



Enterprise AI's Missing Piece

End-to-End Encrypted Vector Databases

Nicolas Dupont, CEO



What's Holding Up AI Deployments?



The Missing Piece for Secure AI



Securing the Vector DB Gap



Deploying the Fix to Production



AI Everywhere... Except in **Production**

What stops AI pilots from
evolving to deployment?
Security.

95%

of generative AI pilots are failing; security is a primary factor (MIT, 2025)

76%

of enterprises in regulated sectors cite privacy as their top AI barrier (SAS, 2024)



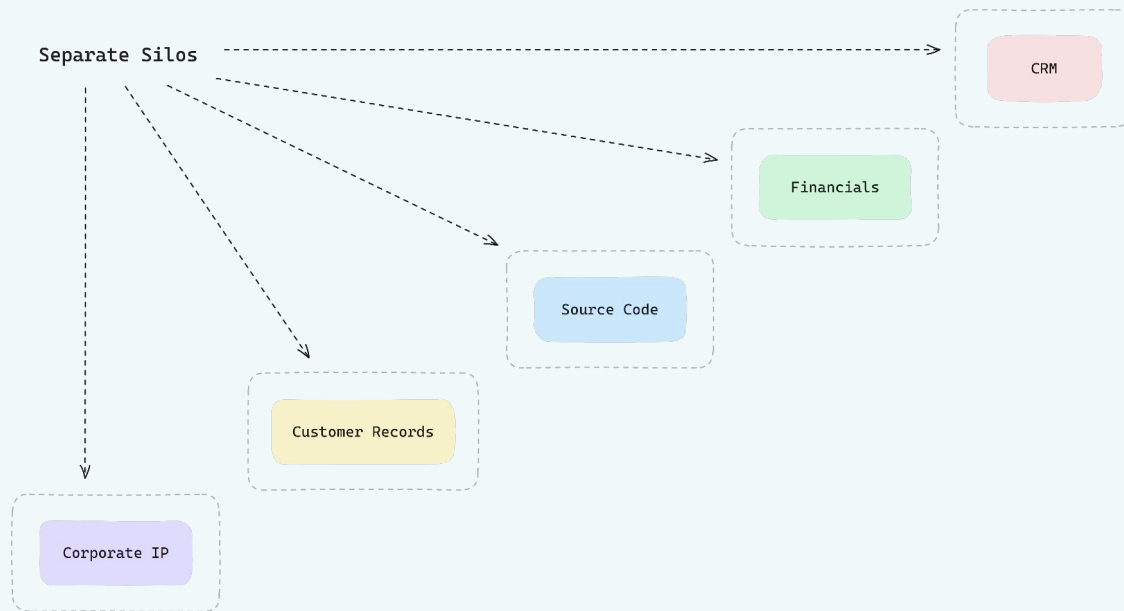
Enterprise AI requires

Proprietary Data

...but there's a **security gap**

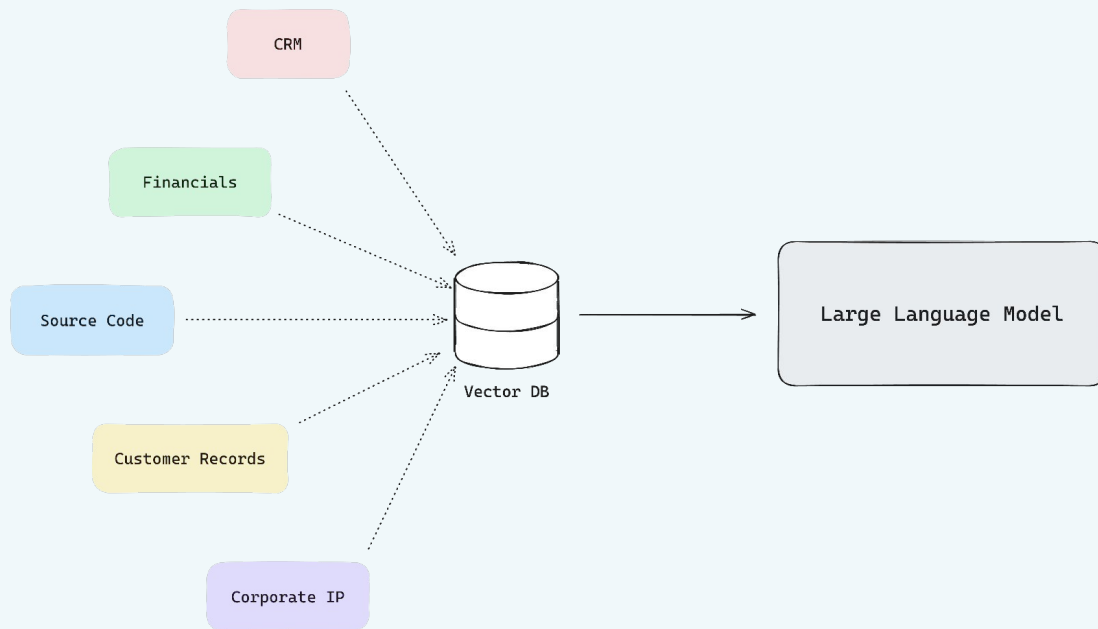


Enterprises Before AI



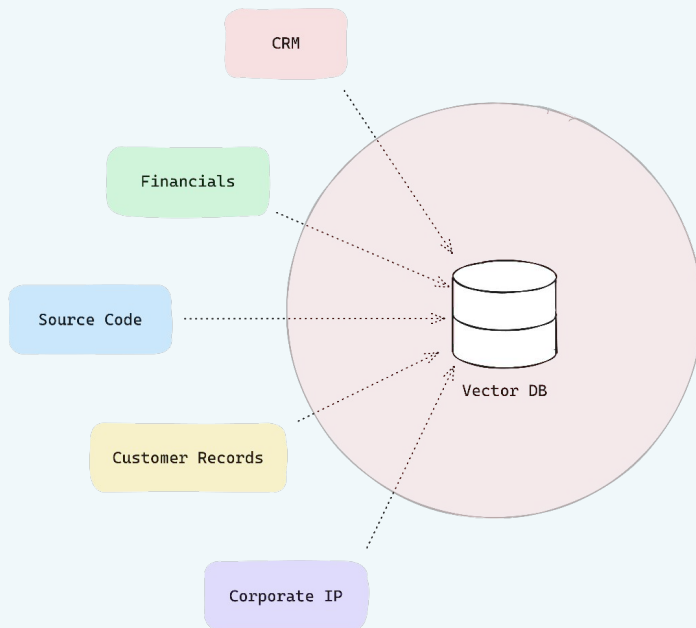


Enterprises With AI





Enterprises With AI



Centralized data =
**massive breach
potential**

Vector DBs are not
equipped to deal
with this risk



Vulnerability Demo



1

Vector embeddings can be **inverted to original data**

3

Standard vector databases **have little security** against embedding leakage

Current Vulnerabilities

2

Embeddings should be **protected** like source data



Must have **cryptographic protections** to prevent embedding leakage



Must maintain **high performance**, not sacrifice it for security

Solution Requirements



Must be compatible with existing frameworks & **simple to implement**



Solution Demo



[cyborginc/vectordb-inversion-demo](https://github.com/cyborginc/vectordb-inversion-demo)



