
CryptoMove

SMART CITIES

About CryptoMove

5+ years R&D

Patents:

Hello programming language

Fortune 100 & Federal case studies

Backed by:

SOCIALCAPITAL

DRAPER ASSOCIATES

TechCrunch

FORTUNE

BUSINESS INSIDER

CB INSIGHTS

Smart cities run on data

Data powers new services

Smart lights | Smart meters | Health services | Disaster & resiliency

City threat surface is large and not well understood

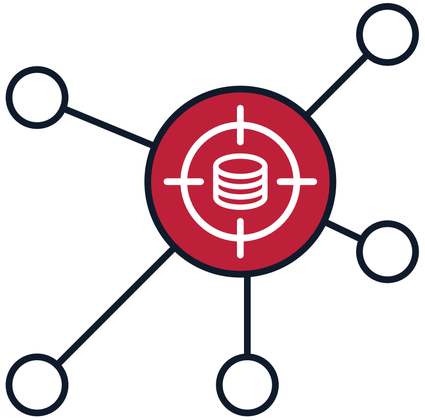
Data distributed

Overlap of digital + physical world

Lack of security awareness & capability

Citizen privacy

Stationary target data infrastructure



#1

risk of attack

Encryption doesn’t work

- Long term will fail
- Difficult implementation & key management
- Ransom
- Exfiltration
- Destruction

San Leandro

4k+ smart lights deployment

Long-term innovation focus

Applying security to existing systems

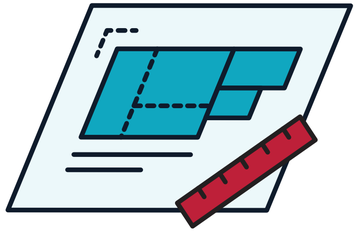
statescoop

Smart Wi-Fi grid is like a Nest Thermostat for the entire city of San Leandro, California

SAN LEANDRO NEXT.com

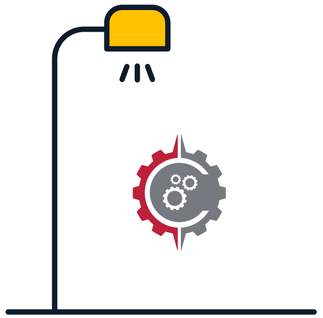
San Leandro Set to Invest $5.2 Million in Smart City Technologies

CryptoMove + San Leandro project



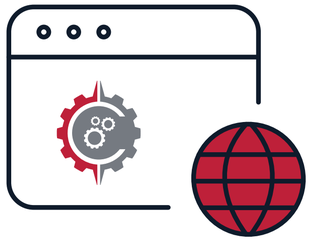
Threat model

Building reference architecture for cities worldwide



Smart lights protection

Keys & data

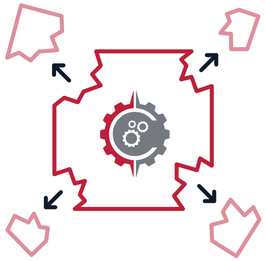


Enterprise data protection

Files, keys, & applications

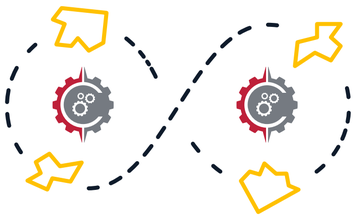
How it works

STEP 1



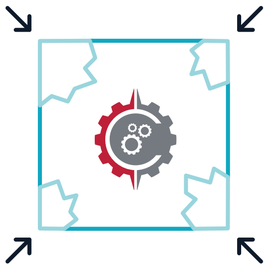
CryptoMove fragments, encrypts, and mutates your data.

STEP 2



Your data fragments move and re-encrypt continuously in the cloud across CryptoMove nodes.

