EXTRAHOP

Securing Critical Infrastructure and Ensuring Grid Resilience

Keep Critical Grid Operations Free From Threats and Disruption with ExtraHop RevealX™

Industry Challenges: From Grid Modernization to National Security

Energy grids are high-consequence environments where digital failures cause physical catastrophe. By 2026, the shift to renewables and microgrids will have destroyed the traditional perimeter. Bidirectional power flow creates a sprawling attack surface where one compromised sensor can trigger systemic load shedding or a total blackout. Utilities face several critical friction points:

- **The Escalation of Nation-State Sabotage and Kinetic Risk:** Geopolitical actors shifted from data theft to functional destruction and grid weaponization. Modern threats target the IT/OT intersection to manipulate physical processes. Protecting these assets requires internal visibility to contain lateral movement before destructive commands reach circuit breakers, turbines, or refinery safety systems. Without deep packet inspection of industrial protocols, subtle shifts in command logic go undetected by traditional security layers.
- **The Visibility Gap in Specialized OT and ICS Environments:** Energy infrastructure relies on life-critical assets like programmable logic controllers (PLCs) and remote terminal units (RTUs) that cannot host security agents without risking system crashes. This agent blind spot leaves protocols like DNP3, IEC 61850, and Modbus invisible to traditional IT tools. This allows attackers to dwell for months, mapping high-voltage environments and preparing coordinated strikes undetected by perimeter defenses.
- **The Myth of the Air Gap and Transient Assets:** In nuclear and high-consequence environments, validating digital perimeters is a constant struggle. The air gap is frequently shattered by maintenance laptops, removable media, or supply chain compromises. Ensuring that critical systems remain secure requires nonintrusive, continuous monitoring to detect unauthorized communication across supposedly isolated zones, providing an essential safety net for reactor stability and safety-critical functions.
- **Regulatory Rigor and the INSM Mandate:** New mandates like NERC CIP-015 explicitly require Internal Network Security Monitoring (INSM) for power grids to identify anomalous activity inside the perimeter. Meeting these standards while maintaining 100% uptime requires a unified approach bridging SOC and NOC workflows. Security alerts must be contextualized with operational performance data to prevent accidental power blackouts or service disruptions during incident response.

KEY CAPABILITIES

Depth and Breadth of NDR Performance

Monitors all network interactions by decrypting and decoding over 90+ protocols, including native support for DNP3, IEC 61850, and Modbus, at speeds up to 100 Gbps to protect high-voltage transmission and high-value distribution automation.

The Definitive Data Source for the AI-Enabled SOC

RevealX provides the high-fidelity wire data required to power the next generation of Energy SOC automation applications and defenses. By delivering unalterable ground truth, RevealX eliminates investigative friction and dramatically accelerates the path from detection to remediation.

AI-Powered Cyber Threat Detection

RevealX NDR identifies sophisticated attacks, lateral movement, and early-stage ransomware targeting critical grid 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 and RTUs, along with hybrid cloud workloads, without installing software or risking system stability or operational 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 grid control operations.

High-Fidelity Performance Metrics

Troubleshoots complex disruptions and verifies service level agreements (SLAs) using over 5,000 wire data metrics for deep operational insight into substation latency and application performance.

Continuous Forensic Capture

Maintains an unalterable record of all network transactions to satisfy audit requirements for NERC CIP 015 and NRC RG 5.71, accelerating root-cause analysis and incident reconstruction.

The Solution: RevealX Network Intelligence

ExtraHop RevealX delivers the network intelligence needed to secure critical infrastructure and maintain energy continuity. By providing a unified view of converged IT and OT environments, RevealX enables teams to detect sophisticated threats across grid services, generation assets, and midstream operations.

