



Flock: A Framework for Deploying On-Demand Distributed Trust

Darya Kaviani*¹

Sijun Tan*¹

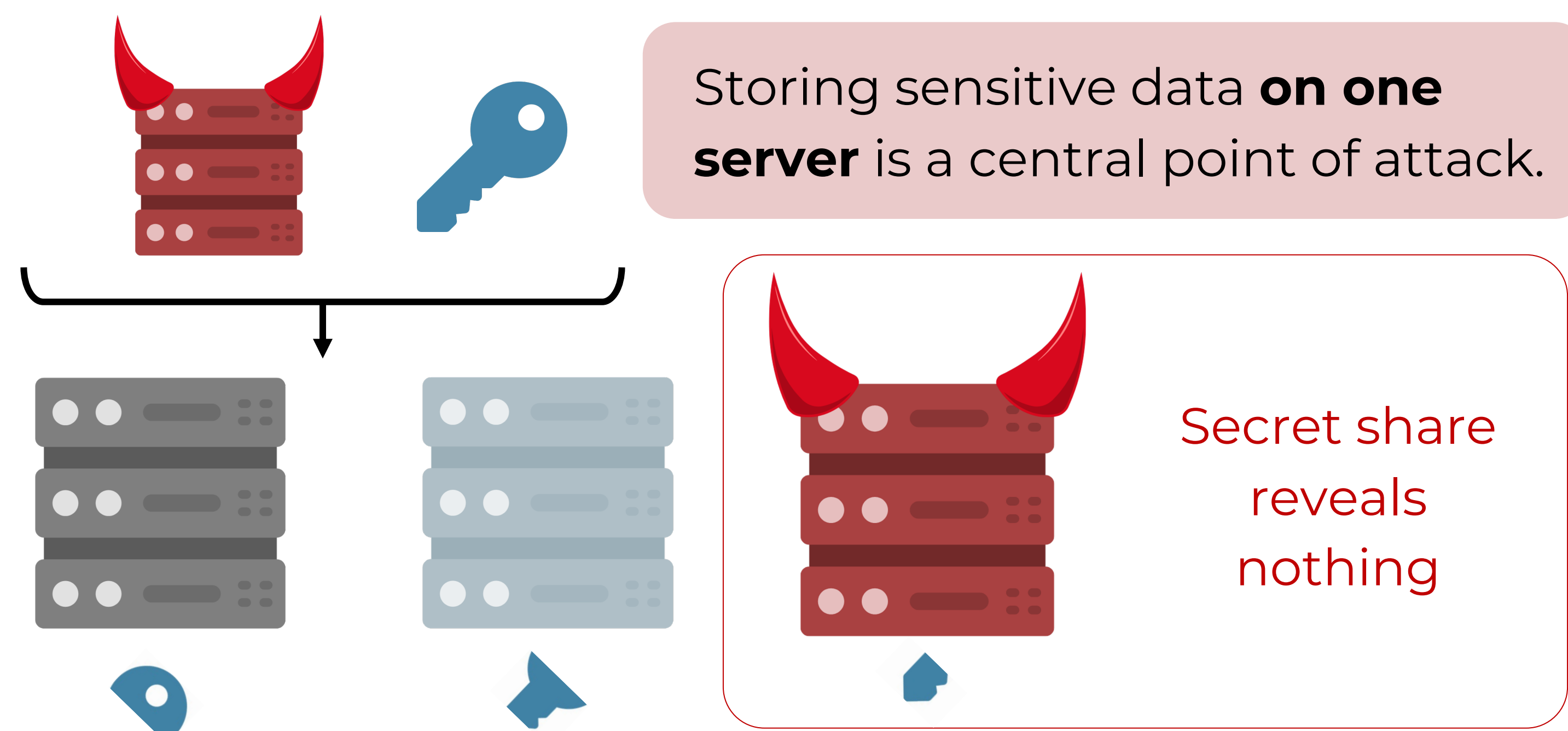
Pravein Govindan Kannan²

Raluca Ada Popa¹

¹UC Berkeley

²IBM Research

Why Distributed Trust?



