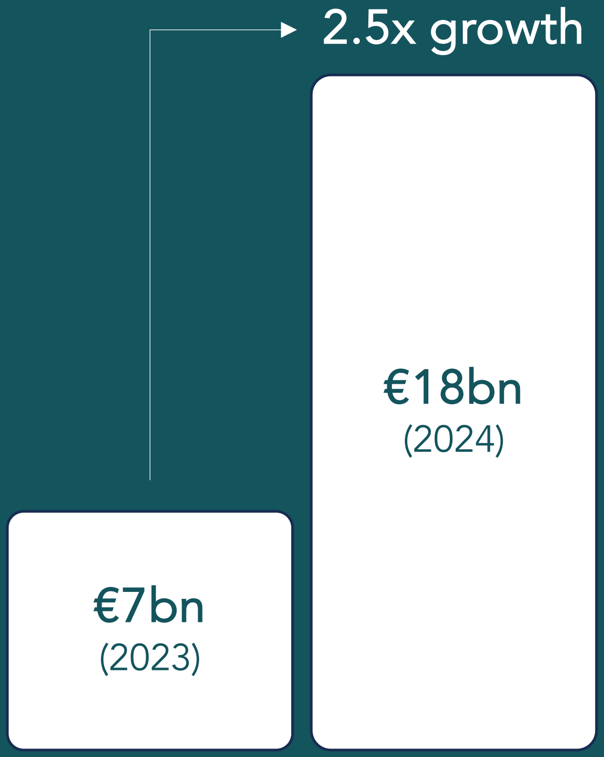
Leanear

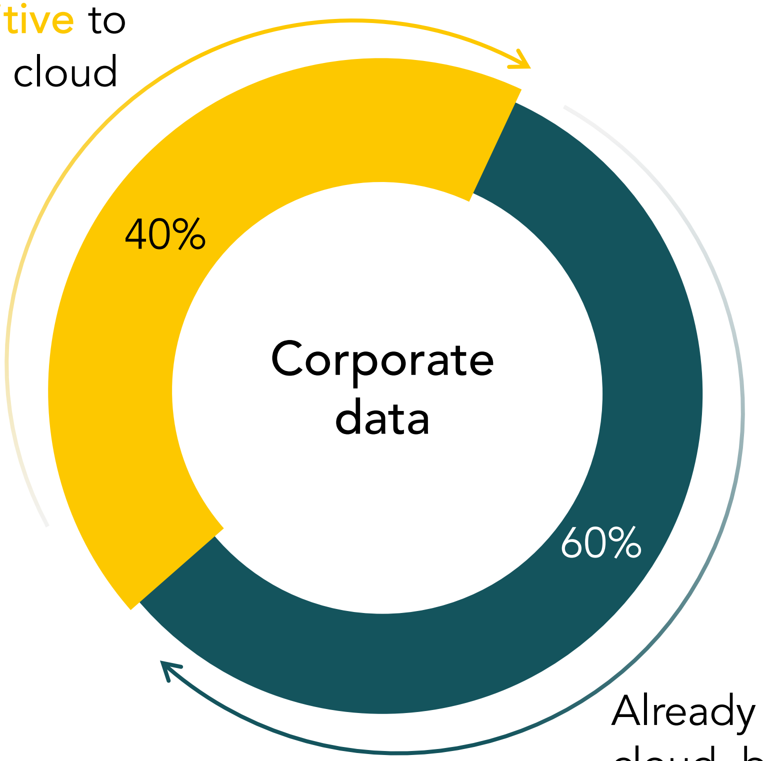
Advanced cryptography for multimodal AI security

Budgets for generative AI are skyrocketing



Average enterprise spend on LLM

But competitive AI models require proprietary datasets in the cloud



Too sensitive to be in the cloud

Already in the cloud, but at risk

Sources: Andreessen Horowitz, Statista

CISOs are still reluctant to store sensitive data in the cloud

As existing data security paradigms fail to provide sufficient assurances

Cyberattacks

94%

of organizations experienced a cyberattack in the last year

Liability

90%

of CISOs feel more liable due to AI/GenAI

Misconfigurations

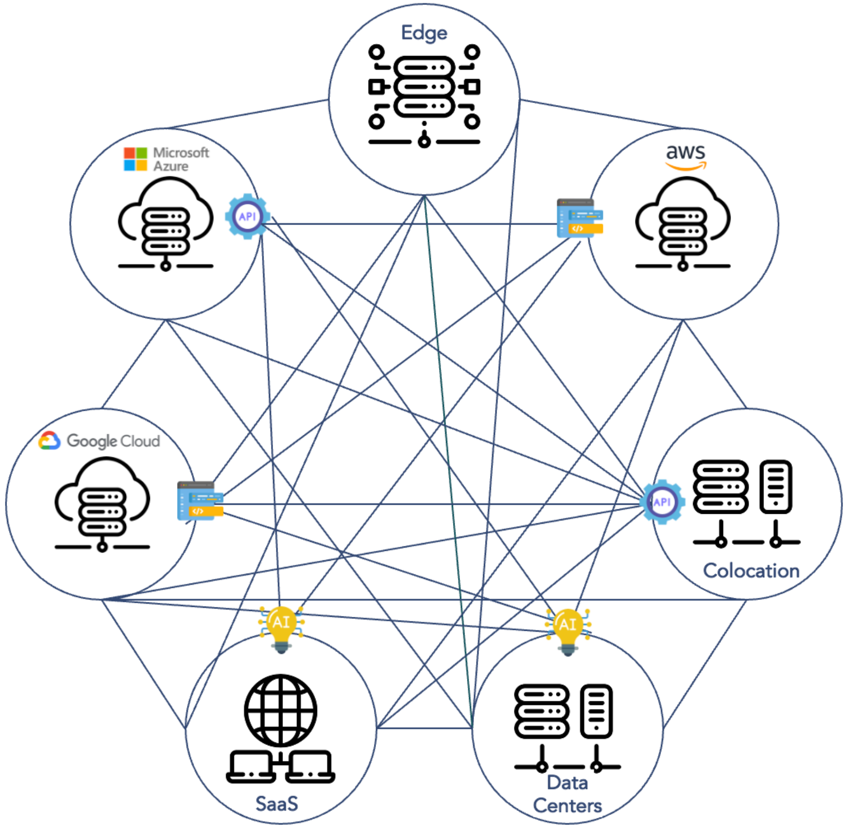
80%

of security exposures stem from identity misconfigurations

Sources: Cloud Security Report 2023

Perimeter security falls short in distributed IT environments

Making suitable data encryption a necessity



Traditional perimeter security is insufficient for the complex reality of cloud computing, especially for multimodal AI solutions. The only solution is to protect data with encryption.

But, classic cryptographic models which assume static environments and direct communication, do not align with today's dispersed data sources and multi-access scenarios.