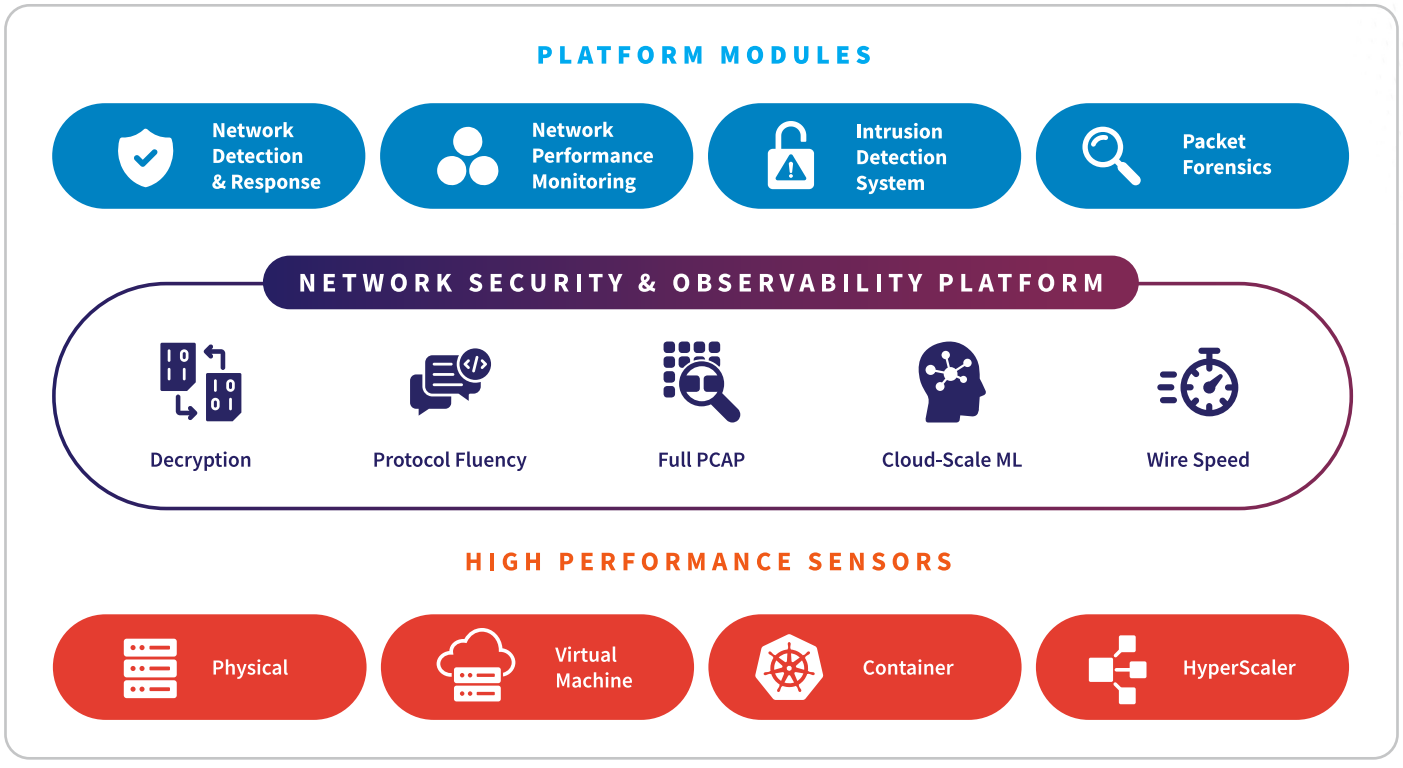
Neutralizing destructive nation-state threats requires intercepting actors before they execute malicious commands. By monitoring the wire rather than relying on vulnerable agents, RevealX detects lateral movement and credential abuse as attackers pivot from corporate networks to the plant floor. This agentless approach identifies anomalies in real time, even if a maintenance laptop or substation gateway is compromised. Teams can then isolate affected segments, preserving industrial control system (ICS) integrity and preventing large-scale functional disruption or blackouts.

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

RevealX provides the scale and deep packet visibility required to comply with mandates like NERC CIP-015, NRC RG 5.71, and NEI 08-09. By combining NDR with performance monitoring, RevealX deconstructs OT complexity without the friction of tool sprawl or the risk of crashing sensitive controllers. This ensures security and operations teams operate from an objective ground truth rather than fragmented data silos.

Utilities can automatically discover IT and OT assets and map interdependencies to eliminate single points of failure. The platform uses machine learning to identify anomalous behavior in east-west traffic, such as unauthorized commands in DNP3 or IEC 61850. This allows teams to immediately understand the full blast radius of an incident, focusing remediation while maintaining an unalterable record for NERC CIP audit trails and forensic reconstruction.

ExtraHop NDR Platform



NDR Technology Use Cases for the Energy Industry

Nation-State Attacks	Provides deep visibility into lateral movement and data exfiltration, detecting long-term nation-state campaigns targeting bulk electric system (BES) assets and transmission control centers.
Threat Detection & Response	Enables proactive investigation into hidden threats across converged IT/OT environments to find what logs are missed within substation automation and energy management systems (EMS).
Threat Hunting	Uncovers stealthy, signature-less threats by leveraging behavioral baselining to find anomalies that evade alerts before they impact grid frequency or voltage regulation.
SOC Modernization	Unifies SOC and NOC workflows to eliminate data silos. AI-powered prioritization reduces alert fatigue, accelerating response times for critical utility service delivery.
Incident Response & Investigation	Provides forensic visibility and "one-click" investigations to determine root causes. Offers an unalterable record of network transactions, including SCADA and industrial protocol commands.
Lateral Movement	Detects internal movement using peer-group clustering and protocol decoding to catch pivots bypassing perimeters toward the electronic security perimeter (ESP) or safety systems (SIS).
Cloud Workload Security	Delivers agentless visibility to defend cloud-integrated Smart Grid workloads 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 and engineering workstations.
Ransomware Attacks	Identifies early-stage ransomware, such as file staging and encryption patterns, to isolate infected hosts before exfiltration of critical infrastructure blueprints or NERC-protected data.
Unmanaged Devices	Fills the visibility gap for unmanaged OT devices like PLCs, RTUs, and IEDs by monitoring network traffic directly, as these mission-critical 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, load forecasting, or automated grid balancing that could be exploited to disrupt service.
Operationalizing Zero Trust	Acts as the independent observer in the Zero Trust loop, detecting policy drift and providing proof that network segmentation, ESP boundaries, and air-gap policies are effective.

