EXTRAHOP

Securing Smart Manufacturing and Protecting Production Uptime

Keep critical production processes free from threats and disruption with ExtraHop RevealX™

Industry Challenges: From Production Uptime to National Security

Global manufacturing operates where digital downtime translates to immediate revenue loss and supply chain collapse. Industry 4.0 and IIoT have turned the factory floor into a hyper-connected ecosystem, making cybersecurity vital for uptime and safety. By 2026, software-defined manufacturing has turned the network into the central nervous system for every assembly line. Manufacturers now face several critical friction points:

- **The Escalation of Nation-State Sabotage and Cyber-Physical Risk:** Geopolitical actors shifted from IP theft to functional destruction. Recent major supplier breaches have demonstrated how compromised edge devices can halt global assembly lines in minutes. By striking the software supply chain, adversaries disrupt just-in-time (JIT) logistics and safety systems. Protecting production requires internal visibility to stop lateral movement before destructive commands execute on the shop floor.
- **The Identity Crisis and the IT-to-OT Gateway:** Adopting OPC UA and MQTT standards expanded the attack surface for cloud-integrated manufacturing. Actors use living-off-the-land (LOTL) tactics to subvert identity controls and mimic engineering behavior. Using stolen credentials to move from corporate IT into operational technology zones, they navigate undetected toward critical controllers. Organizations must detect this activity on the wire before production is sabotaged.
- **The Visibility Gap and the Agent Blind Spot:** Robotic arms, CNC machines, and human-machine interfaces cannot host security agents, leaving industrial traffic invisible to traditional tools. Attackers prioritize disabling EDR agents immediately after gaining a foothold in the corporate network. This creates hurdles for IEC 62443 and NIS2 frameworks, which mandate strict auditing of industrial network access and behavioral baselining.
- **Operational and Regulatory Convergence:** 2026 mandates like CMMC 2.0 and NIS2 make continuous network monitoring non-negotiable. To maintain 100% uptime and overcome tool fatigue, manufacturers must unify SOC and NOC workflows within a Zero Trust Architecture. This approach bridges the gap between security and plant operations, identifying cyber threats and operational inefficiencies before they impact the bottom line.

KEY CAPABILITIES

Depth and Breadth of NDR Performance: Monitors all network interactions by decrypting and decoding over 90+ protocols, including native support for EtherNet/IP, PROFINET, and Modbus, at speeds up to 100 Gbps to protect high-velocity production lines and automated shop floor operations.

The Definitive Data Source for the AI-Enabled SOC: RevealX powers manufacturing SOC automation with unalterable network data, eliminating investigative friction to accelerate detection and remediation.

AI-Powered Cyber Threat Detection: RevealX NDR identifies sophisticated attacks, lateral movement, and early-stage ransomware targeting critical production services and ICS applications using cloud-scale machine learning and behavioral baselining.

Unified Agentless Visibility: Automatically discovers every asset, including unmanaged OT devices like PLCs, HMIs, and robotic controllers, along with hybrid-cloud workloads, without installing software or risking system stability or production performance.

Strategic Line-Rate Decryption: Analyzes modern encrypted traffic, including TLS 1.3 and PFS, to expose hidden threats and unauthorized data staging without adding latency to time-sensitive industrial control operations.

High-Fidelity Performance Metrics: Troubleshoots complex disruptions using over 5,000 wire data metrics for deep operational insight into factory-floor latency and application performance.

Continuous Forensic Recording: Maintains an unalterable record of all network transactions to satisfy audit requirements for IEC 62443, NIS2, and CMMC 2.0, accelerating root-cause analysis and incident reconstruction.

The Solution: RevealX Network Intelligence

ExtraHop RevealX provides the network intelligence required to secure industrial IP, maintain production safety, and ensure operational continuity. By delivering a unified view of converged IT and OT environments, RevealX enables teams to detect sophisticated threats and ensure service availability across critical production lines, automated warehouses, and global supply chains.

