Case Study

From Audit Failure to Audit Ready:

A Pharmaceutical Manufacturer Secures GMP-Critical Systems

How a mid-size pharmaceutical manufacturer resolved FDA warning letter findings, achieved 21 CFR Part 11 compliance for remote access, and established complete individual accountability across 6 manufacturing sites — without disrupting validated GMP systems.

Executive Summary

A mid-size pharmaceutical manufacturer specializing in controlled substance formulations and specialty drugs received an FDA warning letter citing critical deficiencies in electronic records management for GMP-critical computerized systems. The core finding: shared credentials for remote access to batch control systems and clean room HVAC made it impossible to demonstrate individual accountability — a fundamental requirement of 21 CFR Part 11 and EU GMP Annex 11.

The company's OEM vendors — servicing bioreactors, lyophilizers, filling lines, and environmental monitoring systems — accessed production systems using shared TeamViewer and VPN accounts with no session logs, no individual identification, and no audit trail. The quality team could not answer the most basic regulatory question: **who accessed what, when, and what did they do?**

The company deployed the Xona Platform across all six manufacturing sites as a non-disruptive overlay — requiring no changes to validated GMP systems. Xona's credential injection eliminated shared passwords, session recording established a complete audit trail, and moderated file transfer with malware scanning protected data integrity. Within five months, the company passed its FDA re-inspection with zero observations related to remote access or electronic records. The quality team can now retrieve and replay any access session on demand — a capability that has transformed how the organization approaches data integrity.

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. For a pharmaceutical manufacturer operating validated GMP systems, this architecture is decisive: it delivers the access controls and audit trails that regulators require without introducing any change to the validated systems themselves.

RESULTS AT A GLANCE	
FDA Cleared	Re-inspection passed with zero observations on remote access
100%	Individual accountability for all electronic records access
Zero	Shared credentials remaining across all 6 manufacturing sites
Complete	Session audit trails for every OEM and internal access event
75%	Reduction in OEM vendor access provisioning time
6 Sites	Secured across US and EU operations

Industry Context

FDA Enforcement and Data Integrity

The FDA has intensified its focus on data integrity in pharmaceutical manufacturing over the past several years. Warning letters citing 21 CFR Part 11 deficiencies have become increasingly common, with particular attention to electronic records generated by computerized systems — including batch records, environmental monitoring data, and laboratory information management systems.

At the heart of the FDA's concern is a simple principle: **every electronic record must be attributable to a specific individual.** When multiple operators or vendors share a single set of credentials, the resulting electronic records are fundamentally compromised — not because the data itself is wrong, but because the organization cannot prove who generated or modified it. This is a direct violation of 21 CFR Part 11, which requires that electronic signatures and records provide the same level of accountability as handwritten signatures on paper records.

EU GMP Annex 11, which governs computerized systems in European pharmaceutical manufacturing, imposes parallel requirements. For companies operating on both sides of the Atlantic, the compliance burden is compounded — any remote access solution must satisfy both regulatory frameworks simultaneously.

The Ransomware Threat to Pharmaceutical Manufacturing

Beyond compliance, pharmaceutical manufacturers face a growing cybersecurity threat. Ransomware attacks on manufacturing operations have increased by 61% year-over-year, with pharmaceutical companies representing high-value targets due to the time-sensitive nature of drug production and the potential public health consequences of supply disruptions. The convergence of IT and OT networks in pharmaceutical plants — where batch control systems, clean room HVAC, and environmental monitoring are increasingly connected — creates pathways that attackers can exploit.

The Validated Environment Constraint

Pharmaceutical manufacturing operates under a unique constraint: changes to validated systems require extensive documentation, risk assessment, and formal change control. This means that any security solution deployed in a GMP environment must be minimally disruptive — ideally requiring no changes whatsoever to the validated systems it protects. Solutions that require agents installed on production servers, modifications to network configurations, or changes to application software face weeks or months of validation documentation before they can be deployed. This creates a structural advantage for overlay solutions that operate independently of the systems they secure.

The Challenge

The FDA warning letter identified specific deficiencies that demanded immediate corrective action:

Shared Credentials and Lost Accountability

The company's batch control systems — governing formulation, blending, granulation, and tablet compression — were accessed remotely by both internal process engineers and OEM vendors using shared accounts. A single "admin" account with a static password was used by multiple individuals to connect via TeamViewer. The same pattern existed for clean room HVAC systems, where environmental monitoring vendors connected through a shared VPN account to adjust temperature, humidity, and differential pressure setpoints.

> The consequence was stark: when the FDA asked the company to demonstrate who had modified a specific batch parameter on a specific date, the quality team could not answer. The electronic audit trail showed that "admin" had made the change — but "admin" could have been any of **14 different people**. This single finding was sufficient to trigger the warning letter.

