FORWARD NETWORKS

USE CASE

Digital Twins and Digital Resilience: Modeling for DORA Readiness

After several years of drafting, industry consultation and anticipation, the **Digital Operational Resilience Act (DORA)** came into effect across the European Union from January 17th, 2025. Its goal is clear from its opening statement, where it recognizes that in today's financial marketplace, digital services underpin our way of life, "In the digital age, information & communication technology (ICT) supports complex systems used for everyday activities." How best does the industry stay resilient so the complexity of today's digital services remain transparent to the user?

DORA represents one of the most comprehensive regulatory frameworks ever introduced for digital resilience. It requires firms to demonstrate end-to-end visibility of their ICT assets, understand how services depend on interconnected systems, test their resilience under realistic conditions, and produce evidence that risks are identified, mitigated, and continuously monitored. For many organisations, this is a significant shift from traditional compliance exercises toward a more holistic, operationally grounded model of resilience.

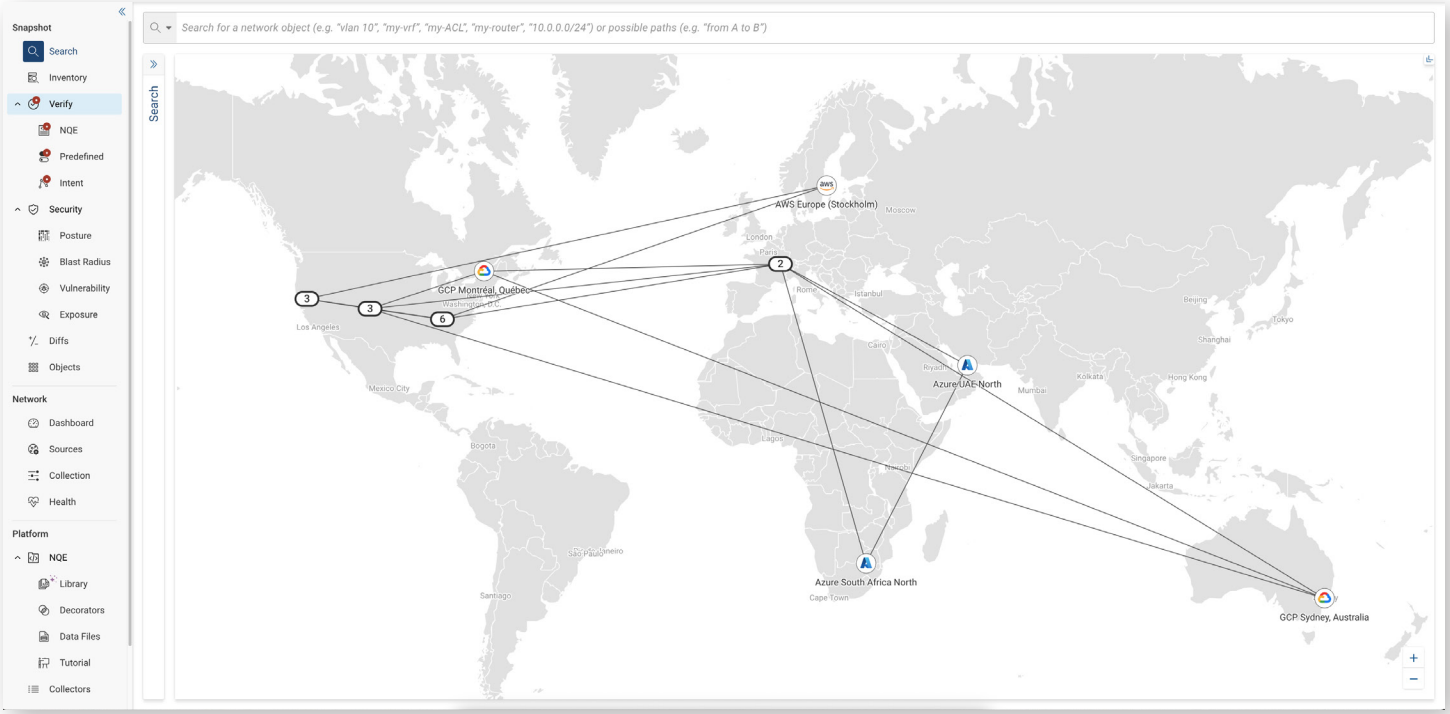
At the same time, the financial industry is grappling with a level of **IT complexity that has become unavoidable.** Modern finance depends on sprawling hybrid networks, multi-cloud environments, third-party integrations, legacy platforms, and a constant cadence of change. This complexity is the foundation of digital innovation—but it also obscures risk, slows incident response, and makes it difficult to produce the precise, audit-ready documentation that DORA now demands.