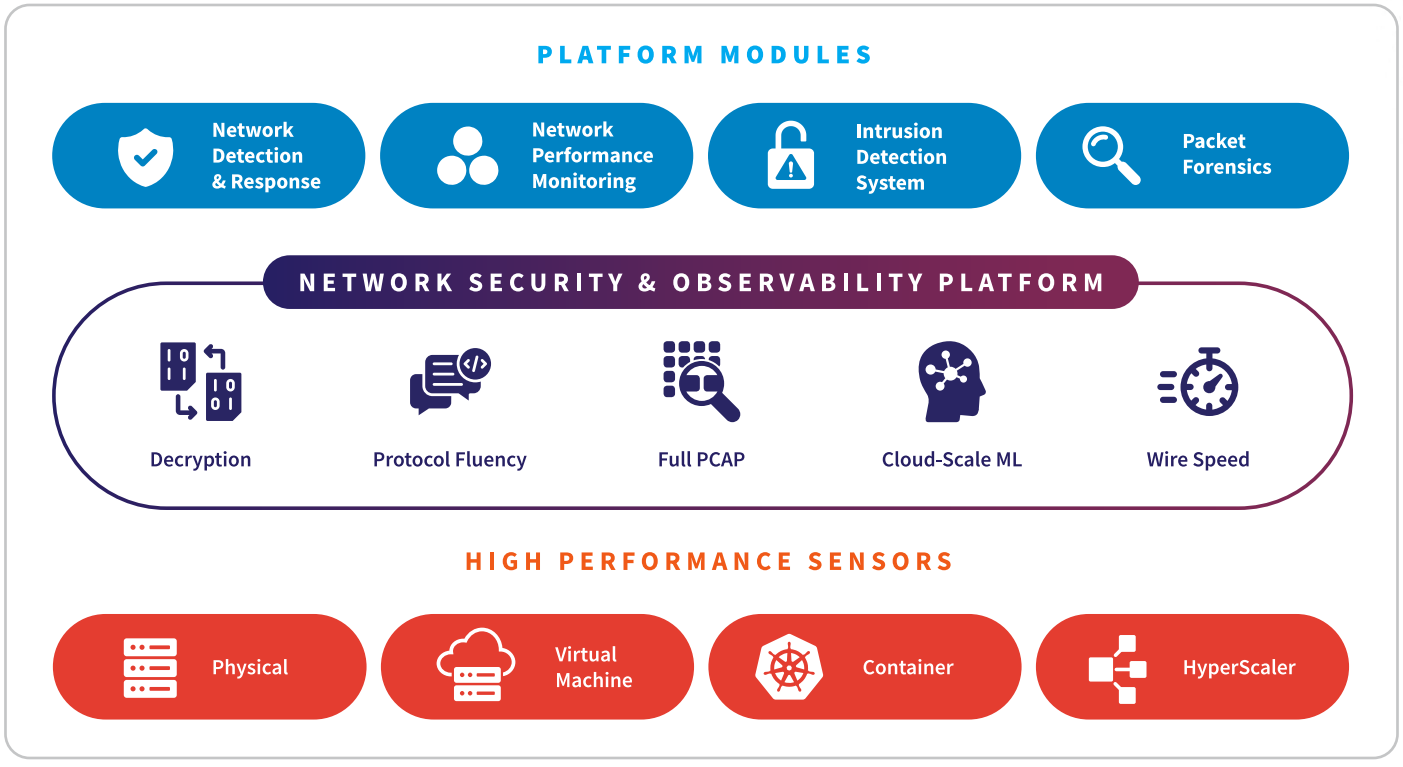
Neutralizing destructive nation-state campaigns or industrial sabotage requires stopping actors before commands execute. By monitoring the wire instead of vulnerable endpoint agents, RevealX detects the subtle lateral movement and credential abuse used to pivot from corporate networks to the factory floor. This agentless approach identifies anomalous behavior in real time, even if a maintenance connection or edge gateway is compromised. Teams can then isolate affected segments, preserving industrial control system (ICS) integrity and protecting uptime from large-scale functional disruption or ransomware-induced shutdowns.

