



PRNewswire (2026-03-20)

Zilliz Cloud Launches Customer-Managed Encryption Keys for Enterprise Data Sovereignty

New CMEK capability gives regulated enterprises full control over encryption keys for AI-scale vector workloads

REDWOOD CITY, Calif., March 20, 2026 /PRNewswire/ -- **Zilliz**, the company behind **Milvus**, the world's most widely adopted **open-source vector database**, today announced the general availability of Customer-Managed Encryption Keys (CMEK) on **Zilliz Cloud**. The new capability allows enterprises to retain full ownership of their encryption keys, delivering true data sovereignty for AI workloads in regulated industries.

As enterprises embed AI into mission-critical workflows, the sensitivity of the underlying data—customer records, medical images, financial transactions—demands security controls that go beyond standard encryption at rest. Regulatory frameworks such as GDPR, HIPAA, PCI-DSS, and SOC 2 increasingly require organizations to demonstrate exclusive control over their encryption keys, not just the data they protect. For [vector database](#) deployments—where embeddings are derived from highly sensitive assets—this requirement is especially acute.

"Security teams in regulated industries don't just want encryption—they want proof that no one else, including their database vendor, can access their data. CMEK gives enterprises the strongest form of data sovereignty available in a managed service, removing one of the last barriers to deploying AI at scale in healthcare, financial services, and government," said Charles Xie, Founder and CEO at Zilliz.

Why CMEK Matters for Enterprise AI

CMEK on Zilliz Cloud separates key ownership from data processing, ensuring that Zilliz never possesses or accesses customer encryption keys.



Key benefits include:

- **True Segregation of Duties:** Zilliz processes data while the customer retains exclusive control over encryption keys, creating the clean separation auditors and compliance teams require.
- **Instant Revocability:** Disabling a key in AWS KMS immediately renders all associated cluster data cryptographically inaccessible—no vendor coordination needed.
- **Unified Audit Trails:** Every key access event is logged in AWS CloudTrail, integrating directly with existing enterprise security monitoring infrastructure.

Setup takes minutes through the **Zilliz Cloud console**, with auto-generated IAM policies and support for zero-downtime key rotation.

Now Available

CMEK is generally available today for Dedicated clusters on the Zilliz Cloud Business-Critical plan, starting with AWS. To get started, visit the **Zilliz Cloud console** or **connect with the Zilliz team** to discuss your deployment requirements.

About Zilliz

Zilliz is the company behind **Milvus**, the world's most widely adopted **open-source vector database**. **Zilliz Cloud** brings that performance to production with a fully managed, cloud-native platform built for scalable, low-latency vector search and hybrid retrieval. It supports billion-scale workloads with sub-10ms latency, auto-scaling, and optimized indexes for GenAI use cases like semantic search and RAG.

Zilliz is built to make AI not just possible — but practical. With a focus on performance and cost-efficiency, it helps engineering teams move from prototype to production without overprovisioning or complex infrastructure. Over 10,000 organizations worldwide rely on Zilliz to build intelligent applications at scale.



Headquartered in Redwood Shores, California, Zilliz is backed by leading investors, including Aramco's Prosperity 7 Ventures, Temasek's Pavilion Capital, Hillhouse Capital, 5Y Capital, Yunqi Partners, Trustbridge Partners, and others. Learn more at [Zilliz.com](https://www.zilliz.com).

SOURCE Zilliz