

Private AI: Building Trust Through Verifiable Computation

Mingshen Sun, Mateus Guzzo

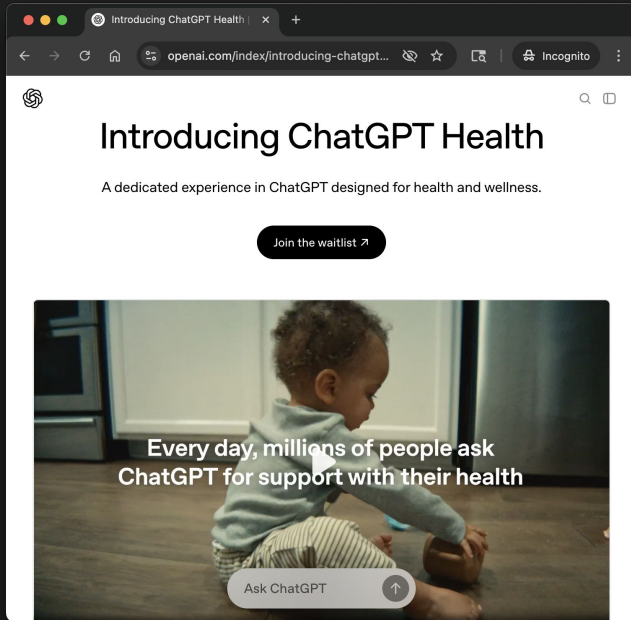
TikTok

PEPR 2026

Data and compute power demands in the AI era

AI has transformed how people learn, work and live.

The most powerful AI today runs on server-class hardware.



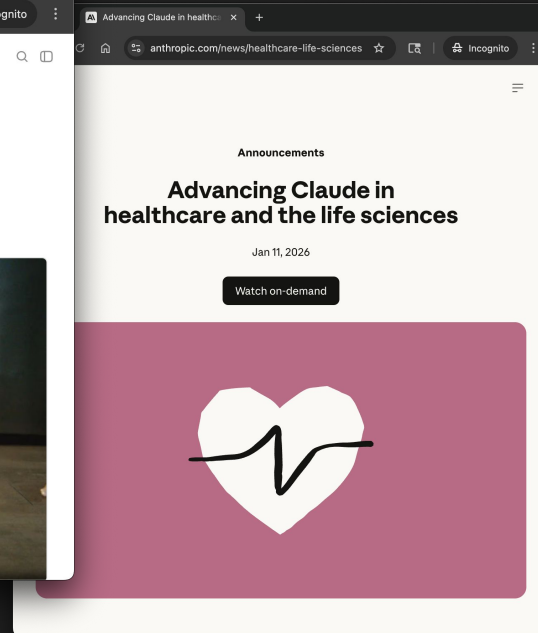
Introducing ChatGPT Health

A dedicated experience in ChatGPT designed for health and wellness.

Join the waitlist →

Every day, millions of people ask ChatGPT for support with their health

Ask ChatGPT ↑

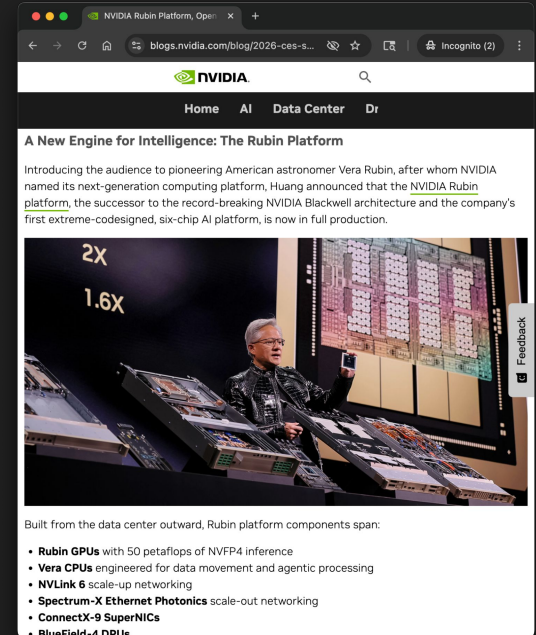
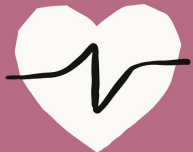


