ebook

Lack of Session Visibility or Recording in Your OT & ICS Environment

How to Eliminate Blind Spots in Your Critical Infrastructure Before They Become Breaches

Every day, privileged users including contractors, IT administrators, vendors, and remote employees connect to sensitive systems to change configurations, access data, manage infrastructure, and interact with industrial controls. In many environments, little of that session activity is captured in a form that is actually useful after the fact.

This gap in session visibility is not a minor monitoring issue. It is a persistent exposure that affects organizations of every size and repeatedly surfaces in breach investigations, insider threat reviews, and compliance audits.

Authentication shows who got in. It does not establish accountable control over what happened next.

This ebook is for security leaders who want to understand why many current approaches fall short, and how to build a defensible, scalable program for recording and monitoring privileged access across critical infrastructure.

Understanding the Blind Spot: Visibility, Logging, and What Most Teams Miss

The session visibility gap is rarely the result of a single decision. More often, it emerges from reasonable architectural choices, tool limitations, and operational tradeoffs that together create a serious blind spot.

The most common root causes include:

- **Legacy remote access tools built for connectivity rather than auditability.** VPNs, jump servers, and traditional RDP solutions were designed to establish access, not to document what users did once connected. That leaves a structural gap between authentication and accountability.
- **Fragmented tooling across environments.** Organizations often use one approach for on-premises systems, another for cloud environments, and no consistent strategy at all for OT or ICS infrastructure. The result is patchy coverage with meaningful gaps at the seams.
- **Over-reliance on endpoint or network logs.** These logs capture connection metadata and data movement, but they rarely show what a user actually did during a session, including which commands they ran, which files they touched, or which configurations they changed.
- **Resource constraints around data management.** Full session recording generates substantial data. Without a clear policy for retention, indexing, and retrieval, many teams default to not recording at all rather than solving the governance and storage problem.
- **Third-party access blind spots.** Vendor and contractor sessions are among the highest-risk activities in most environments, yet they often receive the least monitoring because organizations extend VPN access without attaching session-level controls.

Logging vs. Recording vs. Monitoring

Capability	What It Captures	Use Case	Limitation
Logging	Events and metadata, such as who connected, when, and from where	Audit trails, compliance reporting	Shows that something happened, not what happened
Recording	Full session content, including keystrokes, screen activity, and commands	Forensics, incident review, insider threat investigations	Requires storage, retention policy, and retrieval tooling
Monitoring	Real-time activity analysis and alerting	Active threat detection and response	Incomplete without recording and broader context

A mature visibility program needs all three. Logging establishes who was connected and when. Recording captures what they did during that connection. Monitoring helps determine in real time whether that activity requires attention.

Common Misconceptions

Several widely held assumptions cause organizations to underinvest in session visibility even when they face clear operational and regulatory risk.

"Our VPN logs cover us."

VPN logs show who authenticated, when, and from where. They do not show what the user did once the tunnel was established. A malicious insider or compromised vendor credential can operate for hours and leave little trace beyond the initial authentication event.

"We have SIEM, so we have monitoring."

A SIEM is only as useful as the telemetry it receives. Without session-level content such as commands run, files accessed, and screen activity, a SIEM can surface anomalies in metadata but still leave investigators unable to reconstruct what actually happened.

"Our endpoint agents handle this."

Endpoint detection tools are designed for malware and threat detection on managed devices. They are not purpose-built for capturing and replaying privileged sessions. They also tend to miss third-party or contractor access and often do not apply in OT and ICS environments where agents cannot be deployed on legacy industrial assets.

"Recording everything is too expensive."

The economics have shifted. Modern session recording platforms are more storage-efficient than older approaches, while the cost of not recording continues to rise in the form of delayed investigations, failed audits, regulatory exposure, and reputational damage.

The Consequences of Session Visibility Gaps

When security teams cannot see what privileged users do inside critical systems, many high-risk behaviors become difficult to detect through metadata alone. That includes insider misuse, credential abuse, lateral movement, and poorly monitored vendor activity.