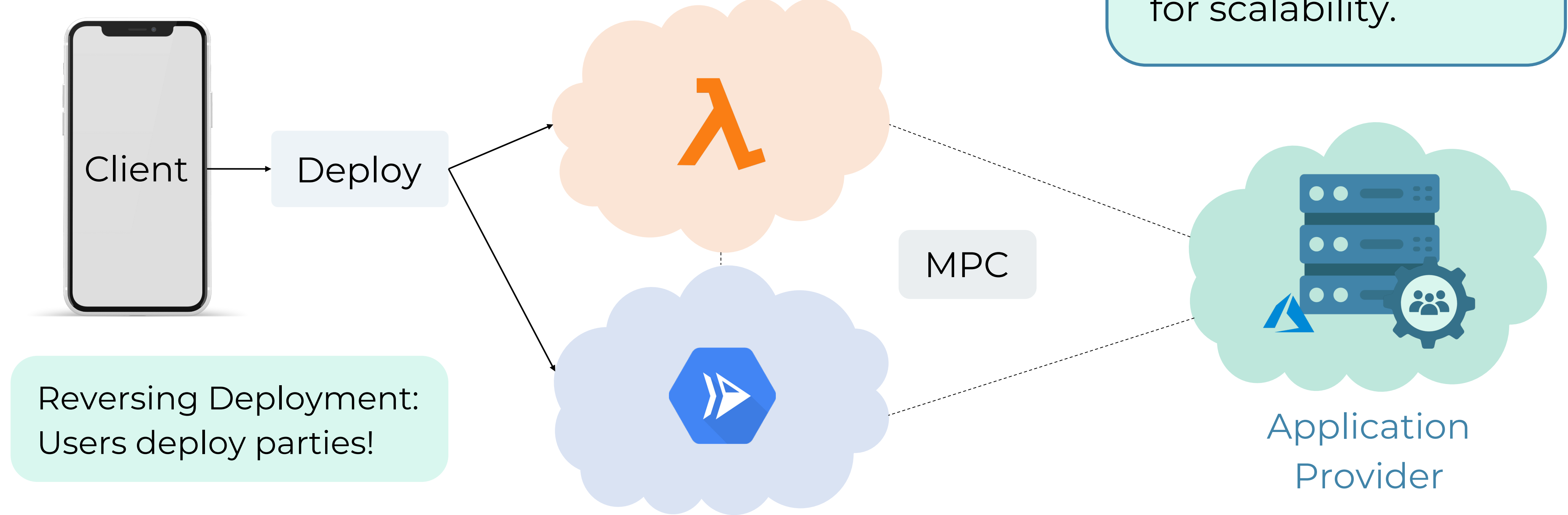
Distributing trust avoids a central point of attack by **distributing sensitive data** among **N trust domains**.

