

PRODUCT OVERVIEW

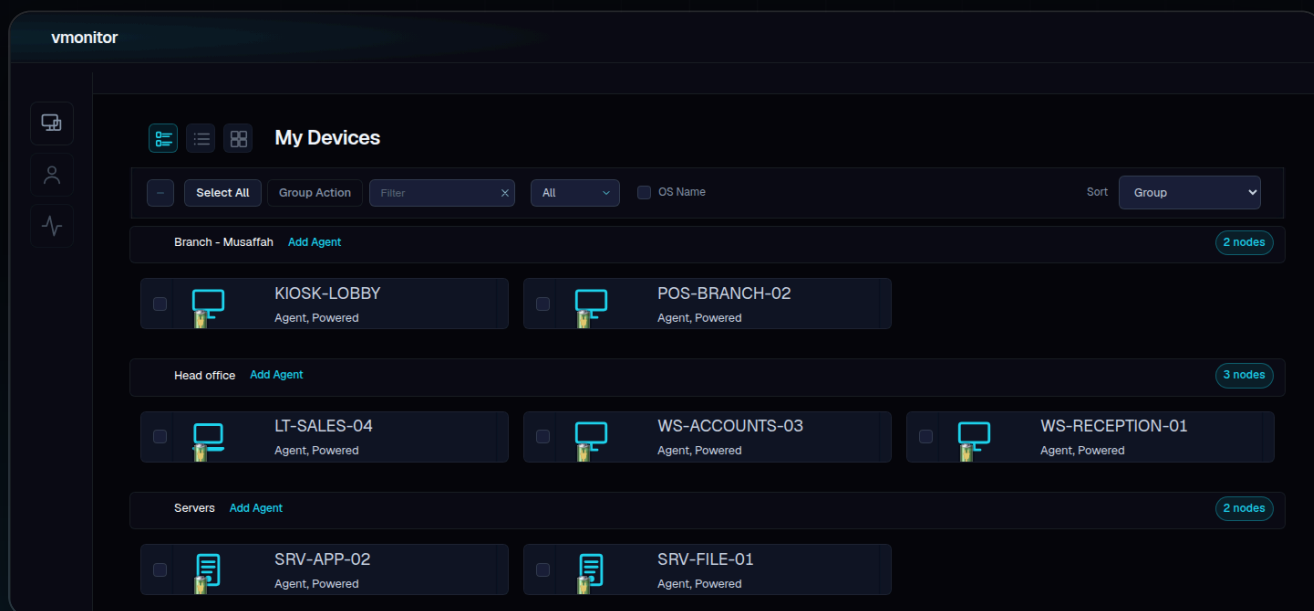
Your entire fleet. One console.

vmonitor is a hosted remote monitoring and management platform for IT teams and managed service providers. Remote desktop, terminal and file access to every device you look after — from any browser, with no server for you to run.

7-day free trial · no card

Windows · macOS · Linux · BSD · Android

Hosted & supported by Future Vision



WHAT IT IS

One place to reach every machine you are responsible for.

A small agent runs on each managed device — a workstation, a server, a kiosk, a laptop on a customer site. It dials out to vmonitor over an encrypted connection and stays there. From that moment the device is in your console: you can see it, control its screen, open a shell on it, move files to and from it, power it on or off, and read its hardware and software inventory. Nothing else has to be installed, opened or configured.

vmonitor is delivered as a service. Future Vision runs, patches and backs up the platform; you sign up, enrol devices, and work. There is no server to provision, no upgrade window to plan, and no second tool for the technician to install — the console is a web page.

50	13+	1 min	TLS
Devices included in every plan	OS platforms and architectures	From agent install to full control	Encrypted device–server–browser

THE PROBLEM IT REMOVES

What support costs today, and what it costs with vmonitor.

WITHOUT A REMOTE PLATFORM	WITH VMONITOR
A technician drives to the site for a ten-minute fix.	The fix happens from the desk, in the time it takes to open a tab.
Remote access means firewall exceptions, port forwards or a VPN account per site.	Agents connect outbound only. NAT, LTE and guest networks are not obstacles.
Screen-sharing tools need the end user present to accept a session.	Unattended access — work on servers and empty desks at night.
One tool for desktop, another for terminal, another for file transfer.	Desktop, shell, files, power and inventory in one console.
No record of who connected to which machine, or what they did.	Every session is authenticated, permission-checked, logged and recordable.

Why teams put their fleet on vmonitor.

The value is measured in journeys not made, tickets closed on first contact, and access your security team can defend.



Site visits become the exception

Most incidents are software, not hardware. Handle them from the console and the travel time, the fuel and the scheduling disappear from the ticket.



Faster resolution, fewer hand-offs

Desktop, shell and files are one click from the device row. No waiting for the user to be free, no walking someone through a menu on the phone.



