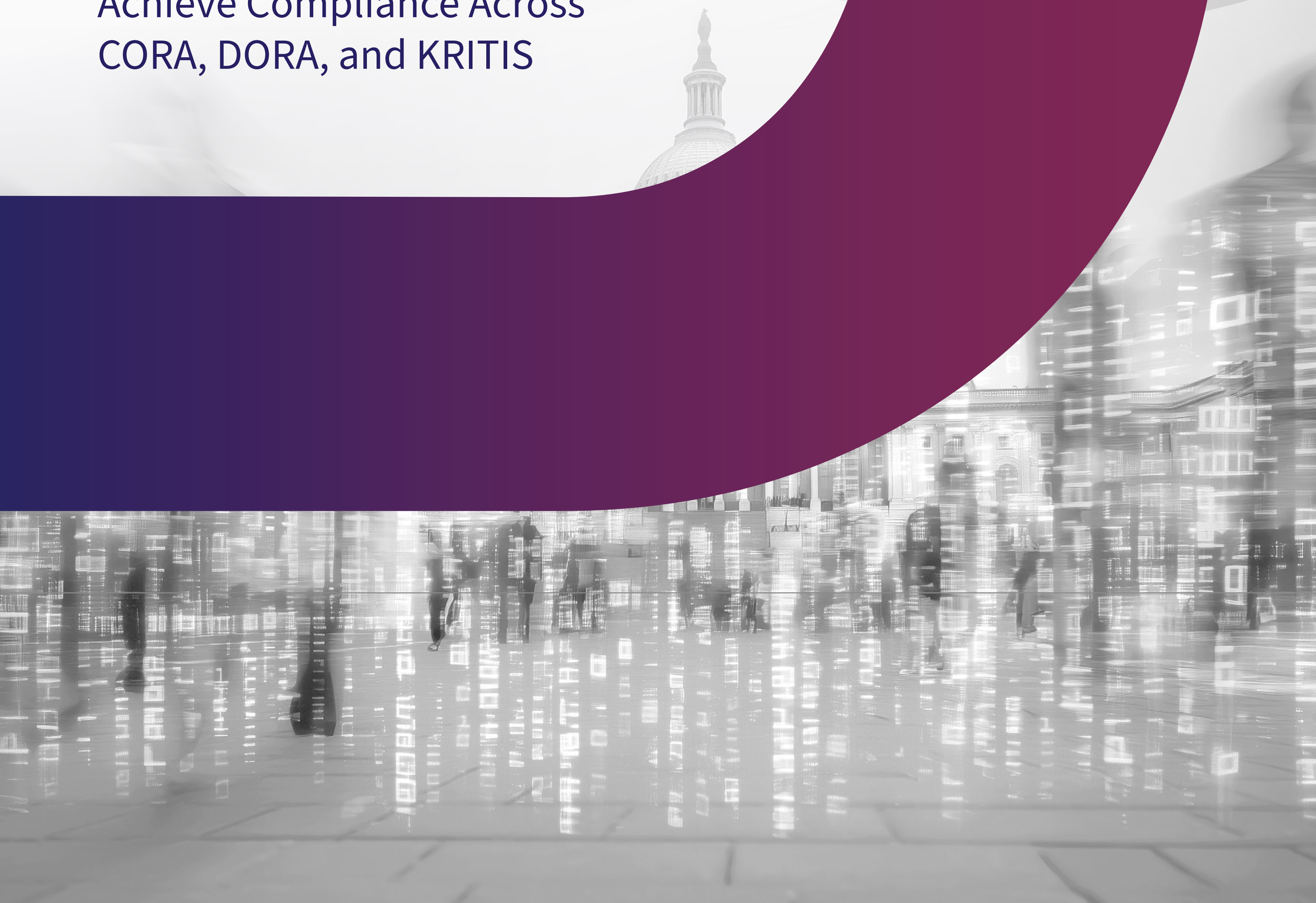
WHITE PAPER

Strengthening NATO Mission Partner Environments

How ExtraHop Helps Organizations Achieve Compliance Across CORA, DORA, and KRITIS



The Advantage of Unified Security

In our current volatile geopolitical climate, where hackers are mobilized, ready, and eager to strike, NATO Mission Partner Environments (MPEs) need to be exceptionally well-prepared. Failure to take every measurable precaution could lead to serious consequences, including classified intelligence leaks, disruptions to critical infrastructure, and social instability.

