



NEWS RELEASE

Corvex Launches Secure Model Weights, Delivering Hardware-Enforced Protection for AI Inference on Third-Party Infrastructure

2026-03-12

Patent-pending solution gives AI model builders and security-conscious enterprises cryptographic, owner-controlled key custody, protecting model weights from even the infrastructure provider

ARLINGTON, Va., March 12, 2026 /PRNewswire/ -- Corvex, Inc., an engineering-led AI infrastructure platform, today announced the early availability of Corvex Secure Model Weights, a patent-pending solution that enables AI model builders and enterprises to deploy inference workloads on third-party GPU infrastructure without exposing their model weights, which can be their most valuable intellectual property.

The Problem with the Current Trust Model

Frontier AI models often represent years of research and hundreds of millions of dollars in compute investment. The risk extends well beyond frontier labs. Any organization fine-tuning models on proprietary data – patient records, financial datasets, defense workloads, trade secrets – is embedding sensitive IP directly into model weights. Traditional cloud security models focus on data at rest and in transit, which leaves data at runtime exposed, creating a critical vulnerability.

Corvex Secure Model Weights addresses this risk. In standard virtualized environments, model weights are decrypted in CPUs and transferred as plaintext into VRAM, leaving them exposed to hypervisor-level introspection or DMA-based attacks by the host. Our architecture closes this gap by leveraging Hardware-based Trusted Execution Environments (TEEs). By utilizing NVIDIA's Confidential Computing instructions, Corvex ensures that model weights remain cryptographically isolated and are only decrypted within the GPU's secure silicon boundary, which renders them invisible even to the infrastructure provider.

"Deploying AI should never require a trade-off between compute power and IP sovereignty," said **Seth Demsey**, co-founder and co-CEO of Corvex. "The industry has long tolerated a 'cleartext gap' where weights are exposed during inference, leaving the host with a structural window into your trade secrets. We are closing that window. By enforcing end-to-end encryption that terminates only inside

the GPU's trusted execution environment, we ensure that the host is never in possession of the keys to the kingdom. Protection is no longer a policy choice; it's a certainty."

Three Layers of Hardware-Rooted Security

Corvex Secure Model Weights combines three integrated technologies to enforce protection at the silicon level:

Trusted Execution Environments. NVIDIA Hopper and Blackwell GPUs running in Confidential Computing mode provide hardware-encrypted GPU memory that the host cannot access at runtime. Intel Trust Domain Extensions (Intel TDX) provide CPU-level isolation on each node.

Remote Attestation. Before any decryption key is released, the model builder cryptographically verifies that the host hardware and software stack match expected configurations. A compromised or misconfigured host fails attestation and never receives keys.

Post-Quantum Key Exchange. Corvex uses ML-KEM (Kyber-768), a post-quantum key encapsulation mechanism, to protect the key handoff between the model builder's infrastructure and the trusted execution environment. The keys for the handoff are ephemeral, and the private key never exists outside the GPU's protected VRAM. Model weights that take years to develop and may remain valuable for decades are protected against future cryptographic threats.

The result: model weights exist in cleartext only inside hardware-protected GPU memory during active inference. They are never present in system RAM and never accessible to the host kernel or hypervisor.

Open Source Foundation, Auditable by Design

Unlike closed-source commercial alternatives, Corvex Secure Model Weights is built on and contributes to the open source community. The solution uses the Confidential Containers (CoCo) project under the Cloud Native Computing Foundation as its orchestration layer, providing vendor-neutral, community-audited security that customers can independently verify.

"Model builders and security-conscious enterprises are now able to choose infrastructure partners based on verifiable security, not just price and availability," said **Jay Crystal**, Co-CEO and Co-Founder of Corvex. "An open source foundation and owner-controlled key custody are what make that security auditable and trustworthy. We built Secure Model Weights so that the model builder never has to take our word for it. The math and the hardware speak for themselves."

Who It Serves

Frontier AI model builders can now deploy at production scale on third-party infrastructure without operator trust assumptions, eliminating the risk of model weight exfiltration while maintaining sovereign key control.

Regulated enterprises, federal customers, and model builders who focus on these customer segments – including those working with healthcare data, financial datasets, defense workloads, and trade-secret-embedded fine-tuned models – can deploy on external infrastructure that previously often required on-premises isolation. Secure Model Weights provides the hardware-enforced, cryptographically verifiable protection required for these sensitive datasets.

Availability

Corvex Secure Model Weights enters early availability on March 12, 2026. To learn more or request early access, visit www.corvex.ai/confidential-computing.

About Corvex

Corvex is an engineering-led AI infrastructure platform specializing in GPU-accelerated infrastructure for AI workloads and purpose-built for secure, high-performance compute. The company designs environments where security and speed are embedded at the core of the product, not layered on top. Corvex engineers provide end-to-end infrastructure architecture, diagnosing misconfigurations, hardening systems against threat exposure, and optimizing GPU utilization at scale. For more information, visit corvex.ai.

As previously announced, on November 10, 2025, Corvex announced a definitive agreement with Movano Inc. (Nasdaq: MOVE) ("Movano") to combine the companies in an all-stock transaction (the "Merger").

