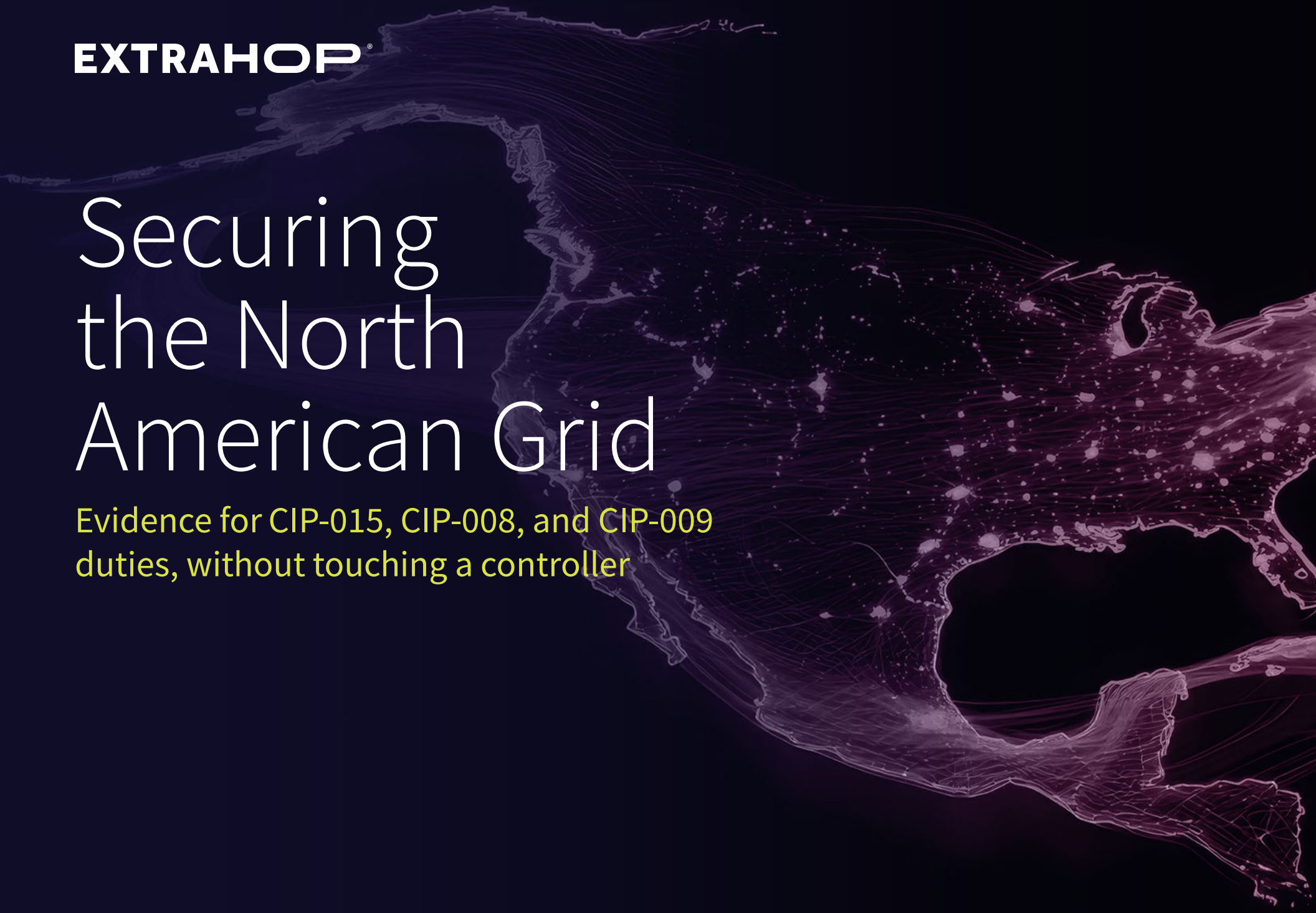
EXTRAHOP

Securing the North American Grid

Evidence for CIP-015, CIP-008, and CIP-009 duties, without touching a controller



What's in This eBook

The Regulatory Picture
One Standard, Three Compliance Waves 3

The Size of the Problem
What the Public Record Already Shows 4

Internal Monitoring Becomes Mandatory
What It Requires, and What Answers It 5

Scope Reaches Beyond the ESP
What It Requires, and What Answers It 7

Applicability is Narrower Than the Whole Estate
What It Requires, and What Answers It 8