Announcements

Advancing Claude in healthcare and the life sciences

Jan 11, 2026

Watch on-demand

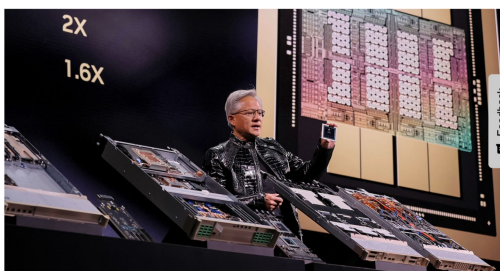


NVIDIA

Home AI Data Center Dr

A New Engine for Intelligence: The Rubin Platform

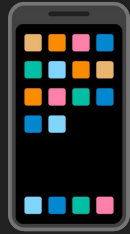
Introducing the audience to pioneering American astronomer Vera Rubin, after whom NVIDIA named its next-generation computing platform, Huang announced that the **NVIDIA Rubín platform**, the successor to the record-breaking NVIDIA Blackwell architecture and the company's first extreme-codedesigned, six-chip AI platform, is now in full production.



Built from the data center outward, Rubín platform components span:

- **Rubin GPUs** with 50 petaflops of NVFP4 inference
- **Vera CPUs** engineered for data movement and agentic processing
- **NVLink 6** scale-up networking
- **Spectrum-X Ethernet Photonics** scale-out networking
- **ConnectX-9 SuperNICs**
- **BlueField-4 DPUs**

Sensitive user prompts and context sent to the service provider to be processed



prompt/context



Server

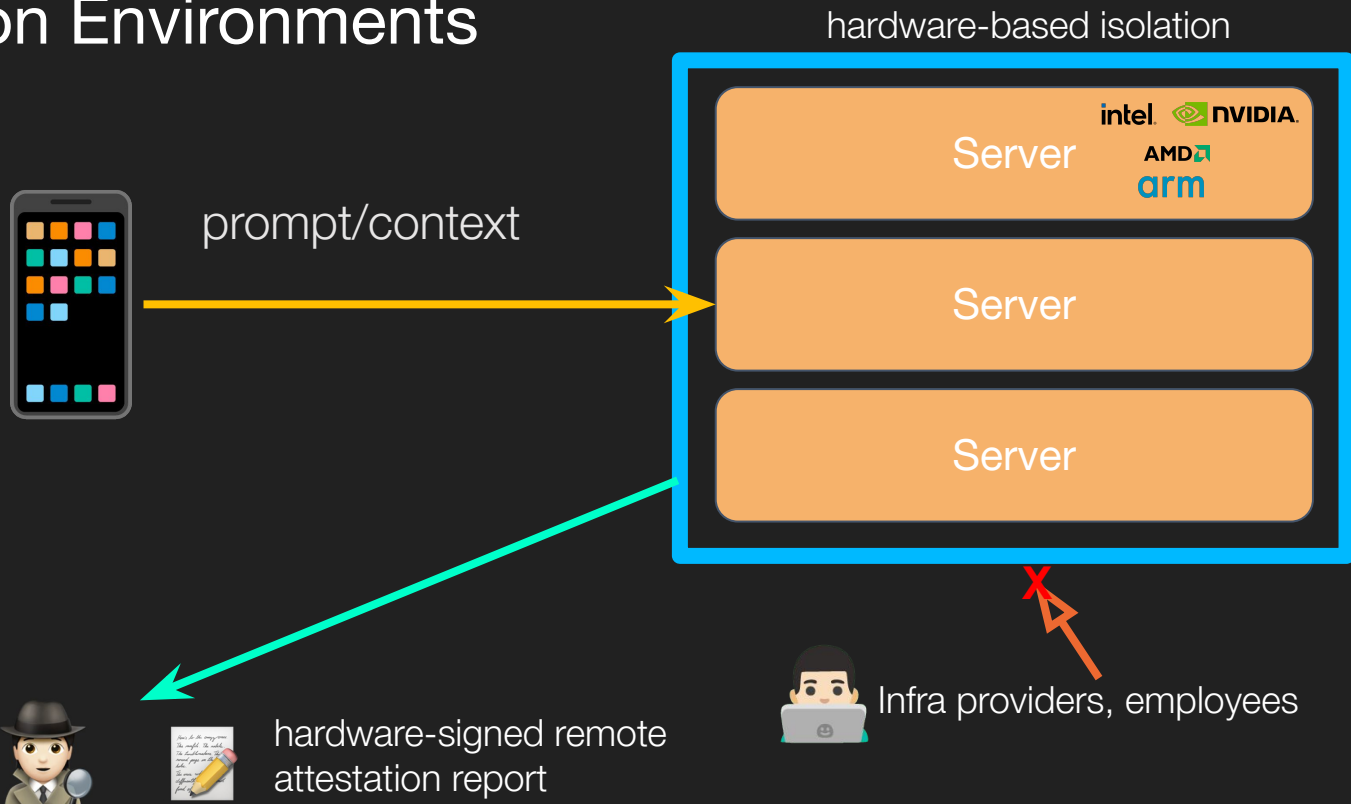
Server

Server

Can service provider see and (mis)-use my prompts and context?

