DASHLANE

AI Without Access: Shipping Intelligence When You Can’t See User Data

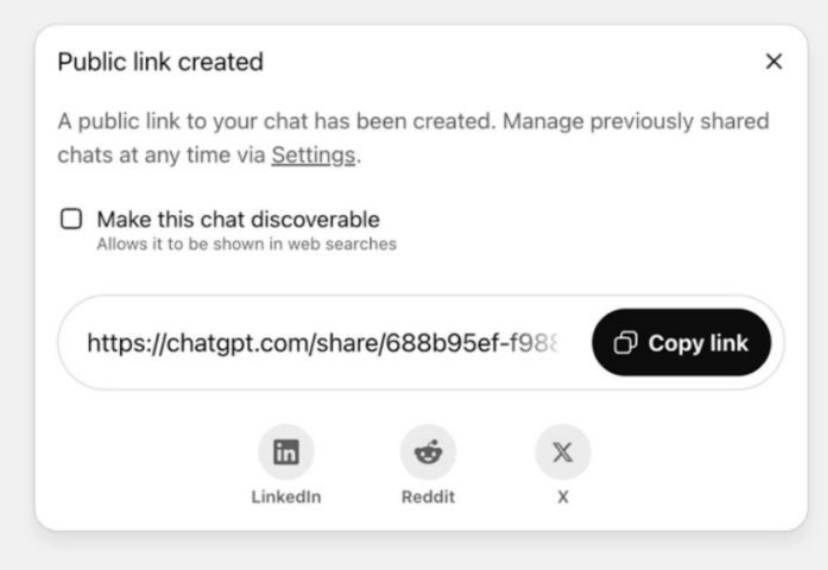
Tech Target - June 17 2026

Frédéric Rivain
CTO Dashlane


AI Capabilities
Locked Data
Machine Learning
Data Processing
Generative AI
Personal Information
Financial Data
Encrypted Content

Nearly 100,000 ChatGPT conversations searchable on Google

- Summer 2025
- Thousands of private AI conversations indexed by search engines
- Users didn’t realize their data could become public



