



cliO®

Smart
Gateway



Every Site

Gets An

AI Operation Never Clocks Out

Device uptime, recording & switch status | watched around the clock, all year long

ARISAN

/ Proactive 24/7 device-issue alerts / Compatible with all hardware
/ Deep analysis that hits the root cause

What Is CliO Smart Gateway? Why Do You Need It?

In monitoring deployments that span cities — or even countries — the real challenge was never installing cameras, but remotely connecting devices scattered across sites and brands into one unified system. The traditional approach demanded a public IP at every location and one-by-one integration with each vendor — costly, slow, and quick to stall as scale grew.

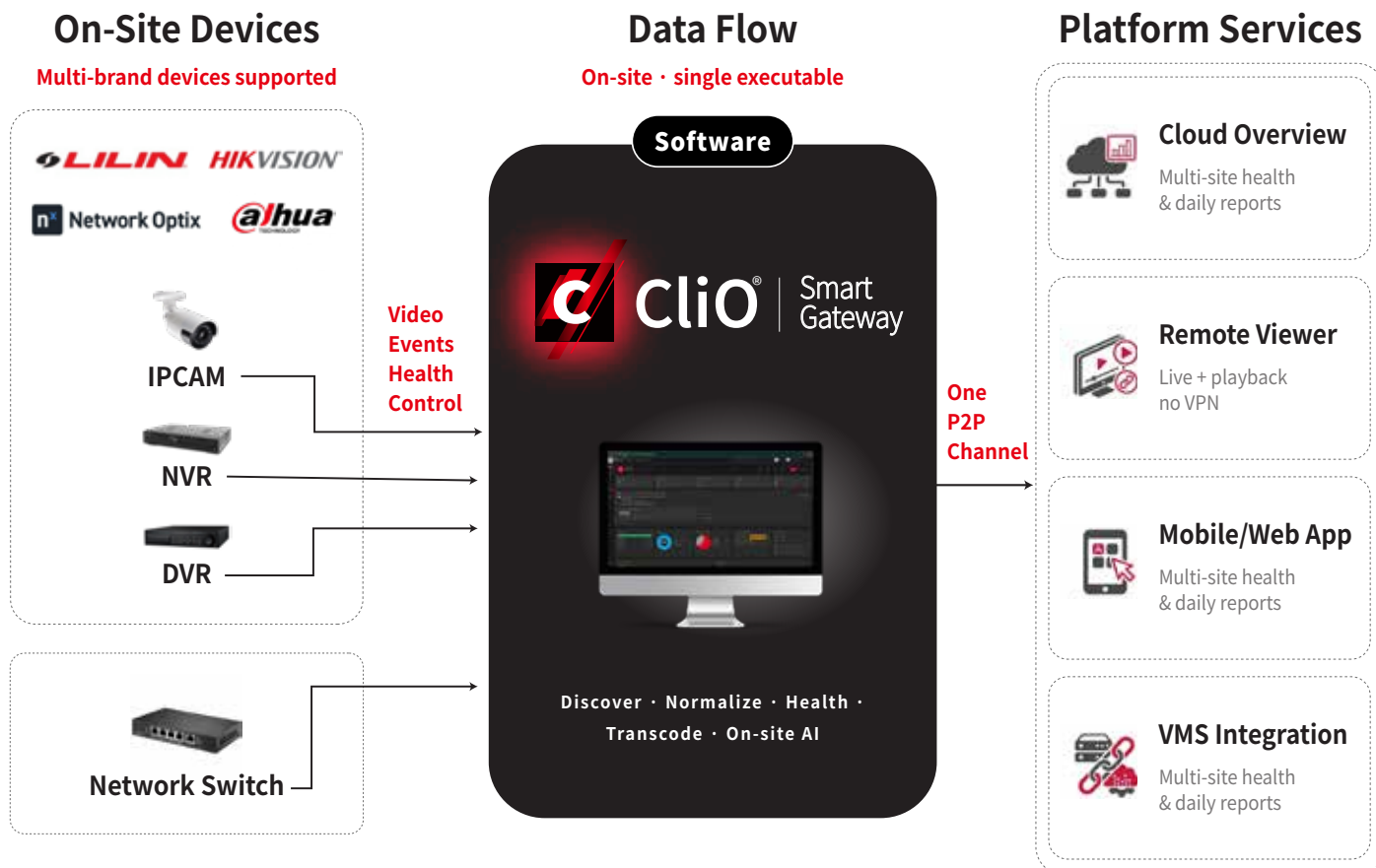
Smart Gateway was built to tear down both of these walls.

