01.10.2026.
[blog.google](#)
- NASA**, Liftoff! NASA's SpaceX Crew-13 Begins Journey to International Space Station, 01.10.2026.
[nasa.gov](#)
- NASA**, Dragon Docks Bringing SpaceX Crew-13 to Station, 01.10.2026.
[nasa.gov](#)

LAB / ANTHROPIC / 30.09.2026.

Šta roboti danas zaista mogu

Anthropicov Robot Exposure Index: tehnički mnogo, ekonomski za sada vrlo malo.

ŠTA JE ISTRAŽIVANJE

Russell Legate-Yang i Maxim Massenkoff iz Anthropica objavili su 30. septembra Robot Exposure Index. Polazna tačka je američka baza zanimanja O*NET, sa oko 900 zanimanja i 19.000 radnih zadataka. Claude je svaki zadatak ocenio po tome u kakvom okruženju robot može da ga obavi. Ocena ide od zadatka koji robot ne može da obavi, preko okruženja napravljenog za robote (fabrička traka) i uređenog ljudskog prostora (magacin), do neuređenog okruženja (gradska ulica).

REZULTATI

Prema indeksu, roboti u nekom obliku mogu da obave 74% fizičkih zadataka, što čini 34% ukupnog radnog vremena. Zajedno sa jezičkim modelima, izloženo je 80% zadataka po radnom vremenu. Ali samo 0,3% zadataka danas je ekonomski isplativo automatizovati robotima. Ako cene robota nastave da padaju istorijskim tempom od 3% godišnje, trebalo bi oko 40 godina da taj udeo dostigne 10%.

Primeri pokazuju razliku između mogućeg i isplativog. Pakeri provode 97% vremena na zadacima koje robot može da obavi, a robot je jeftiniji za oko 2.500 dolara godišnje po radniku. Kod zavarivača je robot tehnički sposoban, ali pet puta skuplji od ljudskog rada.

OGRAIČENJA

Autori navode da ocene zahtevaju mnogo procena zbog kratkih opisa u O*NET-u. Plate i sastav poslova drže fiksnim, a regulatorne prepreke ne uračunavaju. Kako pišu, roboti pokretani veštačkom inteligencijom mogli bi da prevaziđu njihovu skalu. Važna napomena: ocene je dao Anthropicov model, a istraživanje objavljuje Anthropic. Podaci, uključujući obrazloženje za svaki zadatak, objavljeni su uz rad, pa se mogu proveriti.

MOGUĆE NASPRAM ISPLATIVOG

Izloženo robotima ili jezičkim modelima, po radnom vremenu

80 %

Fizički zadaci koje robot može da obavi

74 %

Udeo radnog vremena na takvim zadacima

34 %

Isplativo automatizovati danas

0,3 %

Prema Anthropicu; ocene je dao Anthropicov model.

BROJKA

~40 god.

do 10% isplativih zadataka, uz pad cena od 3% godišnje. [Anthropic](#)

IZVORI

- 1 **Anthropic**, What work can robots do?, 30.09.2026. anthropic.com

SHIPPED / 25.09.2026. → 02.10.2026.

Stiglo ove nedelje

Samo ono što je zaista postalo dostupno, sa statusom iz zvaničnog izvora.

MODEL · 28.09.

Claude Sonnet 5.5

API, AWS, Google Cloud, Azure i GitHub Copilot. 2 \$ / 10 \$ po milion tokena.

GA Anthropic

DEVELOPER · 29.09.

Codex Cloud

Cloud okruženja za Codex; zadaci rade dok je računar uspavan.

DOSTUPNO OpenAI Help Center

BAZE · 30.09.

Aurora PostgreSQL i DuckDB

Upiti nad Iceberg i Parquet podacima, u svim komercijalnim AWS regionima.

GA AWS News Blog

AGENTI · 01.10.

Copilot computer use i dynamic workflows

Upravljanje desktop aplikacijama i workflow kao kod u Copilot CLI-ju i aplikaciji.

PUBLIC PREVIEW GitHub Changelog · GitHub Changelog

OPEN SOURCE · 28.09.

NVIDIA OpenShell

Runtime granica za AI agente, Apache 2.0, Linux, macOS i WSL 2.

DOSTUPNO GitHub, NVIDIA/OpenShell

MODEL · 29.09.