Notification Runs on a One-Hour Clock
What It Requires, and What Answers It 9

Recovery Plans Need Testing Evidence
What It Requires, and What Answers It 10

Pipeline and Nuclear Operators Carry More
Where It is Mapped 11

The Solution
One Platform, Two Disciplines 12

Key Capabilities
Nine Capabilities, Tagged by Product 13

Where the Regions Differ
Where North America Differs from Europe 14

Sources, and How to Start
ExtraHop Can Help. 14

The Regulatory Picture

One Standard, Three Compliance Waves

North American electricity operators face a new internal monitoring standard on a fixed schedule. FERC **Order No. 887** found the CIP standards "focused on perimeter-based security with limited internal security controls" and directed NERC to close that. **Order No. 907** approved **CIP-015-1** on June 26, 2025, and FERC approved **CIP-015-2** by letter order on August 10, 2026, extending monitoring beyond the Electronic Security Perimeter.

The Compliance Clock

Oct 1, 2028	First compliance date	CIP-015-1 at Control Centers and backup Control Centers identified under CIP-002-5.1(a) R1.1 and R1.2.
Oct 1, 2030	Non-Control-Center assets	CIP-015-1 at medium-impact BES Cyber Systems with ERC away from Control Centers, 24 months after the effective date.
Oct 1, 2031	Final CIP-015-2 milestone	Associated EACMS, PACS, and Shared Cyber Infrastructure at non-Control-Center assets. CIP-015-2 itself takes effect October 1, 2029.

CIP-015 becomes enforceable on October 1, 2028, which places the architecture decision in the 2027 and 2028 budget cycles.



The Size of the Problem

What the Public Record Already Shows

Destructive Attacks Have Already Landed

Six federal agencies documented Iranian-affiliated actors disrupting programmable logic controllers across the Energy, Water, and Government Facilities sectors from March 2026. The actors reached internet-exposed controllers through the vendor's own engineering software, then altered HMI and SCADA displays. Victims reported operational disruption.

CISA, NSA, and the FBI Name OT Visibility

CISA, the NSA, and the FBI tell owners to collect network traffic between operational technology assets wherever those assets produce non-standard logs or none at all. The same advisory records Volt Typhoon holding footholds inside victim IT environments for at least five years.

Agents Cannot Reach These Assets

IEDs, RTUs, protection relays, and serial port servers have no capacity to host software. NERC names equipment technical feasibility limitations among the conditions that worsen bulk power system vulnerabilities. Monitoring the wire rather than the device is what makes the estate observable at all.

The Monitored Estate Keeps Growing

NERC brought 449 inverter-based resource owners and operators onto the Compliance Registry effective May 15, 2026, covering 531 facilities. Of those, 322 registered for the first time.



Obligation 1 of 6

Internal Monitoring Becomes Mandatory

CIP-015-1 R1 requires documented processes for internal network security monitoring that provide methods for detecting and evaluating anomalous network activity. R1.1 requires network data feeds selected "using a risk-based rationale."