It is an edge video gateway placed at each site: on the local network it connects to IPCAM / NVR / DVR, normalizes every vendor's protocol into a single interface, then carries video, events, and device health to the cloud through one secure P2P channel.

It is more than a "view video remotely" tool — it is a complete layer of on-site video operations: from cross-brand integration and device health to daily AI reports, running on-site by default and scaling to the cloud when you need it.



Architecture



Core Features

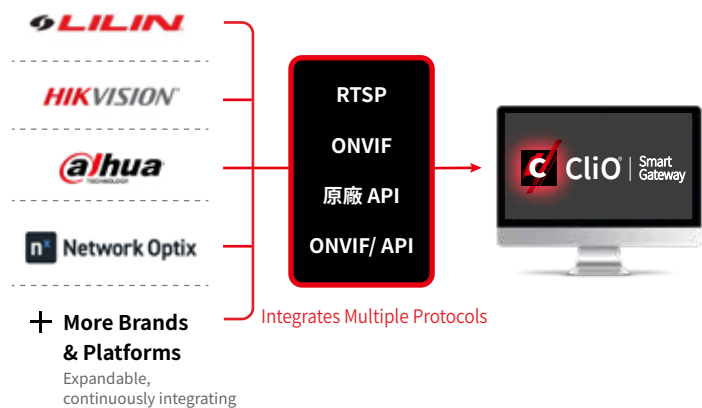


IPCAM / NVR / DVR mixed brands, unified into one interface

Cross-Brand Integration

Traditionally, connecting different-brand devices into one system meant building a separate integration for each vendor — time-consuming and hard to scale. At the site edge, Smart Gateway speaks every vendor's protocol — RTSP, ONVIF, native APIs — and normalizes them all into a single interface for the layer above, so mixed-brand sites are managed as one system.

- **Verified for Lilin / Hikvision / Nx / Dahua:** incl. NVR playback & disk health.
- **Mixed-brand sites:** IPCAM / NVR / DVR coexist as one
- **Vendor details handled internally:** RTSP, ONVIF, native APIs stay transparent.
- **Interface never changes:** adding brands later needs no upper-layer changes.

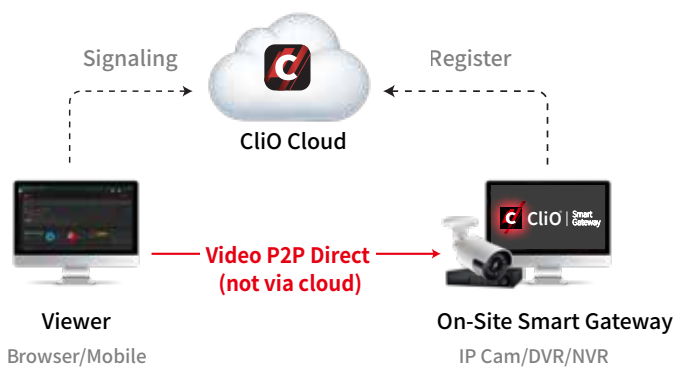


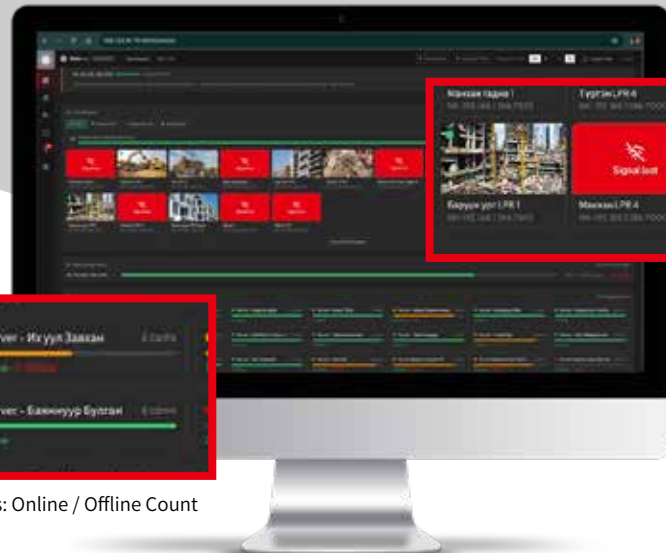
WebRTC peer-to-peer direct connect — no VPN, no extra cloud storage

