Guide

The 2026 Buyer's Guide to Secure Remote Access for OT and ICS

Preface: Why This Decision Belongs in This Quarter

Secure remote access has quietly become one of the highest leverage risk points in operational environments. Not because it is new, but because the way it is used has changed faster than the way it is governed.

Across critical infrastructure, remote access is now relied on during the most sensitive moments: outages, safety events, equipment failures, and regulatory reviews. At the same time, many organizations are still operating on access architectures designed for a different era, one that assumed stable networks, trusted endpoints, and ample time to recover from failure.

Those assumptions no longer hold.

What makes this a near-term decision rather than a future roadmap item is not a single threat or regulation. It is the convergence of several realities that are already in play:

- Remote work and third-party access are increasing, not decreasing
- OT environments are under greater uptime and safety pressure
- Networks are most fragile precisely when access is most critical
- Regulators and insurers are scrutinizing access pathways earlier in investigations

Executive Summary

Remote access is no longer a convenience in operational environments. It is a core dependency. Plants, substations, pipelines, factories, and transportation systems increasingly rely on remote engineers, vendors, and specialists to maintain uptime, safety, and compliance. At the same time, the mechanisms used to grant that access have become one of the most common points of failure.

Many organizations still rely on IT-era remote access models such as VPNs, jump hosts, or lightly adapted zero trust tools. These approaches assume stable networks, trusted endpoints, and recoverable failure conditions. OT environments rarely meet those assumptions.

This guide is designed to help operational and security leaders evaluate secure remote access based on how industrial systems actually behave. It focuses on decision criteria, tradeoffs, and failure modes so teams can move forward confidently without disrupting production or expanding risk.

This is not a product comparison. It is a framework for making the right decision under real operational constraints.

Why Secure Remote Access is Now a Frontline OT Risk

Remote access has shifted from an exception to a default operating model.

Across critical infrastructure sectors, several trends are converging:

- Increased reliance on remote operations, centralized engineering, and third-party maintenance
- Fewer senior engineers permanently on site
- Greater pressure to resolve incidents quickly without physical travel
- Expanding regulatory scrutiny of access control and auditability

At the same time, OT environments remain sensitive to disruption. Networks are often bandwidth constrained. Connectivity may be intermittent. Systems are frequently legacy and fragile. A failed access session can delay recovery, extend downtime, or force unsafe workarounds.

Remote access failures now have direct consequences:

- Delayed troubleshooting during outages
- Engineers bypassing controls to get work done
- Expanded attack surface through standing access
- Loss of visibility into who accessed what and when

In practice, secure remote access is no longer just a security decision. It is an operational reliability decision. When remote access fails during an incident, responsibility shifts in real time between operations, security, and IT. Access models that require negotiation during failure slow response and increase risk.

Why Traditional IT Remote Access Models Fail in OT

Most remote access tools were designed for IT environments. They assume modern endpoints, stable connectivity, and the ability to recover quickly from failure. When applied to OT, these assumptions break down.

VPNs and Standing Access

VPNs create network-level tunnels that extend trust from the user device into the environment. Once connected, the user is often on the network, not just accessing a specific asset.

In OT environments, this introduces several problems:

User devices become part of the trusted network

Malware on a laptop can reach control systems

Access is often broader than required for the task

Sessions depend on continuous network connectivity

When a VPN session drops mid-task, engineers must reconnect, reauthenticate, and reestablish context. During an incident, this delay matters.

Jump hosts and brittle session handling

Jump hosts centralize access but do not fundamentally change the trust model. They often rely on shared desktops, static credentials, or long-lived sessions. Common failure modes include:

Session drops during network instability

Latency that makes control interactions unsafe

Complex login sequences that slow response

Limited visibility into what actions were taken

In many environments, jump hosts become a bottleneck during incidents rather than a control point.

Excessive trust and expanded blast radius

IT access models are designed for environments where systems can be rebuilt and compromised endpoints can be isolated quickly. OT environments prioritize continuity and safety. A single compromised session can have outsized impact. Tools that rely on tunnels, agents, or broad network access expand the blast radius when something goes wrong.

What Good Looks like for OT Secure Remote Access

Effective secure remote access in OT environments looks different from IT. The goal is not maximum control. The goal is predictable, constrained access that holds up under real operating conditions. The following criteria are practical and testable.

Session-level access control

Access should be granted at the session level, not the network level.

- Sessions are scoped to a specific asset
- Permissions align to the task being performed
- Access is time-bound and purpose-bound
- Ending the session fully removes access

The user never becomes part of the OT network.

Resilience in degraded networks

OT networks are not always stable. Secure remote access must behave predictably when conditions degrade.

- Sessions tolerate latency and packet loss
- Temporary connectivity drops do not corrupt state
- Reconnection does not require restarting work
- Behavior under failure is consistent and safe

If a tool only works when the network is perfect, it will fail when it matters most.

Identity, intent, and zero standing trust

Authorization should reflect who the user is and what they are trying to do, without creating persistent trust relationships.

- Roles define what functions are allowed
- Intent is explicit and reviewed
- Privilege does not persist beyond the session
- Credentials are never exposed to the user

In IT environments, Zero Trust is often implemented as a policy decision at login. In OT environments, trust must remain constrained continuously and visibly at the session level. Access that cannot remain least-privileged during latency, interruption, or recovery is not functionally zero trust, regardless of how it is branded.