No holes in the network

Nothing is exposed inbound. Devices behind NAT, on a customer's guest Wi-Fi or on a mobile connection are reachable with no change to their network.



Nothing to run or maintain

The platform is hosted and kept current by Future Vision. No server to size, no database to back up, no patch night — and no per-technician client software.



Access your auditors accept

Rights are granted per user and per device group. Every session is attributable, logged, and can be recorded — the evidence exists before anyone asks for it.



One predictable line item

A single plan with every feature, 50 devices included and no charge per technician or per session. Start on a seven-day trial with no card.

Who it is for. Internal IT teams supporting staff across offices, floors and home desks; managed service providers looking after devices in many customer sites; and any operation with unattended machines — kiosks, signage, POS terminals, remote servers — that must be reachable without sending someone to stand in front of them.

Everything between you and the device, removed.

The full capability set, grouped by what you do with it.

Access and control

- **Remote desktop (KVM)** — full mouse and keyboard control in the browser, multi-monitor aware.
- **Web terminal** — a real PowerShell, bash or sh shell on the device, no SSH keys to manage.
- **Multi-device view** — watch many desktops at once and jump into any of them.
- **Session recording** — capture a remote session for training, dispute or audit.
- **Clipboard and file transfer** — copy text and drop files straight into a live session.
- **File manager** — browse, upload, download, rename and delete on the remote file system.
- **Group actions** — push the same command or file to a whole device group.
- **Unattended access** — no end user has to be present or accept a prompt.

Power and out-of-band

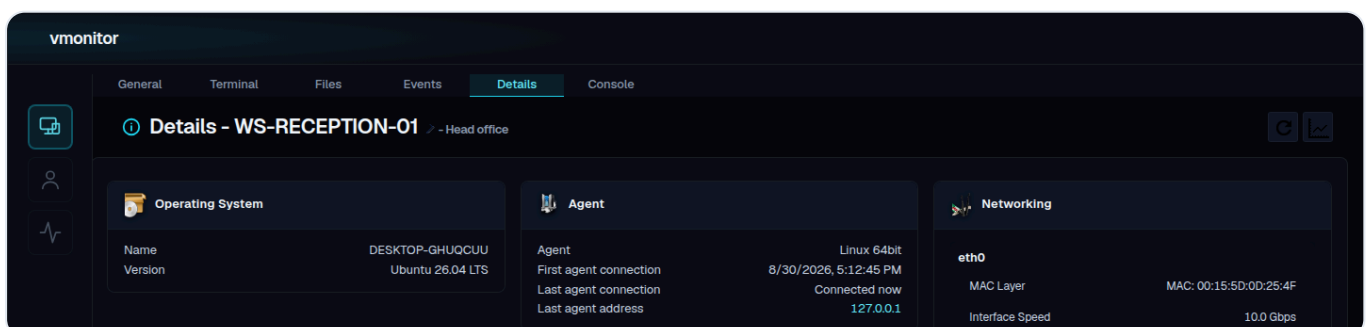
- **Wake-on-LAN** — start a sleeping machine through any online agent on the same network.
- **Intel AMT** — KVM, power and boot control below the operating system.
- **Power control** — shut down, restart, sleep or reset a device from the console.
- **Reach the unreachable** — machines powered off, crashed or mid-reinstall stay in range.

Visibility and monitoring

- **Live presence** — online, offline and idle state for the whole fleet at a glance.
- **Software inventory** — what is installed on each device, and which version.
- **Alerts** — email or messenger notification when devices connect, drop or change.
- **Hardware inventory** — CPU, memory, disks, network adapters, BIOS and serial numbers.
- **Event log per device** — connections, sessions, power events and errors in one stream.
- **Notes and tags** — record what a machine is, where it sits and who owns it.

Organisation and access control

- **Device groups** — unlimited groups, one per customer, site, floor or role.
- **User groups** — give a whole team the same rights in one move.
- **Two-factor authentication** — TOTP apps or FIDO2/WebAuthn hardware keys, enforceable for all users.
- **Granular rights** — view-only, desktop, terminal, files, power, granted per user and per group.
- **One-line installers** — generate a per-platform enrolment command or link from the console.
- **Audit log** — who connected to which device, when, from where, and what was done.



Running in an afternoon, not a quarter.

Three steps from a signup form to full control of a device.

