NETWITNESS

Guide

OT Cybersecurity Solution Buyer's Guide for Industrial Manufacturers

Executive Summary

Industrial manufacturing environments run on operational technology systems that were built for precision, uptime, and safety, not for exposure to modern cyber threats. PLCs (Programmable Logic Controllers), SCADA (Supervisory Control and Data Acquisition) systems, industrial HMIs, and proprietary protocols often operate for decades with minimal change, limited logging, and little tolerance for active security controls. As manufacturing networks become more connected to enterprise IT and external partners, this design gap has become a primary source of cyber risk.

For manufacturers, a cyber incident is not just a data problem. It can halt production lines, damage equipment, create safety hazards, and disrupt supply commitments. Yet many security teams lack continuous visibility into OT network activity and must rely on tools designed for IT environments, where agents, frequent patching, and standardized logs are assumed.

This guide is designed to help industrial manufacturers evaluate OT cybersecurity solutions through a practical, operationally aware lens. It focuses on how network-based detection and response capabilities support OT security by passively monitoring industrial traffic, identifying abnormal behavior across control systems, and enabling investigation without interfering with production processes.

The content follows a use-case-driven structure aligned to real manufacturing scenarios, including unauthorized access to control networks, lateral movement from IT into OT, protocol misuse, and stealthy changes to industrial communications. Each chapter explains the detection challenge, the OT-specific constraints involved, and the criteria security leaders should use when assessing solution capabilities.

Rather than prescribing a single architecture, the guide emphasizes evaluation frameworks, technical considerations, and operational trade-offs relevant to multi-site manufacturing environments. The final chapter demonstrates how these principles are applied in practice using NetWitness, showing how deep network visibility and investigation capabilities can support OT security while respecting the realities of industrial operations.

What This Guide Covers

Security teams often hear about NDR, but struggle to answer practical questions:

- What visibility does NDR actually provide that other tools miss?
- How does NDR support investigations, not just alerting?
- Where does it fit alongside SIEM, EDR, and SOAR?
- How do you evaluate vendors beyond feature checklists?

This guide addresses those questions directly, using real-world scenarios, technical examples, and buyer-focused frameworks.

Who This Guide is for

- CISOs and security leaders shaping detection strategy
- SOC managers responsible for investigation workflows
- Security architects evaluating NDR, SIEM, and detection platforms
- Organizations facing visibility gaps across hybrid and encrypted networks

Why This Guide Matters

Industrial manufacturers operate security environments that look nothing like traditional IT-only enterprises. Production networks run legacy protocols, segmented zones, and systems that were never designed to be monitored, patched, or taken offline. At the same time, these environments are now tightly connected to IT, cloud platforms, remote access tools, and third-party service providers.

This convergence creates a visibility gap that most security programs underestimate.

When incidents occur in manufacturing environments, the impact isn't limited to data loss. It shows up as halted production lines, unsafe operating conditions, missed delivery commitments, and regulatory exposure. Yet many security teams still rely primarily on logs and endpoint agents that either do not exist on OT assets or cannot be safely deployed.

Network traffic becomes the most reliable source of truth in these environments.

This guide focuses on how Network Detection and Response helps manufacturers:

- Monitor industrial networks without deploying agents on fragile OT systems
- Detect abnormal communication between PLCs, HMIs, historians, and IT assets before it disrupts operations
- Identify lateral movement that crosses IT-OT boundaries, where many attacks escalate quietly
- Investigate incidents using session and packet-level evidence when system logs are incomplete or unavailable
- Support plant operations teams with visibility that improves security without introducing downtime

Rather than treating NDR as another security layer, the guide shows how it functions as a non-intrusive detection and investigation capability that aligns with manufacturing constraints such as uptime, safety, and regulatory compliance.

For CISOs in industrial organizations, the challenge is not whether threats exist. It is how to gain reliable detection and investigation capabilities without breaking production environments. This guide is written to address that exact problem.

Table of Contents

Chapter 1 Understanding OT Cybersecurity in Industrial Environments

Why OT Cybersecurity is a Different Problem

Operational technology refers to an environment that was built with reliability, determinism, and long-life characteristics as the primary design goals. Programmable Logic Controllers (PLCs), Distributed Control Systems (DCS), Supervisory Control and Data Acquisition (SCADA) systems, and safety systems are all considered operational technology and are designed to keep running for long periods of time (often years or decades) with very little change. Since security is not typically one of the original design goals, many assets in the operational technology space do not have native authentication controls, do not log activity, and do not use encryption.

