TITANIA

PCI DSS 4.0 compliance reporting made easy

Your guide to the innovative new features in Nipper's PCI DSS Compliance Report

Report Highlights | PCI DSS 4.0

Nipper reveals the impact of non-compliances, calculating the risk to the network if the configuration is exploited, to drive risk-prioritized remediation.

A faster way to a secure and compliant Cardholder Data Environment

Demonstrating compliance with the Payment Card Industry Data Security Standard (PCI DSS) has typically involved manually mapping CDE network infrastructure device checks to requirements – a process which is inherently time-consuming and prone to error.

The latest versions of Nipper solutions deliver a new, dedicated PCI DSS 4.0 compliance report that changes all this. Providing an automated way for ISAs and QSAs to:

- Assess network segmentation effectiveness
- Validate compliance with evidence
- Automate security as a continuous process

Risk Focus | Evidence | Best Practice

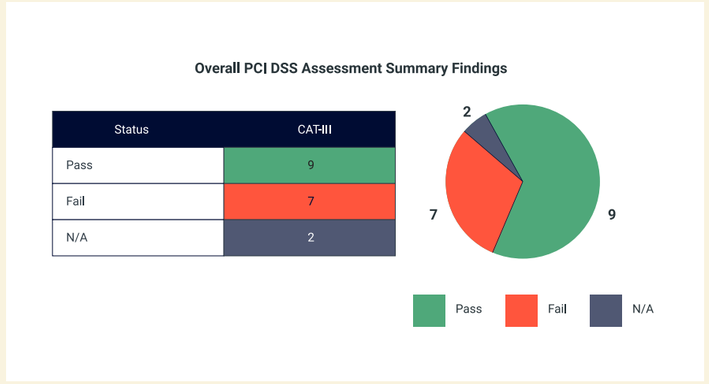
Commercial CNI organizations that are mandated to evaluate and report their compliance will benefit from:

- **Automated requirements mapping of PCI DSS network device checks with drill down to testing procedures.**
- **An assessor-ready report providing evidence for both passed and failed checks and a risk-prioritzed view of non-compliances.**
- **Device-specific guidance on how to fix misconfigurations – including command line scripts in some cases – to decrease mean time compliance risks.**

Automate PCI DSS 4.0 compliance assessments for every router, switch and firewall in your CDE - and beyond.

Nipper automatically analyzes any PCI DSS non-compliances it identifies, to reveal the impact to the device if the configuration is exploited, as well as the ease of exploit, and ease of fix, providing an informed view of the device's risk posture to drive risk-prioritized remediation

To assure continuous PCI DSS compliance, Nipper Resilience leverages the precision of Nipper to assess every router,switch and firewall in the CDE, on an up to hourly basis, or whenever configuration changes are detected.



1. At-a-glance compliance posture

Innovation

- Nipper checks are automatically mapped to PCI DSS 4.0 requirements.
- Drill down from the summary to the testing procedure to examine the results.

Benefit

Get a high-level overview of the PCI DSS assessment results, summarizing passes, fails, and any checks that are not applicable to the specific devices that have been assessed.

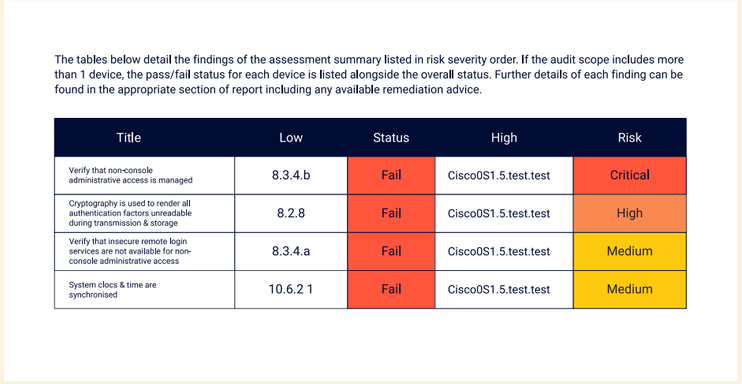
2. Potential impact summary

Innovation

- Nipper automatically prioritizes findings based on ease of exploitation and impact to the network if exploited.
- Non-compliances are prioritized based on RAG status, reflecting risk criticality.

Benefit

Understand the potential impact of non-compliances with a color-coded display that ranks findings based on vulnerability risk and ease of exploitation.



