VisionOn Cloud Connect unit

The VisionOn Systems **Cloud Connect** unit transforms any networkable ONVIF DVR or NVR into a Cloud Connected remotely viewable device. (Not sure give us a call on **03302234724** and we can sort this out for you)

The unit comes in two formats:

1. Where no current broadband connection is available the unit is delivered with a 4G 450GB Per month mobile data connection. (as shown above)
2. Where the client has a broadband connection available then the unit comes with two ethernet ports, one for connecting the device and one for connecting to the client's router.

These systems are designed to create a secure VPN tunnel into the remote device and allow the operator to use the system as if they were sat there in front of it.

Additionally, the system can be configured to enable Cloud recording and live view of up to five selectable cameras and these can then be accessed via and web enabled device, such as a PC, Laptop, Tablet or Mobile Phone.

You can buy the unit outright and pay a monthly subscription for the data and cloud services, or rent it on a month-by-month all-inclusive basis (No long-term commitment)

Other Applications

In addition to be used to remotely enable DVR & NVR products or event up to 5 standalone IP camera, the unit can be used in domestic abuse cases, where the victim is being pestered or abused by a 3rd Party who is not resident at the premises. The camera(s) can be installed inside the front door and set up with an internal, Audio enabled covert camera which will record any activity at or near the front door.

Specifications

Security:

All communication between your Cloud Connect unit and the Cloud is done via a VPN with SSLv3 certificates using 4096-byte sized keys, each connection is challenged to reauthorised once a week. Each certificate can be revoked if we detect a unit has been cloned or detect any suspicious traffic. All communication is encoded into ‘msg packs’ using tokens and sent through a secure MQTT message broker. These safeguards protect against MITM (man in the middle) attacks, MAC spoofing and other types of attack.

All access is done either via an API (e.g., control rooms or CMS applications) or using a web browser (HTTPS). The application has many safeguards against many types of attacks, including Cross-Site Request Forgery (CSRFs), Self-contained XSS, Brute Force, Account Hi-Jacking and many other types of attacks.

Every single request goes through two layers of auth and auth (authentication and authorisation) which includes a full audit log of all access and changes. Even a single snapshot from a camera is susceptible to this security. No access or changes are possible without going through these layers. The audit log part of the system also geolocates every request, discovers details such as what is the Internet Service Provider of the person accessing, what hardware they are using, what software they are using (for example, an iPhone 11 Pro using Safari from a BT connection in London, England). Using this information, the system can make intelligent decisions when any access is deemed “suspicious” e.g., access from a new city. When using intelligent local streaming, temporary tokens are generated for each accessing user to pull live and recorded events directly from the Unit.

Power:

The cloud connect unit can simply be plugged into any UK 3 pin mains socket and draws a maximum of 60 Watts power. The system is internally earthed and produces a maximum output voltage of 48v DC.

Where required the system can be hardwired into a suitable fused spur or similar.

The unit does not power the DVR or NVR but can independently power up to 2 IP PoE cameras that comply with PoE: 802.3af, class 3, in addition to the DVR or NVR.

Connection:

MOBILE:

Mobile module	4G (LTE) – Cat 4 up to 150 Mbps, 3G – Up to 42 Mbps, 2G – Up to 236.8 kbps
Status	Signal strength (RSSI), SINR, RSRP, RSRQ, EC/IO, RSCP, Bytes sent/received, connected band, IMSI, ICCID
SMS	SMS status, SMS configuration, send/read SMS via HTTP POST/GET, EMAIL to SMS, SMS to EMAIL, SMS to HTTP, SMS to SMS, scheduled SMS, SMS autoreply, SMPP
Black/Whitelist	Operator black/whitelist
Band management	Band lock, Used band status display
APN	Auto APN
Bridge	Direct connection (bridge) between mobile ISP and device on LAN
Passthrough	Router assigns its mobile WAN IP address to another device on LAN
Multiple PDN (optional)	Possibility to use different PDNs for multiple network access and services (not available in standard FW)

ETHERNET LAN 5 x LAN ports, 10/100/1000 Mbps, compliance with IEEE 802.3, IEEE 802.3u, 802.3az standards, supports auto MDI/MDIX crossover