As companies move toward digitizing their operations, many operational technology systems have become interconnected to their enterprise information technology networks, and thus, they are now being exposed to threats and vulnerabilities that were never considered when these systems were initially implemented, which increases the risk that these threats pose to the business. Once operational technology has been compromised.

through an information technology connection, the risk of attack from an information technology connection exists and will occur through a number of potential vulnerabilities, such as using compromised account credentials and exposing operational technology to malware.

Availability, integrity, and safety are the primary priorities of operational technology cybersecurity. While the confidentiality of data is important, a security breach in operational technology will generally be measured by how much production downtimes there are, the amount of damage done to the equipment, whether or not a safety issue has arisen, and whether or not there has been any exposure to regulatory risk. All of these measures lead to financial impacts and will affect operations greatly beyond the affected operational technology system.

Consider a ransomware infection that compromises an HMI or historian server. Even if PLC logic is not altered, operators may lose visibility into process states or control interfaces. In many plants, this forces a controlled shutdown. The disruption stems from loss of trust and visibility, not from physical system damage.

Buyer Checklist

- Is OT risk defined in terms of uptime, safety, and production impact?
- Do security and engineering teams share ownership of OT risk?
- Is OT cybersecurity embedded into operational risk discussions?

Chapter 2

How OT Threats Actually Impact Manufacturing Operations

Threats That Matter Most to Industrial Manufacturers

OT threats rarely resemble classic IT data breaches. The most common and damaging scenarios involve unauthorized remote access, shared credentials between IT and OT, misuse of legitimate engineering tools, and malware that disrupt control system availability.

Manufacturing continues to be the most targeted sector globally. IBM's 2023 X-Force Threat Intelligence Index identified manufacturing as the leading ransomware target for the fourth consecutive year. Importantly, attackers are no longer focused primarily on data theft. Operational disruption and extortion tied to downtime have become the dominant objectives.

