

Can your VPN meet the minimum requirements for OT access?

Use these seven questions to evaluate whether your current VPN-based approach gives you the control, visibility and security your operations require.

		YES	NO	NOT SURE
01	Can your VPN prove who is connected to a critical asset by name? Look for individual identity verification, MFA and no shared accounts.	☐	☐	☐
02	If a contractor finished the job last Tuesday, can they still connect today? Look for automatic access expiration, time-boxed permissions and automated removal of access when the work ends.	☐	☐	☐
03	When you offboard a vendor, what do you have to rotate? Look for credentials that are injected into sessions and never handled or stored by users.	☐	☐	☐
04	If the connecting laptop is compromised, what can it reach? Look for an architecture where OT protocols terminate at a gateway and there is no routable path from endpoint to asset.	☐	☐	☐
05	A vendor needs to push a firmware update. What inspects it before it reaches the control network? Look for policy-driven file transfer with malware scanning and administrative approval in both directions.	☐	☐	☐
06	Can you stop a live session, or only review what happened afterward? Look for real-time session oversight, intervention and termination – not just recording.	☐	☐	☐
07	Which of your OT access paths doesn't run through the same controls? Look for consistent controls across remote vendors, employees, onsite operators, legacy assets and low-bandwidth or fully on-prem environments.	☐	☐	☐

TRADITIONAL VPN

Connects an endpoint to a network.



XONA

Connects an authorized user to a specific OT asset without placing the endpoint directly on the OT network.

