IP FABRIC

# Automate Network Security to meet evolving PCI compliance standards



ipfabric.io

# Network assurance gives you the insights you need to proactively secure your growing attack surface

The Payment Card Industry Data Security Standard (PCI DSS) is a set of security standards designed to ensure that all companies that accept, process, store, or transmit credit card information maintain a secure environment. It is a global regulation and applies across industries (e-commerce, retail, hospitality, financial services); the mission is to protect valuable cardholder data. Established by the PCI Security Standards Council, PCI DSS outlines 12 key requirements, including maintaining firewalls, encrypting cardholder data (CHD), and regularly testing security systems.

Enterprise must comply to avoid hefty fines, and prevent potential legal issues and reputational damage due to data breaches. Maintaining this knowledge manually is not just slow and resource-heavy, but futile thanks to the continuously changing nature of modern enterprise networks. Automating the collection, documentation, standardization, and analysis of this not only saves the business valuable time and money but:

- **Shifts your approach to compliance from reactive to proactive, with the ability to set up automatic daily audits**
- **Removes the risk associated with network changes**
- **Democratizes access to key network insights that other teams need**

# 12 Requirements

Regulatory requirements are not necessarily strictly prescriptive as to how you achieve this operationally resilient state, but they all require proof of your processes, people, and technology that underlie your compliance program.

Producing the necessary documentation for an audit can feel like another burden thrust upon the network teams' ever-growing responsibilities. However, having this evidence at audit time - and all the time - drives stability, security, and business acceleration.

When you have an easy way to document assets, interdependencies, and traffic flows on a daily basis, everyone from the Board of directors to individual engineering benefit:

- → **Install and maintain a firewall configuration to protect cardholder data (CHD)**
- → **Do not use vendor-supplied defaults for system passwords and other security parameters**
- → **Protect stored CHD**
- → **Encrypt transmission of CHD across open, public networks**
- → **Use and regularly update anti-virus software or programs**
- → **Develop and maintain secure systems and applications**
- → **Restrict access to cardholder data by "business need to know"**
- → **Assign a unique ID to each person with computer access**
- → **Restrict physical access to CHD**
- → **Track and monitor all access to network resources and CHD**
- → **Regularly test security systems and processes**
- → **Maintain a policy that addresses information security for all personnel**

## Proactive Data Security with PCI-DSS 4.0 and beyond

The PCI DSS is a continually updated regulation, meaning that passing an audit this year does not guarantee that your same practices, processes, and security controls will be compliant when the standard is updated. Continually, the PCI DSS is updated to encourage a more proactive and ongoing approach to data security, prioritizing it as a continuous business activity, with more frequent testing, strengthened security, and streamlined compliance reporting. This is the case for **PCI DSS 4.0**.

Additionally, more flexibility has also been introduced, with the acknowledgment and support of alternate methods of securing payment data, as long as security objectives are reached. Keep up to date with the PCI Security Standards Council here: **PCI SSC.**

## Assuring a PCI Compliant IT Network Environment

Although PCI DSS extends beyond securing the network to cybersecurity activities, the network is still the foundation for all the applications that card holder data will be transmitted through, and accurate, complete, and up-to-date network intelligence must be available to satisfy PCI DSS compliance requirements.

Network assurance provides this key intelligence in three ways:

1. **Determine and Define Audit Scope**
2. **Inventory and Topology**
3. **End to End Path Tracing**

## Determine and Define Audit Scope

To prepare for a PCI audit, you must identify all parts of your network that interact with cardholder data (CHD) or sensitive authentication data (SAD). This includes components with "unrestricted connectivity" to systems handling CHD/SAD, which likely includes your network. Given the complexity and scale of modern networks, it's crucial to accurately scope what needs auditing. IP Fabric streamlines this process, reducing the time, cost, and complexity of your audit by identifying and documenting the necessary components to be assessed, according to user-prescribed parameters.