P2P Live Video & Playback

Live viewing and recorded playback are monitoring's two most common tasks. Smart Gateway uses WebRTC peer-to-peer to stream live and recorded video directly between viewer and site — no extra cloud storage or per-channel recording license. It goes direct P2P when the network allows, and auto-falls back to relay when it can't, without interruption

- **P2P direct + auto relay:** switches automatically when blocked, no interruption.
- **UTC timeline playback:** seek, pause / resume, and speed control.
- **Gaps reported live:** recording gaps and end-of-stream flagged to viewer.





Online / Offline View



Devices: Online / Offline Count

Green / yellow / red at a glance; proactive alerts when something breaks

Device Health Monitoring

Smart Gateway already sits right beside every device, so health monitoring is almost effortless — and cross-brand by nature. It probes each camera and recorder on a short cycle, marks status in green / yellow / red, and watches whether storage and recording are healthy — so you know which unit needs attention before trouble hits, not after.

- **Online / offline at a glance:** green/yellow/red, dropouts flagged instantly.
- **Storage & recording health:** free space, full-disk, coverage, and gaps.
- **Retention audit:** how many days of recording remain, reviewed regularly.
- **Multi-device overview:** dozens of units on one screen, no unit-by-unit checks.

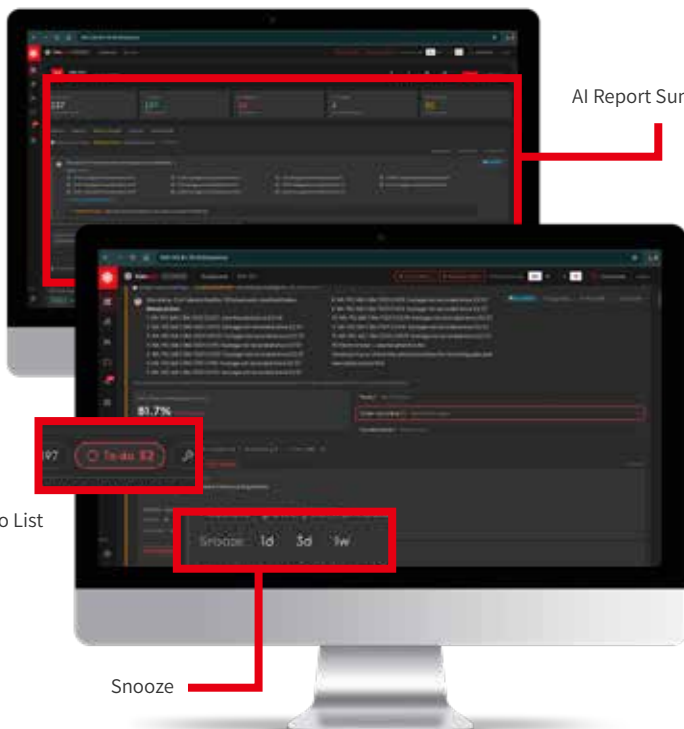


Daily per-device scored report; raw footage never leaves the site

Daily AI Video Check + Report

About every 30 minutes, Smart Gateway checks each camera's image for problems, then compiles a daily per-device scored report. Detection runs locally on-site and only reports structured findings — raw footage is never uploaded. Rules make the judgment, cameras are the eyes, and AI just writes the results in plain language.

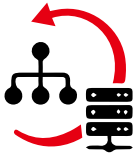
- **Five image faults:** blur, occlusion, freeze, over/under-exposure, view shift.
- **Auto-flags anomalies:** zero detections where people/cars usually appear; gapped recordings.
- **Per-device scored report:** one a day — what's fine, what needs action.
- **Footage stays on-site:** only structured findings sent, never raw video.



