IP FABRIC

EU’s NIS 2 Directive

ipfabric.io

EU's NIS 2 Directive

By October 2024, each EU Member State will have set out its mandate for affected Essential Entities and Important Entities under the NIS 2 Directive. This second take on the Network and Information Systems Directive expands in scope to include more industries and stricter security and reporting requirements.

While each Member State will have its own particular set of laws and obligations, **Gartner researchers** have extrapolated some common key pillars that everyone affected by NIS 2 should use to ground their compliance strategy: Cyber Risk Management, Corporate Accountability, Reporting Obligations, and Business Continuity.

Each of these areas involves the cloud and network infrastructure in specific ways, and therefore, automated network assurance is invaluable in supporting your NIS 2 compliance goals. Here are four key areas to assess and potentially remediate, along with how IP Fabric's network assurance platform can help:

01. Cyber Risk Management

NIS 2 Directive

Security risk assessments will be conducted by both EU Member States and the European Union Agency for Cybersecurity (ENISA).

"Member States shall ensure that essential and important entities take appropriate and proportionate technical, operational and organizational measures to manage the risks posed to the security of network and information systems which those entities use for their operations or for the provision of their services, and to prevent or minimize the impact of incidents on recipients of their services and on other services. Including:

(a) policies on risk analysis and information system security;

(c) security in network and information systems acquisition, development and maintenance, including vulnerability handling and disclosure;

(h) policies and procedures regarding the use of cryptography and, where appropriate, encryption;

(i) human resources security, **access control policies and asset management**;" (**Chapter IV, Article 21**).

IP Fabric Solution

IP Fabric continuously validates your cloud and network security posture, whichever approach you take. If your focus is Zero-Trust architecture; IP Fabric will discover, map, and alert you to deviations from your access control policies. If you've established network segmentation and micro-segmentation within your architecture, IP Fabric will, with every snapshot, ensure that segments are properly separated, and no planned or unplanned changes have caused unexpected paths through your infrastructure. IP Fabric automates your essential asset management tasks, through comprehensive discovery including End of Life and End of Support data. IP Fabric can then, for example, **match this inventory data against the CVE (Common Vulnerability and Exposure)** database to understand if your network is affected by any new additions. Built-in and custom intent checks, which validate the actual observed network state against your desired or intended network state, ensure that the success of your cyber risk management policies is measurable.

02. Corporate Responsibility

NIS 2 Directive

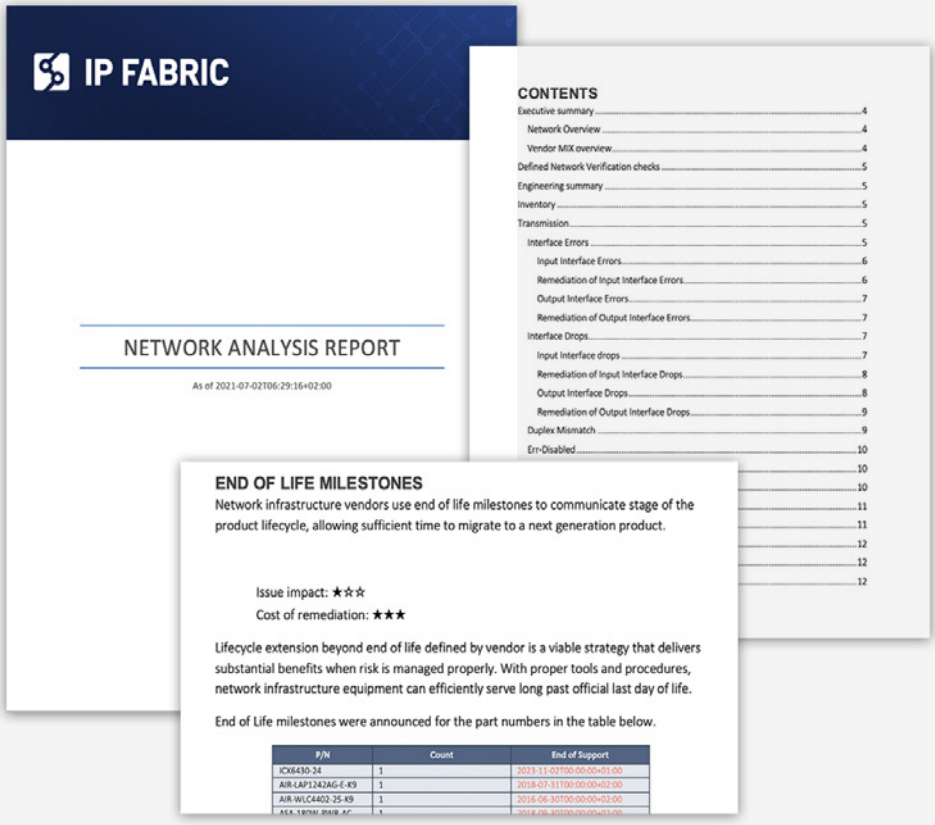
"Member States shall ensure that the management bodies of essential and important entities approve the cybersecurity risk-management measures taken by those entities in order to comply with Article 21, oversee its implementation and can be held liable for infringements by the entities of that Article (Chapter IV, Article 20).