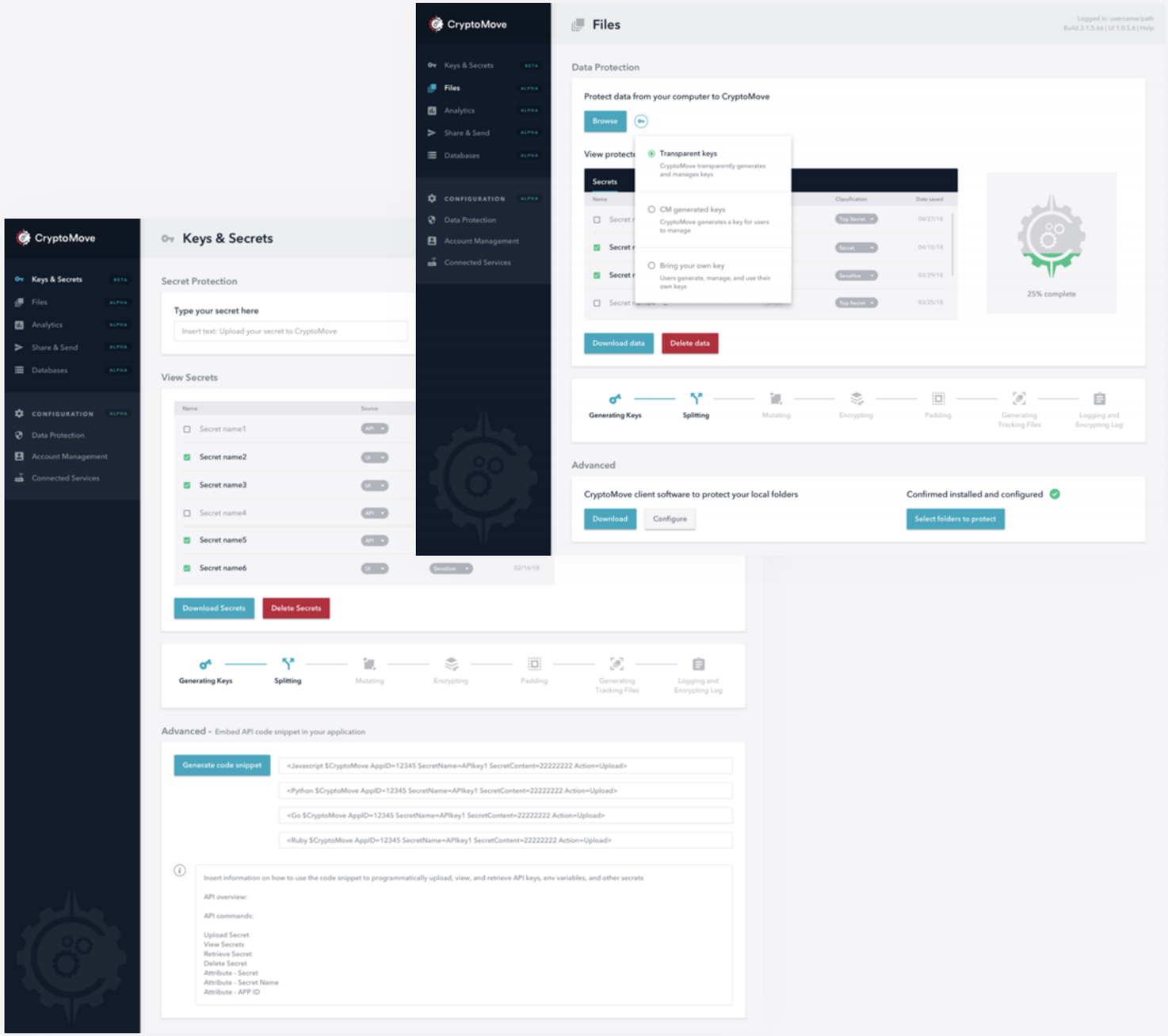
STEP 3



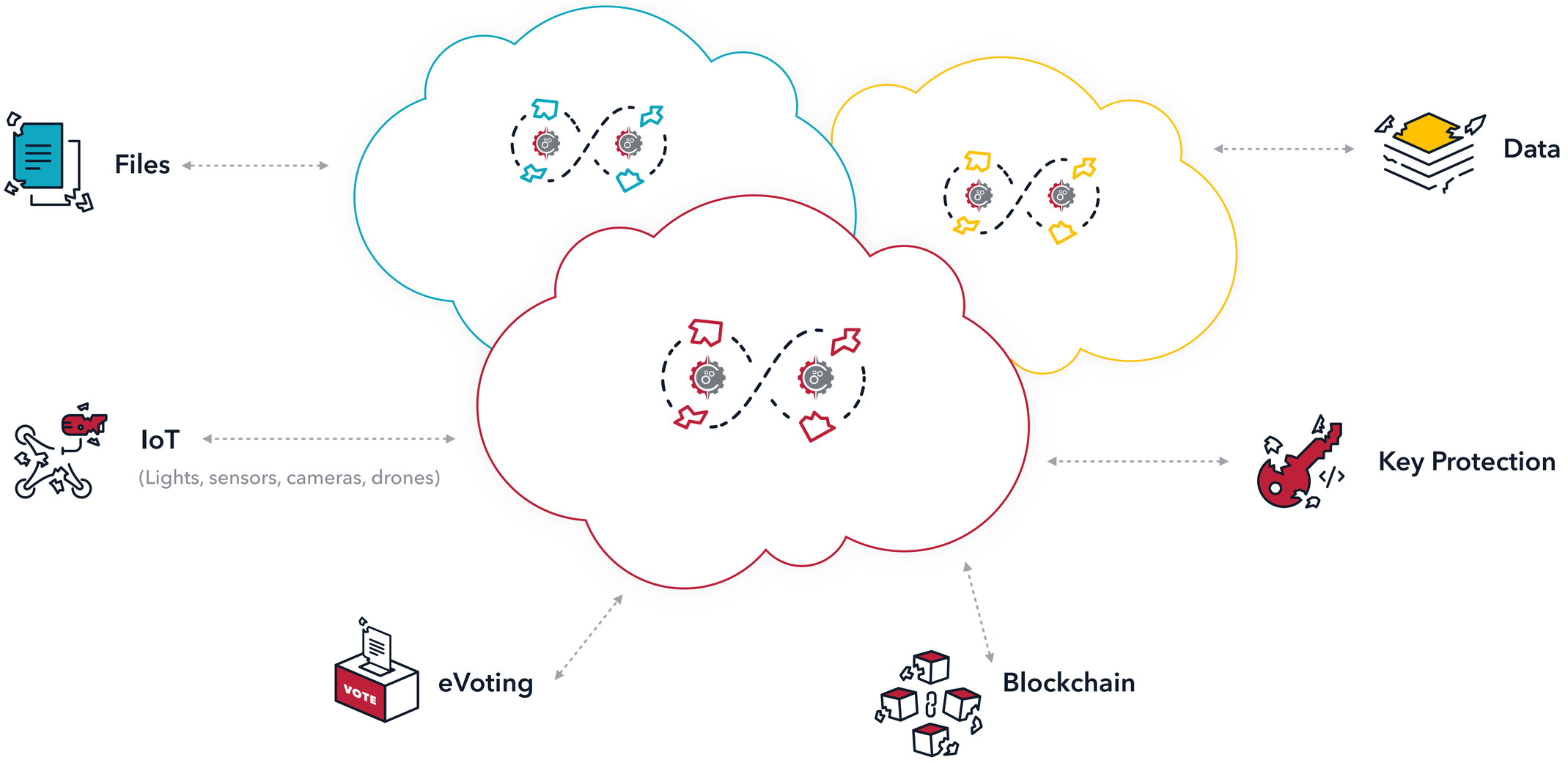
CryptoMove's decentralized ledger recovers your fragments on your authorization.

CryptoMove - DPaaS

- Advanced data protection delivered as a service from the cloud
- Citizen & user centric
- Adds on to existing tools and technologies



Use cases



Case studies

DHS

Drones

Sensors

Cameras

Fortune 100

Data Protection

Cloud

Key Vault