



CryptoMove



CLOUD

SMART CITIES

3RD PARTY
VENDOR

ON-PREM

STORAGE





DATABASE

CONTAINER
SHIPS



About CryptoMove

5+ years R&D

Patents:    

Hello programming language

Fortune 100 & Federal case studies

Backed by:

SOCIALCAPITAL



 **TechCrunch**

FORTUNE

BUSINESS INSIDER





Smart cities run on data

Data powers new services

Smart lights

Smart meters

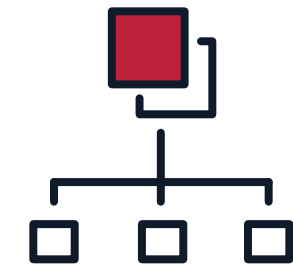
Health services

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

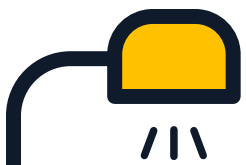


San Leandro

4k+ smart lights deployment

Long-term innovation focus

Applying security to existing systems



statescoop

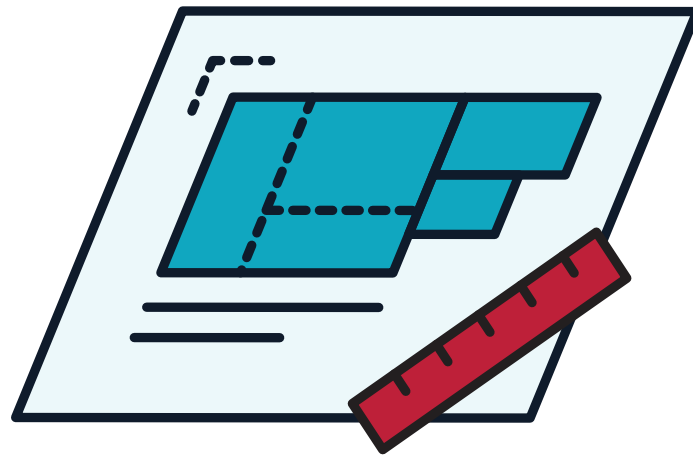
Smart Wi-Fi grid is like a Nest Thermostat for the entire city of San Leandro, California