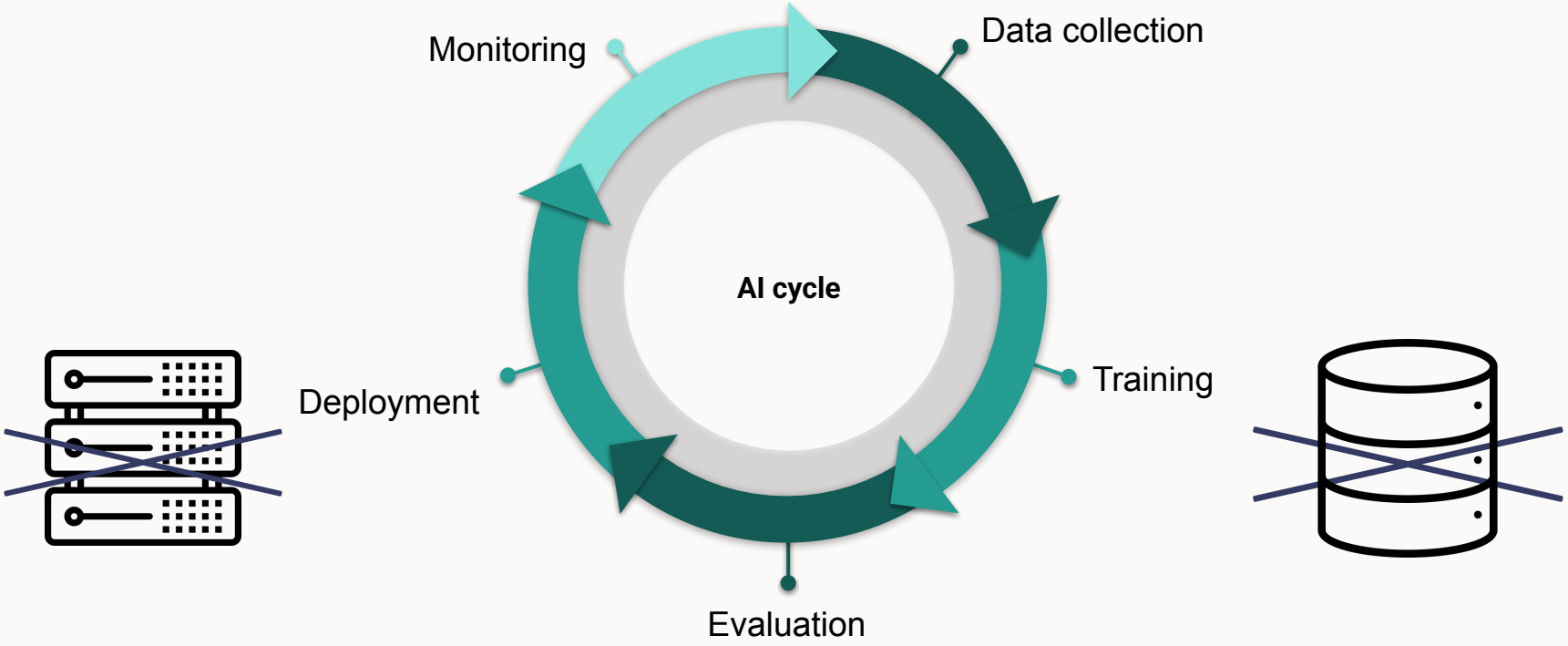
Three forces you can't ignore

1. Customers → “Don’t look at my data”
2. Regulators → “Prove you don’t”
3. Enterprises → “Put it in the contract”

68% of consumers globally are (…) somewhat or very concerned about their privacy online, and 57% of consumers agree that AI poses a significant threat to their privacy.