01

Create your account

Sign up with an email address and you are in the console within a minute. Nothing to install, no server to provision, no card for the trial.

vmonitor.ae → free trial

02

Enrol devices

Generate a one-line installer per platform from the console and run it on the device. Agents connect outbound — no inbound ports, no VPN.

windows · macos · linux · bsd

03

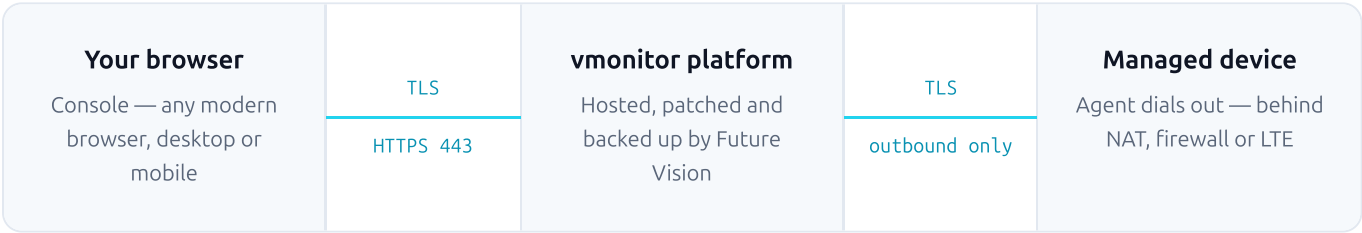
Take control

Devices appear in the console within a minute of install. Open desktop, terminal or files for any of them, from any browser, anywhere.

desktop · terminal · files

ARCHITECTURE

Two outbound connections, and nothing exposed.



The managed device never listens for an incoming connection: the agent opens a single encrypted WebSocket to the platform and keeps it alive. That is why enrolment needs no firewall rule, no port forward and no VPN, and why a laptop works the same in the office, at home or on a phone hotspot.

SUPPORTED PLATFORMS

PLATFORM	COVERAGE
Windows	Desktop and Server editions, 32-bit and 64-bit, installed as a service
macOS	Intel and Apple Silicon
Linux	x86, x86-64, ARM (including single-board devices) and MIPS
FreeBSD	x86-64
Android	Agent app for tablets and handsets
Intel AMT	Out-of-band control with no agent running on the machine at all

Remote access your security team can sign off on.

Remote control is a powerful right. vmonitor treats it as one — authenticated, scoped, encrypted and recorded.



Encrypted end to end

TLS on every hop — browser to platform, platform to agent. Agents authenticate with certificate hashes rather than a shared password, so a stolen installer string is not a stolen device.



Strong authentication

TOTP two-factor and FIDO2/WebAuthn hardware keys for console accounts, with lockout policies on repeated failures. Two-factor can be required for every user in the account.



Least privilege by design

Rights are assigned per user and per device group and can stop at view-only. A technician sees the customers they support and holds only the powers their role needs.



Accountable by design

Sign-ins, connections and administrative changes are written to an audit log, and remote sessions can be recorded — so an incident review has evidence rather than recollection.

AUDIT STREAM — EXAMPLE

AUDIT STREAM — LIVE

● CONNECTED

```
12:03:41  agent connect — WS-FRONT-04 (cert verified)
12:03:42  tls 1.3 channel established
12:05:10  auth ok — admin@fv (totp + webauthn)
12:05:33  desktop session → WS-FRONT-04 (recorded)
12:18:02  session closed — audit entry #84122 written
```

Operated by one team. vmonitor is designed, built, hosted and supported by Future Vision. Deployment, updates and support come from the people who wrote the software — there is no third-party vendor between you and a fix.

PLANS

One plan. Every feature.

Start with seven days free and no card. Subscribe from inside the console when the trial ends and keep every device and group exactly where it is.

MONTHLY

AED 375

per month · excl. 5% VAT

Cancel any time from the console.

YEARLY

BEST VALUE

AED 3,750

per year · excl. 5% VAT

Two months free compared with paying monthly.

INCLUDED IN EVERY PLAN

- ✓ Up to 50 managed devices
- ✓ Remote desktop, terminal and file access
- ✓ Wake-on-LAN and power control
- ✓ Two-factor authentication
- ✓ Session audit log and recordings
- ✓ Unlimited device groups
- ✓ Multi-device view and group actions
- ✓ Hardware and software inventory
- ✓ Per-user, per-group permissions
- ✓ Support from the team that builds it

COMMON QUESTIONS

Do devices need open ports or a VPN?

No. Agents make one outbound encrypted connection, so devices behind NAT, a firewall or a mobile connection work with no network change.

What happens after the trial?

Subscribe from inside the console and the same account, devices and groups carry on. Without a subscription the account stays, but device access stops.

Do we have to run a server?

No. vmonitor is hosted, patched and backed up by Future Vision — you sign up, enrol devices and use the console in a browser.

Can we control what each technician can do?

Yes. Rights are set per user and per device group — view-only, desktop, terminal, files or power — and every session is logged.

Start your seven-day trial

Sign up, enrol a device and control it before the kettle boils. No card, no call, no installation on your side.

CONSOLE & SIGNUP

vmonitor.ae

WHATSAPP

+971 50 350 0766

PHONE

+971 2 6327 566

EMAIL

info@thefuturevision.com

COMPANY

Future Vision · Abu Dhabi, UAE