ebook

Third-Party Vendor Access Risk in Critical OT Environments

Somewhere on your OT network, there are active vendor credentials tied to projects that closed months ago. Nobody submitted the revocation request because nobody owned that step. The project manager moved on, the plant engineer assumed IT handled it, and IT assumed OT did. Those credentials are live access points on a network segment connected to your process control systems, and both auditors and attackers are better at finding them than most organizations are at tracking them.

This ebook covers the five ways ungoverned vendor access exposes your operations, why tightening policy cannot fix the underlying problem, and the architecture controls that actually close the gap.

Five Risks Your Vendor Access Architecture Cannot Govern

Legacy remote access tools authenticate the vendor and nothing more. What the vendor does after that authentication, which assets they touch, how long they stay, and whether anyone is watching, sits entirely outside what these tools were designed to govern. The same is true of jump servers, remote desktop gateways, and vendor-managed support portals.

Below are five risks that live in that blind spot.

Stale Credentials Nobody Revokes

Most organizations have a well-designed process for provisioning vendor access and no process at all for ending it. When a project closes, the credential typically stays active because there is no automated link between your work order system and your access system, and nobody owns the gap between them. This plays out across every access method your organization uses, accumulating VPN accounts, jump server logins, remote desktop sessions, and vendor portal credentials that outlive their purpose by months or years.

31% of organizations lack even a basic inventory of their remote access points (SANS, 2025), and CIP-003-9 Section 6 reflects that reality by requiring organizations to demonstrate on demand that they can identify every active vendor electronic remote connection. Credentials you cannot see are credentials you cannot govern.

Supply Chain Amplification

A controls integrator typically maintains active credentials across 20 or 30 customer sites, and a DCS vendor may have standing access to hundreds of facilities through a combination of VPN tunnels, remote desktop tools, and vendor-managed portals. When one of those vendor environments is compromised, every customer who trusted that vendor with a credential is exposed. Dragos reported that 73% of their incident response cases involved compromise of VPN or jump-host credentials (Dragos, 2026), and their 2026 Year in Review documented both KAMACITE and PYROXENE reaching OT environments through trusted vendor relationships rather than direct attacks on asset owners.

IEC 62443-2-4 requires service providers to maintain verifiable identity and access controls across every customer engagement precisely because a vendor's security posture becomes indistinguishable from your own the moment you hand them a credential.

No Time-Bounded Access

Vendor credentials get provisioned when a project starts and are left to expire through a manual process that depends entirely on someone remembering to act. That dependency exists whether the credential is a VPN account, a jump server login, or a vendor portal credential, and it means access persists long after the work that justified it is finished. In December 2024, Team82 documented how IOCONTROL malware exploited persistent, unmonitored access across multiple OT vendors by specifically targeting environments where expiration depended on human memory rather than technical enforcement (Team82, 2024).

TSA SD-02F requires the ability to disable vendor access on demand for exactly this reason, and that requirement assumes your organization already knows which connections are active and which credentials are still live.

No Vendor Action Visibility

Connection logs record that a session opened and closed, and nothing more about what happened during it. Jump servers, remote desktop gateways, and vendor-managed support portals all share this blind spot because connection-layer logging has no visibility into application-layer activity. SANS found that only 13% of organizations implement session recording for vendor access while 50% of ICS/OT incidents originated from external connectivity or remote access (SANS, 2025).

CIP-003-9 requires detecting malicious communications during vendor sessions, a standard that organizations without application-layer visibility have no means of meeting.

Why Policy Cannot Fix an Architecture Problem

The five risks above share a common thread. None of them are the result of poor configuration or inadequate policy. They are the predictable consequences of access architectures that were built for convenience rather than control, and no amount of policy refinement changes what those architectures are capable of governing.