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

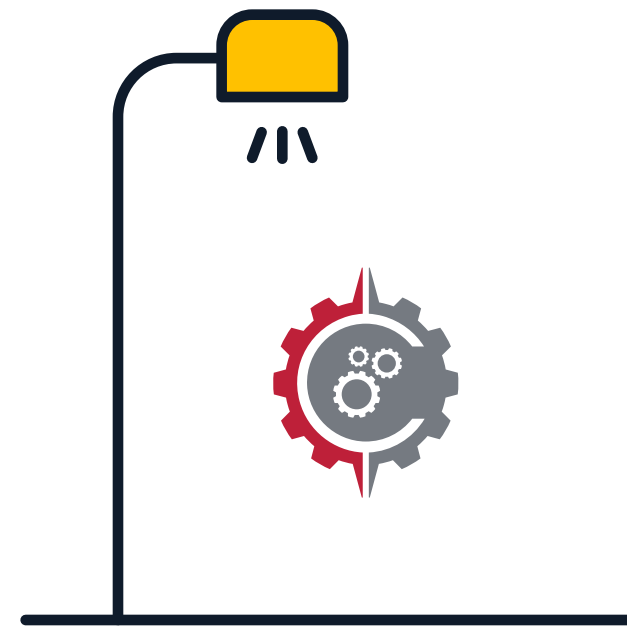


CryptoMove + San Leandro project



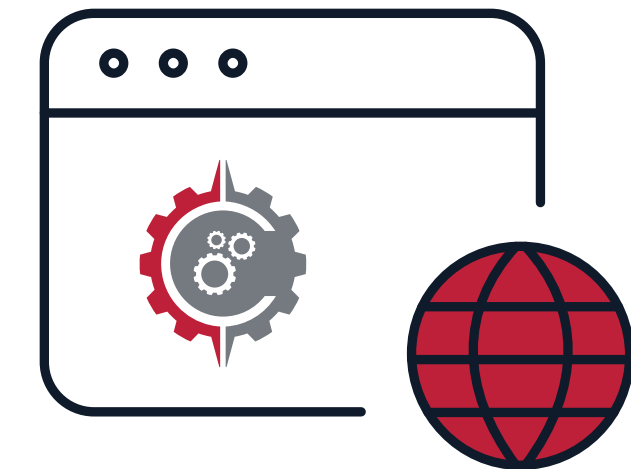
Threat model

Building reference architecture for cities worldwide



Smart lights protection

Keys & data



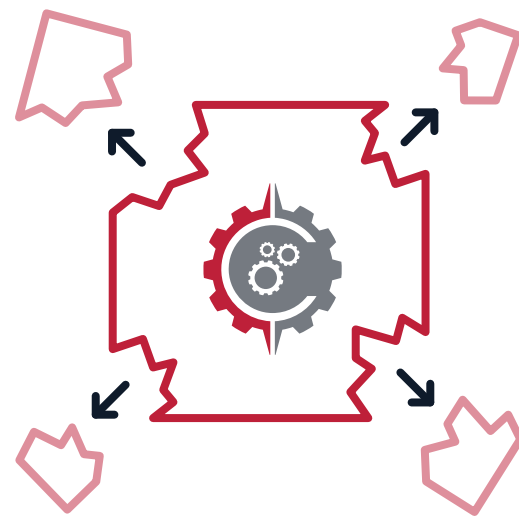
Enterprise data protection

Files, keys, & applications



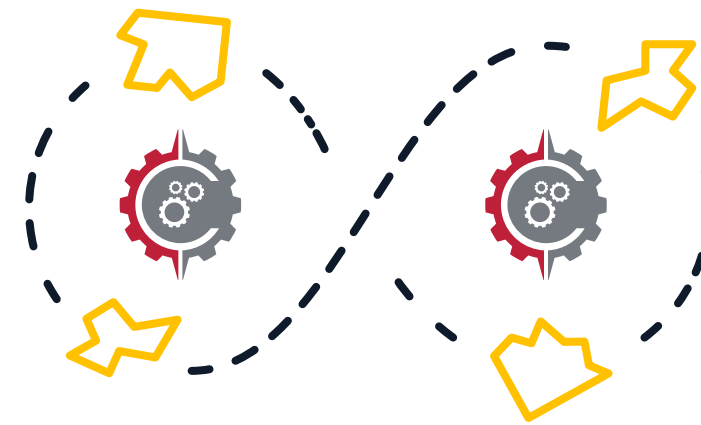
How it works

STEP 1



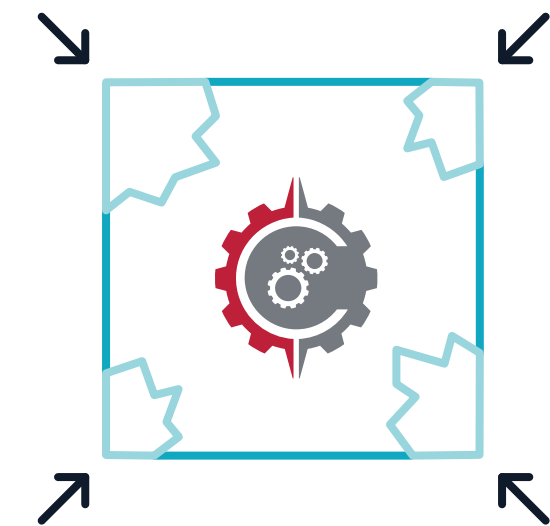
CryptoMove fragments, encrypts, and mutates your data.

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

The image displays several screenshots of the CryptoMove web application interface, illustrating its features and user experience.

Keys & Secrets Management: The interface shows a sidebar menu with options like Keys & Secrets, Files, Analytics, Share & Send, Databases, and CONFIGURATION. The main content area includes a 'Secret Protection' form for uploading secrets and a 'View Secrets' table listing secrets with columns for Name, Source, and Date saved.