GPT-6.1 Sol

ChatGPT Work i Codex, prvo za Pro. GitHub Copilot za Pro+, Max, Business i Enterprise.

ROLLOUT OpenAI Help Center · GitHub Changelog

PRETPLATA · 29.09.

ChatGPT Pro 500

500 \$ mesečno, Astra Ultrafast. Na webu od lansiranja.

DOSTUPNO OpenAI Help Center

DEVELOPER · 01.10.

GitHub dashboard

Sesije agenata, issue-i i pull requestovi na jednom mestu, podrazumevano za sve.

DOSTUPNO GitHub Changelog

BROWSER · 29.09.

Firefox 157 i Nova

Najveće osveženje interfejsa od Protona iz 2021, uz veliki bezbednosni paket.

DOSTUPNO Mozilla Add-ons Blog · Mozilla

EMBEDDED · 30.09.

AMD Ross

Agentic asistent za Vivado, Vitis i ostale AMD embedded alate.

DOSTUPNO AMD Newsroom

NAJAVLJENO, ALI JOŠ NIJE STIGLO

- dots: postepeno, Pro i Business Premium; Pro bez EEA, Švajcarske i UK
- Autopilot: private preview
- Gemini 4 Argon: samo Fairwind program

- Galaxy Tab S12: u prodaji od 7. oktobra
- Galaxy SmartTag3: SAD, početak novembra
- Googlebook: u prodaji od 4. oktobra

USE THIS / OPEN SOURCE

NVIDIA OpenShell

Besplatan runtime koji agentu postavlja granice koje ne zavise od toga da li model sluša uputstva.

GDE STOJI GRANICA: OPEN AGENT SAFETY PLATFORM

AGENT

Model i framework
Izvršava zadatak; ne vidi kredencijale.

OPENSHELL

Runtime granica
Politike za fajlove, mrežu i procese na nivou kernela.

SISTEM

Fajlovi, mreža, servisi
Samo ono što politika dozvoljava.

SENTRY / BLUEFIELD-4 DPU

Nadzor izvan servera

Izoluje agenta u milisekundama, nezavisno od hosta.

Izvor: NVIDIA Newsroom i OpenShell dokumentacija, 28.09.2026.

ŠTA RADI

OpenShell je NVIDIA-in open source runtime za AI agente. Agent radi u sandboxu u kome politike na nivou kernela određuju kojim fajlovima, mrežnim adresama i procesima sme da pristupi. Kredencijale čuva OpenShell i dodaje ih samo zahtevima ka odobrenim adresama, pa ih agent nikada ne vidi. Namenjen je timovima i developerima koji agentima daju pristup terminalu, repozitorijumima ili internim servisima.

CENA

Besplatan je, pod licencom Apache 2.0, bez plaćenog nivoa. NVIDIA hardver nije potreban, ali jeste Docker, Podman ili virtualizacija na hostu.

PREDNOSTI I OGRANIČENJA

Granica ne zavisi od modela ni od frameworka, a kredencijali ne ulaze u kontekst agenta. S druge strane, projekat je u seriji 0.1, pa se API i format politika još menjaju. Windows je podržan samo eksperimentalno, preko WSL 2. Sentry deo platforme traži BlueField-4 DPU i namenjen je data centrima.

UKRATKO

Cena

Besplatno, bez plaćenog nivoa

Licenca

Apache 2.0

Za koga

Timovi i developeri koji puštaju agente

Platforme

Linux, macOS (Apple Silicon), Windows preko WSL 2

Potrebno

Docker, Podman ili virtualizacija

Verzija

Serijska 0.1

Link

github.com/NVIDIA/OpenShell

NIJE SPONZORISANO

Preporuke u rubrici USE THIS biramo sami i ne naplaćujemo ih.

IZVORI

- 1 [GitHub, NVIDIA/OpenShell](#), OpenShell, 02.10.2026. github.com
- 2 [NVIDIA Docs, Why OpenShell](#), 02.10.2026. docs.nvidia.com
- 3 [NVIDIA Newsroom, NVIDIA Open Agent Safety Platform](#), 28.09.2026. nvidianews.nvidia.com

5 MINUTES / 25.09.2026. → 02.10.2026.

Kratko

FIREFOX · 29.09.