WHAT IT REQUIRES, AND WHAT ANSWERS IT

	THE REQUIREMENT	HOW REVEALX CONTRIBUTES
Internal network security monitoring CIP-015-1 – R1, Part 1.1	Documented processes for internal network security monitoring of networks protected by the ESP of high-impact BES Cyber Systems and medium-impact BES Cyber Systems with ERC, providing methods for detecting and evaluating anomalous network activity. Part 1.1 requires network data feeds implemented "using a risk-based rationale."	Agentless monitoring of network interactions across the applicable systems. The risk-based rationale stays the entity's: RevealX™ collects from the feeds the entity selects, and the deployment record supports measure M1.
Detecting anomalous activity CIP-015-1 – R1, Part 1.2	One or more methods to detect anomalous network activity using the network data feeds from Part 1.1.	Real-time behavioral machine learning and baselining surface signature-less east-west activity, including unauthorized commands in DNP3 or IEC 61850, lateral movement, and credential abuse.
Evaluating anomalous activity CIP-015-1 – R1, Part 1.3	One or more methods to evaluate anomalous network activity detected in Part 1.2 to determine further actions.	One-click investigation runs from detection to packets, and RevealX NPM metrics sit beside the same record, so a team can judge whether an anomaly is an attack or a fault before it acts.

	THE REQUIREMENT	HOW REVEALX CONTRIBUTES
Retention of anomalous-activity data CIP-015-1 – R2	Retain internal network security monitoring data associated with activity the entity determined to be anomalous, at a minimum until the action in Part 1.3 is complete. The standard sets no fixed retention period, and data not relevant to detected anomalous activity need not be retained.	Long-term metadata and scalable packet capture hold the record for as long as an investigation runs, and the entity sets the retention policy the standard leaves open. Automated Retrospective Detection re-checks stored traffic when a new indicator emerges.
Protection of monitoring data CIP-015-1 – R3	Documented processes to protect monitoring data collected under R1 and retained under R2, to mitigate the risks of unauthorized deletion or modification.	Records are written once and held outside the monitored estate, so an adversary with control of a substation gateway cannot edit the evidence of the intrusion.
Evaluating an anomaly before acting CIP-015-1 – R1, Part 1.3	Evaluate anomalous network activity to determine further actions. The standard leaves the evaluation method to the entity.	RevealX NDR and RevealX NPM read the same wire data, so a team separates a cyber-attack from an operational fault in one investigation. An isolation step taken on incomplete information can shed more load than the intrusion would have.

Obligation 2 of 6

Scope Reaches Beyond the ESP

CIP-015-2 adds associated EACMS, PACS, PCA, and Shared Cyber Infrastructure to the applicable systems. A program scoped to the Electronic Security Perimeter alone is already behind the standard.

WHAT IT REQUIRES, AND WHAT ANSWERS IT

Scope beyond the perimeter

CIP-015-2 – R1, Applicable Systems

THE REQUIREMENT

Applicable systems extend to high-impact and medium-impact, with ERC BES Cyber Systems and their associated EACMS, PACS, and PCA, plus Shared Cyber Infrastructure supporting an applicable system. Order No. 907-A narrowed the environment for segments outside the ESP to communications between those system classes.

HOW REVEALX CONTRIBUTES

RevealX monitors the segments that carry those communications from a tap or SPAN port, so extending coverage to associated EACMS and PACS adds sensors rather than a second monitoring architecture.



Obligation 3 of 6

Applicability is Narrower Than the Whole Estate

High-impact BES Cyber Systems and medium-impact BES Cyber Systems with external routable connectivity are in scope. Medium-impact without ERC and all low-impact systems sit outside it.

WHAT IT REQUIRES, AND WHAT ANSWERS IT

Identifying what is in scope

CIP-002-5.1(a) – R1

THE REQUIREMENT

Categorize BES Cyber Systems by impact rating. The CIP-015-1 implementation plan keys its first tranche to Control Centers and backup Control Centers identified under R1.1 and R1.2.

HOW REVEALX CONTRIBUTES

A run-time inventory records what is actually communicating, including the unmanaged estate agent-based tools miss, with mapped interdependencies. The categorization decision remains the entity's.



Obligation 4 of 6

Notification Runs on a One-Hour Clock

CIP-008-6 R4 starts from the entity's determination of a Reportable Cyber Security Incident, with the end of the next calendar day for an attempted compromise and updates inside seven calendar days.