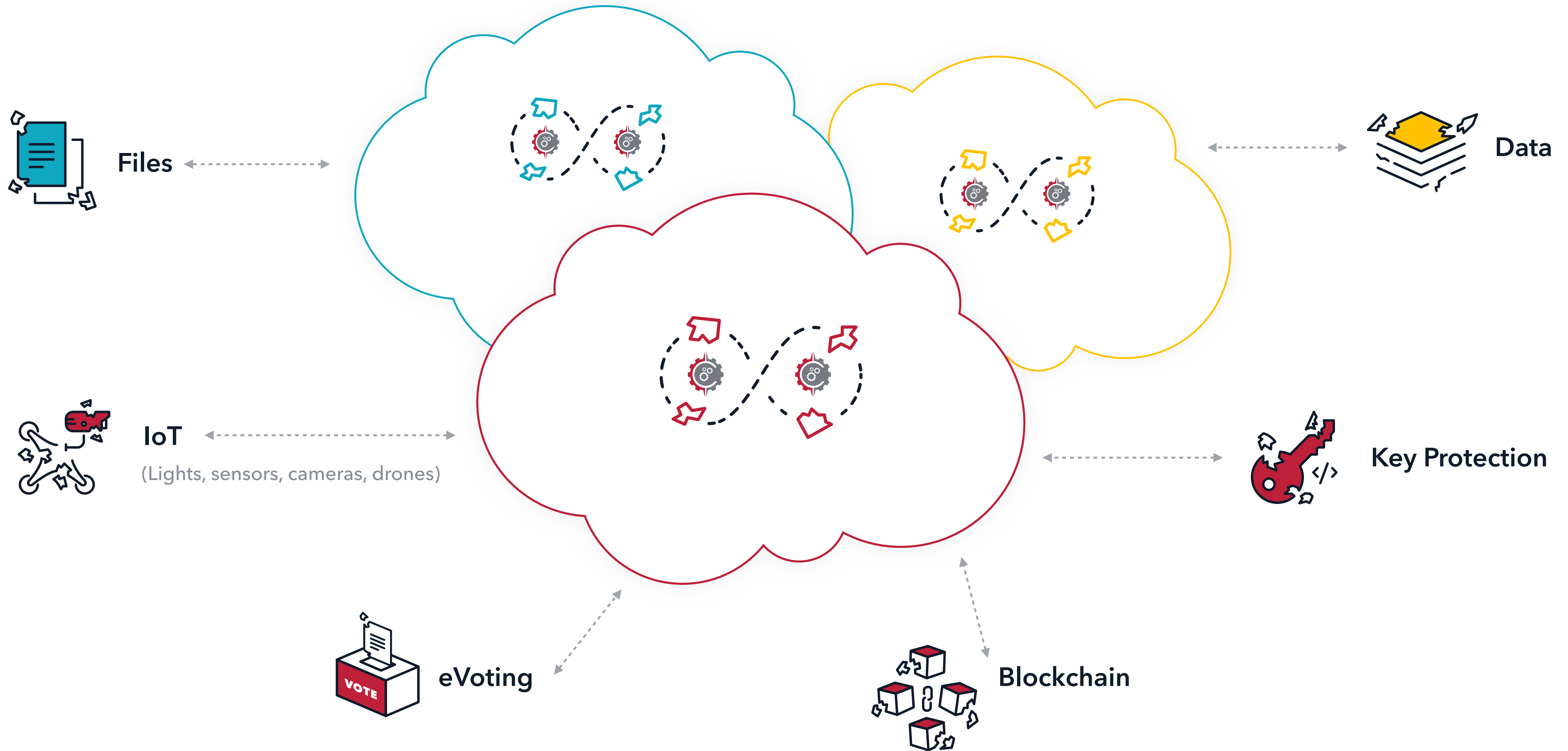
Data Protection: A 'Data Protection' overlay is shown, allowing users to protect data from their computer to CryptoMove. It offers options for key management: Transparent keys (CryptoMove transparently generates and manages keys), CM generated keys (CryptoMove generates a key for users to manage), and Bring your own key (Users generate, manage, and use their own keys). A progress indicator shows '25% complete'.

Advanced Features: The interface includes advanced options like Generating Keys, Splitting, Mutating, Encrypting, Padding, Generating Tracking Files, and Logging and Encrypting Log. A notification indicates that the CryptoMove client software is confirmed installed and configured, with a 'Select folders to protect' button.

API Integration: An 'Advanced - Embed API code snippet in your application' section provides code snippets for various actions: JavaScript, Python, Go, and Ruby. It also includes an API overview and a list of API commands: Upload Secret, View Secrets, Retrieve Secret, Delete Secret, Attribute - Secret, Attribute - Secret Name, and Attribute - APP ID.



Use cases





Case studies



DHS

Drones

Sensors

Cameras

FORTUNE
100

Fortune 100

Data Protection

Cloud

Key Vault