CyborgDB

Makes Enterprise AI Secure



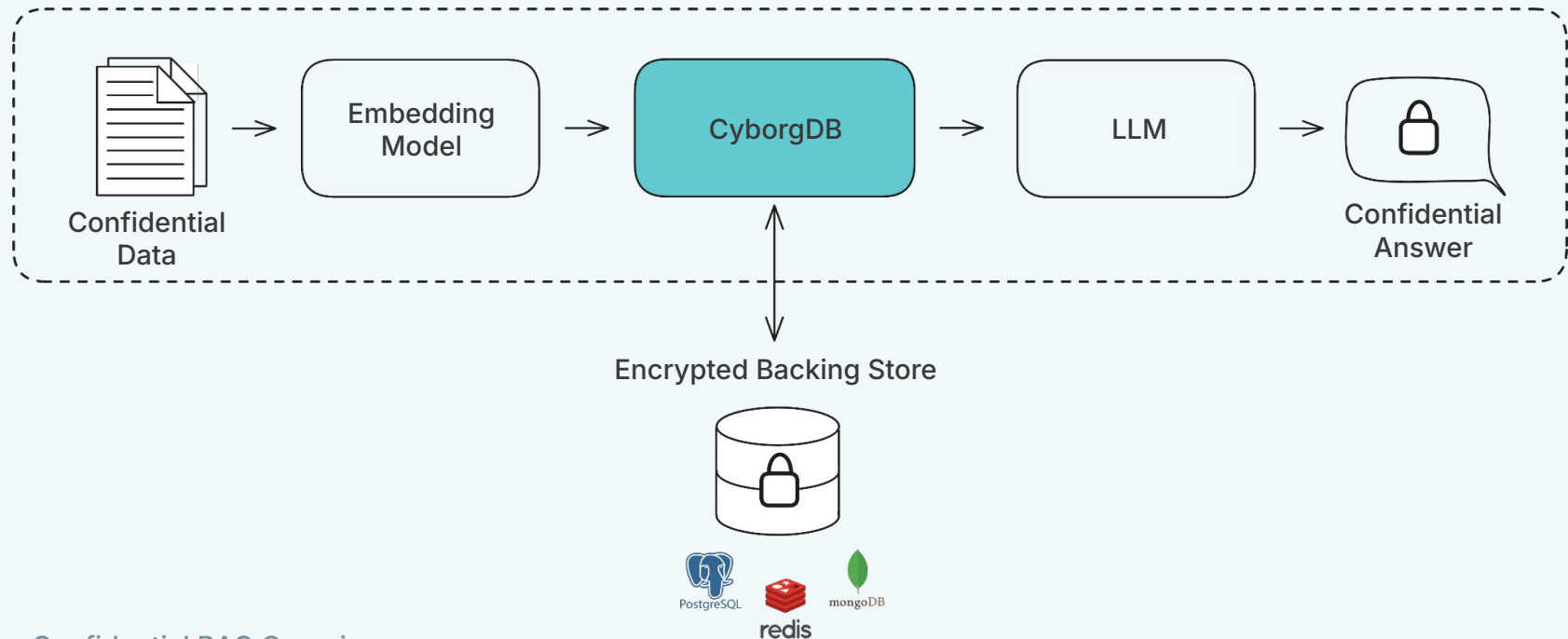
**End-to-end
encrypted** for the
entire inference
process