WHAT IT REQUIRES, AND WHAT ANSWERS IT

Incident notification

CIP-008-6 – R4, Parts 4.1–4.3

THE REQUIREMENT

Initial notification within one hour of determining a Reportable Cyber Security Incident, and by the end of the next calendar day for a determination that an incident was an attempt to compromise. Notifications carry functional impact, attack vector, and level of intrusion, with updates within seven calendar days.

HOW REVEALX CONTRIBUTES

Forensic capture supplies all three attributes inside the window, without waiting on log aggregation across dispersed substations, and preserves the record the seven-day update depends on.

Establishing functional impact

CIP-008-6 – R4, Part 4.1

THE REQUIREMENT

A notification must carry the functional impact of the incident, where known, alongside the attack vector and the level of intrusion.

HOW REVEALX CONTRIBUTES

RevealX NPM quantifies service degradation across substation latency, RTU sessions, and application performance, which turns functional impact into a measured statement rather than an estimate.



Obligation 5 of 6

Recovery Plans Need Testing Evidence

CIP-009-6 R2 requires a test at least once every 15 calendar months, high-impact systems add an operational exercise every 36 calendar months, and R3 requires lessons learned within 90 calendar days.

WHAT IT REQUIRES, AND WHAT ANSWERS IT

	THE REQUIREMENT	HOW REVEALX CONTRIBUTES
Recovery plan testing CIP-009-6 – R2, Parts 2.1–2.2	Test each recovery plan at least once every 15 calendar months, by recovering from an actual incident, a paper drill or tabletop exercise, or an operational exercise. Test a representative sample of recovery information on the same cadence. Applies to high-impact BES Cyber Systems and to medium-impact BES Cyber Systems at Control Centers, with their associated EACMS and PACS.	RevealX NPM establishes the performance baseline a test is measured against and records whether a recovery path behaved as designed, which supports the documented outcome. The entity performs the test.
Operational exercise CIP-009-6 – R2, Part 2.3	Test each recovery plan at least once every 36 calendar months through an operational exercise in an environment representative of the production environment. Applies to high-impact BES Cyber Systems.	Observation runs from a tap or SPAN port, so an exercise proceeds without polling controllers or introducing traffic into the production path.
Lessons learned CIP-009-6 – R3, Part 3.1	No later than 90 calendar days after a recovery plan test or an actual recovery, document any lessons learned or their absence, update the plan, and notify each person or group with a defined role.	Before-and-after baselines evidence what the test revealed and what the update corrected, which gives the documented lessons a measured basis.
Maintaining reliability during response Operational, not a CIP requirement	No CIP requirement governs how an entity protects reliability while it responds. The constraint is real and it sits outside the standard.	Continuous monitoring of mission-critical SCADA services surfaces infrastructure degradation before it reaches grid continuity, and validates EMS migrations by auto-mapping dependencies against established OT baselines.

Obligation 6 of 6

Pipeline and Nuclear Operators Carry More

TSA Security Directive Pipeline-2021-02G applies to designated pipeline owners and operators, and CIP-015 exempts systems covered by an NRC 10 CFR 73.54 cybersecurity plan.

WHERE IT IS MAPPED

Use Case	Jurisdiction	Framework	RevealX	How RevealX Contributes
Internal network security monitoring	North America	NERC CIP-015-1 – and CIP-015-2	NDR	Detects and evaluates anomalous east-west activity across the applicable systems, and holds the retained, protected record R2 and R3 call for.
Incident reporting	North America	NERC CIP-008-6 – R4	NDR	Supplies functional impact, attack vector, and level of intrusion inside the one-hour notification window, and preserves the record behind the seven-day update.
Recovery plan testing	North America	NERC CIP-009-6 – R2–R3	NPM	Establishes the baseline a 15-calendar-month test is measured against and records whether a recovery path behaved as designed.
Pipeline cybersecurity	United States	TSA SD – Pipeline-2021-02G (May 2026)	NDR	Provides the continuous monitoring and segmentation analysis needed to protect critical pressure and flow control systems. TSA reissues these directives annually, so confirm the current revision.
Nuclear digital protection	United States	10 CFR 73.54 – via RG 5.71 or NEI 08-09	NDR	Monitors secure zones through non-intrusive taps, supporting program controls without active scanning or agent interference. CIP-015 §4.2.3.4 exempts systems under a 73.54 cybersecurity plan, so the two populations do not overlap.
Maturity assessment	United States, Australia	DOE C2M2 v2.1 – AEMO AESCSF v2	NDR NPM	Supplies the telemetry behind the Threat and Vulnerability Management and Situational Awareness domains. Both models are self-evaluations scored per domain rather than certifications.