The tables below detail the findings of the assessment summary listed in risk severity order. If the audit scope includes more than 1 device, the pass/fail status for each device is listed alongside the overall status. Further details of each finding can be found in the appropriate section of report including any available remediation advice.

Title	Low	Status	High	Risk
Verify that non-console administrative access is managed	8.3.4.b	Fail	Cisco0S1.5.test.test	Critical
Cryptography is used to render all authentication factors unreadable during transmission & storage	8.2.8	Fail	Cisco0S1.5.test.test	High
Verify that insecure remote login services are not available for non-console administrative access	8.3.4.a	Fail	Cisco0S1.5.test.test	Medium
System clocs & time are synchronised	10.6.2 1	Fail	Cisco0S1.5.test.test	Medium

3. Risk-prioritized findings

Innovation

- Nipper then lists the detail of each of the assessment findings (pass and fail).
- And identifies the specific devices affected that carry a non-compliance risk.

Benefit

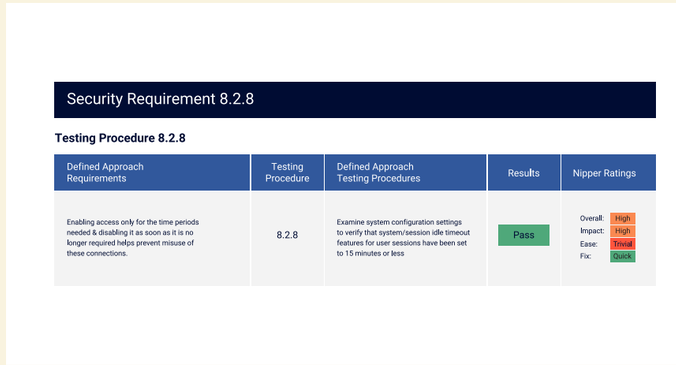
Drill down to passes and failures prioritizing the most critical non-compliances first and identifying the devices that require remediating action.

Five innovative new report features

Streamlining compliance reporting so you can focus on fortifying CDE security

Delivering so much more than accurate compliance reporting, Nipper's new PCI DSS 4.0 report is packed with powerful insights to help embed the risk focus, evidence and best practice required to deliver security from compliance.

Here's your guide to risk-prioritizing non-compliances for remediation, tracking changes between audits, and driving further investigation into whether drift was accidental or deliberate.



Security Requirement 8.2.8

Testing Procedure 8.2.8

Defined Approach Requirements	Testing Procedure	Defined Approach Testing Procedures	Results	Nipper Ratings
Enabling access only for the time periods needed & disabling it as soon as it is no longer required helps prevent misuse of these connections.	8.2.8	Examine system configuration settings to verify that system/session idle timeout features for user sessions have been set to 15 minutes or less	Pass	Overall: High Impact: High Ease: Trivial Fix: Quick

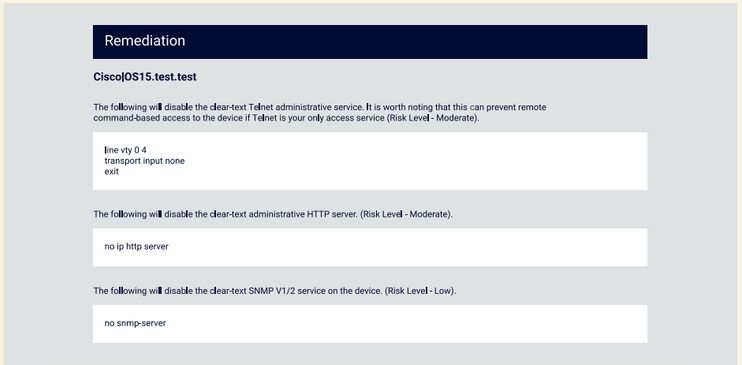
4. Evidence-based analysis

Innovation

- Nipper's risk analysis of each non-compliance harnesses networking know-how to determine the ease of exploit and potential impact to security.
- The 'fix rating' automatically provides an 'ease of fix guide' for each non-compliance found.

Benefit

For each device tested, view findings against applicable PCI DSS requirements, with an explanation of the testing procedure and Nipper's detailed risk assessment to validate compliance posture.



