CUBRO
NETWORK VISIBILITY

Network Visibility in the Era of NIS2 and DORA

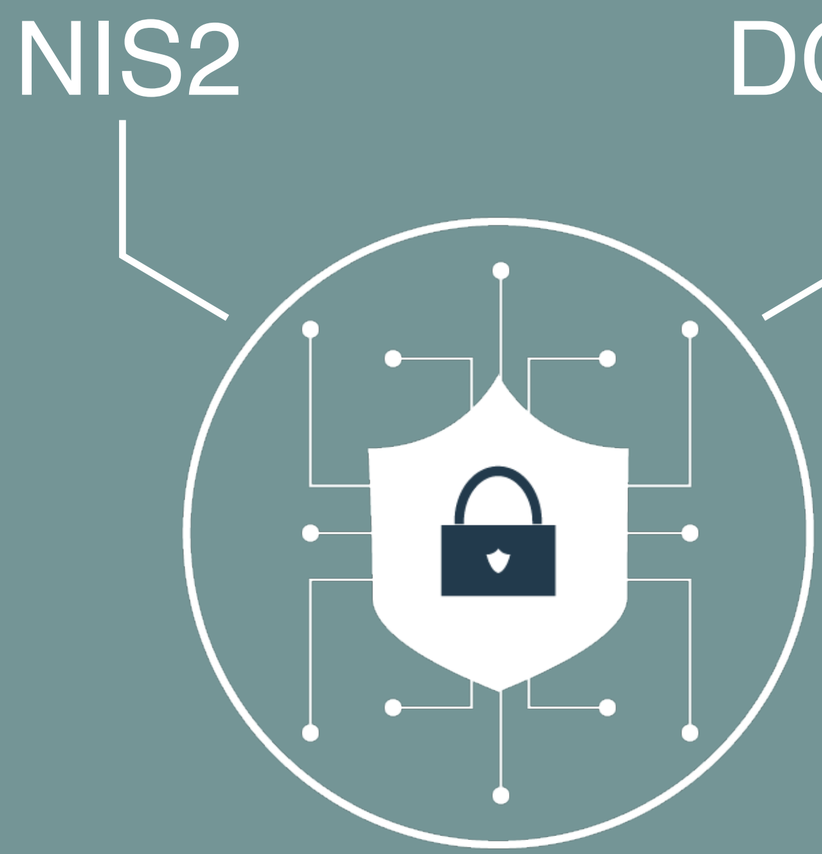
Ebook

Table of contents

The New Regulatory Landscape

Across the European Union, cybersecurity regulation has entered a new phase. With the enforcement of NIS2 (Network and Information Security) and DORA (Digital Operational Resilience Act), compliance is now a matter of corporate and executive accountability.

The Liability Shift: Breaches may now result in penalties for management, including personal liability and a potential temporary ban from management roles.



The Scope of NIS2 & DORA

High Criticality: Energy, transport, banking, financial market infrastructures, health, drinking/waste water, digital infrastructure, ICT service management, public administration, and space.

Other Critical Sectors: Postal/courier, waste management, chemicals, food distribution, manufacturing (medical devices, electronics, vehicles), digital services (marketplaces, search engines, social platforms), and research.

Supply Chain Focus: Includes the entire ecosystem of direct suppliers and vendors. Entities must ensure vendor adherence to security standards and continuous monitoring.

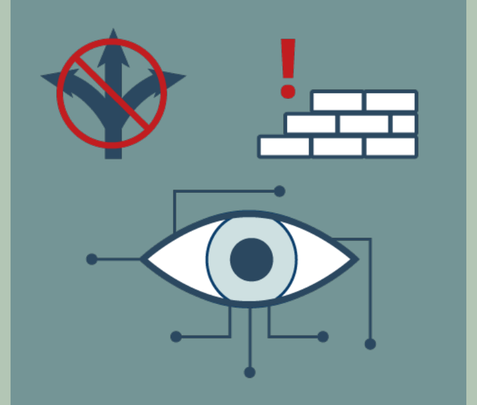
DORA Specifics: Targets financial firms and their ICT service providers to ensure operational continuity and risk management.

A Fundamental Shift for Leadership

This introduces a shift in how infrastructure is viewed at the board level:

Cybersecurity is no longer discretionary spending

Compliance is no longer periodic; it is continuous.



Visibility is no longer optional; it is foundational.