Nova menja izgled Firefoxa

Firefox 157 donosi Nova dizajn, najveće osveženje interfejsa od Protona iz 2021. Toolbar i sidebar sada se spajaju sa ivicama prozora, a vertikalni tabovi postaju ravnopravan raspored. Teme sa pozadinskim slikama možda će trebati prilagoditi.

[Mozilla Add-ons Blog](#)

SAMSUNG · 30.09.

SmartTag3 radi i sa iPhoneom

Prvi Samsung tracker sa podrškom za Galaxy i iOS uređaje. Prema Samsungu, manji je 35% po zapremini, Compass View radi do 60 metara, a baterija traje do 550 dana. U SAD stiže početkom novembra po ceni od 29,99 \$.

[Samsung Newsroom](#)

OPENAI · 29.09.

Prijava ChatGPT nalogom

Sign in with ChatGPT omogućava prijavu na druge servise ChatGPT nalogom. Servis dobija ime, email i profilnu sliku, ali ne i razgovore ni memoriju. Dodatni pristup korisnik odobrava posebno.

[OpenAI Help Center](#)

AWS · 30.09.

S3 Tables i Iceberg V3

S3 Tables sada podržavaju sve tipove podataka iz Apache Iceberg V3, uključujući podrazumevane vrednosti kolona, deletion vectors i row lineage, uz automatsku kompakciju.

[AWS News Blog](#)

SAMSUNG · 30.09.

Galaxy Tab S12 Ultra i S12+

Ultra ima ekran od 14,6 inča i debljinu od 5,1 mm, što je čini najtanjim Galaxy Tabom do sada. Oba modela koriste MediaTek Dimensity 9500, a Ultra izdržava do 23 sata reprodukcije videa. Prodaja počinje 7. oktobra.

[Samsung Newsroom](#)

AMD · 30.09.

Ross za embedded developere

AMD Ross je agentic asistent koji kroz prirodni jezik pretražuje dokumentaciju, pokreće alate i pomaže u debugovanju za FPGA, Versal i x86 embedded platforme. Dostupan je odmah, a AMD najavljuje nove alate svakog meseca.

[AMD Newsroom](#)

OPENAI · 25.09.

Istorija bezbednosti naloga

ChatGPT na webu sada prikazuje prijave, odjave i promene MFA podešavanja i passkeyeva, sa vremenom, lokacijom i uređajem. Nalazi se u Settings, pod Security and login.

[OpenAI Help Center](#)

AMD · 01.10.

Versal AI Core za svemir

AMD šalje uzorke Versal AI Core čipa u kućištu za svemirske misije. Kućište će imati Class Y kvalifikaciju, najviši nivo pouzdanosti, i namenjeno je misijama dužim do 15 godina.

[AMD Newsroom](#)

THIS WEEK IN NUMBERS / 25.09.2026. → 02.10.2026.

Nedelja u brojkama

1M

izlaznih tokena za Gemini 4 Argon, umesto dosadašnjih 64 hiljade

GOOGLE · 30.09.

500\$

mesečno košta ChatGPT Pro 500, jedini Pro plan sa Astra Ultrafast režimom

OPENAI HELP CENTER · 29.09.

12_{min}

od prvog uspešnog DNS upita OpenAI agenta do P0 uzbune

OPENAI ALIGNMENT · 25.09.

100+

organizacija koje je OpenAI do 26. septembra obavestio o aktivnosti svojih agenata

OPENAI · 30.09.

9,5

CVSS v4 ocena dva NetScaler zero-daya u aktivnoj eksploataciji

CITRIX · 27.09.

26

Starlink V3 satelita izbačeno na prvom orbitalnom letu Starshipa

SPACEX · 28.09.

150_{mlrd \$}

povećanje NVIDIA programa otkupa akcija; ukupno preostalo 235 milijardi

NVIDIA NEWSROOM · 28.09.

8,2_{mlrd \$}

približna vrednost AMD kupovine World Labsa, isključivo u akcijama

AMD NEWSROOM · 28.09.

800K+

linija Zircon kernela u Googleovoj migraciji iz C/C++ u Rust uz Argon, prema Googleu

GOOGLE · 30.09.

NEXT / 25.09.2026. → 02.10.2026.

Šta pratimo

Zakazani događaji i teme koje se razvijaju. Ništa od ovoga nije predviđanje.