No Session Logs for Vendor Access

OEM vendors for the company's bioreactors, lyophilizers, filling lines, and water-for-injection systems connected to production equipment using a variety of tools — TeamViewer, AnyDesk, vendor-specific VPN clients, and in some cases, direct RDP connections through firewall exceptions. None of these tools provided session recording. The quality team had no way to review what vendors had done during maintenance sessions — a critical gap for both regulatory compliance and GMP investigation support.

File Transfer Without Controls

OEM vendors routinely transferred files to and from production systems — firmware updates, configuration files, calibration data, and diagnostic logs. These transfers occurred through the same uncontrolled remote access pathways, with no malware scanning, no approval workflow, and no audit trail. In a validated GMP environment where every change must be documented and justified, this represented an unacceptable data integrity risk.

Multi-Site Inconsistency

The company operated six manufacturing sites — four in the United States and two in the European Union. Each site had evolved its own remote access practices independently. Remote access tools, credential management practices, and vendor onboarding procedures differed across sites, making it impossible to demonstrate a consistent, company-wide approach to electronic records management — a key expectation during both FDA and EU competent authority inspections.

The Validation Dilemma

The company needed to act quickly — the FDA expected a corrective action response within 15 business days. But any solution that required changes to validated GMP systems would trigger a formal change control process, requiring Installation Qualification (IQ), Operational Qualification (OQ), Performance Qualification (PQ), and updated validation documentation for every affected system. For a company with hundreds of validated computerized systems across six sites, this could take a year or more — time the company did not have.

The Solution

The company selected the Xona Platform specifically because of its overlay architecture — Xona sits between users and GMP-critical systems without modifying, touching, or integrating into the validated systems themselves.

A Non-Disruptive Overlay for Validated Environments

This was the decisive factor in the selection. Xona's architecture means that the validated state of batch control systems, HVAC controllers, environmental monitoring systems, and other GMP-critical equipment is **entirely unaffected** by the deployment. The Xona XCM is deployed in the network DMZ and brokers all remote access sessions — but from the perspective of the validated systems, nothing has changed. They still receive RDP, SSH, or VNC connections from within the trusted network from the Xona CSG, exactly as before. The difference is that those connections now originate from the Xona gateway, not from uncontrolled vendor endpoints.

Credential Injection for Individual Accountability

Xona's credential injection capability was the direct answer to the FDA's core finding. Privileged credentials for GMP-critical systems are stored in Xona's encrypted vault.

When a user — whether an internal process engineer or an OEM vendor technician — authenticates to Xona (via SAML-based SSO with MFA), the gateway injects the appropriate system credentials on their behalf. The user never sees, handles, or knows the password for the target system.

This achieves two critical outcomes simultaneously: every access event is tied to a named individual (satisfying 21 CFR Part 11's individual accountability requirement), and the privileged credentials themselves are never exposed to users or their endpoints (eliminating the shared credential problem entirely).

Session Recording for Complete Audit Trail

Every remote access session — whether internal or vendor-initiated — is recorded in full-fidelity video with timestamps, keystroke logging, and mouse action capture. The quality team can search for any session by user, date, target system, or site, and replay it in its entirety. This transforms the audit trail from a log entry ("user connected at 14:32") into a complete, reviewable record of every action taken during the session.

Moderated File Transfer for GMP Data Integrity

All file transfers through the Xona gateway follow a moderated workflow: files are quarantined, scanned for malware via ICAP antivirus scanning, with options including Palo Alto WildFire and VirusTotal integration, and held for explicit approval before being delivered to the target system. Every file transfer is logged with the sending user, receiving system, filename, hash, scan results, and approval record — providing a complete chain of custody that satisfies GMP documentation requirements.

Cryptographic Log Signing

Session logs and access records are cryptographically signed, providing non-repudiation — the mathematical certainty that logs have not been altered after the fact. For a pharmaceutical company where data integrity is not just a compliance requirement but a fundamental quality principle, this capability closes the loop on the audit trail: records are not only complete, they are provably authentic.

Solution Highlights: Xona Key Features
• **Xona Critical System Gateway (CSG)**
• **Credential Injection (No Shared Passwords)**
• **Full Session Recording with Timestamps**
• **Cryptographic Log Signing (Non-Repudiation)**
• **Moderated File Transfer with Malware Scanning**
• **Role-Based Access Control (RBAC)**
• **Just-In-Time (JIT) Vendor Access**
• **Moderated Access / Wait Room**
• **Xona Central Manager (XCM)**
• **SIEM Integration for Audit Export**
• **Protocol Isolation (Pixel Streaming)**
• **Zero-Footprint Browser-Based Access**

Implementation

Quality-Validated Deployment

While Xona itself requires no changes to validated GMP systems, the company chose to validate the Xona deployment as a GMP-supporting infrastructure component. The quality team developed a streamlined IQ/OQ/PQ protocol specifically for the Xona CSG — a process that was significantly simpler than validating changes to the production systems themselves.

