EXTRAHOP

Securing Chemicals, Mining, and Natural Resources: Protecting Industrial Integrity and Ensuring Operational Continuity

Defend Critical Industrial Assets and Ensure Continuity with ExtraHop RevealX™

SOLUTION BRIEF

Industry Challenges: From Physical Extraction to Digital Sabotage

Chemicals, mining, and natural resources are high-consequence environments where digital failures trigger physical catastrophes. By the end of 2026, the transition to autonomous extraction, remote operations centers (ROCs), and smart chemical processing will have destroyed the traditional perimeter. Bidirectional data flow between the extraction site and the cloud creates a sprawling attack surface where one compromised sensor can disrupt global supply chains or trigger environmental disasters.

The chemicals, mining, and natural resources industries face several critical friction points:

- **The Escalation of Kinetic Risk and Sabotage:** Geopolitical actors have shifted from data theft to functional destruction. Modern threats target the IT/OT intersection to manipulate physical processes like pressure levels in chemical reactors or ventilation in deep-shaft mines. In 2024, a major conglomerate with operations in mining and chemicals was hit by a ransomware attack, which shut down IT systems across a variety of business units. In another cyberattack, a large aluminum mining and processing company was hit by a disastrous ransomware attack, which paralyzed the company's global network. Protecting these assets requires internal visibility to contain lateral movement before destructive commands reach safety systems. Without deep packet inspection, subtle shifts in command logic go undetected.
- **The Visibility Gap in Hardened OT Environments:** Industrial infrastructure relies on life-critical assets like PLCs and RTUs that cannot host security agents without risking system crashes. This agent blind spot leaves protocols like Modbus and DNP3 invisible to IT tools. This allows attackers to dwell for months, mapping high-voltage environments and preparing coordinated strikes.
- **The Myth of the Air Gap in Remote Sites:** Validating digital perimeters is a constant struggle. The air gap is frequently shattered by maintenance laptops, removable media, or supply chain compromises. Securing these systems requires nonintrusive, continuous monitoring to detect unauthorized communication across supposedly isolated zones, providing a safety net for environmental stability.
- **Regulatory Rigor and Safety Mandates:** New mandates require internal network security monitoring (INSM) to identify anomalous activity inside the perimeter. Meeting these standards, while maintaining 100% uptime, requires bridging SOC and NOC workflows. Security alerts must be contextualized with operational performance data to prevent accidental shutdowns or service disruptions during incident response.

KEY CAPABILITIES

Depth and Breadth of NDR Performance

Decodes and decrypts 90+ protocols, including Modbus and DNP3, at 100 Gbps to protect high-volume extraction and remote operations.

The Definitive Data Source for the AI-Enabled SOC

Delivers unalterable wire data to power industrial SOC automation, eliminating friction and accelerating remediation.

AI-Powered Cyber Threat Detection

Identifies lateral movement and ransomware targeting OT/ICS applications using behavioral baselining and cloud-scale machine learning.

Unified Agentless Visibility

Discovers all assets, including PLCs and RTUs, without software installs or risking stability of sensitive industrial processes.

Strategic Line-Rate Decryption

Analyzes TLS 1.3 and PFS to expose hidden threats without adding latency to time-sensitive control operations.

High-Fidelity Performance Metrics

Troubleshoots disruptions using 5,000+ metrics for deep insight into refinery latency and application performance.

Continuous Forensic Capture

Maintains unalterable transaction records to satisfy NERC CIP and safety audits, accelerating incident reconstruction.

The Solution: RevealX Network Intelligence

ExtraHop RevealX delivers the network intelligence required to secure the high-value IT networks and converged OT environments critical to chemical, mining, and natural resource operations. By providing a unified view across refineries, remote extraction sites, and corporate data centers, RevealX enables security teams to detect sophisticated threats before they impact safety or production.