Once a network tunnel opens, the connected user has access to every device reachable on that subnet. Annual access reviews, stronger passwords, and additional MFA factors do not change what the vendor can reach or what they can do once they are there. Gartner recognized this in their 2026 Market Guide by identifying Cyber-Physical Systems Secure Remote Access as a distinct product category and noting that VPNs create unacceptable risk for OT environments (Gartner, 2026). CISA and eight international partner agencies reinforced this in January 2026, recommending a push-only architecture where the OT environment initiates all connections and no unsolicited inbound traffic is permitted (CISA, 2026). That recommendation is structurally incompatible with VPN, which by definition opens an inbound tunnel from the vendor's network to yours.

The conversation worth having is not how to improve existing vendor access controls but which architecture can actually govern identity, scope, time, and session activity?

What Governed Vendor Access Looks Like

Governed vendor access means the vendor connects to one specific asset, for one specific time window, with every action recorded and no standing credentials involved. No standing credentials. No network-level tunnels. No shared accounts.

Just-in-time provisioning addresses the credential lifecycle problem by creating access only at the moment of approval and destroying it when the session ends. The vendor requests access, an administrator approves a connection to a specific asset for a defined window, and when that window closes the credential is gone with nothing left to track, audit, or revoke.

Individual identity enforcement ties every session to a named individual rather than a group credential, so the session log records who connected, when, to which asset, and for how long. This satisfies CIP-003-9's requirement for individual vendor session identification and makes incident investigations tractable rather than dead ends.

Protocol-level session recording captures every keystroke, screen interaction, and command at the application layer rather than the network layer. Recordings are tamper-evident and reviewable after the fact, which is what CIP-003-9 means by detecting malicious communications during vendor sessions and what your incident response team will need when something goes wrong.

Network isolation routes sessions through a protocol-terminating gateway rather than granting direct OT network access. The vendor receives an encrypted image stream of the session with no routable path into your environment, which means a compromised vendor credential cannot be used as a pivot point regardless of what else that vendor's environment contains.

IEC 62443-2-4 requires service provider identity verification, access logging, and session termination controls (ISA/IEC, 2023). CISA's *Secure by Demand* guidance directs OT owners to require these capabilities from their vendors and technology providers (CISA/NSA/FBI, 2025). This is the architecture that those frameworks describe.

Four Steps to Governed Vendor Access

Moving from ungoverned vendor access to a governed architecture does not require a hard cutover. The transition can happen incrementally, one vendor relationship at a time, without disrupting production systems or requiring change management tickets on the OT side.

1

Inventory every vendor credential. Catalog every active VPN account, jump-host credential, and remote desktop session granted to a third party, documenting who approved each one, when it was created, and what project justifies its existence. Most organizations find accounts at this stage they did not know were active, and that discovery alone is usually enough to make the case for a governed architecture internally.

2

Map credentials to assets and projects. For each credential, identify which OT assets it can reach and which active project justifies the access. Credentials tied to completed projects are your first revocation candidates and typically your highest-risk exposures because they represent access with no active oversight and no operational justification.

3

Deploy session-brokered access in parallel. Stand up a governed access architecture alongside your existing infrastructure and migrate vendor sessions one relationship at a time, starting with your highest-risk vendors. Running both systems during the transition means no vendor loses access mid-project and no production system requires modification before you are ready.

4

Decommission legacy vendor access. As each vendor migrates, disable their legacy credential and track decommissioning against your Step 1 inventory. When the last tunnel closes, your attack surface is limited to only the access you explicitly approved for each session, governed by technical controls rather than the assumption that someone will remember to act.

How Xona Systems Delivers Secure Remote Access for Third-Party Vendors

The architecture described in this ebook is not theoretical. Xona applies just-in-time provisioning, individual session identity, protocol-level recording, and network isolation to third-party access to OT environments. These controls map directly to the five risks your current vendor access architecture cannot govern.