"Member States shall ensure that any natural person responsible for or acting as a legal representative of an essential entity on the basis of the power to represent it, the authority to take decisions on its behalf or the authority to exercise control of it **has the power to ensure its compliance with this Directive**. Member States shall ensure that it is possible to hold such natural persons liable for breach of their duties to ensure compliance with this Directive." (Chapter VII, Article 32).

IP Fabric Solution

IP Fabric normalizes the complex and diverse cloud and network data contained in enterprises to make it consumable and actionable beyond a technical audience. Responsible management bodies need to understand the state of the network, and therefore a mechanism to democratize this data is invaluable.

There are exportable reports – Network Analysis and Low-Level Site Design - readily available in the platform.



Additionally, the normalized data in IP Fabric can be shared easily via API or pre-built integrations so teams can review the status of the network easily (i.e. **Grafana** dashboards, **Power BI reports**).

03. Reporting Obligations

NIS 2 Directive

There are time-bound obligations for reporting cybersecurity incidents.

“Each Member State shall ensure that essential and important entities notify, without undue delay, its CSIRT or, where applicable, its competent authority in accordance with paragraph 4 of any incident that has a significant impact on the provision of their services as referred to in paragraph 3 (significant incident).” (Chapter IV, Article 23).

IP Fabric Solution

IP Fabric's daily or on-demand discovery snapshots mean you have a historical record of your cloud and network state. This detailed information is essential for fast and accurate incident post-mortems; it gives you the evidence to understand the root cause of network incidents, as well as the blast radius so you can understand the full effect.

It's also your proof of remediation activity, and that these activities have had the desired effect - proactive security against future, similar incidents.

The normalization of complex and diverse network data also means less data collection, analysis, and interpretation of data surrounding incidents to produce required reports in the required time frames.

04. Business Continuity

NIS 2 Directive

"Develop plans including considerations about backup management, disaster recovery and crisis management to ensure business continuity in the case of cyber incidents." (**Gartner**)

"Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the measures referred to in the first subparagraph shall ensure a level of security of network and information systems appropriate to the risks posed.

The measures referred to in paragraph 1 shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents, and shall include at least the following:

(c) business continuity, such as backup management and disaster recovery, and crisis management;

(d) supply chain security, including security-related aspects concerning the relationships between each entity and its direct suppliers or service providers;" (**Chapter IV, Article 21**)

