OT Minimum Access Requirements Checklist

Cyberattacks on OT systems jumped to 87% in 2024, with over 50% of ransomware starting through vendor access points.*

Your endpoints are now the primary attack vector into critical systems. Every uncontrolled connection is a potential entry point for attackers who can shut down production, create safety hazards, or trigger compliance violations.

Use this checklist to evaluate any OT access solution and ensure you have the foundational security elements in place.

1. NO DIRECT NETWORK ACCESS

Endpoints never connect directly to critical systems

Impact

Direct connections enable lateral movement across your entire OT network. Without proper isolation, a single compromised laptop becomes a pathway to HMIs, historians, and engineering workstations.

Look for: Secure proxy connections instead of VPN-style network access.

2. SESSION-LEVEL CONTROLS

Full audit trails and video recordings for all access types

Impact

Session recordings provide forensic evidence and prove compliance with NERC-CIP, TSA SD02E, and SOX requirements. Without them, incident response becomes guesswork.

Look for: Screen activity and command-level recording with timestamps and user attribution.

3. ZERO TRUST ARCHITECTURE

Authenticate based on verified individual identity, not location

Impact

Zero trust principles eliminate blind spots from shared credentials and location-based assumptions. Traditional perimeter security fails when attackers gain "inside" access.

Look for: Integration with existing identity providers (SAML, OIDC) for seamless authentication.

4. ENFORCED MULTI-FACTOR AUTHENTICATION

MFA required for all users without exceptions

Impact

MFA stops attackers even when passwords are compromised. Over 80% of breaches involve stolen credentials that MFA would have prevented.

Look for: Multiple MFA options (TOTP, push notifications, smart cards) to accommodate user preferences.

5. ASSET ISOLATION

Endpoint devices remain completely separate from core OT systems

Impact

Proper isolation contains malware to the access layer only. Without it, compromised devices can infect production systems, requiring offline cleanup and extensive forensics.

Look for: Network and application-layer isolation, not just software controls that can be bypassed.

6. UNIFIED ACCESS MODEL

Consistent security policies for both remote and local connections

Impact

Attackers don't distinguish between connection types. Inconsistent controls mean your strongest remote protections become meaningless when local access uses shared passwords.

Look for: Same authentication, authorization, and monitoring for all access points.

7. RAPID DEPLOYMENT

Implementation in days or weeks, not months

Impact

Quick deployment means faster risk reduction and easier adoption across multiple sites. Complex rollouts often fail when operational pressures mount.

Clientless, browser-based solutions requiring no endpoint software or network changes.

Your Security Foundation

These seven elements work as an integrated system, not standalone controls. If you cannot check every box with your current solution, you are operating with gaps that attackers exploit.

Your vendors and employees need access to keep critical systems running. Secure endpoint access is the foundation that makes that access possible without compromising safety or uptime.

** Dragos 2024 OT Cyber Security Year in Review*