Supporting Industry 4.0 modernization while meeting stringent regulatory demands requires complete visibility. A real-time view across assembly lines, distribution centers, and hybrid-cloud-managed sites allows teams to stay ahead of outages and breaches. Since logs and endpoint data are modifiable, the network provides the only immutable source of truth. RevealX decodes over 90+ protocols at 100 Gbps, providing persistent visibility across unmanaged PLCs, HMIs, and robotics where agents cannot be installed.

RevealX uses cloud-scale machine learning to identify attacks that evade signature-based tools. By establishing behavioral baselines, the AI detects LOTL tactics and credential abuse targeting critical shop floor controllers. A key differentiator is the line-rate decryption of TLS 1.3 and PFS, ensuring attackers cannot hide lateral movement or unauthorized data staging within encrypted industrial traffic. This provides the independent observation necessary for an industrial Zero Trust Architecture.

Integrating NDR and NPM eliminates silos between SOC and NOC workflows. Teams can troubleshoot issues ranging from production latency to active ransomware staging before functional damage occurs. This unified approach allows manufacturers to enforce robust segmentation and manage vulnerability disclosure programs for connected devices. High-fidelity wire data ensures compliance with 2026 mandates, including IEC 62443, the EU NIS2 Directive, and CMMC 2.0.

ExtraHop NDR Platform



NDR Technology Use Cases for the Manufacturing Industry

Nation-State Attacks	Detects lateral movement and exfiltration in long-term nation-state campaigns targeting global supply chains, industrial IP, and production facilities.
Threat Detection & Response	Investigates hidden threats across converged IT/OT environments, filling visibility gaps in factory-floor automation and MES where logs and agents fail.
Threat Hunting	Leverages behavioral baselining to find signature-less threats and anomalies before they impact production uptime, safety protocols, or product quality.
SOC Modernization	Unifies SOC/NOC workflows and uses AI prioritization to reduce alert fatigue, accelerating response times and efficiency for industrial service delivery.
Incident Response & Investigation	Delivers forensic visibility and unalterable records of SCADA/Industrial Protocol commands (Modbus, EtherNet/IP, PROFINET) for one-click root-cause analysis.
Lateral Movement	Uses peer-group clustering and protocol decoding to detect pivots bypassing perimeters toward SIS, critical OT segments, and engineering zones.
Cloud Workload Security	Provides agentless visibility for cloud-integrated Smart Factory workloads, discovering shadow IT and unmanaged assets across AWS, Azure, and Google Cloud.
Identity-Based Attacks	Correlates network behavior with IAM to unmask credential abuse and privilege escalation targeting high-value Jump Hosts and Engineering Workstations.
Ransomware Attacks	Identifies ransomware staging and encryption patterns to isolate hosts before exfiltration of trade secrets or JIT logistics disruption.
Unmanaged Devices	Monitors network traffic for unmanaged PLCs, HMIs, and robotic controllers that cannot support traditional security agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity when agents are disabled, ensuring visibility across legacy plant-floor hardware and HMI stations.
AI Security	Monitors generative AI and autonomous agents used for product design, supply chain optimization, or autonomous logistics in containerized cloud workloads.
Operationalizing Zero Trust	Detects policy drift and provides empirical proof that IEC 62443 zone/conduit policies and Purdue Model segmentation are effective.

NPM Technology Use Cases for the Manufacturing Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for factory-floor automation and PLC-to-HMI sessions.
Operational Resilience	Resolves infrastructure degradation before it hits production continuity, ensuring availability through proactive monitoring of mission-critical SCADA services.
Troubleshooting & Resolution	Accelerates root-cause analysis via a 3-click workflow, eliminating friction between plant operations (OT) and IT network teams.
Migrate Workloads to the Cloud	Maintains performance during MES or ERP migration by auto-mapping dependencies and using OT baselines to validate cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes, ensuring performance for IIoT gateways and Supply Chain APIs.
Forensic-Grade Investigations	Combines metadata and scalable PCAP for an unalterable record, enabling deep-dive analysis into past production outages or telemetry drops.
Application Performance Monitoring	Fills network gaps by decoding 90+ protocols (e.g., Modbus, EtherNet/IP), providing real-time insights into command processing time vs. network latency.