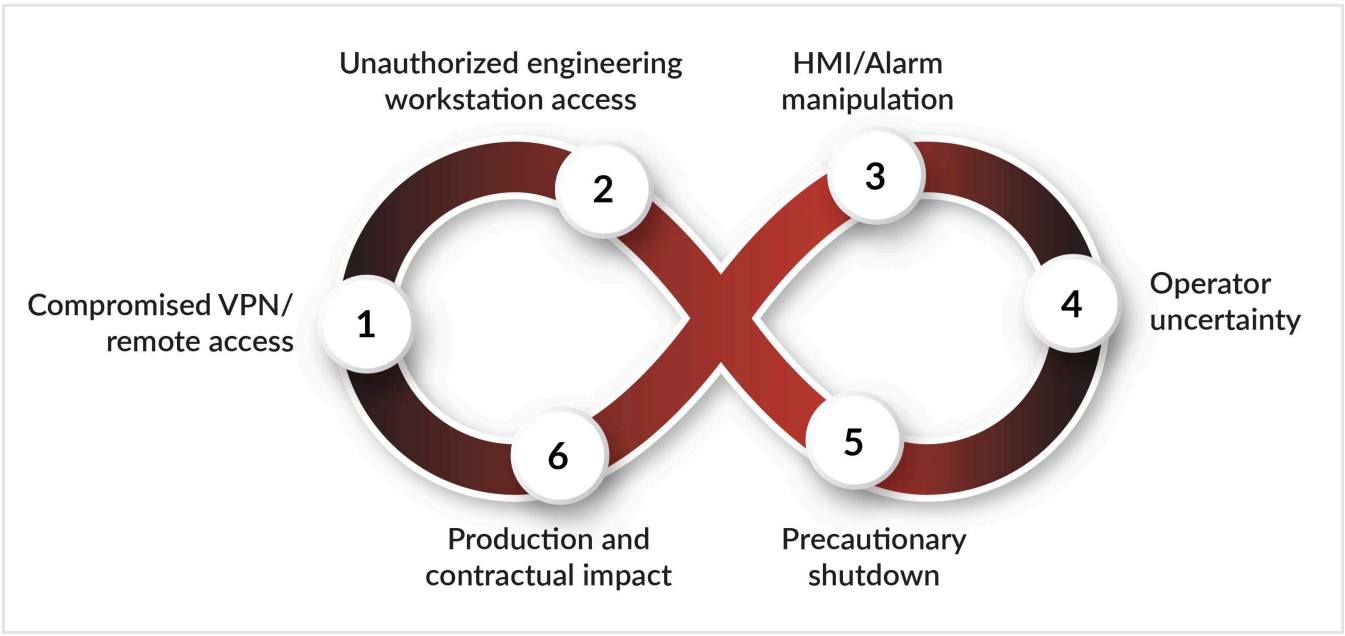
Business Impact Beyond Security

The effects of an OT incident reach far beyond the production area. Delays in production lead to unmet delivery obligations, financial penalties, regulatory examination, and harm to reputation. Recovery timelines frequently exceed those in IT environments since systems need to be verified for safety and process integrity prior to resuming operations.

Buyer Checklist

- Can unauthorized remote access into OT be detected quickly?
- Is lateral movement between OT zones visible?
- Can incidents be reconstructed without shutting down systems?

OT Attack Impact Chain



Chapter 3

OT vs IT Security - Where Traditional Models Break Down

Why IT-Centric Security Falls Short

Most IT security tools assume frequent patching, endpoint agents, and the ability to reboot systems on demand. These assumptions do not hold in OT environments. Many industrial assets cannot be patched without vendor recertification, planned outages, or risk to safety systems.

Additionally, industrial protocols behave differently from standard IT protocols. Security tools that lack protocol awareness may generate false positives or miss malicious activity entirely.

Bridging the Gap Between IT and OT

Effective OT cybersecurity integrates enterprise security measures into industrial settings without imposing IT controls on systems that are unable to accommodate them. Passive network observation, protocol-sensitive identification, and central analysis features enable OT data to be integrated into SOC processes without interfering with operations.

Buyer Checklist

- Is monitoring passive and non-intrusive?
- Are industrial protocols understood natively?
- Can OT alerts be investigated alongside IT incidents?

Chapter 4

Core Capabilities to Evaluate in an OT Cybersecurity Solution

Capabilities That Translate to Operational Value

Operational value in OT cybersecurity comes from understanding exactly what occurred on the network, not simply knowing that something triggered an alert. In an industrial environment, the difference between a benign maintenance activity and a malicious action may be a single command sent to a controller.

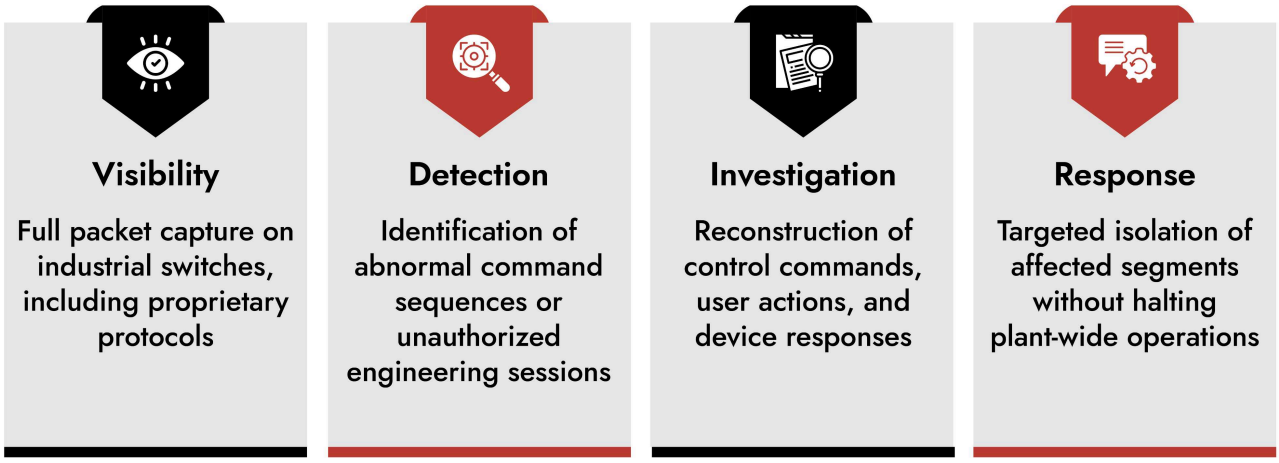
Capabilities that consistently deliver value in manufacturing environments include:

- Full packet capture that preserves command-level detail for industrial protocols
- Detection of deviations from approved control sequences, not just traffic volume changes
- Session reconstruction that allows engineers and security teams to review actions safely after the fact
- Investigation workflows that avoid live interaction with production systems

Buyer Checklist

- Does the platform provide historical visibility for investigations?
- Can detections be tuned to specific plant environments?
- Is the investigation depth sufficient to support a confident response?

Detection Capabilities That Shorten Dwell Time



In industrial environments, understanding normal network behavior is often more critical than simply flagging anomalies. Security teams gain confidence not from alert volume, but from the ability to quickly place activity in operational context, validate intent, and reach decisions without interrupting critical systems. Solutions should be judged on how effectively they turn visibility into actionable understanding, providing teams with the evidence they need to respond confidently and maintain operational continuity.

Chapter 5 Deployment Models, Architecture, and Operational Fit

Designing for Manufacturing Reality

OT environments are geographically distributed and operationally diverse. A single manufacturer may operate dozens of plants with different equipment generations, network architectures, and regulatory requirements. OT cybersecurity solutions must support centralized visibility with distributed data collection.

Operational Consideration

Security implementations must coincide with maintenance periods, support isolated or air-gapped networks, and prevent adding latency or instability. The most efficient architectures seamlessly blend into current networks and expand as operations develop.

Buyer Checklist

- Can the architecture support multi-site visibility?
- Does deployment respect segmentation and safety requirements?
- Is operational disruption minimized during rollout?

Chapter 6

Building a Business Case for OT Cybersecurity Investment

Translating Risk into Business Terms

Executive decision-makers prioritize operational resilience, safety assurance, and predictable output. Successful OT cybersecurity business cases frame risk in these terms rather than focusing on technical controls.

According to a 2024 Ponemon Institute study on cyber resilience, unplanned operational outages now represent the largest cost component of industrial cyber incidents, exceeding response and recovery costs. For large manufacturers, a single hour of downtime can result in losses ranging from hundreds of thousands to several million dollars, depending on production volume.

Metrics That Matter

- Mean time to detect OT incidents
- Mean time to investigate without disrupting operations
- Reduction in unplanned downtime and near-miss safety events

Buyer Checklist

- Are OT cyber risks quantified financially?
- Is OT security integrated into enterprise risk reporting?
- Can operational improvements be measured over time?

Chapter 7 Applying These Principles with NetWitness for OT Security

Aligning Vendor Capabilities with Buyer Requirements

This guide has intentionally focused on capabilities rather than products. When evaluating platforms, buyers should assess how well a solution delivers deep visibility, investigation, and operational alignment across both IT and OT environments.

NetWitness aligns with these requirements by extending network-level visibility, full session reconstruction, and threat detection into industrial networks without relying on agents or intrusive controls. Its approach supports forensic investigation, long-term visibility, and integration with existing SOC processes.

Why This Matters for Industrial Manufacturers

For manufacturers seeking to unify IT and OT security operations, NetWitness enables teams to investigate incidents in context, understand attacker behavior across domains, and respond without unnecessary operational disruption. This supports more confident decision-making during incidents and reduces reliance on precautionary shutdowns.

Chapter 8 Deep Dive into NetWitness for OT Security

NetWitness Architecture and OT Integration

NetWitness offers an architecture that supports both IT and OT environments without compromising production operations. Its network-level packet capture, session reconstruction, and protocol-aware detection allow security teams to see exactly what is happening in industrial networks.