→ 04.10.

Googlebook u prodaji

Prvi Googlebook laptopovi Acera, ASUS-a, Della, HP-a i Lenova mogu da se kupe od 4. oktobra. Cene u SAD počinju od 899 \$, zavisno od proizvođača i konfiguracije.

[Android Authority](#)

→ 07. DO 09.10.

Open Source Summit Europe, Prag

Open Source Summit i Embedded Linux Conference Europe, sa razgovorom sa Linusom Torvaldsom povodom 35 godina Linuxa.

[The Linux Foundation](#)

→ KRAJEM OKTOBRA

Uslovi za dots

Posle prvog meseca, u kome se korišćenje ne računa u kvote, OpenAI treba da objavi uslove korišćenja po planovima.

[OpenAI Help Center](#)

→ U TOKU

FTC i AI laboratorije

Prema Reutersu, FTC vodi istragu na nivou industrije o rizicima koje AI laboratorije, uključujući Anthropic i OpenAI, predstavljaju za potrošače.

[Reuters](#)

→ BEZ DATUMA

Sledeći let Starshipa

Posle prvog orbitalnog leta, pratimo analizu otkaza motora i datum sledeće misije.

[SpaceX](#)

→ 07.10.

Galaxy Tab S12 u prodaji

Početak prodaje Tab S12 Ultra i Tab S12+.

[Samsung Newsroom](#)

→ OKTOBAR

Autopilot i novi Copilot

Autopilot ulazi u private preview, a Home i Code stižu u Frontier program u narednim nedeljama.

[Official Microsoft Blog](#)

→ U TOKU

OpenAI i agenti

Pregled oko 50 petabajta zapisa trajaće mesecima, prema kompaniji. Pratimo nova obaveštenja organizacijama i odgovor na subpoena iz Kalifornije.

[OpenAI](#) · [Reuters](#)

→ BEZ DATUMA

Gemini 4 Argon za sve

Google najavljuje postepeno širenje sa Fairwind programa na plaćeni API i Google AI Ultra.

[Google](#)

→ DO KRAJA 2026.

AMD i World Labs

Zatvaranje transakcije zavisi od regulatornih odobrenja.

[AMD Newsroom](#)

Svi izvori broja

Izvori su grupisani po stranama na kojima se prvi put pojavljuju. Primarni izvori, zvanične objave i dokumentacija, imaju prednost. Sekundarni izvori su korišćeni za kontekst i nezavisnu potvrdu.

05 SIGNAL: ŠTA SE PROMENILO

- 1. **OpenAI Alignment.** An agent used DNS to reach an external chatbot. 25.09.2026.
alignment.openai.com/misalignment-reports/an-agent-used-dns-to-reach-an-external-chatbot/
- 2. **OpenAI Help Center.** ChatGPT Release Notes. 29.09.2026.
help.openai.com/en/articles/6825453-chatgpt-release-notes
- 3. **Official Microsoft Blog.** Introducing the new Copilot with Home, Code and Autopilot. 25.09.2026.
blogs.microsoft.com/blog/2026/09/25/introducing-the-new-copilot-with-home-code-and-autopilot/
- 4. **Google.** Gemini 4 Argon. 30.09.2026.
blog.google/innovation-and-ai/models-and-research/gemini-models/gemini-4-argon/
- 5. **GitHub Changelog.** Dynamic workflows in Copilot CLI and the Copilot app. 01.10.2026.
github.blog/changelog/2026-10-01-dynamic-workflows-in-copilot-cli-and-the-copilot-app/

06 SIGNAL: KONTROLA

- 6. **OpenAI.** The Hugging Face incident and other third-party impacts from misaligned models. 30.09.2026.
openai.com/hugging-face-incident-and-misalignment/
- 7. **OpenAI.** The Hugging Face incident and the road ahead. 26.08.2026.
openai.com/index/hugging-face-incident-and-the-road-ahead/
- 8. **Reuters.** California attorney general issues investigative subpoena to OpenAI. 01.10.2026.
reuters.com/legal/litigation/california-attorney-general-issues-investigative-subpoena-openai-2026-10-01/
- 9. **Reuters (preko Yahoo Tech).** OpenAI alerts more than 100 groups about rogue AI agent activity. 01.10.2026.
tech.yahoo.com/ai/articles/openai-alerts-more-100-groups-222158670.html
- 10. **NVIDIA Newsroom.** NVIDIA Open Agent Safety Platform. 28.09.2026.
nvidianews.nvidia.com/news/open-agent-safety-platform