The threats most commonly enabled by session visibility gaps include:

- **Insider threats.** Malicious or negligent users can operate for extended periods before detection. Without session recording, their activity may remain unclear even after an investigation begins.
- **Compromised privileged credentials.** Attackers who obtain administrator or vendor credentials through phishing, credential stuffing, or dark web purchases can operate interactively on systems without producing a clear behavioral signature in connection metadata alone.
- **Supply chain and vendor access abuse.** Third-party vendors with remote access are a common attack vector in enterprise breaches because they often combine broad privileges with minimal monitoring.

- **Lateral movement.** Attackers who gain an initial foothold frequently use privileged sessions to explore the environment and expand access. Without session-level recording, security teams may have little visibility into the commands and actions used to move deeper into the network.
- **Data exfiltration without file-based indicators.** Sophisticated actors may read, copy, or manually transmit sensitive data rather than using obvious file transfer mechanisms. In those cases, screen and keystroke recording may be the only reliable way to reconstruct what occurred.

Debugging and Support Without Data

Session visibility also has operational value beyond security. Operations and engineering teams rely on session records to reconstruct what happened during maintenance windows, patching cycles, and vendor interventions. Without that data, resolution takes longer and accountability gets murky.

Common scenarios include:

- A configuration change to a production database causes an outage. Without a session recording, the team must reconstruct events from memory and incomplete logs, which can stretch resolution from hours into days.
- A vendor performs maintenance on industrial equipment and introduces a software change that degrades performance. Without a record of the exact actions taken, identifying root cause depends on vendor recollection and transparency rather than independent evidence.
- A critical system fails after a routine patching cycle involving multiple engineers. Without recordings that document the sequence and content of each session, isolating the responsible change can require extensive manual investigation with no guarantee of certainty.

Session recordings provide a precise, timestamped record of what was done and by whom. That can materially reduce mean time to resolution and eliminate the ambiguity that often slows post-incident analysis.

Compliance Failures and Legal Exposure

Many regulatory frameworks now expect organizations to monitor and account for privileged access. When session visibility is missing, that often creates audit gaps, weakens incident evidence, and increases legal exposure.

The most directly relevant frameworks include:

- **NERC CIP (energy sector):** Requires documented controls for electronic access to critical cyber assets, including the ability to generate audit records that support accountability for user activity on covered systems.
- **NIST SP 800-53 / 800-82:** Federal guidance on information security controls emphasizes audit and accountability, including the need to capture enough detail to reconstruct the sequence of events surrounding a security incident.
- **SOC 2:** Organizations pursuing SOC 2 certification must demonstrate logical access controls and monitoring capabilities. Session recording is increasingly expected as auditor-reviewable evidence of those controls.
- **HIPAA:** Healthcare organizations handling protected health information must implement audit controls that examine access and activity in systems containing PHI, with the expectation that those controls produce records usable during a breach investigation.

- **IEC 62443 (industrial cybersecurity):** Requires monitoring and logging for industrial control systems, with increasing specificity in recent revisions around what must be captured to satisfy audit and accountability requirements.

Beyond compliance, session recordings can also play an important legal role. They can exonerate employees wrongly accused of misconduct, support vendor liability proceedings, and provide evidence in cases involving malicious insiders or external actors operating through compromised credentials.

Steps to Full Visibility for Your Critical Infrastructure

Auditing Your Current State

Before closing the visibility gap, you need a precise map of it. Most organizations find coverage is narrower than assumed, especially around third-party access, legacy systems, and higher-risk workflows.

A structured audit should answer the following questions:

1. Which systems and assets are in scope for privileged access, including not only servers and databases but also network devices, industrial systems, cloud management consoles, and security infrastructure?
2. Which users and roles have privileged access to those systems, including employees, contractors, vendors, and service accounts whose credentials could be compromised or misused?
3. For each access path, what is actually being captured? Is it connection metadata only, or full session content including commands and screen activity?
4. How long is that data retained, and is it searchable and replayable in a format that would be useful during an investigation or audit?
5. Where are the gaps in coverage? Which environments, systems, or access methods fall outside current monitoring because they rely on unsupported protocols, legacy workflows, or newer infrastructure added after the monitoring program was defined?

