P2P cloud vs port forwarding vs VPN: which way to view cameras remotely

There are three common ways to reach a camera system from outside the building. They differ in setup effort, what breaks them, and how much of your network they expose. Here is how to choose.

Networking · Published 2026-10-25 · Online version: vuepointsecure.com/support/p2p-cloud-vs-port-forwarding-vs-vpn-for-remote-viewing

Your recorder sits behind a router that, by default, blocks every connection that starts on the internet. Remote viewing means getting through that router somehow. Each method does it differently, and the difference matters for security.

The three methods in one paragraph each

- **P2P / cloud app.** The recorder makes an outbound connection to the manufacturer's servers and registers itself by serial number or UID. Your phone app finds it through those servers. Nothing inbound is opened on your router. Examples: Hik-Connect, the Reolink App's UID connection, Amcrest View Pro.
- **Port forwarding.** You tell the router to pass specific inbound ports to the recorder, then connect directly to your public IP. Works with any client that supports direct IP. Every forwarded port is reachable by anyone on the internet.
- **VPN.** Your phone or laptop joins the site's network through an encrypted tunnel (to a VPN server on the router, a firewall, or a small dedicated box). Once connected you use the recorder's local IP as if you were in the building. Nothing on the recorder is exposed.

	P2P / cloud app	Port forwarding	VPN
Setup effort	Low: scan a QR code or enter serial	Medium: router rules, DDNS, fixed IP	Medium to high: VPN server plus client on each device
Inbound ports open	None	One or more, to the recorder	One, to the VPN server only (or none with some hosted VPN services)
Works behind carrier-grade NAT	Yes	No	Only with a hosted/relay VPN service
Depends on vendor servers	Yes	No	No
Exposure if recorder has a flaw	Lower: no direct inbound path	Highest: recorder faces the internet	Lowest: attacker must get through the VPN first
Third-party software access (VMS, RTSP)	Usually no	Yes	Yes
Best for	Owners viewing on a phone	Legacy systems with no alternative	Admins, multi-site, anything sensitive

Side by side.

What breaks each method

- **P2P:** the vendor ends cloud support for older models, the cloud service has an outage, or a firewall blocks outbound UDP. Reolink, for example, notes that UID access uses random UDP ports, so the router must allow outbound UDP.
- **Port forwarding:** carrier-grade NAT on cellular or some fixed-wireless service, a changed public IP without DDNS, the recorder's internal IP changing, or the ISP blocking common ports.
- **VPN:** the VPN server's own public address changes, the client app is not installed on the phone that needs it, or the site and home networks use the same subnet (both 192.168.1.x), which confuses routing.

How to choose

1. **Start with the vendor's app**
   If the recorder supports it and you only need to view on phones, use P2P. It is the lowest-effort option with no inbound ports. Keep firmware current and use a strong password on the cloud account and the device.

2. **Use a VPN when you need more than viewing**
   Configuration, third-party VMS access, multi-site management or anything where the recorder's web interface is involved should go over a VPN. Many business routers and firewalls include a VPN server.

3. **Use port forwarding only when the other two are not possible**
   If you must, forward only the client/app port, never the admin web port unless essential, and follow every step in how to set up port forwarding.

4. **Check whether you are behind CGNAT before deciding**
   If the router's WAN address is in 100.64.0.0 to 100.127.255.255, or is a private address, port forwarding and self-hosted VPN will not work without help from the ISP. P2P or a hosted connection is the practical route.

> **If a monitoring company needs access**
> A professional monitoring service needs reliable, continuous access to your cameras, not a phone app. VuePoint's edge device sits on your network, connects outbound, and links your existing cameras and recorder to our monitoring platform without any port forwarding.

Frequently asked questions

Is P2P safe?

It avoids exposing the recorder to inbound internet traffic, which removes the most common attack path. You are trusting the manufacturer's cloud, so use a strong unique password, enable two-factor authentication on the account if offered, and keep firmware updated.

Why is P2P video slower than on site?

P2P connections sometimes fall back to relaying video through the vendor's servers, and they are limited by the site's upload speed. Viewing the sub-stream on a phone is normal and expected. See how much upload bandwidth security cameras need.

Related guides

- How to set up port forwarding for a camera or NVR — vuepointsecure.com/support/how-to-set-up-port-forwarding-for-a-camera-recorder
- How to secure a camera system — vuepointsecure.com/support/how-to-secure-a-camera-system-passwords-firmware-and-exposure
- How much upload bandwidth do security cameras need? — vuepointsecure.com/support/how-much-upload-bandwidth-do-security-cameras-need
- How to set up DDNS for a camera recorder — vuepointsecure.com/support/how-to-set-up-ddns-for-a-camera-recorder
- All support articles — vuepointsecure.com/support

Need help with a site? Call (888) 203-2260 or visit vuepointsecure.com/contact. Menu names and defaults vary by model and firmware; check your device's documentation.