Reporting obligations (often within **24–72 hours**) demand a level of accuracy that cannot be achieved without verifiable, complete data. Companies must prove what happened, not estimate it.

The Hidden Financial Risk of Conventional Scaling

Many companies attempt to meet these demands by simply purchasing higher-capacity firewalls or moving to advanced NDR platforms. While a step in the right direction, this approach often leads to unanticipated surprises:

The 400G Cost Trap:

As networks evolve to 100G/400G, security tools must process exponentially larger volumes of data at disproportionately higher costs.

The Noise Problem:

Inspection tools are often forced to process irrelevant data (e.g., backups/internal replication). This leads to packet drops and blind spots.

ROI Erosion:

Security teams spend more time managing data noise than mitigating actual risk.

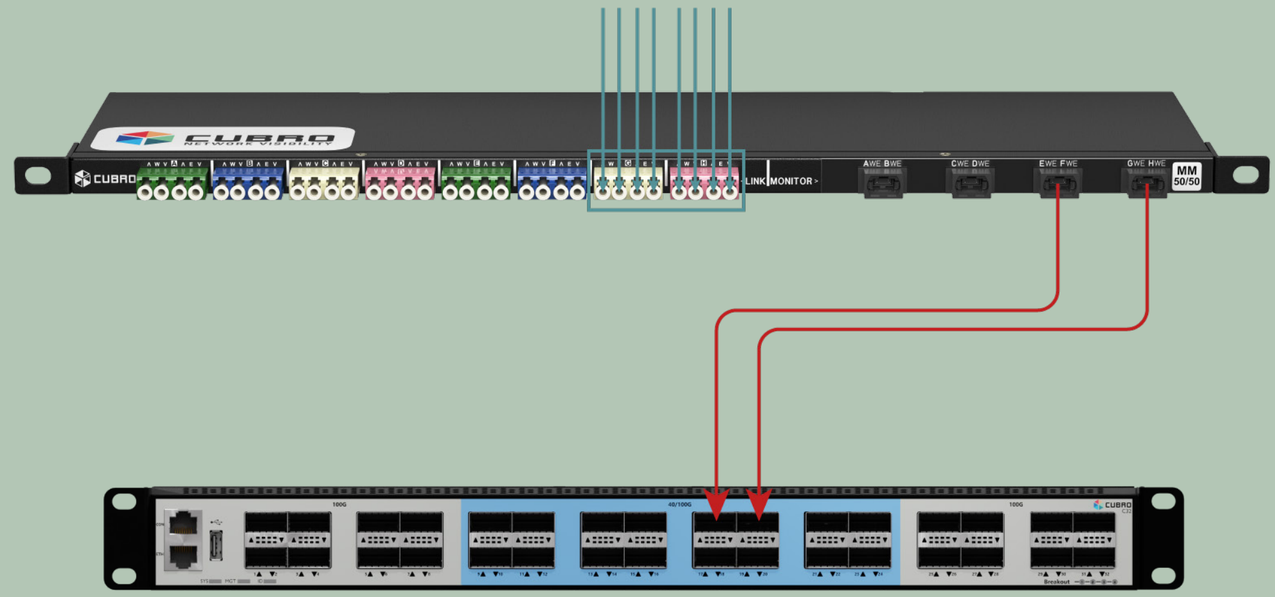
Why “More Tools” Is Not the Answer: NIS2 and DORA mandate outcomes (continuous monitoring, accurate reporting), not specific tools. Tools are evaluated on capability, but Compliance depends on data integrity.

Network Visibility as an Enabler

Bridging this gap requires a dedicated Visibility Layer built on two components:

Test Access Points (TAPs): Hardware-based devices that create an exact, lossless copy of network traffic. Unlike SPAN ports, TAPs provide data without latency or packet loss.

Network Packet Brokers (NPBs): These aggregate, filter, and deduplicate traffic, ensuring tools receive only the data they need.



Financial & Operational Impact

Optimised Tool Utilisation:
Reduce the data volume sent to tools by 30–50% through filtering and deduplication.

Extended Asset Lifecycle:
Decouple network speed from tool processing power to avoid premature upgrades of high-cost security appliances

Audit Readiness:
Provide packet-level evidence for investigators strengthening the organization's ability to respond to regulatory audits and incident investigations

Reduced Operational Overhead:
Security teams can focus on actionable insights rather than managing excessive data volumes and false positives.

