EXTRAHOP

EXTRAHOP REVEALX™

Protect grid operations first. Pass the CIP-015 audit.

Continuous, fully passive monitoring inside the Electronic Security Perimeter. No agents, no taps into control logic, no operational risk.

The Mandate: What CIP-015-1 Requires

For years, NERC CIP focused on the perimeter, the north-south traffic crossing the Electronic Security Perimeter (ESP). That approach left a critical blind spot. Once an adversary is inside a trusted zone, they use the environment's own protocols to move laterally, escalate privileges, and issue commands. Perimeter tools never see it.

FERC Order No. 887 directed NERC to close that gap. The result is CIP-015-1, Cyber Security: Internal Network Security Monitoring (INSM), the first NERC standard to mandate continuous monitoring of east-west traffic inside the ESP.

The standard imposes three enforceable requirements on all high-impact Bulk Electric System (BES) Cyber Systems and medium-impact BES Cyber Systems with External Routable Connectivity (ERC):

- **R1 · Collect, detect, and analyze**
  Implement risk-based network data feeds (R1.1), detect anomalous activity (R1.2), and evaluate it to determine whether action is required (R1.3).
- **R2 · Retain**
  Retain INSM data associated with anomalous activity at least until the R1.3 evaluation and resulting actions are complete.
- **R3 · Protect**
  Protect collected and retained INSM data against unauthorized deletion or modification.

Compliance deadlines are firm. **October 1, 2028** applies to high-impact BES Cyber Systems and medium-impact systems with ERC. **October 1, 2030** applies to the remaining medium-impact BES Cyber Systems with ERC. Regulatory expansion is already underway: CIP-015-2 extends INSM to EACMS and PACS outside the ESP, adds Shared Cyber Infrastructure (SCI), and shifts to broader "Cyber Systems" language.

These are not simple last-minute deployments. Energy organizations need time to assess coverage gaps, design monitoring architecture, align security and operations teams, and build the evidence processes auditors will expect. The planning window is open now.

What This Means for Grid Operations

Grid operations leaders have three non-negotiable priorities: keep the system running, keep it safe, and don't introduce new risks. Every security decision gets measured against those standards.

No operational risk

Any solution that touches PLCs, RTUs, relays, or HMIs is a non-starter. RevealX is agentless and fully out-of-band. It analyzes a mirror copy of network traffic via SPAN or TAP, never sits in-line, and cannot disrupt a process. It deploys without downtime.

Resilience

The threats INSM is designed to catch, including lateral movement, unauthorized industrial commands, and abnormal device behavior inside substations and generation plants, are precisely the precursors to blackouts and sabotage. Early detection stops trouble before it spreads.

Uptime

Security and operations teams should not be fighting over different tools. RevealX surfaces both security threats and performance issues, including latency, errors, and failing links, from a single platform, giving the SOC and NOC one shared source of truth.

Fits air-gapped environments

RevealX can run a curated set of machine learning detectors on-prem with no cloud dependency, so it works in air-gapped, sovereign, and sensitive substation environments that cannot send traffic to the cloud.

Built for the People Who Run the Grid

Speak your protocols

RevealX decodes 90+ protocols, including OT protocols such as DNP3, Modbus, and BACnet, providing native visibility into substations, generation plants, and unmanaged OT devices that IT-only tools cannot reach.

See the whole picture

RevealX auto-discovers and maps every communicating device, including assets you did not know were talking, so you have an accurate, continuously updated inventory rather than a point-in-time snapshot that drifts the moment something changes.

Nothing hides in encryption

RevealX decrypts encrypted protocols, including TLS 1.3, Kerberos, NTLM, and SMB3, so an attacker cannot use encrypted internal traffic as cover. The east-west blind spot closes even for threats hiding inside legitimate-looking sessions.

Detection that can stay on-prem

Behavioral machine learning can run without sending data off-site.

Fewer tools, fewer taps

RevealX consolidates network detection and response with network performance monitoring in a single platform. Because one high-capacity sensor does the work of several, you also need fewer packet brokers and taps, which cuts cost and complexity for the data center team. Fewer tools in CIP scope means less to deploy, maintain, audit, and defend to your Regional Entity.

Future proofed

CIP-015-2 is already in motion, expanding INSM to EACMS, PACS, and Shared Cyber Infrastructure outside the ESP. RevealX is designed for that expanded scope, with no rip-and-replace when the next standard arrives.

How RevealX Satisfies the Three Requirements

R1.1 · Collect network data feeds inside the ESP

RevealX deploys agentless and out-of-band, collecting traffic from SPAN, TAP, and packet-broker connections at line rates up to 100 Gbps with zero impact on control-system performance. It auto-discovers every communicating device, including unmanaged OT assets like PLCs and RTUs, and decodes 90+ protocols including DNP3, BACnet, and Modbus, so feeds reflect actual operational communications.

> **Audit evidence:** Device inventory and communication maps; documented sensor placement per ESP; protocol and transaction records demonstrating the breadth of monitored connections.