Because so much is at stake, each NATO MPE needs to solidify its reputation as a secure and reliable international partner—one that's capable of operating in a hyper-threat environment.

At the heart of this challenge is the need to adhere to multiple, overlapping preparedness standards. Today, NATO MPEs must comply with both U.S. and European assessment frameworks and mandates, including the U.S. Department of Defense's Cyber Operational Readiness Assessment (CORA), the EU's Digital Operational Resilience Act (DORA), and Germany's Kritische Infrastrukturen (KRITIS). This means MPEs need a way to streamline their processes and ensure consistent compliance across these diverse requirements.

Mission Partner Environment Challenges

MPEs are collaborative networks where NATO members and mission partners exchange information, coordinate operations, and execute missions across multiple domains.

These environments are inherently complex, requiring:

- Interoperable security controls across U.S. and European frameworks.
- Continuous situational awareness to detect cyber threats that could disrupt joint operations.
- Compliance with national and supranational standards.
- Rapid detection and response capabilities to contain threats before they propagate through interconnected mission networks.

Achieving Compliance With ExtraHop

ExtraHop provides modern network detection and response (NDR) capabilities that directly align with the U.S. Cyber Operational Readiness Assessment (CORA), the EU Digital Operational Resilience Act (DORA), and Germany's KRITIS requirements, among other regulations, enabling NATO mission partners to achieve operational readiness, continuous monitoring, and compliance across allied networks.

Meeting CORA Requirements (U.S.)

ExtraHop directly addresses CORA's emphasis on readiness assessments, situational awareness, and rapid response through its continuous, agentless network visibility and real-time behavioral analytics. ExtraHop captures detailed Layer 2–7 transaction records, enabling comprehensive east-west and north-south monitoring, and produces forensic-level evidence for incident investigations, ensuring that environments can demonstrate validated security measures during CORA assessments.

Supporting DORA Compliance (EU)

ExtraHop helps meet mandates for operational resilience of critical digital infrastructure by providing continuous monitoring, automated threat detection, and actionable intelligence to identify ICT-related incidents before they impact mission continuity. ExtraHop's ability to baseline network behavior across hybrid and cloud environments aligns with DORA's requirements for proactive risk management and incident preparedness.

Enabling KRITIS Readiness (Germany)

KRITIS demands robust detection, anomaly identification, and rapid response for critical infrastructure operators, including defense partners. ExtraHop detects advanced threats in real time and offers comprehensive visibility into encrypted and unencrypted traffic, ensuring mission environments meet KRITIS expectations for resilience and defense-in-depth strategies.

Unified Value for NATO Mission Partners

By meeting the requirements of CORA, DORA, and KRITIS in a single platform, ExtraHop enables NATO MPEs to:

- Establish a common cybersecurity standard accepted by U.S. and European mission partners.
- Enhance interoperability of security operations, ensuring every partner nation benefits from the same situational awareness and threat detection capabilities.
- Provide forensic-quality evidence across all mission partners, supporting coordinated response, accountability, and compliance reporting.
- Deploy mission-ready assessment kits to tactical environments, maintaining security in disconnected, degraded, intermittent, or limited (DDIL) communications scenarios.
- Align with NATO's modernization goals, including the integration of Zero Trust principles and the strengthening of collective cyber defense postures.

As NATO mission partners face evolving threats and increasingly complex regulatory environments, ExtraHop is here to help.

By providing continuous visibility, real-time detection, and forensic-level analysis across multinational environments, ExtraHop not only makes it easier to achieve compliance but also strengthens the resilience and operational effectiveness of NATO's Mission Partner Environments.

Unlock the full power of network detection and response with ExtraHop. To learn more, visit www.extrahop.com or follow us on LinkedIn.

ABOUT EXTRAHOP

ExtraHop is the cybersecurity partner enterprises trust to reveal cyber risk and build business resilience. The ExtraHop RevealX platform for network detection and response and network performance management uniquely delivers the unparalleled visibility and decryption capabilities that organizations need to investigate smarter, stop threats faster, and move at the speed of risk. Learn more at extrahop.com.

EXTRAHOP

info@extrahop.com
extrahop.com