Case Study

# Midstream Pipeline Operator Achieves TSA Compliance Across 20 Sites in Hours

How Zero-Trust Secure Access Eliminated Shared Credentials, Enabled Instant Revocation, and Delivered TSA-SD-2E Compliance Under a Tight Deadline.

# Executive Summary

| INDUSTRY | SITES | DEPLOYMENT | COMPLIANCE |
| --- | --- | --- | --- |
| Oil & Gas — Midstream Pipeline | 20 Distributed Pipeline Locations | All 20 Sites in Hours | Full TSA-SD-2E Compliance |

A leading midstream pipeline operator with 20 distributed pipeline and compressor station sites faced an approaching TSA Security Directive compliance deadline. The operator's existing remote access infrastructure relied on legacy tools that provided broad network access, supported cached credentials on shared OT assets, and offered no mechanism for instant access revocation during a cybersecurity incident. Low-bandwidth conditions at remote pipeline locations compounded the problem, making existing solutions unreliable.

The operator deployed Xona, a purpose-built zero-trust secure access platform, across all 20 sites in just a few hours — not weeks, not months. SSO configuration eliminated credential caching on shared OT assets. Centralized management enabled instant provisioning, monitoring, and termination of remote sessions. The result is zero direct network connectivity — users interact with OT systems in real time, but their endpoints are never connected to the OT network. The operator achieved full TSA-SD-2E compliance and gained the ability to immediately disconnect remote access fleet-wide in the event of a cybersecurity incident.

# Industry Context: Pipeline Cybersecurity After Colonial

On May 7, 2021, a ransomware attack on Colonial Pipeline — the largest refined-products pipeline in the United States — forced the shutdown of 5,500 miles of pipeline carrying 45% of the East Coast's fuel supply. The attack, which entered through a compromised VPN credential, triggered fuel shortages, panic buying, and emergency declarations across multiple states. Colonial paid a $4.4 million ransom. The incident became a watershed moment for pipeline cybersecurity.

The federal response was swift and unprecedented. Within weeks, the Transportation Security Administration issued its first mandatory cybersecurity directive for pipeline operators — SD Pipeline-2021-01, followed by increasingly prescriptive revisions. The current directive, TSA-SD Pipeline-2021-02E (commonly referred to as TSA-SD-2E), requires pipeline operators to implement:

- **Network segmentation between IT and OT systems**
- **Access control measures enforcing least-privilege principles**
- **Continuous monitoring and detection capabilities for OT networks**
- **Secure remote access with multi-factor authentication**
- **The ability to instantly disconnect remote access during cybersecurity incidents**
- **Incident reporting within 24 hours of discovery**

The threat landscape reinforces the urgency. Dragos tracked **176 ransomware attacks targeting oil and gas in 2024** organizations, and ransomware attacks in the industrial sector spiked **87% year-over-year in 2024**. Pipeline operators — with their geographically distributed SCADA systems, remote compressor stations, and constrained network links — present an attractive target profile for threat actors who understand that operational disruption creates immediate economic pressure.

For midstream operators, the compliance challenge is particularly acute. These companies operate sprawling networks of pipelines, compressor stations, metering facilities, and tank farms across hundreds or thousands of miles of often-rural terrain. Many sites have limited bandwidth. Personnel are distributed. And OT systems at these sites — PLCs, RTUs, flow computers, compressor controls — are accessed regularly by both internal staff and third-party vendors.

In late 2024, TSA issued a Notice of Proposed Rulemaking (NPRM) signaling the directive's evolution into permanent regulation. The NPRM expands the scope of covered operators and introduces requirements for comprehensive Cybersecurity Risk Management Programs aligned with IEC 62443 and NIST 800-82. For pipeline operators, the message is clear: cybersecurity compliance is not temporary — it is the new permanent operating requirement.

# The Challenge: Distributed Sites, Legacy Access, Hard Deadline

The operator managed 20 distributed pipeline and compressor station sites across a geographically dispersed midstream network. Maintaining reliable, secure remote access to OT systems at these sites was essential for both daily operations and vendor support.

However, the existing infrastructure had critical gaps that put TSA compliance — and operational security — at risk.

- **TSA-SD-2E compliance deadline.** The operator needed to demonstrate zero-trust enforced remote access controls across all sites. Existing tools did not meet the directive's requirements for access governance, session monitoring, or instant revocation. The deadline was approaching, and the operator could not afford a months-long deployment.
- **Low-bandwidth environments.** Many pipeline and compressor station sites are in rural or remote locations served by constrained network links. Existing remote access tools performed poorly — sessions were slow, unreliable, and frequently dropped. This drove technicians to create workarounds that further compromised security posture.
- **Shared assets with cached credentials.** OT assets at pipeline sites — HMIs, engineering workstations, compressor control systems — were shared among multiple operators and vendors. Credentials were cached locally on these devices, meaning anyone with physical or remote access to the device could access it without re-authenticating. Individual accountability was impossible.
- **No instant-disable capability.** TSA-SD-2E explicitly requires the ability to immediately disconnect remote access in the event of a cybersecurity incident. The operator had no mechanism to do this. Revoking a vendor's access required manual intervention across multiple systems and sites — a process that could take hours, precisely when speed mattered most.
- **Inconsistent access controls.** Access policies varied from site to site. Some sites used VPN, others relied on different tools. There was no centralized view of who was connected, to which assets, or what they were doing. The operator's security team lacked the visibility required by TSA directives and the operational confidence needed to manage 20 distributed sites effectively.