AI Report Summary

To-Do List

Snooze

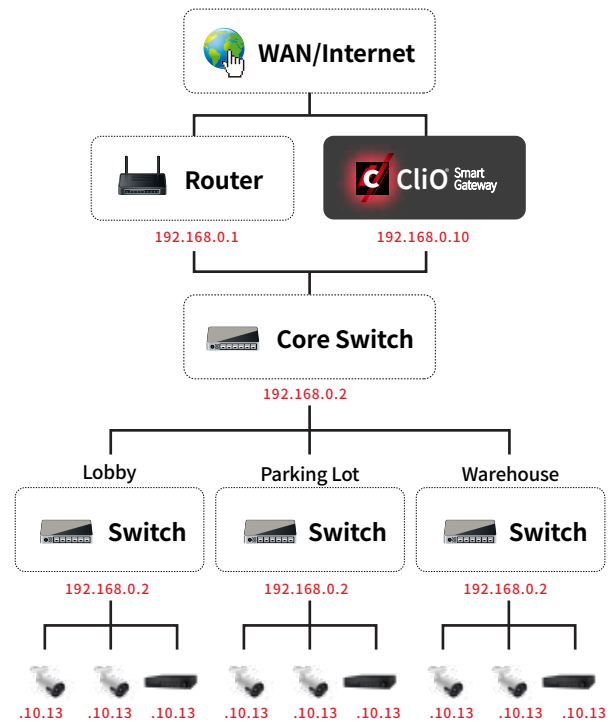


Auto-discovers and maps your entire reachability network

Automatic Network Topology Scan

Plug in Smart Gateway and it automatically discovers every device on the network — cameras, recorders, and switches — and draws a reachability map. No manual IP entry, no SSH; vendors are auto-identified, with one-click rescan when needed, so you always know what the site's network looks like.

- **Auto-discover devices:** cameras, NVRs, switches all found.
- **Reachability map:** no manual IP, no SSH, vendors auto-identified.
- **One-click rescan:** update topology whenever the site changes.
- **Full port mapping:** with SNMP, managed switches show physical links.

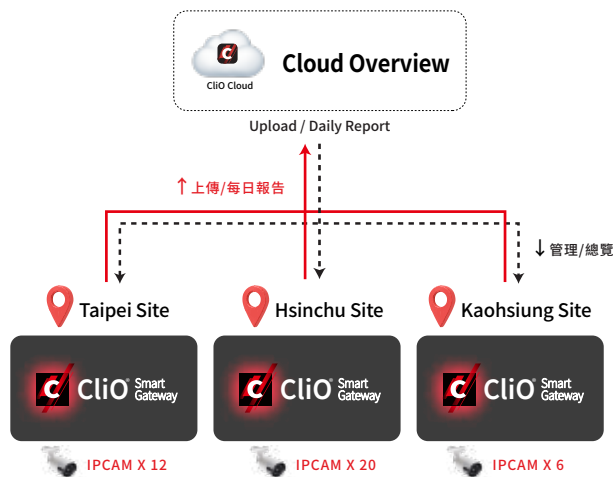


One overview across sites; runs standalone even offline

Cloud Management · One Multi-Site Overview

A single Smart Gateway can run entirely on-site; when you manage more than one location, the online platform consolidates every Gateway into a single device overview, with no changes needed at the site. Cross-site health roll-ups show at a glance which site is flashing red — then drill into any device, with remote access that needs no VPN.

- **Multi-site device overview:** manage Gateways across sites on one screen.
- **Cross-site health roll-up:** spot which site is red at a glance.
- **VPN-free remote access:** reach any site via cloud relay.



Use Cases

1 Cross-Border Retail Chain

One box unifies mixed brands — see every store from one phone

Pain point: A retail chain spanning three countries and 40 stores, each with monitoring devices from different brands and different network environments. HQ wanted live view of any store at any time but had no single entry point; worse, a broken or non-recording camera was usually discovered only when footage was needed after an incident — blind spots and gaps caught no one's eye in advance.

Solution: Without replacing existing gear, place one Smart Gateway per store to integrate all brands locally, then carry video and device health to the cloud over a single P2P channel. This lets HQ:

See every store on one phone: mixed brands and locations on one screen, no per-site login.

Proactive fault alerts: instant alarms on camera offline or image anomaly, no on-site patrols.

Keep existing gear: adopt without swapping hardware — low cost, fast rollout.



2 Security Firm Managing Multiple Sites

One secure channel into every client site

Pain point: A security company manages dozens of client sites, each with different device brands, networks, and permissions. Opening a public IP or firewall port at every site is both cumbersome and a security risk; knowing in real time which site has a problem is even harder.