## Network Segmentation to Limit Audit Scope

You use network segmentation to limit the flow within your network by source, destination, or by traffic type. When dealing with the CHD environment in your network, using segmentation means a reduction in the number of users and devices that would have access to segments on which CHD is stored.

Since we can limit traffic flows based on certain networks (or subnetworks, as the case may be), we can limit the networks in which PCI data would traverse. Therefore, you can limit the scope of a PCI audit.

## Network Assurance to Validate and Prove Segmentation

IP Fabric's comprehensive discovery feature allows you to visualize your entire network estate through point-in-time network snapshots, which can be viewed according to different protocols holistically or by turning layers on or off to view traffic flows according to individual protocols.

To validate and prove this continuously, you can set custom rules for your network (called intent checks) and validate adherence to these rules every time a snapshot is run.

This provides continuous peace of mind and a historical track record of actively protecting cardholder data that touches the network, which is exactly what auditors want to see.

## What can I do with this proof?

The data collected from your network by IP Fabric includes the behavior of interconnection points between network segments and the deployed policy. It can be viewed in tabular form or network topology diagrams to ensure data is flowing through these enforcement points as planned. The data is also accessible via API, which can be integrated into other observability or security tools.

Leveraging single sign-on (SSO) and role-based access control (RBAC), granular permissions to view this data can be applied to anyone in an organization, ensuring that the relevant people (leadership, security, operations) can keep up to date on whether your network is correctly segmented with the appropriate level of security.

# Inventory & Topology

## Requirement 12.3

**12.3.4 Hardware and software technologies in use are reviewed at least once every 12 months, including at least the following:**

- Analysis that the technologies continue to receive security fixes from vendors promptly.
- Analysis that the technologies continue to support (and do not preclude) the entity's PCI DSS compliance.
- Documentation of any industry announcements or trends related to a technology, such as when a vendor has announced "end of life" plans for a technology.
- Documentation of a plan, approved by senior management, to remediate outdated technologies, including those for which vendors have announced "end of life" plans.