# The Solution: Purpose-Built Zero-Trust Access for OT

The operator selected a purpose-built zero-trust secure access platform designed for the specific constraints of OT environments — including the low-bandwidth, distributed, and operationally demanding conditions of midstream pipeline operations.

## Protocol Isolation

The platform deploys a gateway at each site that terminates OT protocols (RDP, SSH, VNC) inside the trusted network. Users connect through a browser over HTTPS port 443 and receive only encrypted pixel streams — never a direct connection to the OT asset. This architecture eliminates lateral movement, prevents malware traversal from endpoints to OT systems, and satisfies TSA requirements for network segmentation between IT and OT.

## SSO-Enforced Re-Authentication

The platform integrates with the operator's identity provider via SAML 2.0, enforcing single sign-on with multi-factor authentication for every session. This eliminates the credential caching problem at its root — users must authenticate through the platform for every session, and credentials for OT assets are injected by the gateway without ever being exposed to the user. Shared passwords on OT devices are no longer a security risk.

## Centralized Access Management

A central management console provides the operator's security team with a single view across all 20 sites. From this console, they can provision new users, define role-based and time-based access policies, monitor active sessions, and — critically — instantly revoke access for any user or disable all remote access to any site with a single action.

## Low-Bandwidth Optimization & Instant Revocation

The platform's PNG-based pixel streaming is engineered for constrained network conditions. Unlike traditional remote access tools that require substantial bandwidth for responsive sessions, the platform delivers usable, interactive sessions over the low-bandwidth links typical of remote pipeline sites. Operators and vendors can access compressor controls, flow computers, and SCADA interfaces without the lag and disconnections that plagued previous solutions.

## Instant Revocation and Lockbox

The platform provides multiple layers of emergency control. A kill button terminates any individual session instantly. A lockbox feature can disable all remote access to a specific site — logically, or by physically disabling Ethernet ports on the gateway hardware. These capabilities directly satisfy the TSA requirement for immediate disconnection of remote access during a cybersecurity incident.

| Solution Highlights — Xona Features Deployed |
| --- |
| • **Protocol Isolation — OT protocols contained within the trusted site network** |
| • **Zero-Footprint Access — Browser-based, no VPN client or agent required** |
| • **SSO + MFA Integration — SAML 2.0 federation eliminates credential caching** |
| • **Credential Injection — OT passwords managed by the gateway, never exposed to users** |
| • **Centralized Management — Single console for all 20 sites** |
| • **Instant Kill Button — Terminate any session immediately** |

- **Lockbox Emergency Disable — Cut all remote access to a site in seconds**
- **Low-Bandwidth Optimized — Reliable sessions over constrained pipeline links**
- **Full Session Recording — Video-fidelity capture of every remote session**
- **Role-Based + Time-Based Access — Least-privilege policies per user, per asset**

# Implementation

For a midstream operator with an approaching compliance deadline, deployment speed was not a nice-to-have — it was a **hard requirement**. The operator needed a solution that could be deployed across 20 geographically distributed sites without sending teams to every location, without reconfiguring networks, and without any downtime to pipeline operations.

- **All 20 sites deployed in just a few hours.** The platform's overlay architecture requires only HTTPS port 443 outbound. Gateways were pre-configured and activated at each site without modifying existing network topology, firewall rules, or OT asset configurations. No agents or software were installed on OT devices. No network reconfiguration was required.
- **SSO and MFA configuration.** The operator integrated the platform with their enterprise identity provider. SSO configuration ensures that every session requires fresh authentication — eliminating the cached credential problem that had persisted on shared OT assets. Multi-factor authentication is enforced for every connection, whether internal or third-party.
- **Centralized policy deployment.** Access policies — defining which users can reach which assets, during what time windows, with what level of privilege — were configured centrally and pushed across all 20 sites simultaneously. This consistency eliminated the site-by-site policy variations that had previously created gaps.
- **Zero operational disruption.** Pipeline operations continued uninterrupted throughout the entire deployment. No compressor stations were taken offline. No SCADA systems were restarted. The platform's overlay design means it sits alongside existing infrastructure without modifying it — precisely the kind of non-disruptive deployment that pipeline operations demand.