Solution: Place one Smart Gateway per site, connect in via encrypted relay with no port-opening, and consolidate all sites' device health. On-duty staff can then:

No VPN, no open ports: leave client firewalls untouched, lowering security risk.

Cross-site health overview: spot the red site at a glance, then drill in.

Daily report accountability: explain device status to clients with structured reports.



3 Industrial Parks / Logistics

However vast the site, no recording gap slips through

Pain point: Industrial parks and logistics centers are vast with many cameras, and recordings often hide invisible gaps; when an incident needs footage, you find a stretch was never recorded. With varied on-site network conditions, the traditional all-to-cloud approach strains both bandwidth and stability.

Solution: Place one Smart Gateway per park; audit device health and recording coverage regularly, with AI daily inspection proactively flagging image anomalies — and data stays in-plant, running even when the network drops. This lets managers:

Recording-coverage audit: gaps reported regularly, no more after-the-fact surprises.

AI daily inspection: blur, occlusion, and view shift auto-flagged.

Runs offline: keeps monitoring when the network drops, data stays in-plant.



Compared with a Typical Gateway

Capability	Typical Gateway	CliO Smart Gateway
Connect to sites from cloud	✗ Public IP per site / P2P per vendor	✓ One Smart Gateway, one P2P per site
Keep your existing gear	✗ Often full replacement	✓ Reuse existing gear, any brand
Playback storage	✗ Extra cloud storage / license	✓ Reads the device's own disk directly
Multi-brand on one screen	✗ Usually single-vendor	✓ Mixed brands, unified
Device health & daily report	✗ Live video only	✓ Health, storage & AI report
Where AI runs	✗ Uploads video to cloud	✓ On-site; footage never leave
Can run offline	✗ Depends on cloud	✓ Runs standalone

Q&A

Q: Which brands/devices are supported? Does mixed-brand work?

Yes. Smart Gateway natively supports four major brands — Lilin, Hikvision, Dahua, and NX Witness (Network Optix) — covering IPCAM, NVR, DVR, and network switches, with the list always expanding. For other brands on your site, just provide the device's remote access and integration docs and we integrate it remotely, free. On-site it normalizes each vendor's protocols (RTSP, ONVIF, native API) into one interface — mixed brands and models managed together; video is converted to standard WebRTC for the browser, so you needn't learn a separate tool per vendor.

Q: Do I need to replace my cameras or recorders? Is rollout a hassle?

No replacement. Smart Gateway is an edge video gateway placed on-site; once on the LAN it auto-discovers every camera, recorder, and switch and draws a reachability map — no manual IP, no per-unit setup. It coexists with existing gear, reuses your disks and recordings — low cost, fast rollout; one-click rescan updates the topology when the site changes.

Q: What does the daily AI video check actually look for? Won't it flag false alarms constantly?

About every 30 minutes it checks each camera against explainable threshold rules for five common faults: blur, occlusion, freeze, over/under-exposure, and view shift from a moved camera. The logic is deterministic (not a black box), with buffering against flag delay and brief jitter to reduce false alarms. Each day it compiles a per-device scored report — what's fine, what needs action — written as easy-to-read handover notes in both Chinese and English.

Q: Where are recordings stored? Do I buy extra cloud storage or licenses?

No. Playback reads the device's own disk (NVR / camera SD card) directly — no forced move to the cloud, no per-channel cloud-recording license. It also audits recording coverage and retention regularly, proactively flagging "should-have-recorded but didn't" gaps, so you know before an incident which stretch wasn't captured — not when you go to pull the footage.

Specifications

	Entry	Standard	GPU Model
Hardware	4-core · no GPU · 4GB	8-core · iGPU · 8GB	10-core · dGPU · 16GB
Devices monitored	Hundreds	Hundreds	Hundreds
Concurrent streams	~2-4	~12-24	~30+
On-site AI (option)	+4 GB	+4 GB	+4 GB

On-demand 隨選串流:相機串流只有在有人點開觀看時才啟動,閒置約 10 分鐘後自動釋放 — 沒人看的相機完全不耗資源。支援 Linux x86/ARM/Windows/macOS。

Agent/Reseller	Headquarters  +886-2-2767-0367 info@arisan.io Rm.701, 7F No.205 Sec 1 Dunhua S Rd Daan Dist Taipei City 106 Taiwan
----------------	--