Replacing Permanent Vendor VPNs with Controlled OT Access

Why Permanent Vendor VPNs Are a Risk

For years, industrial organisations gave external vendors a VPN account that stayed active around the clock. The reasoning was simple: the vendor needed to reach the OT network whenever a machine broke down or a controller needed a firmware update. A permanent connection eliminated the back-and-forth of requesting credentials every time. But that convenience came at a cost. A VPN tunnel that never closes is a door that never locks. If an attacker compromises a vendor's laptop or steals their credentials, they can move laterally into the OT network at any hour, often without anyone noticing until damage is done.

The shift toward controlled OT access replaces that always-on model with a system where each session is requested, approved, and monitored. The goal is not to block vendors from doing their work. It is to give them exactly the access they need, exactly when they need it, and nothing more. This article walks through the steps to make that change without disrupting operations or alienating the vendors who keep your plant running.

Step 1: Inventory Every Vendor Connection

Before you can replace anything, you need to know what currently exists. Start by listing every vendor that has a VPN account into your OT environment. For each one, record the purpose of the connection: which PLCs, RTUs, or engineering workstations they touch, how often they connect, and what protocols they use (Modbus, DNP3, proprietary SCADA protocols, etc.). Also note whether the account is shared among multiple people at the vendor or assigned to a single engineer.

Watch out for "ghost accounts" that were created for a one-time project years ago and never removed. These are common in OT environments where change management is slow. A vendor who no longer works with your site may still have a live VPN profile. Remove those first before building the new system. Documenting the baseline also helps you size the replacement infrastructure: how many concurrent sessions you need to support, and which network segments must be reachable.

Step 2: Segment the OT Network for Remote Access

A flat OT network where every device can talk to every other device is dangerous, especially when outsiders are involved. The replacement model relies on a controlled gateway that sits in an industrial DMZ. The vendor never gets a direct route into the plant-floor subnet. Instead,

they connect to a jump host or a bastion server inside the DMZ, and from there they can initiate outbound connections to specific targets.

This design gives you a chokepoint where you can enforce policies. Traffic passes through a single point that logs everything. If a vendor needs to reach a specific PLC on cell 3, the firewall rules allow that one destination on that one port, not the whole subnet. The industrial DMZ also keeps the vendor's traffic away from your corporate IT network, which reduces the attack surface for both sides.

What to watch: do not assume your existing switches can support VLAN segmentation for OT traffic. Some older industrial switches handle broadcast traffic poorly when you add VLANs. Test the segmentation in a lab or during a scheduled outage before cutting over. Also, check whether the vendor's software expects to discover devices by broadcast. If it does, you may need to configure a helper service or a proxy inside the DMZ.



Step 3: Set Up an Access Window and Approval Workflow

The core of controlled access is the time-bound session. Instead of a permanent VPN tunnel, the vendor requests a window: "I need access to the SCADA server at 10.0.0.25 from 14:00 to 16:00 UTC." The request goes through an approval workflow. A plant engineer or a shift supervisor reviews it and either approves or denies it. Once approved, the gateway automatically opens the necessary firewall rules for that duration and closes them when the window expires.

An access window should always have a defined end time. If the vendor finishes early, they should manually close the session. If they run over, they request an extension, which goes through the same approval process. This discipline prevents the slow drift from "just one more hour" to a connection that stays open for days.

Watch out for time-zone friction. Your vendor may be in a different country, and their working hours might not align with your engineering team's schedule. Plan for a way to handle urgent off-hours requests without forcing someone to wake up and approve a window. A common approach is to pre-approve a set of emergency windows for critical vendors, with the understanding that the session recording will be reviewed the next business day.

Step 4: Enforce Multi-Factor Authentication for Every Session

A VPN password alone is not enough. The vendor account should require MFA, ideally using a time-based one-time password (TOTP) or a hardware token. This applies even for the jump host inside the DMZ. If the vendor's credentials are stolen, the second factor stops the attacker from logging in.

The trick is to make MFA practical for the vendor's workflow. Some vendors connect from a laptop that has no cellular signal, so a phone-based authenticator app may not work. In that case, consider a hardware token that generates codes offline. Also, think about shared accounts: if multiple engineers at the same vendor use the same login, MFA becomes awkward because the token lives with one person. The better long-term fix is to give each individual their own vendor account, even if that means managing more accounts on your side.

Step 5: Record Every Session

Session recording is your audit trail. Every keystroke, every command sent to a PLC, every file transfer - record it all. The recording should capture the screen output or the terminal session, not just the network packets. That way, if something goes wrong (a production line stops, a parameter changes unexpectedly), you can replay the exact session to see what the vendor did.

Session recordings also act as a deterrent. When vendors know their actions are recorded, they tend to be more careful. They are less likely to make "quick fixes" that bypass standard procedures. Store the recordings in a secure location that the vendor cannot access or delete. Retention policies vary by industry, but a common minimum is 90 days, with longer retention for sessions that involved safety-critical systems.

What to watch: session recording software can generate large amounts of data. A single eight-hour session with screen capture can be several gigabytes. Plan your storage capacity and consider compression. Also, test that the recording captures the vendor's actual interaction

with the OT device, not just the connection to the jump host. Some recording tools stop at the jump host and miss what happens after the vendor logs into the target workstation.

Step 6: Migrate Vendors One by One

Do not flip a switch that disconnects every vendor at once. Pick a vendor who is cooperative and whose work schedule is predictable. Migrate them first. Set up their account on the new gateway, configure the firewall rules for their specific targets, and give them a test window. Let them run through a normal support call while you monitor the session. Once they confirm it works, revoke their old permanent VPN account.

Repeat for the next vendor, and the next. Each migration is an opportunity to clean up stale rules and refine the approval workflow. Expect some resistance. Vendors who are used to the old model may complain that the new system is slower or more bureaucratic. Remind them that the goal is security, not inconvenience, and that the recorded sessions also protect them from false accusations if something goes wrong. Over time, most vendors come to appreciate the clarity of having a defined window instead of an always-on connection that they have to remember to disconnect.



Monitoring and Maintenance After the Switch

Once all vendors are on the new system, the work is not over. Review the access logs regularly. Look for patterns: vendors who frequently request extensions, sessions that are approved but never used, or connections that happen at odd hours. These patterns may indicate poor planning on the vendor's side, or they may point to an account that has been compromised and is being used for reconnaissance.

The controlled gateway itself needs patching and updates, just like any other OT device. Treat it as a critical security appliance. A study by Hans Study on OT vendor remote access highlights that organisations which combine a gateway with time-bound approvals and session recording see a significant reduction in security incidents related to third-party access. That is the model

you are aiming for: not just replacing the VPN, but building a process that makes every remote session predictable and auditable.

Finally, keep the vendor relationship healthy. Send them a quarterly summary of their access windows and any anomalies. This transparency builds trust. If a vendor sees that you are serious about security, they are more likely to cooperate when you ask them to change their tools or procedures. The permanent VPN may be gone, but the partnership is stronger for it.

Replacing permanent vendor VPNs with controlled OT access is not a one-time project. It is a change in how you think about remote access. The technology - gateways, MFA, session recording - is the easy part. The harder part is the culture shift, both inside your team and with your vendors. Take it step by step, record everything, and never let a session stay open longer than it needs to. Your OT network will be safer, and your vendors will still get their work done. For more guidance on securing vendor access, **Hans Study** offers practical resources on building these controls into existing OT environments.