As institutions work to interpret and meet these new requirements, one challenge stands out above the rest: **how to gain a complete, accurate, and continuously updated understanding of highly complex ICT environments.** Without that, resilience becomes difficult to measure—and nearly impossible to prove.

Understanding DORA and Its Requirements

DORA raises the bar for operational resilience. Unlike previous EU directives, which combined guidance across several frameworks (PSD2, NIS, EBA guidelines), DORA unifies digital-resilience obligations into a single, enforceable regulatory regime.

While it is an EU directive it is clear that it applies to any business conducting operations in the European Union, effectively meaning all of global finance, and an expanded set of organizations, including crypto-asset firms, crowd-funding platforms, and crucially ICT 3rd-party Service Providers, the technology providers themselves. Built around five core pillars, its scope is wider and its expectations more rigorous.



How DORA's Five Pillars Apply

PILLAR 1: ICT RISK MANAGEMENT FRAMEWORK

DORA requires a comprehensive, documented ICT-risk framework approved by the management body, such as the executive board, or compliance committee.

This includes:
- A clear governance model for ICT risk, embedded in business strategy.
- A complete inventory of ICT assets and dependencies — hardware, software, networks, cloud and third-party services — with identification of critical functions.
- Regular risk assessments and controls to prevent, detect, respond to, and recover from ICT incidents, supported by business continuity and disaster recovery plans.

In short: firms must know **what exists, how it connects, and how risk is managed** across the full digital estate.

PILLAR 2: ICT-RELATED INCIDENT MANAGEMENT, CLASSIFICATION & REPORTING

DORA mandates structured detection, logging, classification, and escalation of ICT incidents.

Firms must:
- Maintain processes for managing incidents end-to-end.
- Classify major ICT incidents and report them to authorities within strict timelines using standard templates.

This requires the ability to quickly produce accurate root-cause analysis and technical impact assessments, even in complex or hybrid environments.

PILLAR 3: DIGITAL OPERATIONAL RESILIENCE TESTING

DORA elevates testing expectations significantly. Institutions must:
- Conduct regular resilience testing of critical ICT systems.
- Perform threat-led penetration testing (TLPT) for critical functions, examining real-world attack paths and dependencies.
- Document findings, remediate weaknesses, and validate improvements.

Compliance depends on being able to continuously test and verify ICT resilience — not rely on static documentation.