Forbes, March 18 2025

What actually breaks


Monitoring
Data collection
AI cycle
Deployment
Training
Evaluation

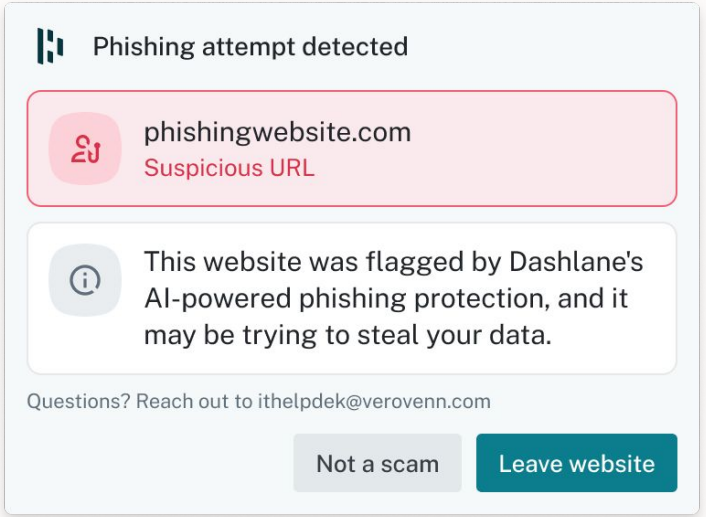
Encrypting data is not enough

End-to-end encrypted…
except when it isn't.

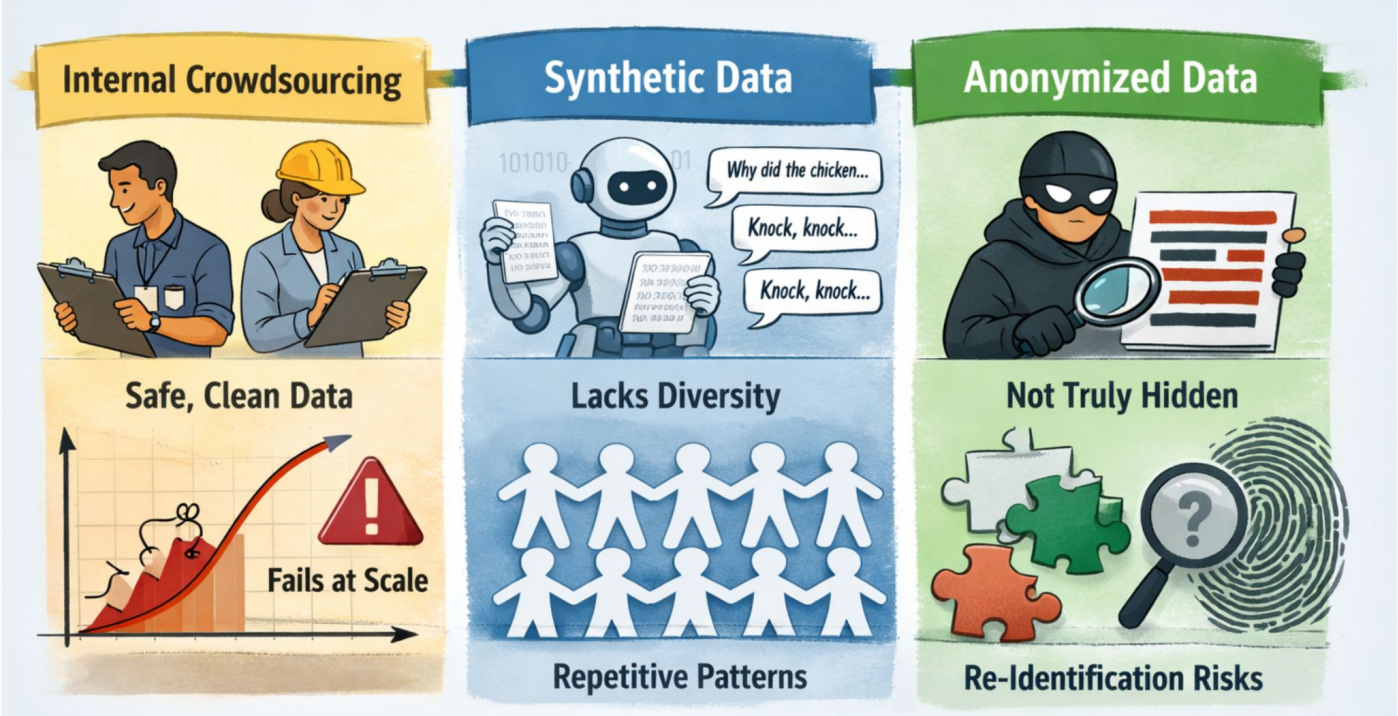
Building private AI by design, in practice