NPM Technology Use Cases for the Energy Industry

Performance Monitoring	Uses high-fidelity telemetry to troubleshoot disruptions. Provides visibility into latency and throughput for substation automation and remote terminal unit (RTU) sessions.
Operational Resilience	Reduces disruption impact by resolving infrastructure degradation before it hits grid continuity. Ensures availability through proactive monitoring of mission-critical SCADA services.
Troubleshooting & Resolution	Accelerates root-cause analysis via a 3-click workflow from metrics to packets, eliminating friction between grid operations (OT) and IT network teams.
Migrate Workloads to the Cloud	Maintains performance during Energy Management System (EMS) migration by auto-mapping dependencies, using OT baselines to validate successful cloud-integrated delivery.
Monitor Critical Workloads	Provides deep L2-L7 visibility into high-value apps and Kubernetes environments. Ensures performance for critical services like AMI gateways and load forecasting APIs.
Forensic-Grade Investigations	Combines long-term metadata with scalable PCAP for an unalterable record, enabling deep-dive analysis into past grid outages or intermittent telemetry degradations.
Application Performance Monitoring	Complements APM by filling network gaps, decoding 90+ protocols, including DNP3 and IEC 61850, to provide real-time insights into command processing time versus network latency.

Energy Industry Compliance & Regulatory Use Cases

Internal Network Security	North America	FERC 887 / NERC CIP-015	Automates continuous monitoring of "east-west" traffic within electronic security perimeters. RevealX identifies lateral movement and unauthorized station-to-station communication, bypassing traditional defenses.
Nuclear Digital Protection	United States	NRC RG 5.71	Fulfills NRC requirements for protecting safety-related digital systems. RevealX uses non-intrusive taps to monitor secure zones, ensuring isolation without active scanning or agent interference.
Air-Gap System Integrity	United States	NEI 08-09	Validates "air-gapped" integrity and digital design bases. RevealX inspects packets for protocol anomalies or unauthorized cross-zone communications, indicating breaches of logical or physical isolation.
Pipeline Infrastructure Safety	United States	TSA SD 02D	Addresses TSA performance-based mandates for pipelines. RevealX provides continuous monitoring and segmentation analysis required to protect critical pressure and flow control systems.
Essential Service Resilience	European Union	NIS2	Supports critical entities by monitoring update channels and detecting "living-off-the-land" attacks. RevealX provides forensic evidence and line-rate visibility for rapid regulatory incident disclosure.
Critical Process Detection	United Kingdom	UK CAF	Supports "Detecting Cyber Security Events" objectives. RevealX provides automated event discovery and monitoring needed for Operators of Essential Services (OES) to reach "achieved" status.
Grid Maturity Assessment	Global	C2M2	Provides telemetry for US DOE C2M2 and Australian AESCSF. RevealX maps interactions to help organizations move from "ad-hoc" to "managed" maturity levels in threat detection.

Customer Benefits: Ensuring Grid Resilience and Operational Continuity Across the Energy Ecosystem

Visibility into network truth is the cornerstone of modern grid protection. RevealX provides the real-time insights required for substation automation, load balancing, and pipeline leak detection. By monitoring the wire, utilities safeguard against cyber threats and protocol anomalies that jeopardize local stability and bulk electric system (BES) reliability.

The shift to smart grids and renewables creates exploitable blind spots in the OT path. RevealX secures legacy plants and distributed resources by observing actual traffic, including DNP3, IEC 61850, and Modbus, rather than modifiable logs. This provides the definitive forensic evidence needed to satisfy NERC CIP 015, TSA SD 02D, NRC RG 5.71, and NIS2 mandates.

RevealX also secures the unmanaged ecosystem of Intelligent Electronic Devices (IEDs) and SCADA sensors that agent-based tools miss. It identifies lateral movement and credential abuse before they compromise safety instrumented systems (SIS) or expose sensitive grid blueprints. Through continuous, real-time discovery and classification, RevealX ensures that critical power delivery and fuel transport remain uninterrupted.

> "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
Central Europe's Leading Electricity Company

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 energy:
American Gas Retailer

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