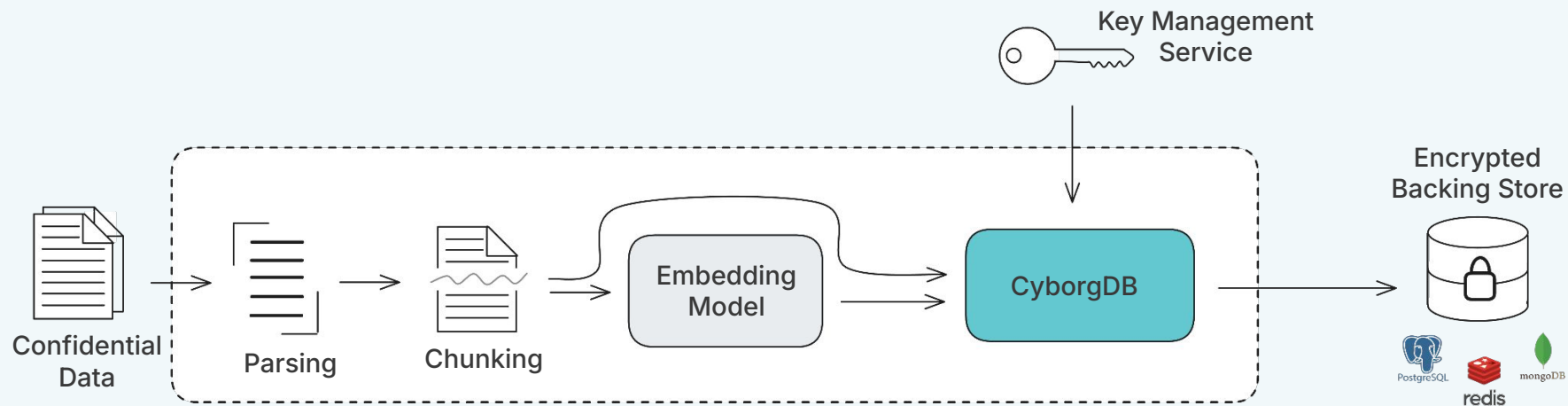
High-performance
encrypted search
for **production
workloads**



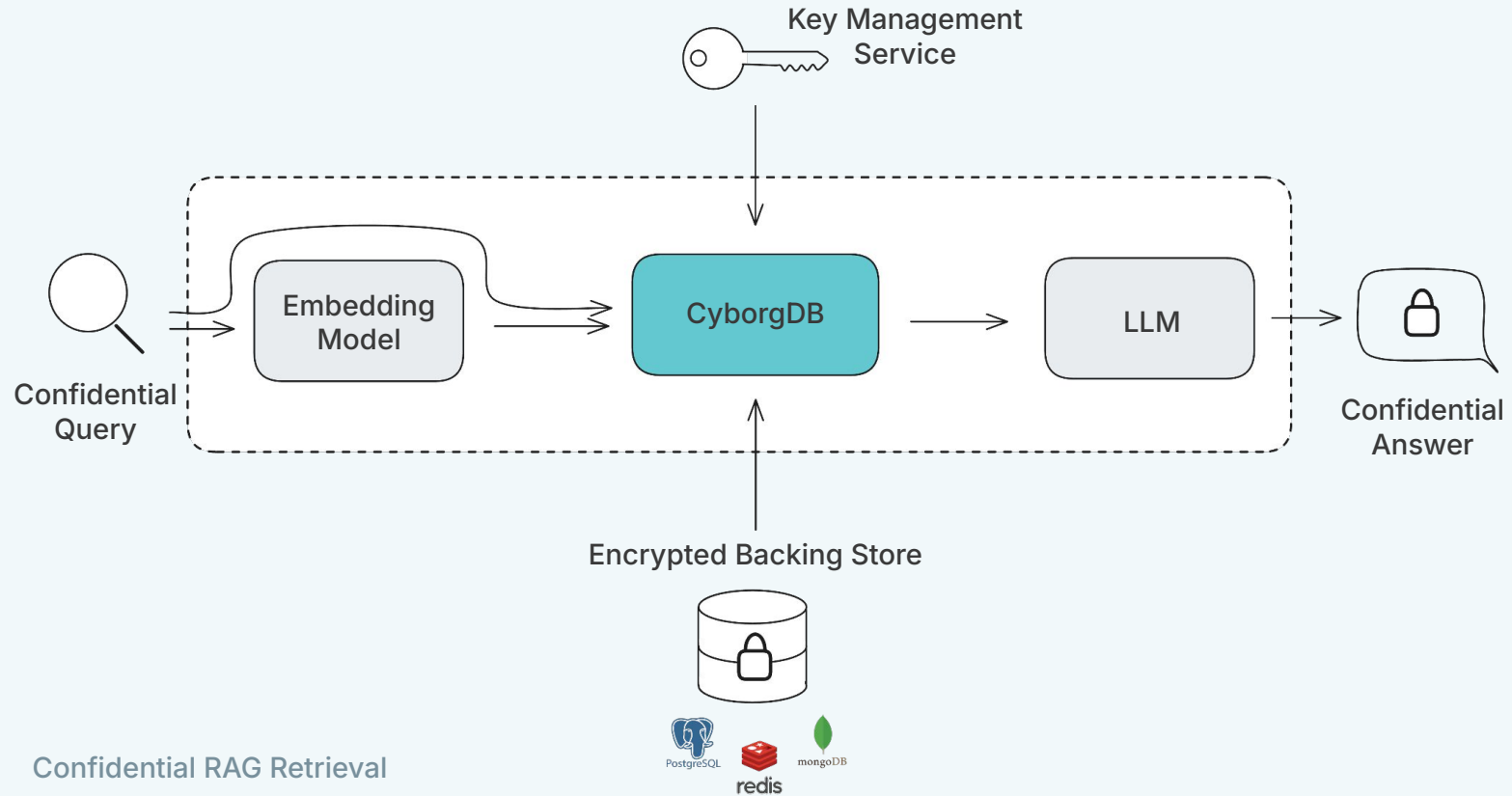
Drop-in API for
deployment
**in minutes, not
days**