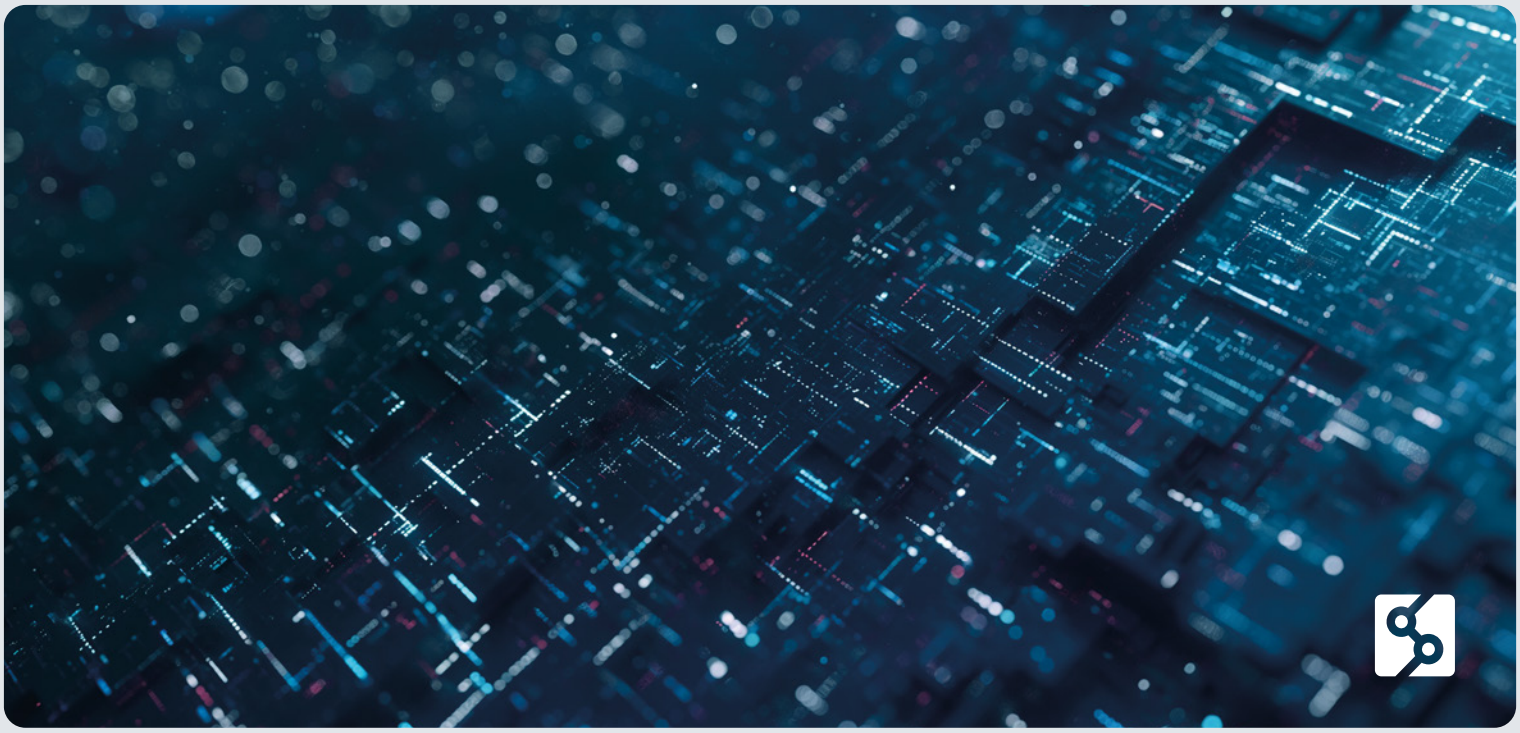
IP Fabric Solution

Any well-architected network system has built-in redundancies to ensure outages of connectivity interruptions (and potentially, business interruptions) are a rarity. But if you aren't regularly, consistently testing and validating these systems, you simply won't know if redundancies are actually working as expected until its too late. The nature of networks – especially large, enterprise, network-of-networks means every day brings change, both planned and unplanned. Change over time means potential degradation of your established security posture. Therefore, you must be able to view, understand, and access the following:

- **Critical Service Paths:** Show that you understand how services are dependent on network infrastructure client to workload.
- **Backups:** Store configuration backups for devices so they can be restored to new devices in case of failure, and use IP Fabric to prove to auditors that these backups are available.
- **Validation Of Business Continuity:** Show that services will continue to function after Disaster Recovery invocation.

The Network and Security Directive aims to ensure a unified standard of cybersecurity across the European Union. In the obligation for affected enterprises to comply, there is an opportunity to make use of automated network assurance to not only provide the controls and evidence necessary for NIS2, but also related security frameworks and regulations (e.g. **The Digital Operational Resilience Act** (DORA) for financial institutions or NIST2.0), by discovering, normalizing, and actioning all the state and configuration data needed from your cloud and network infrastructure.

With the elimination of manual data collection and analysis, and a means to proactively assure network security, stability, and resilience, the compliance burden is recontextualized. It becomes an opportunity to progress toward strategic transformation with the peace of mind that your network – the foundation of these pursuits – is properly secured.



About IP Fabric

IP Fabric is a vendor-neutral network assurance platform that automates the holistic discovery, verification, visualization, and documentation of large-scale enterprise networks, reducing the associated costs and required resources whilst improving security and efficiency.

It supports your engineering and operations teams, underpinning migration and transformation projects. IP Fabric will revolutionize how you approach network visibility and assurance, security assurance, automation, multi-cloud networking, and trouble resolution.

Don’t take our word for it

See how assurance can transform your approach to network management.

Access the demo

IP FABRIC

AUTOMATED NETWORK ASSURANCE PLATFORM

Support & Documentation
https://docs.ipfabric.io

HQ Office Boston
98 North Washington St.
Suite 407
Boston, MA 02114
United States

+1 617-821-3639

IP Fabric UK Ltd.
Gateley Legal,
1 Paternoster Square,
London,
England EC4M 7DX

+420 720 022 997

IP Fabric s.r.o.
Kateřinská 466/40
Praha 2 - Nové Město,
12000
Czech Republic

+420 720 022 997

ipfabric.io