R1.2 · Detect anomalous network activity

Behavioral machine learning establishes a baseline of normal communications and flags deviations, catching activity that has bypassed perimeter controls. That detection can run on-prem with no requirement for a cloud connection, which matters for air-gapped and sovereign grid environments. Multiple complementary detection layers cover behavioral ML, network-indicator detections, routinely-exploited-vulnerability detections, emerging-exploit detections, and signature-based malware detection. RevealX detects lateral movement, credential abuse, privilege escalation, and unauthorized external connections.

> **Audit evidence:** Time-stamped detection records with MITRE ATT&CK mapping; baseline definitions; tuning history demonstrating an operating detection capability.

R1.3 · Evaluate anomalous activity to determine action

Context-enriched detection cards correlate the who, what, where, and when of an event, with associated transaction records and packets one or two clicks away. Guided investigation workflows reach ground truth in three clicks or fewer and map blast radius to the specific assets involved. Native integrations push enriched detections into SIEM, SOAR, and ticketing tools so evaluation feeds existing incident-response and CIP-008 processes.

> **Audit evidence:** Investigation timelines and a detection-to-decision audit trail; documented disposition of each evaluated event; linkage from detection to IR or ticketing record.

R2 · Retain

RevealX provides continuous, always-on full packet capture (PCAP) with a scalable repository that extends modularly to petabytes as lookback requirements grow. Transaction records are retained for up to 365 days. Detections, records, and packets are indexed together, making it straightforward to retain exactly the data tied to a given anomaly through the close of the R1.3 evaluation. System-generated retention reports with timelines satisfy M2 evidence requirements.

> **Audit evidence:** Retention configuration and policy reports; system-generated reports showing retained data with timelines tied to specific detections; demonstration that anomaly-linked PCAP persists through evaluation.

R3 · Protect

RevealX's out-of-band architecture keeps collection and stored evidence off the production OT path, reducing exposure to tampering from the monitored environment. Role-based access control governs who can view and act on INSM data and supporting packets. Immutable, packet-level records provide a defensible, tamper-evident source of truth. Detailed access and activity logging demonstrates evidence integrity to auditors.

> **Audit evidence:** RBAC and access-control configuration; audit logs of access to INSM data; architecture documentation showing separation and integrity controls.

KEY PROOF POINTS

- Line-rate analysis, including encrypted traffic: up to 100 Gbps
- Agents on control-system assets: zero
- Protocols decoded: 90+, including DNP3, BACnet, and Modbus
- Encrypted protocols decrypted: TLS 1.3, Kerberos, NTLM, SMB3
- Machine learning: runs on-prem, no dedicated appliance, no cloud dependency
- Transaction record lookback: 365 days
- Detection to ground truth: 3 clicks or fewer
- Packet repository scalability: petabytes

Start your internal network security monitoring program now

The earlier you map coverage and build evidence, the smoother the audit and the more resilient the grid. A phased approach helps manage deployment complexity across multi-site environments.

STEP 1	STEP 2	STEP 3
Readiness workshop	**Scoped RevealX demo**	**Evidence and rollout plan**
Map your current visibility against R1 through R3 and identify ESP coverage gaps. Understand where your sensor placement needs to go.	See detection, retention, and evidence capabilities in a substation or generation context relevant to your environment.	Build the documentation and deployment path to the 2028 deadline, including the evidence processes auditors will expect.

About ExtraHop

ExtraHop is a global leader in network detection and response (NDR). ExtraHop RevealX turns network traffic, including the encrypted traffic most tools can't see, into clear, real-time evidence of what's happening across the environment, so security and operations teams can detect threats early, investigate with proof, and act fast.

The RevealX platform runs on a single all-in-one sensor that delivers NDR, network performance monitoring, IDS, and packet forensics at up to 100 Gbps. It decodes 90+ protocols and decrypts encrypted protocols including TLS 1.3, SMB3, Kerberos, and NTLM, and produces pre-correlated context across assets, identities, behaviors, and threats. The same sensor feeds both an agentic SOC and an agentic NOC from one investment, removing the tool sprawl and blind spots that fragmented architectures leave behind.

For energy organizations, RevealX is built for the complexity of converged IT and OT. It is passive and agentless, adding zero risk to fragile control-system assets while delivering the behavioral detection, packet-level forensics, and audit-ready evidence that NERC CIP-015-1 now requires. Its machine learning can run on-prem with no dedicated appliance and no cloud dependency, so it fits air-gapped and sovereign environments. The same sensor that closes the east-west monitoring gap inside the ESP also supports investigation, performance assurance, and compliance across the enterprise.

ExtraHop is recognized across major analyst evaluations, including the Gartner Magic Quadrant for Network Detection and Response, the Forrester Wave for Network Analysis and Visibility Solutions, the IDC MarketScape for Network Detection and Response, and the GigaOm Radar for NDR.

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

EXTRAHOP®

info@extrahop.com
extrahop.com