



How Ubuntu enables verifiably private AI with confidential computing on bare metal

Tinfoil success story

EXECUTIVE SUMMARY

AI can no longer rely on trust. Enterprises need proof, not promises, that their most sensitive data remains private, even from the platform provider. They need verifiably private AI, where all data is encrypted end-to-end and executed exclusively inside hardware trusted execution environments (TEEs).

Tinfoil is a US-based cybersecurity company focused on verifiably private AI. Its platform ensures that sensitive data, including financial records, health information, legal documents, and proprietary models, remains encrypted at every stage of processing. Unlike traditional AI services, Tinfoil itself cannot access the data it handles. Every workload executes inside hardware TEEs, enabling enterprises to benefit from advanced AI capabilities without transferring trust to the AI operator, the cloud provider, or any third-party infrastructure.

AI tools now process unprecedented amounts of sensitive data, demanding complete trust across many third parties. To unlock AI's full potential, individuals and enterprises must have proof, not just promises, that their data stays under their control.

Enter confidential-computing hardware. Just as secure chips in phones safeguard biometric data, trusted execution

environments (TEEs) in the cloud can protect your data from any unwanted access. AMD, Intel, and NVIDIA have all recently integrated these capabilities into their modern processors and accelerators.

These hardware technologies are full of potential, but require domain expertise to integrate in applications. Tinfoil pioneers verifiably private AI by wrapping all sensitive data processing in a layer of hardware security, guaranteeing that even system administrators cannot access the sensitive data. For all these guarantees to be verifiable, Tinfoil is fully open source and proves supply-chain transparency before any data is sent.

To achieve this across heterogeneous hardware infrastructure, without custom kernels or cloud lock-in, Tinfoil needed a fully open, audit-ready operating system with native confidential-computing support.

Only Ubuntu provided that foundation. With official AMD SEV-SNP and Intel TDX enablement, reproducible-build tooling, and a proven security pedigree, Ubuntu enabled Tinfoil to build a single, attested image that runs securely on any platform, accelerating deployment, audit readiness, and customer trust.

AI'S NEW PRIVACY FRONTIER

Modern AI systems demand unprecedented access to personal and enterprise data, calendars, communications, internal documents, and strategic IP. At the same time, AI pipelines now span multiple third-party services, introducing greater risk of exposure, commercial misuse, or unintended leakage.

Confidential computing provides a hardware-based path forward. But most implementations only protect against cloud providers. Tinfoil brings these guarantees to the application level by protecting data from everyone, including from itself, and the privileged administrators of the AI platform.

THE CHALLENGE: BEYOND CONVENTIONAL CONFIDENTIAL VMS

Traditional confidential computing assumes a trusted operator. Cloud offerings focus on protecting workloads from the infrastructure provider, but still rely on proprietary hypervisors, firmware, and opaque attestation services. This creates circular trust in the infrastructure provider, and always expects the service operators to be trusted.

To remove blind trust in the application layer and in Tinfoil itself, Tinfoil needed to go further:

- Enforce cryptographically verifiable code and supply chain transparency.
- Deliver an audit-ready codebase where every component touching sensitive data is open source
- Produce a single, attested image deployable across AMD SEV-SNP, Intel TDX, and NVIDIA GPUs

Existing platforms could not meet these demands. Custom kernels prevented auditability. Proprietary attestation broke verifiability. The conclusion was clear: only a bare-metal, audit-ready, fully open-source software stack could support verifiable privacy at scale.

WHY UBUNTU: A FULLY OPEN, HARDWARE-NEUTRAL FOUNDATION

Tinfoil evaluated multiple Linux distributions and cloud solutions. Ubuntu emerged as the only platform capable of meeting both the engineering and security standards required to build verifiable AI. Ubuntu delivered three critical advantages:

Native, upstream confidential computing support

Ubuntu 25.04, Plucky Puffin, was the first production OS to ship official support for both AMD SEV-SNP and Intel TDX, without patched kernels or experimental branches, as well as support for NVIDIA confidential computing mode on GPUs, critical for private AI without performance overheads.