PILLAR 4: ICT THIRD-PARTY RISK MANAGEMENT

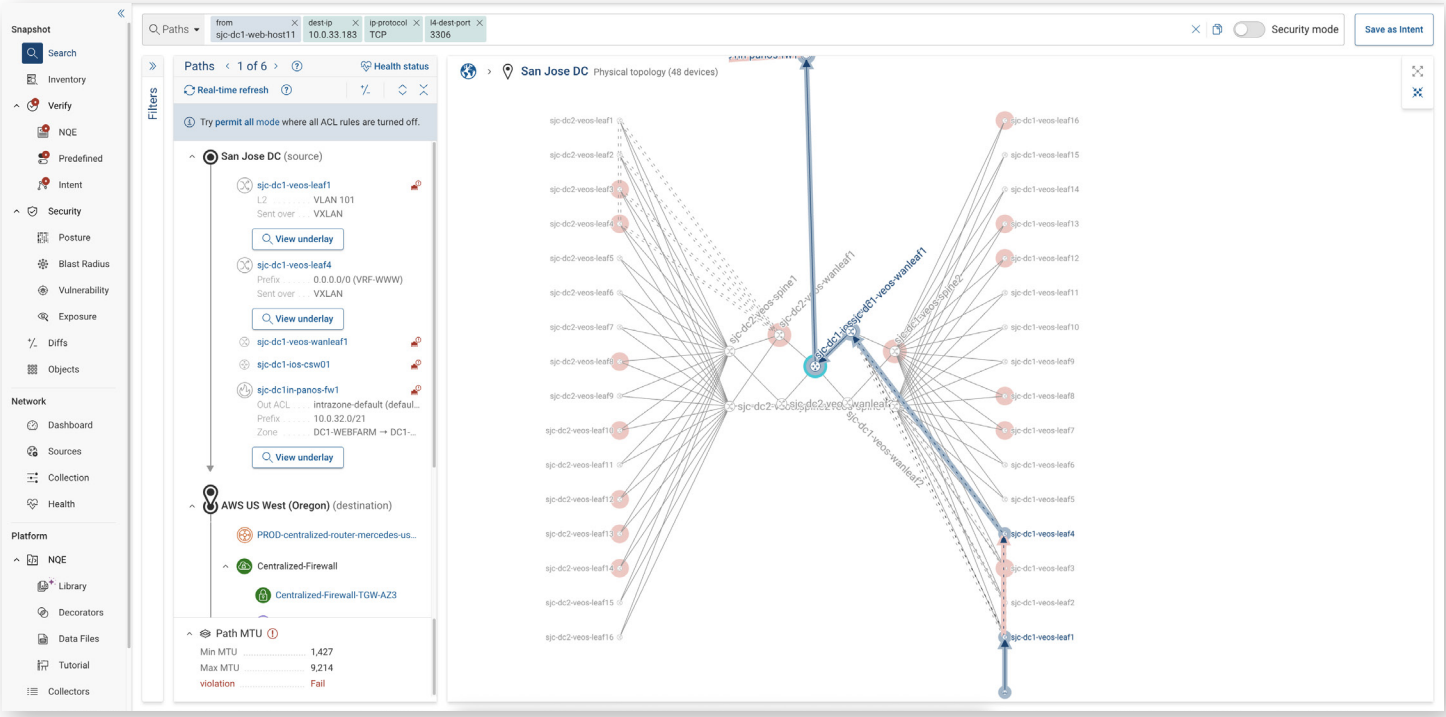
DORA requires rigorous oversight of ICT service providers, including subcontractors. Firms must:

- Maintain a register of all third-party ICT services and their dependencies.
- Perform due diligence before onboarding providers, assessing resilience, contract terms, audit rights, and exit strategies.
- Continuously monitor third-party risk, including concentration risks, where many critical services depend on a single vendor, and cascading risks, where an issue with one provider ripples through other systems that rely on it, directly or indirectly.

Third-party services remain inside the regulated risk perimeter — and must be managed as such.

PILLAR 5: INFORMATION SHARING ARRANGEMENTS

DORA encourages sector-wide information sharing on cyber threats, vulnerabilities and incidents. The aim is to strengthen collective situational awareness and coordinate responses to systemic risks.



Why These Pillars Create a High Bar — And Why Many Firms Struggle

Taken together, these five pillars impose stringent operational, technical, and governance requirements: full visibility of ICT assets and dependencies; continuous risk assessments; frequent testing; strong third-party oversight; coordinated incident management; and collaboration across the industry.

For many financial services organisations — especially those with hybrid infrastructure (on-prem + cloud), multi-vendor networks, legacy and modern systems, and outsourced dependencies — this is a significant compliance and operational challenge.

Common difficulties include:

- Fragmented knowledge of network topology and dependencies
- Partial visibility (some systems monitored, others opaque)
- Disjointed tools across cloud, network, on-prem, vendor, legacy
- Manual or static documentation, which becomes stale quickly
- Lack of ability to reliably simulate failures or verify all possible interdependencies

In short: traditional tools and practices often fall short of what DORA demands — and more importantly, what auditors and regulators will expect now that enforcement is a real possibility.

What This Means for Resilience Strategies

Given DORA's scope and complexity, a compliance strategy must include a unified, continuously updated view of the entire ICT estate — not just servers or applications, but also network connectivity, segmentation, cloud links, third-party connections, hybrid links, remote access, and more.