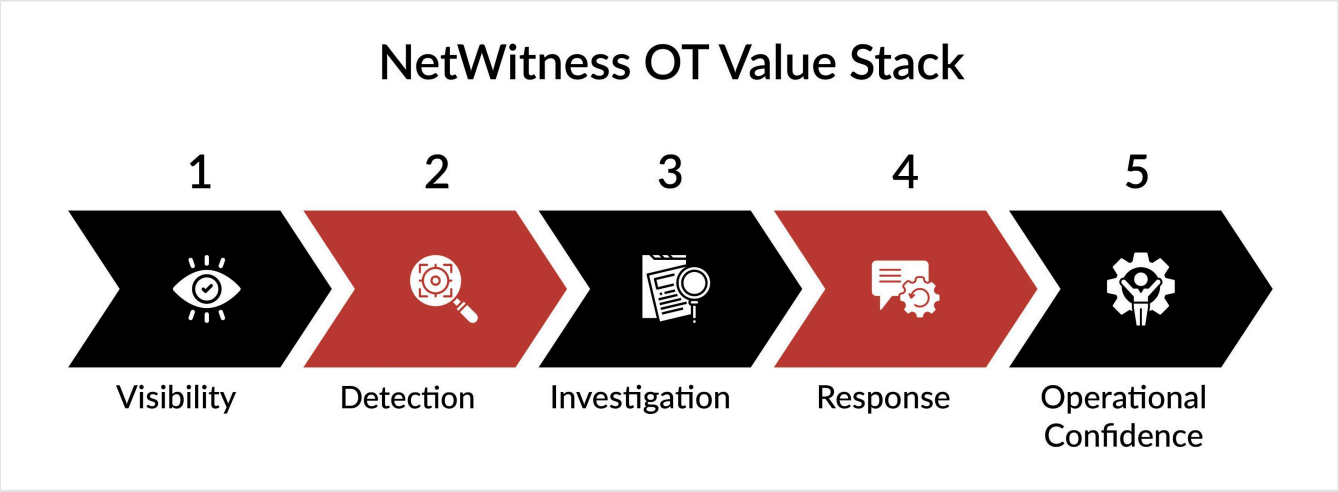
- **Full Packet Capture:** Captures command-level detail across industrial protocols, including Modbus, DNP3, Profinet, and OPC-UA.
- **Session Reconstruction:** Reconstructs activity from individual sessions to show exact operator commands and system responses.
- **Threat Detection:** Identifies deviations from expected control sequences and unauthorized engineering access.
- **Operational Integration:** Alerts and investigation data can be integrated into SOC dashboards for unified IT/OT oversight.

Key Use Cases in Manufacturing

- Detecting unauthorized remote access to OT workstations
- Investigating anomalous command sequences without halting production
- Maintaining audit trails for compliance and safety verification
- Supporting incident response while minimizing operational impact

Business Benefits

- Detecting unauthorized remote access to OT workstations
- Investigating anomalous command sequences without halting production
- Maintaining audit trails for compliance and safety verification
- Supporting incident response while minimizing operational impact



Conclusion

OT cybersecurity is no longer optional for industrial manufacturers; it is integral to operational continuity, safety, and financial resilience. Decision-makers must evaluate solutions that provide deep, protocol-aware visibility, thorough investigation workflows, and seamless integration with enterprise SOC operations. Effective platforms enable teams to detect, reconstruct, and respond to incidents without disrupting production or introducing new risks.

A successful OT cybersecurity strategy combines technical capabilities with operational alignment, ensuring that every security control contributes to uptime, process integrity, and safety compliance. Solutions like NetWitness demonstrate how integrated visibility and investigation can support these objectives, helping manufacturers transform cyber risk into manageable operational insight while protecting critical assets and business outcomes.

OT cybersecurity is no longer an operational afterthought. It is a board-level risk consideration tied directly to uptime, safety, regulatory exposure, and revenue continuity. If your manufacturing environment cannot provide evidentiary visibility and defensible response across IT and OT, the architecture requires reassessment.

NetWitness delivers full-fidelity network visibility, advanced detection engineering, and investigation workflows designed for complex industrial environments. The objective is not more alerts. It is command-level clarity, forensic depth, and coordinated response that protects production without compromising operational stability.

Connect with NetWitness to schedule an executive briefing and technical workshop tailored to your manufacturing footprint. Make your OT cybersecurity program measurable, defensible, and aligned with operational performance.

Connect with NetWitness to make your OT cybersecurity program measurable, defensible, and aligned with operational performance.

Contact Us

Contact Information

Email for customer Service
support@netwitness.com

Website
www.netwitness.com

Follow us for regular updates

NETWITNESS