Audit-ready build infrastructure

Ubuntu's compatibility with mkosi, reproducible snapshots, and automated CI enabled Tinfoil to fully automate its build pipeline, measure each image, and publish those measurements to the Sigstore transparency logs. Every artifact is independently verified client-side before sending any sensitive data for private processing.

Security legacy & community scrutiny

Ubuntu's security reputation and deep open-source ecosystem aligned with Tinfoil's "open security" principle, replacing trust with auditability.



"Ubuntu provides the strongest foundation for building trustworthy, multi-platform confidential-computing workloads, allowing Tinfoil to build a verifiably private AI platform with minimal custom code, ensuring maximum auditability."

Tanya Verma
Co-Founder, Tinfoil

IMPLEMENTATION: BUILDING VERIFIABLE PRIVACY WITH UBUNTU

Tinfoil's architecture relies on a strict, fully automated, verifiable build pipeline. Every image is constructed in CI, cryptographically measured, and published publicly for users to verify. There are no manual changes, no mutable infrastructure, and no reliance on proprietary attestation services.

Ubuntu integrated directly into this model. With native AMD SEV-SNP and Intel TDX support, Tinfoil was able to produce a single image deployable across both AMD and Intel hardware. Ubuntu's snapshot service allowed precise pinning of dependencies, ensuring identical builds weeks later, essential for deriving offline measurements and guaranteeing immutability.

Rather than maintaining multiple OS forks or patched kernels, Tinfoil kept the Ubuntu base untouched. Their custom logic was reduced to a minimal, auditable layer on top of a widely scrutinized operating system. This aligned infrastructure with their core promise to users: "You don't need to trust us, verify everything yourself."

**OUTCOMES:
AUDITABILITY, PORTABILITY, AND ACCELERATION**

Standardizing on Ubuntu significantly reduced deployment complexity. Starting from an image supporting AMD SEV-SNP, enabling Intel TDX support took days, not months, because the host OS was already feature-complete. Engineering effort could focus on attestation libraries and customer onboarding, not kernel maintenance.

For customers, Tinfoil gained the ability to support heterogeneous infrastructure with a single security posture. Whether deployed on-prem or in private clouds, enterprises in finance, healthcare, and law could adopt verifiable AI without infrastructure redesign.

Operationally, Ubuntu's packaging, support lifecycle, and ecosystem maturity reduced maintenance overhead, allowing a lean team to manage a high-assurance confidential computing stack.



"Ubuntu is the only distribution where we could move from prototype to production immediately. Ubuntu lets us use a shared OS between the host and guest, and also build once and deploy on all our platforms without worrying about changing repos or missing packages."

Jules Drean
Co-Founder, Tinfoil

**LOOKING AHEAD:
UBUNTU PRO IN REGULATED INDUSTRIES**

Tinfoil plans to extend its security posture using Ubuntu Pro, gaining access to:

- Managed, long-term security updates
- Compliance-grade images for regulated environments, including finance and defense

CONCLUSION

By building on Ubuntu, Tinfoil created more than a platform, it created verifiable trust. Privacy in AI no longer depends on promises, it is proven in code and enforced in hardware. Ubuntu remains the strongest foundation for confidential computing at scale, enabling a new generation of AI platforms where operators are optional, and verifiable privacy is the default.

FURTHER READING

- [Confidential Computing on Ubuntu](#)
- [Download Ubuntu's defense in depth whitepaper](#)
- [Tinfoil website](#)



© 2026 Canonical Limited. Ubuntu, Kubuntu, Canonical and their associated logos are the registered trademarks of Canonical Ltd. All other trademarks are the properties of their respective owners. Any information referred to in this document may change without notice and Canonical will not be held responsible for any such changes.