# Results

The deployment delivered the compliance, security, and operational improvements the operator needed — on a timeline that matched the urgency of the TSA directive.

| Results at a Glance | |
|---|---|
| ✓ **20 Sites in Under 4 Hours** | All 20 pipeline and compressor station sites deployed in under 4 hours |
| ✓ **Full TSA-SD-2E Compliance** | All directive requirements met, including instant disconnection capability |

| | |
|---|---|
| ✓ **Zero Cached Credentials** | SSO-enforced re-authentication eliminated credential caching on shared OT assets |
| ✓ **Instant Revocation** | Under 10 seconds to cut all remote access; site-wide lockbox in one click |
| ✓ **100% Elimination** | Of direct endpoint-to-OT connectivity via protocol isolation |
| ✓ **Reliable Low-Bandwidth Access** | Responsive sessions at remote pipeline sites where previous tools failed |
| ✓ **Centralized Visibility** | Single console monitoring all 20 sites with full session recording |

- **TSA-SD-2E compliance achieved.** The operator met all requirements of the TSA Security Directive, including access control with least-privilege enforcement, multi-factor authentication, continuous session monitoring, and the ability to immediately disconnect remote access during a cybersecurity incident. Compliance evidence — session recordings, access logs, policy configurations — is available on demand.
- **Shared credential risk eliminated.** With SSO-enforced authentication and credential injection, OT asset passwords are managed by the gateway and never exposed to users. Even on shared devices accessed by multiple operators and vendors, every session is attributable to a named individual. The operator can answer the question regulators care about most: who did what, on which asset, and when.
- **Instant incident response capability.** The operator's security team can now terminate any remote session with a single click and disable all remote access to any site using the lockbox feature. During the operator's most recent incident response drill, the team demonstrated the ability to cut all remote access to a site in under 10 seconds — a capability that simply did not exist before deployment.
- **Reliable access at constrained sites.** Vendors and internal operators report that remote sessions are now responsive and stable, even at pipeline sites with limited bandwidth. Issues that previously required dispatching a technician for a multi-hour drive to a remote compressor station can now be diagnosed and often resolved remotely — reducing both response time and operational cost.
- **Unified security posture.** For the first time, the operator has a single, consistent access governance framework across all 20 sites. The security team has real-time visibility into every active session, with the ability to shadow, record, or terminate any connection. Policy changes propagate across the entire network instantly.

## Regulatory Alignment: TSA-SD-2E Requirements Mapping

| TSA-SD-2E Requirement | How Xona Addresses It |
|---|---|
| **Network Segmentation** | **Protocol isolation ensures OT protocols are terminated at the gateway inside the trusted network. User endpoints connect via HTTPS 443 only — no direct OT network access. IT and OT traffic are architecturally separated.** |

| | |
|---|---|
| **Access Control (Least Privilege)** | **Role-based access control (RBAC) scopes each user to specific assets. Time-based access control (TBAC) limits sessions to defined maintenance windows. No user has broader access than their role requires.** |
| **Multi-Factor Authentication** | **MFA enforced at the gateway for every session via SAML 2.0 SSO integration. Supports TOTP apps, hardware tokens, and IdP-delivered MFA.** |
| **Continuous Monitoring** | **Every session is monitored in real time. Security personnel can shadow live sessions. Full video-fidelity recording captures all session activity for forensic review.** |
| **Immediate Disconnection** | **Kill button terminates individual sessions instantly. Lockbox disables all remote access to a site — logically or by physically disabling gateway Ethernet ports.** |
| **Incident Reporting Support** | **Comprehensive session logs and video recordings provide the forensic evidence needed for 24-hour incident reporting. SIEM integration enables automated alerting.** |
| **Supply Chain Security** | **Third-party vendor access governed through centralized policies. Credential injection prevents credential exposure. Just-in-time access with moderated approvals eliminates standing vendor access.** |

# Looking Ahead

With TSA-SD-2E compliance achieved, the operator is now positioned for the next phase of pipeline cybersecurity regulation and operational expansion:

- **NPRM preparation.** TSA's 2024 Notice of Proposed Rulemaking signals the transition from security directives to permanent regulation, with expanded scope and IEC 62443 alignment. The operator's deployed solution already addresses many anticipated NPRM requirements, including comprehensive access governance, session monitoring, and supply chain security controls.
- **Additional site deployment.** The operator plans to extend the platform to additional pipeline assets as its network grows. Given the hours-not-weeks deployment model, scaling to new sites requires minimal planning and zero disruption to existing operations.
- **SIEM/SOAR integration.** The operator is implementing integration between the platform and its SIEM and SOAR environment, enabling automated playbooks that can trigger session termination or lockbox activation based on threat intelligence feeds and anomaly detection.
- **Vendor risk scoring.** Using session analytics and access patterns, the operator intends to develop risk-based vendor access policies that dynamically adjust privileges based on vendor behavior and external threat conditions.

The Colonial Pipeline attack demonstrated that a single compromised VPN credential can shut down critical energy infrastructure. For this midstream operator, that lesson has been translated into action: a fundamentally different access architecture that eliminates the vulnerabilities exploited in that attack and the dozens of pipeline-targeting incidents that have followed.

> ***"The centralized access management capabilities have been invaluable for Security Directive compliance requirements and protecting our critical infrastructure. We can quickly disconnect remote access in the event of a cybersecurity incident."***
>
> **— IT/OT Sr. Systems Administrator**

# 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***