Proof and remote attestation of privacy and security?

Sensitive user prompts and context protected by Trusted Execution Environments



High-level goals of Private Verifiable Compute

Use powerful cloud AI on sensitive data, while making sure no one — not even the platform provider — can see who you are or what you sent. And let you verify that for yourself.

- **Private** — your data is protected the whole way through.
- **Anonymous** — your identity is separated from your request.
- **Verifiable** — you don't have to take our word for it; you can check.

Design goals and privacy & security guarantees

Private processing

Data Security

Privacy preserving

Enforcement guarantees

No privileged access

Private storage

*User-controlled
encryption key*

Verifiable transparency

*Code transparency and
assurance*

Verifiable privacy

Remote attestation

Value proposition for users and business

Build user trust

PVC leverages multiple innovations of Privacy Enhancing Technologies. With the nature of privacy, transparency and verifiability, it showcases the technical advancements of PET in private AI processing.

Mitigate risk

Due to the design of private processing and storage, sensitive data is not visible even to the service provider during processing, and additionally, this can be remotely attested by reviewers independently.

Unblock business innovation

New business scenarios with AI features relying on sensitive user data might face privacy and compliance challenges. Privacy and security guarantees ensured by PVC could potentially unblock valuable business innovations.

What does the remote attestation report look like?

```
MR_TD: ab62561a173acbd18ee50ff37750db44
184c6cf5e886df74247cc575e163b04
c34b9e18374757c235affa614d4127f6
b
RTMRO: d4001543d209c21538e3ef34023caa8
283cdb7ac1489188e667ceb7f694c3f4
db2bc1100baacec1e58c73cc4dae882
d3
RTMR1: 557aa1246f530ea30cedcb846bfae5a
be31d6adc75ed154f5a500ec805964a
45a5e00fafc18bcb7207bf8940c5a7e
e4
RTMR2: 4b287584188785e43a681f1232bd142
64c5cadac94a6ce3a5fb62c4775b046
84c82c6bb88ea2e1c35ef9d28cec170
035
RTMR3: 00000000000000000000000000000000
00000000000000000000000000000000
00000000000000000000000000000000
0000000000
TCB SVN: 0f010a00000000000000000000000000
00
CPU Hardware Model: GH100
<-nvidia-gpu-attestation-report-cert-
chain-fwid-match: true
<-nvidia-gpu-attestation-report-nonc
e-match: true
<-nvidia-gpu-attestation-report-cert-
chain: valid
```