It must enable:

- Real-time visibility into what systems exist, where, and how they are connected
- Verification that configurations (routing, firewall, ACLs, segmentation) genuinely match documented security policies
- Automated evidence of infrastructure state and change history for audits
- Scenario and failure testing — including network failures, cloud region outages, third-party service disruption, and more
- Inclusion of third-party infrastructure in risk and resilience assessments
- Rapid root-cause analysis and incident reporting with full traceability of network paths and dependencies

Only with this sort of holistic visibility and behavioral verification can an organization realistically satisfy all five of DORA's pillars — without creating unmanageable operational overhead.

Digital Twins and Digital Resilience: Why the Financial Sector Needs a New Approach

As financial institutions face unprecedented operational-resilience expectations under DORA, many are discovering a fundamental issue: traditional tooling cannot deliver the unified, accurate, continuously updated view of ICT infrastructure that the regulation implicitly demands. Modern financial networks have become too complex — too hybrid, too interconnected, too dynamic — for manual documentation, scattered inventories, or siloed monitoring systems to keep pace.

This is where **network digital twin technology** is emerging as a transformative category.

At its core, a digital twin is a **mathematically accurate, continuously synchronized model of an institution's end-to-end network and connectivity** — across data centres, public cloud, hybrid environments, and third-party integrations. Unlike conventional mapping tools that rely on snapshots or polling, a true digital twin computes all possible behaviour of the network: every path, every rule, every control, every dependency.

For financial-services firms navigating DORA, this model offers a powerful foundation for compliance because it enables:

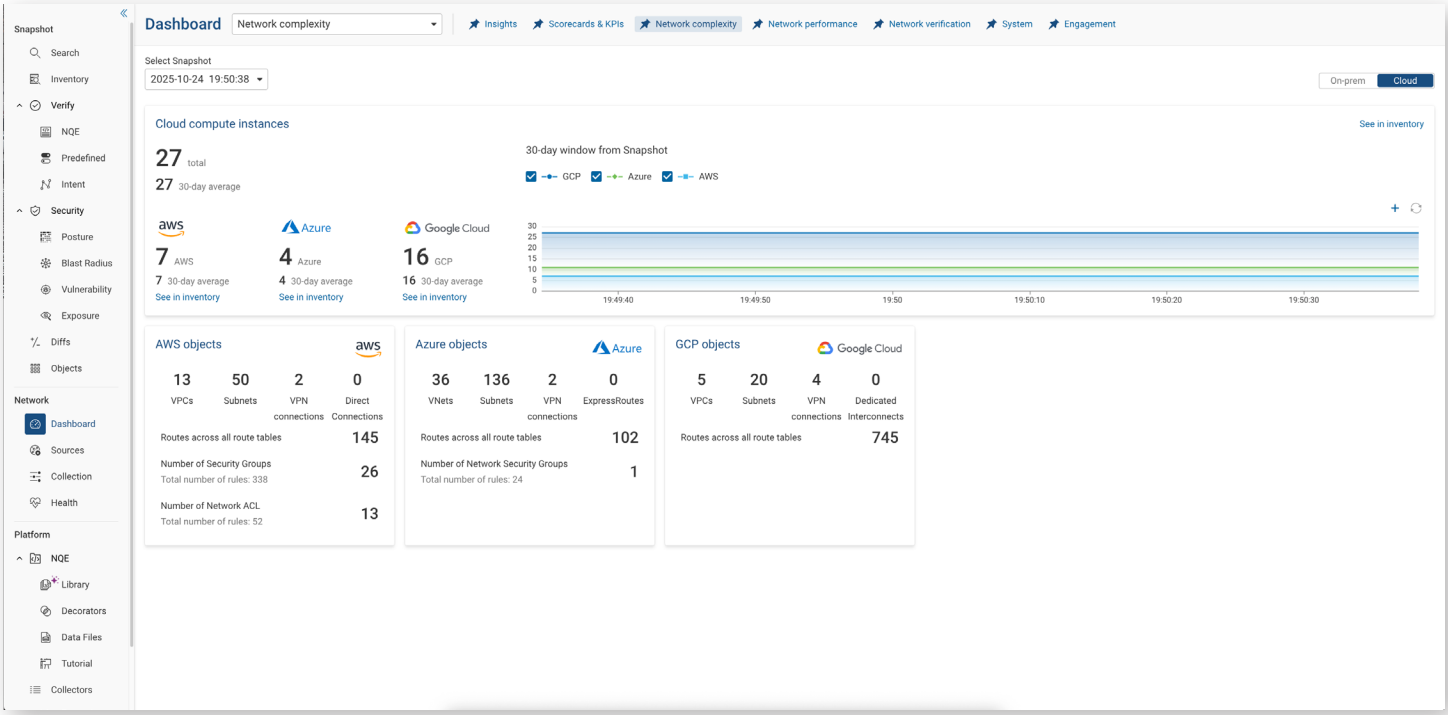
- **Unified visibility** across on-prem, cloud, and third-party ICT assets
- **Accurate dependency mapping** needed for critical-function identification and risk assessments
- **Immediate detection of misconfigurations,** inconsistencies, policy drift, and exposure paths
- **Reliable incident analysis**, root-cause identification, and regulatory reporting
- **Continuous verification**, simulation, and resilience testing without disrupting production