Remediation

CiscoIOS15.test.test

The following will disable the clear-text Telnet administrative service. It is worth noting that this can prevent remote command-based access to the device if Telnet is your only access service (Risk Level - Moderate).

```
line vty 0 4
transport input none
exit
```

The following will disable the clear-text administrative HTTP server. (Risk Level - Moderate).

```
no ip http server
```

The following will disable the clear-text SNMP V1/2 service on the device. (Risk Level - Low).

```
no snmp-server
```

5. Remediation advice

Innovation

- Nipper determines exactly how the configuration does not comply with PCI DSS 4.0 requirements, and how the risk can be mitigated.
- Command line instructions are provided, where possible, to reduce the mean time to remediate risks.

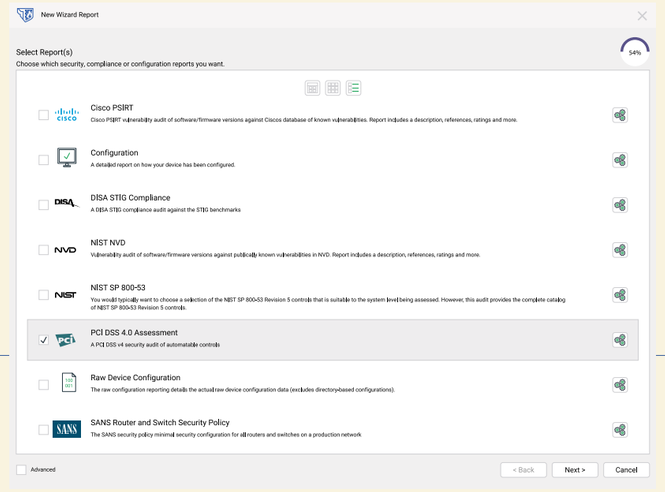
Benefit

Reduce mean time to remediate vulnerabilities with detailed advice on how to mitigate non-compliances and improve PCI DSS compliance posture.

Whether you are an ISA or QSA looking to automate periodic PCI DSS 4.0 compliance assessments or for continuous compliance assurance – Titania has a solution for you.

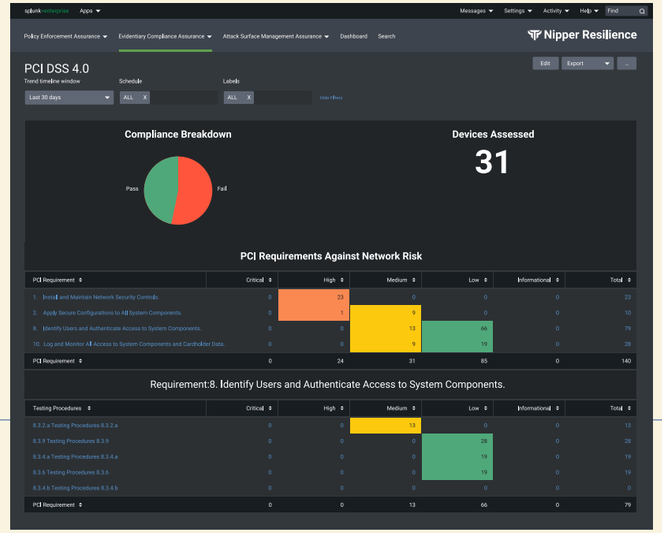
On-demand compliance with Nipper

Auditors and external assessors choose Nipper to quickly verify configurations are secure and/or meet regulatory compliance standards, reducing their audit times by up to 80%.



Validate networks are secure and compliant with Nipper Resilience

Deployed by SOCs to assure the security and compliance posture of network infrastructure, Nipper Resilience also adds a transformative proactive security layer to the NOC tech stack. Nipper Resilience integrates with SIEM, SOAR, ITSM and GRC solutions.

