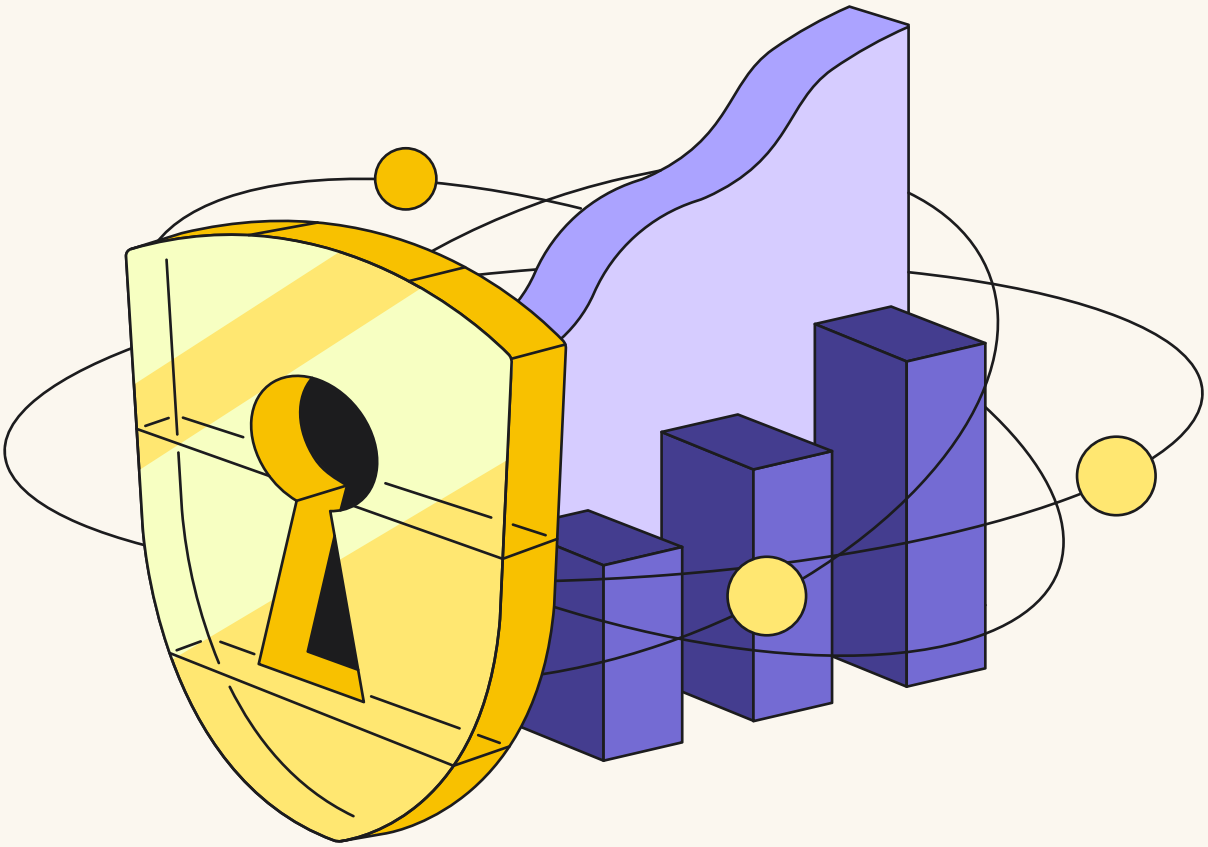


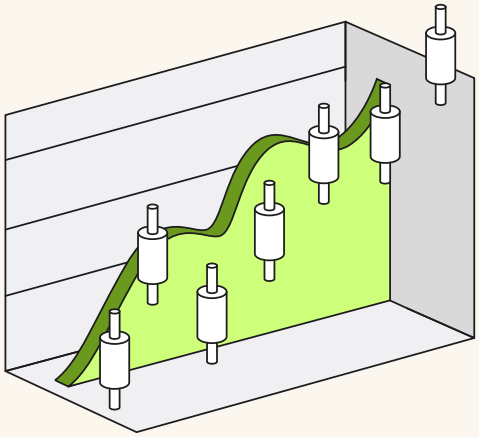
Miro Enterprise Key Management

miro

miro

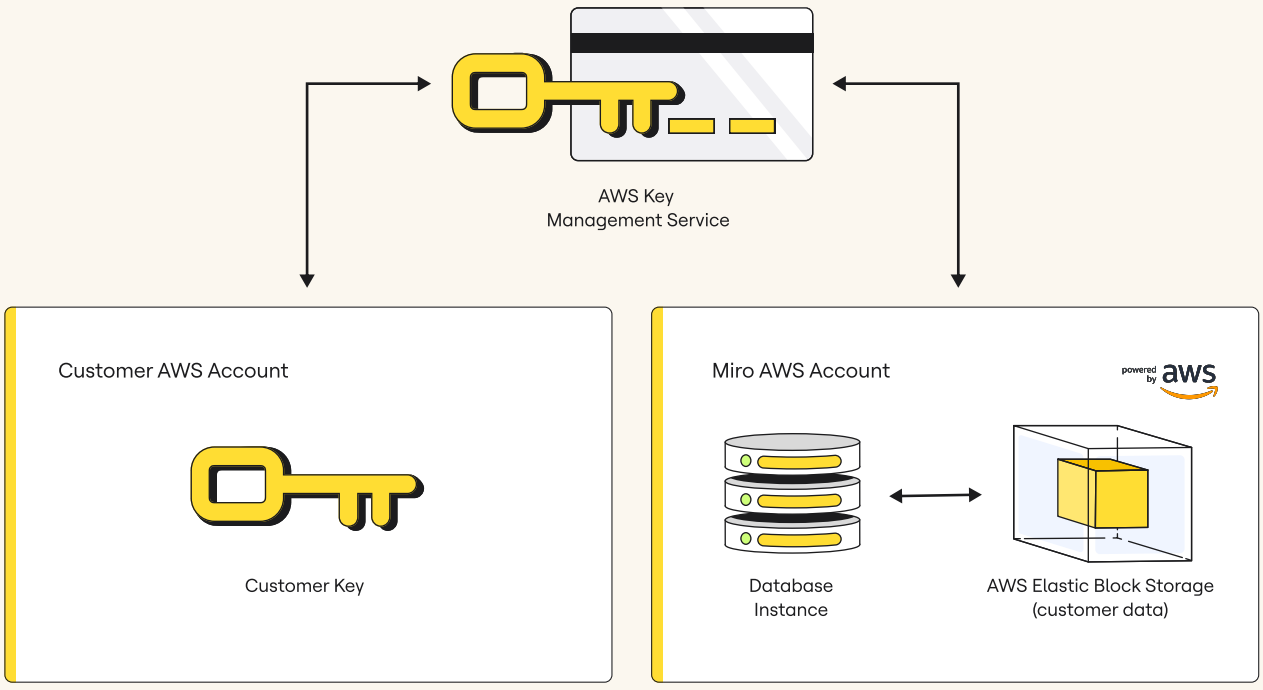
Take Control of Your Growth

Do you want more control over your data in Miro, and visibility into how your encryption keys are used? Now you can bring your own key (BYOK), so you can control and manage the encryption of your organization's data in Miro.



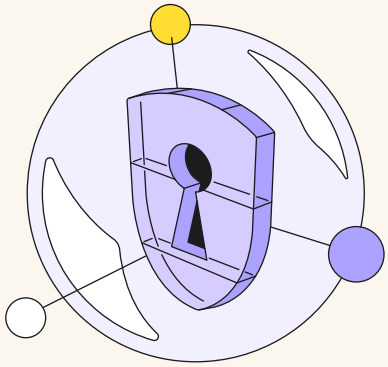
Why Miro EKM

- **Easy to implement.**
  100% cloud-based solution. No hardware to install or maintain.
- **Full control over key access.**
  Revoke your key at any time to render all encrypted data unreadable to Miro and end users.
- **Detailed access visibility.**
  Monitor activity logs related to your encryption key via AWS CloudTrail.



How Miro EKM works

Miro supports encryption key management with a key hosted in your own AWS account via AWS KMS. Miro's EKM lets you segregate the storage of content at rest. With EKM, you gain greater auditing visibility and increased access control over data (user-generated content), such as shapes, widgets,and uploaded files.



Data encryption at Miro

Securing your data is a top priority at Miro. Customer data is encrypted in transit and at rest for all Miro customers by default, regardless of their plan. When you connect to Miro over the internet, your data is protected by TLS 1.3 encryption and PKI certificates issued by Amazon Web Services (AWS). Once your data reaches Miro, it is encrypted at rest with AES-256 encryption using keys managed by Miro via AWS Key Management Service (KMS).

Learn more about security at Miro.
https://miro.com/trust/security/