07 SIGNAL: ŠTA TO ZNAČI

- 11. **Vercel Changelog.** Vercel Agent now installs private packages from npm and custom registries. 30.09.2026.
vercel.com/changelog/vercel-agent-now-installs-private-packages-from-npm-and-custom-registries
- 12. **GitHub Changelog.** Opt-in dist-tag permissions for npm trusted publishing. 30.09.2026.
github.blog/changelog/2026-09-30-opt-in-dist-tag-permissions-for-npm-trusted-publishing
- 13. **GitHub Changelog.** GitHub Copilot can now interact with desktop apps with computer use. 01.10.2026.
github.blog/changelog/2026-10-01-github-copilot-can-now-interact-with-desktop-apps

08 OPENAI DEVDAY

- 14. **OpenAI.** OpenAI DevDay 2026. 29.09.2026.
devday.openai.com/
- 15. **BGR.** Everything OpenAI Announced At DevDay 2026. 29.09.2026.
bgr.com/2272332/openai-devday-2026-announcements/

09 OPENAI DEVDAY: CODEX I PRO 500

- 16. **NVIDIA Blog.** How NVIDIA GPUs Help Accelerate OpenAI's GPT-6 Astra Ultrafast. 01.10.2026.
blogs.nvidia.com/blog/gpus-openai-gpt-6-astra-ultrafast/
- 17. **GitHub Changelog.** GPT-6.1 Sol in GitHub Copilot. 29.09.2026.
github.blog/changelog/2026-09-29-gpt-6-1-sol-in-github-copilot

11 GEMINI 4 ARGON

- 18. **Claude Docs.** Models overview. 02.10.2026.
platform.claude.com/docs/en/about-claude/models/overview

12 AMD KUPUJE WORLD LABS

- 19. **AMD Newsroom.** AMD to Acquire World Labs. 28.09.2026.
newsroom.amd.com/news/amd-acquire-world-labs/
- 20. **NVIDIA Newsroom.** NVIDIA Announces a \$150 Billion Share Repurchase Authorization Increase. 28.09.2026.
nvidianews.nvidia.com/news/nvidia-announces-a-150-billion-share-repurchase-authorization-increase
- 21. **Samsung Newsroom.** Samsung To Invest USD 1 Billion in AI Infrastructure Company Helix. 29.09.2026.
news.samsung.com/global/samsung-to-invest-usd-1-billion-in-ai-infrastructure-company-helix

IZVORI / NASTAVAK

13 MODEL WATCH

22. **Anthropic.** Claude Sonnet 5.5. 28.09.2026.
anthropic.com/claude-sonnet-5-5

23. **GitHub Changelog.** Claude Sonnet 5.5 in GitHub Copilot. 28.09.2026.
github.blog/changelog/2026-09-28-claude-sonnet-5-5-in-github-copilot/

14 BUILD: GITHUB

24. **GitHub Changelog.** New dashboard experience now the default. 01.10.2026.
github.blog/changelog/2026-10-01-new-dashboard-experience-now-the-default

25. **GitHub Changelog.** HydraFusion in VS Code and the GitHub Copilot app. 30.09.2026.
github.blog/changelog/2026-09-30-hydrfusion-in-vs-code-and-the-github-copilot-app

15 BUILD: BAZE, DEPLOY, NPM

26. **AWS News Blog.** Amazon Aurora PostgreSQL now supports direct querying of Apache Iceberg and Parquet data in your data lake. 30.09.2026.
aws.amazon.com/blogs/aws/amazon-aurora-postgresql-now-supports-direct-querying-of-apache-iceberg-and-parquet-data-in-your-data-lake/

16 PATCH NOW

27. **Citrix.** NetScaler ADC and NetScaler Gateway Security Bulletin CTX697096. 27.09.2026.
support.citrix.com/external/article?articleNumber=CTX697096

28. **CISA.** Known Exploited Vulnerabilities Catalog. 27.09.2026.
cisa.gov/known-exploited-vulnerabilities-catalog