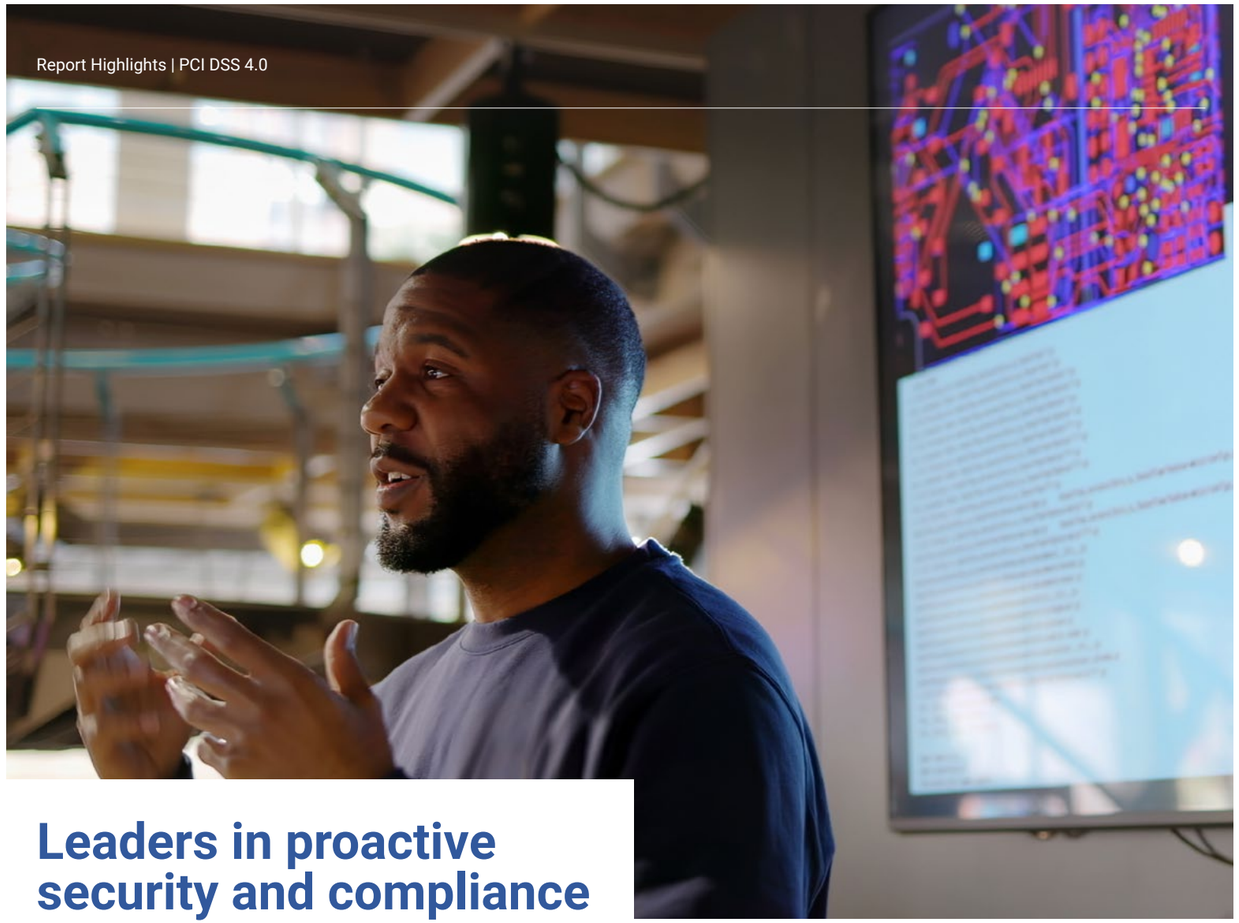


Splunk dashboard visualizing Nipper Resilience's PCI DSS 4.0 assessment of CDE

Request a demo to see for yourself how Nipper solutions will be of value to you. **titania.com/try/demo**

Diagrams for illustrative purposes only.

Report Highlights | PCI DSS 4.0



Leaders in proactive security and compliance assurance

Titania is a world leader in continuous configuration drift analysis for routers, switches and firewalls, helping NOCS and SOCs around the world build configuration confidence in their network infrastructure. Automating an inside-out view of security and compliance vulnerabilities across network infrastructure, Nipper solutions enable risk-prioritized remediation to shut down attack vectors that pose real-world threats to the enterprise. And now, for the first time, the solutions automate evidence-based compliance reporting against the new PCI DSS 4.0 standard.

Why Titania

At the forefront of proactive network security, Titania's multi-award-winning vulnerability and exposure management solutions are trusted by NOC, SOC, Incident Response and Cyber Protection teams to safeguard critical infrastructure and commercial entities, globally.

For organizations ready for real-time visibility and analysis of every network change, Titania enables them to get ahead of threats, segmentation violations, and potential network disruptions. Titania's scheduled network posture and device vulnerability assessments also help to enhance attack surface security and demonstrate compliance. Ensuring there's an industry-leading solution for every organization, wherever they are on the journey to network readiness and resilience.

USA
Suite 600, 2451 Crystal Dr, 6th Floor,
Arlington, VA 22202

UK
167-169 Great Portland Street,
London, England, W1W 5PF

TITANIA
www.titania.com