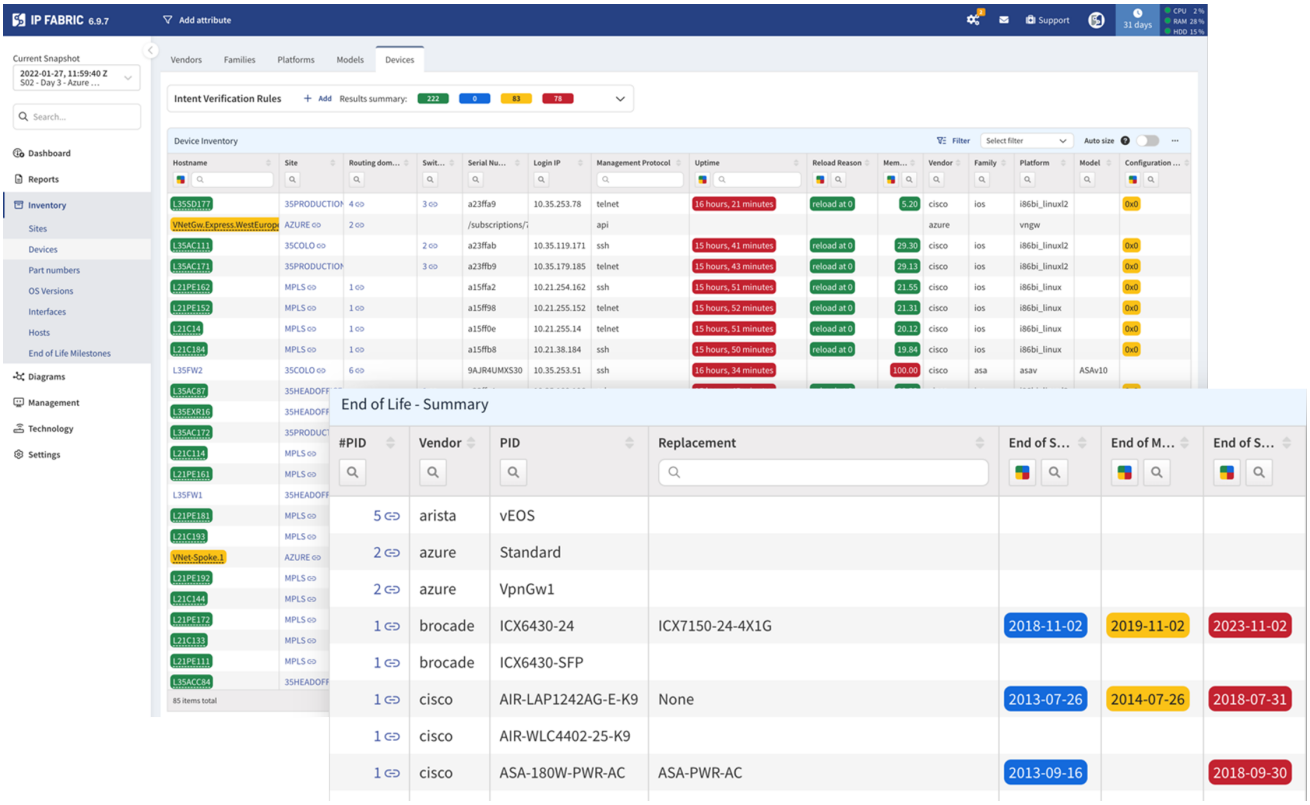
## Requirement 12.5

**12.5.1 An inventory of system components that are in scope for PCI DSS, including a description of function/use, is maintained and kept current.**

PCI DSS Requirement 12 emphasizes the importance of maintaining an up-to-date and well-documented inventory of network components and end-of-life (EoL) plans. Though it's the final requirement, starting with this is crucial to avoid unforeseen issues, much like securing a house requires knowing all access points. Specifically, Requirement 12.3.4 mandates that enterprises review their hardware and software technologies annually to ensure they receive security fixes and support PCI DSS compliance, with documented and senior management-approved EoL plans in place.

Additionally, Requirement 12.5.1 requires enterprises to maintain a current inventory of all system components within the PCI DSS scope, including their functions and uses, covering network devices, servers, virtual components, cloud elements, and software.

Pulling from published vendor information, IP Fabric compares your network data against End-of-Life (EoL) dates from hardware manufacturers, to put maintenance information in your hands.




***Examples of Inventory Information as Visualized in IP Fabric***

During the discovery process, IP Fabric connects to supported network devices—covering hundreds of models across various vendors—to collect configuration and state data, including make, model, and serial numbers. IP Fabric provides enterprises with up-to-date EoL data for every discovered device, enabling proactive lifecycle management planning. It also offers vendor-suggested replacements, ensuring seamless hardware transitions without network gaps.

Additionally, IP Fabric captures software data and allows the creation of intent rules to identify potential network issues, such as inconsistent OS updates. With the ability to schedule regular network snapshots, IP Fabric ensures that inventory data is always accurate and current, aligning with PCI DSS Requirement 12.5.1.

## Requirement 1.2

**1.2.3 An accurate network diagram(s) is maintained that shows all connections between the CDE and other networks, including any wireless networks.**

**1.2.4 An accurate data-flow diagram(s) is maintained that meets the following:**

- Shows all account data flows across systems and networks.
- Updated as needed upon changes to the environment.