Manufacturing Industry Compliance & Regulatory Use Cases

Industrial Network Security	Global	IEC 62443	Validates Purdue Model and stops lateral malware. RevealX ensures conduit traffic matches security policies via continuous monitoring.
Essential Service Resilience	European Union	NIS2 Directive	Detects "living-off-the-land" attacks and unauthorized updates. RevealX provides forensic evidence and visibility for 2026 72-hour mandates.
Defense Supply Chain Integrity	United States	CMMC 2.0	Automates CUI protection. RevealX identifies exfiltration or credential abuse targeting engineering blueprints and technical specifications.
Critical Process Integrity	Global	NIST CSF 2.0	Detects unauthorized changes to Modbus, EtherNet/IP, or PROFINET. RevealX monitors protocol anomalies indicating production or safety system tampering.
Supply Chain/ Third-Party Risk	Germany / Global	Supply Chain Act (LkSG)	Monitors third-party maintenance for unauthorized pivots to shop floors, ensuring JIT logistics and production integrity are not compromised.
Operational Resilience	United Kingdom	UK CAF	Supports NIS event detection objectives. RevealX provides automated discovery and metadata history required for regulatory "Achieved" status.

Customer Benefits: Ensuring Production Resilience and Operational Continuity Across the Manufacturing Ecosystem

Visibility into network truth is the cornerstone of every modern industrial protection and operational resilience framework. Complete, real-time visibility from RevealX is vital for ensuring the sub-second response times required for factory-floor automation, CNC precision, and automated fulfillment systems. By monitoring the wire, manufacturers safeguard against cyber threats and protocol anomalies that could jeopardize production uptime, just-in-time (JIT) logistics, and broader supply chain reliability.

The transition to smart factories, Industry 4.0, and cloud-integrated manufacturing provides the agility required for rapid innovation, yet it creates exploitable blind spots in the operational technology (OT) path. RevealX enables organizations to embrace a digital-first approach while maintaining operational resilience across legacy assembly plants and distributed supply chains. By observing actual traffic flows, including EtherNet/IP, PROFINET, and Modbus, instead of relying on modifiable logs, firms gain the definitive, forensic evidence needed to satisfy stringent regulatory audits for IEC 62443, NIS2, and CMMC 2.0.

RevealX also provides essential visibility for the expanding ecosystem of unmanaged devices and third-party maintenance connections. Monitoring these unknowns from PLCs and HMIs to autonomous warehouse robotics and IIoT sensors eliminates the blind spots inherent in agent-based security. RevealX identifies lateral movement and credential abuse before they lead to the compromise of safety instrumented systems (SIS) or the exfiltration of sensitive product blueprints and industrial trade secrets. With RevealX, manufacturing firms gain continuous, real-time discovery and classification of every entity on the network to ensure that critical production and public safety remain uninterrupted.

> "With ExtraHop, we're not spending time looking for a needle in a haystack. That means we can spend more time on projects that are strategically valuable to the business. It's a win-win."
>
> IT Security Manager
> American Manufacturer

ExtraHop Can Help

ExtraHop NDR provides a critical advantage by delivering the comprehensive network intelligence required to surface sophisticated lateral movement and internal threats that legacy tools often miss.

Learn more about our successful customer deployments in manufacturing:
Leading Manufacturer
Transportation Manufacturer

Or contact us to schedule your personalized demo and security assessment.

ABOUT EXTRAHOP

ExtraHop turns the network—the enterprise's ultimate source of truth—into actionable insight to power security, performance, and resilience. Delivering superior data by design, we ensure superior defense by default.

The ExtraHop modern network detection and response (NDR) platform provides visibility that thinks, analyzing behavior to intercept evasive risks before they cause damage. We transform network noise into definitive context, enabling security teams to make faster decisions and operate at uncompromised scale.

Whether securing cloud modernization or de-risking AI adoption, ExtraHop gives global enterprises the ground truth they need to thrive.

To learn more, visit extrahop.com or follow us on LinkedIn.

EXTRAHOP®

info@extrahop.com
extrahop.com