Mapping Visibility to Regulatory Mandates

The relevance of network visibility becomes particularly clear when mapped directly to regulatory expectations:

Continuous Monitoring	Risk Management	Incident Reporting
Enabled through uninterrupted access to real-time traffic data	Strengthened by comprehensive visibility into network behavior	Supported by accurate, packet-level evidence rather than aggregated logs

Strategic Considerations for Financial Leadership

For CFOs and board members, the key question is not whether to invest in security, but how to ensure that investment translates into measurable risk reduction and regulatory assurance.

A visibility-first approach introduces an improved financial model:

Cost control through optimized use of existing tools	Risk reduction through elimination of blind spots	Regulatory alignment through verifiable data

This aligns cybersecurity investment more closely with broader financial objectives: predictability, efficiency, and accountability.

Real-World Audit Scenarios

The Forensic Evidence Question

Audit Scenario:

If an incident occurred at 03:00 AM last night, can you prove to an auditor exactly what data left your network?

Operational Reality:

Most companies rely on logs. Logs are summaries; they can be faked or missed during a CPU spike.

Visibility Approach:

Evidence requires Integrity. By using passive Network TAPs, you capture 100% of the raw traffic. It's the 'Unbiased Witness' that provides the forensic proof required by NIS2/NISG 2026 (Austria) and DORA.

The Data Loss (Blind Spot) Question

Audit Scenario:

Is your expensive security software currently dropping 20% of your data because of 'Network Noise'?

Operational Reality:

Streaming (e.g. Netflix/YouTube) and background updates flood security tools. This leads to Packet Loss, meaning non-compliance because you aren't actually monitoring everything.

Visibility Approach:

Our Packet Brokers act as a high-speed filter. We strip out the "junk" and only send relevant security data to your tools. You save on license costs and ensure your tools never miss a packet.

Real-World Audit Scenarios

The Resilience Question

Audit Scenario:

If your IPS or Firewall fails, does your entire business go offline, or do you have a Plan B?

Operational Reality:

DORA and NIS2 demand "Digital Operational Resilience." A security tool becoming a ‘Single Point of Failure’ is a major compliance risk.

Visibility Approach:

Safeguard your Uptime. Cubro Bypass Switch automatically detects tool failure and reroutes traffic in milliseconds. You stay secure and stay online. Resilience isn't just about stopping hacks; it's about keeping the lights on.

The Sovereignty Question

Audit Scenario:

Is your hardware visibility layer protected by European Law?

Operational Reality:

For Austrian critical infrastructure (Energy, Health), using non-EU hardware creates a ‘Supply Chain Risk’ under NIS2/ NISG 2026 (NISG 2026 - Network and Information Systems Security Act 2026) Section 18.

Visibility Approach:

Sovereignty by Design. Cubro headquartered in Vienna addresses this through locally engineered solutions and strong control over design, development, and security standards. When an auditor asks about your supply chain, you can point to a local partner who follows the same Austrian laws as you.

Real-World Audit Scenarios

The OT / Production Question

Audit Scenario:

Can you monitor your factory floor robots without the risk of a software update crashing the production line?

Operational Reality:

In manufacturing environments, many legacy systems (10 - 20+ years old) run on heterogeneous connectivity - often copper-based, sometimes with fiber backbone links. These systems typically cannot support agents, and even light probing or scanning can cause instability or downtime.

Visibility Approach:

Visibility without Contact. Cubro Passive Optical TAPs and electric TAPs take a copy of the traffic without interfering with the network thus getting the data needed for NIS2 without ever touching the sensitive machinery.

The Executive Liability Question

Audit Scenario:

Are you, as a CEO/Managing Director, prepared to sign off on a 'Self-Declaration' of security without a hardware-verified report?

Operational Reality:

NISG 2026 makes CEOs personally liable. Relying on best guesses from software is a huge personal risk.

Visibility Approach:

Protect the Board. Cubro provides a hardware-level Source of Truth. When you sign that declaration, you aren't guessing, you are basing it on physical, verifiable network data.

Conclusion: Visibility is a Foundation, Not an Add-On




In the current regulatory landscape, compliance cannot be achieved through tools alone. It requires confidence in the data that underpins every security and reporting decision.

Network visibility provides that foundation and it enables organizations to:

- See their entire network without gaps
- Use their existing tools more effectively
- Respond to regulatory demands with evidence, not assumptions

The question is no longer whether visibility is needed, but how it is implemented.

Reach out to us at sales@cubro.com