## Requirement 1.3

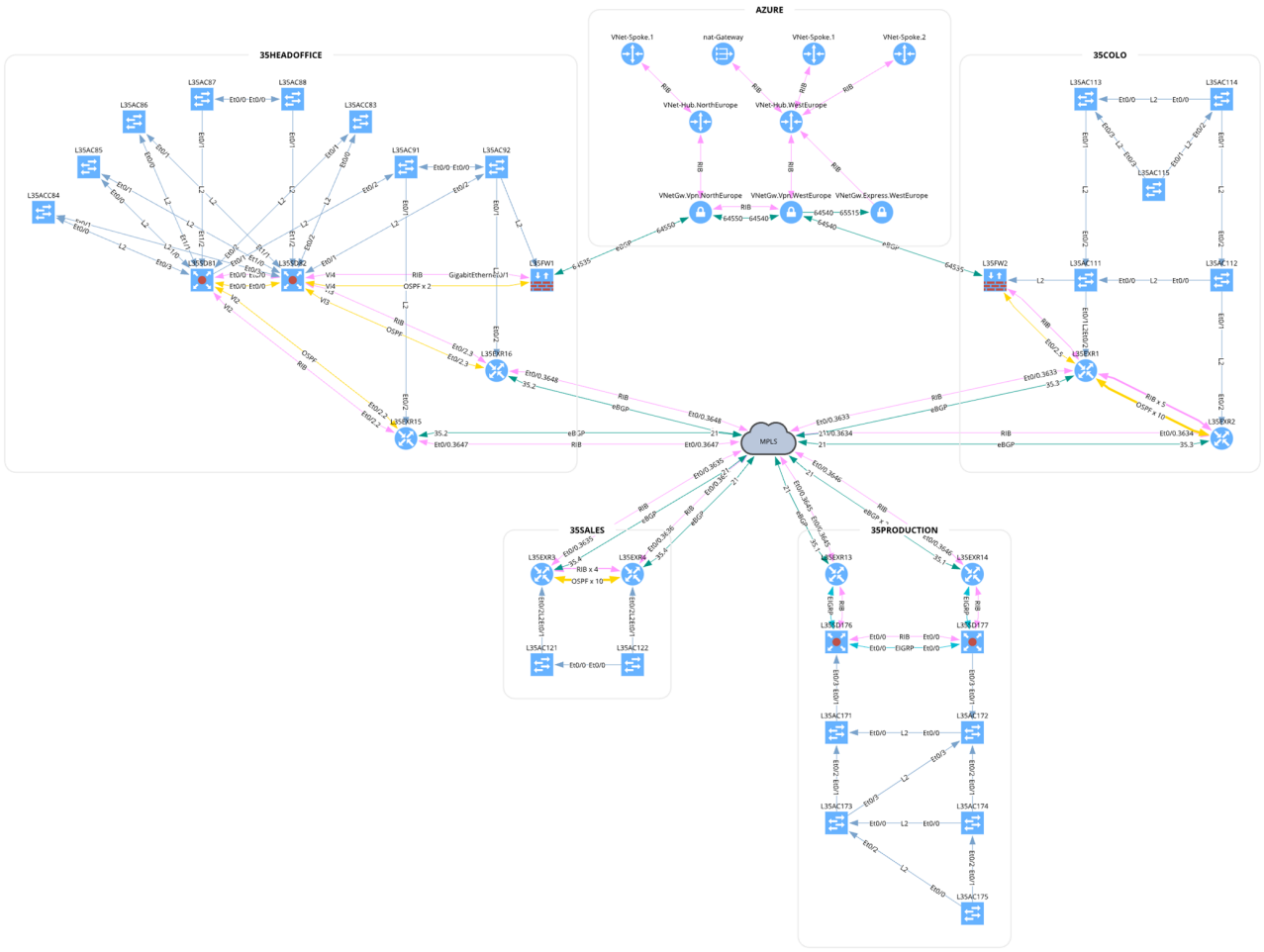
**1.3.1 Inbound traffic to the CDE is restricted as follows:**

- To only traffic that is necessary.
- All other traffic is specifically denied.

After completing a full inventory of your network with IP Fabric, the next step is to build a network topology. There are specific network topology requirements set out in PCI DSS; Requirements 1.2.3 and 1.2.4 mandate that enterprises maintain accurate network diagrams showing all connections between the card data environment and other networks. This includes wireless networks and mandates that these diagrams are updated when changes occur.