The Solution

One Platform, Two Disciplines

RevealX NDR
Detection and Evidence

ExtraHop RevealX NDR delivers the network intelligence North American operators need to detect and evaluate anomalous activity inside the CIP-networked environment. RevealX unifies the view across transmission control centers, substation automation, generation plants and distributed renewable sites.

The network holds the one record an attacker cannot edit. Logs and endpoint agents can be modified or disabled. IEDs, RTUs, and protection relays have no capacity to run agents at all. RevealX monitors the wire instead of the device, so an operator keeps visibility even when a substation gateway or a maintenance laptop is compromised.

CIP-015-1 R1 asks for methods that detect anomalous network activity and then methods that evaluate it. RevealX applies machine learning to east-west traffic and flags unauthorized commands in DNP3 or IEC 61850, lateral movement toward the plant floor, and credential abuse against engineering workstations. One-click investigation carries a team from the detection to the packets.

RevealX NPM
Continuity and Context

Responding inside a grid carries its own risk. An isolation step taken on incomplete information can cost more load than the intrusion would have. RevealX NPM measures latency, throughput, and error rates across substation automation, SCADA services, and energy management systems, using over 5,000 wire data metrics.

CIP-015-1 R1 Part 1.3 asks an entity to evaluate detected anomalies and determine further action. RevealX NDR and RevealX NPM read the same wire data, so a team can separate a cyber-attack from an operational fault in one investigation rather than two.

CIP-009-6 R2 requires recovery plan testing on a 15-calendar-month cadence. RevealX NPM supplies the agentless baseline a test is measured against and records whether a recovery path behaved as designed, observing from a tap or SPAN port so the test runs without polling controllers.

One out-of-band sensor produces NDR, NPM, IDS, and packet forensics at once, so a new mandate is covered by the platform already on the wire rather than by another point tool.

Key Capabilities

Nine Capabilities, Tagged by Product

	CAPABILITY	WHAT IT DOES
RevealX NDR	Monitoring the CIP-Networked Environment	RevealX monitors east-west traffic across the applicable systems, which CIP-015-2 extends beyond the Electronic Security Perimeter to associated EACMS, PACS, PCA, and Shared Cyber Infrastructure.
	Evidence for a One-Hour Clock	RevealX holds a write-once record of network transactions outside the monitored estate. Teams establish functional impact, attack vector, and level of intrusion, which are the three attributes CIP-008-6 R4 Part 4.1 asks a notification to carry.
	Strategic Line-Rate Decryption	RevealX analyzes modern encrypted traffic, including TLS 1.3 and perfect forward secrecy. Decryption runs at line rate and adds no latency to time-sensitive grid control operations.
RevealX NPM	Recovery Plan Test Evidence	RevealX NPM establishes the performance baseline a CIP-009-6 R2 test is measured against and records whether a recovery path behaved as designed, which supports the documented test outcome.
	Operational Resilience	RevealX NPM resolves infrastructure degradation before it reaches grid continuity, monitoring mission-critical SCADA services with high-fidelity wire data telemetry.
	Root Cause Across SOC and NOC	One click runs from the metric to the record, and one more to the packet. Teams separate a cyber-attack from an operational fault in one investigation, which removes the friction between grid operations and IT network teams during an incident.
RevealX Platform	Unified Agentless Visibility	RevealX automatically discovers every asset on the network, including unmanaged OT devices such as PLCs, RTUs, and IEDs, without installing software or risking controller stability.
	North American Protocol Depth	RevealX decodes and decrypts more than 90 protocols at line rate. Native support covers DNP3, IEC 61850, and Modbus. DNP3 dominates North American substation and RTU communication.
	Out-of-Band by Design	RevealX observes traffic from a tap or SPAN port. Controllers stay untouched: no agents, no active scanning, no polling, which matters in nuclear and high-consequence zones.

