

OT Remote Access Security Checklist

Seven questions to evaluate how remote access is secured across your OT environment.

VENDOR QUESTION



Proven identity, not assumed identity

Every session tied to a verified individual through your identity provider. MFA enforced in front of legacy assets, and no shared accounts.

Can you show me every human connected to a critical asset right now, by name?



Access that expires

Just-in-time, time-boxed sessions with approval workflows and no standing access.

What percentage of our current access grants would exist if every one required re-approval today?



Credential custody

Credentials injected into sessions and never displayed or handled by users. When you terminate a contractor, you revoke a person, not launch a rotation project.

When we offboard a vendor, what do we have to rotate?



Endpoint-to-asset separation

Protocols terminate at a gateway and reach the user as a pixel stream, with no routable path from transient device to asset, even if the device is compromised.

Can you diagram the network path from a vendor's machine to our PLC?



Governed content flow

Policy-driven file transfer with malware scanning and admin approval, in both directions.

How do you inspect files for malware and enforce approval before transfer, in both directions?



Live oversight and enforcement

Full session recording, real-time shadowing and takeover, and automated termination triggered by your OT detection stack.

Can you show me a session being killed automatically by a threat detection alert?



No uncovered path

One access model and policy engine for all routes - remote vendors, employees, onsite operators, legacy assets, low bandwidth sites, and fully on premises environments.

Which of our access paths does your platform not cover, and what's the compensating control?