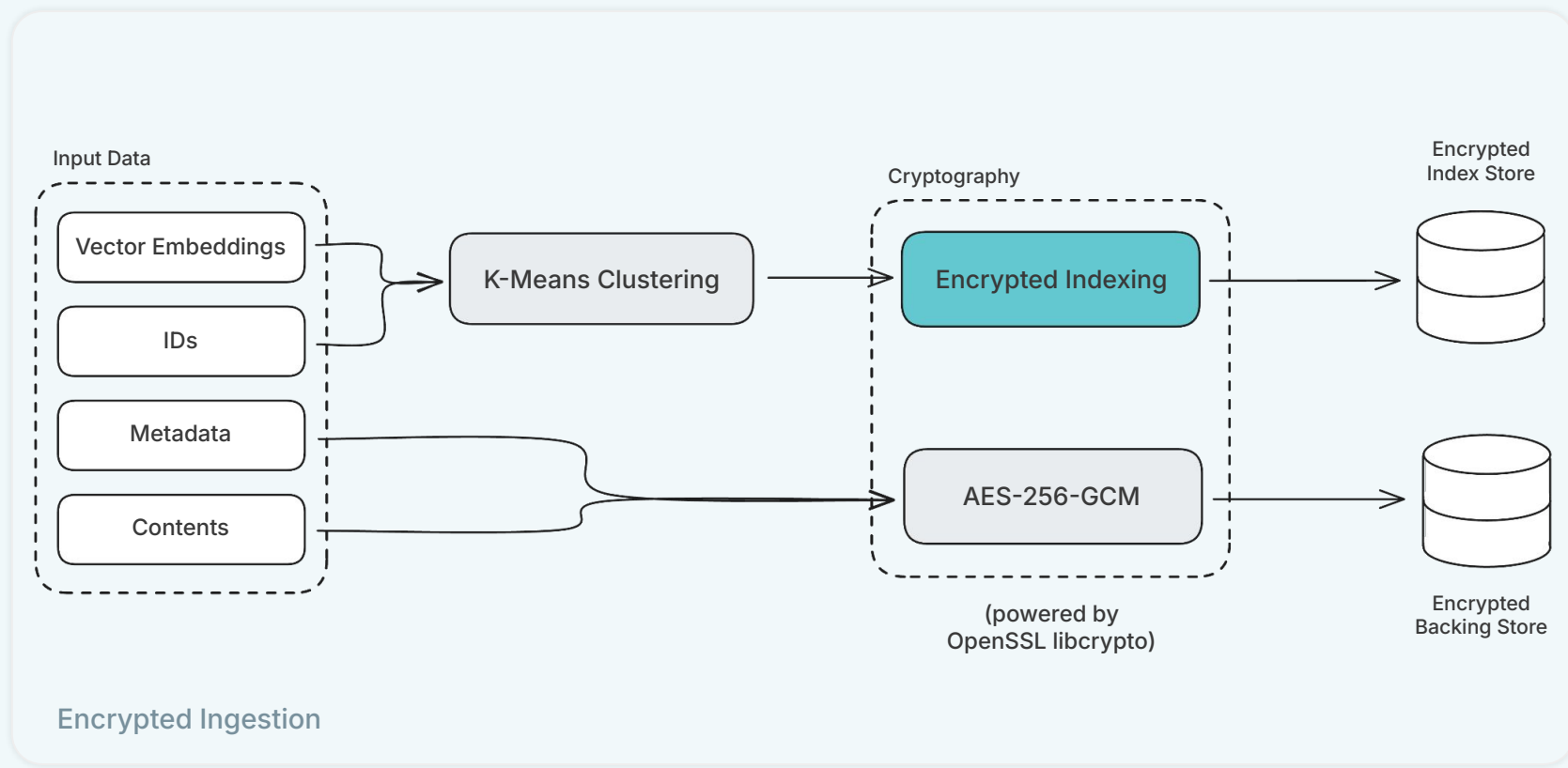


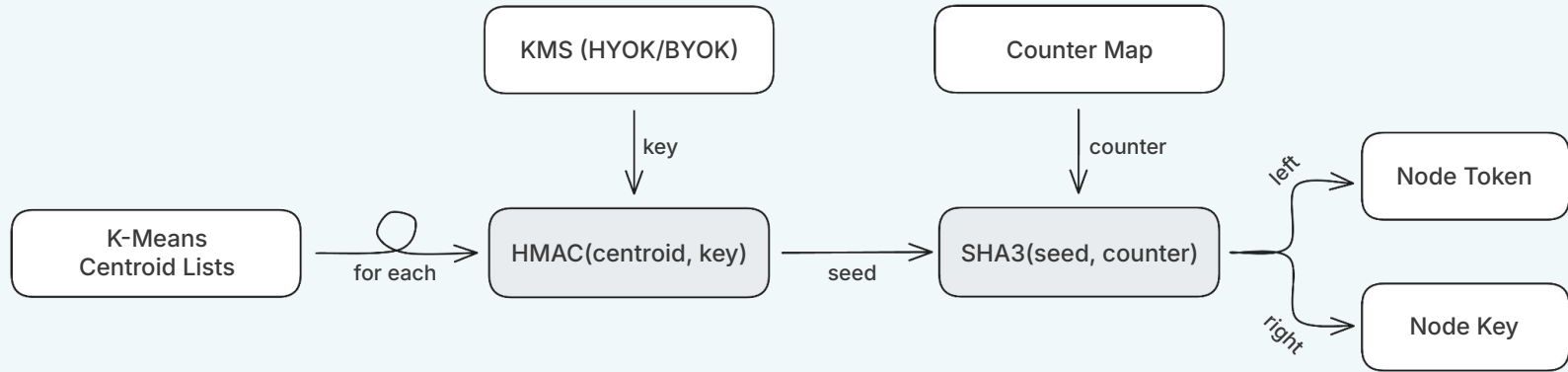
Confidential RAG Overview



Confidential RAG Ingestion



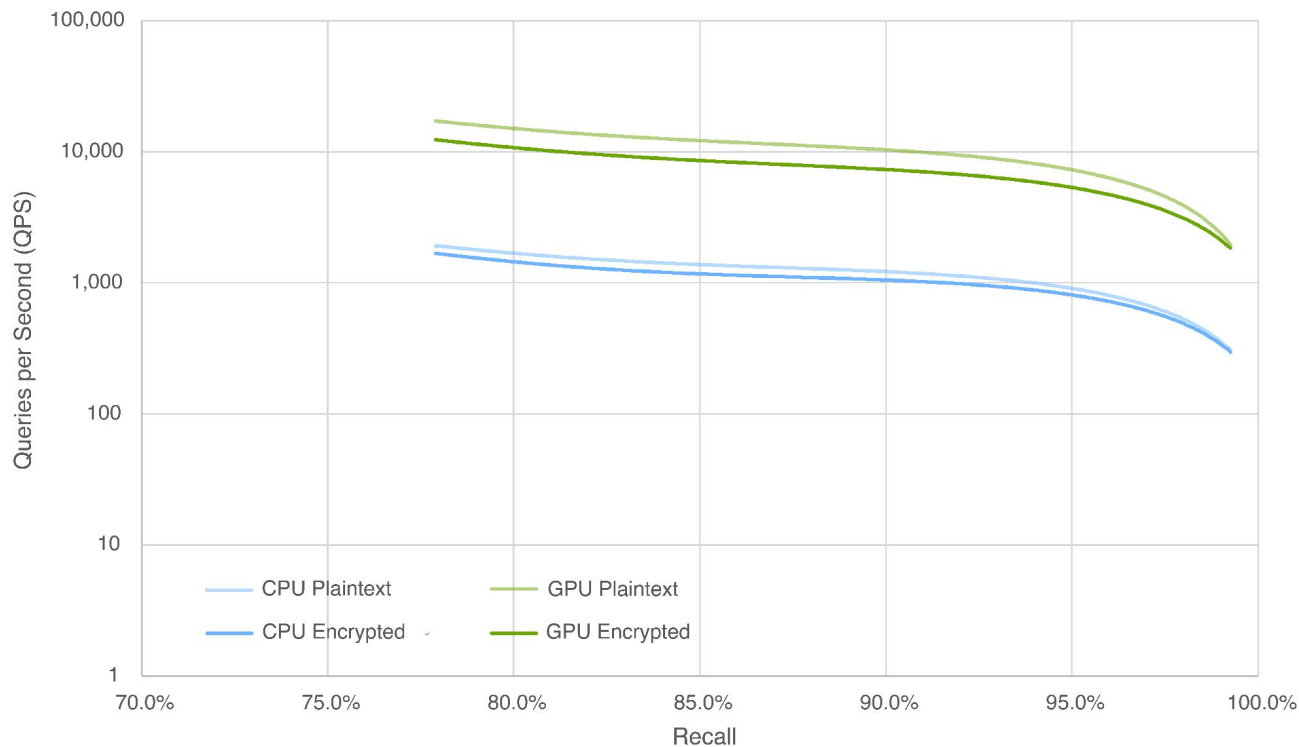




Encrypted Indexing



Recall vs. QPS



15%

Retrieval overhead vs.
plaintext vector search

7x

Performance uplift
running on GPU

1%

Build-time overhead
vs. plaintext indexing



Approach

Security

Performance

Deployment

Practicality

Plaintext DB

✗ No encryption

✓ Fast

✓ Easy to deploy

✗ Leaks data

Homomorphic / SMPC

✓ Strong

✗ Very slow

✗ Hard to integrate

✗ Not production-grade

TEE-only

✓ Strong ¹

✓ Fast

⚠ Complex infra

⚠ Incomplete

Confidential Vector DB

✓ Strong

✓ Fast

✓ Easy to deploy

✓ Production-grade ready

¹ [Recent exploits](#) have shown that TEEs are vulnerable to some attack vectors including physical compromise



CyborgDB

The Encrypted Vector Proxy

Available for your stack:



```
docker pull \
cyborginc/cyborgdb-service
```



```
pip install cyborgdb
```



```
npm install cyborgdb
```



```
go get github.com/cyborginc/
cyborgdb-go
```



//

We believe Secure AI will define the
next decade of the enterprise

— and it's possible with **Secure Vector Databases**



Build Secure AI With Us

Nicolas Dupont, CEO
ndupont@cyborg.co

Cyborg
cyborg.co