Use Case 1: Protecting users from phishing without seeing their browsing activity

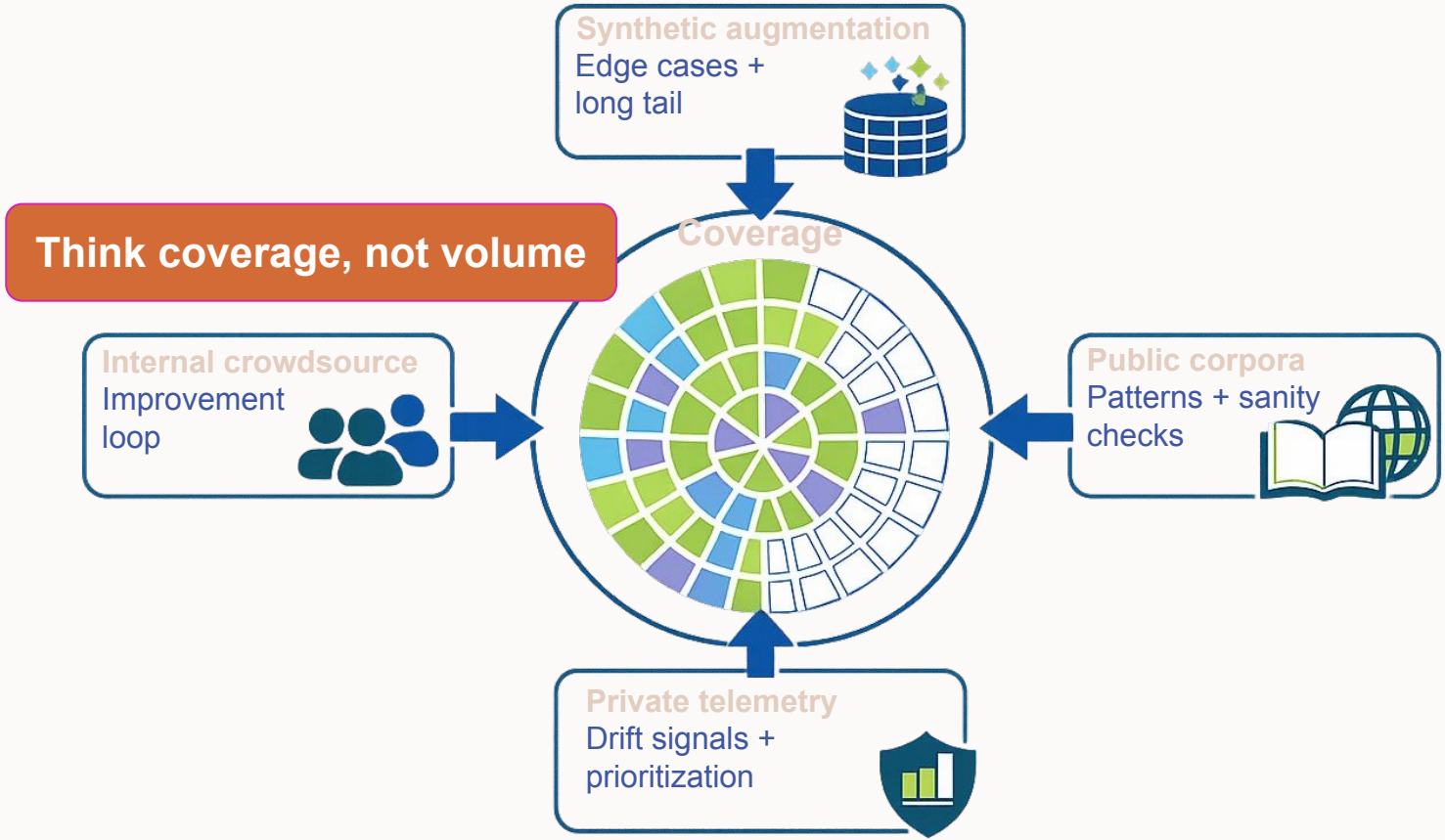
- Data collection
- Model training
- Deployment