The screenshot shows a browser's developer console with a network request for an attestation report. The 'Preview' tab is selected, displaying a JSON response. The response includes fields for 'cpu', 'gpu', 'eat_nonce', 'exp', 'hwmodel', 'iat', 'iss', 'jti', 'measres', 'nbf', 'oemid', 'uid', and 'x-nvidia-gpu-attestation-report-cert-chain'. The 'measres' field is 'fail'. The 'x-nvidia-gpu-attestation-report-cert-chain' field is a long string of hexadecimal characters. The console also shows 5 requests and 313 kB transferred. The bottom of the console shows the 'chrome' console with the message 'IS_SAFARI false' and a command prompt.

```
Name: 34.162.49.83
index-CzuGCdGI.js
index-DFgTojPB.css
config
attestation

{code: 0, message: "", data: {,...}}
code: 0
data: {,...}
  cpu: {advisory_ids: [], collateral_expiration_status: "0", earliest_expiration_date: "2026-06-21T09:15:06Z", ...}
  gpu: {eat_nonce: "53cc40cf98637d4355e4b6ad0087e8fe172d0036cc5afd810ad6c9f73f67f21e", exp: 1779449176, ...}
    eat_nonce: "53cc40cf98637d4355e4b6ad0087e8fe172d0036cc5afd810ad6c9f73f67f21e"
    exp: 1779449176
    hwmodel: "GH100"
    iat: 1779445576
    iss: "https://nras.attestation.nvidia.com"
    jti: "8fb346f7-be38-41ef-be9d-00f17a790ac4"
    measres: "fail"
    nbf: 1779445576
    oemid: "5703"
    uid: "376957556650987879278617257573695684763069260071"
    x-nvidia-attestation-warning: null
    x-nvidia-gpu-arch-check: true
  x-nvidia-gpu-attestation-report-cert-chain: {x-nvidia-cert-expiration-date: "9999-12-31T23:59:59Z", x-nvidia-cert-
x-nvidia-gpu-attestation-report-cert-chain-fwid-match: true
x-nvidia-gpu-attestation-report-nonce-match: true
x-nvidia-gpu-attestation-report-parsed: true
x-nvidia-gpu-attestation-report-raw: "53cc40cf98637d4355e4b6ad0087e8fe172d0036cc5afd810ad6c9f73f67f21e"

5 requests | 313 kB transferred

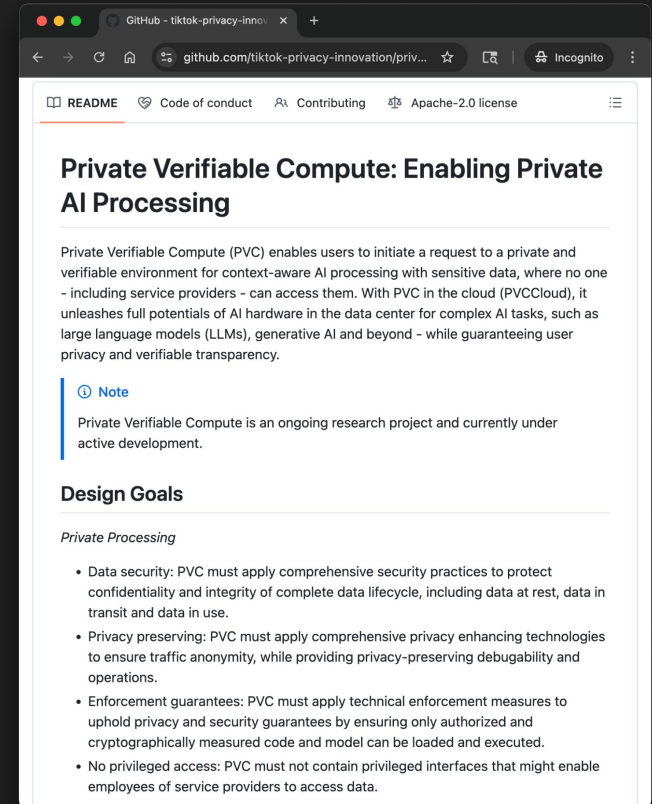
Console Issues
chrome
IS_SAFARI false
  {cpu: {...}, gpu: {...}}
  [cmd] to turn on code suggestions. Don't show again
```

Open source for transparency and verifiability

Private Verifiable Compute is an open source project, published in Dec 2025.

- Cloud, on-premise, and hybrid deployment
- Open & transparent code release

<https://github.com/tiktok-privacy-innovation/private-verifiable-compute>



The screenshot shows a web browser displaying the GitHub repository page for "Private Verifiable Compute: Enabling Private AI Processing". The page includes a navigation bar with links for "README", "Code of conduct", "Contributing", and "Apache-2.0 license". The main content area features the repository title, a brief description of the project, a "Note" section, and a "Design Goals" section. The "Design Goals" section lists four key principles: Data security, Privacy preserving, Enforcement guarantees, and No privileged access.

Private Verifiable Compute: Enabling Private AI Processing

Private Verifiable Compute (PVC) enables users to initiate a request to a private and verifiable environment for context-aware AI processing with sensitive data, where no one - including service providers - can access them. With PVC in the cloud (PVCCloud), it unleashes full potentials of AI hardware in the data center for complex AI tasks, such as large language models (LLMs), generative AI and beyond - while guaranteeing user privacy and verifiable transparency.

Note

Private Verifiable Compute is an ongoing research project and currently under active development.

Design Goals

Private Processing

- **Data security:** PVC must apply comprehensive security practices to protect confidentiality and integrity of complete data lifecycle, including data at rest, data in transit and data in use.
- **Privacy preserving:** PVC must apply comprehensive privacy enhancing technologies to ensure traffic anonymity, while providing privacy-preserving debugability and operations.
- **Enforcement guarantees:** PVC must apply technical enforcement measures to uphold privacy and security guarantees by ensuring only authorized and cryptographically measured code and model can be loaded and executed.
- **No privileged access:** PVC must not contain privileged interfaces that might enable employees of service providers to access data.

Thanks!