29. **Microsoft MSRC.** CVE-2026-65660. 25.09.2026.
msrc.microsoft.com/update-guide/vulnerability/CVE-2026-65660

30. **Security Affairs.** CISA adds Microsoft SharePoint and Mikrotik RouterOS flaws to its KEV catalog. 25.09.2026.
securityaffairs.com/199777/

31. **CERT Polska.** Vulnerabilities in MikroTik RouterOS. 05.09.2026.
cert.pl/en/posts/2026/09/mikrotik-routeros-cve/

32. **Mozilla.** Security Vulnerabilities fixed in Firefox 157 (MFSA 2026-97). 29.09.2026.
mozilla.org/en-US/security/advisories/mfsa2026-97/

18 ORBIT: STARSHIP

33. **SpaceX.** Starship Flight 14. 28.09.2026.
spacex.com/launches/starship-flight-14

19 ORBIT: SUNCATCHER I CREW-13

34. **NASA.** Dragon Docks Bringing SpaceX Crew-13 to Station. 01.10.2026.
nasa.gov/blogs/spacestation/2026/10/01/dragon-docks-bringing-spacex-crew-13-to-station/

35. **Google.** Project Suncatcher prototype. 01.10.2026.
blog.google/innovation-and-ai/models-and-research/google-research/project-suncatcher-prototype/

36. **NASA.** Liftoff! NASA's SpaceX Crew-13 Begins Journey to International Space Station. 01.10.2026.
nasa.gov/blogs/spacestation/2026/10/01/liftoff-nasas-spacex-crew-13-begins-journey-to-international-space-station/

20 LAB: ŠTA ROBOTI MOGU

37. **Anthropic.** What work can robots do?. 30.09.2026.
anthropic.com/research/what-work-can-robots-do

21 SHIPPED

38. **Mozilla Add-ons Blog.** Nova is here: what changes for your Firefox theme. 29.09.2026.
blog.mozilla.org/addons/2026/09/29/nova-is-here-what-changes-for-your-firefox-theme/

39. **GitHub, NVIDIA/OpenShell.** OpenShell. 02.10.2026.
github.com/NVIDIA/OpenShell

40. **AMD Newsroom.** AMD Brings the Power of Agentic AI to Embedded Design and Development Cycle. 30.09.2026.
newsroom.amd.com/news/amd-ross-agentic-ai-embedded-design-development/

22 USE THIS: NVIDIA OPENSHELL

41. **NVIDIA Docs.** Why OpenShell. 02.10.2026.
docs.nvidia.com/openshell/about/why-open-shell

23 5 MINUTES

42. **Samsung Newsroom.** Samsung Introduces Galaxy Tab S12 Series. 30.09.2026.
news.samsung.com/uk/samsung-introduces-galaxy-tab-s12-series-the-ultimate-productivity-powerhouse-built-for-growth

43. **Samsung Newsroom.** Samsung Galaxy SmartTag3 Makes It Easier to Keep Track of What Matters. 30.09.2026.
news.samsung.com/us/samsung-galaxy-smarttag3-makes-easier-keep-track-matters/

44. **AWS News Blog.** Amazon S3 Tables now support all Apache Iceberg V3 data types. 30.09.2026.
aws.amazon.com/blogs/aws/amazon-s3-tables-now-support-all-apache-iceberg-v3-data-types/

45. **AMD Newsroom.** AMD Sampling Versal AI Core Adaptive SoC in Enhanced Space-Grade Package. 01.10.2026.
newsroom.amd.com/news/amd-sampling-versal-ai-core-adaptive-soc/

25 NEXT: ŠTA PRATIMO

46. **Android Authority.** Googlebook availability and release. 2026.
androidauthority.com/googlebook-availability-release-freebies-3713298

47. **The Linux Foundation.** Open Source Summit + Embedded Linux Conference Europe 2026 Schedule. 05.08.2026.
linuxfoundation.org/press/open-source-summit-embedded-linux-conference-europe-2026-schedule-champions-open-source-innovation-and-marks-35-years-of-linux

o0o0o0o0

/ 001

Nedeljni pregled tehnologije. Izlazi
petkom, besplatno, na tutorijali.app.

Izdanje 001

Datum 02.10.2026.

Period 25.09.2026. 08:00 → 02.10.2026. 08:00

Web tutorijali.app



tutorijali.app