Cautionary Statements Regarding Forward-Looking Statements

This press release contains forward-looking statements. All statements contained in this press release other than statements of historical facts, including statements regarding our future results of operations and financial position, projected growth, product capabilities and customer deployment, business strategy and plans and our objectives for future operations, are forward-looking statements. The words "anticipate," "believe," "continue," "could," "estimate," "expect," "intend," "may," "plan," "potential," "predict," "project," "should," "target," "would," and similar expressions are intended to identify forward-looking statements. We have based these forward-looking statements largely on our current expectations and projections about future events and financial trends that we believe may affect our business, financial condition and results of operations. These forward-looking statements are subject to a number of risks, uncertainties and assumptions that may cause actual results to differ materially from those contained in any forward-looking statements we may make. Nothing in this press release should be regarded as a representation by any person that these results will be achieved, and we undertake no duty to update or revise any forward-looking statements, whether as a result of new information, future events or otherwise.

Media Contact

Chris Donahoe, Stillpoint
corvex.media@stillpointglobaladvisors.com

No Offer or Solicitation

This press release and the information contained herein is not intended to and does not constitute a solicitation of a proxy, consent or approval with respect to any securities or in respect of the proposed transactions, including the Merger, between Movano and Corvex (the "Proposed Transactions") or an offer to sell or the solicitation of an offer to subscribe for or buy or an invitation to purchase or subscribe for any securities pursuant to the Proposed Transactions or otherwise, nor shall there be any sale, issuance or transfer of securities in any jurisdiction in contravention of applicable law. No offering of securities shall be made except by means of a prospectus meeting the requirements of Section 10 of the Securities Act, and otherwise in accordance with applicable law, or an exemption therefrom. Subject to certain exceptions to be approved by the relevant regulators or certain facts to be ascertained, the public offer will not be made directly or indirectly, in or into any jurisdiction where to do so would constitute a violation of the laws of such jurisdiction, or by use of the mails or by any means or instrumentality (including without limitation, facsimile transmission, telephone and the internet) of interstate or foreign commerce, or any facility of a national securities exchange, of any such jurisdiction.

Additional Information and Where to Find It

This press release relates to the Proposed Transactions involving Movano and Corvex and may be deemed to be solicitation material in respect of the Proposed Transactions. In connection with the Proposed Transactions, Movano and Corvex have filed relevant materials with the SEC, including a registration statement on Form S-4 (File No. 333-292321) (the "Form S-4") that contains a proxy statement (the "Proxy Statement") and prospectus. This press release is not a substitute for the Form S-4, the Proxy Statement or for any other document that Movano has filed or may file with the SEC and/or send to Movano's stockholders in connection with the Proposed Transactions. MOVANO URGES, BEFORE MAKING ANYVOTING DECISION, INVESTORS AND STOCKHOLDERS TO READ THE FORM S-4, THE PROXY STATEMENT AND ANY OTHER RELEVANT DOCUMENTS THAT MAY BE FILED WITH THE SEC, ASWELL AS ANY AMENDMENTS OR SUPPLEMENTS TO THESE DOCUMENTS, CAREFULLY AND IN THEIR ENTIRETY IF AND WHEN THEY BECOME AVAILABLE BECAUSE THEY WILL CONTAINIMPORTANT INFORMATION ABOUT MOVANO, CORVEX, THE PROPOSED TRANSACTIONS ANDRELATED MATTERS.

Investors and stockholders will be able to obtain free copies of the Form S-4, the Proxy Statement and other documents filed by Movano with the SEC (when they become available) through the website maintained by the SEC at www.sec.gov. Movano's Internet website address is www.movanohealth.com. Movano's Annual Report on Form 10-K, Quarterly Reports on Form 10-Q, Current Reports on Form 8-K, including exhibits, and amendments to those reports filed or furnished pursuant to Section 13(a) or 15(d) of the Exchange Act are available free of charge through the investor relations page of its Internet website as soon as reasonably practicable after it electronically files such material with, or furnish it to, the SEC. Movano's Internet website and the information contained therein or connected thereto are not intended to be incorporated into this report.

Participants in the Solicitation

Movano, Corvex, and their respective directors and certain of their executive officers and other members of management may be deemed to be participants in the solicitation of proxies from Movano's stockholders in connection with the Proposed Transactions under the rules of the SEC. Information about Movano's directors and executive officers, including a description of their interests in Movano, is included in Movano's most recent Annual Report on Form 10-K for the year ended December 31, 2024. Additional information regarding the persons who may be deemed participants in the proxy solicitations, including the directors and executive officers of Corvex, and a description of their direct and indirect interests, by security holdings or otherwise, are also included in the Form S-4, the Proxy Statement and other relevant materials to be filed with the SEC when they become available. These documents can be obtained free of charge from the sources indicated above.

View original content to download multimedia:<https://www.prnewswire.com/news-releases/corvex-launches-secure-model-weights-delivering-hardware-enforced-protection-for-ai-inference-on-third-party-infrastructure-302712911.html>

SOURCE Corvex