By leveraging Layer 2 (CDP, LLDP, MAC address tables) and Layer 3 (routing and ARP tables) data, IP Fabric automatically generates comprehensive logical diagrams that display connectivity across all layers. This helps satisfy Requirement 1.2.3 by ensuring accurate network diagrams that include Layer 1, 2, and 3 topologies.

Scheduling regular snapshots according to your preference means these diagrams are regularly updated, meeting Requirement 1.2.3.b, which mandates that network documentation be kept accurate. IP Fabric also supports Requirement 1.2.4 by allowing users to trace data paths through the network, either on-demand or automatically with each new snapshot, ensuring accurate and up-to-date data-flow diagrams.




*An example of network topology that can be leveraged for PCI*

# End-to-end path Tracing

IP Fabric's path tracing capabilities help satisfy several key PCI DSS requirements, particularly within requirements 1 and 11. Requirement 1.2.4 mandates accurate and up-to-date dataflow diagrams showing all account data flows across systems and networks, which IP Fabric supports through its dynamic tracing and diagramming features. Additionally, the tool aids in meeting requirements 1.3.1 and 1.3.2 by ensuring that only necessary inbound and outbound traffic to and from the card data environment (CDE) is allowed, with all other traffic explicitly denied.

## Requirement 1.4

**1.4.1: Firewalls are implemented between trusted and untrusted networks.**

**1.4.2: Inbound traffic from untrusted networks to trusted networks is restricted to communications with system components that are authorized to provide publicly accessible services or responses to communications initiated by system components in a trusted network; All other traffic is denied.**

**1.4.4: System components that store cardholder data are not directly accessible from untrusted networks.**

Requirements 1.4.1, 1.4.2, and 1.4.4 focus on implementing and verifying Network Security Controls (NSCs) between trusted and untrusted networks, ensuring that unauthorized traffic cannot traverse network boundaries or access cardholder data (CHD) directly from untrusted networks. IP Fabric's path-tracing capabilities facilitate the examination of network configurations and diagrams to ensure compliance with these standards.


*An end-to-end path as represented in IP Fabric*

## Requirement 11.4

**11.4.5 If segmentation is used to isolate the CDE from other networks, penetration tests are performed on segmentation controls as follows:**

- At least once every 12 months and after any changes to segmentation controls/methods.
- Covering all segmentation controls/methods in use.
- According to the entity's defined penetration testing methodology.
- Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.
- Confirming that the segmentation controls/methods are operational and effective, and isolate the CDE from all out-of-scope systems.
- Confirming effectiveness of any use of isolation to separate systems with differing security levels (see Requirement 2.2.3).
- Performed by a qualified internal resource or qualified external third party.
- Organizational independence of the tester exists (not required to be a QSA or ASV).

Requirement 11.4.5 requires penetration testing of segmentation controls to confirm that the CDE is sufficiently isolated from out-of-scope systems, with tests conducted at least annually or after any changes to segmentation methods. IP Fabric's pre- and post-change validation of network state supports this requirement by providing comprehensive insights into network traffic flows and segmentation integrity, helping to confirm the isolation and security of the CDE for your internal testing purposes, leaving no surprises for independent auditors to find.

## Beyond PCI – investing in compliance utomation as a business strategy

The network intelligence available in a network assurance platform is not only useful for PCI compliance but can be applied across multiple regulatory frameworks. Considering that in 2023, almost **70%** of service organizations said they need to demonstrate compliance or conformity to at least **six frameworks** spanning information security and data privacy taxonomies, it is prudent to invest in practical tools that can serve the business across multiple regulations ***(Source: Coalfire Compliance Report 2023).***

### Using network assurance eliminated months of manual data collection and analysis for compliance audits at Air Bank:

*«In the past, we had to spend months preparing network analysis reports for auditing firms, which are required on a regular basis. One of our biggest challenges was collecting all necessary data from our IT network infrastructure, analyzing this data, and identifying possible risks and corresponding impacts.*

*This investment in IP Fabric will return in less than six months. We recommend this tool to all financial service organizations that require regular audits & reporting.»*

## 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

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