Mapping the results visually, with assets on one axis and access paths on the other, can make blind spots visible quickly and provide the basis for a prioritized remediation plan.

Choosing the Right Tools

The wrong solution usually does not fail because it records nothing. It fails because coverage is partial, retrieval is clumsy, or the architecture depends on agents and assumptions that do not hold in OT environments.

When evaluating session visibility and recording platforms, several criteria matter most:

- **Coverage Across Environments**
  A viable solution must cover the environments and protocols that actually exist across the infrastructure, including SSH, RDP, web-based management interfaces, industrial protocols, and cloud consoles. A tool that covers only part of the environment creates new seams even as it closes old ones.
- **Session Recording Quality**
  Not all session recording is equally useful. The most valuable recordings capture keystrokes, commands, screen content, and file operations in a format that supports replay, search, and event correlation. Video-only capture is often harder to search, harder to analyze, and less useful in investigations.
- **Integration with Existing Infrastructure**
  Visibility tooling should integrate with identity providers, SIEM platforms, and ticketing systems. Recording sessions in isolation without tying them back to identity events and security workflows limits the value of the data and adds manual work during investigations.
- **Operational Simplicity**
  Solutions that require heavy maintenance, ongoing tuning, or agent deployment across managed and unmanaged endpoints are more likely to face adoption resistance and long-term coverage gaps. Approaches that operate at the access layer rather than on endpoints are often more sustainable.
- **Compliance Reporting**
  For organizations with regulatory obligations, the solution should generate the reports and evidence required by relevant frameworks without forcing teams to compile them manually from raw logs.

How Xona Provides Session Visibility and Recording

Xona is a purpose-built secure access platform for critical infrastructure in which session visibility and recording are native architectural capabilities rather than features added to an existing remote access product. The platform was designed from the beginning with the specific requirements of operational technology, industrial control systems, and regulated enterprise environments in mind, which shapes both what it can capture and how that data can be used.

The underlying design principle is that every privileged session passing through Xona should be fully visible, fully recordable, and fully auditable without requiring agents on endpoints, modifications to the systems being accessed, or complex integrations with legacy infrastructure.

Active Defense

Xona's approach to session visibility supports active defense. Recording is not treated only as a forensic artifact after the fact. It also supports real-time security operations by giving teams the context they need to identify and respond to suspicious activity during a session.

Full Session Recording

Xona captures complete session content for privileged access sessions, including keystrokes, commands, screen content, and file operations, in a format that supports both replay and full-text search. Recordings can be protected with tamper-evident controls to preserve integrity for investigations and compliance use.

Identity-Correlated Records

Every recorded session in Xona is tied to a verified identity. Recordings can be associated with the authenticated user, the access request that authorized the session, the specific assets accessed, and any workflow steps completed during the access lifecycle, including approval workflows for just-in-time access.

Searchable and Exportable Evidence

For compliance audits and incident investigations, Xona's recording data can be searched by user, asset, time range, or session content. Records can also be exported in standard formats for use in SIEM platforms, ticketing systems, and legal discovery workflows without requiring cumbersome manual extraction.

Zero Trust Architecture

Xona applies a zero trust access model in which each access request is verified against identity, device, and policy before a session is allowed. That creates a natural control point where recording and monitoring can be applied consistently, without leaving a bypass path through direct network access.

Coverage Across IT and OT Environments

Unlike visibility tools designed primarily for IT, Xona is built for the mixed environments common in critical infrastructure, including manufacturing, utilities, energy, water treatment, and transportation. The platform supports industrial protocols and network architectures common in OT without requiring modifications to the underlying systems or agent deployment on legacy industrial hardware.

Protocol-Aware Inspection

Xona's proxy architecture operates at the protocol layer, providing protocol-aware inspection for SSH, RDP, web-based management consoles, and a range of industrial and OT protocols. That allows the platform to interpret session activity with more context than a simple network tunnel and enables more intelligent policy enforcement

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**.