Applications

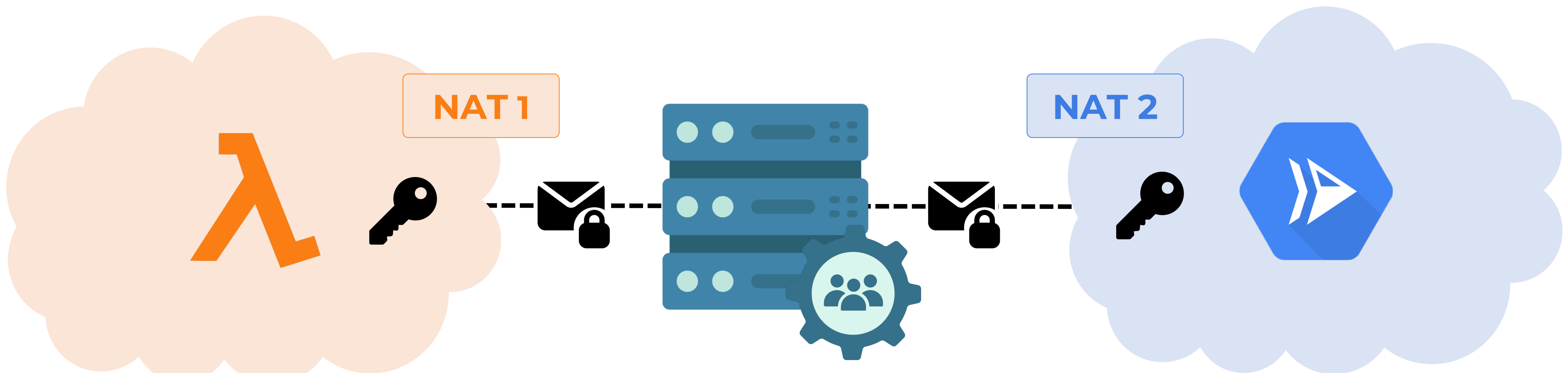
Signature Generation	Secret Recovery
Crypto Custody	Secret Key Recovery
Code Signing	Password Manager
Certificate Authority	Private Queries
AES Decryption	Data Freshness

On-Demand Distributed Trust: Clouds as Trust Domains

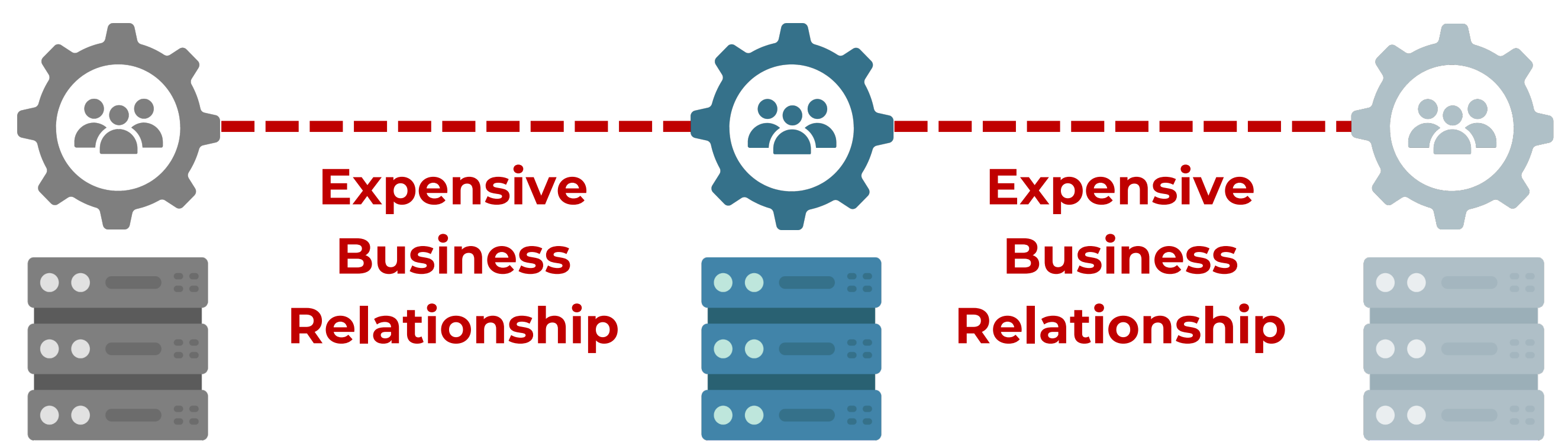
- A user is the trusted owner of its sensitive data.
 - Clouds have APIs for automatic deployment.
- Each user's **client** can **deploy** the user's trust domains, using **serverless** compute instances for scalability.



Flock Relay Protocol



Traditional Distributed Trust



Evaluation: Compared to Traditional

Flock performs comparably to traditional distributed trust!

- 1.05x latency
- 0.7-2.3x cloud cost

* equal contribution