Predictable behavior during failure

Operators and engineers need to know what will happen when something goes wrong.

- Sessions pause cleanly rather than crashing
- Access does not silently expand during recovery
- Local teams retain visibility and control
- Safety procedures remain intact

Unpredictable behavior creates risk and erodes trust.

Minimal operational friction

Security controls that slow engineers during incidents will be bypassed. Good solutions:

- Use simple, repeatable workflows
- Do not require specialized clients or agents
- Work with legacy systems without modification
- Allow engineers to focus on the task, not the tool

Ease of use is not a nice to have. It is a safety requirement.

Auditability without operational overhead

Audit and compliance matter, but not at the expense of operations.
Effective approaches:

- Automatically capture session activity
- Provide clear records of who accessed what
- Avoid manual logging or post-event reconstruction
- Do not require operators to change how they work

Audit should be a byproduct of access, not an additional task.

Questions Buyers Should Ask Vendors

These questions surface real differences quickly.

- [ ] What happens to an active session if the network drops mid-task?
- [ ] How is access constrained to a specific asset rather than a subnet?
- [ ] Are credentials ever exposed to the user or stored on their device?
- [ ] What control does the on-site team have during an active session?
- [ ] How does your zero trust model behave when connectivity or policy enforcement degrades?
- [ ] What changes are required to deploy this in a live environment?

Vague answers usually indicate IT assumptions.

Common Misconceptions and Traps

VPN plus MFA is enough

MFA improves authentication but does not change the trust model. Once connected, the user is still on the network. In OT, that is often too much access.

More controls equal more security

Complex approval chains and multi-step logins slow response. During incidents, teams work around them. Security that cannot be used reliably does not reduce risk.

OT can adopt IT access models

OT systems prioritize continuity and safety over recoverability. Tools designed for IT recovery workflows do not map cleanly to industrial operations.

Audit requires friction

Well-designed systems capture activity automatically. Manual logging and after-the-fact reconstruction are signs of poor integration, not strong control.

Decision Guidance

When evaluating secure remote access, focus on tradeoffs rather than features.

- [ ] Does this reduce blast radius or expand it?
- [ ] Does this fail safely or fail unpredictably?
- [ ] Does this help engineers respond faster or slow them down?
- [ ] Can this be deployed without redesigning the network?

Alignment matters. Involve operations, security, and compliance early. Use real scenarios, not diagrams. Test behavior during degraded conditions, not just demos. The right solution should fit into how the environment already operates.

Positioning Purpose-Built OT Access

Solutions designed specifically for OT environments tend to share common characteristics:

- Session-based access that isolates users from the network
- No agents or software on fragile assets
- Strong alignment with operational workflows
- Clear separation between access and connectivity
- Predictable behavior during outages

These platforms are not incremental add-ons to VPNs. They replace the underlying access model.

Why Delaying this Decision Now Carries Real Operational Risk

Secure remote access failures rarely show up as roadmap items. They show up during outages, safety events, or regulatory reviews, when there is no room to rethink architecture.

Most organizations already know which direction they need to go. What slows action is the assumption that existing access will hold until a future refresh cycle. In operational environments, that assumption is increasingly unsafe.

Several conditions are now common across OT environments:

- More remote work is happening during abnormal operations, not routine maintenance
- Networks are more fragile at the exact moments access is most critical
- Vendor and contractor access is increasing, not decreasing
- Regulatory scrutiny focuses on access pathways first, not last

When remote access fails under these conditions, teams do not pause production to redesign controls. They bypass them. That is when risk actually materializes.

This is why secure remote access has moved from a hygiene control to a frontline operational dependency.

The real cost of waiting

Delaying modernization rarely avoids cost. It shifts it.

- Access delays extend downtime when minutes matter
- Engineers fall back to shared credentials or standing access
- VPN tunnels remain open longer than intended
- Audit gaps are discovered after the fact

None of these outcomes appear on a purchase order. All of them show up in incident reports.

Organizations that move now do not do so because of a looming attack headline. They do it because they recognize that access architecture either supports safe operations or undermines them.

What Action Looks like in Practice

Moving forward does not mean ripping out infrastructure or forcing change on the plant floor.

It means:

01

Evaluating secure remote access using failure scenarios, not feature lists

02

Testing behavior during latency, packet loss, and session interruption

03

Validating that access can be revoked instantly and cleanly

04

Confirming that operators retain visibility and control

These steps can be done quickly and safely when access is session-based and isolated by design.

A Grounded Next Step

If your current remote access approach depends on stable connectivity, trusted endpoints, or standing access, the risk is already present. It simply has not surfaced yet.

The right next step is a focused evaluation using a real asset, a real workflow, and real failure conditions. That conversation is worth having before the next outage forces it.

Visit **www.xonasystems.com** to learn more or **schedule a demo** with our OT security specialists.

About Xona Systems

Xona Systems is the secure access platform purpose-built for OT and critical infrastructure. Recognized as an Overall, Product, Innovation, and Market Leader in KuppingerCole's 2025 Leadership Compass for Secure Remote Access for OT/ICS, Xona is deployed in 40+ countries across energy, utilities, manufacturing, oil & gas, maritime, water, defense, and mining. Learn more at **xonasystems.com.**