Where the Regions Differ

Where North America Differs from Europe

Three distinctions separate a CIP-015 program from the EU Network Code on Cybersecurity. CIP scopes obligations by **asset impact rating plus external routable connectivity**, while the Network Code scopes by business process impact. CIP carries **enforcement with financial penalties** through the NERC Compliance Monitoring and Enforcement Program, while the Network Code sets no fines of its own and monetary exposure there runs through national NIS2 transposition. And the CIP family has no **availability-reporting counterpart** to Network Code Article 27, which requires an estimate of the risk to confidentiality, integrity, and availability for every high-impact process. Operators running assets in both regions should read this brief alongside **Securing the European Grid: NIS2 and the Network Code on Cybersecurity**.

Sources, and How to Start

ExtraHop Can Help

ExtraHop RevealX surfaces the lateral movement and internal threats legacy tools miss, and produces the evidence a CIP audit asks for. Contact us to schedule a demonstration against your Control Center and substation environments.

> “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

Regulatory Sources

NERC Reliability Standards CIP-015-1 and CIP-015-2, CIP-008-6 and CIP-009-6, with the Project 2023-03 and Project 2025-02 Implementation Plans; FERC Order No. 887, 182 FERC ¶ 61,021 (2023); FERC Order No. 907, 191 FERC ¶ 61,224 (2025) and Order No. 907-A, 192 FERC ¶ 61,171 (2025); FERC letter order, Docket No. RD26-6-000 (10 August 2026); TSA Security Directive Pipeline-2021-02G (May 2026); 10 CFR 73.54 and NRC Regulatory Guide 5.71, Revision 1; DOE C2M2 Version 2.1; AEMO AESCSF v2. Sidebar evidence: FBI, CISA, NSA, EPA, DOE and US Cyber Command–CNMF, Iranian-Affiliated Cyber Actors Exploit Programmable Logic Controllers Across US Critical Infrastructure, Joint Cybersecurity Advisory AA26-097A, 7 April 2026; CISA, NSA and FBI, Joint Cybersecurity Advisory AA24-038A, 7 February 2024; NERC RISC, 2025 ERO Reliability Risk Priorities Report, 22 July 2025; NERC, Inverter-Based Resources Work Plan Progress Update, FERC Docket No. RD22-4-001, 29 April 2026.

Regulatory statements reflect the operative text of the instruments cited as at September 2026. CIP-015-1 is approved and future-effective, with first compliance on 1 October 2028. This brief provides information only and does not constitute legal advice. Applicability depends on an entity's own BES Cyber System categorization.

About ExtraHop

ExtraHop is a leader in real-time network intelligence, empowering organizations with the high-fidelity context they need to power security and IT AI automation, detect risks faster, and respond with confidence.

ExtraHop anchors AI agents with the real-time, ground-truth foundation they need to operate reliably in the SOC and NOC. For security, that means surfacing threats and providing definitive evidence to investigate and respond to novel AI attacks and unsanctioned usage at machine speed. For IT operations, it means identifying and resolving performance issues in seconds to keep critical systems running.

Engineered for unmatched scale, the ExtraHop RevealX platform delivers a complete, unified view of the network for the largest enterprises in the world. Capturing and analyzing network data across data centers, campus, branch, cloud, and AI environments, ExtraHop combines behavioral analysis with deep visibility into encrypted traffic to uncover what others miss.

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

© 2026 ExtraHop Networks, Inc., RevealX and ExtraHop are registered trademarks or trademarks of ExtraHop Networks, Inc. in the United States and/or other countries. All other products are the trademarks of their respective owners. 1182B 10.28.26

EXTRAHOP®