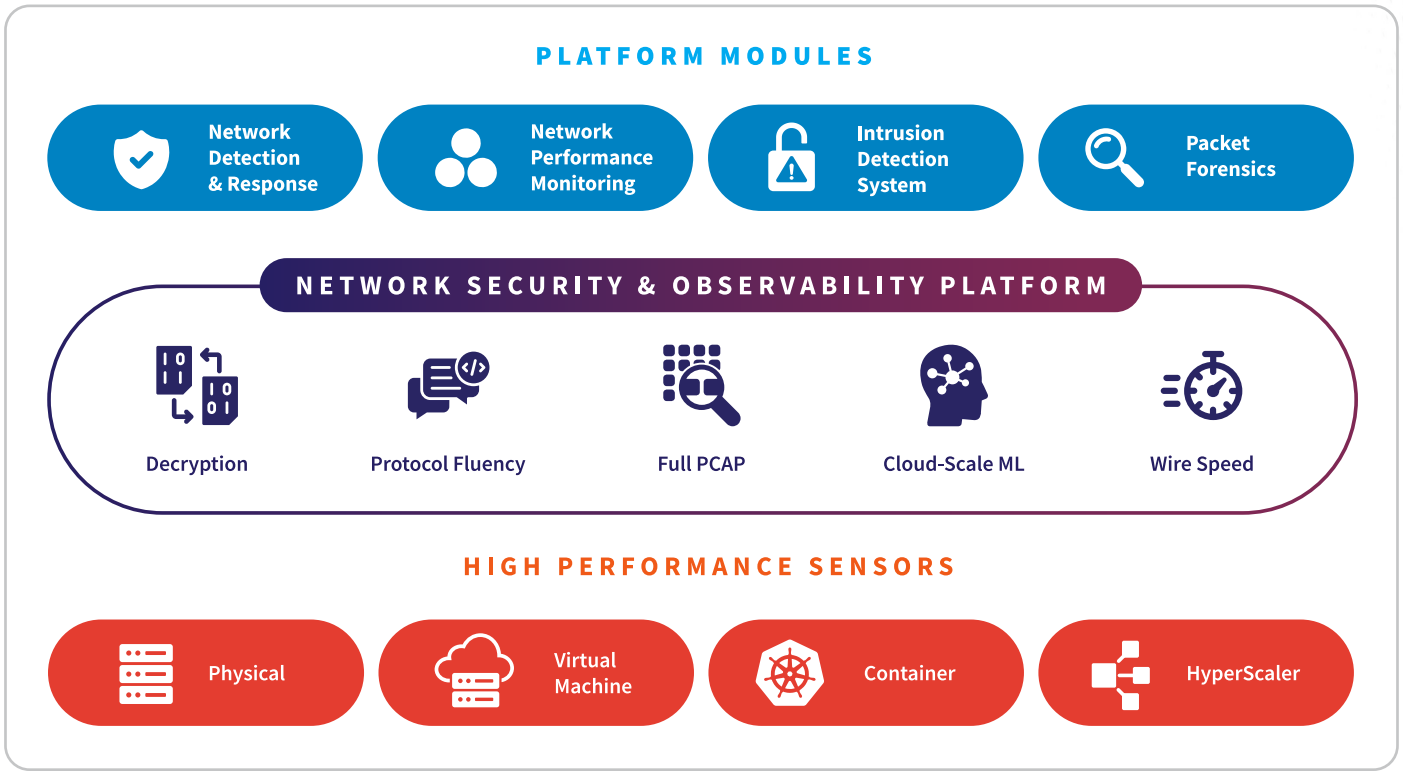
Neutralizing destructive nation-state campaigns or ransomware targeting industrial sectors requires intercepting actors before they execute malicious commands. By monitoring the wire rather than relying on vulnerable endpoint agents, RevealX detects lateral movement and credential abuse as attackers pivot from employee workstations or guest segments toward high-value engineering workstations and plant floor controllers. This agentless approach identifies anomalies in real time, ensuring that if a maintenance laptop or a remote site gateway is compromised, the breach is contained. Teams can then isolate affected segments, preserving the integrity of industrial control systems (ICS) and preventing large-scale functional disruption.

Modernizing resource extraction and chemical processing requires total network visibility to stop threats before they escalate into systemic crises. Only a real-time view across remote resource sites and processing plants allows teams to stay ahead of outages. Because log and endpoint data can be modified or disabled by persistent adversaries, the network provides the only immutable source of truth that cannot be evaded or tampered with.

RevealX provides the scale and deep packet visibility required to comply with global safety mandates and internal network security monitoring (INSM) requirements. By integrating NDR and NPM, RevealX deconstructs industrial complexity without the friction of tool sprawl or the risk of crashing sensitive controllers. This ensures that security and operations teams work from an objective ground truth rather than fragmented data silos.

Mining and chemical firms can automatically discover every network asset and map interdependencies to eliminate single points of failure. The platform uses machine learning and behavioral baselining to identify anomalous behavior in “east-west” traffic, such as unauthorized commands in Modbus or DNP3. This allows teams to immediately understand the full blast radius of an incident, accelerating remediation while maintaining an unalterable record for regulatory audit trails and forensic reconstruction.

ExtraHop NDR Platform



NDR Technology Use Cases for the Chemicals, Mining, and Natural Resources Industry