Training a model without seeing the data



Use Multiple data sources to build diversity



Frugal modeling

Start smaller than you think

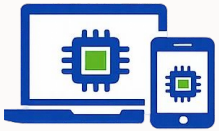
Less data needed

Faster iteration loops

Clearer failure analysis

Lower cost + energy

Easier governance

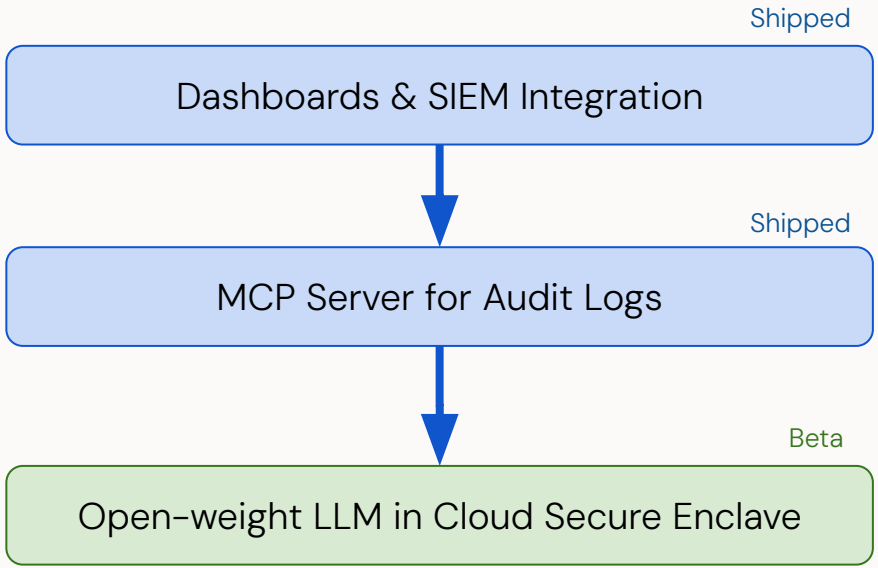


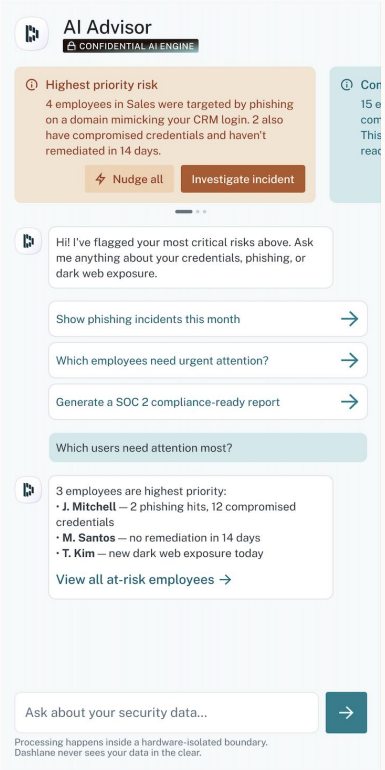
On-device deploy

Lesson 1

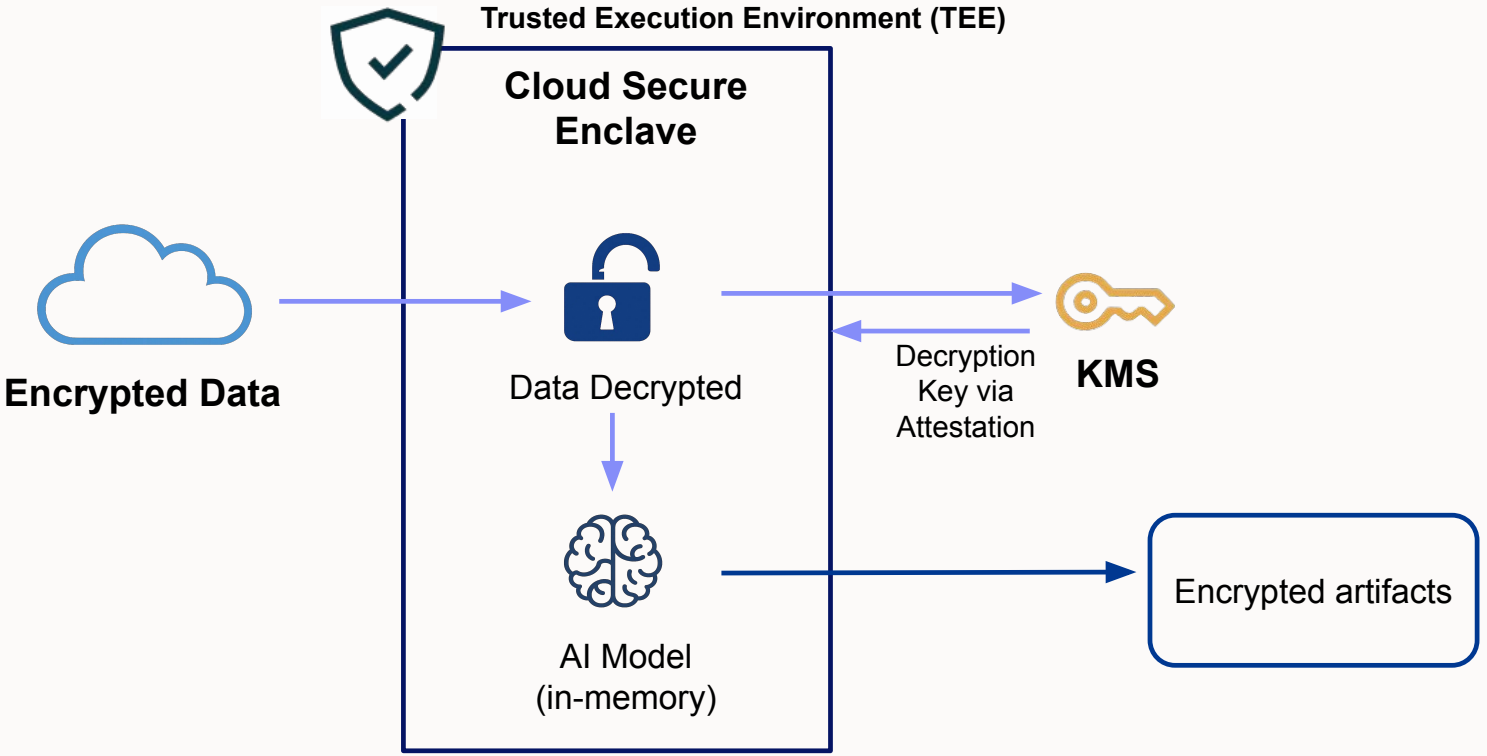
- Data coverage is critical
- Frugal Model may be enough
- Run on device for maximum privacy

Use Case 2: AI Copilot on data we can never see

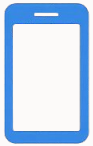




What about Confidential Computing?



Deployment: Right Compute, Right place



ON DEVICE

Fast, Offline

Max privacy

Model size limited, feature engineering needed

CONFIDENTIAL COMPUTING

Bigger models, More context

Confidential boundary

Deployment only, training is limited

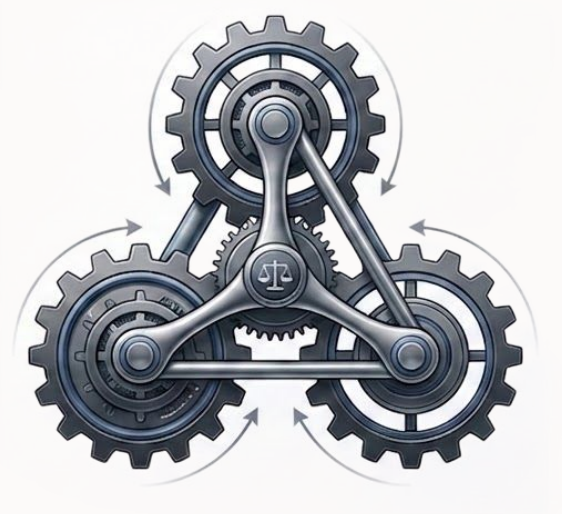
Lesson 2

- Feature Engineering may be enough
- End to end encryption: in transit, at rest, and in use leveraging Confidential Computing

