



Storage

Video remains on-premises, stored locally with AES 256 encryption.



Network

No open ports. Data transfer is secured via HTTPS encryption with TLS v1.2.

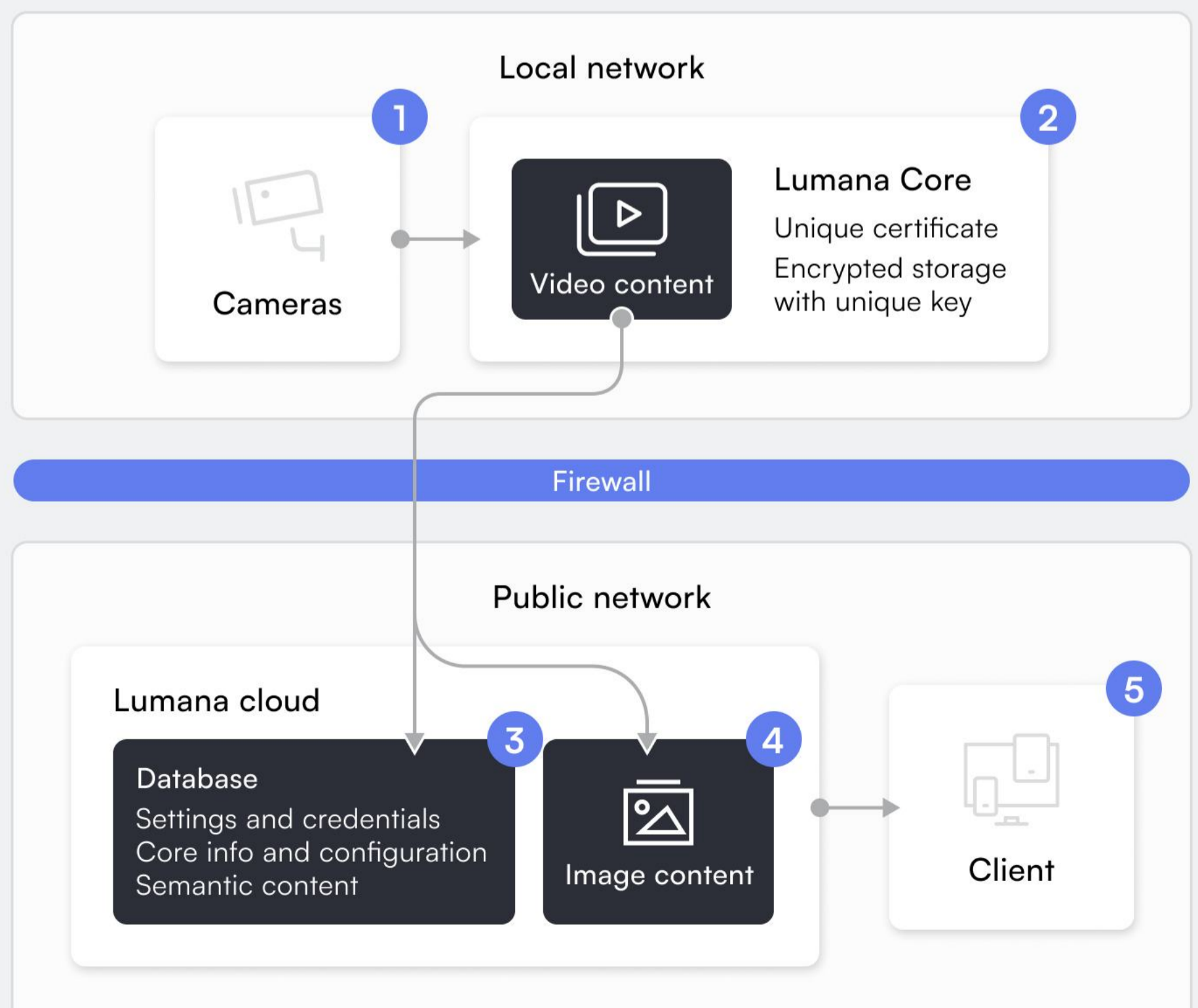


Cloud

Data is accessible and secured, in transit and at rest, with AES 256.

Visual content flow

- 1 Visual content is sent from the Camera to Lumana Core.
- 2 Video content is analyzed and securely stored on Core devices.
- 3 Semantic information (text) is sent to the Lumana Cloud.
- 4 Selected images are sent to the Cloud and stored in an encrypted format.
- 5 When alerted, visual content and semantic information is sent to verified clients.



Application security

Fortified APIs

Unique API keys ensure that only authenticated users gain access to Lumana.

Audit logs

Monitor usage and prevent unauthorized access or malicious activity.

Role-based access control

Grant appropriate levels of access with custom user permissions.

Vulnerability management

Stay ahead of threats with routine pen tests and automatic firmware updates.

Redundant cloud backup

Securely store video offsite and in the cloud for up to 365 days.

Enable external storage

Utilize external storage such as S3 compliance objects to extend backup retention.

Single sign-on

Streamline login and unify credentials across systems with SSO integrations.

Multi-factor authentication

Integrate with MFA solutions to prevent unauthorized external access.

Network security

No port-forwarding

No port forwarding is required, limiting your exposure to open ports, security risks, unauthorized access, and cyber attacks.

User identity authentication

System users are automatically authenticated via Okta, a leading Identity and Access Management (IAM) provider.

HTTPS in transit

All network traffic operates via HTTPS, guaranteeing encryption, authentication, and data integrity during transmission.

Independent local network

Lumana Core enables physical separation of your camera's local network from the internet, utilizing dual NIC configuration.