- **Installation Qualification (IQ)**: Verified that Xona CSG hardware and software were installed per specifications at each site. Completed in one day per site.

- **Operational Qualification (OQ)**: Confirmed that credential injection, session recording, file transfer moderation, and access controls functioned as specified. Completed in two days per site.
- **Performance Qualification (PQ)**: Validated that the system performed reliably under production conditions over a 30-day monitoring period.

Phased Rollout Across 6 Sites

The deployment followed a phased approach:

Phase 1 Weeks 1–3

Pilot deployment at the company's largest US manufacturing site — a controlled substance formulation facility with the most complex OEM vendor landscape. All legacy remote access tools were replaced and all OEM vendors transitioned to the Xona platform.

Phase 2 Weeks 4–8

Rollout to the remaining three US sites, with each site deployment completed in under one day. The Xona Central Manager (XCM) provided centralized policy management across all US sites.

Phase 3 Weeks 9–14

Deployment to the two EU manufacturing sites, with policies configured to satisfy both FDA 21 CFR Part 11 and EU GMP Annex 11 requirements simultaneously.

Total elapsed time from first deployment to full enterprise coverage: 14 weeks. Total disruption to validated GMP systems: zero.

Results: Zero FDA Observations

Regulatory Compliance

- The company passed its FDA re-inspection with zero observations related to remote access, electronic records, or individual accountability — a complete resolution of the warning letter findings.
- EU competent authority inspections at both European sites confirmed compliance with Annex 11 requirements for computerized systems access controls and audit trails.
- The quality team can now respond to any regulatory inquiry about system access within minutes — retrieving session recordings, access logs, and file transfer records on demand.

Operational Efficiency

- OEM vendor access provisioning time reduced by 75% — from an average of 3.5 hours (involving VPN configuration, credential sharing, and manual documentation) to under 50 minutes (including JIT approval, session initiation, and automated documentation).

- Vendor session setup is now a standardized, repeatable process across all six sites — eliminating the inconsistency that previously existed between locations.
- The quality team estimates that automated session documentation saves approximately 120 hours per month in manual record-keeping across the six sites.

Security Posture

- Zero shared credentials remain in use across all six manufacturing sites. Every access event — internal and vendor — is attributable to a named individual.
- Protocol isolation ensures that no vendor endpoint ever touches a GMP-critical system directly. OT protocols are terminated at the Xona gateway; vendors interact through encrypted pixel streams in a standard web browser.
- Moderated file transfer with malware scanning has intercepted two files flagged by automated malware scanning during the first six months of operation — files that would otherwise have been transferred directly to production systems.

The Data Integrity Angle: ALCOA+ Compliance

ALCOA+ is the gold standard for data integrity in pharmaceutical manufacturing.

Here is how Xona's platform satisfies each principle for remote access to GMP-critical systems:

Attributable	Every access event is tied to a named individual through credential injection and federated identity — no shared accounts, no anonymous sessions.
Legible	Session recordings capture full-fidelity video of all interactions in a permanently readable format. Keystroke and mouse action logs provide supplemental detail.
Contemporaneous	Session logs are generated in real time as events occur. Timestamps are system-generated and tamper-resistant.
Original	Session recordings and logs are the original records — not transcribed or summarized. Cryptographic signing ensures they have not been altered.
Accurate	Protocol isolation ensures that what the session recording captures is exactly what the user saw and did — pixel-perfect accuracy with no gap between action and record.
Complete	Every session — including those that are terminated prematurely or encounter errors — is recorded in full with start time, end time, and all actions.
Consistent	The same recording and logging mechanisms apply uniformly across all sites, all users, and all sessions — internal staff and OEM vendors alike.

Enduring	Session records are retained per the company's configurable retention policy and exported to the quality document management system for permanent archival.
Available	Quality reviewers, auditors, and investigators can search, retrieve, and replay any session recording on demand through the Xona Central Manager.

Looking Ahead

Serialization System Access

The company is extending its Xona deployment to cover remote access for serialization and track-and-trace systems — critical for Drug Supply Chain Security Act (DSCSA) compliance. These systems require the same level of individual accountability and audit trail rigor as batch control systems, making Xona a natural fit for governing OEM vendor access to serialization infrastructure.

Cold Chain Monitoring Expansion

As the company expands its biologics portfolio, cold chain monitoring and control systems at distribution centers will require secure remote access for both internal logistics teams and cold storage equipment vendors. The company plans to extend the Xona platform to these facilities, applying the same credential injection, session recording, and moderated file transfer controls that have proven effective in the manufacturing environment.

Continuous Compliance Monitoring

The quality team is developing a continuous compliance dashboard that leverages Xona's SIEM integration to provide real-time visibility into access patterns, session volumes, and compliance metrics across all sites. This moves the organization from periodic audit readiness to continuous audit readiness — a significant maturity step in pharmaceutical quality management.

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***