A playbook for privacy-preserving AI

Privacy-by-design is a balancing act

PRIVACY

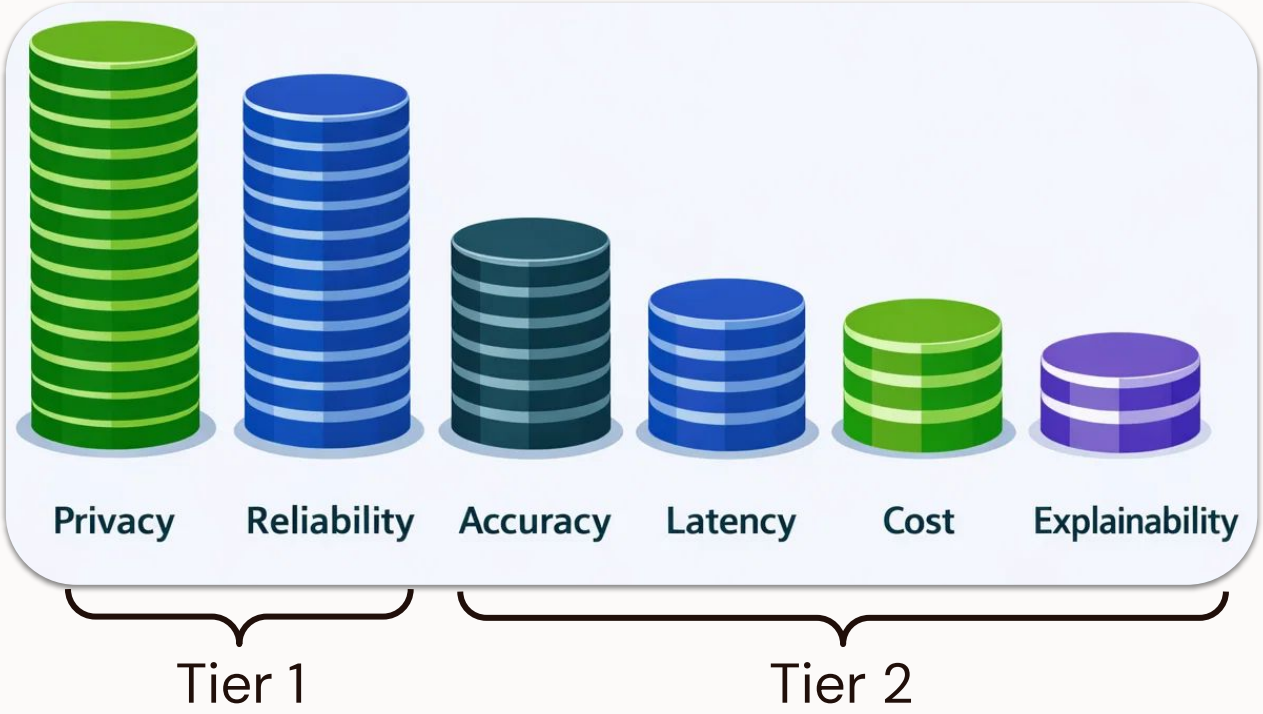


MODEL PERFORMANCE

VELOCITY

Privacy constraints as an input, not a review gate

Privacy Stance
Zero-Knowledge Architecture
Privacy policy
Acceptable Use Policy
AI Policy



Where to start

Next Week	Next 3 months	Next 6 months
● Privacy One-Pager ● Cross-functional accountability	● Launch acceptance criteria ● Training pipeline ● Deployment strategy ● First prototype	● Pilot in production ● Repeat playbook

Takeaways

1. Start with the privacy boundary before the model choice.
2. Optimize training data collection for coverage, not just scale.
3. Use smaller models
4. Choose deployment based on the performance need
5. Ship incrementally. Don’t wait for the “perfect” private AI architecture.


DASHLANE