Nation-State Attacks	Provides deep visibility into lateral movement and data exfiltration, detecting long-term campaigns targeting remote operations centers and extraction site control systems.
Threat Detection and Response	Enables proactive investigation into hidden threats across converged IT/OT environments to find what logs miss within refinery management and mine-site orchestration systems.
Threat Hunting	Uncovers stealthy, signature-less threats by leveraging behavioral baselining to find anomalies in specialized industrial traffic before they impact pressure levels or ventilation systems.
SOC Modernization	Unifies SOC and NOC workflows to eliminate data silos. AI-powered prioritization reduces fatigue, accelerating response times for critical safety and production delivery.
Incident Response and Investigation	Provides forensic visibility and "three-click" investigations to determine root causes. Offers an unalterable record of network transactions, including Modbus and DNP3 commands.
Lateral Movement	Detects internal movement using peer-group clustering and protocol decoding to catch pivots bypassing perimeters toward safety instrumented systems (SIS) or engineering workstations.
Cloud Workload Security	Delivers agentless visibility to defend cloud-integrated remote operations and discover unmanaged assets across AWS, Azure, and Google Cloud environments.
Identity-Based Attacks	Correlates behavior with IAM to unmask credential abuse in real time, providing visibility into threats targeting high-value jump hosts used by maintenance contractors.
Ransomware Attacks	Identifies early-stage ransomware, such as file staging and encryption patterns, to isolate infected hosts before exfiltration of proprietary mining maps or chemical formulas.
Unmanaged Devices	Fills the visibility gap for unmanaged OT devices like PLCs, RTUs, and smart sensors by monitoring network traffic directly, as these systems cannot support agents.
EDR Evasion Detection	Out-of-band monitoring identifies malicious activity even if agents are disabled, ensuring persistent visibility across legacy plant-floor hardware and HMI stations.
AI Security	Monitors interactions with generative AI used for predictive maintenance or automated resource discovery that could be exploited to disrupt production.
Operationalizing Zero Trust	Acts as the independent observer, detecting policy drift and providing proof that network segmentation and air-gap policies are effective across remote extraction sites.

NPM Technology Use Cases for the Chemicals, Mining, and Natural Resources Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions, providing visibility into latency for remote-controlled machinery and automated refinery sessions.
Operational Resilience	Reduces disruption impact by resolving infrastructure degradation before it hits production continuity. Ensures availability for mission-critical SCADA and monitoring services.
Troubleshooting and Resolution	Accelerates root-cause analysis via a 3-click workflow from metrics to packets, eliminating friction between field operations (OT) and IT network teams.
Migrate Workloads to the Cloud	Maintains performance during remote operations center migration by auto-mapping dependencies and using OT baselines to validate successful cloud delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes, ensuring performance for critical services like environmental monitoring and load-out APIs.
Forensic-Grade Investigations	Combines long-term metadata with scalable PCAP for an unalterable record, enabling deep-dive analysis into past production outages or telemetry drops.
Application Performance Monitoring	Complements APM by decoding and decrypting 90+ protocols, including Modbus and IEC 61850, to provide insights into command processing time versus network latency.

Chemicals, Mining, and Natural Resources Industry Compliance & Regulatory Use Cases

Industrial Control Security	Global	ISA/IEC 62443	Automates the discovery and monitoring of "east-west" traffic within industrial zones. RevealX identifies unauthorized station-to-station communication.
Chemical Facility Security	United States	CFATS (CSAT 2.0)	Fulfills requirements for protecting safety-related digital systems. RevealX uses non-intrusive taps to monitor secure zones without agent interference.
Critical Process Resilience	European Union	NIS2	Supports critical entities by detecting "living-off-the-land" attacks. RevealX provides forensic evidence for rapid regulatory incident disclosure.
Mining Safety and Surveillance	Global	MMS / ISO 27001	Validates "air-gapped" integrity and digital design bases for remote sites. RevealX inspects packets for protocol anomalies or unauthorized cross-zone communications.
Pipeline & Flow Infrastructure	United States	TSA SD 02D	Provides continuous monitoring and segmentation analysis required to protect critical pressure and flow control systems in midstream operations.
Cybersecurity Maturity	Global	NIST CSF 2.0 / C2M2	Powers "Detect" and "Respond" functions. RevealX maps interactions to help organizations move from "ad-hoc" to "managed" maturity levels.
Environmental and Safety Data	United Kingdom	UK CAF	Supports "Detecting Cyber Security Events" objectives. RevealX provides automated discovery needed for Operators of Essential Services to reach "achieved" status.

Customer Benefits: Protecting Industrial Integrity and Ensuring Operational Continuity

Visibility into network truth is the cornerstone of protecting modern chemical, mining, and natural resource operations. ExtraHop RevealX provides the real-time insights required for remote operations centers, chemical refinery automation, and environmental safety monitoring. By monitoring the wire, firms safeguard against cyber threats and protocol anomalies that jeopardize production uptime, worker safety, and broader brand reputation.

The shift toward autonomous mining and smart chemical processing creates exploitable blind spots in the OT path. RevealX secures these modern architectures and legacy plants by observing actual traffic flows, including Modbus, DNP3, and IEC 61850, rather than relying on modifiable logs. This provides the definitive forensic evidence needed to satisfy global regulatory audits for ISA/IEC 62443, CFATS, and NIS2.

RevealX also secures the expanding ecosystem of unmanaged IoT devices, from remote sensors and IP cameras to specialized PLC controllers that agent-based tools miss. It identifies lateral movement and credential abuse before they compromise safety instrumented systems (SIS) or result in the exfiltration of sensitive proprietary data. Through continuous, real-time discovery and classification of every network entity, RevealX ensures that critical material extraction and processing remain uninterrupted.

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:
EMEA Industrial Leader
Tarrant Regional Water District

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

> "ExtraHop gives us a holistic view of any situation and the ability to understand how each event impacts all the connected systems. This is a major advantage for us."

OT SECURITY SPECIALIST
European Company

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