But it's important to acknowledge a key point. **Not all "digital twins" are equal, and many tools marketed as twins are simply automated diagrams.**

For a digital twin to genuinely support DORA, certain capabilities are non-negotiable:

- A **mathematically precise behavioural model**, not just a topology drawing
- The ability to ingest, normalize, and reconcile **multi-vendor, multi-cloud, hybrid configurations**
- End-to-end path computation reflecting actual forwarding logic, policy, and segmentation
- Full, historicized visibility for evidence, auditability, and change tracking
- Scalable support for enterprise-grade networks, architectures, and governance

This is the category that Forward Networks pioneered — long before DORA came into effect. The result is a technology stack that aligns unusually well with the regulation's core expectations because it was designed to solve the underlying operational-resilience problems that DORA is now forcing firms to address.



How Network Digital Twins Fulfil DORA's Core Requirements

…and Why Forward Networks' Model Is Uniquely Aligned

DORA's five regulatory pillars impose a level of infrastructure transparency, behavioural accuracy, and evidence-driven assurance that traditional tooling struggles to meet. A mathematically precise network digital twin — the type pioneered by Forward Networks — addresses these demands not by adding more dashboards, but by creating a single source of technical truth that reflects exactly how the ICT estate behaves at any moment in time.
Below, we map the capabilities of a true digital twin to the requirements within each DORA pillar.

1. ICT Risk Management (Articles 5–16)

DORA expects financial entities to maintain a comprehensive, continuously updated understanding of their ICT environment — including configurations, security controls, and interdependencies — and to ensure these are "consistent, complete, and functioning as intended."

A digital twin supports these requirements by:

- **Normalising and unifying configurations** across vendors, clouds, and on-prem infrastructure
- **Computing actual behaviour,** not assumed behaviour — revealing unintended access, policy drift, or misrouting
- **Highlighting deviations** from internal standards or "golden configurations"
- Enabling continuous, automated checks aligned with internal control frameworks

Instead of discovering issues during audits or outages, institutions gain a live, verifiable risk-management baseline.

2. ICT Incident Reporting (Articles 17–23)

DORA mandates timely, detailed, technically accurate reporting for major ICT incidents — including root cause, affected assets, impact scope, and propagation paths.

A behavioural digital twin enhances incident reporting by:

- Providing **instant blast-radius analysis:** which systems were reachable, exposed, or impacted
- Reconstructing network behaviour **before, during, and after** the incident through historic snapshots
- Offering **precise dependency insights** that underpin root-cause identification
- Reducing investigation time so firms can meet the mandated reporting windows

This shifts incident reporting from manual reconstruction to evidence-based analysis.

3. Digital Operational Resilience Testing (Articles 24–28)

DORA requires continuous testing, scenario simulations, configuration reviews, penetration testing support, and examination of critical functions under failure conditions.

A digital twin enables this by:

- Allowing institutions to simulate failure scenarios (link, node, region, or policy failure) without impacting production
- Validating segmentation, zero-trust controls, and routing outcomes with mathematically precise path analysis
- Automating configuration reviews against internal or regulatory benchmarks
- Supporting red-team exercises by showing where a vulnerability could propagate

This provides the “continuous assurance” that DORA expects, without operational risk.