Risk	What Xona Does
Stale credentials nobody revokes	✔ Sessions are created at the moment of approval and destroyed when the window expires. Nothing persists to revoke.
Supply chain amplification	✔ Vendors are routed through a protocol-terminating gateway with no routable path into your environment. A compromised credential cannot become a pivot point.
No session-level identity	✔ Every session ties to a named individual. Logs record who connected, when, to which asset, and for how long.

No time-bounded access	✔ Access windows are defined at approval and enforced by the system. When the window closes the session terminates automatically.
No vendor action visibility	✔ Every keystroke, screen interaction, and command is captured at the protocol level in a tamper-evident audit trail.

When a vendor needs access, an authorized operator approves a session to one specific asset for one specific time window. The vendor sees only that asset, with no subnet access, no lateral movement path, and no network-layer tunnel. When the approved window expires, the session terminates automatically.

The platform deploys in 20 minutes per site with no software agent on OT endpoints and no change management tickets for your production systems. Deployment models include on-premises, hybrid, and air-gapped configurations. Cloud connectivity is not required.

The architecture maps directly to the compliance requirements in this paper: CIP-003-9's vendor connection determination and malicious communication detection; TSA SD-02F's continuous monitoring and on-demand disablement; IEC 62443-2-4's identity verification, access logging, and session termination. One platform addresses all three frameworks.

Xona holds SOC 2 Type II certification and was named Leader in OT/ICS Secure Remote Access by KuppingerCole in 2025.

Every risk in this table is governable today. The only variable is whether your architecture enforces that governance by design or leaves it to a process that depends on someone remembering to act.

Take the Next Step

Connect with Secure Remote Access Experts for OT Environments. Learn how Zero Trust remote access can strengthen your OT security posture while improving operational efficiency. 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.**

Sources

- Dragos. "Dragos 2025 OT Cybersecurity Year in Review: 8th Annual Report." February 2025. **https://www.dragos.com/dragos-2025-ot-cybersecurity-report-a-year-in-review**
- SANS Institute. "State of ICS/OT Cybersecurity 2025." 2025. **https://www.sans.org/blog/why-vpn-mfa-is-not-enough-ot-evidence-sans-state-icsot-security-report**
- NERC. "Reliability Standard CIP-003-9." Now in effect (April 1, 2026). **https://www.nerc.com/standards/reliability-standards/cip/cip-003-9**
- TSA. "Security Directive Pipeline-2021-02F." Active through May 2026. **https://www.tsa.gov/sites/default/files/tsa-security-directive-pipeline-2021-02f-and-memo-508c.pdf**
- Dragos. "Dragos 2026 OT Cybersecurity Year in Review." 2026. **https://www.dragos.com/blog/dragos-2026-ot-cybersecurity-year-in-review**
- Gartner. "Market Guide for Cyber-Physical Systems Secure Remote Access." February 4, 2026. **https://www.gartner.com/en/documents/6046877**
- CISA. "Secure Connectivity Principles for Operational Technology." January 14, 2026. **https://www.cisa.gov/resources-tools/resources/secure-connectivity-principles-operational-technology-ot**
- ISA/IEC. "IEC 62443-2-4:2023 Edition 2.0: Security Program Requirements for IACS Service Providers." 2023. **https://webstore.iec.ch/en/publication/7032**
- CISA/NSA/FBI. "Secure by Demand: Priority Considerations for OT Owners and Operators." January 2025. **https://media.defense.gov/2025/Jan/13/2003626906/-1/-1/0/JOINT-GUIDE-SECURE-BY-DEMAND-PRIORITY-CONSIDERATIONS-OT-OWNERS-OPERATORS.PDF**
- TXOne Networks. "OT Cybersecurity Insurance Requirements." 2025. **https://www.txone.com/blog/ot-cybersecurity-insurance/**
- SecureAIT. "Cyber Insurance Requirements Are Getting Tougher." December 2025. **https://www.secureait.com/2025/12/09/cyber-insurance-requirements-are-getting-tougher-what-every-organization-must-know-in-2026/**