4. ICT Third-Party Risk (Articles 29–33)

DORA requires firms to assess the risks embedded in third-party services, connectivity, and dependencies — not just contracts. Digital-twin visibility supports this by:

- Mapping all dependencies and communication paths involving external providers
- Showing cloud and hybrid connectivity, including security groups, gateways, and firewalls
- Revealing unintended exposures or overly permissive connections to or through third-party systems
- Allowing firms to demonstrate to regulators exactly how third-party traffic is governed

This moves third-party assurance from contractual oversight to technical verification.

5. Information Sharing (Articles 34–36)

DORA encourages structured, evidence-backed information sharing among financial entities, especially around threats and vulnerabilities.

A digital twin supports this by:

- Providing a clear, vendor-neutral technical representation of affected paths or assets
- Enabling consistent reporting of misconfigurations or vulnerabilities across teams
- Reducing ambiguity by grounding conversations in the same canonical data model

This strengthens cross-institution coordination during cyber or operational events.

The Result: A Regulatory Match by Design

Forward Networks did not develop its digital twin in response to DORA — yet its architecture aligns naturally with the regulation's deepest technical expectations. Because it models behaviour, not just assets; because it unifies cloud and on-prem; because it stores historical state; because it normalises multi-vendor configurations; and because its model is mathematically rigorous, it offers a level of fidelity and assurance that DORA implicitly requires.
Where traditional tools show pieces, a digital twin shows the whole system.

Where legacy inventories go stale, a digital twin stays current.
Where diagrams give topology, a digital twin gives precise behaviour.

That makes it not only valuable for DORA compliance — but foundational for digital resilience.

Benefits of Digital Twin Technology for DORA Compliance
Beyond aligning with the five pillars of DORA, a network digital twin delivers tangible operational advantages for financial institutions:

- Full Visibility Across Complex Environments: Understand every device, connection, and dependency — including hybrid cloud, on-prem, and third-party systems — in a single, unified model.
- Faster Risk Detection and Resolution: Automated analysis surfaces misconfigurations, policy drift, and vulnerabilities before they escalate, shortening investigation and remediation cycles.
- Evidence-Based Compliance: Provide auditors and regulators with precise, reproducible records of network state, configuration, and behaviour — reducing audit friction and reporting risk.
- Continuous Assurance: Simulate failures, validate controls, and stress-test critical applications without disrupting live operations, ensuring resilience under real-world conditions.
- Operational Efficiency: Reduce reliance on tribal knowledge, manual documentation, and siloed tooling, freeing teams to focus on higher-value tasks.

Conclusion

The complexity of modern financial infrastructure — from multi-cloud deployments to third-party services — makes DORA compliance a non-trivial challenge. Network digital twins offer a transformative approach, turning the abstract requirements of operational resilience into actionable, verifiable insight.
By providing a mathematically precise, always-current representation of network behaviour, digital twins enable financial institutions to manage risk proactively, report accurately, and validate resilience continuously. In an era where downtime and misconfigurations carry significant regulatory and financial consequences, this technology is more than a compliance tool — it's a foundation for true digital resilience.

ABOUT FORWARD NETWORKS

Forward Networks is revolutionizing the way large networks are managed. The Forward Enterprise platform delivers a vendor-agnostic "digital twin" of the network, based on a mathematical model. The platform scales to support hundreds of thousands of network devices, whether cloud, hybrid cloud, or on-prem. It serves as a single source of truth for the network, enabling network operators to instantly verify security posture, accelerate troubleshooting, avoid outages, and modernize network management.

Over the past few years, Forward Networks has received tremendous industry recognition, including "Cool Vendor in Enterprise Networking" by Gartner and "Product of the Year" by Cloud Computing, and has been named to Fortune Magazine's 2024 Cyber 60 as well as Fortune's 2024 "Best Workplaces in the Bay Area" list.

The company was founded by four Stanford PhD graduates who saw a massive opportunity to improve network operations. Investors include Andreessen Horowitz, Threshold Ventures, and Goldman Sachs.